José Sousa Pinto
Universidade de Aveiro, 1999

Tópicos de Matemática Discreta

Texto de Apoio - 2005/2006

♢♢ • ♢♢

Departamento de Matemática
UNIVERSIDADE DE AVEIRO

Estudar Matemática

...

em memória de Sousa Pinto

O bom desempenho em qualquer disciplina de Matemática depende em primeira análise

1. da capacidade de ler atenta e interessadamente os textos disponíveis, por forma a poder interpretar correcta e rigorosamente as matérias neles expostas. Este resultado não se consegue, em geral, com uma só leitura; frequentemente são necessárias duas, três ou mais leituras variando este número de leitor para leitor. Não se aprende matemática sem LER Matemática!
2. da capacidade de escrever correctamente em Português sobre temas de Matemática, usando uma linguagem precisa e clara. Na apresentação da resolução de um problema

   > *devem ser enunciados com precisão os resultados usados; o rigor das demonstrações e o cuidado prestado à sua redacção são elementos importantes para a apreciação das respostas.*

   Não responde correctamente a uma questão de Matemática quem se limita a efectuar uma série de cálculos sem explicar a sua razão de ser, as suas origens (próximas) e para que servem no respectivo contexto. Não se aprende Matemática sem ESCREVER Matemática!

Quem comunica por escrito deverá fazê-lo em LÍNGUA PORTUGUESA, de uma forma que possa ser claramente entendida por qualquer pessoa minimamente familiarizada com as matérias sobre as quais discursa. É estrita obrigação de quem comunica fazê-lo de forma correcta dentro da *"norma"* da língua portuguesa. Isto significa, em particular, que

- devem ser usadas frases completas e gramaticalmente correctas, por forma a serem produzidas afirmações claras relativamente às quais se possa dizer sem qualquer ambiguidade que são verdadeiras ou falsas (mas não ambas as coisas).
- não deve ser usada notação matemática incorrecta nem formas de escrita estenográfica – as palavras existem para facilitar a comunicação e a sua grafia não deve, por isso, ser adulterada. É preciso respeitar não só a sintaxe, mas também a ortografia e as regras de pontuação da língua portuguesa. A *"norma"* da língua portuguesa é do conhecimento geral dos portugueses (letrados) – os dialectos (naturais ou artificiais) só são reconhecidos por alguns, geralmente poucos!
- deve explicar-se sempre o que se está a fazer.
- devem ligar-se as ideias e as fórmulas matemáticas por partículas adequadas que explicitem o encadeamento dos raciocínios feitos.
- é preciso ter muita atenção com a apresentação: *se o trabalho realizado revelar falta de cuidado de sentido estético e de rigor, não se justifica que alguém gaste tempo para tentar entender o seu conteúdo.* Além disso, qualquer texto será sempre valorizado pela originalidade da exposição!

Quem apresenta um trabalho não pode partir do princípio que quem o está a ler entende o que realmente se passou na mente de quem o escreveu. A resposta (escrita) a um problema é um diálogo com um interlocutor invisível. A comunicação escrita pode não ser simples, mas é certamente da maior importância para a vida do dia a dia de quem tem de agir em sociedade. Dispor de boa capacidade de comunicação escrita é muitas vezes de importância crucial para um bom desempenho em muitas situações da vida real: a comunicação escrita (assim como a oral) aproxima-se muito de uma arte e é como tal que deve ser encarada, mesmo em textos científicos!

José Sousa Pinto, Universidade de Aveiro, 1999

Índice Geral

Capítulo 1

Introdução à Lógica e Teoria de Conjuntos

1.1 Teoria (intuitiva) de Conjuntos

A teoria dos conjuntos foi criada relativamente recentemente por Georg Cantor (1845-1918) que definiu *conjunto* como sendo *"uma colecção de objectos claramente distinguíveis uns dos outros, chamados elementos, e que pode ser pensada como um todo"*. É claro que se não se tiver definido previamente o que se entende por *"colecção"* esta não será uma definição rigorosa para o termo *"conjunto"*. A fim de evitar definições circulares, **conjunto** e **elemento** de um conjunto são duas noções que não se definem; um conceito quando é definido, é-o em termos de outros conceitos mais simples e não é habitual considerar conceitos logicamente mais simples que os de *"conjunto"* e *"elemento de um conjunto"*. Conjunto e elemento de um conjunto são assim termos primitivos que se admite serem do conhecimento de toda a gente (pelo menos de toda a gente que estuda Matemática). Esta secção destina-se a relembrar conceitos baseados na noção de conjunto aqui considerado de forma intuitiva. Trata-se de um conceito de extraordinária importância pois grande parte da matemática dos nossos dias pode ser construída a partir dele. Por este facto, o estudo da construção de conceitos de matemática a partir da noção primitiva de conjunto é muitas vezes se designado por Fundamentos de Matemática.

Um conjunto designa-se geralmente por uma letra maiúscula, [1] reservando-se as letras minúsculas para os seus elementos. A expressão simbólica

$$x \in A$$

significa que *"x é elemento de A"*. A negação de $x \in A$ representa-se simbolicamente por

$$x \notin A$$

e lê-se *"x não pertence a A"* (ou "*x não é elemento de A*"). Um conjunto pode ser descrito em **extensão** (quando o número dos seus elementos for finito e suficientemente pequeno) enumerando explicitamente todos os seus elementos colocados entre chavetas e separados por vírgulas ou em **compreensão**, enunciando uma propriedade caracterizadora dos seus elementos (isto é, uma propriedade que os seus e só os seus elementos possuam).

Exemplo 1.1 :

(1) Conjunto das vogais

$$\mathbf{V} = \{a, e, i, o, u\}$$

descrito em extensão;

(2) Conjunto dos números naturais pares

$$\mathbf{P} = \{p \in \mathbb{N} : p = 2q \text{ para algum } q \in \mathbb{N}\}$$

descrito em compreensão.

Conjunto universal e conjunto vazio. Intuitivamente poderia parecer razoável que se considerasse como conjunto qualquer colecção de objectos (reais ou imaginários). Tal atitude, porém, conduz a situações paradoxais, como se deu conta o filósofo inglês Bertrand Russel, por volta de 1901.

Bertrand Russel começa por observar que se se adoptar a concepção intuitiva de conjunto então pode dizer-se que alguns conjuntos são membros de si próprios enquanto outros não o são. Um conjunto de elefantes, por exemplo, não é um elefante e, portanto, não é um elemento de si próprio; no entanto, o conjunto de todas as ideias abstractas é, ele próprio, uma ideia abstracta, pelo que pertence a si próprio. As propriedades *"ser membro de si próprio"* e *"não ser membro de si próprio"* parecem assim ser propriedades

[1] Não tem que ser assim: trata-se de uma mera convenção para facilitar o estudo.

perfeitamente adequadas para definir conjuntos. Mas, como se verá, estas propriedades conduzem à criação de um paradoxo.

Suponha-se (se possível) que se define o conjunto $\mathcal{A}$ como sendo o conjunto de todos os conjuntos que não são membros de si próprios, isto é,

$$\mathcal{A} = \{X : X \notin X\}$$

Coloca-se então a questão de saber se $\mathcal{A}$ é ou não elemento de si próprio. Se $\mathcal{A}$ não for membro de si próprio, $\mathcal{A} \notin \mathcal{A}$, então satisfaz a propriedade definidora de $\mathcal{A}$ e, portanto, $\mathcal{A} \in \mathcal{A}$; se $\mathcal{A}$ pertence a si próprio, $\mathcal{A} \in \mathcal{A}$ então não satisfaz a propriedade definidora de $\mathcal{A}$ e, portanto, $\mathcal{A} \notin \mathcal{A}$. De cada uma das possíveis hipóteses pode deduzir-se a sua negação, o que constitui um paradoxo.

Para eliminar possibilidades deste tipo supor-se-á, de ora em diante, que os conjuntos considerados são todos constituídos por elementos de um conjunto $\mathcal{U}$ suficientemente grande, chamado **conjunto universal** ou **universo** do discurso.

A ideia de um conjunto universal estará sempre presente mesmo quando não seja explicitamente mencionado. Em Matemática há conjuntos que constituem muito frequentemente os universos do discurso sendo, por isso, conveniente dispôr de nomes para eles. Alguns exemplos de tais conjuntos, dos mais importantes, são:

$$\begin{array}{rcl} \mathbb{R} & = & \{x : x \text{ é um número real}\} \\ \mathbb{Q} & = & \{x : x \text{ é um número racional}\} \\ \mathbb{Z} & = & \{x : x \text{ é um número inteiro}\} \\ \mathbb{N} & = & \{0, 1, 2, 3, \ldots\} \end{array}$$

Os símbolos $\emptyset$ ou $\{\ \}$ usam-se para denotar o **conjunto vazio** (conjunto sem elementos) que pode ser descrito em compreensão por $\{x : x \neq x\}$.

Conjuntos finitos e infinitos. Embora não seja este o lugar adequado para dar definições rigorosas sobre os termos "finito" e "infinito", procurar-se-á esclarecer, por meio de alguns exemplos, o seu significado.

Um conjunto diz-se finito se for possível contar os seus elementos, ou seja, se for o conjunto vazio ou se for possível estabelecer uma correspondência bijectiva entre os seus elementos e os elementos de um conjunto da forma $\{1, 2, 3, \ldots, n\}$ para algum $n \in \mathbb{N}$. Dir-se-á infinito no caso contrário. O conjunto dos números inteiros positivos inferiores a 100 é um conjunto finito

enquanto que o conjunto de todos os números inteiros positivos é um conjunto infinito. De modo semelhante, é finito o conjunto de todos os planetas do sistema solar ou o conjunto de todos os números primos menores que 10^{10^3}; pelo contrário, como mais à frente se mostrará, é infinito o conjunto de todos os números primos.

Se A for um conjunto finito, designar-se-á por **cardinalidade** de A o número dos seus elementos, o qual se representa por $\mathbf{card}(A)$. Um conjunto com cardinalidade igual a 1 diz-se **singular**.

Quando um conjunto é infinito, é impossível defini-lo em extensão (indicando explicitamente os seus elementos); logo, se um conjunto puder ser definido em extensão, então certamente será um conjunto finito. Por vezes para definir certos conjuntos infinitos usa-se uma notação parecida com a definição de um conjunto em extensão: é o caso de

$$\mathbb{N} \;=\; \{0, 1, 2, 3, \ldots\}$$

Note-se contudo que as reticências representam a quase totalidade dos elementos de $\mathbb{N}$ qualquer que seja o número de elementos que aparecem no início.

Igualdade de conjuntos.

Dois conjuntos são iguais se e só se tiverem os mesmos elementos.

Se um conjunto A for **igual** a um conjunto B escreve-se $A = B$. Para verificar se dois conjuntos são iguais basta verificar se todo o elemento de A é elemento de B e se todo o elemento de B é elemento de A. Se todo o elemento de A for também elemento de B (independentemente do facto de todo o elemento de B poder ser ou não elemento de A) dir-se-á que o conjunto A **está contido** no conjunto B, o que se denota por $A \subseteq B$; neste caso também se diz que A é subconjunto de B. Se os conjuntos A e B forem iguais então ter-se-á $A \subseteq B$ e, simultaneamente, $B \subseteq A$; reciprocamente, se $A \subseteq B$ e $B \subseteq A$ se verificarem simultaneamente então tem-se $A = B$. Se for $A \subseteq B$ e $A \neq B$ dir-se-á que A é um subconjunto próprio ou uma parte própria de B e escreve-se $A \subset B$. De acordo com estas definições resulta que quaisquer que sejam os conjuntos A e B

$$\emptyset \subseteq A, \quad A \subseteq A, \quad A = B \text{ se e só se } [\, A \subseteq B \text{ e } B \subseteq A \,]$$

Considere-se a prova de, por exemplo, $\emptyset \subseteq A$ qualquer que seja o conjunto A. A única forma de mostrar que esta inclusão é falsa é verificar que $\emptyset$

possui um elemento que não pertence a A; ora como $\emptyset$ não possui elementos então aquela relação verifica-se sempre.

Exercícios 1.1.1

1. *Mostrar que os conjuntos $\emptyset$, $\{\emptyset\}$ e $\{\{\emptyset\}\}$ são distintos dois a dois.*
2. *Mostrar que se A for um subconjunto do conjunto vazio então $A = \emptyset$.*
3. *Dado um conjunto arbitrário A,*
   (a) *será A membro do conjunto $\{A\}$?*
   (b) *será $\{A\}$ membro do conjunto $\{A\}$?*
   (c) *será $\{A\}$ um subconjunto de $\{A\}$?*
4. *Dados os conjuntos*

$$\begin{array}{rcl} A & = & \{5, 10, 15, 20, \ldots\} \\ B & = & \{7, 17, 27, 37, \ldots\} \\ C & = & \{300, 301, 302, \ldots, 399, 400\} \\ D & = & \{1, 4, 9, 16, 25, 36, 49, \ldots\} \\ E & = & \{1, 1/2, 1/4, 1/8, 1/16, \ldots\} \end{array}$$

   indicar, para cada um deles, uma propriedade que o especifique completamente.
5. *Indicar quais dos conjuntos que se seguem são iguais:*

$$\begin{array}{rcl} A & = & \{-1, 1, 2\} \\ B & = & \{-1, 2, 1\} \\ C & = & \{0, 1, 2\} \\ D & = & \{2, 1, -1, -2\} \\ E & = & \{x : x^2 = 4 \text{ ou } x^2 = 1\} \end{array}$$

6. *Determinar em extensão os seguintes conjuntos*

$$\begin{array}{rcl} A & = & \{x \in \mathbb{N} : 8 = x + 3\} \\ B & = & \{x \in \mathbb{N} : (x-2)(x-5) = 0\} \\ C & = & \{x \in \mathbb{N} : x^2 + 22 = 13x\} \\ D & = & \{x \in \mathbb{N} : \sqrt{5x-1} + \sqrt{3x-2} = 3\} \\ E & = & \{x \in \mathbb{N} : (x+1)(x+2) < 11\} \end{array}$$

7. *Dizer quais dos conjuntos que se seguem são finitos e quais são infinitos.*
   (a) *O conjunto das linhas do plano que são paralelas ao eixo xx'.*
   (b) *O conjunto das letras do alfabeto.*
   (c) *O conjunto dos múltiplos de 5.*
   (d) *O conjunto dos animais existentes na Terra.*
   (e) *O conjunto das raízes da equação*

$$x^{38} + 42x^{23} - 17x^{18} - 2x^5 + 19 = 0$$

   (f) *O conjunto das circunferências centradas na origem.*

1.1.1 Operações com conjuntos

Sendo A, B dois conjuntos, denota-se por $A \cup B$ a **união** (ou **reunião**) de A com B, que é o conjunto cujos elementos são os elementos de A e os elementos de B. Mais geralmente, se $A_1, A_2, \ldots, A_n$ forem conjuntos então a sua união

$$\cup_{i=1}^{n} A_i \equiv A_1 \cup A_2 \cup \ldots \cup A_n$$

é o conjunto constituído pelos elementos que pertencem pelo menos a um dos conjuntos $A_i, i = 1, 2, \ldots, n$. Simbolicamente pode traduzir-se esta definição por

$$\cup_{i=1}^{n} A_i = \{x : x \in A_i \text{ para algum } i = 1, 2, \ldots, n\}$$

A **intersecção** de dois conjuntos A e B, denotada por $A \cap B$, é o conjunto cujos elementos pertencem simultaneamente a A e B. Analogamente, se $A_i, i = 1, 2, \ldots, n$, forem conjuntos então

$$\begin{aligned} \cap_{i=1}^{n} A_i &\equiv A_1 \cap A_2 \cap \ldots \cap A_n \\ &= \{x : x \in A_i \text{ para todo } i = 1, 2, \ldots, n\} \end{aligned}$$

As definições de união e intersecção de conjuntos estendem-se, de forma natural, a famílias infinitas de conjuntos. Assim, dada uma família arbitrária de conjuntos $\{A_\alpha\}_{\alpha \in I}$ (onde I denota um conjunto de índices)

$$\begin{aligned} \cup_{\alpha \in I} A_\alpha &= \{x : x \in A_\alpha \text{ para algum } \alpha \in I\} \\ \cap_{\alpha \in I} A_\alpha &= \{x : x \in A_\alpha \text{ para todo } \alpha \in I\} \end{aligned}$$

Dois conjuntos A e B dizem-se **disjuntos** se e só se for $A \cap B = \emptyset$, isto é, se não possuirem elementos comuns.

A **diferença** de A e B é o conjunto $A \backslash B$ definido por

$$A \backslash B = \{x : x \in A \text{ e } x \notin B\}$$

ou seja é o conjunto constituído pelos elementos de A que não pertencem a B. Se, em particular, se fizer $A = \mathcal{U}$, o universo do discurso, então ao conjunto $\mathcal{U} \backslash B = \{x : x \notin B\}$ dá-se o nome de **conjunto complementar** de B e denota-se por B^c.

Conjunto das partes de um conjunto. Podem construir-se conjuntos cujos elementos são eles próprios, no todo ou em parte, conjuntos. Assim,

por exemplo, a letra x, o conjunto $\{a, b\}$, o conjunto $\{\emptyset\}$ e o número 4 podem constituir um novo conjunto que é o seguinte

$$\{x, \{a, b\}, \{\emptyset\}, 4\}$$

Dado um conjunto arbitrário, é possível construir novos conjuntos cujos elementos são partes do conjunto inicial. Em particular, sendo A um conjunto qualquer, denota-se por $\mathcal{P}(A)$ o conjunto constituído por todos os subconjuntos (próprios ou impróprios) de A, isto é,

$$\mathcal{P}(A) \;=\; \{X : X \subseteq A\}$$

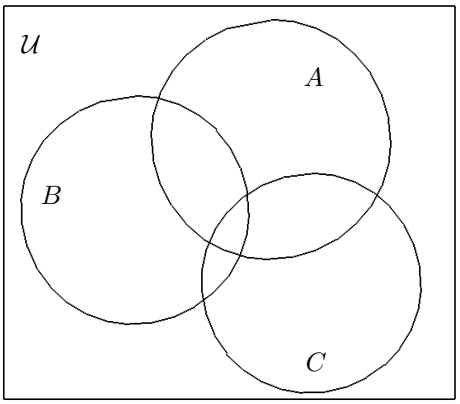
Seja, por exemplo, $A = \{a, b, c\}$; então

$$\mathcal{P}(A) \;=\; \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

é o conjunto das partes de A, com cardinalidade igual a $8 = 2^3$.

Diagramas de Venn. As operações com conjuntos podem ser representadas pictoricamente pelos chamados diagramas de Venn que, embora não sirvam de prova formal, permitem visualizar e conjecturar muitos resultados sobre conjuntos.

O conjunto universal é representado pelo interior de um rectângulo no qual são representados por círculos os vários conjuntos com os quais se está a operar. Assim, por exemplo,



é um diagrama de Venn com três conjuntos A, B e C onde se pode realçar (com tracejado) o resultado das várias operações realizadas com eles.

Nota 1.2 Os diagramas de Venn tornam-se de difícil ou mesmo impossível utilização quando o número de conjuntos a considerar for superior ou igual a 4.

Exercícios 1.1.2 :

1. *Qual é a cardinalidade dos seguintes conjuntos*

$$\{1, 2, \emptyset\}, \quad \{1, \{1, \emptyset\}\}, \quad \{\emptyset\}, \quad \{1\}, \quad \{\{1\}\}$$

2. *Determinar a cardinalidade do conjunto*

$$S = \left\{ \frac{p}{q} : p, q \in \mathbb{N}_1 \wedge p, q \leq 10 \right\}$$

3. *Seja* $\mathcal{U} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *o conjunto universal. Dados os conjuntos* $A = \{1, 3, 5, 7\}$, $B = \{2, 3, 4, 5, 6\}$ *e* $C = \{0, 2, 4, 6, 8\}$, *definir em extensão os conjuntos*

$$A \cap B, \ B \cup C, \ B \cup C^c, \ A \cap (B \cup C),$$
$$(A \cap B) \cup (A \cap C), \ (A \cap B) \cup C, \ A \cup \emptyset, \ B \cap \emptyset, \ A \cap C, \ \mathcal{U}^c$$

4. *Sejam* A, B *e* C *três conjuntos quaisquer contidos no universo* $\mathcal{U}$. *Verificar as seguintes igualdades:*
   (a) $A \cup A^c = \mathcal{U}$
   (b) $A \cap A^c = \emptyset$
   (c) $A \cap B \subseteq A$
   (d) $A \cup B \supseteq A$
   (e) $(A^c)^c = A$

5. *Em que circunstâncias são verdadeiras as igualdades que se seguem*

$$\begin{aligned} A \cup B &= A \cap B \\ A \cap B^c &= A \\ A &\subseteq \emptyset \\ A \cap B &= B \\ (A \cup B) \cap B^c &= A \\ (A \cap B^c) \cup B &= A \cup B \end{aligned}$$

6. *O facto de ser* $A \cup B = D$ *implica que seja* $D \backslash B = A$? *Se não, o que pode concluir-se do facto de ser* $A \cup B = D$ *e* $D \backslash B = A$?

7. *Sejam* A *e* B *dois subconjuntos do universo* $\mathcal{U} = \{1, 2, 3, 4, 5, 6\}$ *tais que*

$$A \cup B = \{1, 2, 3, 4\}, \ A \cap B = \{3\}, \ A \backslash B = \{1, 2\}, \ A^c = \{4, 5, 6\}$$

   Determinar A, B *e* $B \backslash A$.

8. *Mostrar que*
   (a) *se* $A \subseteq C$ *e* $B \subseteq C$ *então* $A \cup B \subseteq C$.
   (b) *se* $C \subseteq A$ *e* $C \subseteq B$ *então* $C \subseteq A \cap B$.
9. *Determinar os conjuntos das partes dos conjuntos*
$$A = \{1\}, \quad B = \{1, 2\} \quad c = \{1, 2, 3\}$$
10. *Sendo* $M = \{1, 2, 3, 4\}$ *determinar* $\{x \in M : x \notin \emptyset\}$. *Quantos elementos terá o conjunto das partes de* M*?*
11. *Descrever os elementos do conjunto* $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.
12. *Mostrar que*
   (a) $A \supseteq B$ *implica* $\mathcal{P}(A) \supseteq \mathcal{P}(B)$
   (b) $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$
   (c) $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$
   Em que condições se verificam as igualdades nas duas últimas alíneas?
13. *Determinar o conjunto das partes do conjunto das partes do conjunto* $\{a\}$.

Concluir-se-á esta secção com os dois teoremas que se seguem que relacionam várias das operações que se podem realizar com conjuntos.

Teorema 1.3 (Propriedade distributiva.) *Sendo* A, B, C *três conjuntos arbitrários, ter-se-á*
(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Demonstração: Uma forma de mostrar a veracidade destas igualdades consiste em verificar que cada um dos seus membros está contido no outro. Far-se-á esta verificação para a primeira alínea deixando a outra a cargo do leitor interessado, como exercício.

Para mostrar que se tem $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ é suficiente verificar que qualquer elemento $t \in A \cap (B \cup C)$ também pertence ao conjunto $(A \cap B) \cup (A \cap C)$. De facto, da hipótese resulta que t pertence a A e a $B \cup C$ ou seja que t pertence a A e t pertence a B ou t pertence a C. Então t pertence a A e a B, isto é, $t \in A \cap B$, ou t pertence a A e a C, isto é, $t \in A \cap C$. Consequentemente, $t \in (A \cap B) \cup (A \cap C)$ e, portanto,

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \tag{1.1}$$

como se pretendia mostrar.

Suponha-se agora que $s \in (A \cap B) \cup (A \cap C)$. Então $s \in A \cap B$ ou $s \in A \cap C$, ou seja, s pertence simultaneamente a A e B ou s pertence simultaneamente a A e C. Portanto, s pertence a A e pertence a B ou a C, donde resulta

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \tag{1.2}$$

De (1.1) e (1.2) resulta a igualdade pretendida. □

Exercícios 1.1.3 *Verificar a demonstração do teorema 1.3 usando um diagrama de Venn apropriado.*

Teorema 1.4 (Leis de Morgan.) *Sendo A e B dois conjuntos arbitrários, ter-se-á*

(a) $(A \cap B)^c = A^c \cup B^c$

(b) $(A \cup B)^c = A^c \cap B^c$

Demonstração: Tal como no teorema anterior, far-se-á a demonstração da primeira alínea deixando a segunda a cargo do leitor interessado, como exercício.

Para mostrar que se tem $(A \cap B)^c \subseteq A^c \cup B^c$ é suficiente verificar que qualquer elemento $t \in (A \cap B)^c$ também pertence ao conjunto $A^c \cup B^c$. Da hipótese feita resulta que t não pertence à intersecção de A e B e, portanto, não pertence simultaneamente a A e a B. Logo pertencerá ao complementar de A ou pertencerá ao complementar de B, isto é, tendo em conta a arbitrariedade de t ter-se-á

$$(A \cap B)^c \subseteq A^c \cup B^c \tag{1.3}$$

Suponha-se agora que $s \in A^c \cup B^c$. Então $s \in A^c$ ou $s \in B^c$ e, portanto, $s \notin A$ ou $s \notin B$, donde decorre que $s \notin A \cap B$. Consequentemente,

$$A^c \cup B^c \subseteq (A \cap B)^c \tag{1.4}$$

De (1.3) e (1.4) resulta a igualdade pretendida. □

Exercícios 1.1.4 *Verificar a demonstração do teorema 1.4 usando um diagrama de Venn apropriado.*

Exercícios 1.1.5

1. *Sendo P, Q, R três conjuntos, indicar quais das afirmações que se seguem são verdadeiras.*
   - *(a)* Se P é um elemento de Q e Q é um subconjunto de R, então P é um elemento de R.
   - *(b)* Se P é um elemento de Q e Q é um subconjunto de R, então P é também um subconjunto de R.
   - *(c)* Se P é um subconjunto de Q e Q é um elemento de R, então P é um elemento de R.
   - *(d)* Se P é um subconjunto de Q e Q é um elemento de R, então P é um subconjunto de R.
2. *Sendo P, Q, R três conjuntos, provar*
   - *(a)* $(P \backslash Q) \backslash R = P \backslash (Q \cup R)$
   - *(b)* $(P \backslash Q) \backslash R = (P \backslash R) \backslash Q$

(c) $(P \backslash Q) \backslash R = (P \backslash R) \backslash (Q \backslash R)$

3. *Chama-se* **diferença simétrica** *de dois conjuntos A e B ao conjunto constituído pelos elementos que pertencem a A ou a B, mas não a ambos simultaneamente.*

   (a) *Denotando por $A \oplus B$ a diferença simétrica de A e B , mostrar que $A \oplus B = (A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$.*

   (b) *Representar num diagrama de Venn a diferença simétrica de dois conjuntos A e B quaisquer.*

   (c) *Se a diferença simétrica entre dois conjuntos A e B for igual ao conjunto A que poderá dizer-se a respeito de A e B?*

   (d) *Usando diagramas de Venn, verificar quais das igualdades que se seguem são verdadeiras e quais são falsas*

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

   (e) *Se a diferença simétrica de A e B for igual à diferença simétrica de A e C poderá concluir-se que se tem, necessariamente, $B = C$?*

1.2 Elementos de Teoria da Dedução

"... depuis les Grecs qui dit Mathématique dit Demonstration."

in **Bourbaki**

A Matemática divide-se geralmente em partes chamadas **teorias matemáticas**. O desenvolvimento de uma qualquer daquelas teorias é constituído por três etapas fundamentais:

(1) a construção dos objectos matemáticos da teoria;

(2) a formação de relações entre aqueles objectos;

(3) a pesquisa daquelas relações que são verdadeiras, ou seja, a demonstração de teoremas.

Objectos matemáticos são, por exemplo, os números, as funções ou as figuras geométricas; a Teoria dos Números, a Análise Matemática e a Geometria são, respectivamente, as teorias matemáticas que os estudam. Os objectos matemáticos (provavelmente) não existem na natureza; são apenas modelos

abstractos de objectos reais mais ou menos complicados. As relações entre os objectos matemáticos são afirmações (ou proposições ou sentenças), verdadeiras ou falsas, que podem enunciar-se a seu respeito e que, de algum modo, correspondem a propriedades hipotéticas dos objectos reais que eles modelam.

Para provar os seus resultados a matemática usa um determinado processo de raciocínio que se baseia na **Lógica**; existe uma interligação profunda entre a Matemática e a Lógica. Deve observar-se desde já que, embora existam outros tipos de Lógica, aqui o termo deve entender-se no sentido da chamada *Lógica bivalente* que adopta como regras fundamentais de pensamento os dois princípios seguintes:

> **Princípio da não contradição:** Uma proposição não pode ser verdadeira **e** falsa (ao mesmo tempo).
>
> **Princípio do terceiro excluído:** Uma proposição **ou** é verdadeira **ou** é falsa (isto é, verifica-se sempre um destes casos e nunca um terceiro).

A matemática, como qualquer outra ciência, utiliza a sua linguagem própria constituída por **termos** – palavras ou símbolos – e **proposições** que são combinações de termos de acordo com determinadas regras. Numa teoria matemática qualquer podem distinguir-se dois tipos de termos:

(1) **termos lógicos**, que não são específicos daquela teoria e fazem parte da linguagem matemática geral, e

(2) **termos específicos** da teoria que se está a considerar.

Termos lógicos como, por exemplo, *"variável"*, *"relação"*, etc. são comuns a todas as teorias matemáticas. Pelo contrário, *"ponto"*, *"recta"* e *"ângulo"* são termos específicos da geometria, enquanto que *"número"*, "$<$", *"adição"* são termos específicos da teoria dos números, etc. Uma relação entre objectos pode enunciar-se, por exemplo, sob a forma de uma implicação[2] "$p \Rightarrow q$", tanto em geometria como em teoria dos números; os termos específicos que aparecem em "p" e "q" são, no entanto, distintos quando os objectos pertencem à geometria ou à teoria dos números. Assim, se for

$$\begin{array}{rcl} p & \equiv & \text{"}A, B, C \text{ são três pontos não colineares"} \\ q & \equiv & \text{"existe um e um só plano que passa por } A, B \text{ e } C\text{"} \end{array}$$

[2] A definição de implicação bem como de outras operações lógicas é feita mais à frente.

a implicação "$p \Rightarrow q$" tem um significado geométrico; se for

$$\begin{array}{rcl} p & \equiv & \text{"2 é primo"} \\ q & \equiv & \text{"}2^2 - 1 \text{ é primo"} \end{array}$$

a implicação "$p \Rightarrow q$" tem significado em teoria dos números. Os termos lógicos dão a *forma* a uma teoria matemática; os termos específicos dão-lhe o *conteúdo*. O papel principal da lógica em matemática é o de comunicar as ideias de forma precisa evitando erros de raciocínio.

1.2.1 Conjectura e demonstração

Como atrás se referiu, uma das etapas fundamentais no desenvolvimento de uma teoria matemática é a pesquisa de relações verdadeiras entre os objectos da teoria. Ou seja, dada uma afirmação relativa aos objectos da teoria, é necessário demonstrar a sua veracidade ou falsidade; só depois deste processo é que tal afirmação, se for demonstrada a sua veracidade, adquire o estatuto de teorema.

Chama-se **demonstração formal** a uma sequência finita $p_1, p_2, \ldots, p_n$ de proposições cada uma das quais ou é um axioma (proposição cuja veracidade se admite *à priori*) ou resulta de proposições anteriores por regras de inferência (que são formas muito simples e frequentes de argumentação válida, tradicionalmente designadas por silogismos). Cada uma das proposições p_j, $1 \leq j \leq n$, é designada por **passo** da demonstração. Neste sentido, **teorema** será o último passo de uma dada demonstração, isto é, demonstrar um teorema consiste na realização de uma demonstração cujo último passo é o teorema em questão.

As demonstrações formais raramente são praticadas fora dos livros de Lógica. Como uma demonstração formal inclui todos os passos possíveis (nada é deixado à imaginação) então a demonstração formal de um teorema, ainda que simples, é normalmente longa (e fastidiosa). Assim, fora da Lógica raramente se fazem demonstrações formais rigorosas: o que em geral se faz é estabelecer os passos fundamentais da demonstração suprimindo todos os detalhes lógicos que, muitas vezes, não ajudam a esclarecer a verdadeira natureza da proposição sob análise. Estes procedimentos designar-se-ão simplesmente por **demonstrações** (ou demonstrações matemáticas) por contraposição a demonstrações formais.

Exemplo. Na tabela que se segue, para cada número natural n de 2 a 10, calculou-se o número $2^n - 1$ obtendo-se os seguintes resultados:

n	É primo?	$2^n - 1$	É primo?
2	sim	3	sim
3	sim	7	sim
4	não	15	não
5	sim	31	sim
6	não	63	não
7	sim	127	sim
8	não	255	não
9	não	511	não
10	não	1023	não

Observando cuidadosamente a tabela *parece* verificar-se o seguinte: *sempre que n é um número primo, o número $2^n - 1$ também é primo!* Será verdade? É tentador pensar que sim, mas de momento não há qualquer razão suficientemente forte que garanta este resultado de forma indiscutível. Em matemática dá-se o nome de **conjectura** a este tipo de afirmações cujo valor lógico de *verdade* ou *falsidade* carece de ser provado. Assim, esta tabela suscita as duas conjecturas seguintes:

> **Conjectura I** *Dado um número inteiro n superior a 1, se n for primo então o número $2^n - 1$ é primo.*
>
> **Conjectura II** *Dado um número inteiro n superior a 1, se n não for primo o número $2^n - 1$ também não é primo.*

Destas duas conjecturas a primeira pode refutar-se imediatamente: para tal é suficiente continuar a desenvolver a tabela para valores de n superiores a 10. Assim, para $n = 11$ vem

$$2^{11} - 1 \;=\; 2047 \;=\; 23 \times 89$$

o que mostra que a conjectura é falsa: 11 é um número superior a 1 e é primo, mas $2^{11} - 1$ é um número composto. O número 11, neste caso, constitui o que se designa geralmente por **contra-exemplo** para a conjectura: um simples contra-exemplo é suficiente para mostrar que a conjectura é falsa. Mas há mais contra-exemplos: 23 e 29, por exemplo, são outros contra-exemplos.

Considere-se agora a segunda conjectura: estendendo a tabela a outros números inteiros não primos superiores a 10 não se encontra nenhum contra-exemplo. Isto, contudo, não nos permite concluir que a conjectura é verdadeira pois por muito que se prolongue a tabela nunca será possível

experimentar todos os números compostos possíveis: eles são em número infinito! Poderá haver contra-exemplos que sejam tão grandes que nem com os actuais meios computacionais seja possível testá-los. Para demonstrar ou refutar a conjectura é necessário adoptar então outros métodos.

A conjectura II é, de facto, verdadeira.

Demonstração: Visto que n não é primo então existem inteiros positivos a e b maiores que 1 tais que $a < n$ e $b < n$ e $n = ab$. Sendo $x = 2^b - 1$ e $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$, então

$$\begin{aligned} xy &= \left(2^b - 1\right) \cdot \left(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}\right) \\ &= 2^b \cdot \left(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}\right) - \left(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}\right) \\ &= \left(2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}\right) - \left(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}\right) \\ &= 2^{ab} - 1 \\ &= 2^n - 1 \end{aligned}$$

Visto que $b < n$ pode concluir-se que $x = 2^b - 1 < 2^n - 1$; por outro lado como $b > 1$ então $x = 2^b - 1 > 2^1 - 1 = 1$ donde se segue que $y < xy = 2^n - 1$. Então $2^n - 1$ pode decompor-se num produto de dois números inteiros positivos x e y maiores que 1 e menores que $2^n - 1$ o que prova que $2^n - 1$ não é primo. □

Uma vez que se provou que a conjectura II é verdadeira, esta passou a adquirir o estatuto de **teorema**, podendo então escrever-se:

> **Teorema 1.5** *Dado um número inteiro n superior a 1, se n não for primo então o número* $2^n - 1$ *também não é primo.*

Exercícios 1.2.1 *Aproveitando as ideias usadas na demonstração anterior,*

1. *mostrar que* $2^{12} - 1$ *não é primo, exibindo explicitamente dois factores (maiores que 1) em que se pode decompor este número;*
2. *determinar um inteiro* x *tal que* $1 < x < 2^{32\,767} - 1$ *por forma que o número* $2^{32\,767} - 1$ *seja divisível por* x*.*

Como se viu acima o facto de n ser um número primo não garante que $2^n - 1$ seja também primo. Mas para alguns inteiros $n > 1$ primos o número $2^n - 1$ é primo: aos número primos da forma $2^n - 1$ dá-se o nome de **números primos de Mersenne**. Assim, 3, 7, 31, etc., são números primos de Mersenne, mas 5 é um número primo que não é número primo de Mersenne. Com a ajuda dos computadores muitos números primos de

Mersenne têm sido encontrados ultimamente. Em Maio de 1994 o maior número primo de Mersenne conhecido era $2^{859\,433}-1$ que tem 258 716 dígitos. Em Novembro de 1996 foi obtido um novo recorde com o número $2^{1\,398\,269}-1$ que tem 420 921 casas decimais e é o 35º número primo de Mersenne conhecido. Contudo não se sabe ainda se há uma infinidade de números primos de Mersenne ou se, pelo contrário, o número de primos de Mersenne, embora eventualmente muito grande, é finito. Consequentemente, de momento, apenas se poderá conjecturar uma ou outra das hipóteses. Já o mesmo se não dirá sobre os números primos propriamente ditos: há cerca de 2400 anos, Euclides (*c.* 350 *a.C.*) provou nos seus célebres *Elementos* o seguinte:

Teorema 1.6 *Há uma infinidade de números primos.*

Demonstração: Suponha-se, pelo contrário (redução ao absurdo), que há apenas um número finito de números primos. Podemos então enumerá-los: seja $p_1, p_2, \ldots, p_k$ a lista de **todos** os números primos e considere-se o número

$$m \;=\; p_1 \cdot p_2 \cdots p_k + 1$$

O resto da divisão de m por p_1 é igual a 1 e, portanto, o número m não é divisível por p_1; de modo semelhante se pode concluir que m não é divisível nem por p_2 nem por ... nem por p_k.

Usar-se-á agora o facto de *todo o número inteiro maior que 1 ser primo ou poder decompor-se num produto de factores primos.* Ora m é claramente maior que 1 e, portanto, m ou é um número primo ou pode decompor-se num produto de factores primos.

Suponha-se que m é primo. Como m é maior que qualquer um dos números $p_1, \ldots, p_k$ então existiria um número primo que não faria parte da lista que se admitiu conter todos os números primos existentes. Então m não pode ser primo e, portanto, será um produto de números primos estritamente compreendidos entre 1 e m. Seja q um dos primos desta decomposição. Então m é divisível por q pelo que q não pode ser nenhum dos números primos da lista de todos os números primos considerada inicialmente. De novo temos uma contradição a qual resulta de se ter admitido que era finito o número de números primos existentes. Esta hipótese, que conduz sempre a contradições, é falsa ficando, assim, provado que existe uma infinidade de números primos. □

Os números primos de Mersenne estão relacionados com um outro tipo de números – os números **perfeitos** – relativamente aos quais está também por resolver outra conjectura famosa. Um número inteiro n diz-se perfeito se for igual à soma de todos os inteiros positivos menores que n que o dividem exactamente. Assim, 6 é perfeito pois $6 = 1+2+3$ e $28 = 1+2+4+7+14$ é o número perfeito que se lhe segue.

Euclides provou que que se $2^n - 1$ for um número primo então $2^{n-1}(2^n - 1)$ é perfeito. Então, cada número primo de Mersenne dá origem, por este processo, a um número perfeito. Cerca de 2000 anos mais tarde o matemático suíço Leonhard Euler (1707-1783) provou que todo o número perfeito par é gerado por este processo.[3] Como não se sabe se há infinitos números primos de Mersenne também não se sabe se há ou não infinitos números perfeitos pares. Quanto aos números perfeitos ímpares não se sabe sequer se existe algum.

Exercícios 1.2.2 *Seja n um inteiro positivo arbitrariamente escolhido. Mostrar que existe uma sequência de n inteiros consecutivos que não contém qualquer número primo.* [SUGESTÃO: considerar o número $x = (n+1)! + 2$ e mostrar que nenhum dos números x, $x+1$, ..., $x+(n-1)$ pode ser primo.] *Aplicar este resultado a $n = 7$.*

1.2.2 Lógica proposicional

> "Poder-se-á definir a Lógica como a ciência das regras que legitimam a utilização da palavra PORTANTO."
>
> B. Ruyer in **Logique**

Como foi referido acima, a demonstração de conjecturas é essencial em matemática. A Lógica estuda os métodos de raciocínio, especialmente os que podem expressar-se sob a forma de argumentos. Um *argumento* consiste numa série (finita) de proposições declarativas, chamadas *premissas*, a partir das quais se infere uma outra proposição, a *conclusão*. Há vários tipos de argumentos: os dois principais são os *argumentos indutivos* e os *argumentos dedutivos*. O primeiro, usado no dia a dia pelas ciências empíricas, parte de dados da experiência para concluir que uma dada proposição, *provavelmente*, é verdadeira. Os dados da experiência tornam provável a veracidade da conclusão, mas não a garantem em absoluto.

Um argumento dedutivo, pelo contrário, garante que se todas as premissas forem verdadeiras a conclusão também o será. A argumentação dedutiva está na base das demonstrações matemáticas. Por este facto, far-se-á, antes de mais, uma breve resenha dos aspectos mais importantes da lógica elementar. Relembrar-se-á, para começar, o significado das conectivas lógicas mais comuns.

[3] Note-se que $6 = 2^1(2^2 - 1)$ e $28 = 2^2(2^3 - 1)$.

Os elementos básicos da lógica são as **proposições** ou **sentenças** que são afirmações precisas (verdadeiras ou falsas, mas não ambas as coisas). Por exemplo, *"2 é maior que 3"* é uma proposição cujo valor lógico é o de *"falsidade"* enquanto que *"todos os triângulos têm três lados e três ângulos"* é uma proposição cujo valor lógico é o de *"verdade"*. Por outro lado *"$x < 3$"* não é uma proposição (depende do valor que venha a ser atribuído à variável x). Representar-se-ão por letras (geralmente minúsculas) as proposições genéricas (ou variáveis proposicionais) e por 1 e 0 os valores lógicos de *"verdade"* e *"falsidade"*, respectivamente.

Exemplo 1.7 As afirmações

1. A Lua é feita de queijo verde.
2. $(e^{\pi})^2 = e^{2\pi}$.
3. 6 é um número primo.
4. O milionésimo dígito na dízima de $\sqrt{2}$ é 6.

são exemplos de proposições. Por outro lado,

1. Será $(e^{\pi})^2$ igual a $e^{2\pi}$?
2. Se ao menos todos os dias pudessem ser como este!
3. Toda a gente é aardlingueede.
4. Esta proposição é falsa.

claramente não são proposições.

Por vezes combinam-se várias proposições para obter proposições compostas: neste caso, em geral, pretende-se obter os valores lógicos das proposições compostas em função dos valores lógicos conhecidos das proposições mais simples que as compõem.

Uma conectiva lógica que modifica o valor de uma dada proposição "p" é a sua negação "**não** p", denotada geralmente por "$\neg p$", que é uma proposição falsa quando "p" é verdadeira e verdadeira quando "p" é falsa. Isto pode expressar-se à custa da chamada tabela de verdade da negação:

p	$\neg p$
1	0
0	1

Há diversas formas pelas quais se podem combinar duas proposições. Em particular as conectivas "**e**" e "**ou**", *conjunção* e *disjunção*, denotadas geralmente por "$\wedge$" e "$\vee$", respectivamente, são definidas pelas seguintes tabelas de verdade:

p	q	$p \wedge q$	$p \vee q$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

A conjunção de duas proposições é verdadeira quando e só quando as duas proposições forem *simultaneamente* verdadeiras; a disjunção é verdadeira desde que *pelo menos uma* das proposições seja verdadeira.

A conectiva "$\Rightarrow$" que se lê "**se ..., então ...**", designada por *"implicação"*, obedece, por seu lado, à seguinte tabela de verdade:

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Por fim considere-se a conectiva lógica "p **se e só se** q", por vezes abreviada para "p **sse** q", e geralmente denotada por "$p \Leftrightarrow q$". A sua tabela de verdade é dada por

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

A proposição "$p \Leftrightarrow q$" é verdadeira quando "p" e "q" são ambas verdadeiras ou ambas falsas e falsa quando "p" e "q" têm valores lógicos distintos. É fácil verificar que "$p \Leftrightarrow q$" tem o mesmo significado lógico que a proposição "$(p \Rightarrow q) \wedge (q \Rightarrow p)$". Para o confirmar basta escrever a tabela de verdade para esta proposição e verificar que é idêntica à da primeira.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
1	1	1	1	1
1	0	0	1	0
0	1	1	0	0
0	0	1	1	1

Na prática usa-se frequentemente esta relação: para mostrar que uma proposição da forma "$p \Leftrightarrow q$" é verdadeira decompõe-se essa proposição nas duas partes "$p \Rightarrow q$" e "$q \Rightarrow p$" e mostra-se separadamente que cada uma delas é verdadeira.

Nota 1.8 (A implicação.) A tabela de verdade da conectiva $\Rightarrow$ funciona como *aquela* definição[4] para a *implicação* que a experiência mostrou ser a mais adequada. No entanto há aqui um certo conflito em relação ao que se passa na conversação usual: nesta não se dirá geralmente *"p implica q"* quando se sabe à priori que "p" é falsa. A implicação é verdadeira quando o antecedente "p" é falso qualquer que seja o consequente "q". Esta situação pode ilustrar-se com a implicação *"se dois mais dois são cinco então a terra é um queijo"* que é verdadeira uma vez que o antecedente é falso.

As duas primeiras linhas da tabela da implicação não apresentam qualquer problema sob o ponto de vista intuitivo do senso comum. Quanto às duas últimas, qualquer outra escolha possível apresentaria desvantagens sob o ponto de vista lógico, o que levou à escolha das soluções apresentadas: de facto, fazendo 0 na 3ª linha e 0 na 4ª linha obtém-se a tabela da conjunção, $\wedge$; fazendo 0 na 3ª linha e 1 na 4ª linha obtém-se a equivalência. Resta a possibilidade de fazer 1 na 3ª linha e 0 na 4ª linha que não é também desejável pois isso equivaleria a recusar a equivalência

$$[p \Rightarrow q] \;\Leftrightarrow\; [\neg q \Rightarrow \neg p]$$

Ora esta equivalência é aconselhável, ela própria, pelo senso comum: por exemplo, a proposição *"se o Pedro fala, existe"* é (intuitivamente) equivalente à proposição *"se o Pedro não existe, não fala"*. A aceitação desta equivalência impõe a tabela considerada para a implicação.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$
1	1	1	0	0	1
1	0	0	1	0	0
0	1	1	0	1	1
0	0	1	1	1	1

Dada uma implicação $p \Rightarrow q$ há outras implicações envolvendo as proposições p e q (ou as suas negações $\neg p$ e $\neg q$) que estão relacionadas com aquela. A proposição $\neg q \Rightarrow \neg p$, que lhe é equivalente, como já foi referido acima, é conhecida por **contra-recíproca** ou **conversa** da primeira. A proposição $q \Rightarrow p$ designa-se por **recíproca** e a proposição $\neg p \Rightarrow \neg q$ designa-se por **inversa** ou **contrária**. Observe-se que, embora a contra-recíproca seja equivalente à proposição original, o mesmo não acontece com a recíproca (e a contrária, que lhe é equivalente) o que pode verificar-se através das respectivas tabelas de verdade.

[4] Outras definições para a implicação seriam, em princípio, possíveis.

1.2.2.1 Tautologias e contradições

Chama-se **tautologia** a uma proposição que é sempre verdadeira quaisquer que sejam os valores atribuídos às variáveis proposicionais que a compõem. Dito de outra forma, chama-se tautologia a uma proposição cuja tabela de verdade possui apenas 1s na última coluna. Exemplo de uma tautologia é a proposição $p \vee (\neg p)$, o princípio do terceiro excluído,

p	$\neg p$	$p \vee (\neg p)$
1	0	1
0	1	1

Se p designar a proposição *"5 é uma raiz primitiva de 17"* então $p \vee (\neg p)$ é sempre verdadeira independentemente do significado (ou sentido) atribuído à expressão *"raiz primitiva de"*.

Chama-se **contradição** à negação de uma tautologia: trata-se de uma proposição cuja tabela de verdade apenas possui 0s na última coluna.

Nota 1.9 Não deve confundir-se contradição com proposição falsa, assim como não deve confundir-se tautologia com proposição verdadeira. O facto de uma tautologia ser sempre verdadeira e uma contradição ser sempre falsa deve-se à sua forma lógica (sintaxe) e não ao significado que se lhes pode atribuir (semântica).

A tabela de verdade

p	q	$p \vee q$	$p \Rightarrow (p \vee q)$	$p \Rightarrow q$	$\neg q$	$p \wedge (\neg q)$	$(p \Rightarrow q) \wedge [p \wedge (\neg q)]$
1	1	1	1	1	0	0	0
1	0	1	1	0	1	1	0
0	1	1	1	1	0	0	0
0	0	0	1	1	1	0	0

mostra que $p \Rightarrow (p \vee q)$ é uma tautologia, enquanto que $(p \Rightarrow q) \wedge [p \wedge (\neg q)]$ é uma contradição.

Exercícios 1.2.3 :

1. *Indicar os valores (de verdade ou falsidade) das seguintes afirmações:*

   (a) $3 \leq 7$ *e 4 é um número inteiro ímpar*

   (b) $3 \leq 7$ *ou 4 é um número inteiro ímpar*

   (c) 5 é ímpar ou divisível por 4

2. *Suponha-se que p, q, r representam as seguintes sentenças:*

$$\begin{array}{lcl} p & \equiv & \text{“7 é um número inteiro par”} \\ q & \equiv & \text{“3+1=4”} \\ r & \equiv & \text{“24 é divisível por 8”} \end{array}$$

   (a) *Escrever em linguagem simbólica as proposições*

   - $3 + 1 \neq 4$ *e 24 é divisível por 8*
   - *não é verdade que 7 seja ímpar ou 3+1=4*
   - *se 3+1=4 então 24 não é divisível por 8*

   Construir as tabelas de verdade das proposições compostas obtidas.

   (b) *Escrever por palavras as sentenças*

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

   e construir as suas tabelas de verdade.

3. *Construir as tabelas de verdade das seguintes proposições*

   (a) $[(p \Rightarrow q) \wedge p] \Rightarrow q$

   (b) $p \Leftrightarrow (q \Rightarrow r)$

   (c) $[p \wedge (\neg p)] \Rightarrow q$

   (d) $[p \vee r) \wedge (q \vee r)] \wedge [(\neg p) \vee (\neg r)]$

   (e) $[p \wedge (q \vee r)] \wedge [q \wedge (p \vee r)]$

4. *Suponha-se que se define uma nova conectiva, denotada por $*$, tal que $p * q$ é verdadeira quando q é verdadeira e p falsa e é falsa em todos os outros casos. Construir as tabelas de verdade para*

   (a) $p * q$

   (b) $q * p$

   (c) $(p * q) * p$

5. *Determinar*

   (a) *a contra-recíproca de* $(\neg p) \Rightarrow q$

   (b) *a inversa de* $(\neg q) \Rightarrow p$

   (c) *a recíproca da inversa de* $q \Rightarrow (\neg p)$

   (d) *a negação de* $p \Rightarrow (\neg q)$

6. *Quantas linhas terá a tabela de verdade de uma proposição contendo n variáveis proposicionais?*

1.		$p \vee \neg p$	
2.		$\neg[p \wedge (\neg p)]$	
3.		$p \Rightarrow p$	
4.	a)	$p \Leftrightarrow (p \vee p)$	idempotência
	b)	$p \Leftrightarrow (p \wedge p)$	idempotência
5.		$\neg\neg p \Leftrightarrow p$	dupla negação
6.	a)	$(p \vee q) \Leftrightarrow (q \vee p)$	comutatividade
	b)	$(p \wedge q) \Leftrightarrow (q \wedge p)$	comutatividade
	c)	$(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$	comutatividade
7.	a)	$(p \vee (q \vee r)) \Leftrightarrow ((p \vee q) \vee r)$	associatividade
	b)	$(p \wedge (q \wedge r)) \Leftrightarrow ((p \wedge q) \wedge r)$	associatividade
8.	a)	$(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$	distributividade
	b)	$(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$	distributividade
9.	a)	$(p \vee 0) \Leftrightarrow p$	identidade
	b)	$(p \wedge 0) \Leftrightarrow 0$	identidade
	c)	$(p \vee 1) \Leftrightarrow 1$	identidade
	d)	$(p \wedge 1) \Leftrightarrow p$	identidade
10.	a)	$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$	lei de Morgan
	b)	$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$	lei da Morgan
11.	a)	$(p \Leftrightarrow q) \Leftrightarrow [(p \Rightarrow q) \wedge (q \Rightarrow p)]$	equivalência
	b)	$(p \Leftrightarrow q) \Leftrightarrow [(p \wedge q) \vee (\neg p \wedge \neg q)]$	equivalência
	c)	$(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q)$	equivalência
12.	a)	$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$	implicação
	b)	$\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$	implicação
13.		$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$	contrarecíproca
14.		$(p \Rightarrow q) \Leftrightarrow [(p \wedge \neg q) \Rightarrow 0]$	redução ao absurdo
15.	a)	$[(p \Rightarrow r) \wedge (q \Rightarrow r)] \Leftrightarrow [(p \vee q) \Rightarrow r]$	
	b)	$[(p \Rightarrow q) \wedge (p \Rightarrow r)] \Leftrightarrow [p \Rightarrow (q \wedge r)]$	
16.		$[(p \wedge q) \Rightarrow r] \Leftrightarrow [p \Rightarrow (q \Rightarrow r)]$	
17.		$p \Rightarrow (p \vee q)$	adição
18.		$(p \wedge q) \Rightarrow p$	simplificação
19.		$[p \wedge (p \Rightarrow q)] \Rightarrow q$	*modus ponens*
20.		$[(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$	*modus tollens*
21.		$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$	silogismo hipotético
22.		$[(p \vee q) \wedge \neg p] \Rightarrow q$	silogismo disjuntivo
23.		$(p \Rightarrow 0) \Rightarrow \neg p$	absurdo
24.		$[(p \Rightarrow q) \wedge (r \Rightarrow s)] \Rightarrow [(p \vee r) \Rightarrow (q \vee s)]$	
25.		$(p \Rightarrow q) \Rightarrow [(p \vee r) \Rightarrow (q \vee r)]$	

Na tabela acima apresentam-se alguns exemplos importantes de tautologias onde p, q, r designam variáveis proposicionais (isto é, afirmações que ou

são verdadeiras ou falsas, mas não ambas as coisas) e 1 e 0 designam as proposições tautológica e contraditória, respectivamente.

Definição 1.10 *Duas proposições a e b dizem-se* **logicamente equivalentes** *se tiverem os mesmos valores lógicos em todas as circunstâncias, ou seja, se a proposição $a \Leftrightarrow b$ for uma tautologia.*

Dir-se-á que a proposição a **implica logicamente** *a proposição b se a veracidade da primeira arrastar necessariamente a veracidade da segunda, ou seja, se a proposição $a \Rightarrow b$ for uma tautologia.*

Exercícios 1.2.4 :

1. *Indicar quais das sentenças seguintes é que são equivalentes*
   (a) $p \wedge (\neg q)$
   (b) $p \Rightarrow q$
   (c) $\neg[(\neg p) \vee q)]$
   (d) $q \Rightarrow (\neg q)$
   (e) $(\neg p) \vee q$
   (f) $\neg[p \Rightarrow q]$
   (g) $p \Rightarrow (\neg q)$
   (h) $(\neg p) \Rightarrow (\neg q)$
2. *Mostrar que cada uma das proposições que se seguem*
   (a) $(\neg p) \vee q$
   (b) $(\neg q) \Rightarrow (\neg p)$
   (c) $\neg[p \wedge (\neg q)]$

   é equivalente à implicação $p \Rightarrow q$.
3. *Mostrar que*
   (a) $p \vee (q \wedge r)$ *não é logicamente equivalente a* $(p \vee q) \wedge r$.
   (b) $p \vee (q \wedge r)$ *é logicamente equivalente a* $(p \vee q) \wedge (p \vee r)$.
   (c) $p \vee [\neg(q \wedge r)]$ *é logicamente equivalente a* $[p \vee (\neg q)] \vee (\neg r)$.
4. *Indicar quais dos pares de sentenças que se seguem é que são logicamente equivalentes e quais não são.*
   (a) $[p \wedge [q \vee r]]$; $[[p \wedge q] \vee [p \wedge r]]$
   (b) $\neg[p \wedge q]$; $[(\neg p) \wedge (\neg q)]$
   (c) $[p \vee [q \wedge r]]$; $[[p \vee q] \wedge [p \vee r]]$
   (d) $[p \Leftrightarrow q]$; $[p \Rightarrow q] \wedge [q \Rightarrow p]$
   (e) $[p \Rightarrow q]$; $[q \Rightarrow p]$
   (f) $[p \Rightarrow q]$; $[(\neg q) \Rightarrow (\neg p)]$

(g) $\neg[p \Rightarrow q]$; $[(\neg p) \Rightarrow (\neg q)]$

5. *Verificar que as proposições da tabela da página 23 são, de facto, tautologias. Usando as tautologias apropriadas simplificar as seguintes proposições:*
   (a) $p \vee [q \wedge (\neg p)]$
   (b) $\neg[p \vee [q \wedge (\neg r)]] \wedge q$
   (c) $\neg[(\neg p) \wedge (\neg q)]$
   (d) $\neg[(\neg p) \vee q] \vee [p \wedge (\neg r)]$
   (e) $[p \wedge q] \vee [p \wedge (\neg q)]$
   (f) $[p \wedge r] \vee [(\neg r) \wedge [p \vee q]]$
6. *Por vezes usa-se o símbolo $\downarrow$ para denotar a proposição composta por duas proposições atómicas p e q que é verdadeira quando e só quando p e q são (simultaneamente) falsas e é falsa em todos os outros casos. A proposição $p \downarrow q$ lê-se "nem p nem q".*
   (a) *Fazer a tabela de verdade de $p \downarrow q$.*
   (b) *Expressar $p \downarrow q$ em termos das conectivas $\wedge$, $\vee$ e $\neg$.*
   (c) *Determinar proposições apenas constituídas pela conectiva $\downarrow$ que sejam equivalentes a $\neg p$, $p \wedge q$ e $p \vee q$.*
7. *Determinar se a expressão composta*

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

   é uma tautologia, uma contradição ou não uma coisa nem outra.
8. *Expressar a proposição $p \Leftrightarrow q$ usando apenas os símbolos $\neg, \wedge$ e $\vee$.*
9. *Mostrar que não são logicamente equivalentes os seguintes pares de proposições*
   (a) $\neg(p \wedge q)$; $(\neg p) \wedge (\neg q)$
   (b) $\neg(p \vee q)$; $(\neg p) \vee (\neg q)$
   (c) $p \Rightarrow q$; $q \Rightarrow p$
   (d) $\neg(p \Rightarrow q)$; $(\neg p) \Rightarrow (\neg q)$
10. *Mostrar que $p \Rightarrow (q \vee r)$ implica logicamente $p \Rightarrow q$.*

1.2.3 Teoremas e demonstrações

Sejam p, q, r três proposições das quais se sabe seguramente que p e q são proposições verdadeiras. Se for possível provar que a implicação

$$(p \wedge q) \Rightarrow r \tag{1.5}$$

é verdadeira (isto é, que da veracidade de p e de q resulta sempre a veracidade de r), então pode argumentar-se que r é necessariamente verdadeira. Se,

numa contenda, as proposições p e q forem aceites como verdadeiras por ambas as partes assim como a implicação (1.5), então a veracidade de r resulta logicamente dos pressupostos. A uma tal proposição (composta) dá-se o nome de *argumento* e constitui o método usado numa discussão para convencer uma parte das razões que assistem à outra.

