

Matemática Discreta

Combinatória, Teoria dos Grafos e Algoritmos

Domingos Moreira Cardoso

Jerzy Szymański

Mohammad Rostami

Versão Revista

(2011)

Conteúdo

Introdução	ix
I Conceitos e Resultados Gerais	1
1 Linguagem Matemática e Lógica Informal	3
1.1 Sistemas matemáticos	3
1.2 Noção de conjunto	6
1.3 Linguagem proposicional	7
1.4 Operações sobre conjuntos	11
1.5 União e intersecção generalizadas e quantificadores	14
1.6 Relações	16
1.6.1 Relações de ordem	19
1.6.2 Relações de equivalência	20
1.6.3 Funções	22
1.7 Cardinalidade	26
1.8 Algumas notas históricas	31
1.9 Exercícios.	33
2 Contextos e Estratégias de Demonstração	37
2.1 Estratégias de demonstração da implicação	37
2.1.1 Prova directa	37
2.1.2 Demonstração por contraposição	39
2.1.3 Demonstração por redução ao absurdo	40
2.2 Princípio de indução	41
2.3 Princípio da gaiola dos pombos	49
2.4 Exercícios.	51
II Combinatória	55
3 Princípios de Enumeração Combinatória	57
3.1 Princípio da bijecção	57
3.2 Princípios da adição e da multiplicação	60
3.3 Princípio de inclusão-exclusão	64
3.4 Exercícios	68

4 Agrupamentos e Identidades Combinatórias	71
4.1 Arranjos com repetição	71
4.2 Arranjos e combinações simples	72
4.3 Combinações e permutações com repetição	77
4.4 Permutações	81
4.5 Identidades combinatórias	85
4.6 Exercícios	90
5 Recorrência e Funções Geradoras	93
5.1 Dependências recursivas simples	93
5.2 Equações de recorrência homogéneas	95
5.3 Equações de recorrência lineares não homogéneas	102
5.4 Equações de recorrência não lineares	106
5.5 Funções geradoras	109
5.5.1 Séries formais de potências	110
5.5.2 Funções geradoras ordinária e exponencial	115
5.6 Equações de recorrência e funções geradoras	118
5.7 Funções geradoras de várias variáveis	123
5.8 Exercícios	124
6 Números Combinatórios	127
6.1 Factoriais e números binomiais	127
6.2 Números de Fibonacci e o número de ouro	130
6.3 Números de Stirling	136
6.4 Números de Euler	141
6.5 Números de Bell	144
6.6 Números de Catalan	145
6.7 Exercícios	150
III Abordagens Algébricas da Combinatória	153
7 Conjuntos Parcialmente Ordenados e Reticulados	155
7.1 Conjuntos ordenados – definições básicas	155
7.2 Funções entre conjuntos parcialmente ordenados	158
7.3 Reticulados	161
7.3.1 Definições e conceitos básicos	162
7.3.2 Subreticulados e isomorfismos	164
7.3.3 Reticulados distributivos	167
7.3.4 Representação de reticulados distributivos	170
7.3.5 Topologias finitas e reticulados	171
7.4 Cadeias e anticadeias	180
7.5 Relações de ordem fraca, intervalar e semi-transitivas	185
7.6 Teorema da inversão de Möbius	189
7.7 Conjuntos extremais	194
7.8 Exercícios	197

8 Divisibilidade e Aritmética Modular	201
8.1 Algoritmo de Euclides	202
8.2 Funções de Euler e de Möbius	204
8.3 Relações de congruência	208
8.4 Equações e polinómios em corpos finitos	212
8.5 Corpos de Galois	216
8.6 Quadrados latinos e quadrados mágicos	225
8.7 Exercícios	233
9 Designs Combinatórios e Geometrias Finitas	237
9.1 Designs combinatórios	237
9.2 Planos projectivos e afins	244
9.3 Quadrados latinos e planos afins e projectivos	254
9.4 Espaços projectivos	259
9.5 Matrizes de Hadamard	263
9.6 Exercícios	267
10 Álgebras de Boole	271
10.1 Definições e resultados básicos	271
10.2 Cálculo proposicional e circuitos lógicos	277
10.3 Átomos e isomorfismos	285
10.4 Funções booleanas	289
10.5 Mapas de Karnaugh	293
10.6 Exercícios	300
11 Grupos Finitos e Enumeração de Pólya	305
11.1 Introdução aos grupos finitos	305
11.2 Lema de Burnside	310
11.3 Teorema de Pólya	314
11.4 Grupo diedral	319
11.5 Exercícios.	322
IV Teoria dos Grafos e Algoritmos	327
12 Conceitos e Resultados Fundamentais	329
12.1 Grafos orientados e não orientados	329
12.2 Representações de grafos em computador	333
12.3 Isomorfismos, grafos etiquetados e não etiquetados	335
12.4 Conceitos métricos	336
12.5 Grafos e subgrafos particulares	338
12.6 Exemplos de enumeração de grafos simples	341
12.7 Sequências de graus de vértices	343
12.8 Algoritmos de pesquisa em grafos	347
12.9 Exercícios	350
13 Conexidade	357
13.1 Grafos Conexos	357
13.2 Determinação de componentes conexas	361
13.3 Algoritmo de fusão de vértices	362
13.4 Grafos orientados fortemente conexos	369

13.5 Algoritmo de Leifman	371
13.6 Exercícios	375
14 Caminhos	379
14.1 Relações entre diâmetro, cintura e número de vértices	379
14.2 Pesquisa em largura em grafos sem custos nas arestas	385
14.3 Custos não negativos – algoritmo de Dijkstra	387
14.4 Custos arbitrários – algoritmo de Bellman-Ford	393
14.5 Algoritmo de Floyd	395
14.6 Exercícios	398
15 Árvores	401
15.1 Árvores e florestas	401
15.2 Número de árvores abrangentes	403
15.3 Geração de todas as árvores abrangentes	406
15.4 Código de Prüfer	410
15.5 Árvores abrangentes de custo mínimo	413
15.5.1 Algoritmo de Kruskal	413
15.5.2 Algoritmo de Prim	415
15.6 Exercícios	418
16 Fluxos em Redes	423
16.1 Fluxo máximo em redes	423
16.1.1 Teorema de Ford e Fulkerson	425
16.1.2 Algoritmo para o fluxo máximo	428
16.2 Fluxo de custo mínimo	432
16.2.1 Soluções básicas admissíveis	433
16.2.2 Método simplex para redes	437
16.3 Exercícios	444
17 Emparelhamentos	449
17.1 Emparelhamentos máximos e perfeitos	449
17.2 Emparelhamentos em grafos bipartidos	452
17.2.1 Sistemas de representantes distintos	454
17.2.2 Uma aplicação à partição mínima de cpos em cadeias	457
17.2.3 Problema de afectação de tarefas	460
17.2.4 Problema de afectação óptima de tarefas	463
17.3 Emparelhamentos em grafos arbitrários	468
17.4 Emparelhamentos em grafos com pesos nas arestas	473
17.5 Exercícios	476
18 Grafos de Euler e Grafos de Hamilton	479
18.1 Grafos de Euler	480
18.1.1 Algoritmos de Hierholzer e de Fleury	483
18.1.2 Problema do carteiro chinês	485
18.2 Grafos de Hamilton	489
18.2.1 Código de Gray	493
18.2.2 Problema do caixeiro viajante	496
18.3 Exercícios	502

19 Independentes, Cliques e Colorações	507
19.1 Conjuntos independentes e cliques	507
19.2 Coloração de vértices	511
19.2.1 Uma aplicação das funções booleanas	518
19.2.2 Polinómios cromáticos	522
19.2.3 Colorações parciais e Sudoku	526
19.3 Coloração de arestas	533
19.3.1 Números de Ramsey para grafos simples	536
19.4 Exercícios	541
20 Grafos Planares e Generalizações	547
20.1 O ponto de vista topológico	547
20.1.1 Realização de grafos em superfícies orientáveis	548
20.1.2 Menores e menores topológicos	550
20.2 Grafos planares	553
20.2.1 Propriedades dos grafos planares	554
20.2.2 Teorema de Kuratowski	556
20.2.3 Dualidade em grafos e digrafos planares	559
20.2.4 Grafos platónicos	562
20.3 Grafos com genus positivo	564
20.3.1 Fórmula de Euler generalizada	565
20.3.2 Grafos g -platónicos	567
20.4 Mapas e colorações	568
20.4.1 Teorema das quatro cores	569
20.4.2 Colorações em superfícies de genus positivo	574
20.4.3 Conjecturas de Hadwiger e Hajós	576
20.5 Exercícios	578
Apêndices	583
A Notação Assimptótica	585
A.1 Notação "O-grande" (O)	585
A.2 A notação "o-pequeno" (o)	588
A.3 Outras notações assimptóticas	589
A.4 Teorema da recorrência universal	591
A.5 Exercícios	593
B Notação	597
Bibliografia	601
Índice	607