De um modo mais geral, chama-se **argumento** a uma sequência finita de proposições organizadas na forma seguinte

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q \tag{1.6}$$

onde $p_1, p_2, \ldots, p_n$ são designadas as **premissas** (ou **hipóteses**) e q a **conclusão** (ou **tese**). Ao fazer-se a leitura de (1.6) é costume inserir uma das locuções "PORTANTO", "POR CONSEGUINTE", "LOGO", etc., lendo-se, por exemplo, "$p_1, \ldots, p_n$, portanto, q". Para sugerir esta leitura usa-se, frequentemente, a seguinte notação

$$\begin{array}{l} p_1 \\ \vdots \\ \underline{p_n} \\ q \end{array} \quad \text{ou} \quad p_1, \ldots, p_n/q$$

Interessa distinguir entre argumentos correctos ou válidos e argumentos incorrectos ou inválidos ou falaciosos.

Definição 1.11 *Um argumento*

$$p_1, \ldots, p_n/q$$

diz-se **correcto** *ou* **válido** *se a conclusão for verdadeira sempre que as premissas* $p_1, \ldots, p_n$ *forem simultaneamente verdadeiras e diz-se* **incorrecto** *ou* **inválido** *ou* **falacioso** *no caso contrário, isto é, se alguma situação permitir que as premissas sejam todas verdadeiras e a conclusão falsa.*

Construção de demonstrações elementares. Os matemáticos são pessoas muito cépticas[5]. Têm vários métodos para resolver problemas matemáticos que vão desde a *experimentação* à *tentativa e erro*. Mas não se convencem da validade das respostas obtidas a menos que possam prová-las! A prova ou demonstração é uma espécie de *"puzzle"* para o qual não há

[5] *pessoa céptica* – pessoa que duvida de tudo, especialmente do que é comummente aceite (Dicionário, Porto Editora, 7ª ed.)

regras de resolução rígidas. A única regra fixa diz respeito ao produto final: todas as peças do *"puzzle"* devem estar encaixadas e o resultado obtido deve parecer correcto.

A demonstração de teoremas é feita de muitas formas dependendo em geral do próprio conteúdo do teorema. Os próprios teoremas são formulados de muitas maneiras distintas. Uma das mais frequentes é a que involve uma conclusão do tipo

$$p \Rightarrow q$$

Para demonstrar a veracidade desta implicação começa-se por *supor* que p é uma proposição verdadeira para depois se concluir que *então* q também é verdadeira. [Note-se que se p for falsa a implicação é sempre verdadeira quer q seja verdadeira quer seja falsa.] Observe-se também que desta forma se prova a validade da implicação $p \Rightarrow q$ e não a veracidade de q. Para provar a veracidade de q seria necessário para além de provar a veracidade da implicação $p \Rightarrow q$ que se afirmasse a veracidade de p: *supor* que p é verdadeira não é a mesma coisa que *afirmar* que p é verdadeira.

Exemplo 1.12 *Suponha-se que a e b são números reais. Provar que se $0 < a < b$ então $a^2 < b^2$.*

Resolução: Os dados do problema são as afirmações $a \in \mathbb{R}$ e $b \in \mathbb{R}$ e o objectivo é o de obter uma conclusão da forma $p \Rightarrow q$ onde p é a afirmação $0 < a < b$ e q é a afirmação $a^2 < b^2$. *Supor* que p é uma proposição verdadeira é equivalente a juntar p aos dados do problema. Assim, equivalentemente, pode ter-se

hipóteses	tese
$a \in \mathbb{R}, b \in \mathbb{R}$	$a^2 < b^2$
$0 < a < b$	

A técnica de demonstração, neste caso, obtém-se por comparação das duas desigualdades $a < b$ e $a^2 < b^2$. Multiplicando a primeira desigualdade por a (que é um número real positivo!) vem

$$a^2 < ab \tag{1.7}$$

e multiplicando-a agora por b (que é também um número real positivo) vem

$$ab < b^2 \tag{1.8}$$

De (1.7) e (1.8) obtém-se

$$a^2 < ab < b^2$$

e, portanto, por transitividade, $a^2 < b^2$ como se pretendia mostrar.

Mais formalmente, poder-se-ia apresentar este exemplo da seguinte forma:

Teorema 1.13 *Suponha-se que a e b são dois números reais. Se $0 < a < b$ então $a^2 < b^2$.*

Demonstração: Suponha-se que $0 < a < b$. Multiplicando a desiguladade $a < b$ pelo número positivo a conclui-se que $a^2 < ab$ e, de modo semelhante, multiplicando-a por b obtém-se $ab < b^2$. Então $a^2 < ab < b^2$ e, portanto, $a^2 < b^2$ como se pretendia mostrar. Consequentemente, se $0 < a < b$ então $a^2 < b^2$. □

Para provar uma implicação da forma $p \Rightarrow q$, muitas vezes, é mais fácil supor $\neg q$ e provar que então se verifica $\neg p$ obtendo-se assim

$$\neg q \ \Rightarrow \ \neg p$$

o que, como se sabe, equivale logicamente a $p \Rightarrow q$.

Exemplo 1.14 *Suponha-se que a, b e c são três números reais e que $a > b$. Mostrar que se $ac \leq bc$ então $c \leq 0$.*

Resolução: A demonstração neste caso tem o seguinte esquema:

hipóteses	tese
$a \in \mathbb{R}, b \in \mathbb{R}, c \in \mathbb{R}$	$ac \leq bc \Rightarrow c \leq 0$
$a > b$	

A contra-recíproca da tese é a implicação

$$\neg(c \leq 0) \ \Rightarrow \ \neg(ac \leq bc)$$

ou seja,

$$c > 0 \ \Rightarrow \ ac > bc$$

e, portanto, pode realizar-se a demonstração de acordo com o seguinte esquema:

hipóteses	tese
$a \in \mathbb{R}, b \in \mathbb{R}, c \in \mathbb{R}$	$ac > bc$
$a > b$	
$c > 0$	

A tese resulta agora imediatamente de se multiplicar a desigualdade $a > b$ por $c > 0$.

Mais formalmente, ter-se-á

Teorema 1.15 *Sejam a, b, c três números reais tais que $a > b$. Se $ac \leq bc$ então $c \leq 0$.*

Demonstração: Far-se-á a prova pela contra-recíproca. Suponha-se $c > 0$. Então multiplicando ambos os membros da desigualdade $a > b$ por c obter-se-á $ac > bc$. Consequentemente,

$$ac \leq bc \ \Rightarrow \ c \leq 0$$

como se pretendia mostrar. □

Exercícios 1.2.5

1. *Sejam A, B, C, D quatro conjuntos e suponha-se que $A \backslash B \subseteq C \cap D$ e seja $x \in A$. Mostrar que se $x \notin D$ então $x \in B$.*
2. *Sejam a, b números reais. Mostrar que se $a < b$ então $(a + b)/2 < b$.*
3. *Suponha-se que x é um número real tal que $x \neq 0$. Mostrar que se*

$$\frac{\sqrt[3]{x} + 5}{x^2 + 6} \ = \ \frac{1}{x}$$

então $x \neq 8$.

4. *Sejam a, b, c, d números reais tais que $0 < a < b$ e $d > 0$. Provar que se $ac > bd$ então $c > d$.*

As regras que permitem passar de hipóteses feitas e resultados já demonstrados a novas proposições são conhecidas por **regras de inferência**. A regra de inferência mais frequentemente usada, conhecida por **modus ponens**, é a seguinte:

$$\begin{array}{l} p \ \Rightarrow \ q \\ p \\ \hline\hline q \end{array}$$

Se forem verdadeiras a proposição p e a implicação $p \Rightarrow q$, então q é necessariamente verdadeira.

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$[p \wedge (p \Rightarrow q)] \Rightarrow q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

A proposição q é *logicamente implicada* por p e $p \Rightarrow q$ o que se escreve

$$p, p \Rightarrow q \ \models \ q$$

De um modo geral,

$$p_1, p_2, \ldots, p_n \models q$$

é uma regra de inferência se e só se

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \Rightarrow q$$

for uma tautologia.

Outras regras de inferência são as seguintes:

$p, p \Rightarrow q$	$\models$	q	modus ponens
$p \Rightarrow q, q \Rightarrow r$	$\models$	$p \Rightarrow r$	
$p \Rightarrow q, \neg q$	$\models$	$\neg p$	modus tollens
p	$\models$	$p \vee q$	
$p \wedge q$	$\models$	p	
p, q	$\models$	$p \wedge q$	

Exercícios 1.2.6 *Sendo p, q, r e s quatro proposições dadas, estabelecer a validade ou invalidade dos seguintes argumentos.*

1. $(\neg p) \vee q, p \models q$
2. $p \Rightarrow q, r \Rightarrow (\neg q) \models p \Rightarrow (\neg r)$
3. $(\neg p) \vee q, (\neg r) \Rightarrow (\neg q) \models p \Rightarrow (\neg r)$
4. $q \vee (\neg p), \neg q \models p$
5. $\neg p \models p \Rightarrow q$
6. $(p \wedge q) \Rightarrow (r \wedge s), \neg r \models (\neg p) \vee (\neg q)$
7. $p \Rightarrow q, (\neg q) \Rightarrow (\neg r), s \Rightarrow (p \vee r), s \models q$
8. $p \vee q, q \Rightarrow (\neg r), (\neg r) \Rightarrow (\neg p) \models \neg(p \wedge q)$
9. $p \Rightarrow q, (\neg r) \Rightarrow (\neg q), r \Rightarrow (\neg p) \models \neg p$
10. $p \Rightarrow (\neg p) \models \neg p$
11. $p \vee q, p \Rightarrow r, \neg r \models q$
12. $p, q \Rightarrow (\neg p), (\neg q) \Rightarrow [r \vee (\neg s)], \neg r \models \neg s$
13. $p \Rightarrow (q \vee s), q \Rightarrow r \models p \Rightarrow (r \vee s)$
14. $p \Rightarrow (\neg q), q \Rightarrow p, r \Rightarrow p \models \neg q$
15. $p \Rightarrow q, r \Rightarrow s, \neg(p \Rightarrow s) \models q \wedge (\neg r)$

1.2.4 Lógica com quantificadores

Há muitas espécies de afirmações que se fazem em matemática que não podem ser simbolizadas e logicamente analisadas em termos do cálculo proposicional. Para além das complexidades externas introduzidas pelas diferentes conectivas uma afirmação pode conter complexidades por assim dizer internas que advêm de palavras tais como *"todo"*, *"cada"*, *"algum"*, etc. as quais requerem uma análise lógica que está para além do cálculo proposicional. Tal análise é objecto da chamada **Lógica de Predicados**.

No exemplo que se segue mostram-se as dificuldades que poderiam aparecer se se usasse apenas o cálculo proposicional.

Exemplo 1.16 Sejam P e Q dois conjuntos. Represente-se por p a afirmação *"x é um elemento de P"* e por q a afirmação *"x é um elemento de Q"*. Analisar a sentença

$$(p \Rightarrow q) \vee (q \Rightarrow p)$$

em termos de cálculo proposicional.

Discussão: Antes de mais considere-se a tabela de verdade da sentença dada.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \vee (q \Rightarrow p)$
1	1	1	1	1
1	0	0	1	1
0	1	1	0	1
0	0	1	1	1

O resultado obtido é algo surpreendente visto que a tabela de verdade indica que esta sentença é uma tautologia (sempre verdadeira). Tendo em conta o significado de p e q tem-se então que *"$x \in P$ implica $x \in Q$ ou $x \in Q$ implica $x \in P$"* o que de acordo com o resultado obtido seria sempre verdadeiro. Mas *"$x \in P$ implica $x \in Q$ ou $x \in Q$ implica $x \in P$"* parece afirmar que a proposição *"P é um subconjunto de Q ou Q é um subconjunto de P"* constitui uma afirmação sempre verdadeira.Ora, a própria experiência mostra que há outras situações possíveis para os conjuntos P e Q, nomeadamente P pode não estar contido em Q e, por seu turno, Q pode também não estar contido em P.

Esta análise assim feita conduz a um aparente paradoxo que resultou do facto de nem p nem q serem, de facto, proposições: trata-se de fórmulas abertas ou predicados. Por outro lado uma proposição do tipo *"P é um subconjunto de Q"* tem uma estrutura que requer o uso de quantificadores, isto é, o uso de expressões do tipo *"todo"* (P é um subconjunto de Q se TODO o $x \in P$ pertencer a Q.)

1.2.4.1 Variáveis e conjuntos

No desenvolvimento de qualquer teoria matemática aparecem muitas vezes afirmações sobre objectos genéricos da teoria que são representados por letras designadas por **variáveis**.

Representando por x um número inteiro positivo genérico, pode ser necessário analisar (sob o ponto de vista lógico) afirmações do tipo

"x é um número primo"

Como já foi referido, tal afirmação não é uma proposição: o seu valor lógico tanto pode ser o de verdade como o de falsidade. Uma afirmação deste tipo denota-se genericamente por "$p(x)$" para mostrar que "p" depende da variável x obtendo-se, assim, uma **fórmula** com uma **variável livre**, x. Substituindo x em $p(x)$ por um dado valor, 2 por exemplo, obtém-se $p(2)$ que é uma proposição: $p(2)$ é uma proposição verdadeira; $p(6)$, no entanto, é uma proposição falsa.

Quando se estudam proposições – fórmulas sem variáveis livres – pode falar-se no seu valor lógico de verdade ou falsidade. Mas se uma fórmula contiver variáveis livres (uma ou várias) então não poderá falar-se no seu valor lógico e dizer simplesmente que tal fórmula é verdadeira ou falsa. O seu valor lógico depende do valor atribuído à variável (ou variáveis). A tais afirmações (com variáveis livres) associam-se então os chamados **conjuntos de verdade** que são os conjuntos de valores para os quais $p(x)$ é verdadeira. Escreve-se com este sentido

$$A \;=\; \{\, x : p(x) \,\}$$

o que se lê da seguinte forma: A é o conjunto cujos elementos satisfazem $p(x)$ ou para os quais $p(x)$ é verdadeira. Observe-se que, reciprocamente, dado um conjunto A qualquer pode sempre definir-se uma fórmula com variáveis livres que tem A por conjunto de verdade: basta fazer $p_A(x) \equiv x \in A$ e, portanto,

$$A \;=\; \{\, x : p_A(x) \,\}$$

Conjuntos de verdade e conectivas lógicas. Suponha-se que A é o conjunto de verdade de uma fórmula $p(x)$ e B é o conjunto de verdade de uma fórmula $q(x)$. Então,

$$\begin{array}{rcl} A & = & \{x : p(x)\} \;\equiv\; \{x \in \mathcal{U} : p(x)\} \\ B & = & \{x : q(x)\} \;\equiv\; \{x \in \mathcal{U} : q(x)\} \end{array}$$

O conjunto de verdade da fórmula $p(x) \wedge q(x)$ é tal que

$$\{x \in \mathcal{U} : p(x) \wedge q(x)\} \;=\; \{x \in \mathcal{U} : x \in A \wedge x \in B\} \;=\; A \cap B$$

De modo semelhante,

$$\{x \in \mathcal{U} : p(x) \vee q(x)\} \;=\; \{x \in \mathcal{U} : x \in A \vee x \in B\} \;=\; A \cup B$$

Exercícios 1.2.7 *Determinar os conjuntos de verdade das fórmulas* $\neg p(x)$, $\neg q(x)$, $p(x) \wedge (\neg q(x))$, $p(x) \Rightarrow q(x)$ *e* $p(x) \Leftrightarrow q(x)$.

1.2.4.2 Os quantificadores universal e existencial

Como se referiu acima, uma fórmula $p(x)$, contendo uma variável x, pode ser verdadeira para alguns valores de x pertencentes ao universo do discurso e falsa para outros. Por vezes pretende-se dizer que uma dada fórmula $p(x)$ se verifica para todos os elementos x (do universo). Escreve-se, então

"para todo o x*,* $p(x)$*"*[6]

e representa-se, simbolicamente, por

$$\forall_x \; p(x) \tag{1.9}$$

O símbolo $\forall$ é designado por **quantificador universal**. A fórmula (1.9) diz que $p(x)$ se verifica para todo o elemento x ou que $p(x)$ se verifica universalmente. Sendo $\mathcal{U}$ o universo do discurso, (1.9) equivale ao seguinte

$$\forall_x \; [\, x \in \mathcal{U} \;\Rightarrow\; p(x) \,]$$

A quantificação universal pode ser feita apenas sobre uma parte de $\mathcal{U}$. Assim, se D designar um subconjunto próprio de $\mathcal{U}$ e $p(x)$ for uma fórmula com uma variável cujo domínio é D, então

$$\forall_{x \in D} \; p(x) \quad \text{ou} \quad \forall_x \; [\, x \in D \Rightarrow p(x) \,] \tag{1.10}$$

afirma que $p(x)$ se verifica para todo o $x \in D$.

Exemplo 1.17 Suponha-se que $p(x)$ é a fórmula "$x^2 + 1 > 0$". Então,

$$\forall_x \; [x \in \mathbb{R} \Rightarrow p(x)]$$

é uma proposição verdadeira, enquanto que

$$\forall_x \; [x \in \mathbb{C} \Rightarrow p(x)]$$

é uma proposição falsa.

[6] Ou, *"qualquer que seja* x*,* $p(x)$*"*.

É claro que é sempre possível supor que x é uma variável em $\mathcal{U}$, para o que basta escrever

$$\forall_x \, [\, x \in \mathcal{U} \Rightarrow \, [\, x \in D \Rightarrow p(x) \,] \,]$$

No exemplo 1.17 com a fórmula "$p(x) \equiv x^2 + 1 > 0$", pode sempre supor-se que o universo é $\mathcal{U} \equiv \mathbb{C}$. Então,

$$\forall_x \;\; p(x)$$

é uma proposição falsa, enquanto que

$$\forall_x \, [\, x \in \mathbb{R} \Rightarrow p(x) \,]$$

é uma proposição verdadeira.

Supondo que D é um conjunto finito, por exemplo,

$$D \;=\; \{a_1, a_2, \ldots, a_n\}$$

a fórmula (1.10) é (logicamente) equivalente à conjunção

$$p(a_1) \wedge p(a_2) \wedge \ldots \wedge p(a_n)$$

o que mostra bem que (1.10) não tem variáveis livres, tratando-se, portanto, de uma proposição. O mesmo significado pode ser dado no caso em que D é um conjunto infinito envolvendo agora, correspondentemente, um número infinito de conjunções.

Por outro lado, escreve-se

$$\exists_x \, p(x) \tag{1.11}$$

para significar que existe (no universo do discurso) pelo menos um elemento x para o qual $p(x)$ se verifica, o que se pode ler da seguinte forma

"existe pelo menos um x tal que $p(x)$"

A fórmula (1.11) é uma abreviatura (usada normalmente) para a expressão

$$\exists_x \, [\, x \in \mathcal{U} \wedge p(x) \,]$$

onde, novamente, $\mathcal{U}$ designa o universo do discurso. O símbolo $\exists$ é chamado o **quantificador existencial**.

Se D for um subconjunto de $\mathcal{U}$ e $p(x)$ for uma fórmula com uma variável cujo domínio é D, então

$$\exists_{x \in D} \, p(x) \;\; \text{ou} \;\; \exists_x \, [x \in D \wedge p(x)]$$

é uma fórmula com o quantificador existencial. É claro que é sempre possível supor que x é uma variável em $\mathcal{U}$, para o que basta escrever o seguinte

$$\exists_x \, [x \in \mathcal{U} \wedge x \in D \wedge p(x)]$$

Supondo, novamente, que D é um conjunto finito,

$$D \; = \; \{a_1, a_2, \ldots, a_n\}$$

então a fórmula existêncial

$$\exists_{x \in D} \, p(x) \;\text{ ou }\; \exists_x \, [x \in D \wedge p(x)]$$

é (logicamente) equivalente à disjunção

$$p(a_1) \vee p(a_2) \vee \ldots \vee p(a_n)$$

o que mostra que tal fórmula não tem variáveis livres, sendo, portanto, uma proposição. O mesmo significado pode ser dado no caso em que D é um conjunto infinito, mas envolvendo agora, correspondentemente, disjunções infinitas.

O valor lógico (de verdade ou falsidade) de uma proposição quantificada depende, naturalmente, do domínio considerado. As duas proposições

$$\begin{array}{l} \forall_x \, [x \in \mathbb{Q} \Rightarrow x^2 - 2 = 0\,] \\ \exists_x \, [x \in \mathbb{Q} \, \wedge \, x^2 - 2 = 0\,] \end{array}$$

são falsas enquanto que das duas seguintes

$$\begin{array}{l} \forall_x \, [x \in \mathbb{R} \Rightarrow x^2 - 2 = 0\,] \\ \exists_x \, [x \in \mathbb{R} \, \wedge \, x^2 - 2 = 0\,] \end{array}$$

a primeira é falsa, mas a segunda é verdadeira.

Por uma questão de generalidade interessa considerar também o caso em que o domínio da variável da fórmula $p(x)$ é o conjunto vazio. Que valor lógico terão expressões da forma

$$\forall_x \, [x \in \emptyset \, \Rightarrow p(x)\,] \quad \text{e} \quad \exists_x \, [x \in \emptyset \, \wedge \, p(x)\,]$$

Na primeira expressão a implicação é sempre verdadeira quando o antecedente é falso: é o que acontece aqui. Visto que $x \in \emptyset$ é sempre falso, então

$$\forall_x \, [x \in \emptyset \Rightarrow p(x)\,]$$

é uma proposição sempre verdadeira. Quanto à segunda expressão ela tem a forma de uma conjunção de proposições, das quais uma é sempre falsa. Então,

$$\exists_x \, [x \in \emptyset \wedge p(x)\,]$$

é uma proposição sempre falsa.

Nota 1.18 *Observe-se que enquanto a fórmula $p(x)$ tem uma variável livre, x, as fórmulas $\forall_x \; p(x)$ e $\exists_x \; p(x)$ não têm qualquer variável livre: nestas fórmulas x é sempre uma variável ligada (ou muda). Trata-se então de proposições, relativamente às quais se pode afirmar que são verdadeiras ou falsas (mas não ambas as coisas).*

Por vezes emprega-se o quantificador existêncial numa situação simultânea de unicidade, ou seja, quer-se afirmar não só que

$$\exists_x \; p(x)$$

mas ainda que a fórmula $p(x)$ se transforma numa proposição verdadeira só para um elemento do domínio de quantificação. Neste caso emprega-se a abreviatura

$$\exists!_x \; p(x)$$

que significa *"existe um e um só x tal que $p(x)$"*.

Exercícios 1.2.8

1. *Escrever as frases que se seguem usando notação lógica na qual x designa um gato e $p(x)$ significa "x gosta de creme".*
   (a) *Todos os gatos gostam de creme.*
   (b) *Nenhum gato gosta de creme.*
   (c) *Um gato gosta de creme.*
   (d) *Alguns gatos não gostam de creme.*
2. *Sendo A, B, C três conjuntos, analise em termos lógicos, usando quantificadores, a proposição* "se $A \subseteq B$ então A e $C \backslash B$ são disjuntos".
3. *Traduzir em linguagem simbólica as proposições que se seguem, indicando as escolhas que são apropriadas para os domínios correspondentes.*
   (a) *Existe um inteiro x tal que $4 = x + 2$.*
   (b) *Para todos os inteiros x, $4 = x + 2$.*
   (c) *Cada triângulo equilátero é equiângulo.*

(d) *Todos os estudantes gostam de Lógica.*

(e) *Todos os que entendem Lógica gostam dela.*

(f) $x^2 - 4 = 0$ *tem uma raiz positiva.*

(g) *Toda a solução da equação* $x^2 - 4 = 0$ *é positiva.*

(h) *Nenhuma solução da equação* $x^2 - 4 = 0$ *é positiva.*

4. *Seja* $\mathbb{N}_1 = \{1, 2, 3, 4, \ldots\} = \mathbb{N}\backslash\{0\}$, $p(x)$ *a afirmação "x é par", $q(x)$ a afirmação "x é divisível por 3" e $r(x)$ a afirmação "x é divisível por 4". Expressar em linguagem corrente cada uma das proposições que se seguem e determinar o seu valor lógico.*

(a) $\forall_{x\in\mathbb{N}_1}\ p(x)$

(b) $\forall_{x\in\mathbb{N}_1}\ [p(x) \vee q(x)]$

(c) $\forall_{x\in\mathbb{N}_1}\ [p(x) \Rightarrow q(x)]$

(d) $\forall_{x\in\mathbb{N}_1}\ [p(x) \vee r(x)]$

(e) $\forall_{x\in\mathbb{N}_1}\ [p(x) \wedge q(x)]$

(f) $\exists_{x\in\mathbb{N}_1}\ r(x)$

(g) $\exists_{x\in\mathbb{N}_1}\ [p(x) \wedge q(x)]$

(h) $\exists_{x\in\mathbb{N}_1}\ [p(x) \Rightarrow q(x)]$

(i) $\exists_{x\in\mathbb{N}_1}\ [q(x) \wedge q(x+1)]$

(j) $\exists_{x\in\mathbb{N}_1}\ [p(x) \Rightarrow q(x+1)]$

(k) $\forall_{x\in\mathbb{N}_1}\ [r(x) \Rightarrow p(x)]$

(l) $\forall_{x\in\mathbb{N}_1}\ [p(x) \Rightarrow \neg q(x)]$

(m) $\forall_{x\in\mathbb{N}_1}\ [p(x) \Rightarrow p(x+2)]$

(n) $\forall_{x\in\mathbb{N}_1}\ [r(x) \Rightarrow r(x+4)]$

(o) $\forall_{x\in\mathbb{N}_1}\ [q(x) \Rightarrow q(x+1)]$

5. *Indicar se as proposições são sempre, às vezes ou nunca verdadeiras. Dar exemplos para os domínios D.*

(a) $[\forall_{x\in D}\ p(x)] \Rightarrow [\exists_{x\in D}\ p(x)]$

(b) $[\exists_{x\in D}\ p(x)] \Rightarrow [\forall_{x\in D}\ p(x)]$

(c) $[\forall_{x\in D}\ \neg p(x)] \Rightarrow \neg[\forall_{x\in D}\ p(x)]$

(d) $[\exists_{x\in D}\ \neg p(x)] \Rightarrow \neg[\exists_{x\in D}\ p(x)]$

(e) $\neg[\forall_{x\in D}\ p(x)] \Rightarrow [\forall_{x\in D}\ \neg p(x)]$

(f) $\neg[\exists_{x\in D}\ p(x)] \Rightarrow [\exists_{x\in D}\ \neg p(x)]$

Quantificação múltipla. Uma fórmula matemática pode ter mais de uma variável. Considere-se, por exemplo, a afirmação

> *"para cada número inteiro par n existe um número inteiro k para o qual se verifica a igualdade $n = 2k$"*

Denotando por $p(n, k)$ a fórmula $n = 2k$ e por $\mathbb{P}$ o conjunto dos números inteiros pares, a afirmação pode ser assim apresentada simbolicamente

$$\forall_{n\in\mathbb{P}}\ \exists_{k\in\mathbb{Z}}\ p(n,k) \ \text{ ou } \ \forall_n\,[\,n \in \mathbb{P} \Rightarrow \exists_k\,[\,k \in \mathbb{Z} \wedge p(n,k)\,]\,]$$

que constitui uma proposição verdadeira.

Considere-se agora a proposição que se obtém trocando a ordem dos quantificadores

$$\exists_{k\in\mathbb{Z}}\ \forall_{n\in\mathbb{P}}\ p(n,k) \ \text{ ou } \ \exists_k\,[\,k \in \mathbb{P} \wedge\ \forall_n\,[\,n \in \mathbb{P} \Rightarrow p(n,k)\,]\,]$$

que, em linguagem comum, significa

> *"existe um número inteiro k tal que para todo o número inteiro par n se tem a igualdadde $n = 2k$"*

que é obviamente falsa. Outro exemplo de uma proposição com dois quantificadores é a seguinte

$$\forall_x\ \exists_y\,[\,x + y = 5\,]$$

onde o domínio de quantificação é o conjunto dos números reais. Em linguagem corrente, escrever-se-ia

> *"para todo o número real x existe um número real y tal que $x + y = 5$"*

que constitui uma proposição verdadeira (sendo $y = 5 - x$ para cada $x \in \mathbb{R}$). Se se trocarem os quantificadores obter-se-á

$$\exists_y\ \forall_x\,[\,x + y = 5\,]$$

que significa

> *"existe um número real y tal que para todo o número real x se tem $x + y = 5$"*

Esta proposição é manifestamente falsa pois não existe nenhum número real y, sempre o mesmo, para o qual todo o número real x satisfaz a equação dada.

Estes exemplos ilustram a **não comutatividade** dos dois quantificadores universal, $\forall$, e existencial, $\exists$.

Mais geralmente, uma fórmula pode ter um número qualquer $n \in \mathbb{N}_1$ de variáveis

$$p \;=\; p(x_1, x_2, \ldots, x_n)$$

Para transformar uma tal fórmula numa proposição são necessários n quantificadores. Denotando um quantificador genérico (universal ou existencial) por $\mathbf{Q}$, então

$$\mathbf{Q}_1\, \mathbf{Q}_2 \cdots \mathbf{Q}_n\; p(x_1, x_2, \ldots, x_n)$$

é uma proposição. Dois quantificadores da mesma espécie são sempre comutativos enquanto que dois quantificadores de espécie diferente são geralmente não comutativos, isto é, a sua permuta conduz a proposições de conteúdo distinto.[7]

Negação de proposições quantificadas. Dadas as proposições com quantificadores

$$\forall_x\, [x \in \mathcal{U} \;\Rightarrow p(x)\,] \quad \text{e}$$
$$\exists_x\, [x \in \mathcal{U} \;\wedge\; p(x)\,]$$

pode ser necessário analisar (logicamente) as proposições que são a negação destas, ou seja

$$\neg\,(\forall_x\, [x \in \mathcal{U} \Rightarrow p(x)\,])$$
$$\neg\,(\exists_x\, [x \in \mathcal{U} \;\wedge\; p(x)\,])$$

Suponha-se, por exemplo, que $p(x)$ é a fórmula "x é perfeito" e $\mathcal{H}$ o universo dos seres humanos. Então a proposição

$$\neg\,(\exists_x\, [x \in \mathcal{H} \wedge p(x)\,])$$

[7] Em certos casos muito particulares a permuta dos quantificadores universal e existencial não altera o valor lógico da proposição obtida. É o que se passa, por exemplo, com as proposições seguintes

$$\forall_{x \in \mathbb{N}}\, \exists_{y \in \mathbb{N}}\, [x + y = x]$$
$$\exists_{y \in \mathbb{N}}\, \forall_{x \in \mathbb{N}}\, [x + y = x]$$

onde y é o elemento neutro da adição ($y = 0$).

corresponde a afirmar que "não é verdade que exista um ser humano que seja perfeito" ou, de modo mais coloquial, "ninguém é perfeito". Isto equivale a afirmar que "todos os seres humanos são *não perfeitos* (isto é, *imperfeitos*)", o que pode simbolizar-se assim

$$\forall_x \, [x \in \mathcal{H} \Rightarrow \neg p(x)\,]$$

Tendo em conta que $a \Rightarrow (\neg b)$ é equivalente a $\neg(a \wedge b)$, então

$$\neg\,(\exists_x \, [x \in \mathcal{H} \wedge p(x)\,]) \Leftrightarrow \forall_x \, \neg\,[x \in \mathcal{H} \wedge p(x)\,] \Leftrightarrow \forall_x \, [x \in \mathcal{H} \Rightarrow \neg p(x)\,]$$

De modo semelhante, pode verificar-se que

$$\neg\,(\forall_x \, [x \in \mathcal{U} \Rightarrow p(x)\,])$$

equivale a

$$\exists_x \, \neg\,[x \in \mathcal{U} \Rightarrow p(x)\,] \;\text{ ou }\; \exists_x \, [\,\neg p(x)\,]$$

ou

$$\exists_x \, [x \in \mathcal{U} \wedge \neg p(x)\,]$$

Em resumo, de um modo genérico, têm-se as equivalências

$$\begin{array}{lcl} \neg\,(\forall_x \, p(x)) & \Leftrightarrow & \exists_x \, [\,\neg p(x)\,] \\ \neg\,(\exists_x \, p(x)) & \Leftrightarrow & \forall_x \, [\,\neg p(x)\,] \end{array}$$

conhecidas por **Segundas Leis de Morgan**.

Exercícios 1.2.9

1. *Traduzir em linguagem simbólica, escolhendo em cada caso os universos apropriados, as seguintes afirmações:*
   (a) "Para cada linha l e cada ponto P não pertencente a l existe uma linha l' que passa por P e é paralela a l."
   (b) "Para cada x no conjunto A existe y no conjunto B tal que $f(x) = y$."
   (c) "Para todo o x pertencente ao domínio da função f e para todo o $\epsilon > 0$ existe $\delta > 0$ tal que $|x - c| < \delta$ implica $|f(x) - L| < \epsilon$."
   (d) "Para cada x em G existe x' em G tal que $xx' = e$".
   (e) "A soma de dois números pares é par."
2. *Indicar em linguagem comum a negação de cada uma das afirmações do exercício anterior.*
3. *Seja $p(x, y)$ a fórmula "$x + 2 > y$" e seja $\mathbb{N} \equiv \{0, 1, 2, \ldots\}$ o conjunto dos números naturais. Escrever em linguagem comum o significado das expressões que se seguem e determinar os seus valores lógicos.*

(a) $\forall_{x\in\mathbb{N}}\ \exists_{y\in\mathbb{N}}\ p(x,y)$
(b) $\exists_{x\in\mathbb{N}}\ \forall_{y\in\mathbb{N}}\ p(x,y)$

4. *Indicar o significado das proposições que se seguem, sendo a quantificação feita sobre* $\mathbb{N}$.
   (a) $\forall_x\ \exists_y\ (x<y)$
   (b) $\exists_y\ \forall_x\ (x<y)$
   (c) $\exists_x\ \forall_y\ (x<y)$
   (d) $\forall_y\ \exists_x\ (x<y)$
   (e) $\exists_x\ \exists_y\ (x<y)$
   (f) $\forall_x\ \forall_y\ (x<y)$

   Dizer qual o valor lógico de cada uma delas.

5. *Sendo* $\mathbb{N}$ *o domínio da quantificação, indicar quais das proposições que se seguem são verdadeiras e quais são falsas.*
   (a) $\forall_x\exists_y\ (2x-y=0)$
   (b) $\exists_y\forall_x\ (2x-y=0)$
   (c) $\forall_y\exists_x\ (2x-y=0)$
   (d) $\forall_x\ [\,x<10\Rightarrow\forall_y\ [\,y<x\Rightarrow y<9\,]\,]$
   (e) $\exists_y\exists_z\ (y+z=100)$
   (f) $\forall_x\exists_y\ [\,y>x\wedge(y+x=100)\,]$

   Fazer o mesmo exercício considerando primeiro $\mathbb{Z}$ *e depois* $\mathbb{R}$ *para universos do discurso.*

6. *Dada a proposição* $A\subseteq B$,
   (a) *expressá-la em termos lógicos,*
   (b) *negar a expressão obtida,*
   (c) *traduzir em linguagem comum o resultado obtido na alínea anterior (que equivale a* $A\not\subseteq B$*).*

7. *Negar a proposição* "toda a gente tem um parente de quem não gosta" *usando a simbologia lógica.*

8. *Sendo* $\mathbb{R}$ *o universo do discurso traduzir em linguagem simbólica as seguintes afirmações:*
   (a) *A identidade da adição é o 0.*
   (b) *Todo o número real tem simétrico.*
   (c) *Os números negativos não têm raízes quadradas.*
   (d) *Todo o número positivo possui exactamente duas raízes quadradas.*

9. *Determinar que relação existe entre as duas proposições*

$$\exists_{x\in D}\ [\,p(x)\Rightarrow q(x)\,]\quad\text{e}\quad\exists_{x\in D}\ p(x)\Rightarrow\exists_{x\in D}\ q(x)$$

   Justificar e apresentar exemplos.

10. *Seja M um conjunto e $q(x)$ uma fórmula cujo conjunto de verdade em M é Q, isto é, $Q = \{x \in M : q(x)\}$.*
    (a) *Expressar a proposição $\exists_{x \in M}\ q(x)$ em termos de conjuntos.*
    (b) *Formular a negação do resultado da alínea (a) em termos de Q.*
    (c) *Formular o resultado da alínea (b) em termos de Q^c.*
    (d) *Interpretar logicamente a alínea (c) com uma proposição que envolva $\neg q(x)$.*

1.3 Relações e Aplicações

1.3.1 Produto cartesiano de conjuntos

Os conjuntos $\{a, b\}, \{b, a\}$ e $\{a, b, a\}$ são iguais porque têm os mesmos elementos; a ordem pela qual se escrevem os elementos é irrelevante, assim como não tem qualquer significado que um elemento apareça escrito uma só vez ou várias vezes. Em certas situações, porém, é necessário distinguir conjuntos com os mesmos elementos colocados por ordens diferentes ou conjuntos nos quais um mesmo elemento aparece mais que uma vez. Tais situações aparecem, por exemplo, em geometria analítica plana onde a cada ponto do plano se associa o par de números reais (x, y) que são as suas coordenadas: $(2, 3)$ e $(3, 2)$, por exemplo, são coordenadas de dois pontos distintos. Expressões como estas são designadas por **pares ordenados** e, em termos de conjuntos, podem representar-se da seguinte forma

$$\begin{aligned} (2,3) &= \{\{2\}, \{2,3\}\} \\ (3,2) &= \{\{3\}, \{2,3\}\} \end{aligned}$$

(onde a assimetria dos elementos no segundo membro determina qual é o primeiro elemento e qual é o segundo elemento no primeiro membro). O caso de de um par ordenado cujos elementos são iguais reduz-se ao seguinte:

$$(a, a) = \{\{a\}\}$$

Expressões do tipo (a, b, c) designam-se por **ternos ordenados** e, de um modo geral, expressões da forma $(a_1, a_2, \ldots, a_n)$ designam-se por n**-uplos** ou sequências ordenadas de n elementos. Um n-uplo pode definir-se recursivamente por

$$(a_1, \ldots, a_{n-1}, a_n) \equiv ((a_1, \ldots, a_{n-1}), a_n), \quad n > 2$$

sendo $(a_1, a_2) \equiv \{\{a_1\}, \{a_1, a_2\}\}$. Dois pares ordenados são iguais se tiverem o mesmo primeiro elemento **e** o mesmo segundo elemento, isto é,

$$(a, b) = (a', b') \Leftrightarrow a = a' \wedge b = b'$$

o que decorre imediatamente da definição de par ordenado dada acima. Considerações análogas se podem fazer relativamente à igualdade de dois n-uplos.

Definição 1.19 *Sejam A e B dois conjuntos não vazios. Chama-se* **produto cartesiano** *de A por B, e representa-se por $A \times B$, ao conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$, ou seja*

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

No caso particular em que se tem $A = B$ obtém-se o conjunto

$$A^2 = \{(a, a') : a, a' \in A\}$$

designado por **quadrado cartesiano** *de A.*

O conceito de produto cartesiano pode ser estendido a mais de dois conjuntos de modo natural. Assim, sendo A, B e C três conjuntos quaisquer, o produto cartesiano de A por B por C, denotado por $A \times B \times C$, é o conjunto de todos os ternos ordenados (x, y, z) onde $x \in A$, $y \in B$ e $z \in C$:

$$A \times B \times C = \{(x, y, z) : x \in A \wedge y \in B \wedge z \in C\}$$

Analogamente, o produto cartesiano de n conjuntos $A_1, A_2, \ldots, A_n$, denotado por $A_1 \times A_2 \times \cdots \times A_n$ é definido por

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_1 \in A_1 \wedge x_2 \in A_2 \wedge \ldots \wedge x_n \in A_n\}$$

Se, em particular, se tiver $A_1 = A_2 = \cdots = A_n = A$ obtém-se

$$\begin{aligned} A_1 \times \cdots \times A_n &= A^n \\ &= \{(x_1, \ldots, x_n) : x_i \in A \text{ para todo } i = 1, 2, \ldots, n\} \end{aligned}$$

que é a potência cartesiana de ordem n do conjunto A.

Definição 1.20 *Chama-se* **relação binária** *de A para B a todo o subconjunto não vazio $\mathcal{R}$ do produto cartesiano $A \times B$. Se, em particular, for $A = B$ então $\mathcal{R}$ diz-se uma relação binária definida em A.*

Exemplo 1.21 Sejam dados os conjuntos

$$\mathbf{A} = \{1, 2, 3\} \quad \text{e} \quad \mathbf{B} = \{r, s\}$$

Então

$$\mathcal{R} = \{(1, r), (2, s), (3, r)\}$$

é uma relação de $\mathbf{A}$ para $\mathbf{B}$.

Exemplo 1.22 Sejam $\mathbf{A}$ e $\mathbf{B}$ conjuntos de números reais. A relação $\mathcal{R}$ (de igualdade) define-se da seguinte forma

$$a\mathcal{R}b \text{ se e só se } a = b$$

para todo o $a \in \mathbf{A}$ e todo o $b \in \mathbf{B}$.

Exemplo 1.23 Seja dado o conjunto

$$\mathbf{A} = \{1, 2, 3, 4, 5\} = \mathbf{B}$$

Definindo a relação $\mathcal{R}$ (menor que) em $\mathbf{A}$:

$$a\mathcal{R}b \text{ se e só se } a < b$$

então

$$\mathcal{R} = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$$

Dada uma relação $\mathcal{R}$ do conjunto A para o conjunto B chama-se **domínio** e **contradomínio** de $\mathcal{R}$, respectivamente, aos conjuntos assim definidos:

$$\begin{aligned} \mathbf{D}(\mathcal{R}) &= \{x \in A : \exists_y \, [y \in B \wedge (x, y) \in \mathcal{R}]\} \\ \mathbf{I}(\mathcal{R}) &= \{y \in B : \exists_x \, [x \in A \wedge (x, y) \in \mathcal{R}]\} \end{aligned}$$

Exemplo 1.24 Seja dado o conjunto $\mathbf{A} = \{a, b, c, d\} = \mathbf{B}$ e a relação $\mathcal{R}$ definida por

$$\mathcal{R} = \{(a, a), (a, b), (b, c), (c, a), (d, c), (c, b)\}$$

Então,

$$\begin{aligned} \mathcal{R}(a) &= \{a, b\} \\ \mathcal{R}(b) &= \{c\} \\ &\vdots \\ \mathbf{D}(\mathcal{R}) &= \{a, b, c, d\} = A \\ \mathbf{I}(\mathcal{R}) &= \{a, b, c\} \end{aligned}$$

1.3.1.1 Representação de relações

Apresentar-se-ão dois modos distintos para representar relações, um de tipo algébrico e outro de tipo geométrico. Cada um deles tem vantagens e desvantagens em relação ao outro, tudo dependendo da aplicação particular a que se destinam.

Matriz de uma relação. Sejam $A = \{a_1, a_2, \ldots, a_m\}, B = \{b_1, b_2, \ldots, b_n\}$ dois conjuntos finitos com m e n elementos respectivamente. Uma relação $\mathcal{R}$ de A para B pode representar-se por uma matriz $R = [r_{ij}]_{1 \leq i \leq m; 1 \leq j \leq n}$ cujos elementos são definidos por

$$r_{ij} = \begin{cases} 1 & \text{se} \quad (a_i, b_j) \in \mathcal{R} \\ 0 & \text{se} \quad (a_i, b_j) \notin \mathcal{R} \end{cases}$$

A matriz R tem $m = \mathbf{card}(A)$ linhas e $n = \mathbf{card}(B)$ colunas.

Exemplo 1.25 *Dados os conjuntos* $A = \{1, 2, 3\}$ *e* $B = \{r, s\}$ *considere-se a relação de* A *para* B

$$\mathcal{R} \ = \ \{(1, r), (2, s), (3, r)\}$$

Determinar a matriz de $\mathcal{R}$.
Resolução: Tomando A para definir os índices de linha e B para definir os índices de coluna, vem

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

Reciprocamente, dados dois conjuntos A e B de cardinalidades m e n, respectivamente, uma matriz de $m \times n$ cujos elementos são 0's e 1's determina sempre uma relação de A para B.

Exemplo 1.26 A matriz

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

tem 3 linhas e 4 colunas. Fazendo $A = \{a_1, a_2, a_3\}$ e $B = \{b_1, b_2, b_3, b_4\}$, aquela matriz pode representar a relação de A para B definida por

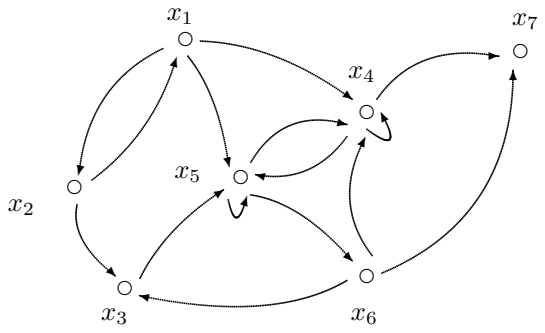
$$\mathcal{R} \ = \ \{(a_1, b_1), (a_1, b_4), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_3)\}$$

Digrafo de uma relação. Seja dado um conjunto $\mathbf{X}$ no qual se encontra definida uma relação $\mathcal{R}$. Esta relação pode representar-se graficamente por um diagrama com pontos que são os elementos do conjunto $\mathbf{X}$ e arcos orientados que ligam dois vértices x_i, x_j (com a orientação de x_i para x_j) sempre que se tenha $(x_i, x_j) \in \mathcal{R}$. A tal representação dá-se o nome de **grafo orientado** ou, mais simplesmente, **digrafo**.[8]

Exemplo 1.27 Seja dado o conjunto $\mathbf{X} = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ e a relação $\mathcal{R}$ definida sobre $\mathbf{X}$ por

$$\begin{aligned}\mathcal{R} \;=\; & \{(x_1,x_2),(x_1,x_4),(x_1,x_5),(x_2,x_1),(x_2,x_3),(x_3,x_5),\\ & (x_4,x_4),(x_4,x_5),(x_4,x_6),(x_4,x_7),(x_5,x_4),(x_5,x_5),\\ & (x_6,x_3),(x_6,x_6),(x_6,x_7)\}\end{aligned}$$

A representação gráfica de $\mathcal{R}$ sobre $\mathbf{X}$ toma, neste caso, a forma



1.3.2 Partições e relações de equivalência

Seja A um conjunto não vazio. Chama-se **partição** de A a uma família $\mathcal{P}_A$ de subconjuntos não vazios de A tais que:

1. Cada elemento de A pertence a um e um só conjunto de $\mathcal{P}_A$.
2. Se A_1 e A_2 forem dois elementos distintos da partição $\mathcal{P}_A$ então $A_1 \cap A_2 = \emptyset$.

Os elementos de $\mathcal{P}_A$ são designados por **blocos** ou **células** da partição.

[8] Do inglês *"di*rected *graph"*.

Exemplo 1.28 Seja dado o seguinte conjunto

$$A = \{a, b, c, d, e, f, g, h\}$$

e considerem-se os seguintes subconjuntos de A:

$$A_1 = \{a, b, c, d\}, \quad A_2 = \{a, c, e, f, g, h\},$$

$$A_3 = \{a, c, e, g\}, \quad A_4 = \{b, d\}, \quad A_5 = \{f, h\}$$

Então $\{A_1, A_2\}$ não é uma partição de A visto que $A_1 \cap A_2 \neq \emptyset$; $\{A_1, A_5\}$ também não é uma partição visto que $e \notin A_1$ e $e \notin A_5$. A família $\mathcal{P}_A = \{A_3, A_4, A_5\}$ é uma partição de A.

Definição 1.29 *Seja A um conjunto não vazio e $\mathcal{R}$ uma relação binária definida em A. A relação $\mathcal{R} \subseteq A^2$ dir-se-á uma* **relação de equivalência** *em A se satisfizer as seguintes propriedades:*

- **(a) reflexividade:** $\forall_a \, [\, a \in A \Rightarrow a\mathcal{R}a \,]$,
- **(b) simetria:** $\forall_{a,b \in A} \, [\, a\mathcal{R}b \Rightarrow b\mathcal{R}a \,]$
- **(c) transitividade:** $\forall_{a,b,c \in A} \, [\, [\, a\mathcal{R}b \wedge b\mathcal{R}c \,] \Rightarrow a\mathcal{R}c \,]$

Sendo A um conjunto e $\mathcal{R} \subseteq A^2$ uma relação de equivalência chama-se **classe de equivalência** que contém o elemento $a \in A$ ao conjunto, denotado geralmente por $[a]$, definido por

$$[a] = \{x \in A : (x, a) \in \mathcal{R}\},$$

onde o elemento $a \in A$ se diz **representante** da classe.

Teorema 1.30 *Seja $\mathcal{R}$ uma relação de equivalência definida num conjunto A. Então:*

- **(1)** *cada elemento de A pertence à sua classe de equivalência, isto é, $a \in [a]$, qualquer que seja $a \in A$;*
- **(2)** *a reunião de todas as classes de equivalência é o conjunto A, isto é, $\cup_{a \in A}[a] = A$;*
- **(3)** *dados dois elementos $a, b \in A$ ter-se-á $a\mathcal{R}b$ quando e só quando a e b pertencerem à mesma classe de equivalência, isto é,*

$$\forall_{a,b \in A} \, [\, a\mathcal{R}b \Leftrightarrow [a] = [b] \,];$$

(4) *as classes de equivalência de dois elementos a, b de A para as quais é falsa a proposição "$a\mathcal{R}b$" são disjuntas, isto é,*

$$\forall_{a,b\in A}\ [\ \neg(a\mathcal{R}b)\ \Rightarrow\ [a]\cap[b]=\emptyset\ ]$$

Demonstração: (1) Seja $a \in A$. Já que $\mathcal{R} \subset A^2$ é uma relação reflexiva então $a\mathcal{R}a$ é uma proposição verdadeira e, portanto, $a \in [a]$.
(2) Decorre imediatamente de (1).
(3) Sejam $a, b \in A$. Se $[a] = [b]$ então $a \in [a] = [b]$, donde, $a\mathcal{R}b$. Reciprocamente, suponha-se que se tem $a\mathcal{R}b$. Então se $x \in [a]$ tem-se $x\mathcal{R}a$ e, portanto, atendendo à transitividade de $\mathcal{R}$ será também $x\mathcal{R}b$ o que significa que $x \in [b]$. Isto é, qualquer que seja $x \in A$, se $x \in [a]$ tem-se também que $x \in [b]$; de modo semelhante (usando adicionalmente a simetria da relação $\mathcal{R}$) se prova que qualquer que seja $x \in A$ se $x \in [b]$ então será necessariamente $x \in [a]$. Consequentemente $[a] = [b]$.
(4) Equivale a provar que se $[a] \cap [b] \neq \emptyset$ então $a\mathcal{R}b$ é uma proposição verdadeira. Ora se existir $x \in A$ tal que $x \in [a]$ e $x \in [b]$ então tem-se que $x\mathcal{R}a$ e $x\mathcal{R}b$, donde, por simetria e transitividade, se tem também $a\mathcal{R}b$, como se pretendia mostrar. □

Definição 1.31 *Seja A um conjunto e $\mathcal{R}$ uma relação de equivalência em A. Chama-se* **conjunto quociente** *de A por $\mathcal{R}$, e denota-se por $A/\mathcal{R}$, ao conjunto de todas as classes de equivalência determinadas em A por $\mathcal{R}$,*

$$A/\mathcal{R}\ =\ \{[a] : a \in A\}$$

Uma relação de equivalência num conjunto não vazio A origina uma partição desse conjunto em classes de equivalência que são os blocos da partição obtida. Reciprocamente,

Teorema 1.32 *Seja $\mathcal{P}$ uma partição de um conjunto não vazio A e $\mathcal{R}$ a relação definida em A por*

$$a\mathcal{R}b \Leftrightarrow a \text{ e } b \text{ pertencem ao mesmo bloco de } \mathcal{P}$$

Então $\mathcal{R}$ é uma relação de equivalência.

Demonstração: (a) É claro que se $a \in A$ então $a\mathcal{R}a$ (o elemento a estás no mesmo bloco dele próprio).
(b) Se $a\mathcal{R}b$ então a e b estão no mesmo bloco e, portanto, $b\mathcal{R}a$.
(c) Se $a\mathcal{R}b$ e $b\mathcal{R}c$, então a, b e c estão no mesmo bloco. Logo $a\mathcal{R}c$
Visto que $\mathcal{R}$ é reflexiva, simétrica e transitiva então é uma relação de equivalência, designada **relação de equivalência determinada pela partição** $\mathcal{P}$. □

Exemplo 1.33 *Seja dado o conjunto* $A = \{1, 2, 3, 4\}$ *e considere-se a partição* $\mathcal{P} = \{\{1, 2, 3\}, \{4\}\}$. *Determinar a relação de equivalência determinada em* A *pela partição* $\mathcal{P}$.

Resolução: Visto que os blocos de $\mathcal{P}$ são $\{1, 2, 3\}$ e $\{4\}$, então

$$\mathcal{R} \;=\; \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3),(4,4)\}$$

é a relação de equivalência induzida em A pela partição $\mathcal{P}$.

1.3.3 Relações de ordem

Seja A um conjunto não vazio e $\mathcal{R} \subseteq A^2$ uma relação binária qualquer definida em A. Para indicar que o par ordenado $(a, b) \in A^2$ pertence à relação $\mathcal{R}$ escreve-se também frequentemente $a\mathcal{R}b$, ou seja,

$$a\mathcal{R}b \;\Leftrightarrow\; (a, b) \in \mathcal{R}$$

quaisquer que sejam $a, b \in A$.

Exemplo 1.34 Se $A = \{0, 1, 2, 3, 4, 5\} \subset \mathbb{N}$ e $\mathcal{R}$ for a relação $\leq$ usual em $\mathbb{N}$, então

$$\begin{aligned} \leq \;=\; \{&(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),\\ &(1,1),(1,2),(1,3),(1,4),(1,5),\\ &(2,2),(2,3),(2,4),(2,5),(3,3),(3,4),(1,5),(4,4),(4,5),(5,5)\} \end{aligned}$$

e escreve-se

$$a \leq b \;\;\Leftrightarrow\;\; (a, b) \in \leq$$

quaisquer que sejam $a, b \in A$.

Definição 1.35 *Chama-se* **relação de ordem** *definida no conjunto* A *a uma relação binária* $\mathcal{R} \subseteq A^2$ *com as seguintes propriedades:*

(1) reflexividade: $\forall_a \, [\, a \in A \Rightarrow a\mathcal{R}a \,]$,

(2) anti-simetria: $\forall_{a,b \in A} \, [\, [\, a\mathcal{R}b \wedge b\mathcal{R}a \,] \;\Rightarrow\; a = b \,]$

(3) transitividade: $\forall_{a,b,c \in A} \, [\, [\, a\mathcal{R}b \wedge b\mathcal{R}c \,] \;\Rightarrow\; a\mathcal{R}c \,]$

Se, adicionalmente, $\mathcal{R}$ *satisfizer a proposição*

(4) dicotomia: $\forall_{a,b} \, [\, a, b \in A \;\Rightarrow\; [\, a\mathcal{R}b \vee b\mathcal{R}a \,] \,]$

dir-se-á uma **relação de ordem total**. *Se* $\mathcal{R}$ *não for uma relação de ordem total também se designa, por vezes, relação de ordem parcial.*

Exemplo 1.36

1. Seja $\mathcal{A}$ uma família de conjuntos. A relação em $\mathcal{A}$ definida por *"A é um subconjunto de B"* é uma ordem parcial.
2. Seja A um subconjunto qualquer de números reais. A relação $\leq$ em A é uma relação de ordem total – é a chamada *ordem natural*.
3. A relação $\mathcal{R}$ definida em $\mathbb{N}$ por *"$x\mathcal{R}y$ se e só se x é múltiplo de y"* é uma relação de ordem parcial em $\mathbb{N}$.