Introdução

Matemática discreta é uma área da matemática que, ao longo das últimas décadas, se tem revelado de interesse crescente para um grande número de investigadores e estudantes em todo o mundo e que, neste período, tem tido um desenvolvimento exponencial. A este facto não são alheias as suas múltiplas aplicações, nomeadamente, nas *ciências da computação*, da qual também tem recebido muitas das suas principais motivações. Adicionalmente, as aplicações da matemática discreta estendem-se a áreas tais como: *as biociências, telecomunicações, electrónica, indústria de processadores, desenho de circuitos integrados, criptografia e segurança na transmissão de comunicações, sistemas de tráego automóvel ou outro, etc.* Por outro lado, a influência recíproca da matemática discreta com outras áreas da matemática é cada vez mais visível, como no caso da *investigação operacional, álgebra, teoria dos números, geometria e topologia*. O crescimento da matemática discreta obrigou à sua actual divisão em duas grandes áreas: a *combinatória* e a *teoria dos grafos*. É surpreendente o modo como a matemática discreta lida com processos que consistem em sequências de estados separados, ou conjuntos numeráveis (ou seja, contáveis) de objectos, onde se incluem, naturalmente, os conjuntos finitos, com padrões comuns, em muitos casos difíceis de identificar sem recurso às suas poderosas técnicas de análise. A enumerabilidade dos objectos de estudo é responsável pela designação de matemática *discreta* em oposição a *contínua*. No caso particular das estruturas finitas, entre os seus vários instrumentos de análise, devem salientar-se a *álgebra finita* (que inclui grupos, reticulados e corpos finitos), a *geometria finita* (que inclui a geometria projectiva e a geometria afim) e a *topologia finita* (que inclui a topologia digital), pelo papel de relevo que desempenham no respectivo contexto de actuação.

Objectivos

Este livro inclui os tópicos mais importantes em matemática discreta, os quais, na sua grande maioria, são apresentados a um nível intermédio, acessível à generalidade dos estudantes detentores de uma formação matemática básica ao nível do ensino secundário ou dos primeiros anos da universidade (no caso de alguns capítulos). No entanto, a necessidade de uma certa abrangência levou-nos a considerar tópicos mais avançados (que podem integrar cursos de pós-graduação) que, numa primeira leitura, devem ser ignorados por principiantes sem maturidade matemática suficiente. Podemos afirmar, porém, que este livro é auto-contido, no sentido em que inclui toda a informação necessária para a sua compreensão, a qual, convenientemente trabalhada, permitirá ao leitor atingir um nível de estudos adequado, no contexto da matemática discreta. Pretende-se também que este livro desperte, em muitos dos jovens estudantes, o interesse pela matemática e suas aplicações, captando-os e motivando-os para o seu aprofundamento. Com efeito, o facto de aqui se cruzarem várias das áreas mais relevantes da matemática, transforma este livro num instrumento privilegiado para um primeiro contacto com a linguagem, os conceitos e as metodologias mais actuais da matemática superior e da ciência em geral.

Embora a formação abrangente em matemática discreta seja o principal objectivo deste livro, por razões de espaço, ele não é suficientemente exaustivo para incluir todos os tópicos que, actualmente,

fazem parte da matemática discreta. Assim, ficaram de fora do âmbito deste texto, a *teoria dos códigos, criptografia, estruturas de dados, partições de inteiros e de conjuntos, estruturas aleatórias, teoria algébrica dos grafos, complexidade de algoritmos*, etc.

Para além dos cursos de matemática, este livro pode ser utilizado, de um modo geral, nos cursos de ciências e engenharia e, com especial importância, nos cursos de computação e informática.

A escolha dos tópicos, exercícios, aplicações e algoritmos, bem como a sua apresentação, foi dominada por muitos anos de experiência docente a diferentes níveis, para estudantes de diferentes cursos e com preparação distinta. Como resultado, este livro contém uma sequência de exemplos cuidadosamente escolhidos, acompanhados de resoluções detalhadas. No seu conjunto, eles constituem um caminho didáctico, com grau de dificuldade crescente, no qual se ilustra, de forma sistemática, o modo de se ultrapassarem dificuldades, o que é de grande utilidade para a compreensão da generalidade dos tópicos abordados. Note-se que em algumas secções, muitos conceitos e propriedades são introduzidos com recurso, exclusivo, a exemplos.