Definição 1.37 *Seja $\mathcal{R}$ uma relação de ordem definida em A; a relação $\mathcal{R}^* \subset A^2$ definida por*

$$\forall_{a,b\in A}\,[\, a\mathcal{R}^* b \;\Leftrightarrow\; [\, a\mathcal{R}b \wedge a \neq b\,]\,] \tag{1.12}$$

diz-se uma **relação de ordem estrita** *definida em A.*

Definição 1.38 *Chama-se* **conjunto ordenado** *a um par ordenado $(A, \mathcal{R})$ onde A é um conjunto não vazio e $\mathcal{R}$ é uma relação de ordem (parcial ou total) em A.*

Se, para $a, b \in A$ se tiver $a\mathcal{R}b$ dir-se-á que b **domina** a ou que a **precede** b.

Seja $\mathcal{R}$ uma relação de ordem num conjunto A. Então a relação inversa $\mathcal{R}^{-1}$, definida por

$$a\mathcal{R}^{-1}b \;\Leftrightarrow\; b\mathcal{R}a$$

quaisquer que sejam os elementos $a, b \in A$, é também uma relação de ordem (*verificar!*). As ordens parciais mais familiares são as relações $\leq$ ou $\geq$ em $\mathbb{Z}$ ou $\mathbb{R}$ (que são inversas uma da outra). Por isso, muitas vezes se denota um conjunto ordenado simplesmente por

$$(A, \leq) \quad \text{ou} \quad (A, \geq)$$

embora as ordens $\leq$ ou $\geq$ possam não corresponder às relações usuais em $\mathbb{Z}$ ou $\mathbb{R}$ denotadas por aqueles símbolos.

Elementos extremais de um conjunto ordenado. Sendo $(A, \leq)$ um conjunto (total ou parcialmente) ordenado dá-se o nome de **máximo** de A ao elemento de $a \in A$, se existir, tal que

$$\forall_x\,[\, x \in A \;\Rightarrow\; x \leq a\,]$$

ou seja, a é o máximo de A se dominar todos os outros elementos de A. Note-se que se a ordem $\leq$ não for total pode acontecer que não exista um

elemento $a \in A$ comparável com todos os elementos $x \in A$ nos termos acima indicados: neste caso A não possuirá máximo.

Um elemento $a \in A$ diz-se **maximal** de $(A, \leq)$ se se verificar a condição

$$\forall_{x \in A} \, [\, a \leq x \, \Rightarrow \, x = a \,]$$

ou, equivalentemente,

$$\neg \, \exists_{x \in A} \, [\, a \leq x \, \wedge \, x \neq a \,]$$

Isto é, $a \in A$ é um elemento maximal de $(A, \leq)$ se não existir nenhum outro elemento em A que o domine estritamente.

De modo semelhante, chama-se **mínimo** de A ao elemento $b \in A$, se existir, que satisfaz a condição

$$\forall_{x} \, [\, x \in A \, \Rightarrow \, b \leq x \,]$$

ou seja, b é o mínimo de A se preceder todos os outros elementos de A. Tal como no caso anterior um conjunto ordenado pode não possuir mínimo.

Um elemento $b \in A$ diz-se **minimal** se se verificar a condição

$$\forall_{x \in A} \, [\, x \leq b \, \Rightarrow \, x = b \,]$$

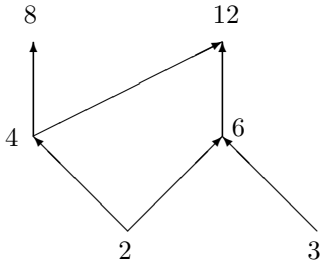
ou, equivalentemente,

$$\neg \, \exists_{x \in A} \, [\, x \leq b \, \Rightarrow \, x \neq b \,]$$

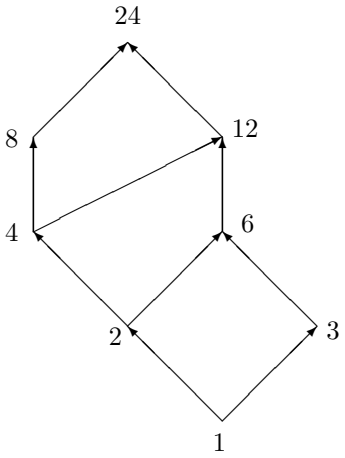
Isto é, $b \in A$ é um elemento minimal de $(A, \leq)$ se não existir nenhum outro elemento em A que o preceda estritamente.

Exemplo 1.39 (Diagramas de Hasse.) Seja A um conjunto finito com uma ordem parcial $\leq$ e considere-se o digrafo desta relação. Visto que $\leq$ é uma relação de ordem então é reflexiva e, portanto, em todos os vértices aparecerá um lacete. Para simplificar o diagrama neste caso suprimam-se todos os lacetes. Eliminando também todos os arcos que se obtêm por transitividade o digrafo resultante é o que se designa por **diagrama de Hasse** correspondente à ordem parcial $\leq$.

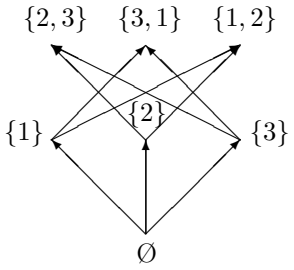
1. Seja $A = \{2, 3, 4, 6, 8, 12\}$ e defina-se a relação $\leq$ pondo *"$x \leq y$ se e só se x divide y"*. Então 2 e 3 são elementos minimais e 8 e 12 são elementos maximais. O conjunto ordenado $(A, \leq)$ não possui mínimo nem máximo. Esta situação pode representar-se pelo diagrama de Hasse



2. Seja agora $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$ $(= A \cup \{1, 24\})$ com a ordem $\leq$ tal como foi definida no exemplo anterior. Então 1 é o mínimo de B e 24 é o máximo de B. 1 é o único elemento minimal de B e 24 é o único elemento maximal de B. O diagrama de Hasse agora tem o seguinte aspecto:



3. Seja $C = \{1, 2, 3\}$ e considere-se o conjunto D das partes próprias de C ordenado pela relação $\subseteq$. Então $\emptyset$ é o mínimo de D e há três elementos maximais, $\{2, 3\}$, $\{3, 1\}$ e $\{1, 2\}$.



Contra-exemplo 1.40 O conjunto $A = \{x \in \mathbb{R} : 0 < x < 1\}$ não possui máximo nem mínimo nem possui elementos maximais nem minimais.

Teorema 1.41 *Seja A um conjunto ordenado pela relação de ordem (parcial ou total) $\leq$. Se $a \in A$ é máximo então a é um elemento maximal e é o único elemento maximal de A. Se $b \in A$ é mínimo então b é um elemento minimal e é o único elemento minimal de A.*

Demonstração: Seja a o máximo de A e seja $x \in A$ tal que $a \leq x$. Pela definição de máximo de A tem-se também $x \leq a$ e, portanto, pela antisimetria da relação $\leq$ obter-se-á $x = a$, o que mostra que a é um elemento maximal de A.

Para provar que aquele elemento maximal é único suponha-se agora que a' é outro elemento maximal. Visto que a é, por hipótese, o máximo de A então ter-se-á $a' \leq a$ o que, pela definição de elemento maximal, implica que seja $a = a'$. Consequentemente, não pode haver outro elemento maximal.

A demonstração para o caso do mínimo é semelhante, sugerindo-se que seja feita a título de exercício. □

Definição 1.42 *Seja $(A, \leq)$ um conjunto ordenado. Chama-se* **cadeia** *de A a um subconjunto de A que é totalmente ordenado por $\leq$.*

No exemplo 1 acima, o conjunto $\{2, 4, 12\}$ é uma cadeia; no exemplo 2, o conjunto $\{1, 2, 6, 12, 24\}$ é uma cadeia e no exemplo 3, o conjunto $\{\emptyset, \{1\}, \{1, 2\}\}$ é uma cadeia.

Definição 1.43 *Seja A um conjunto totalmente ordenado pela relação $\leq$. Dir-se-á que $\leq$ é uma* **boa ordem** *ou que A é* **bem ordenado** *por $\leq$ se todo o subconjunto não vazio de A possuir mínimo.*

O exemplo típico de um conjunto bem ordenado é dado por $\mathbb{N}$ provido com a relação de ordem $\leq$ usual, enquanto que $\mathbb{Z}$ com a ordenação usual não é bem ordenado. Por razões análogas também $\mathbb{Q}$ ou $\mathbb{R}$ com as suas ordenações usuais também não são conjuntos bem ordenados.

Exercícios 1.3.1

1. *Sendo o par ordenado (a, b) definido em termos de conjuntos por $(a, b) = \{\{a\}, \{a, b\}\}$ mostrar que se verifica a seguinte equivalência:*

$$(a, b) = (c, d) \Leftrightarrow [a = c \wedge b = d]$$

   quaisquer que sejam os pares ordenados (a, b) e (c, d).

2. *Sejam dados os conjuntos $A = \{a, b, c\}$, $B = \{1, 2\}$ e $C = \{4, 5, 6\}$.*

(a) *Descrever em extensão os conjuntos* $A \times B$, $B \times A$ *e* $A \times C$.

(b) *Dar exemplos de relações de* A *para* B *e de* B *para* A *com quatro elementos.*

(c) *Dar um exemplo de uma relação simétrica em* C *com três elementos.*

3. *Seja* $A = \{1, 2, 3\}$. *Para cada uma das relações* $\mathcal{R}$ *indicadas a seguir, determinar os elementos de* $\mathcal{R}$, *o domínio e o contradomínio de* $\mathcal{R}$ *e, finalmente, indicar as propriedades que possui* $\mathcal{R}$.

(a) $\mathcal{R}$ *é a relação* $<$ *em* A.

(b) $\mathcal{R}$ *é a relação* $\geq$ *em* A.

(c) $\mathcal{R}$ *é a relação* $\subset$ *em* $\mathcal{P}(A)$.

4. *Sejam* A, B, C *e* D *conjuntos dados. Provar ou dar contra-exemplos para as seguintes conjecturas:*

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(c) $(A \times B) \cap (A^c \times B) = \emptyset$

(d) $[A \subseteq B \wedge C \subseteq D] \Rightarrow A \times C \subseteq B \times D$

(e) $A \cup (B \times C) = (A \cup B) \times (A \cup C)$

(f) $A \cap (B \times C) = (A \cap B) \times (A \cap C)$

(g) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

(h) $A \times (B \backslash C) = (A \times B) \backslash (A \times C)$

5. *Sejam* A *e* B *dois conjuntos e* $\mathcal{R}$ *e* $\mathcal{S}$ *duas relações de* A *para* B. *Mostrar que*

(a) $\mathbf{D}(\mathcal{R} \cup \mathcal{S}) = \mathbf{D}(\mathcal{R}) \cup \mathbf{D}(\mathcal{S})$

(b) $\mathbf{D}(\mathcal{R} \cap \mathcal{S}) \subseteq \mathbf{D}(\mathcal{R}) \cap \mathbf{D}(\mathcal{S})$ *e dar um exemplo para mostrar que a igualdade não se verifica necessariamente.*

(c) $\mathbf{I}(\mathcal{R} \cup \mathcal{S}) = \mathbf{I}(\mathcal{R}) \cup \mathbf{I}(\mathcal{S})$

(d) $\mathbf{I}(\mathcal{R} \cap \mathcal{S}) \subseteq \mathbf{I}(\mathcal{R}) \cap \mathbf{I}(\mathcal{S})$ *e dar um exemplo para mostrar que a igualdade não se verifica necessariamente.*

6. *Seja* $\mathcal{R}$ *uma relação num conjunto não vazio* A. *Sendo* $x \in A$ *define-se a classe-*$\mathcal{R}$ *de* x, *denotada por* $[x]_{\mathcal{R}}$, *por*

$$[x]_{\mathcal{R}} \;=\; \{y \in A : y \mathcal{R} x\}$$

(a) *Sendo* $A = \{1, 2, 3, 4\}$ *e*

$$\mathcal{R} \;=\; \{(1,2), (1,3), (2,1), (1,1), (2,3), (4,2)\}$$

determinar $[1]_{\mathcal{R}}$, $[2]_{\mathcal{R}}$, $[3]_{\mathcal{R}}$ *e* $[4]_{\mathcal{R}}$.

(b) *Mostrar que* $\mathcal{R}$ *é reflexiva se e só se* $\forall_{x \in A} \, [x \in [x]_{\mathcal{R}}]$.

(c) *Mostrar que* $\mathcal{R}$ *é simétrica se e só se*

$$\forall_{x,y \in A} \, [x \in [y]_{\mathcal{R}} \Rightarrow y \in [x]_{\mathcal{R}}]$$

(d) *Mostrar que* $\forall_{x\in A}\,[\,[x]_{\mathcal{R}} \neq \emptyset \Leftrightarrow \mathbf{I}(\mathcal{R}) = A\,]$.

(e) *Suponha-se que* $\mathbf{D}(\mathcal{R}) = A$ *e* $\mathcal{R}$ *é simétrica e transitiva. Mostrar que*

$$\forall_{x,y\in A}\,[[x]_{\mathcal{R}} \subseteq [y]_{\mathcal{R}} \;\Rightarrow\; x\mathcal{R}y]$$

Mostrar ainda que $\forall_{x,y\in A}\,[[x]_{\mathcal{R}} \subseteq [y]_{\mathcal{R}} \Rightarrow [x]_{\mathcal{R}} = [y]_{\mathcal{R}}]$.

(f) *Suponha-se que* $\mathcal{R}$ *é simétrica e transitiva. Mostrar que*

$$\forall_{x,y\in A}\,[[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \emptyset \;\Rightarrow\; [x]_{\mathcal{R}} = [y]_{\mathcal{R}}]$$

7. *Seja* $\mathcal{R}$ *uma relação de* A *para* B *e* $\mathcal{S}$ *uma relação de* B *para* C. *Então a* **relação composta** $\mathcal{S}\circ\mathcal{R}$ *é a relação constituída por todos os pares ordenados* (a,c) *tais que* $(a,b) \in \mathcal{R}$ *e* $(b,c) \in \mathcal{S}$. *Sendo* $A = \{p,q,r,s\}$, $B = \{a,b\}$, $C = \{1,2,3,4\}$, $\mathcal{R} = \{(p,a),(p,b),(q,b),(r,a),(s,a)\}$ *e* $\mathcal{S} = \{(a,1),(a,2),(b,4)\}$ *determinar* $\mathcal{S}\circ\mathcal{R}$.

8. *Seja* $\mathcal{R}$ *uma relação de* A *para* B. *Chama-se* **relação inversa** $\mathcal{R}^{-1}$ *de* B *para* A *ao conjunto de pares ordenados da forma* (b,a) *com* $(a,b) \in \mathcal{R}$. *Mostrar que uma relação* $\mathcal{R}$ *num conjunto é simétrica se e só se* $\mathcal{R} = \mathcal{R}^{-1}$.

9. *Mostrar que uma relação num conjunto é reflexiva se e só se a sua inversa for reflexiva.*

10. *Seja* $\mathcal{R}$ *a relação no conjunto* $A = \{1,2,3,4,5,6,7\}$ *definida por*

$$(a,b) \in \mathcal{R} \;\Leftrightarrow\; (a-b) \text{ é divisível por } 4$$

Determinar $\mathcal{R}$ *e* $\mathcal{R}^{-1}$.

11. *Seja* $\mathcal{R}$ *a relação definida em* $\mathbb{N}_1$ *por*

$$(a,b) \in \mathcal{R} \;\Leftrightarrow\; b \text{ é divisível por } a$$

Estudar $\mathcal{R}$ *quanto à reflexividade, simetria, antisimetria e transitividade.*

12. *Quais das relações que se seguem são equivalências?*

(a) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(3,1)\}$

(b) $\{(1,2),(2,2),(3,3),(4,4)\}$

(c) $\{(1,1),(2,2),(1,2),(2,1),(3,3),(4,4)\}$

13. *Seja* $\mathcal{R} = \{(x,y) : x,y \in \mathbb{Z} \text{ e } x-y \text{ é inteiro}\}$. *Mostrar que* $\mathcal{R}$ *é uma relação de equivalência em* $\mathbb{Z}$.

14. *Seja* $A = \{2,3,4,5,\ldots\}$ *um conjunto ordenado pela relação "*x *divide* y. *Determinar todos os elementos minimais e todos os elementos maximais.*

1.3.4 Funções

Definição 1.44 *Seja* $f \subset A \times B$ *uma relação de* A *para* B. *Se, para todo o* $x \in A$ *existir* **um e um só** $y \in B$ *tal que* $(x,y) \in f$ *dir-se-á que* f *é uma*

aplicação *(ou* **função***) de A em B; para significar que f é uma aplicação de A em B costuma escrever-se*

$$f : A \rightarrow B$$

e, neste caso, escreve-se $y = f(x)$, dizendo-se que $y \in B$ é a **imagem** *por f de $x \in A$.*

Dada uma aplicação $f : A \rightarrow B$, ao conjunto A também se dá o nome de **domínio** de f e com este significado representa-se por $\mathbf{D}(f) \equiv \mathbf{D}_f$ (ou, mais simplesmente, por $\mathbf{D}$).

Exemplo 1.45 Como exemplos de algumas relações que são funções e outras que o não são, considere-se

$$\begin{array}{rcl} A & = & \{1,2,3,4\} \\ B & = & \{1,2,3,4,5\} \\ f & = & \{(1,2),(2,3),(3,4),(4,5)\} \\ g & = & \{(1,2),(1,3),(2,4),(3,5),(4,5)\} \\ h & = & \{(1,1),(2,2),(3,3)\} \end{array}$$

Então f, g e h são relações de A para B mas apenas f é uma função definida em A; g e h não são funções definidas em A a primeira porque tanto $(1,2)$ como $(1,3)$ são elementos de g e a segunda porque $\mathbf{D}(h) = \{1,2,3\} \neq A$. A função f é particularmente simples, podendo ser descrita pela fórmula $f(x) = x+1$ qualquer que seja $x \in A$. Embora a maior parte das funções normalmente consideradas nas disciplinas de Cálculo sejam dadas de forma semelhante, em geral, não se podem especificar as funções deste modo; de facto, a maioria das funções que se podem definir não podem ser descritas de forma tão simples à custa de uma fórmula algébrica.

O conjunto

$$\mathbf{I}(f) \equiv f(A) \ = \ \{y \in B : \ [\, \exists_x \, [\, x \in A \wedge y = f(x) \,]\,]\}$$

designa-se por contradomínio da aplicação f. Se $f(A) = B$ dir-se-á que f é uma **aplicação sobrejectiva** (ou aplicação sobre B); a aplicação $f : A \rightarrow B$ diz-se **injectiva** (ou unívoca) se cada elemento de $f(A)$ for imagem de um só elemento de A, isto é, f é injectiva se e só se

$$\forall_{x,x'} \, [\, x, x' \in A \Rightarrow \ [\, x \neq x' \ \Rightarrow \ f(x) \neq f(x') \,]\,]$$

o que significa que elementos distintos de A têm necessariamente imagens por f diferentes em $f(A) \subset B$. Se a aplicação $f : A \rightarrow B$ for simultaneamente

injectiva e sobrejectiva traduzir-se-á o facto dizendo que f é uma **aplicação bijectiva**.

Do que atrás ficou dito resulta que duas aplicações f, g são iguais, escrevendo-se então $f = g$, se e só se forem satisfeitas as duas condições seguintes

(1) $\mathbf{D}_f = \mathbf{D}_g \equiv \mathbf{D}$;

(2) $\forall_x \, [\, x \in \mathbf{D} \Rightarrow f(x) = g(x) \,]$.

Sejam A, B, C três conjuntos não vazios e $f : A \to B$ e $g : B \to C$ duas aplicações de A em B e B em C, respectivamente. Chama-se **aplicação composta** de g com f à aplicação

$$g \circ f : A \ \to \ C$$

definida por $A \ni x \rightsquigarrow g \circ f(x) = g(f(x)) \in C$. A composição goza de algumas propriedades importantes das quais se destacam as seguintes:

Teorema 1.46 *A composição de aplicações é associativa.*

Demonstração: Dadas as aplicações $f : A \to B$, $g : B \to C$ e $h : C \to D$ terá de mostrar-se que são iguais as aplicações $(h \circ g) \circ f$ e $h \circ (g \circ f)$.

(1) A aplicação $(h \circ g) \circ f$ tem o mesmo domínio que a aplicação f que é o conjunto A; a aplicação $h \circ (g \circ f)$ tem o mesmo domínio que $g \circ f$ que, por seu turno, tem por domínio o domínio de f ou seja o conjunto A. Ambas as aplicações têm portanto o mesmo domínio.

(2) Seja $x \in A$ qualquer. Então

$$\begin{array}{rcl} [(h \circ g) \circ f](x) & = & [h \circ g](f(x)) \\ & = & h[g(f(x))] \ = \ h[(g \circ f)(x)] \ = \ [h \circ (g \circ f)](x) \end{array}$$

o que mostra que

$$\forall_x \, [\, x \in A \Rightarrow [(h \circ g) \circ f](x) \ = \ [h \circ (g \circ f)](x) \,]$$

De (1) e (2) resulta a igualdade pretendida. □

Definição 1.47 *Dado um conjunto A chama-se* **aplicação identidade** *em A à aplicação* $\mathbf{id}_A : A \to A$ *definida por*

$$\mathbf{id}_A(x) \ = \ x$$

qualquer que seja $x \in A$.

Teorema 1.48 *Sendo $f : A \to B$ uma aplicação arbitrária então $\mathbf{id}_B \circ f = f$ e $f \circ \mathbf{id}_A = f$.*

Demonstração: Por definição de composição de aplicações o domínio de $\mathbf{id}_B \circ f$ é igual ao domínio de f. Por outro lado, para x qualquer, pertencente ao domínio de f, tendo em conta a definição da aplicação identidade, vem

$$(\mathbf{id}_B \circ f)(x) \;=\; \mathbf{id}_B(f(x)) \;=\; f(x)$$

Consequentemente, $\mathbf{id}_B \circ f = f$. Analogamente se provaria que $f \circ \mathbf{id}_A = f$. □

Seja a aplicação $f : A \to B$ e E uma parte de A. Chama-se **imagem** de E por f e representa-se por $f(E)$ ao conjunto assim definido

$$f(E) \;=\; \{y \in B : [\,\exists_x\,[\,x \in E \;\wedge\; y = f(x)\,]\}$$

podendo também escrever-se

$$f(E) \;=\; \{\, f(x) \in B : x \in E \,\}$$

Se F for uma parte de B, chama-se **imagem recíproca** ou **inversa** de F e representa-se por $f^{-1}(F)$ ao conjunto assim definido

$$f^{-1}(F) \;=\; \{x \in A : [\,\exists_y\,[y \in F \;\wedge\; y = f(x)\,]\}$$

podendo também escrever-se equivalentemente

$$f^{-1}(F) \;=\; \{x \in A : f(x) \in F\,\}$$

Teorema 1.49 *Se $f : A \to B$ for uma aplicação bijectiva a correspondência recíproca, que a cada $y \in B$ associa $f^{-1}(y)$, o único elemento do conjunto $f^{-1}(\{y\})$, é uma aplicação bijectiva e $f \circ f^{-1} = \mathbf{id}_B$, $f^{-1} \circ f = \mathbf{id}_A$.*

Demonstração: (1) Antes de mais terá de mostrar-se que a correspondência recíproca define, de facto, uma aplicação. Como $f : A \to B$ é uma bijecção então todo o elemento $y \in B$ é imagem por f de um e um só elemento $x \in A$. Consequentemente tem-se que

$$\forall_{y \in B}\; \exists!_{x \in A}\,[\,x = f^{-1}(y)\,]$$

o que mostra ser $f^{-1} : B \to A$ uma aplicação.

(2) Visto que todo o elemento de A é imagem por f^{-1} de pelo menos um elemento de B a aplicação f^{-1} é sobrejectiva. Sejam agora y_1, y_2 dois elementos quaisquer de B. Suponha-se que se tem $f^{-1}(y_1) = f^{-1}(y_2)$ e que x_1, x_2 são as pré-imagens por f de y_1 e y_2, isto é, que $x_1 = f^{-1}(y_1)$ e $x_2 = f^{-1}(y_2)$. Então

$y_1 = f(x_1)$ e $y_2 = f(x_2)$ e como $x_1 = x_2$, atendendo a que f é uma aplicação, tem-se que $y_1 = y_2$, o que mostra ser f^{-1} injectiva. Logo f^{-1} é bijectiva como se afirmou.

(3) Como $f : A \to B$ é uma bijecção então quaisquer que sejam $x \in A$ e $y \in B$, $y = f(x)$ é equivalente a $x = f^{-1}(y)$ donde vem $\left(f \circ f^{-1}\right)(y) = f(x) = y$, $\forall_{y \in B}$ e $\left(f^{-1} \circ f\right)(x) = f^{-1}(y) = x$, $\forall_{x \in A}$ o que prova a terceira parte do teorema. □

A aplicação $f^{-1} : B \to A$ definida nos termos do Teorema 1.49 é chamada **aplicação inversa** ou **recíproca** de $f : A \to B$.

Exercícios 1.3.2

1. *Seja* $A = \{1, 2, 3, 4, 5, 6\}$ *e* $f : A \to A$ *a função definida por*

$$f(x) = \begin{cases} x + 1 & \text{se } x \neq 6 \\ 1 & \text{se } x = 6 \end{cases}$$

   (a) *Determinar* $f(3), f(6), f \circ f(3)$ *e* $f(f(2))$.

   (b) *Determinar a pré-imagem de* 2 *e* 1.

   (c) *Mostrar que* f *é injectiva.*

2. *Mostrar que a função* $f : \mathbb{R} \to \mathbb{R}$ *dada por* $f(x) = x^3$ *é injectiva e sobrejectiva enquanto que a função* $g : \mathbb{R} \to \mathbb{R}$ *dada por* $g(x) = x^2 - 1$ *não é injectiva nem sobrejectiva.*

3. *Seja* $\mathcal{R}$ *uma relação de equivalência num conjunto não vazio* A. *Define-se uma relação* α *de* A *para* $A/\mathcal{R}$ *pondo*

$$\alpha = \{(x, [x]) : x \in A\}$$

   (a) *Mostrar que* α *é uma função definida em* A.

   (b) *Mostrar que* α *é sobrejectiva.*

   (c) *Em que condições será* α *injectiva?*

4. *Seja dada a função* $f : A \to A$ *que se sabe ser uma relação de equivalência. Que mais se pode dizer relativamente a* f*?*

5. *Seja* $f : \mathbb{R} \to \mathbb{R}$ *a função definida por* $f(x) = \operatorname{sen} x$.

   (a) *Mostrar que* f *não é injectiva.*

   (b) *Mostrar que a restrição de* f *ao intervalo* $[-\pi/2, \pi/2]$ *é uma função injectiva.*

6. *Seja* $\mathbb{R}$ *o conjunto dos números reais e* $f : \mathbb{R} \to \mathbb{R}$ *a função definida por* $f(x) = x^2$.

   (a) *Qual é o domínio, o conjunto dos valores e o contradomínio de* f*?*

   (b) *Será* f *injectiva?*

(c) *Será f sobrejectiva?*

(d) *Determinar o conjunto das pré-imagens de 4.*

(e) *Determinar a imagem recíproca do conjunto $\{t : 1 \leq t \leq 4\}$.*

7. *Sendo $\mathbb{R}$ o conjunto dos números reais explicar porque é que as funções definidas por*

$$f(x) = \frac{1}{x-2} \quad \text{e} \quad g(x) = \sqrt{x}$$

não são funções de $\mathbb{R}$ em $\mathbb{R}$.

8. *Sendo $\mathbb{N}$ o conjunto dos números naturais e $f : \mathbb{N} \to \mathbb{N}$ a função definida por*

$$f(n) = 2n + 5$$

mostrar que f é injectiva e determinar a função inversa. Será f sobrejectiva? E a função inversa será sobrejectiva?

9. *Seja $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2 - 4$. Determinar as imagens dos seguintes conjuntos*

(a) $\{-4, 4, 5\}$

(b) $\{4, 5\}$

(c) $\{t : t \in \mathbb{R} \wedge t \geq 0\}$

10. *Dar um exemplo de uma função real de variável real tal que*

(a) *seja injectiva e sobrejectiva,*

(b) *não seja injectiva nem sobrejectiva.*

11. *Seja $X = \{p, q, r\}$, $Y = \{a, b, c, d\}$ e $Z = \{1, 2, 3, 4\}$ e sejam $g : X \to Y$ definida pelo conjunto dos pares ordenados $\{(p, a), (q, b), (r, c)\}$ e $f : Y \to Z$ definida pelo conjunto de pares ordenados $\{(a, 1), (b, 1), (c, 2), (d, 3)\}$. Escrever a função composta $f \circ g$ sob a forma de um conjunto de pares ordenados.*

12. *Sendo $A = \{p, q, r\}$ e $f : A \to A$ definida por $f(p) = q$, $f(q) = p$ e $f(r) = q$. Dar a função $f \circ f$ sob a forma de um conjunto de pares ordenados.*

13. *Seja A e f como no problema anterior. Definir*

$$g = f \circ f \circ \cdots \circ f \quad (n\text{vezes})$$

Descrever g como um conjunto de pares ordenados quando n é par e quando n é ímpar.

14. *Sejam $f : B \to C$ e $g : A \to B$. Mostrar que*

(a) *se f e g são injectivas então $f \circ g$ é injectiva.*

(b) *se f e g são sobrejectivas então $f \circ g$ é sobrejectiva.*

(c) *suponha-se que $f \circ g$ é injectiva. Será f necessariamente injectiva? Será g necessariamente injectiva?*

(d) *suponha-se que $f \circ g$ é sobrejectiva. Será f necessariamente sobrejectiva? Será g necessariamente sobrejectiva?*

15. *Se $f(x) = ax + b$ e $g(x) = cx + d$ e $f \circ g = g \circ f$, determinar uma equação que relacione as constantes a, b, c, d.*

16. *Seja $f : X \to Y$ e suponha-se que A e B são subconjuntos de X. Mostrar que*

(a) $f(A \cup B) = f(A) \cup f(B)$

(b) $f(A \cap B) \subseteq f(A) \cap f(B)$

17. *Nas condições do problema anterior, mostrar que se f for injectiva então $f(A \cap B) = f(A) \cap f(B)$.*

18. *Seja $f : A \to B$ onde A e B são conjuntos finitos com a mesma cardinalidade. Mostrar que f é injectiva se e só se for sobrejectiva.*

19. *Seja A um subconjunto do conjunto universal $\mathcal{U}$. A função*

$$f_A : \mathcal{U} \to \{0, 1\}$$

definida por

$$f_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

chama-se **função característica** *do conjunto A.*

Sejam A e B dois subconjuntos de $\mathcal{U}$. Mostrar que para todo o $x \in \mathcal{U}$

(a) $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$

(b) $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$

(c) $f_A(x) + f_{A^c}(x) = 1$

(d) $f_C(x) = f_A(x) + f_B(x) - 2f_A(x) \cdot f_B(x)$ *onde C designa a diferença simétrica de A e B.*

1.4 Álgebras de Boole

Se se observarem bem as propriedades das operações com conjuntos e as propriedades das operações lógicas do cálculo proposicional, chegar-se-á à conclusão de que, sob um ponto de vista formal, elas são muito semelhantes. (Recordar, por exemplo, a distributividade das operações $\cup, \cap$ e a distributividade das operações $\vee, \wedge$ ou as leis de Morgan relativas às operações $\cup, \cap$ e as leis de Morgan relativas às operações $\vee, \wedge$.) Este facto mostra que a

álgebra dos conjuntos e o cálculo proposicional têm uma estrutura algébrica idêntica, constituindo dois exemplos típicos do que se designa por álgebras de Boole ou álgebras booleanas.

Começar-se-á por definir o que se entende por álgebra de Boole abstracta, podendo depois verificar-se como esta estrutura é comum tanto à teoria dos conjuntos como à lógica proposicional.

1.4.1 Operações booleanas fundamentais

Seja B um conjunto não vazio. Chama-se **operação unária** definida sobre B a uma regra que a cada elemento $x \in B$ faz corresponder um elemento $y \in B$ que é único. Denotar-se-á esta operação por um traço sobre a letra que designa o elemento sob consideração. Assim $y = \bar{x}$. No caso da teoria dos conjuntos a operação de complementação, que a cada conjunto A associa o seu complementar A^c, é uma operação unária; no cálculo proposicional a negação de uma proposição, que a cada proposição p faz corresponder a proposição $\neg p$, é uma operação unária.

Designa-se por **operação binária** definida sobre B a toda a correspondência que a cada par de elementos a, b, por esta ordem, faz corresponder um elemento único c de B. A reunião e intersecção de conjuntos são exemplos de operações binárias na teoria dos conjuntos; a conjunção e a disjunção são exemplos de operações binárias no cálculo proposicional.

Numa álgebra booleana abstracta representam-se geralmente por $+$ e $\cdot$ (ou simples justaposição) as duas operações binárias que intervêm na sua definição.

Definição 1.50 *Chama-se* **álgebra booleana** $\mathcal{B}$ *à estrutura matemática constituída por um conjunto não vazio B no qual se definem uma operação unária e duas operações binárias que obedecem aos seguintes axiomas:*

B1 *as operações binárias são comutativas, isto é, para $a, b \in B$ quaisquer*

$$a + b = b + a \quad \text{e} \quad a \cdot b = b \cdot a$$

B2 *as operações binárias são associativas, isto é, quaisquer que sejam $a, b, c \in B$,*

$$a+(b+c) = (a+b)+c \equiv a+b+c \text{ e } a\cdot(b\cdot c) = (a\cdot b)\cdot c \equiv abc$$

B3 *as operações binárias são distributivas uma em relação à outra, ou seja, para $a, b, c \in B$ quaisquer*

$$a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{e} \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

B4 *existem dois elementos* $0, 1 \in B$ *(o zero e a unidade) tais que* $0 \neq 1$ *e para todo o* $a \in B$*,*

$$a + 0 = a \quad \text{e} \quad a \cdot 1 = a$$

B5 *para todo o* $a \in B$ *existe* $\bar{a} \in B$ *tal que*

$$a + \bar{a} = 1 \quad \text{e} \quad a \cdot \bar{a} = 0$$

A família de todos os subconjuntos de um universo $\mathcal{U}$ com as operações de reunião, intersecção e complementação constitui uma algebra booleana na qual $\mathcal{U}$ é o elemento unidade e $\emptyset$ é o zero. A família de todas as proposições compostas formadas a partir de n proposições simples, com as operações de disjunção, conjunção e negação, constitui uma álgebra de Boole. Nesta álgebra a unidade é a proposição universalmente verdadeira enquanto que o zero é a proposição universalmente falsa. Qualquer resultado provado numa álgebra booleana abstracta tem a sua interpretação quer em teoria de conjuntos quer no cálculo proposicional.

Exemplo 1.51 (Soma e produto booleanos.) *Seja* $B = \{0, 1\}$ *um conjunto no qual se definem duas operações da forma seguinte:*

$+$	1	0
1	1	1
0	1	0

$\cdot$	1	0
1	1	0
0	0	0

a	$\bar{a}$
1	0
0	1

O terno $\mathcal{B} \equiv (B, +, \cdot)$*, com a complementação tal qual está indicada na última tabela, constitui uma álgebra booleana.*

Antes de estabelecer algumas propriedades das álgebras de Boole considere-se o conceito de dualidade. Por definição, o **dual** de qualquer proposição numa álgebra booleana é a proposição que se obtém por substituição na primeira da operação $+$ pela operação $\cdot$ e da constante 1 pela constante 0.

Teorema 1.52 (Princípio de Dualidade) *O dual de qualquer teorema numa álgebra de Boole é também um teorema.*

O princípio de dualidade verifica-se em qualquer álgebra de Boole. Cada axioma da definição de álgebra de Boole tem duas partes e a única diferença entre estas duas partes é o papel desempenhado pelas operações $+$ e $\cdot$ que estão trocados bem assim como o papel desempenhado pelas constantes 1

e 0 que estão também trocados. Assim, numa álgebra de Boole, qualquer teorema que envolva as operações binárias tem sempre duas partes, cada uma das quais é dual da outra. Nas demonstrações de teoremas deste tipo que se seguem é suficiente provar uma (qualquer) das suas partes; a outra aparece por dualidade.

Exercícios 1.4.1

1. *Escrever as expressões duais das seguintes expressões numa álgebra booleana*
   (a) $x\bar{y}\bar{z} + x\bar{y}z$
   (b) $x(\bar{x} + y)$
2. *Escrever as igualdades duais das seguintes igualdades numa álgebra booleana*
   (a) $x + xy = x$
   (b) $x\bar{y} + y = x + y$

Teorema 1.53 (Leis da idempotência.) *Para todo o* $a \in B$

$$a + a = a \quad \text{e} \quad a \cdot a = a$$

Demonstração:

(a)
$$\begin{aligned} a + a &= (a + a) \cdot 1 && \text{por B4} \\ &= (a + a) \cdot (a + \bar{a}) && \text{por B5} \\ &= a + (a \cdot \bar{a}) && \text{por B3} \\ &= a + 0 && \text{por B5} \\ &= a && \text{por B4} \end{aligned}$$

(b)
$$\begin{aligned} a \cdot a &= (a \cdot a) + 0 && \text{por B4} \\ &= (a \cdot a) + (a \cdot \bar{a}) && \text{por B5} \\ &= a \cdot (a + \bar{a}) && \text{por B3} \\ &= a \cdot 1 && \text{por B5} \\ &= a && \text{por B4} \end{aligned}$$

Teorema 1.54 (Leis das identidades.) *Para todo o* $a \in B$

$$a + 1 = 1 \quad \text{e} \quad a \cdot 0 = 0$$

Demonstração:

$$\begin{array}{lrcll} \text{(a)} & a+1 & = & 1\dot{(}a+1) & \text{por B4} \\ & & = & (a+\bar{a})\cdot(a+1) & \text{por B5} \\ & & = & a+(\bar{a}\cdot 1) & \text{por B3} \\ & & = & a+\bar{a} & \text{por B4} \\ & & = & 1 & \text{por B5} \end{array}$$

$$\begin{array}{lrcll} \text{(b)} & a\cdot 0 & = & (a\cdot 0)+0 & \text{por B4} \\ & & = & (a\cdot 0)+(a\cdot\bar{a}) & \text{por B5} \\ & & = & a\cdot(0+\bar{a}) & \text{por B3} \\ & & = & a\cdot\bar{a} & \text{por B4} \\ & & = & 0 & \text{por B5} \end{array}$$

Teorema 1.55 (Leis de absorção.) *Quaisquer que sejam* $a, b \in B$

$$a+(a\cdot b)=a, \quad a\cdot(a+b)=a$$

Demonstração:

$$\begin{array}{lrcll} \text{(a)} & a+(a\cdot b) & = & (a\cdot 1)+(a\cdot b) & \text{por B4} \\ & & = & a\cdot(1+b) & \text{por B3} \\ & & = & a\cdot 1 & \text{pelo teorema 1.54} \\ & & = & a & \text{por B4} \end{array}$$

(b) A segunda propriedade obtém-se por dualidade. □

Teorema 1.56 (Involução.) *Para todo o elemento* $a \in B$

$$\overline{(\bar{a})}=a$$

Demonstração: (a) Seja $b \in B$ qualquer. Então por B5

$$\bar{b}+b \;=\; 1 \quad \text{e} \quad \bar{b}\cdot b \;=\; 0$$

Fazendo, em particular, $b=\bar{a}$ obter-se-á

$$\overline{(\bar{a})}+\bar{a} \;=\; 1 \quad \text{e} \quad \overline{(\bar{a})}\cdot\bar{a} \;=\; 0 \tag{1.13}$$

Por outro lado, por B5, tem-se também

$$a+\bar{a} \;=\; 1 \quad \text{e} \quad a\cdot\bar{a} \;=\; 0 \tag{1.14}$$

pelo que, comparando (1.13) com (1.14) se obtém o resultado pretendido. □

Teorema 1.57 (Leis de Morgan.) *Para todo o par de elementos* $x, y \in B$

$$\overline{x \cdot y} = \bar{x} + \bar{y} \quad \text{e} \quad \overline{x + y} = \bar{x} \cdot \bar{y}$$

Demonstração: Considerando, por um lado, a expressão $(x \cdot y) \cdot (\bar{x} + \bar{y})$, vem

$$\begin{array}{rcll} (x \cdot y) \cdot (\bar{x} + \bar{y}) & = & (x \cdot y) \cdot \bar{x} + (x \cdot y) \cdot \bar{y} & \text{por B3} \\ & = & x \cdot (y \cdot \bar{x}) + x \cdot (y \cdot \bar{y}) & \text{por B2} \\ & = & x \cdot (\bar{x} \cdot y) + x \cdot (y \cdot \bar{y}) & \text{por B1} \\ & = & (x \cdot \bar{x}) \cdot y + x \cdot (y \cdot \bar{y}) & \text{por B2} \\ & = & (0 \cdot y) + (x \cdot 0) & \text{por B5} \\ & = & 0 & \text{pelo teorema 1.54} \end{array}$$

Por outro lado, considerando a expressão $(x \cdot y) + (\bar{x} + \bar{y})$

$$\begin{array}{rcll} (x \cdot y) + (\bar{x} + \bar{y}) & = & (\bar{x} + \bar{y}) + (x \cdot y) & \text{por B1} \\ & = & [\bar{x} + \bar{y}) + x] \cdot [(\bar{x} + \bar{y}) + y] & \text{por B3} \\ & = & [x + (\bar{x} + \bar{y})] \cdot [(\bar{x} + \bar{y}) + y] & \text{por B1} \\ & = & [(x + \bar{x}) + \bar{y}] \cdot [x + (y + \bar{y})] & \text{por B2} \\ & = & (1 + \bar{y}) \cdot (x + 1) & \text{por B5} \\ & = & 1 & \text{pelo teorema 1.54} \end{array}$$

Tem-se então

$$(x \cdot y) \cdot (\bar{x} + \bar{y}) = 0 \quad \text{e} \quad (x \cdot y) + (\bar{x} + \bar{y}) = 1$$

pelo que, tendo em conta B5,

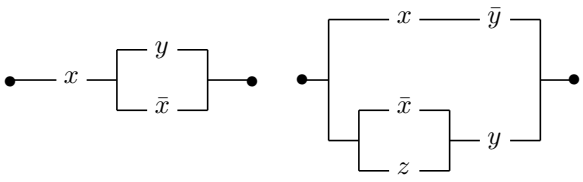
$$\overline{x \cdot y} = \bar{x} + \bar{y}$$

A segunda proposição obtém-se por dualidade. □

Exemplo 1.58 (Circuitos com interruptores.) Sejam $x, y, \ldots$ interruptores eléctricos e suponha-se que $x, \bar{x}$ designam sempre dois interruptores com a propriedade de que se um está ligado o outro está desligado e vice-versa.

Dois interruptores, x e y, por exemplo, podem ser ligados por fios, em série ou em paralelo, como segue

o que se denota por $x \cdot y$ (ou, simplesmente, xy) e $x + y$, respectivamente. Um circuito booleano é um arranjo de fios e interruptores que pode ser montado com o uso repetido de combinações em série e em paralelo podendo, portanto, ser descrito pelo uso dos sinais + e · (ou simples justaposição). Assim,



$x \cdot (y + \bar{x})$ $\qquad$ $(\bar{x} + z)y + x\bar{y}$

são dois exemplos, um pouco mais complicados, de circuitos com interruptores.

As variáveis $x, y, \ldots$ que representam os interruptores apenas podem tomar os valores

$$1 \qquad \text{e} \qquad 0$$

que significam *"interruptor fechado"* e *"interruptor aberto"*, respectivamente

As duas tabelas que se seguem descrevem o comportamento de um circuito em série, xy, e em paralelo, $x + y$,

x	y	xy
1	1	1
1	0	0
0	1	0
0	0	0

x	y	x+y
1	1	1
1	0	1
0	1	1
0	0	0

enquanto que a tabela que se segue mostra a relação entre um interruptor x e o interruptor complementar $\bar{x}$,

x	$\bar{x}$
1	0
0	1

Observe-se que as três tabelas acima são idênticas às tabelas da conjunção, disjunção e negação de proposições.

Para determinar o comportamento de um circuito booleano constrói-se uma tabela que é análoga às tabelas de verdade do cálculo proposicional. Para os dois circuitos acima, por exemplo, tem-se o seguinte:

x	y	$\bar{x}$	$\bar{x} + y$	$x(y + \bar{x})$
1	1	0	1	1
1	0	0	0	0
0	1	1	1	0
0	0	1	1	0

A corrente só passará se os interruptores x e y estiverem ligados simultaneamente.

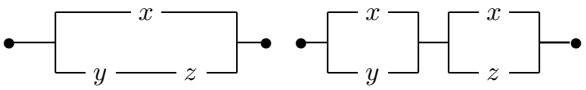
x	y	z	$\bar{x}$	$z+\bar{x}$	$(z+\bar{x})y$	$\bar{y}$	$x\bar{y}$	$(z+\bar{x})y+x\bar{y}$
1	1	1	0	1	1	0	0	1
1	1	0	0	0	0	0	0	0
1	0	1	0	1	0	1	1	1
1	0	0	0	0	0	1	1	1
0	1	1	1	1	1	0	0	1
0	1	0	1	1	1	0	0	1
0	0	1	1	1	0	1	0	0
0	0	0	1	1	0	1	0	0

Neste caso a corrente passará para 5 configurações possíveis dos três interruptores.

Desenhando os circuitos apropriados e enumerando todas as situações possíveis, pode verificar-se que todos os axiomas de álgebra de Boole são válidos quando interpretados em termos de circuitos com interruptores.

Teorema 1.59 *A álgebra dos circuitos com interruptores é uma álgebra booleana.*

Por exemplo, os dois circuitos equivalentes



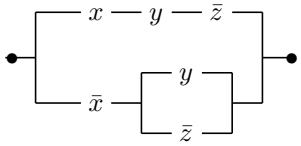
$x+yz$ $\qquad$ $(x+y)(x+z)$

representam, em termos de circuitos, a distributividade da operação $\cdot$ relativamente à operação $+$.

Exemplo 1.60 *Determinar o circuito que realiza a expressão booleana*

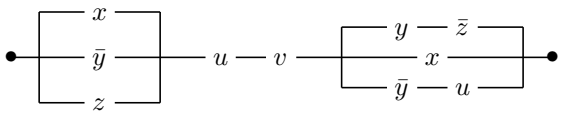
$$xy\bar{z}+\bar{x}(y+\bar{z})$$

Esta expressão indica que a ligação em série de x, y e$\bar{z}$ está ligada em paralelo com o circuito correspondente à expressão $\bar{x}(y+\bar{z})$. Este último circuito, por seu turno, consiste num interruptor $\bar{x}$ ligado em série com uma ligação em paralelo de y e $\bar{z}$. Então, ter-se-á



$xy\bar{z}+\bar{x}(y+\bar{z})$

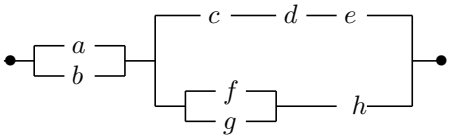
Exemplo 1.61 *Determinar a expressão booleana correspondente ao seguinte circuito*



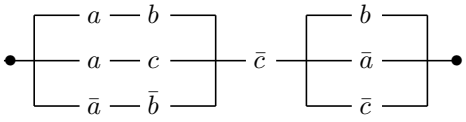
$$(x + \bar{y} + z)uv(y\bar{z} + x + \bar{y}u)$$

Exercícios 1.4.2

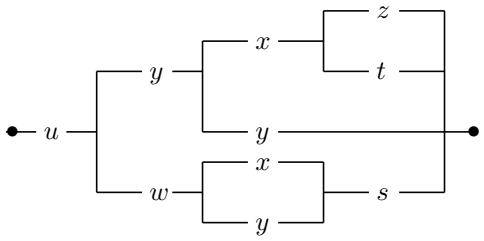
1. *Desenhar os circuitos com interruptores que realizam as expressões booleanas que se seguem sem efectuar qualquer simplificação prévia.*
   (a) $xyz + xy(zw + st)$
   (b) $x + y(z + wt) + su$
   (c) $x[y(z + w) + z(u + v)]$
   (d) $(x + \bar{y} + z)(x + y\bar{z}) + \bar{z}w + w(\bar{y} + z)$
   (e) $(xy + x\bar{y}z + x\bar{z})z$
   (f) $xz + \bar{y} + \bar{y}z + x\bar{y}z$
   (g) $(xy + z)(y + z) + z$
   (h) $\bar{x}z + \bar{x}y + \bar{z}$
2. *Determinar as expressões que representam algebricamente os seguintes circuitos:*
   (a)



   (b)



(c)



Exercícios 1.4.3

1. *Seja A um conjunto qualquer e $\mathcal{P}(A)$ o conjunto das partes de A. Verificar que $\mathcal{B} \equiv (\mathcal{P}(A), \cup, \cap)$ constitui uma álgebra de Boole quando, para cada $x \in \mathcal{P}(A)$ se define $\bar{x} = A \backslash x$.*
2. *Mostre que o conjunto $\{a, b, c, d\}$ com as operações definidas pelas tabelas seguintes é uma álgebra de Boole.*

$+$	a	b	c	d
a	a	b	b	a
b	b	b	b	b
c	b	b	c	c
d	a	b	c	d

$\cdot$	a	b	c	d
a	a	a	d	d
b	a	b	c	d
c	d	c	c	d
d	d	d	d	d

3. *No conjunto $\mathbb{Z}$ considere as operações $+$, $\cdot$ e complementação definidas, para $a, b \in \mathbb{Z}$ quaisquer, por*

$$\begin{aligned} a + b &= \max\{a, b\} \\ a\dot{b} &= \min\{a, b\} \\ \bar{a} &= -a \end{aligned}$$

Verifique se o sistema $(\mathbb{Z}, +, \cdot)$ constitui ou não uma álgebra de Boole.

1.4.2 Funções booleanas

Chama-se função booleana de n variáveis booleanas $x_1, x_2, \ldots, x_n$ a uma aplicação de $\{0,1\}^n$ em $\{0,1\}$. A função de três variáveis

$$f(x_1, x_2, x_3) \;=\; x_1 + \bar{x}_2 x_3$$

onde $x_1 \in \{0,1\}$, $x_2 \in \{0,1\}$ e $x_3 \in \{0,1\}$ e as operações são entendidas no sentido booleano, isto é, sujeitas às tabelas

x	y	xy	x+y
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

e

x	$\bar{x}$
1	0
0	1

é um exemplo de uma função booleana de três variáveis booleanas. A função $f(x_1, x_2, x_3)$ tem a seguinte tabela de valores

x_1	x_2	x_3	$\bar{x}_2$	$\bar{x}_2 x_3$	$f(x_1, x_2, x_3)$
1	1	1	0	0	1
1	1	0	0	0	1
1	0	1	1	1	1
1	0	0	1	0	1
0	1	1	0	0	0
0	1	0	0	0	0
0	0	1	1	1	1
0	0	0	1	0	0

Por vezes é conveniente expressar uma função na chamada **forma canónica** que é uma expressão constituída por produtos cada um dos quais contém todas as variáveis (com ou sem barra). Por exemplo, a função

$$g(x_1, x_2, x_3) \;=\; x_1 x_2 \bar{x}_3 + x_1 x_2 x_3$$

é uma função booleana na forma canónica.

Para converter uma dada função na forma canónica pode usar-se a lei de complementação $1 = x + \bar{x}$ de forma adequada. Assim, considerando de novo a função $f(x_1, x_2, x_3)$ dada acima, tem-se o seguinte

$$\begin{aligned}
f(x_1, x_2, x_3) &= x_1 + \bar{x}_2 x_3 \\
&= x_1 \cdot 1 + \bar{x}_2 x_3 \\
&= x_1(x_2 + \bar{x}_2) + \bar{x}_2 x_3 \\
&= x_1 x_2 + x_1 \bar{x}_2 + \bar{x}_2 x_3 \\
&= x_1 x_2 (x_3 + \bar{x}_3) + x_1 \bar{x}_2 (x_3 + \bar{x}_3) + (x_1 + \bar{x}_1) \bar{x}_2 x_3 \\
&= x_1 x_2 x_3 + x_1 x_2 \bar{x}_3 + x_1 \bar{x}_2 x_3 + x_1 \bar{x}_2 \bar{x}_3 + x_1 \bar{x}_2 x_3 + \bar{x}_1 \bar{x}_2 x_3 \\
&= x_1 x_2 x_3 + x_1 x_2 \bar{x}_3 + x_1 \bar{x}_2 x_3 + x_1 \bar{x}_2 \bar{x}_3 + \bar{x}_1 \bar{x}_2 x_3
\end{aligned}$$

Esta técnica pode ser usada para expressar uma função booleana com qualquer número de variáveis booleanas na forma canónica. Cada um dos termos que contém todas as variáveis (com ou sem barra) chama-se **termo canónico**.

A forma canónica de uma função booleana pode também obter-se directamente a partir da sua tabela de valores como se indica no exemplo que se segue.

Exemplo 1.62 Seja $f : \{0,1\}^3 \to \{0,1\}$ a função definida por

x	y	z	$f(x,y,z)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

Então

$$\begin{aligned} f(x,y,z) &= 1 \cdot xyz + 0 \cdot xy\bar{z} + 0 \cdot x\bar{y}z + 1 \cdot x\bar{y}\bar{z} + 0 \cdot \bar{x}yz + 1 \cdot \bar{x}y\bar{z} + \\ &\quad 0 \cdot \bar{x}\bar{y}z + 1 \cdot \bar{x}\bar{y}\bar{z} \\ &= xyz + x\bar{y}\bar{z} + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z} \end{aligned}$$

é a expressão analítica da função $f(x,y,z)$ na sua forma canónica.

Teorema 1.63 *Duas funções booleanas são iguais se e só se as suas formas canónicas forem idênticas.*

Demonstração: É claro que se duas funções tiverem a mesma forma canónica elas são iguais. Por outro lado, se duas funções forem iguais então têm tabelas de valores idênticas as quais, por seu turno, originam formas canónicas idênticas. □

Exercícios 1.4.4 *Considere-se de novo a função $f(x,y,z)$ do exemplo 1.62.*

1. *Determinar a expressão de $\bar{f}(x,y,z)$ a partir da forma canónica de $f(x,y,z)$.*
2. *Determinar a tabela de valores de $\bar{f}(x,y,z)$ a partir da tabela de valores de $f(x,y,z)$.*
3. *Determinar a forma canónica de $\bar{f}(x,y,z)$ a partir da sua tabela de valores.*

   As funções obtidas em 1. e 3. são iguais – uma está expressa como um produto de somas e a outra está expressa como uma soma de produtos. A forma de $\bar{f}(x,y,z)$ obtida em 1. é designada por **forma canónica dual** (da forma canónica usual).

4. *Descrever um método para reduzir a expressão de uma função booleana a um produto finito de um certo número de somas com todas as variáveis (com ou sem barra). Ou seja, descrever um método de obtenção da forma canónica dual de uma função booleana a partir da sua tabela de valores.*

5. *Dar um exemplo de aplicação do método descrito na alínea anterior.*

6. *Determinar a forma canónica das funções booleanas*

   (a) $f(x,y,z) = \overline{(x+y)}z(x+y)$

   (b) $g(x,y,z) = \bar{x}z + \bar{x}y + \bar{z}$

   (c) $h(x,y,z) = (x+y)(\bar{x}+z)$

   (d) $j(x,y,z) = (xy+z)(y+z)+z$

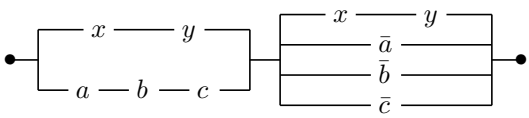
   usando a tabela de valores e por processos algébricos.

Simplificação de funções booleanas. Anteriormente mostrou-se como se pode reduzir uma função booleana à sua forma canónica. Esta, no entanto, nem sempre é a forma mais conveniente para resolver certos problemas. Por vezes é desejável expressar uma função booleana com o número mínimo de termos e variáveis, obtendo-se então a chamada **forma mínima**. Isto é particularmente importante no desenho de circuitos com interruptores: quanto menos termos e menos variáveis mais simples e mais económico será o circuito.

A simplificação de um circuito pode fazer-se muitas vezes apelando à intuição e à esperiência. Contudo, para circuitos muito complexos, tais como os que aparecem nos modernos computadores, é necessário dispor de técnicas mais sistemáticas. Há vários métodos baseados na teoria das funções booleanas. Aqui considerar-se-á apenas o menos sofisticado daqueles métodos que se baseia na aplicação directa das propriedades das álgebras de Boole.

O método geral de simplificação de um circuito consiste em determinar, em primeiro lugar, a função booleana que o representa, simplificar a função booleana obtida e, finalmente, desenhar um novo circuito que realize a função booleana simplificada.

Exemplo 1.64 *Simplificar o circuito*



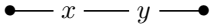
Este circuito é representado pela função booleana

$$f(x,y,a,b,c) \;=\; (xy+abc)(xy+\bar{a}+\bar{b}+\bar{c})$$

a qual se pode simplificar da seguinte forma

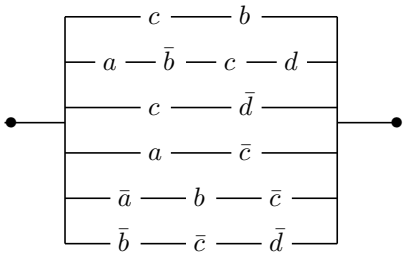
$$\begin{aligned} f(x,y,a,b,c) &= (xy+abc)(xy+\bar{a}+\bar{b}+\bar{c}) \\ &= xyxy+xy\bar{a}+xy\bar{b}+xy\bar{c}+abcxy+abc\bar{a}+abc\bar{b}+abc\bar{c} \\ &= xy+xy\bar{a}+xy\bar{b}+xy\bar{c}+abcxy \\ &= xy(1+\bar{a}+\bar{b}+\bar{c}+abc) \;=\; xy \end{aligned}$$

O circuito simplificado equivalente tem então a forma



Por vezes, no processo de simplificação, é mais fácil reconhecer qual é o procedimento a seguir na função dual do que na função original. Este facto sugere um novo processo de simplificação: toma-se o dual de f, denotado por $d(f)$, simplifica-se $d(f)$ e finalmente tomando de novo o dual obtém-se geralmente uma forma simplificada da função original,

Exemplo 1.65 *Simplificar o circuito*



Este circuito é representado pela função

$$f(a,b,c,d) \;=\; bc + a\bar{b}cd + c\bar{d} + a\bar{c} + \bar{a}b\bar{c} + \bar{b}\bar{c}\bar{d}$$

Sendo

$$\begin{array}{rcl} g(a,b,c,d) & = & bc + a\bar{b}cd + c\bar{d} \\ h(a,b,c,d) & = & a\bar{c} + \bar{a}b\bar{c} + \bar{b}\bar{c}\bar{d} \end{array}$$

então

$$f(a,b,c,d) \;=\; g(a,b,c,d) + h(a,b,c,d)$$

Considerando o dual de g

$$\begin{array}{rcl} d(g) & = & (b+c)(a+\bar{b}+c+d)(c+\bar{d}) \\ & = & (ab + b\bar{b} + bc + bd + ac + \bar{b}c + c + cd)(c+\bar{d}) \\ & = & abc + ab\bar{d} + bcc + bc\bar{d} + bcd + bd\bar{d} + acc + ac\bar{d} + \bar{b}cc + \\ & & \bar{b}c\bar{d} + cc + c\bar{d} + ccd + cd\bar{d} \\ & = & abc + ab\bar{d} + bc + bc\bar{d} + bcd + ac + ac\bar{d} + \bar{b}c + \bar{b}c\bar{d} + c + c\bar{d} + cd \\ & = & abc + ab\bar{d} + bc(1+\bar{d}+d) + ac(1+\bar{d}) + \bar{b}c(1+\bar{d}) + c(1+\bar{d}) + cd \\ & = & abc + ab\bar{d} + bc + ac + \bar{b}c + c + cd \\ & = & (a+1)bc + ab\bar{d} + ac + (\bar{b}+1+d)c \\ & = & bc + ab\bar{d} + ac + c \\ & = & (b+a+1)c + ab\bar{d} \;=\; c + ab\bar{d} \end{array}$$

e tomando de novo o dual, vem

$$g(a,b,c,d) \;=\; c(a+b+\bar{d})$$

Por outro lado,

$$\begin{array}{rcl} d(h) & = & (a+\bar{c})(\bar{a}+b+\bar{c})(\bar{b}+\bar{c}+\bar{d}) \\ & = & (a\bar{a} + ab + a\bar{c} + \bar{a}\bar{c} + b\bar{c} + c\bar{c})(\bar{b}+\bar{c}+\bar{d}) \\ & = & ab\bar{b} + ab\bar{c} + ab\bar{d} + a\bar{b}\bar{c} + a\bar{c}\bar{c} + a\bar{c}\bar{d} + \bar{a}\bar{b}\bar{c} + a\bar{c}\bar{c} + a\bar{c}\bar{d} + \\ & & b\bar{b}\bar{c} + b\bar{c}\bar{c} + b\bar{c}\bar{d} + \bar{c}\bar{b} + \bar{c}\bar{c} + \bar{c}\bar{d} \\ & = & ab\bar{c} + ab\bar{d} + a\bar{b}\bar{c} + a\bar{c} + a\bar{c}\bar{d} + \bar{a}\bar{b}\bar{c} + a\bar{c} + b\bar{c} + b\bar{c}\bar{d} + \bar{b}\bar{c} + \bar{c} + \bar{c}\bar{d} \\ & = & ab\bar{c} + ab\bar{d} + (1+a+\bar{a})\bar{b}\bar{c} + a\bar{c}(1+\bar{d}) + b\bar{c}(1+\bar{d}) + \bar{c}(1+\bar{d}) \\ & = & ab\bar{c} + ab\bar{d} + \bar{b}\bar{c} + a\bar{c} + b\bar{c} + \bar{c} \\ & = & (ab + \bar{b} + a + b + 1)\bar{c} + ab\bar{d} \\ & = & \bar{c} + ab\bar{d} \end{array}$$

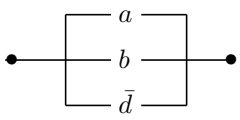
e, portanto, tomando de novo o dual

$$h(a,b,c,d) \;=\; \bar{c}(a+b+\bar{d})$$

Consequentemente, tem-se

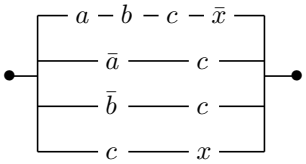
$$f(a,b,c,d) \;=\; c(a+b+\bar{d}) + \bar{c}(a+b+\bar{d}) \;=\; a+b+\bar{d}$$

pelo que o circuito simplificado equivalente é

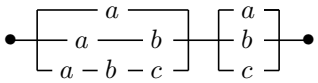


Exercícios 1.4.5 *Simplificar os circuitos seguintes:*

1.



2.



Capítulo 2

Números Naturais, Indução e Cálculo Combinatório

2.1 Axiomática dos Números Naturais

2.1.1 Conceito de axiomática

> "Aqueles que se ocupam da geometria, da aritmética e ciências desse género admitem o par e o ímpar, as figuras, três tipos de ângulos, (...) Estas coisas dão-nas por sabidas, e, quando as usam como hipóteses, não acham que ainda seja necessário prestar contas disto a si mesmos nem aos outros, uma vez que são evidentes para todos. Partindo daí, analisando todas as fases e, tirando consequências, atingem o ponto a cuja investigação se tinham abalançado."
>
> **Platão** in República (VI, 510, cd)

No início de qualquer teoria matemática bem construída apresenta-se, sem explicação, um pequeno número de termos específicos particulares: estes servirão para explicar todos os outros termos específicos. Por este facto, são designados **termos primitivos** (da teoria em questão). O emprego de termos primitivos numa teoria matemática é indispensável. De facto, para explicar um termo é necessário empregar outros termos; estes, por seu turno, para serem eles próprios explicados, sem entrar num ciclo vicioso, exigem o recurso a outros termos novos; e assim sucessivamente. Este processo, se não parasse nalgum ponto, conduziria a uma cadeia infinita de explicações (sempre com novos termos), o que não é possível pois que é limitado o número

de termos distintos disponíveis em qualquer vocabulário. Evita-se esta impossibilidade aceitando, uma vez por todas, o emprego de termos primitivos escolhidos à priori que devem ser em pequeno número e de conteúdo simples. (É o que se faz em teoria dos conjuntos na qual conjunto e elemento de um conjunto não se definem, sendo considerados termos primitivos.)

Numa teoria os termos específicos que não são primitivos dizem-se **termos definidos**. Suponha-se conhecida a lista de todos os termos primitivos de uma dada teoria. A introdução de um novo termo específico na teoria far-se-á à custa destes termos primitivos e de termos lógicos. A explicação assim obtida para o novo termo constitui o que se chama uma **definição** e este termo é o termo definido. Assim, o primeiro termo definido, t_1, é explicado apenas à custa de termos primitivos (e termos lógicos); para definir um segundo termo, t_2, podem agora empregar-se todos os termos primitivos e o termo definido t_1 (e termos lógicos); um terceiro termo, t_3, pode ser explicado à custa dos termos primitivos e de todos os termos já definidos anteriormente, t_1 e t_2 (e os termos lógicos que forem necessários). Este procedimento segundo o qual uma definição atribui um sentido a um termo à custa de termos primitivos e de termos definidos anteriormente, evita o ciclo vicioso que seria o de um termo ser explicado à custa de termos que por sua vez acabariam por ser explicados por ele próprio.

A parte central de qualquer teoria matemática é constituída por enunciados de proposições ou sentenças verdadeiras (no contexto daquela teoria). Estes enunciados estabelecem as ligações entre os termos específicos da teoria. Os termos específicos e os termos lógicos são o material básico para a construção daquelas afirmações. Tal como acontece com os termos específicos, podem subdividir-se as proposições verdadeiras de uma teoria em duas classes:

(1) proposições primitivas ou **axiomas**, e

(2) proposições derivadas ou **teoremas**.

Os axiomas são afirmações que se aceitam como verdadeiras sem qualquer prova; são necessárias por razões análogas às expostas a propósito dos termos primitivos. Os axiomas são geralmente apresentados no início de uma teoria, imediatamente a seguir aos termos primitivos e, tal como estes, são geralmente em pequeno número e dotados de sentido intuitivo.

Uma vez estabelecidos os axiomas de uma teoria, novas proposições podem ser formuladas. Agora, no entanto, para que uma proposição possa ser

considerada um teorema dentro da teoria (isto é, seja uma proposição verdadeira da teoria) torna-se necessário submetê-la a um teste designado por **prova** ou **demonstração**. Serão teoremas as proposições que satisfizerem positivamente aquele teste. Para provar uma primeira proposição, p_1, os únicos argumentos que podem ser usados são os axiomas e as definições já estabelecidas; se p_1 decorrer logicamente destes argumentos (isto é, se for demonstrada) então transforma-se num teorema, T_1. Para provar uma nova proposição, p_2, podem agora usar-se não só os axiomas e as definições estabelecidas mas também o teorema T_1; se a proposição p_2 for demonstrada então transforma-se num teorema, T_2. Este processo vai-se repetindo assim sucessivamente tal como já foi referido no caso das definições, isto é, uma demonstração mostra a veracidade de uma proposição por argumentos que se baseiam nos axiomas da teoria e nas definições e teoremas já estabelecidos.

Note-se que, entendendo-se que uma proposição só é considerada verdadeira se puder ser demonstrada a partir dos axiomas da teoria e de teoremas já demonstrados, isso significa que a veracidade de uma proposição depende directamente dos axiomas da teoria sob consideração; uma proposição pode ser um teorema numa certa teoria e não o ser noutra (por exemplo, em geometria euclidiana plana a proposição

"a soma dos ângulos de um triângulo é igual a um ângulo raso"

é um teorema, mas deixa de o ser no contexto de outras geometrias diferentes daquela). Neste sentido, numa teoria axiomática, a questão que se põe relativamente a uma dada proposição não é a de saber se ela traduz algum tipo de *"verdade"* mas sim a de saber se aquela proposição é ou não uma consequência lógica dos axiomas da referida teoria.

2.1.2 Os axiomas de Dedekind-Peano

Como exemplo típico e relativamente bem conhecido de uma teoria axiomática apresenta-se a Axiomática de Dedekind-Peano para os números naturais que servirá de base para a demonstração de algumas das suas consequências elementares.
A construção axiomática de Dedekind-Peano do conjunto dos números naturais parte de três termos primitivos – **zero, número natural** e **sucessor** – e de cinco axiomas que os relacionam:

N1 O zero é um número natural e representa-se por 0.

N2 Cada número natural n tem um e um só sucessor, representado por $\mathbf{suc}(n)$, que é também um número natural.

N3 O zero não é sucessor de nenhum número natural.

N4 Se m, n são dois números naturais tais que $\mathbf{suc}(m) = \mathbf{suc}(n)$ então $m = n$.

N5 Seja $\mathbf{A}$ um conjunto de números naturais. Se $\mathbf{A}$ for tal que

(1) $0 \in \mathbf{A}$, e

(2) $\forall_n \, [\, n \in \mathbf{A} \Rightarrow \mathbf{suc}(n) \in \mathbf{A} \,]$,

então $\mathbf{A}$ é o conjunto constituído por todos os números naturais que é denotado por $\mathbb{N}$.

O axioma **N5** é a base de todas as demonstrações feitas pelo **método de indução matemática** (ou método de indução finita) que pode formular-se da seguinte maneira:

Suponha-se que a cada número natural $n \in \mathbb{N}$ se pode associar uma proposição denotada por $p(n)$; suponha-se ainda que

(a) *$p(0)$ é uma proposição verdadeira, e que*

(b) *para todo o $j \in \mathbb{N}$, $p\,(\mathbf{suc}(j))$ é verdadeira sempre que $p(j)$ o seja.*

Então a proposição $p(n)$ é verdadeira qualquer que seja o número natural $n \in \mathbb{N}$.

De facto, seja $\mathbf{X}$ o conjunto dos números naturais n para os quais $p(n)$ é uma proposição verdadeira. O conjunto $\mathbf{X}$ contém 0 por **(a)** e por **(b)** contém $\mathbf{suc}(j)$ qualquer que seja $j \in \mathbf{X}$. Então, de acordo com o axioma **N5**, tem-se que $\mathbf{X} = \mathbb{N}$ o que significa que $p(n)$ é uma proposição verdadeira qualquer que seja $n \in \mathbb{N}$ como se afirmou.

De acordo com esta axiomática são então números naturais os seguintes

$$0, \mathbf{suc}(0), \mathbf{suc}\,(\mathbf{suc}(0)), \mathbf{suc}\,(\mathbf{suc}\,(\mathbf{suc}(0))), \ldots$$

os quais, por comodidade de escrita, têm as seguintes designações mais usuais: $1 \equiv \mathbf{suc}(0)$, $2 \equiv \mathbf{suc}\,(\mathbf{suc}(0)) = \mathbf{suc}(1), \ldots$[1]

Exemplo 2.1 *Mostrar, a partir da axiomática de Dedekind-Peano, que todo o número natural diferente do zero é sucessor de um número natural.*

Sendo

$$\mathbf{A} \;=\; \{n \in \mathbb{N} : n = 0 \vee \exists_m \, [\, m \in \mathbb{N} \wedge n = \mathbf{suc}(m) \,]\,\}$$

então

[1] Denotar-se-á por $\mathbb{N}_1$ o subconjunto de $\mathbb{N}$ igual a $\mathbb{N}\backslash\{0\}$ e, de um modo mais geral, para qualquer $p \in \mathbb{N}$, denotar-se-á por $\mathbb{N}_p$ o conjunto $\mathbb{N}_p \equiv \{n \in \mathbb{N} : n \geq p\}$.

1. $0 \in \mathbf{A}$ (pela definição do conjunto $\mathbf{A}$)
2. Suponha-se que $n \in \mathbf{A}$, $n \neq 0$. Então $n = \mathbf{suc}(m)$ para algum $m \in \mathbb{N}$. Consequentemente, $\mathbf{suc}(n) = \mathbf{suc}(\mathbf{suc}(m))$ e como, por $\mathbf{N}2$, $\mathbf{suc}(m) \in \mathbb{N}$ então $\mathbf{suc}(n) \in \mathbf{A}$.

Dos dois argumentos precedentes, tendo em conta $\mathbf{N}5$, vem $\mathbf{A} = \mathbb{N}$ ficando provada a afirmação.

2.1.3 Aritmética dos números naturais

A aritmética dos números naturais baseia-se em duas operações: a adição e a multiplicação. Nenhuma destas operações recebe uma menção explícita na Axiomática de Dedekind-Peano o que significa que as mesmas podem ser definidas em termos das noções já introduzidas. Tal modo de proceder apresenta, no entanto, um acréscimo de dificuldades pelo que se adoptará aqui o ponto de vista que consiste em introduzir as definições de adição e multiplicação em $\mathbb{N}$ de forma axiomática podendo depois deduzir-se toda a aritmética dos números naturais fazendo repetido apelo ao princípio da indução matemática.

A **adição** de números naturais é uma operação interna, denotada pelo símbolo $+$, que é definida recursivamente por

$$\mathbf{A1}\ \forall_n\,[\,n \in \mathbb{N}\ \Rightarrow\ [\,n + 0 = n\,]\,],$$
$$\mathbf{A2}\ \forall_{n,m}\,[\,m, n \in \mathbb{N}\ \Rightarrow\ [\,n + \mathbf{suc}(m) = \mathbf{suc}(n + m)\,]\,]$$

podendo mostrar-se que existe uma e só uma operação interna definida sobre $\mathbb{N}$ que satisfaça **A1** e **A2**.

Podem agora provar-se novas propriedades satisfeitas pelos elementos de $\mathbb{N}$ partindo apenas das proposições aceites como verdadeiras até este momento.

Teorema 2.2 *A adição em* $\mathbb{N}$ *é associativa.*

Demonstração: Seja X o conjunto de números definido por

$$X \equiv \{p \in \mathbb{N} : \forall_{m,n}\,[\,m, n \in \mathbb{N}\ \Rightarrow\ [\,(m + n) + p = m + (n + p)\,]\,]\}$$

Como de **A1** resulta $(m + n) + 0 = m + n = m + (n + 0)$, para todo o $m, n \in \mathbb{N}$ tem-se então que

$$0 \in X \tag{2.1}$$

Seja agora q arbitrariamente fixado em X. Da definição de X tem-se que $(m+n)+q = m+(n+q)$, para todos $m, n \in \mathbb{N}$ e, portanto, tendo em conta **A2**, a hipótese de indução e novamente **A2**, vem para todos os $m, n \in \mathbb{N}_0$

$$\begin{aligned}(m+n)+\mathbf{suc}(q) &= \mathbf{suc}\,((m+n)+q)\\ &= \mathbf{suc}\,(m+(n+q))\\ &= m+\mathbf{suc}(n+q) = m+(n+\mathbf{suc}(q))\end{aligned}$$

o que mostra que $\mathbf{suc}(q) \in X$. Isto é

$$\forall_q\,[\, q \in X \Rightarrow \mathbf{suc}(q) \in X\,] \tag{2.2}$$

De (2.1) e (2.2), tendo em conta o axioma **N5**, resulta que $X = \mathbb{N}$ e que, portanto, para todos os números $m, n, p \in \mathbb{N}$

$$(m+n)+p = m+(n+p)$$

o que prova o teorema. □

Teorema 2.3 *A adição em* $\mathbb{N}$ *é comutativa.*

Demonstração: (a) Demonstrar-se-á antes de mais que qualquer que seja $m \in \mathbb{N}_0$ se tem $0+m = m+0$. Seja $\mathcal{M} \equiv \{m \in \mathbb{N} : 0+m = m+0\}$. Como $0+0 = 0+0$ tem-se imediatamente que

$$0 \in \mathcal{M} \tag{2.3}$$

Seja agora p um elemento arbitrariamente fixado em $\mathcal{M}$. Da definição de $\mathcal{M}$ vem então que $0+p = p+0$ e portanto, atendendo a **A2**, hipótese de indução e **A1** sucessivamente, vem

$$0+\mathbf{suc}(p) = \mathbf{suc}(0+p) = \mathbf{suc}(p+0) = \mathbf{suc}(p) = \mathbf{suc}(p)+0$$

o que mostra que $\mathbf{suc}(p) \in \mathcal{M}$. Então

$$\forall_p\,[\, p \in \mathcal{M} \Rightarrow \mathbf{suc}(p) \in \mathcal{M}\,] \tag{2.4}$$

e de (2.3) e (2.4), tendo em conta o axioma **N5**, resulta que $\mathcal{M} = \mathbb{N}_0$ ou, o que é o mesmo, que

$$0+m = m+0$$

qualquer que seja $m \in \mathbb{N}$.

(b) Para demonstrar a comutatividade no caso geral torna-se necessário provar, antes de mais, os seguintes resultados preliminares:

Lema 2.4 $\forall_{m\in\mathbb{N}}\,[\,\mathbf{suc}(m) = 1+m\,]$.

Demonstração: Seja $S \equiv \{s \in \mathbb{N} : \mathbf{suc}(s) = 1 + s\}$. Visto que, por definição, se tem $1 = \mathbf{suc}(0)$ então, tendo em conta **A1**, vem $\mathbf{suc}(0) = 1 + 0$, o que mostra que

$$0 \in S \tag{2.5}$$

Seja agora $m \in S$ qualquer. Da definição de S vem $\mathbf{suc}(m) = 1 + s$ e portanto, tendo em conta **A2**, obtém-se

$$\mathbf{suc}\,(\mathbf{suc}(m)) = \mathbf{suc}(1 + m) = 1 + \mathbf{suc}(m)$$

o que mostra que

$$\forall_m \,[\, m \in S \Rightarrow \mathbf{suc}(m) \in S \,] \tag{2.6}$$

De (2.5) e (2.6) resulta $S = \mathbb{N}$. □

Lema 2.5 $\forall_m \,[m \in \mathbb{N} \;\Rightarrow\; [\, m + 1 = 1 + m \,]]$.

Demonstração: Da alínea (a) do teorema tem-se que qualquer que seja $m \in \mathbb{N}$ $m + 0 = 0 + m$ e, portanto, tendo em conta o axioma **N2**, vem $\mathbf{suc}(m+0) = \mathbf{suc}(0+m)$, donde por **A2** $m+\mathbf{suc}(0) = 0+\mathbf{suc}(m)$, ou seja, atendendo ao Lema 2.4 e à parte (a) do teorema,

$$m + 1 = 0 + \mathbf{suc}(m) = \mathbf{suc}(m) + 0 = \mathbf{suc}(m) = 1 + m$$

o que prova o lema. □

Seja agora o conjunto X definido por $X \equiv \{n \in \mathbb{N} : \forall_m \,[\, m \in \mathbb{N} \;\Rightarrow\; [\, m + n = n + m \,]]\}$. De (a) resulta

$$0 \in X. \tag{2.7}$$

Seja $p \in X$ qualquer. Então, pela definição de X, tem-se para todo $m \in \mathbb{N}$ que $m+p = p+m$ e portanto tendo em conta resultados anteriores, vem sucessivamente

$$\begin{aligned} m + \mathbf{suc}(p) &= \mathbf{suc}(m + p) \\ &= \mathbf{suc}(p + m) = p + \mathbf{suc}(m) \\ &= p + (1 + m) = (p + 1) + m = \mathbf{suc}(p) + m \end{aligned}$$

o que significa que

$$\forall_p \,[\, p \in X \Rightarrow \mathbf{suc}(p) \in X \,] \tag{2.8}$$

De (2.7) e (2.8) e tendo em conta o axioma **N5** resulta que $X = \mathbb{N}$, o que por seu lado completa a demonstração do teorema. □

A **multiplicação** de números naturais é uma operação interna, denotada pelo símbolo $\cdot$ (ou mais frequentemente por simples justaposição) que se define recursivamente por

M1 $\forall_n\ [\, n \in \mathbb{N} \Rightarrow [\, n \cdot 0 = 0\,]\,]$

M2 $\forall_{n,m}\ [\, m, n \in \mathbb{N} \Rightarrow [\, n \cdot \mathbf{suc}(m) = n \cdot m + n\,]$,

sendo, também neste caso, possível provar que existe uma e uma só operação interna definida sobre $\mathbb{N}_0$ que satisfaça **M1** e **M2**.

Teorema 2.6 *A multiplicação em* $\mathbb{N}$ *é distributiva à direita relativamente à adição, isto é,*

$$m(n+p) = mn + mp$$

quaisquer que sejam os números $m, n, p \in \mathbb{N}$.

Demonstração: Seja X o conjunto de números definido por

$$X \equiv \{p \in \mathbb{N} : \forall_{m,n}\ [m, n \in \mathbb{N} \Rightarrow [\, m(n+p) = mn + mp\,]\,]\}.$$

Tendo em conta **A1** e **M1** tem-se para todos $m, n \in \mathbb{N}$ que $m(n+0) = mn = mn + 0 = mn + m0$ o que mostra que

$$0 \in X. \tag{2.9}$$

Seja agora $q \in X$ arbitrariamente fixado. Então quaisquer que sejam os números $m, n \in \mathbb{N}$, vem $m(n+q) = mn+mq$ e, portanto, tendo em conta A2, M2, a hipótese de indução e o teorema 2.2, obtém-se sucessivamente

$$\begin{aligned} m(n + \mathbf{suc}(q)) &= m \cdot \mathbf{suc}(n+q) = m(n+q) + m \\ &= (mn + mq) + m = mn + (mq + m) \\ &= mn + m \cdot \mathbf{suc}(q) \end{aligned}$$

donde resulta que

$$\forall_q\ [\, q \in X \Rightarrow \mathbf{suc}(q) \in X\,] \tag{2.10}$$

De (2.9) e (2.10), tendo em conta o axioma **N5**, conclui-se que $X = \mathbb{N}$, ficando provado o teorema. □

Teorema 2.7 *A multiplicação em* $\mathbb{N}$ *é associativa.*

Demonstração: Seja X o conjunto de números definido por

$$X \equiv \{p \in \mathbb{N} :\ \forall_{m,n}\ [\, m, n \in \mathbb{N} \Rightarrow [\, (mn)p = m(np)\,]\,]\}$$

Então, visto que quaisquer que sejam $m, n \in \mathbb{N}$, atendendo a **M1**, se tem, $(mn)0 = 0 = m \cdot 0 = m(n \cdot 0)$ conclui-se que

$$0 \in X \tag{2.11}$$

Seja q um elemento qualquer de X. Pela definição de X então tem-se que $(mn)q = m(nq)$ quaisquer que sejam $m, n \in \mathbb{N}$ e portanto, atendendo a **M2**, hipótese de indução e ao teorema 2.6, tem-se sucessivamente

$$\begin{aligned}(mn)\cdot \mathbf{suc}(q) &= (mn)q + mn = m(nq) + mn \\ &= m(nq+n) = m(n\cdot \mathbf{suc}(q))\end{aligned}$$

o que prova que

$$\forall_q \, [\, q \in X \Rightarrow \mathbf{suc}(q) \in X \,] \tag{2.12}$$

De (2.11) e (2.12), atendendo ao axioma **N5** obtém-se $X = \mathbb{N}$, ficando provado, deste modo, o teorema. □

Teorema 2.8 *A multiplicação em* $\mathbb{N}$ *é distributiva à esquerda relativamente à adição, isto é,*

$$(m+n)p = mp + np$$

quaisquer que sejam os números $m, n, p \in \mathbb{N}$.

Demonstração: Seja X o conjunto de números definido por

$$X \equiv \{p \in \mathbb{N} : \forall_{m,n} \, [m, n \in \mathbb{N} \;\Rightarrow\; [(m+n)p = mp + np \,]\,]\}$$

De **A1** e **M1** tem-se, quaisquer que sejam $m, n \in \mathbb{N}$, que $(m+n)0 = 0 = 0 + 0 = m0 + n0$ o que mostra que

$$0 \in X \tag{2.13}$$

Seja agora $q \in X$ qualquer. Então, da definição de X, tem-se que $(m+n)q = mq + nq$ e, portanto, tendo em conta **M2**, hipótese de indução, teoremas 2.2 e 2.3, sucessivamente, vem

$$\begin{aligned}(m+n)\cdot \mathbf{suc}(q) &= (m+n)q + (m+n) = (mq+nq) + (m+n) \\ &= mq + (nq + (m+n)) = mq + ((nq+n)+m) \\ &= mq + (n\cdot \mathbf{suc}(q) + m) = mq + (m + n\cdot \mathbf{suc}(q)) \\ &= (mq+m) + n\cdot \mathbf{suc}(q) = m\cdot \mathbf{suc}(q) + n\cdot \mathbf{suc}(q)\end{aligned}$$

o que mostra que

$$\forall_q \, [\, q \in X \Rightarrow \mathbf{suc}(q) \in X \,] \tag{2.14}$$

De (2.13) e (2.14), atendendo ao axioma **N5**, $X = \mathbb{N}$, ficando o teorema completamente demonstrado. □

Teorema 2.9 *A multiplicação em* $\mathbb{N}$ *é comutativa.*

Demonstração: (a) - Provar-se-á em primeiro lugar que qualquer que seja $m \in \mathbb{N}$ se tem $0m = m0$. Seja $\mathcal{M} \equiv \{m \in \mathbb{N}_0 : 0m = m0\}$. Como $0 \cdot 0 = 0 \cdot 0$ então tem-se imediatamente que

$$0 \in \mathcal{M} \tag{2.15}$$

Seja $n \in \mathcal{M}$ qualquer. Então da definição de $\mathcal{M}$ resulta que $0 \cdot n = n \cdot 0$ e portanto, tendo em conta **M1** e **M2**, a hipótese de indução o lema 2.4 e o teorema 2.8, vem sucessivamente

$$\begin{aligned} 0 \cdot \mathbf{suc}(n) &= 0 \cdot n + 0 \\ &= n \cdot 0 + 1 \cdot 0 = (n+1) \cdot 0 = \mathbf{suc}(n) \cdot 0 \end{aligned}$$

donde resulta

$$\forall_n \, [\, n \in \mathcal{M} \Rightarrow \mathbf{suc}(n) \in \mathcal{M} \,] \tag{2.16}$$

Consequentemente de (2.15) e (2.16) e axioma **N5** fica completamente provada a afirmação em (a).

(b) - Para demonstrar o caso geral torna-se necessário provar primeiramente o seguinte resultado preliminar

Lema 2.10 *Qualquer que seja $m \in \mathbb{N}$ tem-se $1 \cdot m = m$.*

Demonstração: Seja $\mathcal{M}$ o conjunto de números $\mathcal{M} \equiv \{m \in \mathbb{N} : 1 \cdot m = m\}$. De **M1** resulta que $1 \cdot 0 = 0$ e portanto

$$0 \in \mathcal{M} \tag{2.17}$$

Seja $n \in \mathcal{M}$ qualquer. Então da definição de $\mathcal{M}$ tem-se que $1 \cdot n = n$ e portanto tendo em conta também **M2** vem $1 \cdot \mathbf{suc}(n) = 1 \cdot n + 1 = n + 1 = \mathbf{suc}(n)$, o que mostra que

$$\forall_n \, [\, n \in \mathcal{M} \Rightarrow \mathbf{suc}(n) \in \mathcal{M} \,] \,. \tag{2.18}$$

De (2.17) e (2.18) e axioma **N5** fica provado o lema. □

Seja agora X o conjunto de números definido por

$$X \equiv \{n \in \mathbb{N} : \, [\, \forall_m \, [\, m \in \mathbb{N} \;\Rightarrow\; [\, m \cdot n = n \cdot m \,]\,]\}$$

De (a) tem-se imediatamente

$$0 \in X. \tag{2.19}$$

Seja $p \in X$ qualquer. Então da definição de X tem-se que $mp = pm$ qualquer que seja $m \in \mathbb{N}$. Consequentemente, de **M2**, lema 2.10, hipótese de indução, lema 2.4 e teorema 2.8, vem

$$\begin{aligned} m \cdot \mathbf{suc}(p) &= mp + m \\ &= pm + 1 \cdot m = (p+1)m = \mathbf{suc}(p) \cdot m \end{aligned}$$

o que significa que

$$\forall_p \, [\, p \in X \Rightarrow \mathbf{suc}(p) \in X \,] \tag{2.20}$$

De (2.19), (2.20) e axioma **N5** fica provado o teorema. □

2.1.4 O conjunto ordenado $(\mathbb{N}, \leq)$

Seja em $\mathbb{N}$ a relação $\mathcal{R}$ definida por

$$\mathcal{R} \;=\; \{(m,n) \in \mathbb{N}^2 : \exists_p \,[\, p \in \mathbb{N} \wedge m + p = n \,]\}$$

Teorema 2.11 *$\mathcal{R}$ é uma relação de ordem total (em sentido lato) em $\mathbb{N}$.*

Demonstração: Terá de mostrar-se que, assim definida, a relação $\mathcal{R}$ é reflexiva, antisimétrica, transitiva e dicotómica:

(1) Reflexividade. Do axioma **A1** da definição de adição em $\mathbb{N}$ tem-se que $n + 0 = n$, $\forall_{n\in\mathbb{N}}$ e portanto $(n,n) \in \mathcal{R}$, $\forall_{n\in\mathbb{N}}$.

(2) Anti-simetria (lata). Sejam $m, n \in \mathbb{N}$ tais que $(m,n) \in \mathcal{R}$ e $(n,m) \in \mathcal{R}$. Visto que $(m,n) \in \mathcal{R}$ então existe $p \in \mathbb{N}$ tal que $m + p = n$ e, como $(n,m) \in \mathcal{R}$ então existe $q \in \mathbb{N}_0$ tal que $n + q = m$. Destas duas igualdades resulta que

$$n + (q + p) = n$$

o que, como se verá, implica que se tenha $q + p = 0$ (em $\mathbb{N}$). De facto, seja

$$\mathcal{M} \;=\; \{n \in \mathbb{N} : \,[\, n + (p + q) = n \;\Rightarrow\; p + q = 0 \,]\,\}.$$

Visto que de $0+(p+q) = 0$ resulta que se tenha $p+q = 0$ então $0 \in \mathcal{M}$. Suponha-se (hipótese de indução) que $m \in \mathcal{M}$, ou seja, que

$$m + (p + q) \;=\; m \;\Rightarrow\; p + q \;=\; 0.$$

Como da iguldade $\mathbf{suc}(m)+(p+q) = \mathbf{suc}(m)$, pela comutatividade da adição e por **A2**, se obtém $\mathbf{suc}(m + (p + q)) = \mathbf{suc}(m)$ então, tendo em conta **N4**, resulta que $m+(p+q) = m$ o que, por seu turno, implica que seja $p+q = 0$. Consequentemente $m \in \mathcal{M} \Rightarrow \mathbf{suc}(m) \in \mathcal{M}$ e, portanto, por **N5**, $\mathcal{M} = \mathbb{N}$.

Sendo p um elemento de $\mathbb{N}$ ter-se-á de acordo com a Axiomática de Peano (axiomas **N1** e **N2**) que $p = 0$ ou $p = \mathbf{suc}(r)$ para algum $r \in \mathbb{N}_0$. Se fosse $p = \mathbf{suc}(r)$ então, de acordo com **A2** da definição de adição em $\mathbb{N}$, ter-se-ia

$$q + p \;=\; q + \mathbf{suc}(r) \;=\; \mathbf{suc}(q + r) \;=\; 0$$

o que é absurdo já que, pelo axioma **N3**, 0 não é sucessor de nenhum elemento de $\mathbb{N}$; logo será $p = 0$ e, portanto, de **A1** (definição de adição) vem

$$q + p \;=\; q + 0 \;=\; q \;=\; 0.$$

Consequentemente, tem-se que

$$(m,n) \in \mathcal{R} \wedge (n,m) \in \mathcal{R} \;\Rightarrow\; m = n$$

como se pretendia mostrar.

(3) Transitividade. Suponha-se que para $m, n, j \in \mathbb{N}$ se tem que $(m, n) \in \mathcal{R}$ e $(n, j) \in \mathcal{R}$. Então existem números $p, q \in \mathbb{N}$ tais que $m + p = n$ e $n + q = j$; consequentemente, de $(m + p) + q = n + q$ decorre que $m + (p + q) = j$ e como $p + q \in \mathbb{N}$ então ter-se-á que $(m, j) \in \mathcal{R}$.

(4) Dicotomia. Para cada $m \in \mathbb{N}$ seja definido o seguinte conjunto

$$\mathcal{M} \ = \ \{n \in \mathbb{N} : (m, n) \in \mathcal{R} \vee (n, m) \in \mathcal{R}\}.$$

Como $m \in \mathbb{N}$ e $0 + m = m$ tem-se, portanto, $(0, m) \in \mathcal{R}$ e, consequentemente,

(a) $0 \in \mathcal{M}$

Seja $n \in \mathcal{M}$. Então ou $(m, n) \in \mathcal{R}$ ou $(n, m) \in \mathcal{R}$. Se $(m, n) \in \mathcal{R}$ então existe $p \in \mathbb{N}$ tal que $m + p = n$ donde pelo axioma **N4** resulta que $\mathbf{suc}(m + p) = \mathbf{suc}(n)$ e por **A2** da definição de adição resulta que $m + \mathbf{suc}(p) = \mathbf{suc}(n)$ o que, por seu turno, significa que $(m, \mathbf{suc}(n)) \in \mathcal{R}$ e, consequentemente, $\mathbf{suc}(n) \in \mathcal{M}$.
Se for $(n, m) \in \mathcal{R}$ então existe $q \in \mathbb{N}$ tal que $n + q = m$ onde $q = 0$ ou $q = \mathbf{suc}(s)$ para algum $s \in \mathbb{N}_0$. Se for $q = 0$ então $n = m$ e $\mathbf{suc}(n) = m + 1$ o que mostra que $(m, \mathbf{suc}(n)) \in \mathcal{R}$ e portanto que $\mathbf{suc}(n) \in \mathcal{M}$. Se for $q = \mathbf{suc}(s)$ então

$$\begin{aligned} m &= n + q \\ &= n + \mathbf{suc}(s) \ = \ \mathbf{suc}(n + s) \ = \ \mathbf{suc}(s + n) \\ &= s + \mathbf{suc}(n) \ = \ \mathbf{suc}(n) + s \end{aligned}$$

o que mostra que $(\mathbf{suc}(n), m) \in \mathcal{R}$ e, portanto, que $\mathbf{suc}(n) \in \mathcal{M}$. Então

(b) $\forall_{n \in \mathbb{N}} \, [\, n \in \mathcal{M} \Rightarrow \mathbf{suc}(n) \in \mathcal{M} \,]$

De **(a)** e **(b)**, tendo em conta o axioma **N5**, resulta $\mathcal{M} = \mathbb{N}$, ou seja, que

$$\forall_{m,n \in \mathbb{N}} \, [\, (m, n) \in \mathcal{R} \ \vee \ (n, m) \in \mathcal{R} \,]$$

ficando assim completada a demonstração da proposição. □

Dados dois elementos $m, n \in \mathbb{N}$ quaisquer, sempre que $(m, n) \in \mathcal{R}$ é usual escrever $m \leq n$ (ou $n \geq m$). Se, para $m, n \in \mathbb{N}$, se tiver $m \leq n \wedge m \neq n$ então escreve-se $m < n$ (ou $n > m$). O par ordenado $(\mathbb{N}, \leq)$ designa-se por **conjunto ordenado dos números naturais**.

2.2 Indução Matemática – Aplicações

O princípio de indução matemática, decorrente do axioma **N5**, pode ser generalizado da seguinte forma: se $\mathbf{A} \subset \mathbb{Z}$ for um conjunto bem ordenado, tal que

1. $p \in A$ e p é o menor elemento de $\mathbf{A}$,

2. $\forall_{n\in\mathbb{Z}}\,[\,n \geq p \;\Rightarrow\; [\,n \in \mathbf{A} \Rightarrow n+1 \in \mathbf{A}\,]\,]$

então,

$$A \;=\; \{n \in \mathbb{Z} : n \geq p\}$$

O princípio de indução matemática usual é um caso particular deste enunciado no qual $p = 0$.

Este princípio é usado frequentemente em Matemática para provar proposições da forma

$$\forall_n\,[\,n \in \mathbb{N}_r \Rightarrow p(n)\,]$$

onde $\mathbb{N}_r = \{n \in \mathbb{Z} : n \geq r\}$ e $p(n)$ é uma fórmula com uma variável livre cujo domínio é $\mathbb{N}_r$. Considere-se, por exemplo, a seguinte proposição

$$\forall_n\;\left[\,n \in \mathbb{N}_1 \Rightarrow 1+2+3+\cdots+n = \frac{n(n+1)}{2}\,\right]$$

cuja prova se pode fazer apelando ao princípio de indução matemática generalizado. Seja $p(n)$ a fórmula

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

e $\mathbf{A} \subseteq \mathbb{N}$ o conjunto de verdade de $p(n)$.

Fazendo $n = 1$ é imediato comprovar que $p(1)$ é uma proposição verdadeira e, portanto, $1 \in \mathbf{A}$. Suponha-se agora que $n \in \mathbf{A}$, ou seja, que para um dado inteiro $n > 1$, fixado arbitrariamente, se verifica a proposição $p(n)$ – hipótese de indução. Vejamos o que se passa com $p(n+1)$. Ora

$$1+2+3+\quad\cdots\quad+n+(n+1) \;=\; (1+2+3+\cdots+n)+(n+1)$$

$$\begin{aligned} &= \quad \frac{n(n+1)}{2}+(n+1) \\ &= \quad (n+1)\left(\frac{1}{2}\,n+1\right) \;=\; \frac{(n+1)(n+2)}{2} \end{aligned}$$

e, portanto, da validade da proposição $p(n)$ resulta a validade da proposição $p(n+1)$. Isto significa que se $n \in \mathbf{A}$ então $n+1 \in \mathbf{A}$. Pelo princípio de indução pode concluir-se que $\mathbf{A} = \mathbb{N}_1$ o que significa que $p(n)$ se verifica para todo o $n = 1, 2, \ldots$.

Exemplo 2.12 Sendo $x \geq 0$ um número real pretende-se mostrar que

$$\forall_n \, [\, n \in \mathbb{N}_1 \, \Rightarrow \, (1+x)^n \, \geq \, 1 + x^n \,]$$

Por uma questão de comodidade denote-se por $p(n)$ a fórmula $(1+x)^n \geq 1 + x^n$ e aplique-se a $p(n)$ o método de indução.

Para $n = 1$ obtém-se $1 \geq 1$ o que mostra que $p(1)$ é uma proposição verdadeira. Suponha-se, hipótese de indução, que para $n > 1$, arbitrariamente fixado, $p(n)$ se verifica e considere-se então $p(n+1)$:

$$\begin{aligned} (1+x)^{n+1} &= (1+x)^n(1+x) \\ &\geq (1+x^n)(1+x) \, = \, 1 + x + x^n + x^{n+1} \\ &\geq 1 + x^{n+1} \end{aligned}$$

Então da validade de $p(n)$ resulta a validade de $p(n+1)$ e, portanto, pelo princípio de indução matemática pode afirmar-se que $p(n)$ se verifica qualquer que seja $n = 1, 2, 3, \ldots$.

Exemplo 2.13 Sendo $n \in \mathbb{N}$, $n \geq 13$ pretende-se verificar que

$$n^2 \, < \, \left(\frac{3}{2}\right)^n \tag{2.21}$$

Designe-se por $p(n)$ a fórmula (2.21). Fazendo $n = 13$, vem

$$13^2 \, = \, 169 \, < \, 194 \, < \, \frac{1594323}{8192} \, = \, \left(\frac{3}{2}\right)^{13}$$

e, portanto, $p(13)$ é verdadeira. Suponha-se agora, hipótese de indução, que para $n > 13$, fixado arbitrariamente, se tem $n^2 < (3/2)^n$: então

$$\begin{aligned} (n+1)^2 &= \left(1 + \frac{1}{n}\right)^2 n^2 \\ &< \left(1 + \frac{1}{13}\right)^2 n^2 \, = \, \frac{196}{169}\, n^2 \\ &< \frac{3}{2}\, n^2 \\ &< \frac{3}{2}\left(\frac{3}{2}\right)^n \, = \, \left(\frac{3}{2}\right)^{n+1} \end{aligned}$$

verificando-se, portanto, $p(n+1)$ sempre que se verifica $p(n)$. Tendo em conta o princípio de indução generalizado, pode concluir-se que

$$n^2 \, < \, \left(\frac{3}{2}\right)^n$$

para todo o $n \geq 13$.

Exercícios 2.2.1

1. *Provar as seguintes proposições*

   (a) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow 1^2 + 2^2 + \cdots + n^2 \;=\; n(n+1)(2n+1)/6\,]$
   (b) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow 1^3 + 2^3 + \cdots + n^3 \;=\; (n(n+1)/2)^2\,]$
   (c) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow 1 + 3 + 5 + \cdots + (2n-1) \;=\; n^2\,]$
   (d) $\forall_n\,[\,n \in \mathbb{N} \wedge n \geq 2 \;\Rightarrow\; \forall_{x,y}\,[\,x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})\,]\,]$
   (e) $\forall_n\,[\,n \in \mathbb{N} \;\Rightarrow\; 2 \quad \text{divide} \quad n(n+1)\,]$
   (f) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow D_x^n\, x^n = n!\,]$
   (g) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow 2^n \;>\; n\,]$
   (h) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow \forall_{a,b}\,[\,a, b \in \mathbb{R} \wedge a > b > 0 \Rightarrow a^n \;>\; b^n\,]\,]$
   (i) $\forall_n\,[\,n \in \mathbb{N} \Rightarrow \frac{1}{1\cdot 3} + \frac{1}{2\cdot 4} + \cdots + \frac{1}{n(n+2)} \;=\; \frac{3n^2+5n}{4(n+1)(n+2)}\,]$
   (j) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n \cdot (n+1) = n(n+1)(n+2)/3$
   (k) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$
   (l) $n^3 + 2n$ *é divisível por 3 qualquer que seja* $n \in \mathbb{N}$
   (m) $7^n - 1$ *é divisível por 6 qualquer que seja* $n \in \mathbb{N}$
   (n) $11^n - 6$ *é divisível por 5 qualquer que seja* $n \in \mathbb{N}$
   (o) $6 \cdot 7^n - 2 \cdot 3^n$ *é divisível por 4 qualquer que seja* $n \in \mathbb{N}$
   (p) $3^n + 7^n - 2$ *é divisível por 8 qualquer que seja* $n \in \mathbb{N}$

2. *A sucessão* $(a_n)_{n\in\mathbb{N}}$ *é definida por*

$$\begin{cases} a_1 = 1 \\ a_{n+1} = a_n + 8n \end{cases}$$

   Descobrir uma fórmula fechada para a_n *e prove a sua validade por indução.*

3. *Seja* $(a_n)_{n=1,2,\ldots}$ *uma sucessão definida recursivamente por*

$$\begin{cases} a_1 &=& 1 \\ a_n &=& a_{n-1} + 2\sqrt{a_{n-1}} + 1, \quad n \geq 2 \end{cases}$$

   Mostrar que a_n *é um número inteiro qualquer que seja* $n \in \mathbb{N}$.

4. *Descobrir e provar por indução uma fórmula para*

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

2.2.1 Formas equivalentes do princípio de indução finita

A versão do princípio de indução tal como foi estabelecido na axiomática de Dedekind-Peano, apresentada no início deste capítulo, é, muitas vezes, designada por **forma fraca** do princípio de indução, por oposição a uma outra formulação que lhe é equivalente e que é conhecida por **forma forte** do princípio de indução ou, mais simplesmente, por **indução completa**. A indução completa tem a seguinte formulação

> Sendo $\mathbf{A}$ um conjunto de números naturais tal que
>
> 1. $0 \in \mathbf{A}$,
> 2. $\forall_n \, [\, n \in \mathbb{N} \Rightarrow \, [\, \{0, 1, \ldots, n\} \subset \mathbf{A} \Rightarrow n + 1 \in \mathbf{A} \,] \,]$
>
> então $\mathbf{A} = \mathbb{N}$.

Nalgumas situações a aplicação do método de indução completa é mais fácil do que o princípio de indução fraca.

Para demonstrar que as duas formulações são equivalentes é necessário fazer apelo a uma propriedade importante do conjunto $\mathbb{N}$ que é conhecida por **princípio da boa ordenação**.

Seja $\mathbf{A}$ um subconjunto qualquer do conjunto ordenado $\mathbb{N}$. Um elemento $a \in \mathbf{A}$ dir-se-á **primeiro elemento** de $\mathbf{A}$ se e só se verificar a condição

$$\forall_x \, [\, x \in \mathbf{A} \; \Rightarrow \; a \leq x \,]$$

podendo verificar-se que quando um tal elemento existe ele é único.

Teorema 2.14 *Todo o subconjunto não vazio de* $\mathbb{N}$ *possui primeiro elemento.*

Demonstração: Seja $\mathbf{A} \subset \mathbb{N}$ não vazio e suponha-se, por redução ao absurdo que $\mathbf{A}$ não possui primeiro elemento. Designando por $\mathbf{A}^c$ o complementar de $\mathbf{A}$ em $\mathbb{N}$, considere-se o conjunto

$$\mathbf{T} \; \equiv \; \{n \in \mathbb{N} : \; \forall_{m \in \mathbb{N}} \, [\, m \leq n \Rightarrow m \in \mathbf{A}^c \,]\}.$$

Como 0 não pode pertencer a $\mathbf{A}$ (de contrário seria certamente o primeiro elemento de $\mathbf{A}$) então $0 \in \mathbf{A}^c$ e, portanto, $0 \in \mathbf{T}$. Suponha-se agora que $k \in \mathbf{T}$. Da definição de $\mathbf{T}$, resulta então que os números $1, 2, \ldots, k$ pertencem todos a $\mathbf{A}^c$. Quanto a $k+1$ não pode pertencer a $\mathbf{A}$ pois de contrário seria o seu primeiro elemento o que é contra a hipótese feita; então $k + 1 \in \mathbf{A}^c$ e, portanto, $k + 1 \in \mathbf{T}$. Visto que

(a) $0 \in \mathbf{T}$, e

(b) $\forall_k [\, k \in \mathbf{T} \Rightarrow k+1 \in \mathbf{T}]$,

então, pelo Axioma **N5**, segue-se que $\mathbf{T} = \mathbb{N}$. Em consequência vem $\mathbf{A}^c = \mathbb{N}$ e, portanto, $\mathbf{A} = \emptyset$ o que contradiz a hipótese considerada. Logo $\mathbf{A}$ possui primeiro elemento. □

É costume traduzir o resultado deste teorema dizendo que $\mathbb{N}$ é um **conjunto bem-ordenado**.

Seguidamente, com base neste teorema, demonstrar-se-á o seguinte:

Teorema 2.15 *Em* $\mathbb{N}$ *verifica-se o princípio de indução completa, ou seja, sendo* $\mathbf{A}$ *um conjunto de números naturais tal que*

1. $0 \in \mathbf{A}$,
2. $\forall_n [\, n \in \mathbb{N} \Rightarrow [\, \{0, 1, \ldots, n\} \subset \mathbf{A} \Rightarrow n+1 \in \mathbf{A}\,]\,]$

então $\mathbf{A} = \mathbb{N}$.

Demonstração: Seja $\mathbf{A}^c$ o complementar de $\mathbf{A}$. Se $\mathbf{A}^c = \emptyset$ então o teorema está trivialmente demonstrado e, portanto, suponha-se que $\mathbf{A}^c \neq \emptyset$. Pelo princípio da boa ordenação – teorema 2.14 – $\mathbf{A}^c$ possui um primeiro elemento que se designará por k. É claro que $k \neq 0$ visto que $0 \in \mathbf{A}$ por hipótese.; por outro lado, $0, 1, 2, \ldots, k-1$ têm de pertencer todos a $\mathbf{A}$ pois de contrário algum deles seria o primeiro elemento de $\mathbf{A}^c$ e não k como se supôs. Então, pela segunda condição do teorema, ter-se-á também $k \in \mathbf{A}$ o que contradiz a hipótese de ser k o primeiro elemento do complementar de $\mathbf{A}$. Assim, ter-se-á necessariamente $\mathbf{A}^c = \emptyset$ e, portanto, $\mathbf{A} = \mathbb{N}$. □

Para completar o ciclo de implicações que nos permite concluir a equivalência dos dois princípios de indução e do princípio da boa ordenação de $\mathbb{N}$, mostrar-se-á agora que o princípio de indução completa implica a indução fraca.

Teorema 2.16 *Suponha-se que se verifica em* $\mathbb{N}$ *o princípio de indução completa e seja* $\mathbf{A}$ *um conjunto de números naturais tal que*

1. $0 \in \mathbf{A}$,
2. $\forall_n [\, n \in \mathbb{N} \Rightarrow [\, n \in \mathbf{A} \Rightarrow n+1 \in \mathbf{A}\,]\,]$

Então $\mathbf{A} = \mathbb{N}$.

Demonstração: Suponha-se que se verificam as duas condições acima. Visto que a proposição

$$\forall_{n\in\mathbb{N}}\,[\,\{0,1,\ldots,n\}\subseteq\mathbf{A}\;\Rightarrow\;n\in\mathbf{A}\,]$$

é evidentemente verdadeira, então tem-se que

$$\forall_{n\in\mathbb{N}}\,[\,[\,\{0,1,\ldots,n\}\subseteq\mathbf{A}\wedge[\,n\in\mathbf{A}\Rightarrow n+1\in\mathbf{A}\,]\,]$$

donde resulta imediatamente

$$\forall_{n\in\mathbb{N}}\,[\,\{0,1,\ldots,n\}\subseteq\mathbf{A}\;\Rightarrow\;n+1\in\mathbf{A}\,]$$

Pelo princípio de indução completa ter-se-á então $\mathbf{A}=\mathbb{N}$, ficando demonstrado o teorema. □

Suponha-se que $p(n)$ é uma afirmação sobre o número natural n e que r é um número natural fixado. Então a demonstração por indução de que $p(n)$ se verifica para todo o $n\geq r$ requer os dois seguintes passos:

1. Verificar que $p(r)$ é uma proposição verdadeira.
2. Verificar que se $k\geq r$ e se $p(r),p(r+1),p(r+2),\ldots,p(k)$ são proposições verdadeiras, então $p(k+1)$ também é verdadeira.

Exemplo 2.17 *Mostrar, por indução completa, que qualquer número natural maior que 1 se pode decompor num produto de factores primos.*
Resolução. Seja $p(n)$ a afirmação de que quando n é um número natural maior que 1 se pode decompor num produto de factores primos. O objectivo agora é o de provar que $p(n)$ é uma proposição verdadeira qualquer que seja $n>1$.

1 – $p(2)$ é, evidentemente, uma proposição verdadeira pois que 2 (sendo primo) pode ser factorizado num produto de factores primos (neste caso com um só factor).

2 – Suponha-se agora que $p(2),p(3),\ldots,p(k)$ são proposições todas verdadeiras. Pretende-se então mostrar que da veracidade destas proposições resulta a veracidade de $p(k+1)$.

Se $k+1$ for um número primo a afirmação é trivialmente verdadeira. Se $k+1$ não for primo então é um número composto sendo, portanto, possível encontrar dois inteiros positivos m e n tais que $k+1=m\cdot n$ onde tanto m como n são menores que k. Pela hipótese de indução completa, tanto m como n se podem decompor num produto de factores primos e, portanto, o mesmo acontece a $k+1$. Logo $p(k+1)$ é uma proposição verdadeira, como se pretendia mostrar.

Exemplo 2.18 Para mostrar que as três formulações alternativas da indução matemática – princípio de indução finita, princípio da boa ordenação e princípio

da indução completa – podem ser usadas para resolver o mesmo tipo de problemas exemplificar-se-á a demonstração da conhecida proposição

$$\forall_n \, [\, n \in \mathbb{N}_1 \;\Rightarrow\; 1 + 2 + \cdots + n = n(n+1)/2 \,]$$

usando agora o princípio da boa ordenação.

Represente-se por $p(n)$, como é habitual, a fórmula

$$1 + 2 + \cdots + n \;=\; \frac{1}{2}\, n(n+1)$$

Seja

$$\mathbf{A} = \{n \in \mathbb{N}_1 : \neg p(n)\}$$

Se $\mathbf{A} = \emptyset$ então a proposição fica automaticamente demonstrada. Suponha-se então que $\mathbf{A} \neq \emptyset$. Pelo princípio da boa ordenação, $\mathbf{A}$ tem um primeiro elemento, k. Visto que $p(1)$ é evidentemente verdadeira, então $1 \notin \mathbf{A}$ e, portanto, $k \neq 1$, donde se pode concluir que $k - 1 \in \mathbb{N}_1$. Como, por outro lado, $k - 1 \notin \mathbf{A}$ então $p(k-1)$ é verdadeira. Então, tem-se o seguinte:

$$\begin{aligned} 1 + 2 + \cdots + (k-1) + k &= \frac{1}{2}\,(k-1)k + k \\ &= k\left(\frac{1}{2}(k-1) + 1\right) \;=\; \frac{1}{2}\, k(k+1) \end{aligned}$$

o que mostra que $p(k)$ é uma proposição verdadeira. Mas isto é contraditório com o facto de k ser o primeiro elemento de $\mathbf{A}$. A contradição resultou de se supor que $\mathbf{A}$ era não vazio o que, portanto, é falso. Ou seja, $p(n)$ verifica-se para todo o $n \in \mathbb{N}_1$.

Exemplo 2.19 *Mostrar, usando o princípio da boa ordenação, que* $\sqrt{2}$ *é um número irracional.*

Resolução. Suponha-se, pelo contrário, que $\sqrt{2}$ é racional; isto é, que existem números $r, s \in \mathbb{N}_1$ tais que $\sqrt{2} = r/s$. Então,

$$\mathbf{A} \;=\; \{x \in \mathbb{N} : x = n\sqrt{2} \;\text{ para algum }\; n \in \mathbb{N}_1\}$$

será um conjunto não vazio de números naturais (em particular conterá, por hipótese, o número r). Pelo princípio da boa ordenação o conjunto $\mathbf{A}$ possuirá um primeiro elemento: suponha-se que é k esse elemento. Seja $m \in \mathbb{N}$ tal que $k = m\sqrt{2}$. Então $m(\sqrt{2}-1) = k - m$ é um número natural menor que m (visto que $0 < \sqrt{2} - 1 < 1$) e, portanto, $q = m(\sqrt{2}-1)\sqrt{2}$ é menor que k. Mas $q = 2m - k$ o que significa que $q \in \mathbb{N}$, por um lado, e, por outro lado, $q \in \mathbf{A}$. Esta conclusão é contraditória visto que se encontra em $\mathbf{A}$ um elemento menor que k. Então $\mathbf{A}$ deverá ser vazio e, portanto, $\sqrt{2}$ não é um número racional.