Os exercícios propostos, por sua vez, quer em número quer em qualidade, desempenham um papel central no método de estudo a levar a cabo. Com efeito, ao longo dos capítulos, recomenda-se vivamente a resolução sistemática de, pelo menos, parte deles.

Destinatários.

Os principais destinatários deste livro são, naturalmente, os estudantes dos primeiros anos da universidade e, para além destes, os professores de matemática ou de informática do ensino secundário (que aqui podem obter, não só uma actualização de conhecimentos, como também a motivação necessária para a formulação de problemas e para a apresentação de exemplos de interesse prático e didáctico aos seus alunos) e os professores do ensino superior, directa ou indirectamente, ligados à investigação matemática. Alguns capítulos, como são o caso dos que constituem a parte III, *Abordagens Algébricas da Combinatória*, e alguns dos que constituem a parte IV, *Teoria dos Grafos e Algoritmos*, podem ainda ser de grande utilidade como textos de apoio em cursos de pós-graduação ao nível de mestrado. Estes capítulos, incluem tópicos onde se apresentam problemas em aberto que fazem parte dos grandes desafios da investigação matemática contemporânea.

Conteúdo.

O livro está organizado em quatro partes principais. A parte I sobre conceitos e resultados gerais, a parte II sobre combinatória, a parte III sobre abordagens algébricas da combinatória e a parte IV sobre teoria dos grafos e algoritmos.

A parte I é constituída por dois capítulos. O primeiro capítulo inclui a notação básica e, após uma introdução à lógica proposicional, faz uma apresentação de tópicos elementares abstractos, passando pelo estudo de conjuntos (operações sobre conjuntos, conjuntos parcialmente ordenados e cardinalidade de conjuntos) e relações (relações de ordem, relações de equivalência e funções), analisando-se alguns resultados importantes, como são o caso dos teoremas de Tarski, Cantor e Schröder-Bernstein. O segundo capítulo é dedicado às técnicas de demonstração utilizadas em matemática, onde a lógica formal é utilizada para fundamentar directa ou indirectamente os respectivos métodos de prova, destacando-se, na parte final, a indução matemática e o princípio da gaiola dos pombos que é uma ferramenta essencial para muitos problemas de existência em matemática.

A parte II, que incide sobre a combinatória (que é uma área da matemática dedicada à enumeração e estudo de agrupamentos de objectos de acordo com certas regras específicas), é constituída por quatro capítulos (entre os capítulos 3 e 6). No capítulo 3 discutem-se, detalhadamente, os quatro princípios de enumeração mais utilizados em combinatória. O capítulo 4 lida com a contagem de agrupamentos particulares, como são o caso das combinações, permutações e arranjos (com ou sem repetição) e inclui o estudo de algumas identidades combinatórias. O capítulo 5 é dedicado ao estudo das equações de

recorrência e das funções geradoras que são instrumentos muito poderosos, utilizados em problemas de contagem. No capítulo 6 estudam-se algumas famílias de números combinatórios.

A parte III, que cobre várias abordagens algébricas em matemática discreta, é constituída por cinco capítulos (entre os capítulos 7 e 11). O capítulo 7 é dedicado ao estudo aprofundado dos conjuntos parcialmente ordenados, incluindo o estudo dos reticulados, topologias finitas, cadeias, anticadeias, teorema de Dilworth, teorema da inversão de Möbius, etc. No capítulo 8 dá-se especial atenção às funções de Euler e de Möbius (agora na sua versão clássica), ao teorema de Daniel da Silva (que constitui uma generalização do teorema de Euler), às relações de congruência, aos polinómios e corpos finitos, aos corpos de Galois e, finalmente, aos quadrados latinos e mágicos. No capítulo 9 estudam-se os *designs* combinatórios e as geometrias finitas (afins e projectivas) e suas ligações com os quadrados latinos e as matrizes de Hadamard. No capítulo 10 estudam-se, detalhadamente, as álgebras de Boole (que são reticulados muito especiais), discutindo-se, nomeadamente, o teorema da representação (para o caso finito), as funções booleanas e os mapas de Karnaugh com grande aplicação no desenho e projecto de circuitos digitais. O capítulo 11 é dedicado aos grupos finitos (nomeadamente, ao grupo diedral) e a certos problemas de enumeração combinatória de objectos com relações de simetria entre si, cuja resolução obriga à utilização do lema de Burnside ou do teorema de Pólya e que são difíceis de resolver com recurso aos métodos de contagem introduzidos em capítulos anteriores.