Exercícios 2.2.2

1. *Mostrar que $\mathbb{Z}$, o conjunto dos números inteiros, não possui a propriedade da boa ordenação para o que basta apresentar um subconjunto não vazio de $\mathbb{Z}$ que não possua primeiro elemento.*
2. *Mostrar que $\sqrt{3}$ é irracional usando o princípio da boa ordenação de $\mathbb{N}$. Se pretendesse usar a mesma técnica para mostrar que $\sqrt{4}$ é irracional onde é que a demonstração falhava?*
3. *Sejam α e β as soluções da equação*

$$x^2 - x - 1 \;=\; 0$$

com $\alpha > 0$. Para $n \in \mathbb{N}_1$ qualquer define-se

$$f_n \;=\; \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

A sucessão $(f_n)_{n\in\mathbb{N}}$ é conhecida por sucessão de números de Fibonaci de que se voltará a falar no seguimento.

   (a) *Determinar f_1, f_3 e f_4.*
   (b) *Mostrar que $\forall_n\,[n \in \mathbb{N}_1 \Rightarrow f_{n+2} = f_{n+1} + f_n]$.*
   (c) *Mostrar que f_n é inteiro qualquer que seja $n \in \mathbb{N}_1$.*
   (d) *Mostrar que $f_n < (13/8)^n$ qualquer que seja $n \in \mathbb{N}_1$.*
   (e) *Mostrar que $f_{n+1}^2 - f_n f_{n+2} = (-1)^n$ qualquer que seja $n \in \mathbb{N}_1$.*
   (f) *Mostrar que para todo o $n \in \mathbb{N}_1$*

$$\sum_{i=1}^{n} f_i \;=\; f_{n+2} - 1$$

4. *Seja $(a_n)_{n=1,2,\ldots}$ uma sucessão tal que $a_1 = a_2 = 1$ e para $n \geq 3$,*

$$a_n \;=\; 4a_{n-1} + 5a_{n-2}$$

Mostrar que para $n \geq 3$, se tem

$$a_n \;=\; \frac{1}{15}\,5^n + \frac{2}{3}\,(-1)^{n+1}$$

2.3 Introdução ao Cálculo Combinatório

O cálculo combinatório tem por objecto o estudo de problemas relativos ao número de elementos de diferentes conjuntos que podem ser obtidos a partir de conjuntos dados.

Definição 2.20 *Dados dois conjuntos A e B diz-se que A* **é equipotente** *a B se e só se for possível estabelecer uma correspondência bijectiva entre eles.*

Esta relação de equipotência entre conjuntos é reflexiva, simétrica e transitiva. Logo é uma relação de equivalência.

Definição 2.21 *Diz-se que dois conjuntos têm o mesmo número de elementos (ou a mesma potência) se e só se A e B forem equipotentes.*

Deste modo, o número de elementos de um conjunto A – a cardinalidade de A, $\mathbf{card}(A)$ – é, por asssim dizer, a propriedade que esse conjunto tem de comum com todos os conjuntos que se possam pôr em correspondência bijectiva com A. Por conseguinte, o número de elementos de A poderá ser representado indistintamente por qualquer desses conjuntos (equipotentes a A) incluindo o próprio A.

Se A for um conjunto finito então é possível definir uma correspondência bijectiva entre os elementos de A e os elementos de um subconjunto de $\mathbb{N}_1$ da forma

$$\{1, 2, 3, \ldots, n\}$$

para algum $n \in \mathbb{N}_1$. Então $\mathbf{card}(A) = n$.

Cardinal da reunião de conjuntos. Sejam A e B dois conjuntos finitos com cardinalidade $\mathbf{card}(A)$ e $\mathbf{card}(B)$, respectivamente. Se A e B forem conjuntos disjuntos, isto é, se $A \cap B = \emptyset$, então

$$\mathbf{card}(A \cup B) \;=\; \mathbf{card}(A) + \mathbf{card}(B) \tag{2.22}$$

Esta propriedade pode generalizar-se a um número qualquer finito de parcelas. Assim, se $A_1, A_2, \ldots, A_n$ forem n conjuntos com cardinalidade $\mathbf{card}(A_1)$, $\mathbf{card}(A_2)$, ..., $\mathbf{card}(A_n)$, respectivamente, então, se eles forem disjuntos dois a dois, isto é, se se tiver $A_i \cap A_j = \emptyset$ para todo o $i, j = 1, 2, \ldots, n$ tais que $i \neq j$, ter-se-á

$$\mathbf{card}\left(\bigcup_{j=1}^{n} A_j\right) \;=\; \sum_{j=1}^{n} \mathbf{card}(A_j)$$

A fórmula (2.22) é válida sob a condição de A e B terem intersecção vazia, ou seja, sob a condição de ser $A \cap B = \emptyset$. Porém, se tal hipótese não se verificar, a fórmula deixa de ser válida. Visto que $A \cap B$ está contido tanto em A como em B, se se aplicasse a fórmula (2.22) sem qualquer correcção estar-se-ia a considerar os elementos de $A \cap B$ duas vezes. Assim, a fórmula correcta, neste caso, é a seguinte

$$\mathbf{card}(A \cup B) \;=\; \mathbf{card}(A) + \mathbf{card}(B) - \mathbf{card}(A \cap B) \tag{2.23}$$

Exemplo 2.22 *Numa turma de cálculo há 25 estudantes e numa turma de estatística há 31 estudantes. De todos estes estudantes há 13 que frequentam simultaneamente as duas disciplinas. Qual é o número total de estudantes distintos que há nas duas turmas?*

Seja C o conjunto dos alunos da turma de cálculo e E o conjunto dos alunos de estatística. Então o número que se pretende saber é dado por $\mathbf{card}(C \cup E)$. Como $\mathbf{card}(C \cap E) = 13$, tem-se

$$\begin{aligned} \mathbf{card}(C \cup E) &= \mathbf{card}(C) + \mathbf{card}(E) - \mathbf{card}(C \cap E) \\ &= 25 + 31 - 13 \;=\; 43 \end{aligned}$$

Há, portanto, ao todo, 43 estudantes distintos a frequentar as duas disciplinas.

Considerem-se agora três conjuntos finitos arbitrários A, B e C. Aplicando (2.23), sucessivamente,

$$\begin{aligned} \mathbf{card}(A \cup B \cup C) &= \mathbf{card}[(A \cup B) \cup C] \\ &= \mathbf{card}(A \cup B) + \mathbf{card}(C) - \mathbf{card}((A \cup B) \cap C) \\ &= \mathbf{card}(A) + \mathbf{card}(B) - \mathbf{card}(A \cap B) + \mathbf{card}(C) - \\ &\quad \mathbf{card}((A \cup B) \cap C) \end{aligned}$$

Como

$$(A \cup B) \cap C \;=\; (A \cap C) \cup (B \cap C)$$

então

$$\begin{aligned} \mathbf{card}[(A \cup B) \cap C] &= \mathbf{card}[(A \cap C) \cup (B \cap C)] \\ &= \mathbf{card}(A \cap C) + \mathbf{card}(B \cap C) - \\ &\quad \mathbf{card}[(A \cap C) \cap (B \cap C)] \\ &= \mathbf{card}(A \cap C) + \mathbf{card}(B \cap C) - \mathbf{card}(A \cap B \cap C) \end{aligned}$$

Substituindo na fórmula anterior obtém-se finalmente

$$\begin{aligned} \mathbf{card}(A \cup B \cup C) &= \mathbf{card}(A) + \mathbf{card}(B) + \mathbf{card}(C) - \\ &\quad \mathbf{card}(A \cap B) - \mathbf{card}(A \cap C) - \mathbf{card}(B \cap C) + \\ &\quad \mathbf{card}(A \cap B \cap C) \end{aligned}$$

No caso geral de n conjuntos finitos $A_1, A_2, \ldots, A_n$ quaisquer, chega-se à fórmula

$$\mathbf{card}\left(\bigcup_{j=1}^{n} A_j\right) \;=\; \sum_{j=1}^{n} \mathbf{card}(A_j) -$$

$$\sum_{1\leq i<j\leq n} \mathbf{card}(A_i \cap A_j) + \sum_{1\leq i<j<k\leq n} \mathbf{card}(A_i \cap A_j \cap A_k) -$$
$$\cdots + (-1)^{n-1}\mathbf{card}(A_1 \cap A_2 \cap \cdots \cap A_n)$$

que pode demonstrar-se pelo método de indução finita.

Cardinal do produto cartesiano de conjuntos. Suponha-se que numa sala de baile se encontram 4 rapazes que se designam por a_1, a_2, a_3, a_4 e 5 raparigas que se designam por b_1, b_2, b_3, b_4, b_5. Seja

$$\begin{aligned} A &= \{a_1, a_2, a_3, a_4\} \\ B &= \{b_1, b_2, b_3, b_4, b_5\} \end{aligned}$$

Quantos pares diferentes se podem formar, ao todo, sendo cada par constituído por um rapaz e uma rapariga? Este número é, naturalmente, o cardinal do produto cartesiano $A \times B$, ou seja

$$\mathbf{card}(A \times B)$$

Cada rapaz pode figurar em 5 pares diferentes visto haver 5 raparigas; como há quatro rapazes então podem formar-se ao todo 4×5 pares diferentes. Assim,

$$\mathbf{card}(A \times B) \;=\; 20$$

Sejam agora A e B dois conjuntos finitos quaisquer, não vazios, e seja $\mathbf{card}(A) = m$ e $\mathbf{card}(B) = n$. Como B tem n elementos, cada elemento de A dá origem exactamente a n pares diferentes de $A \times B$. Portanto, como A tem m elementos, será $m \cdot n$ o número de elementos de $A \times B$.

Se um, pelo menos, dos conjuntos A, B é vazio, é claro que nenhum par ordenado pode ser formado e, assim, $A \times B$ é também vazio. Por conseguinte, quaisquer que sejam os conjuntos finitos A e B, tem-se sempre:

$$\mathbf{card}(A \times B) \;=\; \mathbf{card}(A) \cdot \mathbf{card}(B)$$

Esta fórmula generaliza-se imediatamente ao caso de produtos cartesianos de 3 conjuntos A, B e C

$$\begin{aligned} \mathbf{card}(A \times B \times C) &= \mathbf{card}[(A \times B) \times C] \\ &= \mathbf{card}(A \times B) \cdot \mathbf{card}(C) \\ &= [\mathbf{card}(A) \cdot \mathbf{card}(B)] \cdot \mathbf{card}(C) \\ &= \mathbf{card}(A) \cdot \mathbf{card}(B) \cdot \mathbf{card}(C) \end{aligned}$$

e, de um modo mais geral, se $A_1, A_2, \ldots, A_n$ forem n conjuntos finitos,

$$\mathbf{card}(A_1 \times A_2 \times \cdots \times A_n) \;=\; \mathbf{card}(A_1) \cdot \mathbf{card}(A_2) \cdots \mathbf{card}(A_n)$$

resultado este que é facilmente provado por indução finita.

Se, em particular, os n conjuntos $A_1, A_2, \ldots, A_n$ forem todos iguais ao conjunto A, obter-se-á

$$\mathbf{card}\,(A^n) \;=\; \mathbf{card}(A)^n$$

Exemplo 2.23 *Quantas multiplicações e quantas adições são executadas para multiplicar duas matrizes quadradas de ordem n?*
Resolução. Recorde-se que se

$$A = [a_{ij}]_{1 \leq i,j \leq n} \quad \text{e} \quad B = [b_{ij}]_{1 \leq i,j \leq n}$$

forem duas matrizes quadradas de ordem n, então a matriz produto

$$C \;=\; AB \;=\; [c_{ij}]_{1 \leq i,j \leq n}$$

é definida, para cada i e cada j, por

$$c_{ij} \;=\; \sum_{k=1}^{n} a_{ik} b_{kj}$$

Esta fórmula envolve n produtos $a_{ik}b_{kj}$ e $(n-1)$ adições (note-se que para somar 2 números se executa uma adição, para somar 3 números se executam duas adições, etc.). Como C possui n^2 elementos então o cálculo de C envolve n^3 multiplicações e $n^2(n-1)$ adições.

Exemplo 2.24 *Um cofre tem três discos, cada um com as mesmas 24 letras e só pode ser aberto quando se coloca uma determinada letra de cada um dos discos numa determinada posição. Supondo que se ignora o segredo do cofre, de quantas maneiras diferentes se podem colocar as letras dos discos nas referidas posições?*
Resolução. As maneiras diferentes de colocar as letras são dadas por todas as sequências de 3 letras escolhidas no conjunto das 24 letras disponíveis. Seja A o conjunto de todas as letras; então

$$A^3 \;=\; \{(a,b,c) : a,b,c \in A\}$$

é o conjunto de todas as sequências possíveis e, portanto, o número pretendido será

$$\mathbf{card}(A^3) \;=\; \mathbf{card}(A)^3 \;=\; 24^3 \;=\; 138\,247$$

Exemplo 2.25 *Quantos números diferentes de 5 algarismos se podem representar com os algarismos 1, 3, 9 no sistema decimal?*
Resolução. Os referidos números tais como 11391, 31933, etc. correspondem a todas as sequências de 5 algarismos escolhidos de 1, 3, 9. Estas sequências são

$$\{1,3,9\}^5 \;=\; \{(a,b,c,d,e) : a,b,c,d,e = 1,3,9\}$$

Assim,

$$\mathbf{card}\left(\{1,3,9\}^5\right) \;=\; \mathbf{card}(\{1,3,9\})^5 \;=\; 3^5 \;=\; 243$$

Exemplo 2.26 *Quantos números de 4 algarismos se podem representar com os algarismos 0, 2, 4, 6, 8 no sistema decimal?*
Resolução. O conjunto de todas as sequências de 4 algarismos escolhidos de entre 0, 2, 4, 6, 8 é dado por

$$\{0,2,4,6,8\}^4 \;=\; \{(a,b,c,d) : a,b,c,d = 0,2,4,6,8\}$$

Destas sequências, no entanto, não representam números com 4 algarismos todas as sequências começadas por 0. Ora o conjunto das sequências que começam por 0 corresponde às sequências da forma $(0,x,y,z)$ onde $x,y,z \in \{0,2,4,6,8\}$, ou seja, ao conjunto

$$\{0,2,4,6,8\}^3 \;=\; \{(x,y,z) : x,y,z = 0,2,4,6,8\}$$

Consequentemente, o número pedido é dado por

$$\mathbf{card}\left(\{0,2,4,6,8\}^4\right) - \mathbf{card}\left(\{0,2,4,6,8\}^3\right) \;=\; 5^4 - 5^3 \;=\; 625 - 125 \;=\; 500$$

A resolução deste problema pode ser pensada de modo um pouco diferente: seja A o conjunto $\{2,4,6,8\}$ e B o conjunto $\{0,2,4,6,8\}$. Então os números pedidos correspondem às sequências do produto cartesiano

$$A \times B^3 \;=\; \{(a,b,c,d) : a \in A \wedge b,c,d \in B\}$$

e, portanto, o número pedido é dado por

$$\mathbf{card}(A \times B^3) \;=\; \mathbf{card}(A) \cdot \mathbf{card}(B)^3 \;=\; 4 \cdot 5^3 \;=\; 500$$

Número de subconjuntos de um conjunto finito. Sendo A um conjunto qualquer, o conjunto

$$\mathcal{P}(A) \;=\; \{X : X \subseteq A\}$$

é, como se sabe, o conjunto das partes de A. Entre os conjuntos pertencentes a $\mathcal{P}(A)$ figuram o conjunto vazio e o próprio conjunto A.

Sendo A finito, a contagem dos elementos de $\mathcal{P}(A)$ pode fazer-se de maneira simples, aplicando a teoria do produto cartesiano. Com efeito, se

for $\mathbf{card}(A) = n$ podem dispor-se os elementos de A numa sequência de n elementos distintos

$$a_1 \;\; a_2 \;\; \cdots \;\; a_n$$

Nestas condições, todo o subconjunto X de A pode ser definido fazendo corresponder a cada elemento a_i o número 1 ou o número 0, conforme $a_i \in X$ ou $a_i \notin X$, respectivamente. Assim, cada subconjunto X de A fica representado por uma sequência de n elementos do conjunto $\{0, 1\}$. Se, por exemplo, for $n = 4$, as sequências

$$0110, \quad 1001, \quad 1111, \quad 0000$$

representam, respectivamente, os conjuntos

$$\{a_2, a_3\}, \quad \{a_1, a_4\}, \quad \{a_1, a_2, a_3, a_4\}, \quad \{\ \}$$

No caso geral é evidente que, por este processo, fica estabelecida uma correspondência bijectiva entre os subconjuntos de A e as sequências de n elementos do conjunto $\{0, 1\}$, isto é, entre $\mathcal{P}(A)$ e $\{0, 1\}^n$. Assim, para todo o conjunto finito A, ter-se-á

$$\mathbf{card}\left(\mathcal{P}(A)\right) \;=\; \mathbf{card}\left(\{0,1\}^{\mathbf{card}(A)}\right) \;=\; 2^{\mathbf{card}(A)}$$

Por este facto, muitos autores denotam o conjunto $\mathcal{P}(A)$ por 2^A.

Exemplo 2.27 *Calcular o número total de relações binárias que se podem definir num conjunto A com n elementos.*
Resolução. Visto que uma relação binária definida em A é um subconjunto do produto cartesiano de A por A, então o número procurado é dado por

$$\mathbf{card}\left(\mathcal{P}(A^2)\right) \;=\; 2^{\mathbf{card}(A^2)} \;=\; 2^{\mathbf{card}(A)^2} \;=\; 2^{n^2}$$

Exercícios 2.3.1

1. *O número de código da segurança social de uma pessoa é uma sequência de 9 dígitos (não necessariamente distintos). Sendo $\mathbf{X}$ o conjunto de todos os possíveis números de código de segurança social, determinar o número de elementos de $\mathbf{X}$.*
2. *Chama-se número binário a uma sequência de 0's ou 1's. Um número binário com 8 dígitos designa-se por "byte".*
   (a) *Quantos "bytes" existem?*
   (b) *Determinar o número de "bytes" que começam por 10 e terminam por 01.*

(c) *Determinar o número de "bytes" que começam por 10 e não terminam em 01.*

(d) *Determinar o número de "bytes" que começam por 10 ou terminam por 01.*

3. *Numa sala há n casais. Determinar o número de escolhas possíveis de pares constituídos por uma mulher e um homen que não seja seu marido.*

4. *Seja* $\mathbf{X}$ *o cojunto de todos os polinómios de grau 4 na indeterminada t cujos coeficientes são números inteiros não negativos de um só dígito. Determinar a cardinalidade de* $\mathbf{X}$*.*

5. *O nome de uma variável na linguagem de programação FORTRAN é uma sequência que tem no máximo seis caracteres dos quais o primeiro é obrigatoriamente uma letra do alfabeto e os restantes, se existirem, são letras ou dígitos. Determinar o número de nomes distintos para variáveis nesta linguagem.*

2.3.1 Arranjos, permutações e combinações

Arranjos. Considere-se o seguinte problema:

> Com panos de 5 cores – amarelo, verde, azul, vermelho e branco – quantas bandeiras tricolores se podem obter, supondo que os panos são colocados só em tiras verticais?

Deste enunciado, duas bandeiras só podem diferir, ou pelas cores que as formam, ou pela ordem em que estão dispostas as cores a partir da haste da bandeira. Assim, se se designarem as 5 cores pelas letras a, b, c, d, e, respectivamente, cada bandeira será representada por 3 destas letras, escritas segundo a ordem das cores, por exemplo

$$abc \quad bca \quad abd \quad dab \quad cde \quad etc.$$

As bandeiras tricolores a que se refere o enunciado são, assim, representadas pelos diferentes conjuntos ordenados de 3 cores, que é possível formar a partir das 5 cores consideradas. A esses conjuntos ordenados dá-se o nome de arranjos das 5 cores 3 a 3.

De um modo geral:

Definição 2.28 *Dados m elementos quaisquer, chamam-se* **arranjos** *dos m elementos p a p a todos os conjuntos ordenados que é possível obter com p elementos escolhidos arbitrariamente entre os m dados.*

O número de todos os possíveis arranjos de m elementos p a p é designado pela notação

$$A_p^m$$

Deduzir-se-á agora uma fórmula que permite calcular o número A_p^m para m e p conhecidos. Não faz sentido considerar arranjos de m objectos tomados p a p se p for maior que m: assim o número de tais arranjos é sempre igual a zero.

Considere-se, para começar, o seguinte caso particular:

> Com as letras a, b, c, d quantos arranjos de duas letras diferentes se podem formar?

Os arranjos com uma só letra são evidentemente os seguintes

$$a, \qquad b, \qquad c, \qquad d,$$

em número de 4. Pode então escrever-se

$$A_1^4 \;=\; 4$$

Os arranjos com duas letras formam-se agora à custa dos anteriores, colocando, à direita de cada arranjo formado por uma só letra, cada uma das letras dadas que ainda não figuram nele. Assim, o arranjo a dá origem aos arranjos

$$ab, \qquad ac, \qquad ad,$$

e não há mais arranjos com duas letras começadas por a. Procedendo analogamente com os restantes obtém-se o seguinte quadro

ab	ba	ca	da
ac	bc	cb	db
ad	bd	cd	dc

Assim, cada arranjo com um elemento dá origem a 3 arranjos com dois elementos, podendo, portanto, escrever-se

$$A_2^4 \;=\; 4 \cdot 3 \;=\; 12$$

Considere-se agora o caso seguinte:

> Determinar o número total de arranjos de três letras escolhidas entre as letras a, b, c, d.

Trata-se de arranjos de 4 elementos, tomados 3 a 3. Para formar estes arranjos pode partir-se dos arranjos já formados de 4 tomados 2 a 2, acrescentando à direita de cada um dos arranjos já formados cada uma das letras que ainda não figuram nele. Assim, do arranjo ab resultam os arranjos

$$abc, \qquad abd,$$

E não há mais arranjos que contenham, nos dois primeiros lugares, as letras ab, por esta ordem. Procedendo analogamente com os restantes arranjos, obtém-se

abc	adb	bca	cab	cda	dba
abd	adc	bcd	cad	cdb	dbc
acb	bac	bda	cba	dab	dca
acd	bad	bdc	cbd	dac	dcb

que é o conjunto de todos os possíveis arranjos de 4 elementos tomados 3 a 3. Pelo esquema de construção realizado obtém-se então

$$A_3^4 \;=\; 4 \cdot 3 \cdot 2 \;=\; 24$$

ou seja, há 24 arranjos de quatro elementos tomados 3 a 3.

Os dois casos particulares anteriores ajudam a resolver o caso geral:

> Determinar o número de arranjos de m objectos tomados p a p (com $p \leq m$).

Para a determinação deste número observe-se que os arranjos de m elementos tomados p a p se podem obter a partir dos arranjos dos mesmos m elementos tomados $p-1$ a $p-1$, juntando à direita de cada um deles uma das letras que ainda ali não figuram. Efectuam-se, então, sucessivamente, as operações:

1. formar os arranjos de m elementos tomados $p-1$ a $p-1$. O número de resultados diferentes é representado por A_{p-1}^m;
2. colocar, à direita de cada um dos arranjos anteriores, um dos elementos que ainda não figuram nele. O número de modos diferentes de efectuar esta operação, em cada caso, é igual a $m-(p-1) = m-p+1$, visto já terem sido, em cada arranjo anterior, utilizados $p-1$ elementos e não figurarem ainda nele $m-p+1$ elementos.

Daqui conclui-se que

$$A_p^m \;=\; A_{p-1}^m \cdot (m-p+1) \quad \text{para } \; p>1 \tag{2.24}$$

Esta é uma fórmula de recorrência que permite calcular A_p^m a partir do valor de A_{p-1}^m. Ora, qualquer que seja $m \neq 0$,

$$A_1^m \;=\; m$$

e, portanto, aplicando a fórmula (2.24) sucessivamente, vem para $p>1$

$$\begin{array}{rcl} A_1^m & = & m \\ A_2^m & = & A_1^m \cdot (m-2+1) \;=\; m(m-1) \\ A_3^m & = & A_2^m \cdot (m-3+1) \;=\; m(m-1)(m-2) \\ & \vdots & \\ A_p^m & = & A_{p-1}^m \cdot (m-p+1) \;=\; m(m-1)(m-2)\cdots(m-p+1) \end{array}$$

Assim,

> O número total de arranjos de m elementos p a p é igual ao produto dos p números inteiros consecutivos por ordem decrescente a partir de m.

Permutações. No caso particular em que se tem $p=m$ obtém-se

$$A_m^m$$

que é o número de arranjos nos quais entram todos os objectos dados. Neste caso aos arranjos de m objectos tomados m a m dá-se o nome de permutações. Denotando o número de permutações de m objectos por P_m, vem

$$P_m \;=\; A_m^m$$

Para $m=1$ vem $P_1 = A_1^1 = 1$ e, para $m>1$ qualquer,

$$P_m \;=\; A_m^m \;=\; m\cdot(m-1)\cdot(m-2)\cdots 2\cdot 1$$

ou seja, o número total de permutações de m elementos é igual ao produto dos primeiros m números naturais $1,2,\ldots,m$. Este produto é, como se sabe, o factorial de m e representa-se por $m!$. Então,

$$P_m \;=\; m!$$

Esta fórmula é válida para $m \geq 0$ fazendo-se, por convenção, $0! = 1$.

Usando a notação de factorial de um número inteiro não negativo pode dar-se à fórmula de A_p^m uma outra expressão que é a seguinte:

$$\begin{aligned} A_p^m &= m(m-1)\cdots(m-p+1) \\ &= \frac{m(m-1)\cdots(m-p+1)(m-p)(m-p-1)\cdots 2\cdot 1}{(m-p)(m-p-1)\cdots 2\cdot 1} \\ &= \frac{m!}{(m-p)!} \end{aligned}$$

Com a convenção de ser $0! = 1$, esta fórmula mantém-se válida para $p = m$, obtendo-se então

$$P_m \;=\; A_m^m \;=\; \frac{m!}{(m-m)!} \;=\; \frac{m!}{0!} \;=\; m!$$

Combinações. Considere-se o seguinte exemplo:

> Um aluno deseja comprar 4 livros diferentes, mas de igual custo, e só tem dinheiro para comprar 3 desses livros. De quantos modos pode o aluno fazer a escolha de 3 livros de entre os 4 que deseja?

Representando os livros pelas letras a, b, c, d a escolha que consiste em comprar os livros

$$a, b, c$$

é diferente daquela que consiste em comprar os livros

$$a, b, d$$

Mas já a escolha a, b, c não é distinta, neste caso, da escolha b, a, c que se refere aos mesmos livros, mas colocados por ordem diferente.

É fácil ver então que o aluno pode fazer a sua escolha de quatro modos diferentes

$$abc, \quad abd, \quad acd, \quad bcd$$

sem que tenha qualquer interesse a ordem pela qual são indicados os elementos. Por conseguinte, os modos de escolher 3 livros entre os 4, correspondem afinal aos diferentes conjuntos que se podem formar com 3 livros tomados

entre os 4, sem que interesse a ordem pela qual são considerados. Tais conjuntos (como simples conjuntos) só podem diferir entre si pelos elementos de que são formados: dá-se-lhes o nome de **combinações** dos 4 livros 3 a 3.

Mais geralmente,

Definição 2.29 *Dados m elementos quaisquer, chamam-se* **combinações** *desses m elementos p a p a todos os conjuntos que é possível obter com p elementos escolhidos entre os m dados (sem atender a qualquer ordem).*

Uma vez que se trata de simples conjuntos e não de sequências ordenadas, duas combinações serão distintas quando, e só quando, existir pelo menos um elemento de uma que não seja elemento da outra.

O número de todas as possíveis combinações de m elementos p a p é designado por

$$C_p^m \quad \text{ou} \quad \binom{m}{p}$$

É imediato concluir que

$$\binom{m}{p} = 0 \quad \text{quando} \quad p > m$$

isto é, com m elementos não é possível formar nenhuma combinação que tenha mais que m elementos. Se for $p = m$, isto é, se todos os elementos são tomados de uma só vez, é claro que só é possível formar uma combinação que é o conjunto de todos esses elementos. tem-se pois

$$\binom{m}{m} = 1$$

Assim, qualquer que seja o número natural $p \leq m$, as combinações dos m elementos p a p serão conjuntos contidos no conjunto total. O caso oposto ao de tomar todos os elementos ($p = m$) será o de não tomar nenhum ($p = 0$). Por comodidade de linguagem, convenciona-se dizer neste caso que o número de elementos da combinação é 0. E como há só uma hipótese possível, escreve-se

$$\binom{m}{0} = 1$$

Da definição dada para as combinações de m elementos tomados p a p pode dizer-se que o número de arranjos de m elementos tomados p a p se

pode obter permutando em cada uma das combinações de m p a p os p elementos que a formam, de todas as maneiras possíveis. Isto quer dizer que os arranjos referidos se podem obter mediante as duas operações seguintes

1. formar as combinações de m elementos p a p. O número de tais combinações distintas é C_p^m;
2. permutar, em cada uma das combinações, os seus p elementos, de todas as formas possíveis. esta operação pode realizar-se de P_p maneiras diferentes.

Deste modo, tem-se

$$A_p^m \;=\; C_p^m \cdot P_p$$

e, portanto,

$$C_p^m \;\equiv\; \binom{m}{p} \;=\; \frac{A_p^m}{P_p}$$

ou, substituindo A_p^m e P_p pelas suas expressões, vem

$$\binom{m}{p} \;=\; \frac{m(m-1)\cdots(m-p+1)}{p!} \;=\; \frac{m!}{p!(m-p)!} \tag{2.25}$$

Esta fórmula é válida mesmo nos casos extremos em que se tem $p = m$ ou $p = 0$.

Da expressão (2.25) resulta imediatamente a seguinte identidade

$$\binom{m}{p} \;=\; \binom{m}{m-p}$$

qualquer que seja $p \leq m$.

Exercícios 2.3.2

1. *Um código é constituído por seis símbolos: três letras (L) do alfabeto (de 26 letras) seguidas de três dígitos (D). Seja* $\mathbf{X}$ *o conjunto de todos os códigos possíveis (LLLDDD). Determinar o número de elementos de* $\mathbf{X}$ *nas seguintes condições:*
   (a) *tanto as letras como os dígitos podem ser repetidos;*
   (b) *os dígitos não podem ser repetidos;*
   (c) *as letras não podem ser repetidas;*
   (d) *nem as letras nem os dígitos podem ser repetidos;*

2. *Repita o problema anterior, supondo que, todos os códigos do conjunto* $\mathbf{X}$ *contêm as três letras e os seis dígitos dispostos de forma alternada (LDLDLD ou DLDLDL).*

3. *Determinar o número de números pares compreendidos entre 0 e 100. Determinar o número de números pares compreendidos entre 0 e 100 com dígitos distintos.*

4. (a) *Quantos números de três algarismos diferentes se podem formar com os algarismos 1, 2, 3, 4, 5 e 6?*
   (b) *Dos números de três algarismos diferentes formados nas condições da alínea anterior, quantos são os que têm o algarismo 1 no primeiro lugar (centenas)?*

5. *Com os algarismos 1, 2, 4, 6 e 8 quantos números ímpares de quatro algarismos diferentes se podem formar? E quantos números ímpares de quatro algarismos se podem formar?*

6. *Com os algarismos 0, 1, 2, 5 e 8:*
   (a) *Quantos números de quatro algarismos diferentes se podem escrever?*
   (b) *Dentre esses quantos são múltiplos de 5?*
   (c) *E quantos contêm o algarismo 2?*

7. *Quantos números menores que 2000 formados por algarismos diferentes se podem escrever com os algarismos 1, 2, 3 e 4?*

8. *Determinar o valor inteiro positivo de* n *tal que*
   (a) $A_2^n = 30$
   (b) $10 \cdot A_2^n = A_2^{3n-1} + 40$

9. *Mostrar que* $A_{r+1}^n = (n-r) \cdot A_r^n$ *e usar depois este resultado para determinar o valor de* n *tal que* $A_9^n = 15 \cdot A_8^n$.

10. *Determinar o valor de* k *de tal forma que se tenha* $A_r^{n+1} = k \cdot A_r^n$. *Usar este resultado para determinar* n *e* r *se for* $k = 5$, $n > r$ r *r for tão pequeno quanto possível.*

11. *Seja* $\mathbf{X}$ *um conjunto com 9 elementos. Determinar*
   (a) *o número total de subconjuntos de* $\mathbf{X}$,
   (b) *o número de sunbconjuntos de* $\mathbf{X}$ *de cardinalidade 3,*
   (c) *o número de pares não ordenados de elementos de* $\mathbf{X}$.

12. *Num departamento trabalham 4 mulheres e 9 homens. Determinar:*
   (a) *o número de comissões com 2 mulheres e 3 homens que se podem formar;*
   (b) *o número de comissões de 5 elementos com, pelo menos, 2 mulheres e 2 homens.*

13. *De quantos modos diferentes é possível dispor numa fila, para fotografia, 3 homens e duas mulheres, se:*

(a) *Os homens e as mulheres puderem ocupar indistintamente qualquer lugar?*

(b) *Se um dos homens, o mais alto, por exemplo, ficar no meio, e todos os restantes indistintamente em qualquer lugar?*

(c) *Se ficarem alternadamente homens e mulheres, nunca dois homens seguidos ou duas mulheres seguidas?*

14. *Com os factores primos 2, 3, 5, 7 e 11 quantos produtos diferentes de três factores se podem formar?*

15. *Numa corrida de automóveis, na qual tomavam parte 10 corredores, verificou-se que, em cada volta, passaram junto das tribunas, ao mesmo tempo, dois concorrentes, e que estes pares, sempre diferentes de volta para volta, foram todos quantos se podiam formar nestas condições com os 10 concorrentes. De quantas voltas constava o percurso?*

16. *Determinar o número de formas distintas de sentar r pessoas retiradas de um grupo de n numa mesa redonda.*

17. *Determinar o número de formas distintas de sentar 17 pessoas 8 das quais numa mesa redonda e as restantes 6 num banco corrido.*

2.3.2 O binómio de Newton

Os números C_k^n de combinações de n elementos tomados k a k aparecem na fórmula do binómio de Newton, razão pela qual são muitas vezes designados por **coeficientes binomiais**.

Teorema 2.30 (Fórmula de Pascal) *Se n e k forem dois números inteiros tais que $1 \leq k \leq n-1$, então*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Este resultado pode obter-se por simples aplicação das regras usuais da álgebra. Assim,

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-k+1)!} \\
&= \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= \frac{(n-1)!(n-k) + k(n-1)!}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} = \binom{n}{k}
\end{aligned}$$

Usando agora esta fórmula

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

conjuntamente com a informação

$$\binom{n}{0} = \binom{n}{n} = 1$$

podem calcular-se os coeficientes binomiais através do chamado **triângulo de Pascal** cujo aspecto se apresenta a seguir

$$\begin{array}{lccccccccc}
n=0 & & & & & 1 & & & & \\
1 & & & & 1 & & 1 & & & \\
2 & & & 1 & & 2 & & 1 & & \\
3 & & 1 & & 3 & & 3 & & 1 & \\
4 & 1 & & 4 & & 6 & & 4 & & 1 \\
\vdots & & & & & & & & &
\end{array}$$

Cada elemento do triângulo, excepto os 1's laterais, é igual à soma dos dois elementos que pertencem à linha anterior e que estão de cada um dos lados do elemento a calcular.

Se em cada linha do triângulo de Pascal se somarem todos os elementos obtém-se a fórmula

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

a qual será demonstrada mais à frente.

A fórmula do binómio de Newton. Para deduzir a fórmula do binḿio de Newton considere-se o seguinte quadro

$$\begin{aligned}
(1+x)^0 &= 1 \\
(1+x)^1 &= 1+x \\
(1+x)^2 &= 1+2x+x^2 \\
(1+x)^3 &= 1+3x+3x^2+x^3 \\
&\vdots
\end{aligned}$$

onde os coeficientes dos desenvolvimentos das diversas potências de $1+x$ são precisamente os números que figuram nas correspondentes linhas do triângulo de Pascal. Pode então conjecturar-se que para todo o n se tem

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{r}x^r + \cdots + \binom{n}{n}x^n \quad (2.26)$$

qualquer que seja o valor de x. Para confirmar esta conjectura far-se-á a prova usando o método de indução.

De facto, designando por $p(n)$ a fórmula (2.26), vem

1. $p(1)$ é verdadeira pois que

$$(1+x)^1 = 1+x = \binom{1}{0} + \binom{1}{1}x$$

2. Suponha-se, hipótese de indução, que a fórmula é válida para um dado número inteiro não negativo k, isto é, que se tem a igualdade

$$(1+x)^k = \binom{k}{0} + \binom{k}{1}x + \binom{k}{2}x^2 + \cdots + \binom{k}{k}x^k$$

Multiplicando ambos os membros por $1+x$, obtém-se

$$\begin{aligned}
(1+x)^{k+1} &= \left\{\binom{k}{0} + \binom{k}{1}x + \binom{k}{2}x^2 + \cdots + \binom{k}{k}x^k\right\}(1+x) \\
&= \binom{k}{0} + \binom{k}{1}x + \binom{k}{2}x^2 + \cdots + \binom{k}{k}x^k + \\
&\quad \binom{k}{0}x + \binom{k}{1}x^2 + \binom{k}{2}x^3 + \cdots + \binom{k}{k}x^{k+1} \\
&= \binom{k}{0} + \left\{\binom{k}{0} + \binom{k}{1}\right\}x + \left\{\binom{k}{1} + \binom{k}{2}\right\}x^2 + \\
&\quad \cdots + \left\{\binom{k}{k-1} + \binom{k}{k}\right\}x^k \cdots + \binom{k}{k}x^{k+1}
\end{aligned}$$

Tendo em consideração a fórmula de Pascal, vem

$$(1+x)^{k+1} = \binom{k}{0} + \binom{k+1}{1}x + \binom{k+1}{2}x^2 + \cdots + \binom{k+1}{k}x^k + \binom{k}{k}x^{k+1}$$

e como

$$\binom{k}{0} = \binom{k+1}{0} = 1 \text{ e } \binom{k}{k} = \binom{k+1}{k+1} = 1$$

pode finalmente escrever-se

$$\begin{aligned}(1+x)^{k+1} &= \binom{k+1}{0} + \binom{k+1}{1}x + \binom{k+1}{2}x^2 + \\ &\quad \cdots + \binom{k+1}{k}x^k + \binom{k+1}{k+1}x^{k+1}\end{aligned}$$

o que mostra a veracidade da proposição

$$\forall_{k\in\mathbb{N}_1}\ [p(k) \Rightarrow p(k+1)]$$

Tendo em conta o princípio de indução finita fica demonstrada a fórmula do binómio de Newton para $n \in \mathbb{N}_1$ qualquer.

A fórmula (2.26) pode generalizar-se. O desenvolvimento de $(x+y)^n$ pode obter-se a partir do desenvolvimento anterior, tendo em atenção que, sendo $x \neq 0$, é

$$(x+y)^n = x^n\left(1+\frac{y}{x}\right)^n$$

Como

$$\left(1+\frac{y}{x}\right)^n = \binom{n}{0} + \binom{n}{1}\left(\frac{y}{x}\right) + \binom{n}{2}\left(\frac{y}{x}\right)^2 + \cdots + \binom{n}{n}\left(\frac{y}{x}\right)^n$$

então multiplicando ambos os membros desta igualdade por x^n vem

$$\begin{aligned}x^n\left(1+\frac{y}{x}\right)^n &= (x+y)^n \\ &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \\ &\quad \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + \binom{n}{n}y^n \qquad (2.27)\end{aligned}$$

Usando a notação de somatório a fórmula (2.27) pode tomar a forma

$$(x+y)^n = \sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j \qquad (2.28)$$

Substituindo em (2.28) y por $-y$ vem

$$(x-y)^n \;=\; \sum_{j=0}^{n} \binom{n}{j} (-1)^j x^{n-j} y^j \tag{2.29}$$

Fazendo na fórmula (2.26) $x = 1$ obtém-se

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \;=\; 2^n$$

que já anteriormente tinha sido referida; por outro lado, fazendo em (2.29) $x = y = 1$ vem

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} \;=\; 0$$

Derivando em ordem a x ambos os membros da igualdade (2.26)

$$n(1+x)^{n-1} \;=\; \binom{n}{1} + 2\binom{n}{2} x + 3\binom{n}{3} x^2 + \cdots + n\binom{n}{n} x^{n-1}$$

pelo que, substituindo x por 1, se obtém a identidade

$$n\, 2^{n-1} \;=\; \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n}$$

Muitas outras identidades entre os coeficientes binomiais se podem obter por processos semelhantes: por exemplo, partindo de

$$(1+x)^n \;=\; \sum_{j=0}^{n} \binom{n}{j} x^j$$

e derivando ambos os membros, vem

$$n(1+x)^{n-1} \;=\; \sum_{j=1}^{n} j \binom{n}{j} x^{j-1}$$

Multiplicando agora ambos os membros por x

$$nx(1+x)^{n-1} \;=\; \sum_{j=1}^{n} j \binom{n}{j} x^j$$

e derivando novamente ambos os membros

$$n(1+x)^{n-1} + n(n-1)(1+x)^{n-2} \;=\; \sum_{j=1}^{n} j^2 \binom{n}{j} x^{j-1}$$

Substituindo x por 1,

$$n(n+1)2^{n-2} \;=\; \sum_{j=1}^{n} j^2 \binom{n}{j}$$

2.3.2.1 O teorema binomial de Newton

Newton (1642-1727) generalizou a fórmula do binómio obtendo uma expressão para $(x+y)^\alpha$ onde α é um número real qualquer. Para valores de α que não sejam inteiros e positivos, no entanto, o desenvolvimento transforma-se numa série infinita relativamente à qual se põem questões de convergência. Limitar-nos-emos a estabelecer aqui o teorema deixando a sua demonstração para os textos de Análise Matemática.

Teorema 2.31 *Seja α um número real qualquer. Então para todo o x, y tais que $|x/y| < 1$*

$$(x+y)^\alpha \;=\; \sum_{j=0}^{\infty} \binom{\alpha}{j} x^j y^{\alpha-j}$$

onde

$$\binom{\alpha}{j} \;=\; \frac{\alpha(\alpha-1)\cdots(\alpha-j+1)}{j!}$$

- Se α for um inteiro positivo n, então visto que para $j > n$ se tem $C_j^n = 0$, o desenvolvimento acima indicado reduz-se a

  $$(x+y)^n \;=\; \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}$$

  que é a fórmula do binómio de Newton já antes considerada.

- Fazendo $z = x/y$ então $(x+y)^\alpha = y^\alpha(z+1)^\alpha$ e, portanto, para $|z| < 1$, vem

  $$(1+z)^\alpha \;=\; \sum_{j=0}^{\infty} \binom{\alpha}{j} z^j$$

Se n for um inteiro positivo e $\alpha = -n$, então

$$\begin{aligned}\binom{\alpha}{j} = \binom{-n}{j} &= \frac{-n(-n-1)\cdots(-n-j+1)}{j!} \\ &= (-1)^j \frac{n(n+1)\cdots(n+j-1)}{j!} = (-1)^j \binom{n+j-1}{j}\end{aligned}$$

e, portanto, para $|z| < 1$

$$(1+z)^{-n} = \frac{1}{(1+z)^n} = \sum_{j=0}^{\infty} (-1)^j \binom{n+j-1}{j} z^j$$

Em particular, para $n = 1$

$$\binom{n+j-1}{j} = \binom{j}{j} = 1$$

e, portanto,

$$\frac{1}{(1+z)} = \sum_{j=0}^{\infty} (-1)^j z^j, \quad |z| < 1$$

Substituindo z por $-z$ vem

$$\frac{1}{1-z} = \sum_{j=0}^{\infty} z^j, \quad |z| < 1$$

que é a fórmula já conhecida para a soma da série geométrica.

O teorema binomial de Newton pode ser usado para a determinação de raízes quadradas com precisão arbitrariamente escolhida. Tomando $\alpha = 1/2$, então

$$\binom{1/2}{0} = 1$$

enquanto que para $j > 0$

$$\begin{aligned}\binom{1/2}{j} &= \frac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-j+1)}{j!} \\ &= \frac{(-1)^{j-1}}{2^j} \frac{1 \cdot 3 \cdots (2j-3)}{j!}\end{aligned}$$

$$
\begin{aligned}
&= \frac{(-1)^{j-1}}{2^j}\,\frac{1\cdot 2\cdot 3\cdot 4\cdots(2j-3)\cdot(2j-2)}{2\cdot 4\cdots(2j-2)j!}\\
&= \frac{(-1)^{j-1}}{j2^{2j-1}}\,\frac{(2j-2)!}{[(j-1)!]^2}\\
&= \frac{(-1)^{j-1}}{j2^{2j-1}}\binom{2j-2}{j-1}
\end{aligned}
$$

Então, para $|z|<1$

$$
\begin{aligned}
\sqrt{1+z} &= 1+\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j2^{2j-1}}\binom{2j-2}{j-1}z^j\\
&= 1+\frac{1}{2}\,z-\frac{1}{2\cdot 2^3}\binom{2}{1}z^2+\frac{1}{3\cdot 2^5}\binom{4}{2}z^3-\cdots
\end{aligned}
$$

Se, por exemplo, se pretender calcular $\sqrt{20}$, aplicando este desenvolvimento, tem-se

$$
\begin{aligned}
\sqrt{20} &= \sqrt{16+4} \;=\; 4\sqrt{1+0,25}\\
&= 4\left[1+\frac{1}{2}(0,25)-\frac{1}{8}(0,25)^2+\frac{1}{16}(0,25)^3-\cdots\right]\\
&= 4,472\ldots
\end{aligned}
$$

Exercícios 2.3.3

1. *Usando o binómio de Newton mostrar que*

$$3^n \;=\; \sum_{k=0}^{n}\binom{n}{k}2^k$$

Generalizando, determinar a soma

$$\sum_{k=0}^{n}\binom{n}{k}r^k$$

para qualquer número real r.

2. *Provar que*

$$\binom{r}{k} \;=\; \frac{r}{r-k}\binom{r-1}{k}$$

qualquer que seja $r\in\mathbb{R}$ e qualquer que seja o inteiro $k\geq 0$ tal que $r\neq k$.

3. *Provar que para n inteiro positivo* ≥ 2

$$\binom{n}{1} - 2\binom{n}{2} + 3\binom{n}{3} - 4\binom{n}{4} + \cdots + (-1)^{n-1} n\binom{n}{n} \;=\; 0$$

4. *Provar que para n inteiro e positivo*

$$1 + \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} + \frac{1}{4}\binom{n}{3} + \cdots + \frac{1}{n+1}\binom{n}{n} \;=\; \frac{2^{n+1}-1}{n+1}$$

5. *Calcular a soma*

$$1 - \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} - \frac{1}{4}\binom{n}{3} + \cdots + (-1)^n \frac{1}{n+1}\binom{n}{n}$$

6. *Provar que para todo o real r e inteiros não negativos k e m*

$$\binom{r}{m}\binom{m}{k} \;=\; \binom{r}{k}\binom{r-k}{m-k}$$

7. *Provar que*

$$\sum_{k=0}^{n} \binom{m_1}{k}\binom{m_2}{n-k} \;=\; \binom{m_1+m_2}{n}$$

usando a fórmula do binómio e a relação $(1+x)^{m_1}(1+x)^{m_2} = (1+x)^{m_1+m_2}$.

8. *Verificar que:*
   (a) $\frac{1}{2}(1 - i\sqrt{3})$ *é uma das raízes cúbicas de* -1.
   (b) $\frac{\sqrt{2}}{2}(1-i)$ *é uma das raízes quartas de* -1.
9. *Determine o coeficiente de* x^{21} *no desenvolvimento de* $(ax + x^2)^{16}$.
10. *Sendo* $10y^{-2}$ *o quarto termo do desenvolvimento de*

$$\left(\sqrt{y} + \frac{1}{y}\right)^n$$

determine o termo seguinte.

11. *Determine m de modo que o* 3º *e o* 8º *termos do desenvolvimento de*

$$\left(\frac{x}{\sqrt{3x}} - 2\,\frac{1}{\sqrt{x}}\right)^m$$

tenham os coeficientes binomiais iguais, e calcule o produto desses dois termos.

2.3.2.2 O teorema multinomial

Permutações generalizadas. Seja $\mathbf{X}$ uma colecção de n objectos (não necessariamente distintos) pertencentes a k grupos diferentes de tal forma que

1. em cada grupo todos os objectos são idênticos;
2. objectos de grupos distintos são diferentes.

Por exemplo, a colecção de letras

$$a, b, a, b, b, d, e, e, d$$

pode ser decomposta em quatro grupos: um para os a's, um para os b's, um para os d's e um para os e's. Na colecção há 2 a's, 3 b's, 2 d's e 2 e's. Alguns autores designam estes tipos de colecções por *multiconjuntos*.

Mais geralmente, suponha-se que em cada grupo há n_i $(i = 1, 2, \ldots, k)$ objectos, sendo $n = n_1 + n_2 + \cdots + n_k$. Chama-se **permutação generalizada** de $\mathbf{X}$ a cada um dos arranjos em linha da totalidade destes objectos. Denota-se o número de permutações generalizadas de $\mathbf{X}$ por

$$P(n; n_1, n_2, \ldots, n_k)$$

o qual seria igual a $n!$ se todos os objectos fossem distintos, isto é, se se tivesse $k = n$ e, portanto, $n_1 = n_2 = \cdots = n_n = 1$.

Teorema 2.32 *Se a colecção* $\mathbf{X}$ *de* n *objectos for constituída por* k *grupos distintos, cada um dos quais tem* n_i *objectos idênticos* $(i = 1, 2, \ldots, k)$*, então o número de permutações generalizadas de* $\mathbf{X}$ *é dado por*

$$P(n; n_1, n_2, \ldots, n_k) \;=\; \frac{n!}{n_1! n_2! \cdots n_k!}$$

Demonstração: Se os objectos que pertencem ao grupo i, por exemplo, fossem todos distintos então originariam $n_i!$ permutações dos elementos desse grupo. Assim, cada permutação generalizada de $\mathbf{X}$ originaria $n_1! n_2! \cdots n_k!$ permutações (simples) se os objectos de $\mathbf{X}$ fossem todos distintos. Então sendo $P(n; n_1, n_2, \ldots, n_k)$ o número de permutações generalizadas ter-se-á que

$$P(n; n_1, n_2, \ldots, n_k) n_1! n_2! \cdots n_k!$$

é igual ao número de permutações (simples) se os objectos de $\mathbf{X}$ fossem todos distintos, ou seja,

$$P(n; n_1, n_2, \ldots, n_k) n_1! n_2! \cdots n_k! \;=\; n!$$

Consequentemente,

$$P(n; n_1, n_2, \ldots, n_k) \;=\; \frac{n!}{n_1! n_2! \cdots n_k!}$$

como se pretendia mostrar. □

Exemplo 2.33 As 9 letras que aparecem na palavra CONSENSOS dividem-se em 5 grupos: um grupo com 1 C, um grupo com 2 O's, um grupo com 2 N's, um grupo com 3 S's e um grupo com 1 E. O número total de permutações generalizadas que se podem realizar com estas 9 letras é igual a

$$P(9; 1, 2, 2, 3, 1) \;=\; \frac{9!}{1!2!2!3!1!} \;=\; 15\,120$$

Combinações generalizadas. Considere-se agora uma colecção de n objectos (não necessariamente distintos) pertencentes a k grupos (cada um dos quais é constituído por objectos idênticos). Os primeiros n_1 objectos idênticos podem ser colocados em n lugares (de tal forma que em nenhum lugar há mais que um objecto) de

$$\binom{n}{n_1}$$

modos distintos. Então os n_2 objectos do grupo seguinte podem ser colocados nos lugares restantes de

$$\binom{n - n_1}{n_2}$$

modos diferentes. E assim sucessivamente até esgotar todos os k grupos de objectos. Ao todo há então

$$\binom{n}{n_1} \times \binom{n - n_1}{n_2} \times \cdots \times \binom{n - n_1 - \cdots - n_{k-1}}{n_k}$$

modos diferentes de colocar os n objectos nos n lugares disponíveis. Cada um destes modos de arrumar os n objectos é designado por **combinação generalizada** de n objectos repartidos por k grupos de objectos idênticos e o seu número total denota-se por

$$C^n_{n_1, n_2, \ldots, n_k} \;\equiv\; \binom{n}{n_1, n_2, \ldots, n_k}$$

Do raciocínio precedente tem-se então

$$\begin{aligned}\binom{n}{n_1, n_2, \ldots, n_k} &= \binom{n}{n_1} \times \binom{n-n_1}{n_2} \times \cdots \times \binom{n-n_1-\cdots-n_{k-1}}{n_k} \\ &= \frac{n!}{n_1!(n-n_1)!} \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdots \frac{(n-n_1-\cdots n_{k-1})!}{n_k!(n-n_1-n_2-\cdots-n_k)!} \\ &= \frac{n!}{n_1!n_2!\cdots n_k!} = P(n; n_1, n_2, \ldots, n_k)\end{aligned}$$

Teorema 2.34 (Teorema Multinomial.) *Seja n um inteiro positivo. Então quaisquer que sejam os números $x_1, x_2, \ldots, x_k$*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1+\cdots+n_k=n} \binom{n}{n_1, n_2, \ldots, n_k} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$$

onde o somatório se estende a todas as sequências de inteiros não negativos $n_1, n_2, \ldots, n_k$ tais que $n_1 + n_2 + \cdots + n_k = n$.

Demonstração: Suponha-se que se desenvolve o produto

$$(x_1 + x_2 + \cdots + x_k)(x_1 + x_2 + \cdots + x_k) \cdots (x_1 + x_2 + \cdots + x_k) \quad n \text{ factores}$$

até terem desaparecido todos os parentesis. Visto que cada factor tem k parcelas, então no final da operação resultarão k^n termos da forma $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ onde $n_1, n_2, \cdots, n_k$ são inteiros não negativos cuja soma é n, isto é, $n_1+n_2+\cdots+n_k = n$.

O termo $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ obtém-se escolhendo x_1 em n_1 dos n factores, x_2 em n_2 dos $n-n_1$ factores, ... e x_k em n_k dos $n-n_1-\cdots-n_{k-1}$ factores restantes. Então o número de vezes que o termo $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ ocorre é igual a

$$\binom{n}{n_1} \times \binom{n-n_1}{n_2} \times \cdots \times \binom{n-n_1-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}$$

o que comprova o teorema. □

Exemplo 2.35 No desenvolvimento do multinómio

$$(x_1 + x_2 + x_3 + x_4 + x_5)^7$$

o coeficiente do termo $x_1^2 x_3 x_4^3 x_5$ é igual a

$$\binom{7}{2, 0, 1, 3, 1} = \frac{7!}{2!0!1!3!1!} = 420$$

Exemplo 2.36 Desenvolvendo o multinómio

$$(2x_1 - 3x_2 + 5x_3)^6$$

o coeficiente do termo $x_1^3 x_2 x_3^2$ é dado por

$$\binom{6}{3,1,2} 2^3(-3)5^2 \;=\; -36\,000$$

Note-se que a fórmula multinomial se reduz à fórmula do binómio quando $k = 2$. De facto, neste caso, $n_2 = n - n_1$ e, portanto,

$$\begin{aligned}(x_1 + x_2)^n &= \sum_{n_1+n_2=n} \binom{n}{n_1, n_2} x_1^{n_1} x_2^{n_2} \\ &= \sum_{n_1=0}^{n} \binom{n}{n_1, n-n_1} x_1^{n_1} x_2^{n-n_1} \;=\; \sum_{n_1=0}^{n} \binom{n}{n_1} x_1^{n_1} x_2^{n-n_1}\end{aligned}$$

Exercícios 2.3.4

1. *Usando o teorema multinomial, mostrar que para n e k inteiros positivos*

$$k^n \;=\; \sum \binom{n}{n_1, n_2, \ldots, n_k}$$

onde a soma se estende a todas as sequências de inteiros não negativos $n_1, n_2, \ldots, n_k$ tais que $n_1 + n_2 + \cdots + n_k = n$.

2. *Desenvolver*

$$(x_1 + x_2 + x_3)^4$$

usando o teorema multinomial.

3. *Determinar o coeficiente de $x_1^3 x_2 x_3^4 x_5^2$ no desenvolvimento de*

$$(x_1 + x_2 + x_3 + x_4 + x_5)^{10}$$

4. *Determinar o coeficiente do termo em $x_1^2 x_2^3 x_3 x_4^2$ no desenvolvimento de*

$$(x_1 - x_2 + 2x_3 - 2x_4)^8$$

5. *Desenvolver $(x_1+x_2+x_3)^n$ observando que $(x_1+x_2+x_3)^n = [(x_1+x_2)+x_3]^n$ e usando então a fórmula do binómio de Newton.*

6. *Simplificar*
   (a) $\sum_{i+j+k=n} \binom{n}{i,j,k}$
   (b) $\sum_{i+j+k=n} (-1)^k \binom{n}{i,j,k} 2^j/3^{i+j}$

2.4 Números Cardinais Transfinitos

> "O infinito! Nenhuma outra questão perturbou tão profundamente o espírito humano; nenhuma outra ideia o estimulou de forma tão frutuosa; apesar disso nenhum outro conceito carece de maior clarificação que o de infinito ..."
>
> *frase atribuída a* **David Hilbert**

2.4.1 Conjuntos equipotentes

Um conjunto infinito de objectos é certamente *"maior"* que um conjunto com um número finito qualquer de objectos. Esta ideia, embora parecendo inteiramente correcta sob um ponto de vista meramente intuitivo, não está formulada em termos rigorosos. Se se tentar fazer o mesmo tipo de comparação quando ambos os conjuntos são infinitos é, em geral, difícil (ou mesmo impossível) dar uma resposta satisfatória. Por exemplo, fará algum sentido perguntar se há um *"maior"* número de fracções (números racionais) que de números inteiros ou se há mais números irracionais que racionais? Como há uma infinidade de cada um deles, então a questão não ficará adequadamente formulada nestes termos antes de se ter clarificado o conceito de ser *"maior"* neste contexto. Ou seja, a questão que, de facto, se deverá formular é a de saber se há algum método que permita comparar dois conjuntos infinitos para saber qual deles é o *"maior"*.

Uma forma de analisar este tipo de problemas poderia, em princípio, ser esta: sabe-se que $\mathbb{N}$ está estritamente contido em $\mathbb{Q}$; pode então parecer que $\mathbb{Q}$ deverá ser maior que $\mathbb{N}$. Num contexto onde fossem considerados só conjuntos finitos este raciocínio teria perfeito cabimento. Contudo nada garante que os conceitos válidos num tal universo (dos conjuntos finitos) se mantenham válidos num universo alargado que contemple conjuntos infinitos. Será o todo maior que as partes quando se trata de quantidades infinitas? Que significado se pode atribuir, por exemplo, a metade de infinito? Graças a Georg Cantor (1845-1918), matemático russo/alemão, podem dar-se algumas respostas a estas questões, pelo menos num certo sentido. Em particular pode estabelecer-se, por exemplo, que $\mathbb{Q}$ tem tantos elementos quantos $\mathbb{N}$, mas que $\mathbb{R}$ tem mais elementos que $\mathbb{N}$. Para se compreenderem estas relações é necessário, antes de mais, analisar a operação matemática de **contagem**. Foi Cantor quem em 1870, pela primeira vez, chamou a atenção para a importância das correspondências bijectivas na procura de formas para comparar conjuntos infinitos.

Dado um número $m \in \mathbb{N}_1$ qualquer, denotar-se-á por $\mathbb{N}_{[m]}$ a secção inicial de $\mathbb{N}_1$ definida por

$$\mathbb{N}_{[m]} \;=\; \{1, 2, \ldots, m\}$$

e sendo $\mathbf{A}$ um conjunto qualquer, diz-se que $\mathbf{A}$ tem m elementos quando existe uma aplicação bijectiva

$$\gamma : \; A \;\rightarrow\; \mathbb{N}_{[m]}$$

Dados agora dois conjuntos $\mathbf{A}$ e $\mathbf{B}$, sejam

$$\gamma : \; \mathbf{A} \;\rightarrow \mathbb{N}_{[m]}, \;\; \psi : \; \mathbf{B} \;\rightarrow\; \mathbb{N}_{[n]}$$

duas bijecções. Se for $m = n$ dir-se-á, naturalmente, que os conjuntos $\mathbf{A}$ e $\mathbf{B}$ têm o mesmo número de elementos. Neste caso, se o objectivo a atingir fosse apenas o de comparar o tamanho dos conjuntos $\mathbf{A}$ e $\mathbf{B}$ e não o de saber exactamente quantos elementos tem cada um deles, a aplicação

$$\varphi = \psi^{-1} \circ \gamma : \; \mathbf{A} \;\rightarrow\; \mathbf{B}$$

resolveria completamente o problema. De facto, visto que ψ e γ são bijecções, então também φ é uma bijecção. Reciprocamente se existirem bijecções $\varphi : \mathbf{A} \rightarrow \mathbf{B}$ e $\gamma : \mathbf{A} \rightarrow \mathbb{N}_{[m]}$ então existe uma bijecção $\gamma \circ \varphi^{-1} : \mathbf{B} \rightarrow \mathbb{N}_{[m]}$. Daqui resulta que, num contexto de conjuntos finitos,

> *dois conjuntos* $\mathbf{A}$ *e* $\mathbf{B}$ *têm o mesmo número de elementos se existir uma bijecção* $\varphi : \; \mathbf{A} \;\rightarrow\; \mathbf{B}$.

A noção de bijecção pode estender-se a conjuntos quaiquer, o que permite fazer comparações de conjuntos arbitrários. Recorde-se e reescreva-se a definição 2.21 já considerada anteriormente.

Definição 2.37 (Cantor) *Sejam* $\mathbf{A}$ *e* $\mathbf{B}$ *dois conjuntos arbitrários.* $\mathbf{A}$ *e* $\mathbf{B}$ *dir-se-ão* **conjuntos equipotentes** *se existir uma bijecção* $\varphi : \mathbf{A} \rightarrow \mathbf{B}$ *entre eles.*

É imediato constatar que a relação de equipotência entre conjuntos é uma relação de equivalência. Escrever-se-á $\mathbf{A} \sim \mathbf{B}$ para significar que $\mathbf{A}$ e $\mathbf{B}$ são equipotentes. Pode agora formalizar-se a definição de conjunto finito do seguinte modo:

Definição 2.38 *Um conjunto* $\mathbf{A}$ *dir-se-á* **finito** *se for vazio ou existir um número* $m \in \mathbb{N}_1$ *tal que* $\mathbf{A} \sim \mathbb{N}_{[m]} \equiv \{1, 2, \ldots, m\}$. *Um conjunto que não é finito dir-se-á* **infinito**.

Se $\mathbf{A}$ for um conjunto finito, o número $m \in \mathbb{N}$ tal que $\mathbf{A} \sim \mathbb{N}_{[m]}$ é, como se sabe, o **cardinal** do conjunto $\mathbf{A}$ que se denota por $\mathbf{card}(\mathbf{A})$. O objectivo agora é dar um significado à noção de cardinalidade no caso de conjuntos infinitos. Antes porém considere-se o seguinte resultado:

Teorema 2.39 *Todo o conjunto infinito contém um subconjunto equipotente a* $\mathbb{N}_1$.

Demonstração: Seja $\mathbf{A}$ um conjunto infinito qualquer. $\mathbf{A}$ é não vazio e, portanto, possui um elemento $a_1 \in \mathbf{A}$. O conjunto $\mathbf{A}\backslash\{a_1\}$ é não vazio pois de contrário $\mathbf{A}$ seria o conjunto finito $\{a_1\}$. Consequentemente existirá $a_2 \in \mathbf{A}\backslash\{a_1\}$; analogamente o conjunto $\mathbf{A}\backslash\{a_1, a_2\}$ não pode ser vazio e, portanto, existirá $a_3 \in \mathbf{A}\backslash\{a_1, a_2\}$. Procedendo assim sucessivamente obter-se-á um subconjunto $\{a_1, a_2, \ldots\ldots\}$, de $\mathbf{A}$, que é equipotente a $\mathbb{N}_1$. □

Este teorema revela que o conjunto $\mathbb{N}_1$ é, de certo modo, *"o mais pequeno conjunto infinito"*, já que cada conjunto infinito possui um subconjunto equipotente a $\mathbb{N}_1$. Com base no Teorema 2.39 pode agora definir-se *conjunto finito* (a partir da noção de conjunto infinito) sem exigir o conhecimento prévio do conjunto $\mathbb{N}_1$. Tal definição deve-se a Dedekind e tem a forma seguinte:

Definição 2.40 *Um conjunto não vazio* $\mathbf{A}$ *diz-se* **Dedekind-finito** *se e só se para toda a aplicação* $\psi : \mathbf{A} \to \mathbf{A}$ *se tem que* ψ *é injectiva se e só se for sobrejectiva. Por convenção dir-se-á também que é Dedekind-finito o conjunto* $\emptyset$.

É possível provar que são equivalentes as Definições 2.38 e 2.40.

Nota 2.41 A definição rigorosa de cardinalidade, que afinal serve para dar um sentido à expressão *"número de elementos de um conjunto arbitrário"*, não é simples e sai fora do âmbito desta introdução. Indicar-se-ão, no entanto, as propriedades básicas que a noção de **cardinal de um conjunto** deve satisfazer e que constituem, de certo modo, uma definição axiomática para esta noção. Essas propriedades são as seguintes:

C1. Todo o conjunto $\mathbf{A}$ possui um cardinal associado, denotado por $\mathbf{card}(\mathbf{A})$. Reciprocamente, para cada cardinal ν existe um conjunto $\mathbf{X}$ tal que $\nu = \mathbf{card}(\mathbf{X})$;

C2. $\mathbf{card}(\mathbf{A}) = 0$ se e só se $\mathbf{A} = \emptyset$;

C3. Se $\mathbf{A} \sim \mathbb{N}_{[m]}$ então $\mathbf{card}(\mathbf{A}) = m$;

C4. $\mathbf{card}(\mathbf{A}) = \mathbf{card}(\mathbf{B})$ se e só se $\mathbf{A} \sim \mathbf{B}$.

Tendo em conta o conceito de aplicação injectiva faz sentido a seguinte definição aplicável a dois conjuntos $\mathbf{A}$ e $\mathbf{B}$ arbitrários.

Definição 2.42 *Dir-se-á que* $\mathbf{card}(\mathbf{A})$ *é menor ou igual que* $\mathbf{card}(\mathbf{B})$*, e escreve-se* $\mathbf{card}(\mathbf{A}) \leq \mathbf{card}(\mathbf{B})$*, se e só se existir uma aplicação injectiva de* $\mathbf{A}$ *para* $\mathbf{B}$*. Escrever-se-á ainda* $\mathbf{card}(\mathbf{A}) < \mathbf{card}(\mathbf{B})$ *para significar que se tem* $\mathbf{card}(\mathbf{A}) \leq \mathbf{card}(\mathbf{B})$ *e* $\mathbf{card}(\mathbf{A}) \neq \mathbf{card}(\mathbf{B})$*.*

2.4.2 Cardinais transfinitos

2.4.2.1 O primeiro número transfinito, $\aleph_0$

Ao lidar com a noção de *infinito* é necessário estar preparado para deparar com aspectos que parecem estranhos aos nossos hábitos finitistas. Como se verá mais tarde, há diferentes *infinitos* (ou, melhor dizendo, *transfinitos*); por isso adoptar-se-á uma notação apropriada para dar conta daquelas diferenças. Usar-se-ão para tal os símbolos (introduzidos por Cantor)

$$\aleph_0, \aleph_1, \aleph_2, \ldots\ldots$$

que se lêem *"alefe zero", "alefe um", etc.*, respectivamente. Visto que $\mathbb{N}_1$ não é equipotente a nenhuma das suas secções iniciais $\mathbb{N}_{[m]} \equiv \{1, 2, \ldots, m\}$ então o conjunto $\mathbb{N}_1$ não é finito; acresce ainda que a aplicação $\varphi : \mathbb{N}_1 \to \mathbb{N}_1$ definida por $\varphi(n) = 2n$, por exemplo, é injectiva, mas não sobrejectiva e, portanto, $\mathbb{N}_1$ não é finito também no sentido da definição 2.40 (o que não admira, dada a equivalência, já referida, das duas definições). Restringindo o conjunto de chegada da aplicação φ ao conjunto $2\mathbb{N}_1 \equiv \{2, 4, 6, \ldots\}$ a aplicação $\varphi_* : \mathbb{N}_1 \to 2\mathbb{N}_1$ é uma bijecção o que prova que $\mathbb{N}_1$ e $2\mathbb{N}_1$ são conjuntos equipotentes. Verifica-se assim um aspecto importante dos conjuntos infinitos, que não tem contrapartida nos conjuntos finitos, e que é o facto de um conjunto infinito conter partes que lhe são equipotentes. Este terá sido o primeiro *"paradoxo do infinito"* de que se terá dado conta Galileu Galilei (1564-1642) e que tanto o terá perturbado!

Teorema 2.43 *Seja* $\mathbf{A}$ *um subconjunto qualquer de* $\mathbb{N}_1$*. Então* $\mathbf{A}$ *é finito ou equipotente a* $\mathbb{N}_1$*.*

Demonstração: Suponha-se que $\mathbf{A}$ não é finito. Então $\mathbf{A}$ é não vazio e, consequentemente, possui um elemento menor que todos os outros. Seja $a_1 \in \mathbf{A}$ esse elemento. Seja agora a_2 o menor elemento de $\mathbf{A}\backslash\{a_1\}$, a_3 o menor elemento de $\mathbf{A}\backslash\{a_1, a_2\}$ e assim sucessivamente. Desta forma todos os elementos de $\mathbf{A}$ são considerados ficando então construída uma bijecção entre $\mathbf{A}$ e $\mathbb{N}_1$. □

De acordo com este resultado todos os subconjuntos infinitos de $\mathbb{N}_1$ são equipotentes a $\mathbb{N}_1$. Estão neste caso, por exemplo, os conjuntos dos números pares positivos, dos números ímpares positivos, dos números primos, etc.

Definição 2.44 *Dir-se-á que um conjunto infinito* $\mathbf{A}$ *tem cardinalidade* $\aleph_0$ *se* $\mathbf{A}$ *for equipotente ao conjunto* $\mathbb{N}_1$*, e escrever-se-á com este sentido* $\mathbf{card}(\mathbf{A}) = \aleph_0$.

Do que atrás ficou dito resulta que há apenas um cardinal transfinito, $\aleph_0$, para todos os subconjuntos infinitos de $\mathbb{N}_1$. No entanto, $\mathbb{N}_1$ é, ele próprio, subconjunto de outros conjuntos, podendo, à primeira vista, ser-se tentado a atribuir-lhes então uma cardinalidade superior à de $\mathbb{N}_1$. Tal não acontece necessariamente, como o provam os seguintes resultados:

Teorema 2.45 *O conjunto* $\mathbb{Z} \supset \mathbb{N}_1$ *é equipotente ao conjunto* $\mathbb{N}_1$ *(ou seja* $\mathbf{card}(\mathbb{Z}) = \aleph_0$*).*

Demonstração: Escrevendo $\mathbb{Z}$ na forma

$$0, +1, -1, +2, -2, +3, -3, \ldots\ldots$$

obter-se-á uma bijecção $\varphi : \mathbb{N}_1 \to \mathbb{Z}$ da seguinte forma: $\varphi(1) = 0$, $\varphi(2) = 1$, $\varphi(3) = -1$, $\varphi(4) = 2$, $\varphi(5) = -2$, $\varphi(6) = 3$, ... □

De certo modo mais inesperado é o seguinte:

Teorema 2.46 *O conjunto* $\mathbb{Q}$ *dos números racionais é numerável (ou seja,* $\mathbf{card}(\mathbb{Q}) = \aleph_0$*).*

Demonstração: A demonstração resulta do processo de numeração dos elementos de $\mathbb{Q}^+$ exemplificado como se segue

$$\begin{array}{cccccccc}
1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \cdots \\
2 & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \frac{2}{6} & \cdots \\
3 & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \frac{3}{6} & \cdots \\
4 & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \frac{4}{6} & \cdots \\
5 & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \frac{5}{6} & \cdots \\
6 & \frac{6}{2} & \frac{6}{3} & \frac{6}{4} & \frac{6}{5} & \frac{6}{6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Assim, dispostos em quadrado semi-infinito, aparecem todos os números racionais positivos pelo menos uma vez; é possível agora ordená-los seguindo o caminho indicado na figura acima. Depois de eliminados todos os números que se encontram repetidos, obter-se-á

$$1,\ 1/2, 2,\ 1/3, 3,\ 1/4, 2/3, 3/2, 4\ \ldots\ldots$$

o que constitui uma enumeração de $\mathbb{Q}^+$. Procedendo agora como na enumeração dos elementos de $\mathbb{Z}$, juntando o 0 no início e colocando alternadamente números racionais positivos e negativos, obter-se-á

$$0, 1, -1, 1/2, -1/2, 2, -2, 1/3, -1/3, 3, -3, 1/4, -1/4, 2/3, -2/3, 3/2, -3/2, 4, \ldots,$$

o que constitui uma enumeração de $\mathbb{Q}$, verificando-se deste modo que $\mathbb{Q}$ é equipotente a $\mathbb{N}_1$ e, portanto, que $\mathbf{card}(\mathbb{Q}) = \aleph_0$, o que constitui um resultado que, à primeira vista, não seria de esperar. □

Teorema 2.47 *O conjunto* **A** *constituído por todos os números algébricos tem a potência do numerável.*

Demonstração: Um número diz-se **algébrico** se for raiz de um polinómio de coeficientes inteiros. Então **A** é o conjunto de todos os zeros de todos os polinómios de coeficientes inteiros, que se denota, geralmente, por $\mathbb{Z}[x]$. Dado um polinómio qualquer

$$p(x) \ = \ a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \ \in \mathbb{Z}[x]$$

chama-se **altura** de p ao número inteiro positivo definido por

$$h(p) \ = \ n + \sum_{j=0}^{n} |a_j|.$$

Como se sabe, para cada $k \in \mathbb{N}_1$ há apenas um número finito, $\omega(k) \in \mathbb{N}$, de maneiras distintas de decompor k como soma de números inteiros não negativos. Então há apenas $\omega(k)$ polinómios distintos de altura $h(p) = k$, cada um dos quais tem grau $< k$ e, portanto, no máximo $k-1$ zeros. Para cada altura $k \in \mathbb{N}_1$ então há, no máximo, $k\omega(k)$ números algébricos. Ordenando os números algébricos de acordo com as sucessivas alturas dos polinómios de $\mathbb{Z}[x]$ de que são zeros, obter-se-á uma enumeração de todos os elementos de $\mathbf{A}$, ficando deste modo provada a afirmação feita. □

2.4.2.2 O segundo número transfinito, $\aleph_1$

Dos exemplos atrás considerados pode ficar a ideia de que, afinal, todos os conjuntos infinitos têm a mesma cardinalidade, $\aleph_0$. Como a seguir se verá, tal não se verifica, no entanto.

Teorema 2.48 *Seja* $\mathbf{A}$ *um conjunto não vazio qualquer e denote-se por* $\mathcal{P}(\mathbf{A})$ *o conjunto das partes de* $\mathbf{A}$*. Então*

$$\mathbf{card}(\mathbf{A}) \ < \ \mathbf{card}\,(\mathcal{P}(\mathbf{A}))$$

(onde a desigualdade é estrita).

Demonstração: Visto que a aplicação

$$\begin{array}{rccl} \varphi: & \mathbf{A} & \to & \mathcal{P}(\mathbf{A}) \\ & a & \rightsquigarrow & \varphi(a) = \{a\} \end{array}$$

é injectiva, então tem-se imediatamente,

$$\mathbf{card}(\mathbf{A}) \ \leq \ \mathbf{card}\,(\mathcal{P}(\mathbf{A}))$$

Para mostrar que, adicionalmente, se tem $\mathbf{card}(\mathbf{A}) \neq \mathbf{card}\,(\mathcal{P}(\mathbf{A}))$ é necessário provar agora que não existe nenhuma bijecção entre $\mathbf{A}$ e $\mathcal{P}(\mathbf{A})$. Para tal, basta mostrar que não há nenhuma aplicação de $\mathbf{A}$ em $\mathcal{P}(\mathbf{A})$ que seja sobrejectiva ou, dito de outro modo, que para toda a aplicação

$$\psi: \ \mathbf{A} \ \to \ \mathcal{P}(\mathbf{A})$$

existe sempre um subconjunto $\mathbf{T}$ de $\mathcal{P}(\mathbf{A})$ que não é imagem por ψ de nenhum elemento de $\mathbf{A}$. Tal demonstração deve-se a Georg Cantor, que introduziu o subconjunto $\mathbf{T} \subseteq \mathbf{A}$ definido por

$$\mathbf{T} \ = \ \{t \in \mathbf{A} : t \notin \psi(t)\}$$

provando em seguida que não existe qualquer $b \in \mathbf{A}$ para o qual se tenha $\psi(b) = \mathbf{T}$.

De facto, seja $x \in \mathbf{A}$ qualquer; então ou $x \notin \mathbf{T}$ ou $x \in \mathbf{T}$. Se $x \notin \mathbf{T}$, da definição de $\mathbf{T}$ resulta que $x \in \psi(x)$ e, portanto, que $\psi(x) \neq \mathbf{T}$. Se $x \in \mathbf{T}$ então $x \notin \psi(x)$ e, portanto, $\psi(x) \neq \mathbf{T}$. Consequentemente ψ não é sobrejectiva, como se afirmou. □

Deste teorema, fazendo $\mathbf{A} \equiv \mathbb{N}_1$, resulta a desigualdade

$$\mathbf{card}(\mathbb{N}_1) \ < \ \mathbf{card}\left(\mathcal{P}(\mathbb{N}_1)\right).$$

Denotando[2] $\mathbf{card}\left(\mathcal{P}(\mathbb{N}_1)\right)$ por $2^{\aleph_0}$, tem-se então

$$2^{\aleph_0} \ > \ \aleph_0$$

onde $2^{\aleph_0}$ é o segundo cardinal transfinito, denotado geralmente por $\aleph_1$.

O mais conhecido conjunto cuja cardinalidade se pode provar ser igual a $\aleph_1$ é o conjunto $\mathbb{R}$ dos números reais. Como a função $f : \mathbb{R} \to (0,1)$ definida por

$$f(x) \ = \ \frac{1}{2} + \frac{1}{\pi}\arctan(x)$$

é bijectiva, então os conjuntos $\mathbb{R}$ e $(0,1) \subset \mathbb{R}$ são equipotentes e têm, portanto, a mesma cardinalidade. Por outro lado, como os intervalos $[0,1]$ e $(0,1)$ têm a mesma cardinalidade,[3] então $\mathbb{R}$ e $[0,1]$ têm também a mesma cardinalidade.

Teorema 2.49 *O cardinal de* $\mathbb{R}$*, igual ao cardinal do intervalo* $[0,1]$*, é igual ao cardinal de* $\mathcal{P}(\mathbb{N}_1)$*, isto é,* $\mathbf{card}(\mathbb{R}) = \aleph_1$*.*

Demonstração: A aplicação $\tau : \mathcal{P}(\mathbb{N}_1) \to [0,1]$ definida, para cada $\mathbf{T} \in \mathcal{P}(\mathbb{N}_1)$, por

$$\tau(\mathbf{T}) \ = \ 0, \tau_1\tau_2\tau_3 \ldots\ldots \ \equiv \ \sum_{i=1}^{\infty} \frac{\tau_i}{10^i} \in [0,1]$$

onde, para cada $i = 1, 2, 3, \ldots\ldots$, se tem

$$\tau_i = \begin{cases} 0 & \text{se} \quad i \notin \mathbf{T} \\ 1 & \text{se} \quad i \in \mathbf{T}, \end{cases}$$

[2]Note-se que se $\mathbf{A}$ for um conjunto finito com n elementos então $\mathcal{P}(\mathbf{A})$ é também um conjunto finito, mas com 2^n elementos.

[3]Para o provar basta verificar que a aplicação $g : [0,1] \to (0,1)$ definida por

$$g(x) = \begin{cases} 0 & \text{se} \quad x = 0, \\ \frac{1}{k+2} & \text{se} \quad x = \frac{1}{k+1} \text{ e } k = 0, 1, 2, \ldots, \\ x & \text{se} \quad x \in]\frac{1}{k+1}, \frac{1}{k}[\text{ e } k = 1, 2, \ldots \end{cases}$$

é bijectiva.

é, como se pode provar, uma aplicação injectiva.

Interpretando agora $0, \tau_1\tau_2\tau_3 \ldots$, definido acima, como representação binária de um número, obtém-se uma nova aplicação $\gamma : \mathcal{P}(\mathbb{N}_1) \to [0,1]$, pondo

$$\gamma(\mathbf{T}) \;=\; 0, \tau_1\tau_2\tau_3 \ldots\ldots|_{[2]} \;\equiv\; \sum_{i=1}^{\infty} \frac{\tau_i}{2^i}$$

Visto que, como se pode mostrar, todo o número $x \in [0,1]$ possui *uma* representação binária da forma $0, \tau_1\tau_2\tau_3 \ldots\ldots$ com $\tau_i \in \{0,1\}$ para $i = 1, 2, 3, \ldots$, então, associando a cada $x \in [0,1]$ o subconjunto $\mathbf{T}_x$ de $\mathbb{N}_1$ definido por

$$\mathbf{T}_x \;=\; \{i \in \mathbb{N}_1 : \tau_i = 1\} \subseteq \mathbb{N}_1$$

pode concluir-se que γ é uma aplicação sobrejectiva. Este facto, por seu turno, implica a existência de uma aplicação injectiva $\alpha : [0,1] \to \mathcal{P}(\mathbb{N}_1)$ (ver exercício 2.4.1 abaixo). Consequentemente, tendo em conta o Teorema de Shröder-Bernstein,[4] existe uma aplicação bijectiva entre $\mathcal{P}(\mathbb{N}_1)$ e $[0,1]$ e, portanto, $\mathcal{P}(\mathbb{N}_1)$ e $[0,1]$ são conjuntos equipotentes, ou seja

$$\mathbf{card}([0,1]) \;=\; \mathbf{card}\left(\mathcal{P}(\mathbb{N}_1)\right).$$

Das considerações feitas resulta então que $\mathbf{card}(\mathbb{R}) = \mathbf{card}\left(\mathcal{P}(\mathbb{N}_1)\right) \equiv \aleph_1$, como se pretendia mostrar. □

Exercícios 2.4.1 Sejam **A** e **B** dois conjuntos quaisquer. Provar que se existir uma aplicação sobrejectiva de **A** em **B** então existe uma aplicação injectiva de **B** em **A**.

Já atrás foi referido que $\sqrt{2}$ não é um número racional o que significa que a diagonal de um quadrado não é comensurável com o seu lado. Isto mostra que não existe uma correspondência bijectiva entre o conjunto $\mathbb{Q}$ e a *recta numérica*, facto este que levou à criação do conjunto $\mathbb{R}$ dos números reais. Daqui pode então inferir-se que existem $\aleph_1$ pontos na recta numérica (ou, em boa verdade, em qualquer segmento da recta numérica que não se reduza a um ponto). O número cardinal transfinito $\aleph_0$ é frequentemente referido na literatura por *"potência do numerável"* enquanto que o número cardinal transfinito $\aleph_1$, por razões óbvias, é designado por *"potência do contínuo"*.

Considere-se agora o segmento de recta

$$I \;=\; (0,1)$$

[4] **Teorema de Shröder-Bernstein:** Dados dois conjuntos **A** e **B**, se existirem duas aplicações injectivas $\alpha : \mathbf{A} \to \mathbf{B}$ e $\beta : \mathbf{B} \to \mathbf{A}$, então existe também uma aplicação bijectiva $\gamma : \mathbf{A} \to \mathbf{B}$.

e o quadrado

$$I^2 \;=\; \{(x,y) \in \mathbb{R}^2 : 0 < x, y < 1\}.$$

O quadrado tem área igual a 1 enquanto que o intervalo tem área igual a 0. Seria de esperar, portanto, que houvesse mais pontos no quadrado que no intervalo. Entretanto pode provar-se o seguinte:

Teorema 2.50 *O segmento da recta real I e o quadrado I^2 do plano real são equicardinais (ou, dito de outra forma, há tantos pontos no plano real quantos na recta real).*

Demonstração: Considere-se um quadrado de comprimento unitário referido a um sistema de eixos cuja origem coincide com o vértice inferior esquerdo e cujos eixos contêm os lados que se cruzam nesse vértice. Seja p a abcissa de um ponto do lado do quadrado assente no eixo Ox. Então p é um número estritamente compreendido entre 0 e 1. Deste número extraiam-se dois números a e b da seguinte forma: em a figuram todos os dígitos existentes nas casas decimais de ordem ímpar e em b todos os dígitos existentes nas casas decimais de ordem par.(Se, por exemplo, for $p = 0.7346982340\ldots$ vem $a = 0.74924\ldots$ e $b = 0.368630\ldots$.) O par (a,b) pode ser representado por um ponto $P \equiv (a,b)$ do interior do quadrado; reciprocamente, a cada ponto do quadrado pode, pela construção inversa, fazer-se corresponder um e um só ponto da aresta considerada. Estabelece-se assim uma correspondência bijectiva $p \leftrightarrow (a,b)$ entre pontos do intervalo $(0,1)$ e pontos do quadrado $(0,1) \times (0,1)$ ou seja: há tantos pontos no quadrado como no segmento de recta. □

De forma análoga, usando agora um cubo de lado 1, pode mostrar-se que há tantos pontos num cubo como em qualquer uma das suas arestas (ou ainda, que há tantos pontos no espaço tridimensional quantos na recta!). Este raciocínio pode generalizar-se a qualquer espaço $\mathbb{R}^n$ para $n \in \mathbb{N}_1$ arbitrário.

O exemplo da equipotência entre o segmento de recta I e o quadrado I^2 merece ainda um pouco mais de reflexão. Os dois objectos matemáticos são claramente distintos, o que significa então que a sua caracterização não pode ser feita apenas à custa da noção de equipotência de conjuntos (dois sacos, um de batatas e outro de feijões, podem conter exactamente o mesmo número de objectos, mas a nossa intuição garante-nos que eles são claramente distintos!). A diferença entre os dois conjuntos acima referidos é de uma índole que não pode ser classificada em termos de cardinalidade, mas que ultrapassa o âmbito desta disciplina.

2.4.2.3 Números cardinais transfinitos superiores

O Teorema 2.48 da secção anterior permite mostrar que o conjunto de todos os cardinais transfinitos é, ele próprio, infinito. De facto, visto que, para

qualquer conjunto não vazio $\mathbf{A}$ se tem

$$\mathbf{card}(\mathbf{A}) \ < \ \mathbf{card}\,(\mathcal{P}(\mathbf{A}))$$

então ter-se-á que

$$\aleph_1 \ < \ \mathbf{card}\,(\mathcal{P}(\mathbb{R})) \equiv \aleph_2$$

onde $\aleph_2$ também se denota por $2^{\aleph_1}$. Obtém-se assim um novo cardinal transfinito estritamente superior aos anteriores. $\aleph_2$ é o cardinal de, por exemplo, o conjunto de todas as funções reais de variável real. Por aplicação repetida do referido Teorema 2.48 pode construir-se uma sucessão de cardinais transfinitos

$$\aleph_0 \ < \ \aleph_1 \ < \ \aleph_2 \ < \ \aleph_3 \ < \ \ldots\ldots$$

cujo estudo mais aprofundado não será aqui feito.

Capítulo 3

Relações de Recorrência e Funções Geradoras

3.1 Introdução

No capítulo anterior, para determinar uma expressão para A_p^m, o número de arranjos de m objectos tomados p a p, partiu-se da relação

$$A_p^m \;=\; A_{p-1}^m \cdot (m-p+1), \quad p = 1, 2, \ldots, m \tag{3.1}$$

onde A_p^m, para cada $m \in \mathbb{N}$ fixado, se expressa à custa do termo anterior A_{p-1}^m. A fórmula (3.1) é um exemplo de uma relação de recorrência.

Outro exemplo do mesmo tipo é dado pelos termos de uma progressão geométrica de razão r: denotando por a_n o termo de ordem n da progressão geométrica então este termo é igual ao produto do termo de ordem $n-1$ pela razão r, isto é,

$$a_n \;=\; r\, a_{n-1}, \quad n = 1, 2, 3, \ldots \tag{3.2}$$

o que constitui também uma relação de recorrência. Supondo que $a_0 = 1$ podem agora determinar-se os termos da sucessão $(a_n)_{n\in\mathbb{N}}$, sequencialmente,

$$\begin{array}{rcccl} a_1 & = & r\, a_0 & = & r \\ a_2 & = & r\, a_1 & = & r^2 \\ a_3 & = & r\, a_2 & = & r^3 \\ & \vdots & & & \\ a_n & = & r\, a_{n-1} & = & r^n \\ & \vdots & & & \end{array}$$

A condição $a_0 = 1$ é chamada condição inicial da relação de recorrência (3.2). Neste caso, foi fácil determinar a forma do termo geral independentemente dos termos anteriores; mas nem sempre assim acontece.

Outro exemplo ainda de uma relação de recorrência muito conhecida é a que é dada para definir os chamados **números de Fibonaci**, que aparecem em muitos problemas,

$$\{f_0, f_1, f_2, f_3, \ldots\}$$

Estes números são definidos pelas condições iniciais

$$f_0 = f_1 = 1$$

e pela relação de recorrência

$$f_n \;=\; f_{n-1} + f_{n-2}$$

Usando esta relação e as condições iniciais, podem calcular-se os primeiros termos da sucessão

$$\{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots\}$$

A partir desta sequência de números, contudo, não é fácil conjecturar uma fórmula fechada para o termo geral da sucessão dos números de Fibonaci. E, no entanto, tal fórmula pode ser importante para avaliar, por exemplo, o grau de crescimento da sucessão para valores grandes da variável n.

Esta sucessão foi estudada no séc. XIII por Leonardo de Pisa – Fibonaci – quando se ocupava de um problema de crescimento de uma população de coelhos. Fibonacci questionava-se sobre o número de pares de coelhos que seria obtido na geração n se se partisse de um único casal de coelhos e se supusesse que cada par de coelhos contribuia com um casal de coelhos para a geração seguinte e um casal de coelhos para a geração que vem a seguir a esta, morrendo de seguida.

Mantendo a mesma relação recursiva, mas variando as condições iniciais, obtém-se outra sequência de números diferente da primeira. Assim, fazendo, por exemplo

$$l_0 = 2 \quad \text{e} \quad l_1 = 1$$

e

$$l_n \ = \ l_{n-1} + l_{n-2}$$

obtém-se a sucessão

$$\{2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, \ldots\}$$

cujos elementos são conhecidos por **números de Lucas**.

Os números de Lucas e de Fibonacci estão relacionados entre si de diversas maneiras: tem-se, por exemplo,

$f_{2n} \ = \ f_n \cdot l_n$	$l_{2n} \ = \ l_n^2 - 2(-1)^n$
$f_0 + f_1 + \cdots + f_n \ = \ f_{n+2} - 1$	$l_0 + l_1 + \cdots + l_n \ = \ l_{n+2} - 1$
$l_n \ = \ f_{n-1} + f_{n+1}$	$5f_n \ = \ l_{n-1} + l_{n+1}$
$2f_{m+n} \ = \ f_m l_n + f_n l_m$	$2l_{m+n} \ = \ l_m l_n + 5f_m f_n$

Definição 3.1 *Dada uma sucessão de números $a_0, a_1, a_2, \ldots, a_n, \ldots$ chama-se* **relação de recorrência** *a uma equação que relaciona o termo a_n com os termos que o antecedem e que é válida para todo o n maior que um dado inteiro fixado n_0.*

Em muitos casos é possível obter a partir da relação de recorrência e das condições iniciais uma fórmula explícita para o termo de ordem n. Isto pode ser feito por iteração sucessiva da fórmula de recorrência ou então

conjecturando adequadamente uma fórmula fechada a qual tem de ser depois demonstrada por indução matemática, usando a relação de recorrência correspondente – é o que acontece com a relação de recorrência (3.2), por exemplo.

Considere-se, de novo, a relação de recorrência de Fibonacci

$$f_n \;=\; f_{n-1} + f_{n-2}, \quad n = 2, 3, 4, \ldots$$

Uma forma de resolver esta relação é procurar para ela soluções da forma

$$f_n \;=\; q^n \tag{3.3}$$

onde q é um número real não nulo.

Como

$$f_{n-1} \;=\; q^{n-1} \quad \text{e} \quad f_{n-2} \;=\; q^{n-2}$$

então a expressão (3.3) será solução da relação de recorrência de Fibonacci se e só se[1] $q \neq 0$ satisfizer a relação algébrica

$$q^n \;=\; q^{n-1} + q^{n-2}$$

ou seja

$$q^n - q^{n-1} - q^{n-2} \;=\; 0$$

Pondo q^{n-2} em evidência

$$q^{n-2}\left(q^2 - q - 1\right) \;=\; 0$$

então, visto que $q \neq 0$, daqui decorre que

$$q^2 - q - 1 \;=\; 0$$

Esta equação admite as duas soluções

$$q_1 \;=\; \frac{1+\sqrt{5}}{2} \quad q_2 \;=\; \frac{1-\sqrt{5}}{2}$$

e, portanto,

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

[1] Para $q = 0$ obter-se-ia a sucessão nula.

são ambas soluções da equação de recorrência de Fibonacci. Visto que a relação de recorrência de Fibonacci é linear e homogénea, então, como se mostrará mais tarde, qualquer combinação linear daquelas duas soluções é ainda solução da equação de recorrência dada. Assim, a solução geral da relação de recorrência de Fibonacci é dada por

$$f_n = c_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

onde c_1, c_2 são constantes arbitrárias. Tendo em conta as condições iniciais

$$f_0 = f_1 = 1$$

obtém-se o seguinte sistema de equações lineares nas incógnitas c_1 e c_2

$$\begin{aligned} 1 &= c_1 + c_2 \\ 1 &= c_1 \frac{1+\sqrt{5}}{2} + c_2 \frac{1-\sqrt{5}}{2} \end{aligned}$$

donde

$$c_1 = \frac{1}{\sqrt{5}} \frac{1+\sqrt{5}}{2}, \quad c_2 = \frac{-1}{\sqrt{5}} \frac{1-\sqrt{5}}{2}$$

Então os números de Fibonacci satisfazem a fórmula

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

para $n = 0, 1, 2, 3, 4, \ldots$ (provar por indução!).

Considerando agora as condições iniciais correspondentes à sucessão dos números de Lucas na solução geral da relação de recorrência de Fibonacci

$$\begin{aligned} l_n &= c_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^n \\ l_0 &= 2, \quad l_1 = 1 \end{aligned}$$

obtém-se

$$\begin{aligned} 2 &= c_1 + c_2 \\ 1 &= c_1 \frac{1+\sqrt{5}}{2} + c_2 \frac{1-\sqrt{5}}{2} \end{aligned}$$

donde

$$c_1 \;=\; \frac{\sqrt{5}-2}{\sqrt{5}}\,, \quad c_2 \;=\; \frac{\sqrt{5}+2}{\sqrt{5}}$$

Os números de Lucas satisfazem assim a fórmula

$$l_n \;=\; \frac{\sqrt{5}-2}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{\sqrt{5}+2}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

para $n = 0, 1, 2, 3, 4, \ldots$ (provar por indução!).

Os números de Fibonacci ocorrem frequentemente na resolução de problemas combinatórios. No teorema que se segue estabelece-se uma representação dos números de Fibonacci em termos dos coeficientes binomiais.

Teorema 3.2 *Para $n \geq 0$ o número de Fibonacci f_n satisfaz a seguinte relação*

$$f_n \;=\; \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-k}{k}$$

onde $k = [n/2]$ (é o maior inteiro contido em $n/2$).

Demonstração: Para $n \geq 0$ seja

$$g(n) \;=\; \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-k}{k}$$

onde $k = [n/2]$. Visto que $C_p^n = 0$ para qualquer inteiro $p > n$, pode escrever-se

$$g(n) \;=\; \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-k}{k} + \binom{n-k-1}{k+1} + \cdots + \binom{0}{n}$$

Para completar a demonstração terá de verificar-se que $f_0 = g(0)$ e $f_1 = g(1)$ e ainda que $g(n)$ é uma solução da relação de recorrência de Fibonacci, $f_n = f_{n-1} + f_{n-2}$. Visto que os valores iniciais juntamente com a relação de recorrência determinam univocamente a sequência de números, pode então concluir-se que $f_n = g(n)$ para todo o $n \geq 0$. Ora,

$$\begin{aligned} g(0) &= \binom{0}{0} \;=\; 1 \;=\; f_0 \\ g(1) &= \binom{1}{0} + \binom{0}{1} \;=\; 1 \;=\; f_1 \end{aligned}$$

Para $n \geq 2$

$$\begin{aligned} g(n-1)+g(n-2) &= \binom{n-1}{0}+\binom{n-2}{1}+\binom{n-3}{2}+\cdots+\binom{0}{n-1}+ \\ &\quad \binom{n-2}{0}+\binom{n-3}{1}+\cdots+\binom{0}{n-2} \\ &= \binom{n-1}{0}+\left[\binom{n-2}{1}+\binom{n-2}{0}\right]+ \\ &\quad \left[\binom{n-3}{2}+\binom{n-3}{1}\right]+\cdots+\left[\binom{0}{n-1}+\binom{0}{n-2}\right] \end{aligned}$$

Tendo em conta a relação entre os coeficientes binomiais

$$\binom{r}{p} = \binom{r-1}{p}+\binom{r-1}{p-1}$$

e aplicando-a adequadamente à expressão anterior, visto que $C_0^{n-1} = 1 = C_0^n$ e $C_n^0 = 0$, vem

$$\begin{aligned} g(n-1)+g(n-2) &= \binom{n-1}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots+\binom{1}{n-1} \\ &= \binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots+\binom{1}{n-1}+\binom{0}{n} \end{aligned}$$

Então

$$g(n-1)+g(n-2) = g(n)$$

o que significa que $g(n)$ é solução da relação de recorrência de Fibonacci para $n \geq 2$. Consequentemente, $f_n = g(n)$ para todo o $n = 0, 1, 2, \ldots$. □

3.1.1 Relações de recorrência e equações de diferenças

Seja $(a_n)_{n=0,1,2,\ldots}$ uma sucessão dada. Chama-se **primeira diferença** desta sucessão à sucessão $(\Delta a_n)_{n=1,2,\ldots}$ definida por

$$\Delta a_n = a_n - a_{n-1}, \quad n = 1, 2, \ldots$$

A segunda diferença $(\Delta^2 a_n)_{n=2,3,\ldots}$ é a primeira diferença da sucessão de primeiras diferenças $(\Delta a_n)_{n=1,2,\ldots}$

$$\begin{aligned} \Delta^2 a_n &= \Delta(\Delta a_n) = \Delta a_n - \Delta a_{n-1} \\ &= a_n - a_{n-1} - (a_{n-1} - a_{n-2}) = a_n - 2a_{n-1} + a_{n-2} \end{aligned}$$

Mais geralmente, para $k \in \mathbb{N}_1$ qualquer, define-se a diferença de ordem k, pondo

$$\begin{aligned} \Delta^k a_n &= \Delta\left(\Delta^{k-1} a_n\right) \\ &= \Delta^{k-1} a_n - \Delta^{k-1} a_{n-1}, \quad n = k, k+1, \ldots \end{aligned}$$

Chama-se **equação de diferenças** a uma equação que envolve o termo a_n e as suas diferenças. Por exemplo, a equação

$$3\Delta^2(a_n) + 2\Delta(a_n) + 7a_n = 0 \tag{3.4}$$

é uma equação de diferenças de 2ª ordem homogénea (porque o segundo membro da equação é zero).

Note-se que cada a_{n-i} (com $i = 1, 2, \ldots, n-1$) pode ser expresso em termos de a_n e das suas diferenças

$$\begin{aligned} a_{n-1} &= a_n - \Delta(a_n) \\ a_{n-2} &= a_{n-1} - \Delta(a_{n-1}) \\ &= a_n - \Delta(a_n) - \Delta(a_n) + \Delta^2(a_n) \\ &= a_n - 2\Delta(a_n) + \Delta^2(a_n) \\ &\vdots \end{aligned}$$

Usando estas relações e substituindo na equação de diferenças, esta transforma-se numa relação de recorrência. Cada relação de recorrência pode assim formular-se em termos de uma equação de diferenças e vice-versa, cada equação de diferencas pode dar origem a uma relação de recorrência. A equação de diferenças (3.4), por exemplo, pode transformar-se na seguinte relação de recorrência

$$3\left(a_n - 2a_{n-1} + a_{n-2}\right) + 2\left(a_n - a_{n-1}\right) + 7a_n = 0$$

ou seja

$$12a_n = 8a_{n-1} - 3a_{n-2}$$

Por este facto, as expressões *equação de diferenças* e *relação de recorrência* são usadas, muitas vezes, indistintamente.

Note-se que para resolver uma relação do tipo

$$12a_n = 8a_{n-1} - 3a_{n-2}$$

é necessário conhecer or termos a_0 e a_1, ou seja, são necessárias duas condições iniciais para resolver a equação de diferenças (3.4).

Exemplo 3.3 A relação de recorrência

$$a_n \;=\; na_{n-1}, \quad n = 1, 2, 3, \ldots$$

com a condição incial $a_0 = 1$ tem a seguinte solução

$$a_n \;=\; n!, \quad n = 0, 1, 2, 3, \ldots$$

3.2 Funções Geradoras

As funções geradoras, que a seguir se definem, aparecem muitas vezes, com grande utilidade, na resolução de problemas de contagens. Para começar, considere-se o seguinte exemplo:

Exemplo 3.4 *Determinar o número de soluções inteiras da equação*

$$a + b + c \;=\; 10$$

onde cada variável só pode tomar valores inteiros entre 2 e 4.
Resolução. Este problema pode resolver-se por enumeração explícita

a	b	c
2	4	4
3	4	3
3	3	4
4	2	4
4	4	2
4	3	3

Há, portanto, 6 soluções para este problema.

Foi possível resolver deste modo este problema por ele ser de pequenas dimensões. Se as dimensões do problema fossem substancialmente maiores, este método, de enumeração explícita, tornar-se-ia de difícil ou impossível aplicabilidade. Vejamos então outro método de aplicação mais geral.

A cada variável, a, b, c, associa-se um polinómio p_a, p_b, p_c assim definido: como cada variável só pode tomar os valores 2, 3 ou 4 então, neste caso, cada um dos polinómios é dado por

$$x^2 + x^3 + x^4$$

Multiplicando os três polinómios correspondentes a cada uma das três variáveis obtém-se o polinómio

$$p(x) \;=\; p_a(x) \cdot p_b(x) \cdot p_c(x) \;=\; (x^2 + x^3 + x^4)^3$$

o qual envolve as potências de x que vão de 6 a 12. Este polinómio é um exemplo de uma **função geradora**.

Visto que $a+b+c=10$ então o coeficiente de x^{10} em $p(x)$ dá o número de soluções da equação original nas condições especificadas. De facto, o coeficiente de x^{10} é igual ao número de produtos da forma $x^a x^b x^c$ onde a, b, c pertencem ao conjunto $\{2,3,4\}$ e são tais que $a+b+c=10$. Visto que

$$\begin{aligned} p(x) &= (x^2+x^3+x^4)(x^2+x^3+x^4)(x^2+x^3+x^4) \\ &= (x^4+2x^5+3x^6+2x^7+x^8)(x^2+x^3+x^4) \\ &= x^6+x^7+x^8+2x^7+2x^8+2x^9+3x^8+3x^9+3x^{10}+2x^9+2x^{10}+ \\ &\quad 2x^{11}+x^{10}+x^{11}+x^{12} \\ &= \cdots+(3+2+1)x^{10}+\cdots \end{aligned}$$

O número de soluções inteiras da equação dada pertencentes ao conjunto $\{2,3,4\}$ é, como já se sabia por enumeração directa, igual a 6.

Definição 3.5 *Chama-se série de potências a uma série da forma*

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$$

onde a_n $(n=0,1,2,3,\ldots)$ são números reais ou complexos e x designa uma variável.

Se

$$\begin{aligned} &a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots \\ &b_0+b_1x+b_2x^2+\cdots+b_nx^n+\cdots \end{aligned}$$

forem duas séries de potências, então a **soma** destas duas séries de potências é a série de potências dada por

$$(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n+\cdots$$

e o **produto** destas duas séries de potências é a série de potências cujo coeficiente de x^n, $n=0,1,2,\ldots$ é dado por

$$a_0b_n+a_1b_{n-1}+a_2b_{n-2}+\cdots+a_nb_0 = \sum_{i,j\geq 0;\, i+j=n} a_ib_j$$

ou seja, a série de potências produto é dada por

$$\sum_{n=0}^{\infty}\left(\sum_{i,j\geq 0;\, i+j=n} a_ib_j\right)x^n$$

Se a_n $(n=0,1,2,\ldots)$ for, para cada n, o número de soluções de um dado problema combinatório, chama-se **função geradora ordinária** para aquele problema combinatório à série de potências

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$$

Note-se que qualquer polinómio é uma série de potências particular: por exemplo, o polinómio

$$3x^2 + 2x^4 + x^7$$

pode ser escrito na forma

$$0 + 0x + 3x^2 + 0x^3 + 2x^4 + 0x^5 + 0x^6 + x^7 + 0x^8 + \cdots$$

que é uma série de potências com os coeficientes quase todos nulos.

A soma e o produto das séries de potências são generalizações imediatas das operações correspondentes com polinómios.

Voltando ao problema inicial, que se pode generalizar, considere-se a equação

$$a + b + c \;=\; r \tag{3.5}$$

onde $a, b, c \in \{2, 3, 4\}$ e $r = 6, 7, \ldots, 12$. Para cada r fixado, seja a_r o número de soluções inteiras da equação (3.5). Então a_r é igual ao coeficiente da potência de ordem r da função geradora ordinária para este problema

$$\begin{aligned} g(x) &= (x^2 + x^3 + x^4)^3 \\ &= x^6 + 3x^7 + 6x^8 + 7x^9 + 6x^{10} + 3x^{11} + x^{12} \end{aligned}$$

Exemplo 3.6 Dado um conjunto com n objectos o número de possíveis escolhas de r objectos ($0 \leq r \leq n$) é dado por

$$C_r^n \;=\; \binom{n}{r} \;=\; \frac{n!}{r!(n-r)!}$$

A função geradora ordinária para este problema combinatório é

$$\begin{aligned} g(x) &= \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n \\ &= (1+x)^n \end{aligned}$$

Exemplo 3.7 *Determinar a função geradora ordinária na qual o coeficiente de x^r seja o número de soluções inteiras não negativas da equação*

$$2a + 3b + 5c \;=\; r$$

Resolução. Escrevendo $x = 2a$, $y = 3b$ e $z = 5c$ procura-se então o número de soluções inteiras não negativas da equação

$$x + y + z \;=\; r$$

onde $x \in \{0,2,4,6,8,\ldots\}$, $y \in \{0,3,6,9,\ldots\}$ e $z \in \{0,5,10,15,20,\ldots\}$. Então, associando às variáveis x, y, z as séries de potências

$$\begin{aligned} g_x(t) &= 1 + t^2 + t^4 + t^6 + \cdots \\ g_y(t) &= 1 + t^3 + t^6 + t^9 + \cdots \\ g_z(t) &= 1 + t^5 + t^{10} + t^{15} + \cdots \end{aligned}$$

a função geradora ordinária associada a este problema é dada por

$$\begin{aligned} g(t) &= (1 + t^2 + t^4 + t^6 + \cdots)(1 + t^3 + t^6 + t^9 + \cdots)(1 + t^5 + t^{10} + t^{15} + \cdots) \\ &= \frac{1}{1-t^2}\,\frac{1}{1-t^3}\,\frac{1}{1-t^5} \end{aligned}$$

Exemplo 3.8 O número de soluções inteiras não negativas da equação

$$a + b + c \;=\; 4$$

é dado pelo coeficiente de x^4 na função

$$g(x) \;=\; (1 + x + x^2 + x^3 + x^4)^3$$

ou na série de potências

$$h(x) \;=\; (1 + x + x^2 + x^3 + x^4 + x^5 + \cdots)^3$$

No que se segue apresentam-se alguns resultados gerais que facilitam a determinação do coeficiente a_n da potência x^n na função geradora ordinária.

Teorema 3.9

1. *Seja a_r o coeficiente de x^r na função geradora ordinária*

   $$g(x) \;=\; (1 + x + x^2 + x^3 + x^4 + x^5 + \cdots)^n$$

   Então $a_r = C_r^{r+n-1}$.
2. $(1 - x^m)^n \;=\; 1 - C_1^n x^m + C_2^n x^{2m} - \cdots + (-1)^n x^{nm}$
3. $(1 + x + x^2 + x^3 + \cdots + x^{m-1})^n \;=\; (1 - x^m)^n (1 + x + x^2 + \cdots)^n$

Demonstração: (1) Tendo em conta o teorema binomial de Newton, tem-se o seguinte

$$\begin{aligned} g(x) &= \frac{1}{(1-x)^n} \;=\; (1-x)^{-n} \\ &= \sum_{r=0}^{\infty} \binom{-n}{r} (-1)^r x^r \end{aligned}$$

onde

$$\begin{aligned}\binom{-n}{r} &= \frac{(-n)(-n-1)(-n-2)\cdots(-n-r+1)}{r!} \\ &= (-1)^r\,\frac{n(n+1)(n+2)\cdots(n+r-1)}{r!} \\ &= (-1)^r\,\frac{(n+r-1)\cdots(n+1)n(n-1)!}{r!(n-1)!} \\ &= (-1)^r\binom{n+r-1}{r} \;\equiv\; (-1)^r\binom{n+r-1}{n-1}\end{aligned}$$

Logo, substituindo na equação anterior, vem

$$g(x) \;\equiv\; (1+x+x^2+\ldots)^n \;=\; \sum_{r=0}^{\infty}\binom{n+r-1}{n-1}x^r$$

e, portanto,

$$a_r \;=\; \binom{n+r-1}{n-1} \;\equiv\; \binom{n+r-1}{r}$$

(2) Fazendo $t = (-x^m)$ no desenvolvimento binomial de $(1+t)^n$ obtém-se o resultado pretendido.

(3) É fácil verificar formalmente que se tem

$$1+x+x^2+\cdots+x^{m-1} \;=\; (1-x^m)(1+x+x^2+x^3+\cdots)$$

e, portanto, tomando a potência de ordem n de ambos os membros obtém-se a igualdade apresentada. □

Da primeira alínea do teorema anterior resulta ainda o seguinte:

Corolário 3.10 *A função $g(x)$ é a função geradora associada ao problema da determinação do número de soluções inteiras não negativas da equação*

$$y_1 + y_2 + \cdots + y_n \;=\; r$$

que é, assim, igual a C_{n-1}^{r+n-1}.

Exemplo 3.11 *Determinar o número de soluções inteiras da equação*

$$a+b+c+d \;=\; 27$$

onde cada variável toma valores entre 3 e 8.

Resolução. O número de soluções procurado é igual ao coeficiente de x^{27} na função geradora ordinária associada a este problema, que é dada por

$$\begin{aligned}g(x) &= (x^3+x^4+x^5+x^6+x^7+x^8)^4 \\ &= x^{12}(1+x+x^2+x^3+x^4+x^5)^4\end{aligned}$$

O número de soluções pretendido é igual ao coeficiente de x^{15} da função

$$h(x) \;=\; (1+x+x^2+x^3+x^4+x^5)^4$$

Tendo em conta o teorema anterior

$$\begin{aligned} h(x) &= (1+x+x^2+x^3+x^4+x^5)^4 \\ &= (1-x^6)^4(1+x+x^2+x^3+\cdots)^4 \end{aligned}$$

Pela alínea (2) do teorema anterior

$$(1-x^6)^4 \;=\; 1-\binom{4}{1}x^6+\binom{4}{2}x^{12}+\cdots+x^{24}$$

e pela alínea (1) do mesmo teorema

$$(1+x+x^2+x^3+\cdots)^4 \;=\; 1+\binom{4}{1}x+\binom{5}{2}x^2+\binom{6}{3}x^3+\cdots$$

Então o coeficiente de x^{15} no produto é igual a

$$\begin{aligned} \sum_{i+j=15} a_i b_j &= a_0b_{15}+a_6b_9+a_{12}b_3 \\ &= 1\binom{18}{15}-\binom{4}{1}\cdot\binom{12}{9}+\binom{4}{2}\cdot\binom{6}{3} \\ &= \frac{18!}{15!3!}-\frac{4!}{3!1!}\,\frac{12!}{9!3!}+\frac{4!}{2!2!}\,\frac{6!}{3!3!} \\ &= 3\times 17\times 16-4\times 2\times 11\times 10+2\times 3\times 5\times 4 \;=\; 56 \end{aligned}$$

Exemplo 3.12 *Determinar o coeficiente de x^{24} de*

$$(x^3+x^4+x^5+\cdots)^5$$

Resolução. Visto que

$$(x^3+x^4+x^5+\cdots)^5 \;=\; x^{15}(1+x+x^2+\cdots)^5$$

então o número pretendido é igual ao coeficiente de x^9 na função

$$g(x) \;=\; (1+x+x^2+x^3+x^4+x^5+\cdots)^5$$

que, de acordo com o teorema (3.9), é igual a

$$\binom{5+9-1}{9} \;=\; \binom{13}{9} \;=\; \frac{13!}{9!4!} \;=\; 13\times 11\times 5 \;=\; 711$$

Se

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^x + \cdots$$

for a série de potências de uma função $g(x)$, então $g(x)$ é a função geradora ordinária da sucessão $(a_n)_{n=0,1,2,\ldots}$. A partir desta função geradora é possível construir as funções geradoras de outras sucessões relacionadas com aquela.

Teorema 3.13 *Se $g(x)$ for a função geradora ordinária associada à sucessão $(a_n)_{n=0,1,2,\ldots}$ e $h(x)$ for a função geradora associada à sucessão $(b_n)_{n=0,1,2,\ldots}$, então*

1. *$\alpha g(x) + \beta h(x)$ é a função geradora ordinária associada à sucessão $(\alpha a_n + \beta b_n)_{n=0,1,2,\ldots}$.*
2. *$(1-x)g(x)$ é a função geradora associada à sucessão $(a_n - a_{n-1})_{n=0,1,2,\ldots}$ (onde se faz $a_{-1} = 0$).*
3. *$(1 + x + x^2 + \cdots)g(x)$ é a função geradora da sucessão*

$$(a_0 + a_1 + \cdots + a_n)_{n=0,1,2,\ldots}$$

4. *$g(x) \cdot h(x)$ é a função geradora da sucessão*

$$(a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0)_{n=0,1,2,\ldots}$$

5. *$xg'(x)$ é a função geradora da sucessão $(na_n)_{n=0,1,2,\ldots}$ onde $g'(x)$ é a derivada de g relativamente a x.*

Demonstração: Sendo

$$\begin{aligned} g(x) &= \sum_{j=0}^{\infty} a_j\, x^j \\ h(x) &= \sum_{j=0}^{\infty} b_j\, x^j \end{aligned}$$

então

1.

$$\alpha g(x) + \beta h(x) = \sum_{j=0}^{\infty} (\alpha a_j + \beta b_j) x^j$$

2.

$$\begin{aligned} (1-x)g(x) &= \sum_{j=0}^{\infty} a_j\, x^j - \sum_{j=0}^{\infty} a_j\, x^{j+1} \\ &= a_0 + (a_1 - a_0)x + (a_2 - a_1)x^2 + \cdots + (a_n - a_{n-1})x^n + \cdots \end{aligned}$$

3.

$$\begin{aligned}(1+x+x^2+\cdots)g(x) &= (1+x+x^2+\cdots)(a_0+a_1x+a_2x^2+\cdots)\\ &= a_0+(a_0+a_1)x+(a_0+a_1+a_2)x^2+\cdots\end{aligned}$$

4.

$$g(x)h(x) \;=\; \sum_{n=0}^{\infty}\left(\sum_{j=0}^{n} a_j b_{n-j}\right)x^n$$

5. Sendo

$$g'(x) \;=\; \sum_{j=1}^{\infty} j\,a_j\,x^{j-1}$$

vem

$$xg'(x) \;=\; \sum_{j=1}^{\infty} j\,a_j\,x^{j}$$

Os resultados obtidos provam cada uma das alíneas do teorema. □

É fácil verificar que

$$(1-x)(1+x+x^2+x^3+\cdots) \;=\; 1$$

e, portanto,

$$g(x) \;=\; 1+x+x^2+x^3+\cdots \;=\; \frac{1}{1-x}$$

(a série de potências converge absolutamente para $|x|<1$). A função $g(x)$ é a função geradora da sucessão constante $a_n=1$, $n=0,1,2,\ldots$ enquanto que

$$h(x) \;=\; g(x)^k \;=\; \frac{1}{(1-x)^k}$$

tendo em conta o teorema 3.9, é a função geradora da sucessão

$$\left(\binom{n+k-1}{n}\right)_{n=0,1,2,3,\ldots}$$

Exemplo 3.14 *Determinar a função geradora associada à sucessão*

$$a_n \;=\; 3n+5n^2, \quad n=0,1,2,\ldots$$

Resolução. A função

$$g(x) \;=\; \frac{1}{1-x}$$

é a função geradora ordinária para a sucessão constante $a_n = 1,\ n = 0, 1, 2, \ldots$ Tendo em conta a alínea 5. do teorema 3.13

$$xg'(x) \ = \ x\ \frac{1}{(1-x)^2} \ = \ \frac{x}{(1-x)^2}$$

é a função geradora da sucessão $(n)_{n=0,1,2,3,\ldots}$. Aplicando este princípio uma vez mais, vem

$$x\left(\frac{x}{(1-x)^2}\right)' \ = \ \frac{x(1+x)}{(1-x)^3}$$

obtém-se a função geradora da sucessão $(n^2)_{n=0,1,2,\ldots}$. Então, tendo agora em conta a primeira alínea do mesmo teorema,

$$\begin{aligned} h(x) &= 3xg'(x) + 5x[xg'(x)]' \\ &= \frac{3x}{(1-x)^2} + \frac{5x(1+x)}{(1-x)^3} \\ &= \frac{2x(4+x)}{(1-x)^3} \end{aligned}$$

é a função geradora associada à sucessão $(3n + 5n^2)_{n=0,1,2,\ldots}$.

Exercícios 3.2.1

1. *Determinar as funções geradoras ordinárias associadas às seguintes sucessões*
   (a) $(1, 1, 1, 1, 0, 0, 0, \ldots)$
   (b) $(1, 1, 1, 1, 1, 0, 0, 0, \ldots)$
   (c) $(0, 0, 0, 0, 1, 1, 1, 1, \ldots)$
   (d) $(1, -1, 1, -1, 1, -1, \ldots)$
   (e) $(1, 2, 3, 4, \ldots)$
   (f) $(1, -2, 3, -4, \ldots)$
2. *Determinar as sucessões associadas às seguintes funções geradoras*
   (a) $g_1(x) = (2 + x)^4$
   (b) $g_2(x) = x^2 + \mathrm{e}^x$
   (c) $g_3(x) = x^3/(1 - x)$
3. *Determinar o coeficiente de* x^7 *na função*

$$g(x) \ = \ (1-x)^k$$

   quando $k = 9$ *e quando* $k = -9$.

4. *Determinar o coeficiente de* x^7 *na função*

$$g(x) \;=\; (1+x)^k$$

quando $k = 9$ *e quando* $k = -9$.

5. *Determinar o coeficiente de* x^{23} *na função*

$$h(x) \;=\; (x^3 + x^4 + x^5 + \cdots)^5$$

6. *Determinar a função geradora ordinária associada ao problema combinatório de determinar o número de soluções inteiras não negativas da equação*

$$a + b + c + d \;=\; r$$

7. *Determinar a função geradora ordinária associada ao problema da determinação das soluções inteiras não negativas da equação*

$$3a + 2b + 4c + 2d \;=\; r$$

8. *Determinar o número de soluções inteiras da equação*

$$p + q + r + s \;=\; 27$$

onde cada variável toma valores entre 3 e 8.

9. *Determinar o número de soluções da equação*

$$x_1 + x_2 + \cdots + x_n \;=\; r$$

onde cada variável toma apenas os valores 0 ou 1.

10. *Determinar o número possível de formas de prefazer um total de 13 pontos quando se atiram 3 dados distintos* $A, B,$ *e* C.

11. *Determinar o número de soluções inteiras da equação*

$$a + b + c + d + e + f \;=\; 20$$

onde $a \in \{1, 2, 3, 4, 5\}$ *e as outras variáveis são maiores ou iguais a 2.*

12. *Determinar a função geradora ordinária associada ao problema da determinação do número de soluções inteiras da desigualdade*

$$a + b + c \;\leq\; r$$

onde cada variável toma valores entre 2 e 5.

13. *Determinar as funções geradoras associadas às sucessões*
    (a) $(a_n)_{n=0,1,2,\ldots}$ *com* $a_n = k^n$
    (b) $(b_n)_{n=0,1,2,\ldots}$ *com* $b_n = nk^n$
    (c) $(c_n)_{n=0,1,2,\ldots}$ *com* $c_n = k + 2k^2 + 3k^3 + \cdots + nk^n$

3.2.1 Relações de recorrência e funções geradoras

Dada uma sucessão $(a_n)_{n=0,1,2,\ldots}$ seja

$$g(x) \;=\; a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

a função geradora associada aquela sucessão. Esta função geradora $g(x)$ contém toda a informação relativa à sucessão $(a_n)_{n=0,1,2,\ldots}$ sendo muitas vezes mais fácil de manipular do que a própria sucessão.

O termo geral da sucessão, a_n, pode ser recuperado a partir do coeficiente de x^n no desenvolvimento em série de potências de $g(x)$. Muitas vezes é possível obter $g(x)$ algebricamente e então, depois de expressar esta função em série de potências, obtêm-se os termos a_n da sucessão correspondente.

Exemplo 3.15 *Resolver a relação de recorrência*

$$a_n \;=\; 2a_{n-1}$$

usando a função geradora ordinária associada à sucessão $(a_n)_{n\in\mathbf{N}}$.
Resolução. Seja

$$g(x) \;=\; a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

a função geradora ordinária associada à sucessão $(a_n)_{n=0,1,2,\ldots}$. Multiplicando ambos os membros da relação de recorrência por x^n, vem

$$a_n x^n \;=\; 2a_{n-1}x^n, \quad n = 1, 2, 3, \ldots$$

Então, fazendo $n = 1, 2, 3, \ldots$, sucessivamente,

$$\begin{array}{rcl} a_1 x & = & 2a_0 x \\ a_2 x^2 & = & 2a_1 x^2 \\ a_3 x^3 & = & 2a_2 x^3 \\ & \vdots & \\ a_n x^n & = & 2a_{n-1} x^n \\ & \vdots & \end{array}$$

Somando, ordenadamente, todas estas igualdades, vem

$$a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots \;=\; 2(a_0 x + a_1 x^2 + a_2 x^3 + \cdots + a_{n-1} x^n + \cdots)$$

ou seja,

$$-a_0 + (a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots) \;=\; 2x(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + \cdots)$$

e, portanto,

$$-a_0 + g(x) \;=\; 2xg(x)$$

donde

$$g(x) \;=\; \frac{a_0}{1-2x}$$

Desenvolvendo $g(x)$ em série de potências, vem

$$g(x) \;=\; a_0\left(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots + 2^nx^n + \cdots\right)$$

e, portanto,

$$a_n \;=\; a_0 \cdot 2^n, \quad n = 0, 1, 2, 3, \ldots$$

é a solução da relação de recorrência dada.

Exemplo 3.16 *Resolver a relação de recorrência*

$$a_n \;=\; 2a_{n-1} - \frac{n}{3}\,, \quad n = 0, 1, 2, 3, \ldots$$

onde $a_0 = 1$.
Resolução. Visto que $a_0 = 1$, a função geradora ordinária associada à sucessão é da forma

$$g(x) \;=\; 1 + a_1x + a_2x^2 + \cdots$$

Multiplicando por x^n a relação de recorrência, vem

$$a_nx^n \;=\; 2a_{n-1}x^n - \frac{n}{3}\,x^n$$

e, portanto, fazendo $n = 1, 2, 3, \ldots$, sucessivamente,

$$\begin{array}{rcl} a_1x &=& 2x - \frac{1}{3}\,x \\ a_2x^2 &=& 2a_1x^2 - \frac{2}{3}\,x^2 \\ a_3x^3 &=& 2a_2x^3 - \frac{3}{3}\,x^3 \\ & \vdots & \\ a_nx^n &=& 2a_{n-1}x^n - \frac{n}{3}\,x^n \\ & \vdots & \end{array}$$

Somando ordenadamente estas equações

$$\begin{array}{rcl} a_1x + a_2x^2 + \cdots + a_nx^n + \cdots &=& 2(x + a_1x^2 + a_2x^3 + \cdots + a_{n-1}x^n + \cdots) - \\ & & \dfrac{1}{3}\left(x + 2x^2 + \cdots + nx^n + \cdots\right) \end{array}$$

donde

$$g(x) - 1 \;=\; 2xg(x) - \frac{x}{3}\left(1 + 2x + 3x^2 + \cdots + nx^{n-1} + \cdots\right)$$

ou seja,

$$g(x) - 1 \;=\; 2xg(x) - \frac{x}{3}\, f(x)$$

onde

$$\begin{aligned} f(x) &= 1 + 2x + 3x^2 + \cdots + nx^{n-1} + \cdots \\ &= \left(x + x^2 + x^3 + \cdots + x^n + \cdots\right)' \\ &= \left(-1 + \frac{1}{1-x}\right)' \;=\; \left(\frac{x}{1-x}\right)' \;=\; \frac{1}{(1-x)^2} \end{aligned}$$

Então,

$$g(x) - 1 \;=\; 2xg(x) - \frac{x}{3}\,\frac{1}{(1-x)^2}$$

e, portanto,

$$(1-2x)\, g(x) \;=\; 1 - \frac{x}{3(1-x)^2}$$

donde,

$$g(x) \;=\; \frac{3(1-x)^2 - x}{3(1-x)^2(1-2x)} \;=\; \frac{3 - 7x + 3x^2}{3(1-x)^2(1-2x)}$$

Decompondo a fracção do lado direito em elementos simples, obtém-se

$$g(x) \;=\; \frac{1}{3}\left(\frac{1}{1-x} + \frac{1}{(1-x)^2} + \frac{1}{1-2x}\right)$$

Como

$$\begin{aligned} \frac{1}{1-x} &= 1 + x + x^2 + x^3 + \cdots + x^n + \cdots \\ \frac{1}{(1-x)^2} &= \left(\frac{1}{1-x}\right)' \;=\; 1 + 2x + 3x^2 + \cdots + (n+1)x^n + \cdots \\ \frac{1}{1-2x} &= 1 + 2x + 2^2x^2 + \cdots + 2^n x^n + \cdots \end{aligned}$$

então o termo a_n, que é o coeficiente de x^n no desenvolvimento de $g(x)$, é dado por

$$a_n \;=\; \frac{1}{3}\left(1 + (n+1) + 2^n\right) \;=\; \frac{2 + n + 2^n}{3}$$

Exercícios 3.2.2

1. *Determinar a função geradora ordinária para a relação de recorrência*

$$a_n \;=\; c_1 a_{n-1} + c_2 a_{n-2}$$

com $a_0 = \alpha$ *e* $a_1 = \beta$ *onde* c_1, c_2, α, β *são constantes dadas.*

2. *Sendo*

$$g(x) \;=\; \frac{2}{(1-x)(1-2x)}$$

a função geradora ordinária associada a uma relação de recorrência que envolve os termos da sucessão $(a_n)_{n=0,1,2,\ldots}$*, determinar a forma do termo geral* a_n*.*

3. *Resolver a relação de recorrência*

$$a_n \;=\; a_{n-2} + 4n$$

com as condições iniciais $a_0 = 3$ *e* $a_1 = 2$*, usando uma função geradora ordinária apropriada.*

4. *Determinar a função geradora ordinária para a relação de recorrência*

$$a_{n+1} \;=\; \alpha a_n + b^n$$

com a condição inicial $a_0 = c$ *onde* α, b *e* c *são constantes e, então, obter o termo geral* a_n*.*

5. *Resolver as relações de recorrência que se seguem usando o método da função geradora ordinária.*

   (a) $a_n = 4a_{n-2}$ *para* $n \geq 2$*;* $a_0 = 0, a_1 = 1$

   (b) $a_n = a_{n-1} + a_{n-2}$ *para* $n \geq 2$*;* $a_0 = 1, a_1 = 3$

   (c) $a_n = a_{n-1} + 9a_{n-2} - 9a_{n-3}$ *para* $n \geq 3$*;* $a_0 = 0, a_1 = 1, a_2 = 2$

   (d) $a_n = 8a_{n-1} - 16a_{n-2}$ *para* $n \geq 2$*;* $a_0 = -1, a_1 = 0$

   (e) $a_n = 3a_{n-2} - 2a_{n-3}$ *para* $n \geq 3$*;* $a_0 = 1, a_1 = 0, a_2 = 0$

   (f) $a_n = 5a_{n-1} - 6a_{n-2} - 4a_{n-3} + 8a_{n-4}$ *para* $n \geq 4$*;* $a_0 = 0, a_1 = 1, a_2 = 1, a_3 = 2$

   (g) $a_n = 2a_{n-1} - 4a_{n-2} + 8a_{n-3} + 16a_{n-4}$ *para* $n \geq 4$*;* $a_0 = 1, a_1 = 2, a_2 = 1, a_3 = 2$

6. *Determinar a função geradora ordinária da sucessão de cubos* $0, 1, 8, \ldots, n^3, \ldots$.

7. *Seja* $a_0, a_1, \ldots, a_n, \ldots$ *a sucessão definida por* $a_n = n^3$ *para* $n = 0, 1, 2, \ldots$. *Mostrar que*

$$a_n = a_{n-1} + 3n^2 - 3n + 1 \quad \text{para} \quad n = 1, 2, \ldots$$

e, usando esta relação de recorrência, determinar a função geradora ordinária para a sucessão.

8. *Seja* $a_0, a_1, \ldots, a_n, \ldots$ *a sucessão definida por* $a_n = C_2^n$ *para* $n = 0, 1, 2, \ldots$. *Determinar a função geradora ordinária para a sucessão.*

3.2.2 Relações de recorrência lineares homogéneas

Não há regras gerais para resolver uma relação de recorrência arbitrária. Para certas classes de relações de recorrência, contudo, há métodos adequados que permitem resolvê-las: é o caso das relações de recorrência lineares homogéneas de coeficientes constantes. Estas relações de recorrência têm a forma geral seguinte

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \quad n = k, k+1, \ldots \tag{3.6}$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_k$ são constantes dadas. Visto que o termo a_n é determinado pelos k termos da sucessão que o antecedem a equação (3.6) diz-se uma relação de recorrência de ordem k. Supõe-se $\alpha_k \neq 0$ pois de contrário a relação de recorrência seria de ordem inferior a k. A relação de recorrência diz-se homogénea por não ter termo independente.

Por exemplo, a relação

$$a_n \;=\; 3\,(a_{n-1})^2 + a_{n-2}, \quad n = 2, 3, 4, \ldots$$

não é uma relação de recorrência linear, embora seja homogénea. Por outro lado,

$$a_n \;=\; (n+2)a_{n-1} + 2a_{n-2}, \quad n = 2, 3, 4, \ldots$$

é uma relação de recorrência linear, mas os seus coeficientes não são constantes – dependem de n.

A sucessão $(a_n)_{n=0,1,2,\ldots}$ fica completamente determinada pela equação (3.6) a partir do momento em que sejam dados os valores iniciais a_0, $a_1, \ldots$, a_{k-1}. Para resolver a equação (3.6) procuram-se soluções da forma

$$a_n \;=\; x^n, \quad n = 0, 1, 2, 3, \ldots$$

onde x é um número a determinar convenientemente. Visto que

$$a_{n-1} \;=\; x^{n-1}, \;\; a_{n-2} \;=\; x^{n-2}, \;\; \ldots, \;\; a_{n-k} \;=\; x^{n-k}$$

então, por substituição na equação (3.6), obtém-se

$$x^n - \alpha_1 x^{n-1} - \alpha_2 x^{n-2} - \cdots - \alpha_k x^{n-k} \;=\; 0$$

ou seja,

$$x^{n-k}\left(x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - \cdots - \alpha_k\right) \;=\; 0$$

Ora x não pode ser nulo pois isso conduziria ao anulamento de todos os termos da sucessão; consequentemente, sendo $x \neq 0$, obtém-se a equação algébrica

$$x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - \cdots - \alpha_k \ = \ 0 \tag{3.7}$$

que é conhecida por **equação característica** associada à equação de recorrência (3.6). As soluções da equação característica designam-se por **raízes características** da relação de recorrência (3.6).

A equação (3.7) possui k raízes reais ou complexas, iguais ou distintas. No entanto, como $\alpha_k \neq 0$, por hipótese, todas as raízes são diferentes de zero.

Exemplo 3.17 A relação de recorrência de Fibonaci

$$f_n \ = \ f_{n-1} + f_{n-2}$$

tem associada a equação característica

$$x^2 - x - 1 \ = \ 0$$

cujas raízes características são

$$q_1 \ = \ \frac{1+\sqrt{5}}{2} \quad \text{e} \quad q_2 \ = \ \frac{1-\sqrt{5}}{2}$$

Pode então enunciar-se o seguinte resultado geral

Teorema 3.18 *Seja q um número real ou complexo não nulo. Então $a_n = q^n$ é solução da relação (3.6) se e só se q for uma raiz característica daquela equação.*

Sejam $\varphi_1(n)$ e $\varphi_2(n)$ duas soluções da relação de recorrência (3.6) e sejam c_1, c_2 duas constantes. Então,

$$c_1\varphi_1(n) + c_2\varphi_2(n)$$

é também solução da relação de recursão (3.6). Para verificar esta afirmação, note-se, antes de mais que φ_1 e φ_2 satisfazem as equações

$$\begin{aligned} \varphi_1(n) &= \alpha_1\varphi_1(n-1) + \alpha_2\varphi_1(n-2) + \cdots + \alpha_k\varphi_1(n-k) \\ \varphi_2(n) &= \alpha_1\varphi_2(n-1) + \alpha_2\varphi_2(n-2) + \cdots + \alpha_k\varphi_2(n-k) \end{aligned}$$

Multiplicando a primeira equação por c_1 e a segunda por c_2 e somando ordenadamente, vem

$$\begin{aligned} c_1\varphi_1(n) + c_2\varphi_2(n) &= c_1\alpha_1\varphi_1(n-1) + c_1\alpha_2\varphi_1(n-2) + \cdots \\ &\quad + c_1\alpha_k\varphi_1(n-k) + \\ &\quad c_2\alpha_1\varphi_2(n-1) + c_2\alpha_2\varphi_2(n-2) + \cdots \\ &\quad + c_2\alpha_k\varphi_2(n-k) \\ &= \alpha_1\left[c_1\varphi_1(n-1) + c_2\varphi_2(n-1)\right] + \alpha_2\left[c_1\varphi_1(n-2)\right. \\ &\quad \left. + c_2\varphi_2(n-2)\right] + \cdots + \\ &\quad \alpha_k\left[c_1\varphi_1(n-k) + c_2\varphi_2(n-k)\right] \end{aligned}$$

o que mostra que

$$a_n \;=\; c_1\varphi_1(n) + c_2\varphi_2(n)$$

é ainda solução da relação (3.6).

Mais geralmente, de forma semelhante, pode provar-se que se $\varphi_1(n)$, $\varphi_2(n)$, $\ldots$, $\varphi_k(n)$ forem soluções da equação (3.6) e $c_1, c_2, \ldots, c_k$ forem constantes arbitrárias, então

$$c_1\varphi_1(n) + c_2\varphi_2(n) + \cdots + c_k\varphi_k(n) \tag{3.8}$$

é também solução da mesma equação. Dir-se-á que tal solução é a **solução geral** da equação (3.6) se todas as possíveis soluções daquela equação se puderem expressar na forma (3.8) para uma conveniente escolha das constantes $c_1, c_2, \ldots, c_k$.

Teorema 3.19 *Se as raízes características $q_1, q_2, \ldots, q_k$ da equação*

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}$$

forem todas distintas, então

$$a_n \;=\; c_1 q_1^n + c_2 q_2^n + \cdots + c_k q_k^n$$

é a solução geral daquela equação.

Demonstração: Seja b_n $(n = 0, 1, 2, 3, \ldots)$ uma solução qualquer da relação de recorrência. Então a sucessão b_n $(n = 0, 1, 2, 3, \ldots)$ fica completamente determinada pelos seus valores iniciais $b_0, b_1, \ldots, b_{k-1}$. Mostrar-se-á que é possível determinar as constantes $c_1, c_2, \ldots, c_k$ (de uma só maneira) de tal forma que b_n se pode expressar

na forma indicada no teorema. Para isso é necessário mostrar que as constantes $c_1, c_2, \ldots, c_k$ podem ser escolhidas de tal forma que

$$\begin{cases} c_1 + c_2 + \cdots + c_k \;=\; b_0 \\ c_1 q_1 + c_2 q_2 + \cdots + c_k q_k \;=\; b_1 \\ \cdots\cdots\cdots \\ c_1 q_1^{k-1} + c_2 q_2^{k-1} + \cdots + c_k q_k^{k-1} \;=\; b_{k-1} \end{cases} \tag{3.9}$$

Neste sistema há k equações lineares nas k incógnitas $c_1, c_2, \ldots, c_k$. A matriz dos coeficientes deste sistema

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ q_1 & q_2 & \cdots & q_k \\ \vdots & \vdots & & \vdots \\ q_1^{k-1} & q_2^{k-1} & \cdots & q_k^{k-1} \end{bmatrix}$$

é conhecida por *matriz de Vandermonde*. O seu determinante, dado por

$$\prod_{1 \le i < j \le k} (q_j - q_i)$$

é constituído por

$$(k-1) + (k-2) + \cdots + [k - (k-1)] \;=\; \frac{(k-1)k}{2} \;=\; \binom{k}{2}$$

factores da forma $q_j - q_i$ com $1 \le i < j \le k$. Visto que para $i \neq j$ se tem sempre, por hipótese, $q_j \neq q_i$, então o determinante da matriz dos coeficientes do sistema (3.9) é diferente de zero. Logo o sistema é possível e determinado, ou seja, admite uma e uma só solução, como se pretendia mostrar. □

Exemplo 3.20 *Resolver a relação de recorrência*

$$a_n \;=\; 2a_{n-1} + a_{n-2} - 2a_{n-3}, \quad n = 3, 4, 5, \ldots$$

com as condições iniciais $a_0 = 1$, $a_1 = 2$ *e* $a_2 = 0$.
Resolução. A equação característica desta relação de recursão é a seguinte:

$$x^3 - 2x^2 - x + 2 \;=\; 0$$

cujas raízes são as seguintes

$$q_1 = 1, \quad q_2 = -1, \quad q_3 = 2$$

Então

$$a_n \;=\; c_1\, 1^n + c_2\, (-1)^n + c_3\, 2^n$$

é a solução geral da relação de recursão dada. Tendo em conta as condições iniciais, as constantes c_1, c_2 e c_3 deverão satisfazer o seguinte sistema de equaçõees lineares

$$\begin{cases} c_1 + c_2 + c_3 &= 1 \\ c_1 - c_2 + 2c_3 &= 2 \\ c_1 + c_2 + 4c_k &= 0 \end{cases}$$

Visto que

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & -1 & 2 \\ 1 & 1 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & -2 & 1 \\ 0 & 0 & 3 \end{vmatrix} = -6$$

então este sistema de equações tem uma e uma só solução, que é

$$c_1 = 2, \quad c_2 = -2/3, \quad c_3 = -1/3$$

A solução procurada é então a seguinte

$$a_n = 2 - \frac{2}{3}(-1)^n - \frac{1}{3}2^n, \quad n = 0, 1, 2, 3, \ldots$$

3.2.2.1 Equação característica com raízes múltiplas

Voltando à equação de recorrência (3.6), pode acontecer que as raízes q_1, q_2, ..., q_k da equação característica não sejam todas distintas. Neste caso

$$a_n = c_1 q_1^n + c_2 q_2^n + \cdots + c_k q_k^n \tag{3.10}$$

não é a solução geral da equação de recorrência dada.

Por exemplo, a equação de recorrência

$$a_n = 4a_{n-1} - 4a_{n-2} \tag{3.11}$$

tem a seguinte equação característica

$$x^2 - 4x + 4 = 0$$

que tem uma raiz dupla igual a 2. Neste caso (3.10) toma a forma

$$a_n = c_1 2^n + c_2 2^n = (c_1 + c_2)2^n = c\,2^n$$

onde $c = c_1 + c_2$ é uma nova constante. Então, de facto, há apenas uma constante não sendo possível, em geral, escolher c de forma que as duas condições iniciais sejam simultaneamente satisfeitas. Supondo, por exemplo, que as condições iniciais são $a_0 = 1$ e $a_1 = 3$ obter-se-ia

$$\begin{cases} c &= 1 \\ 2c &= 3 \end{cases}$$

sistema este que é, evidentemente, impossível. Então,

$$a_n \;=\; c\,2^n, \quad n = 0, 1, 2, 3, \ldots$$

não é a solução geral da equação de recorrência (3.11). Neste caso é necessário encontrar outra solução associada à raiz característica 2. Esta nova solução é da forma

$$a_n \;=\; n\,2^n$$

De facto, tem-se

$$\begin{aligned} 4a_{n-1} - 4a_{n-2} &= 4(n-1)2^{n-1} - 4(n-2)2^{n-2} \\ &= 4[(n-1)2^{n-1} - (n-2)2^{n-2}] \\ &= 4\,2^{n-2}[2(n-1) - (n-2)] \;=\; 4n2^{n-2} \;=\; n\,2^n \;=\; a_n \end{aligned}$$

o que mostra que $n2^n$ satisfaz a equação de recorrência dada. Então

$$a_n \;=\; c_1\,2^n + c_2\,n\,2^n \;=\; (c_1 + c_2\,n)\,2^n$$

é, como se verá, a solução geral da relação de recorrência considerada. Para o confirmar basta verificar que quaisquer que sejam os valores de a_0 e a_1 é sempre possível determinar as constantes c_1 e c_2 e de uma só maneira. Para $n = 0$ e $n = 1$, vem

$$\begin{cases} c_1 \;=\; a_0 \\ 2(c_1 + c_2) \;=\; a_1 \end{cases}$$

que é um sistema nas incógnitas c_1 e c_2 sempre possível e determinado, quaisquer que sejam os valores atribuídos a a_0 e a_1:

$$c_1 \;=\; a_0, \quad c_2 \;=\; \frac{1}{2}(a_1 - 2a_0)$$

A solução procurada é então

$$a_n \;=\; a_0 2^n + \frac{1}{2}(a_1 - 2a_0)n2^n \;=\; \left(a_0 + \frac{1}{2}(a_1 - 2a_0)n\right)2^n, \quad n = 0, 1, 2, 3, \ldots$$

Esta ideia pode generalizar-se a uma relação de recorrência de ordem qualquer superior a 2. Considere-se a relação de recorrência

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \;\; \alpha_k \neq 0, \;\; n = k, k+1, \ldots \quad (3.12)$$

cuja equação característica é

$$p(x) \;=\; x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - \cdots - \alpha_k \;=\; 0$$

Suponha-se que q é, por exemplo, uma raiz tripla desta equação, ou seja, que se tem a seguinte decomposição

$$p(x) \;=\; (x-q)^3 r(x)$$

onde $r(x)$ é um polinómio de grau $k-3$. Então, para cada $n = k, k+1, \ldots$, q é uma raiz tripla do polinómio $p_n(x)$ definido por

$$\begin{aligned} p_n(x) &= x^{n-k}p(x) \\ &= x^n - \alpha_1 x^{n-1} - \alpha_2 x^{n-2} - \cdots - \alpha_k x^{n-k} \end{aligned}$$

Por outro lado, q é uma raiz dupla da primeira derivada de $p_n(x)$

$$p_n'(x) \;=\; nx^{n-1} - \alpha_1(n-1)x^{n-2} - \alpha_2(n-2)x^{n-3} - \cdots - \alpha_k(n-k)x^{n-k-1}$$

e, consequentemente, é uma raiz dupla do polinómio

$$xp_n'(x) \;=\; nx^n - \alpha_1(n-1)x^{n-1} - \alpha_2(n-2)x^{n-2} - \cdots - \alpha_k(n-k)x^{n-k}$$

Em particular, para $x = q$, vem

$$nq^n \;=\; \alpha_1(n-1)q^{n-1} + \alpha_2(n-2)q^{n-2} + \cdots + \alpha_k(n-k)q^{n-k}$$

o que mostra que

$$nq^n$$

é solução da equação (3.12).

Como q é uma raiz dupla de $xp_n'(x)$ então q é raiz simples da sua derivada

$$\left(xp_n'(x)\right)' \;=\; n^2x^{n-1} - \alpha_1(n-1)^2x^{n-2} - \alpha_2(n-2)^2x^{n-3} - \cdots - \alpha_k(n-k)^2x^{n-k-1}$$

e, portanto, é também raiz do polinómio que se obtém a partir deste multiplicando-o por x, ou seja,

$$x\left(xp_n'(x)\right)' \;=\; n^2x^n - \alpha_1(n-1)^2x^{n-1} - \alpha_2(n-2)^2x^{n-2} - \cdots - \alpha_k(n-k)^2x^{n-k}$$

Substituindo x por q, vem

$$n^2q^n \;=\; \alpha_1(n-1)^2q^{n-1} + \alpha_2(n-2)^2q^{n-2} + \cdots + \alpha_k(n-k)^2q^{n-k}$$

o que mostra que a função

$$n^2q^n$$

também é solução da equação de recorrência (3.12).

Em resumo: se q for uma raiz tripla da equação característica associada à relação de recorrência (3.12), então

$$q^n, \quad nq^n, \quad n^2q^n$$

são soluções da equação considerada.

Este raciocínio pode ser generalizado, dando origem ao seguinte teorema:

Teorema 3.21 *Sejam $q_1, q_2, \ldots, q_m$ raízes distintas da equação característica da relação de recorrência*

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \quad \alpha_k \neq 0; \;\; n = k, k+1, \ldots$$

de graus de multiplicidade $p_1, p_2, \ldots, p_m$, respectivamente. Então a solução geral da relação de recorrência dada tem a forma

$$a_n \;=\; a_{1,n} + a_{2,n} + \cdots + a_{m,n}$$

onde, para cada $i = 1, 2, \ldots, m$, a solução correspondente à raiz q_i, de grau de multiplicidade p_i, é

$$a_{i,n} \;=\; c_{i,1}q_i^n + c_{i,2}nq_i^n + \cdots + c_{i,p_i}n^{p_i-1}q_i^n \;=\; (c_{i,1} + c_{i,2}n + \cdots + c_{i,p_i}n^{p_i-1})q_i^n$$

Demonstração: Da análise já feita antes do enunciado do teorema é fácil concluir que cada função $a_{i,n}, i = 1, 2, \ldots, m$ é solução da relação recursiva e, portanto, a função

$$a_n \;=\; a_{1,n} + a_{2,n} + \cdots + a_{m,n}$$

é solução da equação recursiva.

Para mostrar que esta é a solução geral é necessário mostrar que o determinante da matriz dos coeficientes do sistema nas constantes $c_{i,j}, i = 1, 2, \ldots, m; j = 1, 2, \ldots, p_i$, obtido a partir das condições iniciais é diferente de zero. Ora este determinante é, neste caso, uma generalização do determinante de Vandermonde que tem o valor

$$\prod_{i=1}^{m}(-q_i)\binom{p_i}{2}\prod_{1\leq i<j\leq m}(q_j - q_i)^{p_j p_i}$$

Como $q_j \neq q_i$ para $j \neq i$ então este determinante é diferente de zero o que prova que a solução obtida é realmente a solução geral da relação considerada. □

Exemplo 3.22 *Determinar a solução da relação de recorrência*

$$a_n \;=\; -a_{n-1} + 3a_{n-2} + 5a_{n-3} + 2a_{n-4}, \quad n = 4, 5, \ldots$$

sujeita às condições iniciais $a_0 = 1, a_1 = 0, a_2 = 1$ e $a_3 = 2$.

Resolução. A equação característica associada à relação de recorrência é

$$x^4 + x^3 - 3x^2 - 5x - 2 \;=\; 0$$

cujas raízes são $-1, -1, -1$ e 2.

A parte da solução correspondente à raiz tripla -1 é

$$(c_1 + c_2 n + c_3 n^2)(-1)^n$$

enquanto que a parte da solução geral correspondente à raiz simples 2 é

$$c_4 2^n$$

Então a solução geral da relação de recorrência dada é dada por

$$a_n \;=\; (c_1 + c_2 n + c_3 n^2)(-1)^n + c_4 2^n$$

Para determinar as constantes c_1, c_2, c_3, c_4 usam-se agora as condições iniciais

$$\begin{cases} c_1 & & & +c_4 & = & 1 \\ -c_1 & -c_2 & -c_3 & +2c_4 & = & 0 \\ c_1 & +2c_2 & +4c_3 & +4c_4 & = & 1 \\ -c_1 & -3c_2 & -9c_3 & +8c_4 & = & 2 \end{cases}$$

este sistema é possível e determinado, admitindo a solução

$$c_1 \;=\; \frac{42}{52} \quad c_2 \;=\; -\frac{29}{52} \quad c_3 \;=\; \frac{7}{52} \quad c_4 \;=\; \frac{10}{52}$$

e, portanto, a solução procurada é

$$a_n \;=\; \left(\frac{42}{52} - \frac{29}{52}\, n + \frac{7}{52}\, n^2\right)(-1)^n + \frac{10}{52}\, 2^n, \quad n = 0, 1, 2, \ldots$$

Exercícios 3.2.3

1. *Determinar o número k na relação de recorrência*

$$a_{n+1} \;=\; k a_n$$

se

   (a) $a_1 = 5$ *e* $a_2 = 10$

   (b) $a_1 = 5$ *e* $a_3 = 20$

2. *Resolver as relações de recorrência*

   (a) $a_{n+3} \;=\; 6a_{n+2} - 11a_{n+1} + 6a_n$ *com* $a_0 = 3, a_1 = 6$ *e* $a_2 = 14$.

   (b) $a_{n+3} \;=\; 4a_{n+2} - 5a_{n+1} + 2a_n$ *com* $a_0 = 2, a_1 = 4$ *e* $a_2 = 7$.

   (c) $a_{n+3} \;=\; 3a_{n+2} + 4a_{n+1} - 12a_n$ *com* $a_0 = 0, a_1 = -11$ *e* $a_2 = -15$.

3. *As raízes características de uma relação de recorrência linear e homogénea com coeficientes constantes são 1, 2, 2 e 3. Determinar a relação de recorrência e a sua solução.*

4. *Resolver a relação de recorrência*

$$na_n - (5n-5)a_{n-1} \;=\; 0$$

onde $a_1 = 10$. [SUGESTÃO: *Efectuar a substituição* $b_n = na_n$.]

5. *Seja* A *uma matriz quadrada de dimensão* m *cujos elementos da diagonal principal são todos nulos e cujos elementos não diagonais são todos iguais a 1. Designando por* a_n *os elementos da diagonal principal da matriz* A^n *e por* b_n *os elementos não diagonais da mesma matriz, mostrar que*

$$\begin{aligned} a_{n+1} &= (m-1)b_n \quad \text{e} \\ b_{n+1} &= a_n + (m-2)b_n \end{aligned}$$

Usar este facto para obter uma relação recursiva para a_n *com condições iniciais apropriadas. Resolver esta relação de recorrência. Determinar* a_n *e* b_n.

6. *Seja* D_n *o determinante de ordem* $n \geq 1$ *definido por*

$$D_n = \begin{vmatrix} 1+a^2 & a & 0 & 0 & \cdots & 0 \\ a & 1+a^2 & a & 0 & \cdots & 0 \\ 0 & a & 1+a^2 & a & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1+a^2 \end{vmatrix}$$

Mostrar que, para $n \geq 3$,

$$D_n \;=\; (1+a^2)D_{n-1} - a^2 D_{n-2}$$

e então que

$$D_n \;=\; \frac{1-a^{2n+2}}{1-a^2} \;\text{ se }\; a \neq 1$$

Para $a^2 = 1$ *qual será o valor de* D_n.

7. *Resolver as relações de recorrência seguintes calculando primeiro alguns valores, depois conjecturando a solução geral e finalmente provando a sua validade pelo método de indução.*

   (a) $a_n = 3a_{n-1}$, $n \geq 1$; $a_0 = 1$
   (b) $a_n = a_{n-1} - n + 3$, $n \geq 1$; $a_0 = 2$
   (c) $a_n = -a_{n-1} + 1$, $n \geq 1$; $a_0 = 0$
   (d) $a_n = -a_{n-1} + 2$, $n \geq 1$; $a_0 = 1$
   (e) $a_n = 2a_{n-1} + 1$, $n \geq 1$; $a_0 = 1$

3.2.3 Relações de recorrência lineares não homogéneas

Considerem-se agora relações de recorrência da forma

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} + f(n)$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_k$ são constantes e $f(n)$ é uma função de n. Fazendo nesta equação $f(n) = 0$ obtém-se a parte homogénea da relação de recorrência.

Para resolver uma relação de recorrência não homogénea faz-se apelo ao seguinte princípio: *se $a_n = \varphi(n)$ for a solução geral da relação homogénea e $\theta(n)$ for uma solução particular da relação não homogénea, então*

$$a_n \;=\; \varphi(n) + \theta(n)$$

é a solução geral da relação de recorrrência dada.

De facto, se $\varphi(n)$ é a solução geral da equação homogénea, tem-se

$$\varphi(n) \;=\; \sum_{j=1}^{k} \alpha_j \varphi(n-j) \tag{3.13}$$

enquanto que, se $\theta(n)$ é uma solução particular da equação não homogénea, vem

$$\theta(n) \;=\; \sum_{j=1}^{k} \alpha_j \theta(n-j) + f(n) \tag{3.14}$$

Somando (3.13) e (3.14) obtém-se

$$\varphi(n) + \theta(n) \;=\; \sum_{j=1}^{k} \alpha_j [\varphi(n-j) + \theta(n-j)] + f(n)$$

o que mostra que $a_n = \varphi(n) + \theta(n)$ é solução da equação não homogénea.

Exemplo 3.23 *Determinar a solução geral da relação de recorrência*

$$a_n \;=\; 5a_{n-1} - 6a_{n-2} + 6 \cdot 4^n$$

Resolução. A relação de recorrência homogénea associada à relação dada é

$$a_n - 5a_{n-1} + 6a_{n-2} \;=\; 0$$

à qual corresponde a seguinte equação característica

$$x^2 - 5x + 6 \;=\; 0$$

As raízes características desta equação são: $q_1 = 2$ e $q_2 = 3$. Então

$$a_n \;=\; c_1 2^n + c_2 3^n$$

é a solução geral da relação de recorrência homogénea.

A função

$$\theta(n) \;=\; 48 \cdot 4^n$$

é uma solução particular da relação de recorrência não homogénea visto que

$$\begin{aligned} 5\theta(n-1) - 6\theta(n-2) + 6 \cdot 4^n &= 5 \cdot 48 \cdot 4^{n-1} - 6 \cdot 48 \cdot 4^{n-2} + 6 \cdot 4^n \\ &= 5 \cdot 12 \cdot 4^n - 6 \cdot 3 \cdot 4^n + 6 \cdot 4^n \\ &= 48 \cdot 4^n \;=\; \theta(n) \end{aligned}$$

Então, finalmente,

$$a_n \;=\; c_1 2^n + c_2 3^n + 48 \cdot 4^n$$

é a solução geral da relação de recorrência dada.

Ao contrário do que acontece com as relações de recorrência lineares de coeficientes constantes e homogéneas, para as relações do mesmo tipo não homogéneas não existe um método geral para determinação de soluções particulares. Contudo, para certas situações, há algumas técnicas que permitem resolver o problema. É o que se passa quando o termo não homogéneo é da forma $f(n) = n^k$ para algum k inteiro não negativo ou é da forma $f(n) = q^n$ onde $q \in \mathbb{Q}$, $q \neq 1$. Considere-se cada um dos casos separadamente.

1 – Se $f(n) = cq^n$ (onde c é uma constante conhecida) e se q não for raiz da equação característica, procura-se uma solução particular da forma

$$\theta(n) \;=\; Aq^n$$

onde A é uma constante a determinar, substituindo $\theta(n)$ na equação não homogénea.

Se q for uma raiz da equação característica de multiplicidade m, então procura-se uma solução particular da forma

$$\theta(n) \;=\; An^m q^n$$

onde A é uma constante a determinar.

2 – Se $f(n) = cn^j$ e se 1 não for raiz da equação característica, procura-se uma solução particular da forma polinomial

$$\theta(n) \;=\; A_0 + A_1 n + A_2 n^2 + \cdots + A_j n^j$$

onde $A_0, A_1, \ldots, A_j$ são constantes a determinar por substituição de $\theta(n)$ na relação de recorrência não homogénea.

Se 1 for uma raiz da equação característica de multiplicidade r, então procura-se uma solução particular da forma

$$\theta(n) \;=\; A_0 n^r + A_1 n^{r+1} + A_2 n^{r+2} + \cdots + A_j n^{r+j}$$

onde $A_0, A_1, A_2, \ldots, A_j$ são constantes a determinar.

Exemplo 3.24 *Sendo*

$$(x-1)^2(x-2)(x-3)^2 \;=\; 0$$

a equação característica de uma certa relação de recorrência não homogénea, determinar a forma de uma solução particular da relação de recorrência completa nos seguintes casos:

1. $f(n) \;=\; 4n^3 + 5n$
2. $f(n) \;=\; 4^n$
3. $f(n) \;=\; 3^n$

Resolução. As raízes da equação característica são 1, 1, 2, 3, 3. Então a solução geral da relação de recorrência homogénea é

$$a_n \;=\; c_1 + c_2 n + c_3 2^n + c_4 3^n + c_5 n 3^n$$

Para soluções particulares da relação de recorrência completa procuram-se, em cada caso, soluções da forma

1. $\theta(n) \;=\; An^2 + Bn^3 + Cn^4 + Dn^5$
2. $\theta(n) \;=\; A \cdot 4^n$
3. $\theta(n) \;=\; A \cdot n^2 \cdot 3^n$

Por vezes uma relação de recorrência não homogénea apresenta as diversas situações simultaneamente. Neste caso faz-se apelo ao chamado princípio de sobreposição de efeitos que constitui o teorema que se segue.

Teorema 3.25 *Se, para cada $i = 1, 2, \ldots, r$, a função $\theta_i(n)$ for uma solução particular da relação de recorrência*

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} + f_i(n)$$

então a função

$$\theta_1(n) + \theta_2(n) + \cdots + \theta_r(n)$$

é solução particular da relação de recorrência

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} + \sum_{i=1}^{r} f_i(n)$$

Demonstração: Se, para cada $i = 1, 2, \ldots, r$, $\theta_i(n)$ é solução particular da relação de recorrência

$$a_n \;=\; \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} + f_i(n)$$

então tem-se que

$$\theta_i(n) \;=\; \alpha_1 \theta_i(n-1) + \alpha_2 \theta_i(n-2) + \cdots + \alpha_k \theta_i(n-k) + f_i(n)$$

pelo que somando para $i = 1, 2, \ldots, r$

$$\sum_{i=1}^{r} \theta_i(n) \;=\; \alpha_1 \sum_{i=1}^{r} \theta_i(n-1) + \alpha_2 \sum_{i=1}^{r} \theta_i(n-2) + \cdots + \alpha_k \sum_{i=1}^{r} \theta_i(n-k) + \sum_{i=1}^{r} f_i(n)$$

o que prova o teorema. □

Exercícios 3.2.4

1. *Determinar a soma*

$$\sum_{j=1}^{n} j^3$$

começando por estabelecer uma relação de recorrência apropriada.

2. *Resolver as seguintes relações de recorrência não homogéneas.*
   (a) $a_n = a_{n-1} + 12n^2$, $n \geq 1$; $a_0 = 5$
   (b) $a_n - 4a_{n-1} + 4a_{n-2} = f(n)$, $n \geq 2$ *onde*
   - $f(n) = 1$
   - $f(n) = n$
   - $f(n) = 3^n$
   - $f(n) = 2^n$
   - $f(n) = 1 + n + 2^n + 3^n$

   (c) $a_{n+2} - 4a_{n+1} + 3a_n = 16$, $n \geq 0$; $a_0 = 4, a_1 = 2$
   (d) $a_n = 4a_{n-1} + 5 \cdot 3^n$
   (e) $a_n = 4a_{n-1} + 5 \cdot 4^n$
   (f) $a_n = a_{n-1} + 2a_{n-2} + 4 \cdot 3^n$, $n \geq 2$; $a_0 = 11, a_1 = 28$
   (g) $a_n = 4a_{n-1} - 4a_{n-2} + 2^n$, $n \geq 2$; $a_0 = 1, a_1 = 7$
3. *Resolver a relação de recorrência*

$$a_n = a_{n-1} + 6n^2, \quad n \geq 1$$

com $a_0 = 0$*:*
   (a) *usando o princípio de sobreposição,*
   (b) *fazendo repetidas substituições e induzindo a solução.*

Então determinar a soma dos quadrados dos primeiros n números naturais.

4. *Determinar as constantes p, q e r na relação de recorrência*

$$a_n + pa_{n-1} + qa_{n-2} = r, \quad n \geq 2$$

sabendo que a solução geral é da forma

$$a_n \ = \ c_1 2^n + c_2 3^n + 4$$

5. *Seja $p(x) = 2x^2 + x + 3$. Determinar uma fórmula para*

$$\sum_{j=1}^{m} p(j)$$

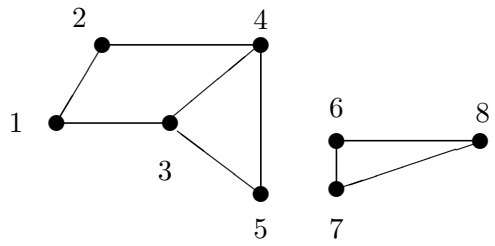
Capítulo 4

Teoria dos Grafos

4.1 Introdução

A teoria dos grafos tem a sua origem na necessidade de representar por esquemas as relações existentes entre os elementos de um conjunto. Neste sentido, constitui um ramo específico da teoria das relações binárias definidas num conjunto. Esta teoria cobre um vasto campo de aplicações que vão desde a física até certos domínios da arte, passando pela química, biologia, sociologia, economia, gestão, engenharia, etc.

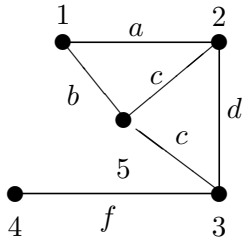
A noção de digrafo ou grafo dirigido, foi já referida a propósito da representação geométrica de uma relação binária definida num conjunto. Se $\mathcal{R}$ for uma relação simétrica, então sempre que (x_i, x_j) pertence ao digrafo também (x_j, x_i) lhe pertencerá. Neste caso a ligação entre dois vértices (quando existe) faz-se sempre nos dois sentidos, podendo representar-se este facto por uma aresta única (não dirigida). Obtém-se, assim, um grafo não dirigido (ou, simplesmente, grafo). Embora a teoria dos grafos seja um instrumento natural para o estudo das relações binárias, há, hoje em dia, muitos outros tópicos de matemática quer pura quer aplicada para os quais o recurso à teoria dos grafos constitui uma atitude natural. Na figura seguinte apresenta-se um exemplo de um grafo (não dirigido).



Embora o aparecimento da teoria dos grafos se possa situar ao tempo de Euler (1707-1783) o seu desenvolvimento enquanto teoria autónoma é bastante recente. Por este facto, muitas das notações e designações que se usam a seguir podem variar bastante na literatura técnica dedicada a este assunto.

4.1.1 Definições básicas

Chama-se **grafo** $\mathcal{G} \equiv (V, E)$ a uma estrutura constituída por um conjunto finito[1] V de **vértices** (também designados por **nós**) e um conjunto finito E de **arestas** de tal forma que cada aresta está associada a um par de vértices



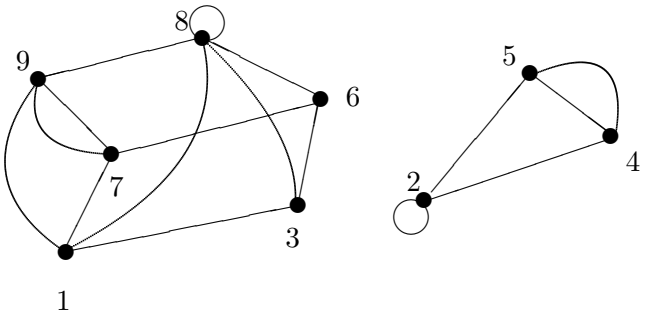
$$V = \{1, 2, 3, 4, 5\}, \quad E = \{a, b, c, d, e, f\}$$

Sendo e uma aresta e v, w dois vértices, escreve-se $e = \{v, w\}$ ou $e = \{w, v\}$ dizendo-se então que e é uma aresta *entre* v e w ou que a aresta e liga os vértices v e w que, por este facto, se dizem **adjacentes**. Uma aresta que liga um vértice a si próprio designa-se por **lacete**.

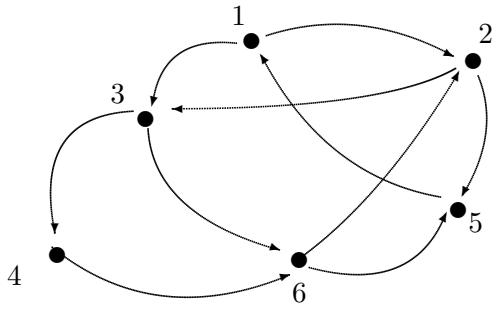
Na representação pictórica de um grafo, os vértices são representados por pequenos círculos afectados de um símbolo que constitui o seu nome, enquanto que as arestas são representadas por linhas que ligam dois vértices (segmentos de recta ou linhas curvas).

[1] Também se podem considerar grafos infinitos com um conjunto numerável de vértices. Aqui, no entanto, apenas se estudará o caso dos grafos com um número finito de vértices.

Se entre dois vértices existir mais que uma aresta então, se for necessário efectuar distinções, o grafo correspondente toma o nome de **multigrafo** e as várias arestas que ligam os mesmos dois vértices também se designam por arestas múltiplas. No entanto, na literatura da especialidade, em geral, o termo grafo é empregue mesmo quando possui arestas múltiplas.

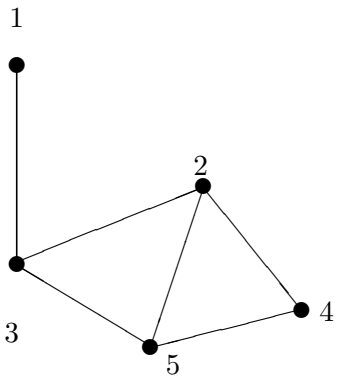


Neste contexto, chama-se **grafo orientado** ou **digrafo** (*"directed graph"*) a uma estrutura $\mathcal{G} \equiv (V, E)$ onde, novamente, V é um conjunto finito de vértices e E um conjunto finito de **arcos** dirigidos. A seguir apresenta-se um exemplo de um digrafo com 6 vértices e 10 arcos dirigidos.



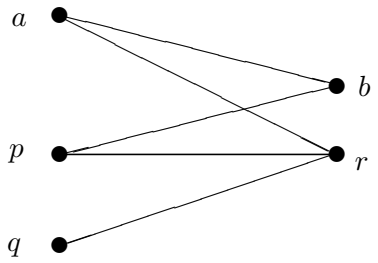
Num digrafo escreve-se $e \equiv (v, w)$ para significar que e é um arco que liga v a w orientado de v para w. Neste caso diz-se que v é **adjacente** ao vértice w, que o arco e é **incidente** sobre w e **emergente** de v.

Um grafo diz-se **simples** quando não possui lacetes nem arestas múltiplas. O grafo que se segue



é um exemplo de um grafo simples.

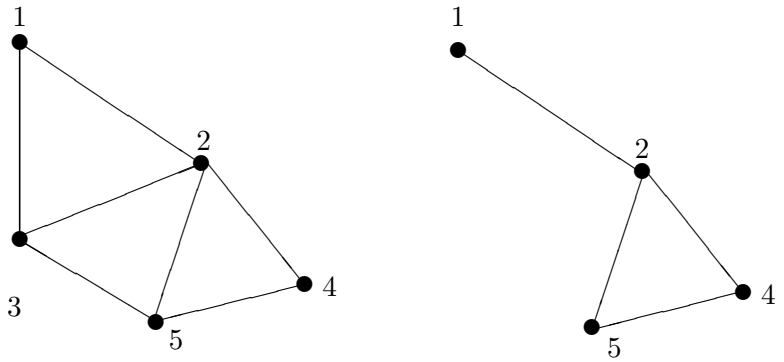
Um tipo de grafos com muita importância em problemas de emparelhamento (casamentos, distribuição de grupos de tarefas por grupos de pessoas, etc.) são os chamados **grafos bipartidos** que são grafos nos quais os vértices podem ser cindidos em dois conjuntos disjuntos V e W tais que cada aresta liga sempre um vértice de V a um vértice de W. Neste caso denota-se por $\mathcal{G} \equiv (V, W; E)$. Na figura que se segue apresenta-se um exemplo de um grafo bipartido



$$V = \{a, p, q\}, \quad W = \{b, r\}, \quad \mathcal{G} = (V, W; E)$$

Um grafo diz-se **nulo** se possuir apenas vértices sem arestas nem lacetes; por outro lado, no extremo oposto, um grafo diz-se **completo** quando entre cada par de vértices há uma aresta. Neste último caso, se o grafo tiver n vértices é habitual denotá-lo por K_n. Um digrafo diz-se completo se entre cada par de vértices existir pelo menos um arco. Um grafo bipartido simples $\mathcal{G} \equiv (V, W; E)$ diz-se completo se existir uma aresta entre cada vértice de V e cada vértice de W. Um grafo bipartido completo denota-se por $K_{p,q}$ onde p e q são o número de vértices de V e W, respectivamente.

Sejam $\mathcal{G} \equiv (V, E)$ e $\mathcal{G}' \equiv (V', E')$ dois grafos dados: $\mathcal{G}'$ dir-se-á um **subgrafo** de $\mathcal{G}$ se V' for um subconjunto de V e E' um subconjunto de E. Suponha-se que W é um subconjunto não vazio de V. Dá-se o nome de **subgrafo de $\mathcal{G}$ induzido por** W ao grafo $\mathcal{H} \equiv (W, F)$ onde para cada aresta $f \in F$ se tem $f = \{u, v\} \in E$ e $u, v \in W$.



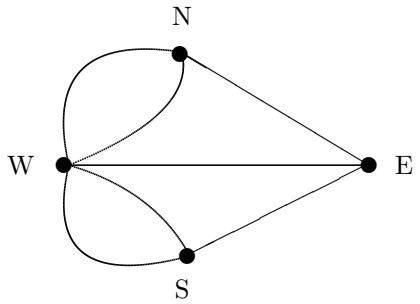
Nesta figura o grafo (b) é um subgrafo do grafo (a) induzido pelo conjunto $W = \{1, 2, 4, 5\}$ que é um subconjunto do conjunto $V = \{1, 2, 3, 4, 5\}$ de vértices do primeiro.

Exemplo 4.1 (Digrafo de comunicações.) Considere-se uma organização com várias secções. Cada secção é representada por um vértice, desenhando-se uma flecha do vértice v para o vértice w se a secção v puder transmitir sinais para a secção w. O digrafo assim resultante é o que se designa por digrafo de comunicação.

Exemplo 4.2 (As pontes de Königsberg.) A primeira publicação em teoria dos grafos foi feita por L. Euler em 1736. O artigo de Euler solucionava um problema conhecido pelo problema das pontes de Königsberg. A cidade de Königsberg (hoje conhecida por Kaliningrad) na Prússia, banhada pelo rio Pregel, é constituída por quatro partes: a parte a norte do rio, $N(\equiv A)$, a parte a sul do rio, $S(\equiv D)$, e duas ilhas situadas no interior do rio, a ilha ocidental, $W(\equiv B)$ e a ilha oriental, $E(\equiv C)$.

Ligando estas quatro componentes da cidade existem 7 pontes tal como se indica na figura. Os habitantes de Königsberg, que gostavam de passear na cidade ao domingo, colocavam a si próprios a seguinte questão: *será possível planear um passeio pela cidade de tal forma que partindo de casa a ela se regressasse após ter atravessado* **uma e uma só vez** *cada uma das sete pontes?*

Se se considerar cada uma das quatro partes da cidade como um vértice e cada ponte como uma aresta, então o problema corresponde ao seguinte grafo (multigrafo) com 4 vértices e 7 arestas



Em termos de teoria dos grafos o problema pode então ser assim formulado: dado um grafo qualquer (não necessariamente simples) será possível percorrer todas as arestas do grafo sem passar por cima de nenhuma delas mais que uma vez?

No caso do problema das pontes de Königsberg, Euler estabeleceu a resposta definitiva, pela negativa, como mais à frente se verá.

Exemplo 4.3 (Rêde de transportes.) Suponha-se que cada vértice de um grafo dado representa uma cidade da Europa, por exemplo. Dois vértices são ligados por uma aresta se existir uma ligação aérea directa entre as cidades que eles representam. Um problema que se pode pôr é o de saber se se pode partir de uma dada cidade e voltar à mesma cidade depois de ter visitado todas as outras. Se a cada aresta se associar um número real não negativo que represente o custo do uso daquela aresta, pode colocar-se um problema de optimização que é o de encontrar

o percurso (se existir) que satisfaz a condição do problema anterior ao menor custo. Este é o conhecido **problema do caixeiro viajante**.

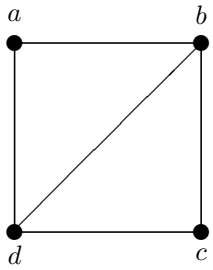
Grafos isomorfos. Definindo grafo como um par ordenado constituído por um conjunto de vértices e um conjunto de arestas, o mesmo grafo pode aparecer com representações pictóricas muito distintas. É, por isso, importante, dispor de um critério que nos permita saber quando é que dois grafos (aparentemente) distintos são afinal o mesmo grafo. Tal critério resulta imediatamente da noção de isomorfismo de grafos.

Definição 4.4 *Dois grafos* $\mathcal{G}_1 \equiv (V_1, E_1)$ *e* $\mathcal{G}_2 \equiv (V_2, E_2)$ *dir-se-ão* **isomorfos** *se existir uma bijecção*

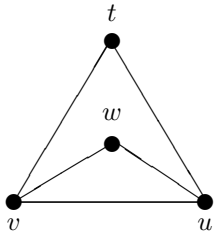
$$\varphi : V_1 \rightarrow V_2$$

tal que $\{\varphi(u), \varphi(v)\}$ *seja uma aresta de* $\mathcal{G}_2$ *se e só se* $\{u, v\}$ *for uma aresta de* $\mathcal{G}_1$.

Exemplo 4.5 Os grafos



$G_1 \equiv (V_1, E_1)$



$G_2 \equiv (V_2, E_2)$

são isomorfos. De facto, sendo

$$\varphi : V_1 \rightarrow V_2$$

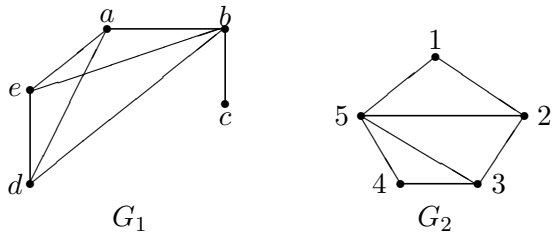
a bijecção definida por

$$\varphi(a) = t, \;\; \varphi(b) = v, \;\; \varphi(c) = w, \;\; \varphi(d) = u$$

pode verificar-se facilmente que φ constitui um isomorfismo de grafos.

Dois grafos isomorfos, aparte os nomes dados aos vértices e às arestas e a sua representação pictórica são, na realidade, o mesmo grafo e é como tal que podem ser encarados no contexto da teoria dos grafos.

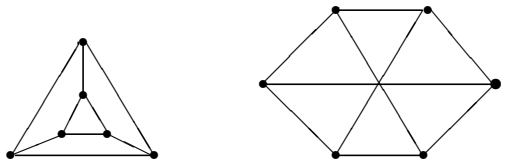
Para mostrar que dois grafos não são isomorfos é necessário mostrar que não existe qualquer bijecção entre os conjuntos de vértices respectivos que transformem arestas em arestas. Se dois grafos não tiverem o mesmo número de vértices então não são isomorfos; se tiverem o mesmo número de vértices mas tiverem diferente número de arestas também não podem ser isomorfos. Finalmente, mesmo que dois grafos tenham o mesmo número de vértices e o mesmo número de arestas, ainda assim eles podem não ser isomorfos. Por exemplo, os dois grafos



G_1 G_2

têm ambos 5 vértices e 7 arestas. No entanto, não são isomorfos. Uma forma de mostrar que isto é verdade é notar que os vértices a, b, d, e de $\mathcal{G}_1$ formam um subgrafo completo de $\mathcal{G}_1$: qualquer isomorfismo com $\mathcal{G}_1$ deverá transformar estes quatro vértices noutros quatro vértices com a mesma propriedade. Ora, em $\mathcal{G}_2$ não há quatro vértices que induza um subgrafo completo de $\mathcal{G}_2$ e, portanto, este não pode ser isomorfo a $\mathcal{G}_1$.

Exercícios 4.1.1 *Mostrar que os grafos*



não são isomorfos.

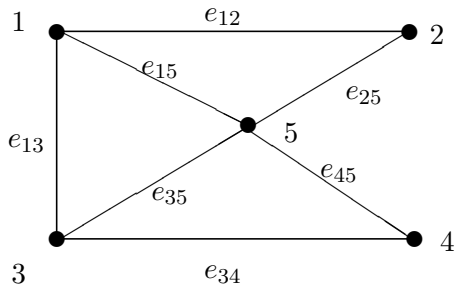
4.1.2 Caminhos de um grafo

Chama-se **caminho** entre dois vértices v_1 e v_r num grafo a uma sequência finita de vértices e arestas da forma

$$v_1, e_1, v_2, e_2, \ldots, e_{r-1}, v_r$$

onde, para cada j, e_j é uma aresta que liga v_j a v_{j+1}. Os vértices e as arestas de um caminho podem não ser todos distintos. Ao número de arestas que compõem um caminho dá-se o nome de **comprimento** desse caminho.

Um caminho diz-se **simples** se não tiver arestas repetidas e diz-se **elementar** se todos os seus vértices forem distintos. Um caminho no qual o vértice inicial e o vértice terminal coincidem chama-se **circuito**. Um circuito diz-se simples se não possuir arestas repetidas e um circuito no qual nenhum vértice é repetido excepto o vértice inicial (terminal) designa-se por **ciclo**. No grafo que se segue, por exemplo,



o caminho $3e_{35}5e_{25}2e_{12}1e_{15}5e_{45}4e_{34}3$ é um circuito simples (não há arestas repetidas e o vértice inicial e terminal coincidem), mas não é um ciclo já que para além do vértice inicial (que é também terminal) há outro vértice, o vértice 5, que está repetido.

Num digrafo estes conceitos podem ter em conta a orientação. Chama-se **caminho orientado** a uma sequência finita de arcos da forma

$$v_1, e_1, v_2, e_2, \ldots, e_{r-1}, v_r$$

onde, para cada $j = 1, 2, \ldots, r-1$, se tem $e_j = (v_j, v_{j+1})$. A partir daqui define-se caminho fechado, circuito e ciclo concordantemente.

Grafos conexos. Seja $\mathcal{G} \equiv (V, E)$ um grafo qualquer. No conjunto V dos vértices define-se a seguinte relação

$$v \mathcal{J} w \text{ } \textit{se e só se } v = w \text{ } \textit{ou}$$
$$\textit{existe um caminho entre } v \text{ } \textit{e} \text{ } w.$$

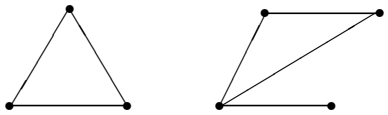
Esta relação é

- reflexiva,

- simétrica e
- transitiva

e, portanto, é uma relação de equivalência. Então V pode decompor-se em classes de equivalência $\{V_1, V_2, \ldots, V_r\}$; cada um dos subgrafos $\mathcal{G}_i$, (com $i = 1, 2, \ldots, r$), induzido por $V_i \subset V$, chama-se **componente conexa do grafo** $\mathcal{G}$.

Exemplo 4.6 O grafo



tem duas componentes conexas.

Definição 4.7 *Um grafo diz-se* **conexo** *se e só se possuir uma só componente conexa, ou seja, se e só se entre dois quaisquer dos seus vértices existir sempre um caminho. Um grafo que possui mais que uma componente conexa diz-se um* **grafo desconexo**.

No caso dos digrafos a questão da conexidade é um pouco mais complexa: assim, se entre dois vértices quaisquer v_i e v_j ($v_i \neq v_j$) existir sempre um caminho orientado de v_i para v_j e um caminho orientado de v_j para v_i o digrafo diz-se **fortemente conexo**; se tal não acontecer, mas o grafo que se obtém do digrafo retirando simplesmente a orientação dos seus arcos (isto é, transformando todos os seus arcos em arestas) for conexo então o digrafo diz-se **fracamente conexo**.

4.1.3 Graus dos vértices de um grafo

Uma aresta e de um grafo diz-se **incidente** sobre o vértice v se este for um dos seus pontos extremos. Chama-se **grau** de um vértice v ao número de arestas que incidem sobre esse vértice. Um vértice diz-se **ímpar** ou **par** consoante o seu grau seja um número ímpar ou par, respectivamente. [Note-se que um lacete incide duas vezes sobre o mesmo vértice pelo que conta duas vezes para efeito do cálculo do grau do vértice respectivo.]

Teorema 4.8 *Em qualquer grafo a soma dos graus dos seus vértices é igual a duas vezes o número das suas arestas.*

Demonstração: Proceder-se-á por indução sobre o número de arestas do grafo: denote-se por $p(n)$ a afirmação de que a soma dos graus de todos os vértices de um grafo com n arestas é igual a $2n$.

(i) – Se o grafo não tem qualquer aresta, então o grau de qualquer dos seus vértices é zero e a soma dos graus de todos os vértices é zero. Assim, $p(0)$ é uma proposição verdadeira.

(ii) – Suponha-se que para um dado $k \in \mathbb{N}$ se verifica $p(k)$, isto é, que a soma dos graus de todos os vértices de um grafo com k arestas é igual a $2k$. Considere-se agora um grafo $\mathcal{G}$ com $k+1$ arestas. Pretende-se provar que a soma dos graus de todos os vértices de $\mathcal{G}$ é igual a $2k+2$. Para tal, considere-se um grafo $\mathcal{G}'$ exactamente igual a $\mathcal{G}$ mas com menos uma aresta, por exemplo, a aresta $\{a, b\}$.

Pela hipótese de indução, $\mathcal{G}'$ tem k arestas e, portanto, a soma dos graus de todos os seus vértices é igual a $2k$. Para obter $\mathcal{G}$ a partir de $\mathcal{G}'$ a única coisa que é necessário fazer é acrescentar a $\mathcal{G}'$ a aresta $\{a, b\}$. Este acrescento aumenta o grau do vértice a de uma unidade e o grau do vértice b de uma unidade: então, ao passar de $\mathcal{G}'$ para $\mathcal{G}$ por adição da aresta $\{a, b\}$ a soma dos graus de todos os vértices de $\mathcal{G}'$ aumenta 2 unidades fazendo com que a soma dos graus de todos os vértices de $\mathcal{G}$ seja igual a $2k+2$. Isto significa que para $k \in \mathbb{N}$ dado

$$p(k) \;\Rightarrow\; p(k+1)$$

Por (i) e (ii), tendo em conta o princípio de indução matemática, fica demonstrado o teorema. □

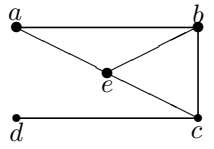
Corolário 4.9 *Em qualquer grafo o número de vértices que tem grau ímpar é um número par.*

Demonstração: A soma dos graus de todos os vértices é um número par e, para que assim seja, o número de termos ímpares não pode ser ímpar pois de contrário a soma total seria também ímpar. □

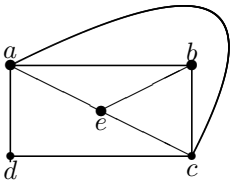
Exercícios 4.1.2

1. *Para os grafos 1, 2, 3 e 4 desenhados a seguir:*
   - *(a) Fazer a descrição formal (como par ordenado de conjuntos).*
   - *(b) Determinar o grau de cada vértice.*
   - *(c) Determinar o número de arestas.*
   - *(d) Verificar o teorema 4.8.*

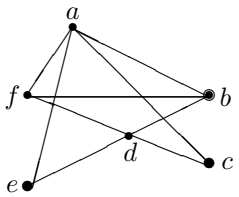
[1]



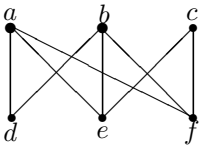
[2]



[3]

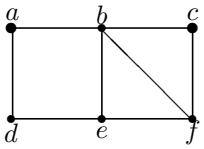


[4]

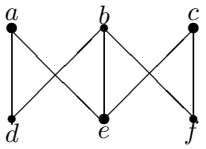


2. Nos grafos que se seguem, 5, 6, 7, e 8,

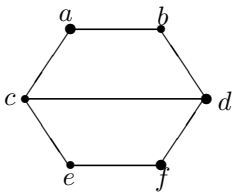
[5]



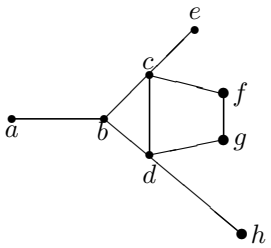
[6]



[7]



[8]



resolver (se possível) os seguintes problemas:

(a) Determinar um caminho elementar de a a f.

(b) Determinar um caminho simples de a a f que não seja elementar.

(c) Determinar um caminho de a a f que não seja simples.

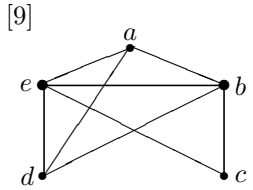
3. Para cada um dos grafos 9, 10, 11 e 12 resolver os seguintes problemas:

(a) Determinar um circuito que não seja um ciclo.

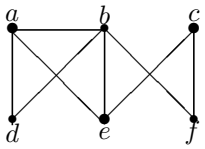
(b) Determinar um circuito que não seja simples.

(c) Determinar um circuito simples.

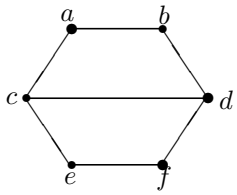
[9]



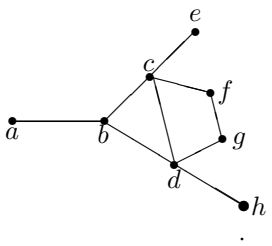
[10]



[11]



[12]



4. *Usando o grafo 5, determinar o subgrafo induzido pelo conjunto de vértices* $\{a, b, c, f\}$.
5. *Usando o grafo 8, determinar o subgrafo induzido pelo conjunto de vértices* $\{a, c, d, f\}$.
6. *Usando o grafo 7, determinar os subgrafos induzidos pelos conjuntos de vértices que se obtêm suprimindo um só vértice do conjunto original.*

4.2 Representação de Grafos por Matrizes

Uma questão que normalmente se põe em teoria dos grafos é a de saber se, dados dois vértices particulares, existirá algum caminho que os una. Se o grafo for de pequena dimensão (isto é, se tiver um pequeno número de vértices e de arestas), esta questão pode resolver-se, em geral, por simples inspecção da representação pictórica do grafo. Nas situações práticas, no entanto, é necessário lidar com grafos de grande dimensão e complexidade, nos quais a resolução de problemas deste tipo, em tempo aceitável, exige o recurso a meios computacionais para os quais a representação pictórica pouca utilidade tem. Para este efeito, utilização de computadores em teoria dos grafos, existem formas mais adequadas para representação de grafos, uma das quais se baseia na utilização de matrizes.

4.2.1 Matriz de adjacência de um grafo

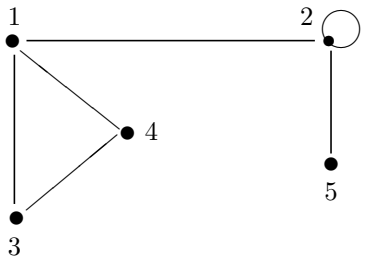
Seja dado um grafo $\mathcal{G} \equiv (V, E)$ onde $V = \{1, 2, \ldots, n\}$ e as arestas entre dois vértices, quando existem, são simples. Chama-se **matriz de adjacência** do grafo $\mathcal{G}$ à matriz quadrada de dimensão n,

$$A \;=\; [a_{ij}]_{1 \leq i,j \leq n}$$

tal que $a_{ij} = 1$ se existe uma aresta entre os vértices i e j e $a_{ij} = 0$ no caso contrário.

A matriz de adjacência de um grafo é simétrica; os elementos da diagonal principal são todos iguais a 0 se e só se o grafo não possuir lacetes.

Exemplo 4.10 O grafo



tem a seguinte matriz de adjacência

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

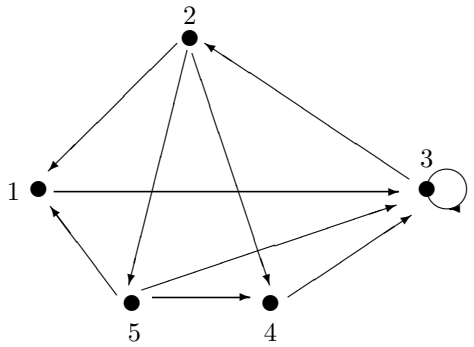
O grau de um vértice i qualquer é igual ao número de elementos iguais a 1 na fila (linha ou coluna) i da respectiva matriz de adjacência.

A matriz de adjacência de um digrafo com n vértices é também uma matriz quadrada de dimensão n

$$A \;=\; [a_{ij}]_{1 \leq i,j \leq n}$$

onde $a_{ij} = 1$ se existir o arco de i para j e $a_{ij} = 0$ no caso contrário.

Exemplo 4.11 Dado o digrafo



corresponde-lhe a matriz de adjacência

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

Como é natural, a matriz de adjacência de um digrafo não é necessariamente simétrica.

No caso de um digrafo chama-se **semi-grau incidente** de um vértice ao número de arcos que incidem sobre esse vértice e **semi-grau emergente** ao número de arcos que partem desse vértice. Assim, no grafo acima, o vértice 1, por exemplo, tem um semi-grau incidente e um semi-grau emergente de 2 e 1, respectivamente, enquanto que o vértice 3 tem semi-graus incidente e emergente iguais a 4 e 2, respectivamente.

Potências da matriz de adjacência. As sucessivas potências da matriz de adjacência de um grafo servem para determinar o número de caminhos de comprimento dado entre os vários pares possíveis de vértices de um grafo. Assim,

Teorema 4.12 *Se A for a matriz de adjacência de um grafo $\mathcal{G}$, então o elemento da linha i e coluna j da matriz A^2 é igual ao número de caminhos de comprimento 2 que ligam os vértices i e j.*

Demonstração: Seja $a_{ij}^{(2)}$ o elemento da linha i e coluna j da matriz A^2. Então, supondo que A é de dimensão n

$$a_{ij}^{(2)} = \sum_{p=1}^{n} a_{ip} a_{pj}$$

Para cada $p = 1, 2, \ldots, n$ fixado o produto $a_{ip}a_{pj}$ é igual a 1 quando e só quando existe uma aresta de i a p **e** uma aresta de p a j, ou seja, quando existe um caminho de comprimento 2 de i a j passando por p. Somando todas as possibilidades quando p varia de 1 a n obtém-se o resultado enunciado. □

O teorema 4.12 pode generalizar-se para o seguinte:

Teorema 4.13 *Se A for a matriz de adjacência de um grafo com n vértices, o elemento da linha i e coluna j da potência de ordem k ($k \geq 1$) de A é igual ao número de caminhos entre os vértices i e j de comprimento k.*

Demonstração: Demonstrar-se-á este teorema por indução finita. Um caminho de comprimento 1 é uma aresta; logo, tendo em conta a definição de matriz de adjacência, o teorema verifica-se para $k = 1$.

Suponha-se então que o teorema se verifica para a potência $k-1$ ($k > 1$). Seja, para cada $r = 1, 2, 3, \ldots$, $a_{ij}^{(r)}$ o elemento de ordem (i, j) da potência de ordem r da matriz A. Então

$$a_{ij}^{(k)} = \sum_{p=1}^{n} a_{ip}^{(k-1)} a_{pj}$$

onde

$$a_{ip}^{(k-1)} a_{pj} = \begin{cases} a_{ip}^{(k-1)} & \text{se } p \text{ e } j \text{ forem adjacentes} \\ 0 & \text{no caso contrário} \end{cases}$$

Por hipótese (indução) $a_{ip}^{(k-1)}$ é o número de caminhos de comprimento $k-1$ entre os vértices i e p e, portanto, $a_{ip}^{(k-1)}$ será o número de caminhos de comprimento k entre os vértices i e j que incluem uma aresta que vai de p a j. Somando todas as possibilidades que vão desde $p = 1$ até $p = n$, obtém-se o resultado pretendido. □

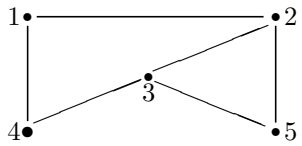
Corolário 4.14 *O elemento $a_{ii}^{(2)}$ de A^2 é igual ao grau do vértice i.*

Demonstração: Visto que

$$a_{ii}^{(2)} = \sum_{p=1}^{n} a_{ip}a_{pi}$$

então, como $a_{ip} = 1$ quando e só quando $a_{pi} = 1$, isto é, quando e só quando há uma aresta entre os vértices i e p, a soma de $p = 1$ até $p = n$ dá o grau do vértice i. □

Exemplo 4.15 Considere-se o seguinte grafo



cuja matriz de adjacência é a seguinte

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

Então,

$$A^2 = \begin{bmatrix} \mathbf{2} & 0 & 2 & 0 & 1 \\ 0 & \mathbf{3} & 1 & 2 & 1 \\ 2 & 1 & \mathbf{3} & 0 & 1 \\ 0 & 2 & 0 & \mathbf{2} & 1 \\ 1 & 1 & 1 & 1 & \mathbf{2} \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 0 & 5 & 1 & 4 & 2 \\ 5 & 2 & 6 & 1 & 4 \\ 1 & 6 & 2 & 5 & 4 \\ 4 & 1 & 5 & 0 & 2 \\ 2 & 4 & 4 & 2 & 2 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 9 & 3 & 11 & 1 & 6 \\ 3 & 15 & 7 & 11 & 8 \\ 11 & 7 & 15 & 3 & 8 \\ 1 & 11 & 3 & 9 & 6 \\ 6 & 8 & 8 & 6 & 8 \end{bmatrix}$$

Em A^2 na posição $(4,4)$ está o número 2 que é o grau do vértice 4 e é igual ao número de caminhos do vértice 4 ao vértice 4: os caminhos 4-1-4 e 4-3-4. Da quarta potência de A pode concluir-se, por exemplo, que há 8 caminhos de comprimento 4 entre os vértices 2 e 5. Os elementos que aparecem na diagonal de A^3 correspondem aos números de triângulos (circuitos de comprimento 3) que passam pelos vértices respectivos.

Para saber se existe algum caminho entre os vértices i e j de um grafo com n vértices é suficiente determinar as primeiras $n-1$ potências da matriz de adjacência. Se existir algum caminho entre o vértice i e o vértice j ele

tem, no máximo, um comprimento igual a $n-1$. De facto, neste caso, ou há um caminho de comprimento inferior a $n-1$ ou então, na pior das hipóteses, existe um caminho que passa por todos os vértices e tal caminho tem comprimento $n-1$ (note-se que, neste caso, se $i \neq j$ e se existir alguma aresta entre i e j esta não faz parte do caminho referido). Pode então enunciar-se o seguinte resultado:

Teorema 4.16 *Seja $\mathcal{G}$ um grafo com n vértices cuja matriz de adjacência é A. Definindo*

$$S = A + A^2 + A^3 + \cdots + A^{n-1}$$

então existe (pelo menos) um caminho entre o vértice i e o vértice j se e só se o elemento de ordem (i,j) na matriz S for diferente de zero.

Corolário 4.17 *Se todos os elementos da matriz S forem diferentes de zero então $\mathcal{G}$ é um grafo conexo.*

Demonstração: Resulta imediatamente do teorema anterior, tendo em conta a definição de grafo conexo. □

O caso dos digrafos. Como já foi referido acima, num digrafo, chama-se **caminho dirigido** do vértice v para o vértice w a uma sequência finita de vértices e arcos

$$v_1, a_1, v_2, a_2, \ldots, v_r, a_r, v_{r+1}$$

tais que $v_1 = v$ e $v_{r+1} = w$ e, para cada i, a_i é um arco dirigido de v_i para v_{i+1}. Se existir um caminho dirigido do vértice v para o vértice w então dir-se-á que v está ligado ou **conectado** a w. A tradução para digrafos do teorema 4.13 pode enunciar-se da seguinte maneira

Teorema 4.18 *Se A for a matriz de adjacência de um digrafo, então o elemento da posição (i,j) da potência A^k $(k \geq 1)$ é o número de caminhos dirigidos de comprimento k do vértice i para o vértice j.*

A demonstração deste teorema é idêntica à demonstração do teorema 4.13, tendo o cuidado de adaptar todos os resultados usados ao caso dos digrafos.

4.2.2 Matriz de incidência de um grafo

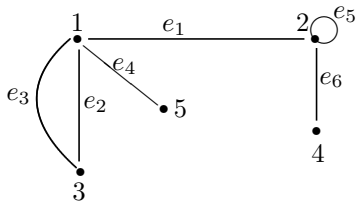
Outra matriz que é útil para representar um grafo sob o ponto de vista computacional é a chamada **matriz de incidência**. Ao contrário da matriz de adjacência, a matriz de incidência pode representar grafos com arestas múltiplas ou (em digrafos) com arcos paralelos.

Seja $\mathcal{G} \equiv (V, E)$ um grafo onde $V = \{1, 2, \ldots, n\}$ e $E = \{e_1, e_2, \ldots, e_m\}$. A matriz de incidência do grafo $\mathcal{G}$ é uma matriz de dimensão $n \times m$

$$B \;=\; [b_{ij}]_{1 \leq i \leq n; 1 \leq j \leq m}$$

onde as linhas correspondem aos vértices e as colunas correspondem às arestas: se, para k dado, o arco e_k ligar os vértices i e j, então todos os elementos da coluna k são 0 excepto $b_{ik} = b_{jk} = 1$.

Exemplo 4.19 A matriz de incidência do grafo



é a seguinte:

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

Cada coluna correspondente a uma aresta que não seja um lacete tem apenas dois elementos não nulos; as colunas correspondentes a lacetes têm apenas um elemento não nulo. Além disso, a soma dos elementos de cada linha dá o grau do vértice que lhe corresponde, num grafo simples (sem lacetes).

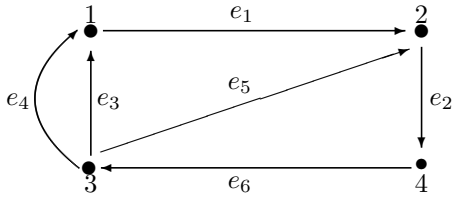
Exercícios 4.2.1 *Mostrar que entre as matrizes de adjacência e de incidência de um grafo simples (sem lacetes) se verifica a relação*

$$B\,B^t \;=\; D + A$$

onde B^t é a matriz transposta da matriz de incidência B e D é uma matriz diagonal de dimensão n (número de vértices do grafo) cujos elementos da diagonal principal são os graus dos vértices respectivos e A é a matriz de adjacência. À matriz D dá-se o nome de **matriz dos graus**.

A matriz de incidência B de um digrafo sem lacetes define-se da seguinte maneira: se e_k for um arco de i para j então todos os elementos da coluna k são iguais a 0 excepto $b_{ik} = -1$ e $b_{jk} = 1$.

Exemplo 4.20 A matriz de incidência do digrafo



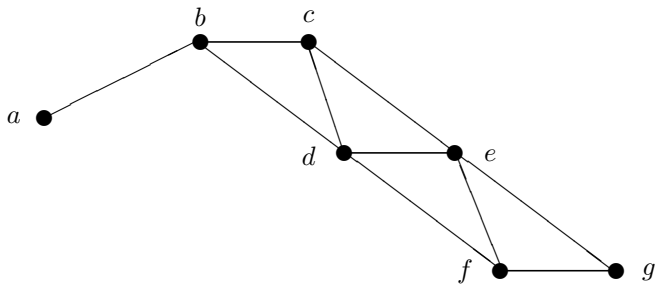
é a seguinte.

$$B = \begin{bmatrix} -1 & 0 & 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & -1 & 1 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

A soma de todos os elementos da linha i é igual ao semi-grau incidente menos o semi-grau emergente do vértice correspondente.

Exercícios 4.2.2

1. *Determinar a matriz de incidência do seguinte grafo*



2. *Seja $\mathcal{G} \equiv (V, E)$ (com $V = \{1, 2, 3, 4, 5\}$ e $E = \{a, b, c, d, e, f\}$) um grafo cuja matriz de incidência é a seguinte*

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

   (a) *Determinar o grau de cada vértice.*
   (b) *Esboçar uma representação pictórica de $\mathcal{G}$.*
   (c) *Determinar a matriz de adjacência de $\mathcal{G}$.*

3. *Seja $\mathcal{G} \equiv (V, E)$ (com $V = \{1, 2, 3, 4, 5, 6\}$ e $E = \{a, b, c, d, e, f, g, h, i\}$) com a seguinte matriz de incidência*

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

   (a) *Determinar o grau de cada vértice.*
   (b) *Esboçar uma representação pictórica de $\mathcal{G}$.*
   (c) *Determinar a matriz de adjacência de $\mathcal{G}$.*

4. *Seja $\mathcal{G}$ o grafo correspondente à seguinte matriz de adjacência*

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

   (a) *Determinar o grau de cada vértice.*
   (b) *Esboçar uma representação pictórica de $\mathcal{G}$.*
   (c) *Determinar a matriz de incidência de $\mathcal{G}$.*

5. *Seja $\mathcal{G}$ o grafo correspondente à seguinte matriz de adjacência*

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

   Por um procedimento matricial indicar se existe um caminho entre os vértices 1 e 5.

6. *Usar um procedimento matricial para determinar se o grafo ao qual corresponde a matriz de adjacência*

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

é ou não conexo.

7. *Determinar o número total de arestas de um grafo completo com n vértices.*
8. *Determinar o número de arestas do grafo bipartido $K_{p,q}$.*
9. *Construir um grafo conexo simples com n vértices por forma que o grau de cada vértice seja igual a 2. Observar a estrutura deste grafo e comentá-la.*
10. *Provar que num grafo simples com 2 ou mais vértices, os graus dos vértices não podem ser todos distintos.*
11. *Considerar o digrafo $\mathcal{G} \equiv (V, E)$ onde*

$$V = \{1, 2, 3, 4, 5, 6\} \text{ e } E = \{(1,2), (2,3), (3,4), (4,5), (5,6), (1,6), (2,6), (5,2)\}$$

   (a) *Determinar um caminho de 1 a 6 de comprimento 6.*
   (b) *Determinar um caminho simples de 1 a 6 com 5 arcos.*
   (c) *Determinar um ciclo com 4 arcos.*
   (d) *Usar a matriz de adjacência de $\mathcal{G}$ para determinar o número de caminhos de 2 a 4 de comprimento 2.*
   (e) **Definição:** Chama-se **matriz de conexão** de um grafo ou digrafo com n vértices a uma matriz

$$R = [r_{ij}]_{1 \leq i,j \leq n}$$

   tal que $r_{ij} = 1$ se existir um caminho (ou caminho orientado, no caso dos digrafos) de i para j e $r_{ij} = 0$ no caso contrário.
   Determinar a matriz de conexão do grafo $\mathcal{G}$.

12. *Desenhar um grafo cuja matriz de adjacência é tal que*

$$A^2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 3 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix} \quad \text{e} \quad A^3 = \begin{bmatrix} 0 & 3 & 1 & 1 \\ 3 & 2 & 4 & 4 \\ 1 & 4 & 2 & 3 \\ 1 & 4 & 3 & 2 \end{bmatrix}$$

13. *Mostrar que a soma dos elementos da diagonal principal da segunda potência da matriz de adjacência de um grafo (traço de A^2) é igual a duas vezes o número de arestas do grafo.*

4.3 Caminhos Eulerianos e Hamiltonianos

Caminhos eulerianos. Os caminhos eulerianos são assim designados pela sua relação com o problema das pontes de Königsberg que foi resolvido por Euler. Considerem-se, antes de mais, as seguintes definições:

Definição 4.21 *Chama-se* **caminho euleriano** *a um caminho de um grafo que contém cada aresta uma e uma só vez. Um caminho euleriano que seja fechado designa-se por* **circuito euleriano**.

O problema das pontes de Königsberg é então o de saber se o correspondente grafo possui ou não algum circuito euleriano. A resposta geral é dada pelo seguinte teorema:

Teorema 4.22 (Euler) *Um grafo (ou multigrafo) conexo possui um caminho euleriano se e só se tiver um número de vértices de grau ímpar igual a 0 ou 2. O caminho euleriano é um circuito euleriano se aquele número for 0; de contrário, o caminho euleriano vai de um dos vértices de grau ímpar ao outro vértice também de grau ímpar.*

Demonstração: Recorde-se, antes de mais, que o número de vértices de grau ímpar é par (v. corolário 4.9). Mostrar-se-á, em primeiro lugar, que se o número de vértices de grau ímpar for 0 ou 2 então o grafo admite um caminho euleriano. Far-se-á a demonstração por indução finita denotando por $p(m)$ a afirmação do teorema onde m designa o número de arestas do grafo.

(i) – Para um grafo conexo com uma única aresta, há apenas duas possibilidades: ou o grafo tem um só vértice com um lacete ou o grafo tem dois vértices. No primeiro caso o grau do vértice é 2 e, portanto, há zero vértices de grau ímpar sendo o caminho obtido um circuito euleriano.

No segundo caso há dois vértices, cada um dos quais tem grau 1 – grau ímpar – pelo que a aresta em questão constitui um caminho euleriano que vai de um vértice de grau ímpar ao outro vértice de grau ímpar.

A proposição

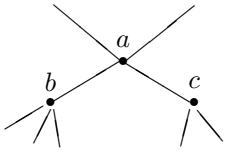
$$p(1)$$

é, assim, uma proposição verdadeira.

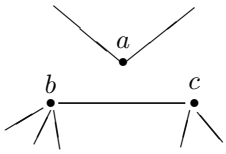
(ii) – Suponha-se agora, hipótese de indução, que $p(m)$ é verdadeira para todo o $m \leq k$ e vejamos o que se passa com $p(k+1)$. Seja $\mathcal{G} \equiv (V, E)$ um grafo conexo com $k+1$ arestas que tem 2 ou menos vértices de grau ímpar. O método de prova agora consiste em reduzir para k o número de arestas a fim de usar a hipótese de indução. O problema que se levanta é o de que o grafo seja desconectado durante o processo.

Visto que a proposição $p(1)$ já foi provada pode admitir-se que $\mathcal{G}$ tem mais de duas arestas (que não são lacetes) e, portanto, possui pelo menos um vértice de

grau par positivo. Seja a esse vértice. Pode então garantir-se que há pelo menos duas arestas incidentes em a que se denotarão, respectivamente, por $\{a, b\}$ e $\{a, c\}$.



Construa-se agora um novo grafo $\mathcal{G}' \equiv (V', E')$ onde $V' = V$ e E' é igual a E exceptuando as arestas $\{a, b\}$ e $\{a, c\}$ que foram retiradas e substituídas por uma nova aresta $\{b, c\}$



O grafo $\mathcal{G}'$ tem k arestas e o mesmo número de vértices ímpares que $\mathcal{G}$. Há então duas possibilidades: ou $\mathcal{G}'$ é conexo ou é desconexo.

Se $\mathcal{G}'$ for conexo então, pela hipótese de indução, pode encontrar-se um caminho euleriano em $\mathcal{G}'$. Este caminho pode tornar-se um caminho euleriano em $\mathcal{G}$ substituindo a parte do caminho que usa a aresta $\{b, c\}$ pela sequência de vértices bac que usa as arestas $\{a, b\}$ e $\{a, c\}$.

Se $\mathcal{G}'$ for desconexo, o problema fica um pouco mais complicado. Neste caso $\mathcal{G}'$ possui duas componentes conexas: uma contém o vértice a e a outra contém os vértices b e c (é claro que b e c devem estar na mesma componente conexa porque $\mathcal{G}'$ contém a aresta $\{b, c\}$). Designem-se estas duas componentes conexas por $\mathcal{G}'_a$ e $\mathcal{G}'_{bc}$, respectivamente. Cada uma destas componentes constitui um grafo conexo com k ou menos arestas. O grafo $\mathcal{G}'$ tem exactamente o mesmo número de vértices de grau ímpar que $\mathcal{G}$: assim, nas duas componentes não há mais que dois vértices de grau ímpar, pelo que se pode aplicar a hipótese de indução tanto a $\mathcal{G}'_a$ como a $\mathcal{G}'_{bc}$.

Se $\mathcal{G}$ tiver 0 vértices de grau ímpar então nenhuma das componentes $\mathcal{G}'_a$ e $\mathcal{G}'_{bc}$ possui vértices de grau ímpar; se $\mathcal{G}$ tiver 2 vértices de grau ímpar então, tendo em conta o corolário 4.9), uma das componentes terá 2 vértices de grau ímpar e a outra componente terá 0 vértices de grau ímpar.

Há, assim, três situações distintas:

- 2 vértices de grau ímpar em $\mathcal{G}'_a$ e 0 vértices de grau ímpar em $\mathcal{G}'_{bc}$,
- 2 vértices de grau ímpar em $\mathcal{G}'_{bc}$ e 0 vértices de grau ímpar em $\mathcal{G}'_a$,
- 0 vértices de grau ímpar tanto em $\mathcal{G}'_a$ como em $\mathcal{G}'_{bc}$.

Considere-se o primeiro caso: 2 vértices de grau ímpar em $\mathcal{G}'_a$ e 0 vértices de grau ímpar em $\mathcal{G}'_b$. Se há dois vértices de grau ímpar em $\mathcal{G}'_a$, tendo em conta a hipótese de indução, existe um caminho euleriano de $\mathcal{G}'_a$

$$i_1 x_1 \dots x_m a x_{m+1} \dots x_k i_2$$

que liga os dois vértices i_1 e i_2 de grau ímpar. Pela hipótese da indução também se sabe que existe em $\mathcal{G}'_{bc}$ um circuito euleriano

$$w_1 \dots w_p b c w_{p+1} \dots w_1$$

Removendo $\{b, c\}$ do circuito e ligando estes dois vértices ao outro caminho de acordo com

$$i_1 x_1 \dots x_m a c w_{p+1} \dots w_1 \dots w_p b a x_{m+1} \dots x_k i_2$$

obtém-se um caminho euleriano do grafo $\mathcal{G}$ (note-se que $\{a, b\}$ e $\{a, c\}$ estão incluídos e que $\{b, c\}$ desapareceu). Então, neste caso, tem-se

$$p(1), p(2), \dots, p(k) \;\Rightarrow\; p(k+1)$$

Invocando agora o princípio de indução matemática fica demonstrado que, neste caso, se o número de vértices de grau ímpar for 0 ou 2 o grafo admite um circuito ou caminho euleriano.

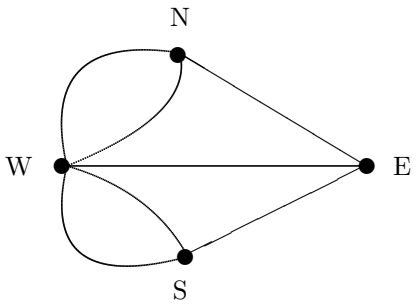
As duas situações restantes tratam-se de forma semelhante.

Reciprocamente, suponha-se que o grafo admite o seguinte caminho euleriano

$$a x_1 \dots x_n b$$

Cada um dos vértices x_i ocorre em duas arestas pelo que o seu grau é par. Os únicos vértices que podem ter grau ímpar são, assim, os vértices a e b. Se $a = b$ todos os vértices têm grau par; se $a \neq b$ há apenas dois vértices de grau ímpar. □

Exemplo 4.23 Regressando ao problema das pontes de Königsberg, recorde-se que o grafo que lhe corresponde é o seguinte:



Neste grafo com 4 vértices todos eles têm grau ímpar: de acordo com o teorema, tal grafo não possui qualquer caminho (ou circuito) euleriano. Ficou assim resolvido, de uma vez por todas, pela negativa, o problema dos habitantes de Königsberg (Kaliningrad).

Caminhos hamiltonianos. Um problema relacionado com o anterior, mas consideravelmente de maior dificuldade de resolução foi colocado pelo matemático irlandês W. Hamilton (1805-1865).

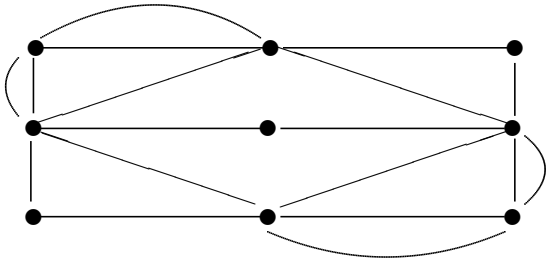
Definição 4.24 *Seja $\mathcal{G} \equiv (V, E)$ um grafo. Um caminho de $\mathcal{G}$ diz-se* **hamiltoniano** *se passar uma e uma só vez por cada um dos vértices do grafo.*

Embora o problema da existência de ciclos hamiltonianos possa parecer semelhante ao problema da determinação de circuitos eulerianos de um grafo, a verdade é que não é nada fácil dizer se um grafo é ou não hamiltoniano em geral. Há alguns resultados parcelares, mas não há resultados gerais.

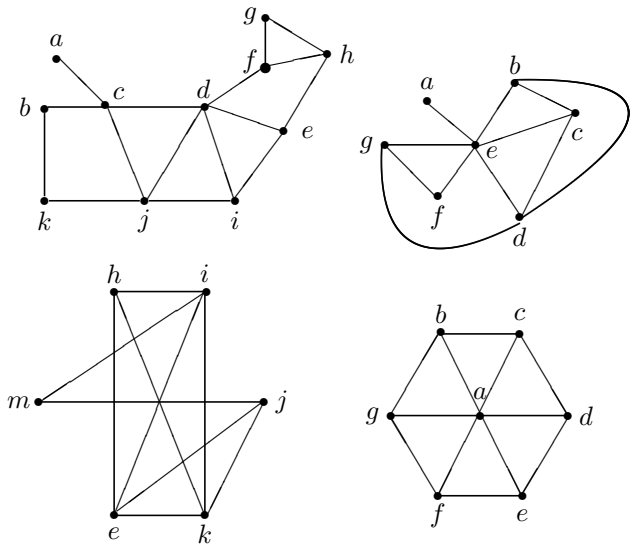
Exemplo 4.25 No exemplo 4.3 foi introduzido o chamado **problema do caixeiro viajante** que pretende elaborar um percurso no qual visite cada cidade exactamente uma vez voltando depois ao ponto de partida. Um tal percurso constitui um ciclo hamiltoniano. Se tais ciclos hamiltonianos existirem o problema que se segue então é o da determinação do percurso (ciclo hamiltoniano) de custo mínimo. O problema do caixeiro viajante, de descrição muito simples, faz parte de uma classe de problemas bem conhecidos que são de resolução geralmente muito difícil.

Exercícios 4.3.1

1. *Determinar um circuito euleriano no seguinte grafo*



2. *Verificar se algum dos grafos que se seguem possui um caminho euleriano. Determiná-lo no caso afirmativo e justificar os casos negativos.*



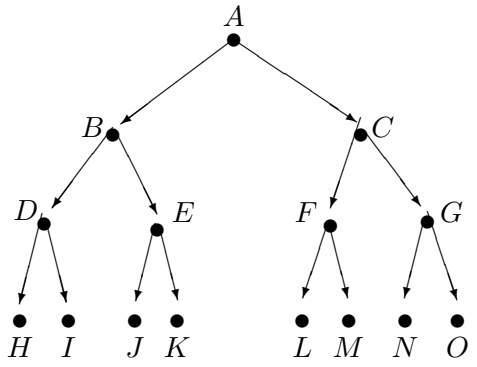
4.4 Árvores e Florestas

Esta secção é dedicada a um tipo especial de grafos que tem grande importância nas ciências da computação.

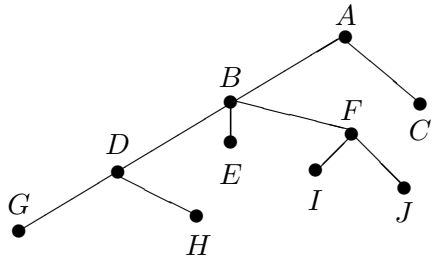
Definição 4.26 *Dir-se-á que um grafo T é uma árvore se possuir as duas propriedades seguintes:*

T1 – *T é um grafo conexo,*
T2 – *não existem ciclos em T.*

Uma árvore pode ser dirigida ou não dirigida consoante T seja um digrafo ou, simplesmente, um grafo. O termo árvore sem qualquer qualificativo interpreta-se sempre no sentido de ser uma árvore não dirigida. O digrafo



é um exemplo de uma árvore dirigida. O grafo



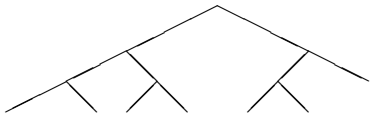
é um exemplo de uma árvore.

As árvores (orientadas ou não) têm muitas aplicações. São especialmente adequadas para representar estruturas hierarquizadas. Em *"coding theory"* e *"searching"* usam-se tipos de árvores especiais que são conhecidas por árvores binárias.

Definição 4.27 *Um grafo diz-se uma árvore binária se for uma árvore e*

1. *possuir um vértice especial, chamado* **raiz** *cujo grau é 2 ou 0,*
2. *qualquer outro vértice (para além da raiz) tem grau 3 ou 1.*

A árvore da figura que se segue



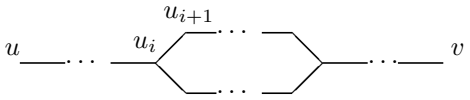
é um exemplo de uma árvore binária.

Enunciar-se-ão agora algumas propriedades importantes das árvores.

Teorema 4.28 *Numa árvore T existe um único caminho simples entre cada par de vértices.*

Demonstração: Sejam u e v dois vértices quaisquer de uma árvore T. Visto que T é um grafo conexo então existe pelo menos um caminho entre u e v e, portanto, existe um caminho simples entre aqueles dois vértices. Suponha-se que, se possível, P e P' são dois caminhos simples entre aqueles dois vértices. Se P e P' forem diferentes então existe uma aresta que pertence a um e não pertence ao outro. Suponha-se que e é a primeira aresta que está em P mas não em P' quando se caminha de u para v, isto é, suponha-se que se tem

$$\begin{array}{lccccccc} P: & u & \ldots\ldots & u_i & \overset{e}{\ldots} & u_{i+1} & \ldots\ldots & v \\ P': & u & \ldots\ldots & u_i & \ldots & v_{i+1} & \ldots\ldots & v \end{array}$$



Seja W o conjunto de vértices intermédios de P situados entre u_{i+1} e v e seja W' o conjunto de vértices intermédios de P' situados entre v_{i+1} e v. Se W e W' não tiverem quaisquer elementos comuns, então obter-se-á um ciclo percorrendo todos os vértices de W a partir de u_i e depois todos os vértices de W' (desde v até u_i). Esta hipótese não pode ocorrer pois T não possui ciclos, por hipótese.

Por outro lado, supondo que W e W' têm vértices comuns seja u_r o primeiro vértice de P que pertence também a W' de tal forma que nenhum vértice entre u_i e u_r está em P'. Então obtém-se novamente um ciclo partindo de u_i até u_r em P e de u_r a u_i em P'.

Quer dizer, a hipótese de existir mais que um caminho simples entre dois vértices distintos de T implica a existência de um ciclo em T. Como T não possui ciclos então entre dois vértices quaisquer de T há apenas um caminho simples. □

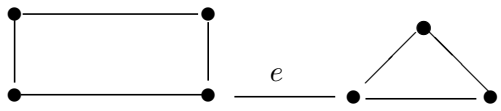
O recíproco é também verdadeiro no seguinte sentido:

Teorema 4.29 *Se num grafo $\mathcal{G}$ existir apenas um único caminho simples entre dois quaisquer dos seus vértices, então $\mathcal{G}$ é uma árvore.*

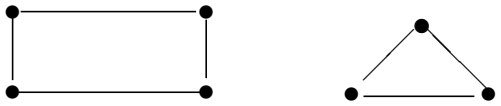
Demonstração: Suponha-se que $\mathcal{G}$ não é uma árvore. Então existe pelo menos um ciclo C em $\mathcal{G}$ o que implica que entre dois vértices de C existem dois caminhos simples contradizendo assim a hipótese feita. Então $\mathcal{G}$ é uma árvore, como se tinha afirmado. □

Definição 4.30 *Uma aresta de um grafo conexo é designada por* **ponte** *se a sua remoção (sem retirar os vértices) tornar o grafo desconexo.*

Por exemplo, no grafo



a aresta e é uma ponte: de facto a sua remoção origina o grafo



que é desconexo. Então, tem-se o seguinte resultado:

Teorema 4.31 *Numa árvore cada aresta é uma ponte.*

Demonstração: Visto que uma aresta entre dois vértices a e b de uma árvore T é o único caminho entre eles, então a sua supressão transforma T num grafo desconexo deixando, portanto, de ser uma árvore. □

Reciprocamente,

Teorema 4.32 *Se $\mathcal{G}$ for um grafo conexo no qual cada aresta é uma ponte então $\mathcal{G}$ é uma árvore.*

Demonstração: Suponha-se que $\mathcal{G}$ não é uma árvore, seja C um ciclo em $\mathcal{G}$ e suponha-se que e designa uma aresta em C. Seja $\mathcal{G}'$ o grafo que se obtém suprimindo a aresta e em $\mathcal{G}$. Visto que, por hipótese, e é uma ponte então $\mathcal{G}'$ é desconexo.

Sejam p e q dois vértices quaisquer de $\mathcal{G}$. Como $\mathcal{G}$ é conexo existe um caminho P entre p e q. Se P não contiver e então existe também um caminho entre p e q no grafo desconexo $\mathcal{G}'$. Por outro lado, se $e = \{v, w\}$ for uma aresta de P que também pertence ao ciclo C que parte, por exemplo, do vértice t, obtém-se o seguinte caminho em $\mathcal{G}'$ entre p e q

$$p \ldots\ldots v \ldots\ldots t \ldots\ldots w \ldots\ldots q$$

(substitui-se a aresta e pelo resto do circuito C que vai de v a w). Por outras palavras, existe sempre um caminho entre cada par de vértices de $\mathcal{G}'$ o que contraria o facto de $\mathcal{G}'$ ser desconexo. □

Teorema 4.33 *Uma árvore T com n vértices tem $n-1$ arestas.*

Demonstração: Far-se-á a demonstração por indução sobre n.

(i) – A proposição é evidentemente verdadeira para $n = 1$ (uma vez que numa árvore não pode haver lacetes).

(ii) – Suponha-se que a proposição é verdadeira para todo o m natural tal que $1 < m < n$. Seja $e = \{u, v\}$ uma aresta de T a qual, como T é uma árvore, tendo em conta o teorema anterior, é uma ponte.

Suprimindo a aresta e obtém-se um subgrafo T' desconexo com duas componentes conexas H e H'. Tanto H como H' são árvores com k e k' vértices que são números inteiros positivos tais que $k + k' = n$. Então tanto k como k' são menores que n. Pela hipótese de indução H tem $k-1$ arestas e H' tem $k'-1$ arestas e as duas componentes juntas têm $(k-1)+(k'-1) = (k+k')-2 = n-2$ arestas. Então T' tem $n-2$ arestas e, consequentemente, T tem $n-1$ arestas.

Fazendo apelo ao princípio de indução completa fica provado o teorema. □

O recíproco é também verdadeiro:

Teorema 4.34 *Qualquer grafo conexo com n vértices e $n-1$ arestas é uma árvore.*

Demonstração: Se $\mathcal{G} \equiv (V, E)$ não fosse uma árvore existiria uma aresta e que não seria uma ponte. Suprima-se e para obter o grafo $\mathcal{G}' \equiv (V, E')$. Continue-se este processo até obter um subgrafo $\mathcal{H} \equiv (V, F)$ no qual cada aresta seja uma ponte. Então $\mathcal{H}$ é uma árvore com $n-1$ arestas. Isto significa que após este processo de remoção de arestas acabou por se ficar com o mesmo número, ou seja, que o grafo inicial já era uma árvore. □

Definição 4.35 *Um subgrafo T de um grafo $\mathcal{G}$ com n vértices diz-se uma* **árvore suporte de $\mathcal{G}$** *se*

1. *T for uma árvore e*
2. *T tiver exactamente n vértices*

Teorema 4.36 *Um grafo $\mathcal{G}$ é conexo se e só se possuir uma árvore suporte.*

Demonstração: Se $\mathcal{G}$ possuir uma árvore suporte então, visto que a árvore é conexa e possui o mesmo número de vértices que $\mathcal{G}$, $\mathcal{G}$ é conexo.

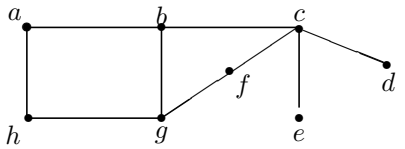
Reciprocamente, suponha-se que $\mathcal{G}$ é um grafo conexo. Sejam $v_1, v_2, \ldots, v_n$ os vértices de $\mathcal{G}$. Seleccione-se um destes vértices e atribua-se-lhe a etiqueta 1. Considerem-se agora os vértices adjacentes ao vértice etiquetado por 1: escolha-se um destes vértices, atribua-se-lhe a etiqueta 2 e marque-se a aresta $\{1, 2\}$, que não pode voltar a ser usada. Procedendo de modo semelhante, suponha-se que se etiquetou o vértice v_i com o número inteiro k. Procure-se entre os vértices adjacentes a k se existe algum que ainda não esteja etiquetado: se tal se verificar, escolha-se um tal vértice, atribua-se-lhe a etiqueta $k + 1$ e marque-se a aresta $\{k, k + 1\}$ para não voltar a ser usada.

Pode, no entanto, acontecer que todos os vértices adjacentes a k estejam já etiquetados. Neste caso recua-se para o vértice $k - 1$ e pesquisa-se a existência de vértices ainda não etiquetados adjacentes a $k - 1$. Se existir um atribua-se-lhe a etiqueta $k + 1$ e marque-se a aresta $\{k - 1, k + 1\}$ para não voltar a ser usada.

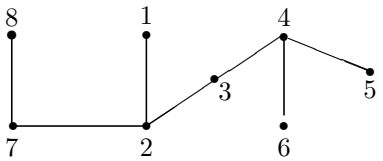
Continua-se este processo até que todos os vértices estejam etiquetados o que acontecerá necessariamente visto o grafo ser conexo. (Se o grafo não fosse conexo recuar-se-ia até ao vértice 1 antes de todos os vértices do grafo estarem etiquetados.)

O subgrafo constituído pelos n vértices originais e as arestas marcadas é uma árvore – a árvore suporte do grafo. □

Exemplo 4.37 Para exemplificar o processo descrito, considere-se o seguinte grafo



Então a árvore



é uma árvore geradora do grafo inicial.

Definição 4.38 *Chama-se* **floresta** *a um grafo constituído por várias componentes conexas, cada uma das quais é uma árvore.*

Exercícios 4.4.1

1. *Seja $\mathcal{G}$ uma floresta com n vértices, m arestas e k componentes. Determinar m em função de n e k.*
2. *Suponha-se que uma árvore tem 2 vértices de grau 5, 3 vértices de grau 4, 6 vértices de grau 3, 8 vértices de grau 2 e r vértices de grau 1. Determinar r.*
3. *Um grafo conexo tem 20 vértices. Determinar o número mínimo de arestas que o grafo pode ter.*
4. *Um grafo $\mathcal{G}$ tem 20 arestas. Determinar o número máximo de vértices que o grafo pode ter.*
5. *Suponha-se que $\mathcal{G}$ tem 4 componentes conexas, 20 arestas e r vértices. Determinar o valor máximo de r.*
6. *Uma aresta e de um grafo conexo $\mathcal{G}$ pertence a todas as possíveis árvores suporte de $\mathcal{G}$. Que se pode afirmar relativamente à aresta e?*

Bibliografia

[1] David C. Kurtz, *Foundations of Abstract Mathematics*, McGraw-Hill International Editions, NY 1992.

[2] J. Sebastião e Silva

[3] J. Sebastião e Silva

[4] V. K. Balakrishnan, *Introductory Discrete Mathematics*, Dover, NY 1991.

[5] Richard A. Brualdi, *Introductory Combinatorics*, North-Holland, NY 1979.

[6] Stephen A. Wiitala, *Discrete Mathematics. A Unified Approach*, McGraw-Hill International Editions, Computer Science Series, NY 1987.

[7] Michael O. Albertson & Joan P. Hutchinson, *Discrete Mathematics with Algorithms*, John Wiley & Sons, NY 1988.

[8] Martin J. Erickson, *Introduction to Combinatorics*, John Wiley & Sons, NY 1996.

[9] Domingos M. Cardoso, *Curso sobre Grafos e Combinatória* (Apontamentos), U. Aveiro, Abril de 1999.

[10] Jorge Picado, *Curso sobre Teoria dos Grafos* (Apontamentos manuscritos), U. Coimbra, 1998

[11] John P. D'Angelo & Douglas B. West, *Mathematical Thinking*, Prentice Hall, 1997.

[12] Alan Tucker, *Applied Combinatorics*, John Wiley & Sons, 1984.

[13] A. Chetwynd & P. Diggle, *Discrete Mathematics*, Arnold, 1995.

[14] J. Eldon Whitesitt, *Boolean Algebra and its Applications*, Dover, 1995.

[15] Douglas Kaye, *Sistemas Booleanos*, Editorial Alhambra, 1970.

[16] Normann L. Biggs, *Discrete Mathematics*, Oxford Science Publications, 1993.

[17] Walter Ladermann & Alan J. Weir, *Group Theory*, Longman, 1996.

[18] Oystein Ore, *Graphs and Their Uses*, The Mathematical Association of America, 1990.