A parte IV é constituída por nove capítulos (entre os capítulos 12 e 20) cobrindo diferentes tópicos da teoria dos grafos e incluindo algoritmos para a resolução dos principais problemas de aplicação que se colocam no respectivo contexto. No capítulo 12 introduzem-se conceitos e resultados básicos fundamentais para a compreensão dos capítulos subsequentes. O capítulo 13 é dedicado ao estudo da conexidade em grafos e inclui algoritmos para a determinação de componentes conexas e fortemente conexas no caso de grafos orientados. No capítulo 14 estudam-se os caminhos, aprofundando-se os conceitos e resultados métricos, anteriormente abordados no capítulo 12, estudam-se majorantes e minorantes para a ordem dos grafos, em função de certas propriedades métricas, e caracterizam-se os grafos para os quais estes majorantes e minorantes são atingidos. Adicionalmente, introduzem-se vários algoritmos para a determinação de caminhos de comprimento mínimo (nomeadamente, a pesquisa em largura para grafos sem custos nas arestas, o algoritmo de Dijkstra para grafos ou digrafos com custos não negativos e os algoritmos de Bellman-Ford e de Floyd para grafos e digrafos com custos arbitrários). No capítulo 15 estudam-se as árvores que são grafos com propriedades particulares e que têm muitas aplicações em problemas práticos, estuda-se a determinação do número de árvores abrangentes de um grafo e respectiva geração, deduz-se o código de Prüfer, e descrevem-se e fundamentam-se os algoritmos de Kruskal e de Prim para a determinação de árvores abrangentes de custo mínimo. O capítulo 16 é dedicado ao estudo do fluxo em redes e inclui a análise do algoritmo de Ford-Fulkerson (de fluxo máximo corte mínimo) e o método simplex para redes, vocacionado para a determinação de fluxos de custo mínimo. No capítulo 17 estudam-se os emparelhamentos e algumas das suas aplicações, incluindo os respectivos algoritmos para a determinação de emparelhamentos máximos em grafos bipartidos e grafos arbitrários, com e sem pesos nas arestas. No capítulo 18 estudam-se os grafos eulerianos e hamiltonianos e alguns algoritmos de resolução de problemas práticos para os quais constituem modelos matemáticos adequados, como são os casos do problema do carteiro chinês, a determinação de códigos de Grey e o problema do caixeiro viajante. Para o problema do carteiro chinês apresenta-se o algoritmo de Edmonds e Johnson, para o problema do caixeiro viajante apresenta-se o algoritmo clássico de *branch and bound* de Little, Marty, Sweeney e Karel e ainda o algoritmo de *premiar e punir*. No capítulo 19 estudam-se os conjuntos independentes de vértices, as cliques, as colorações de vértices (incluindo a sua abordagem como aplicação das funções booleanas), os polinómios cromáticos e as extensões cromáticas de colorações parciais (com aplicação em problemas relacionados com o puzzle Sudoku que é proposto à generalidade dos leitores de muitos jornais e revistas) e as colorações de arestas, conjuntamente com uma introdução aos números de Ramsey. A quarta parte termina com o capítulo 20, dedicado aos grafos planares e suas generalizações, que se inicia com uma abordagem topológica dos grafos, no contexto das suas realizações em superfícies orientáveis e dos

seus menores. Neste capítulo, os grafos planares têm uma especial importância, estudando-se várias das suas propriedades, o teorema de Kuratowski, a dualidade e os grafos platónicos. Adicionalmente, analisam-se os grafos com genus positivo (incluindo a dedução da fórmula de Euler generalizada e os grafos g -platónicos), as colorações de mapas (incluindo o teorema das quatro cores, as colorações em superfícies de genus positivo e duas conjecturas que constituem grandes desafios nesta área).

Deste texto fazem parte ainda dois apêndices, um dedicado à utilização da notação assimptótica e à realização de várias operações com esta notação e outro com a lista de símbolos utilizados ao longo dos capítulos, e uma lista bibliográfica actualizada.

Precedência entre capítulos e modos de estudo

Com o objectivo de flexibilizar a leitura deste livro, os tópicos que aparecem após os capítulos 1, 2, 3 e 4 têm o maior grau de independência possível, como acontece no caso dos capítulos incluídos na parte III que (com poucas excepções) podem ser estudados independentemente uns dos outros. Inevitavelmente, porém, alguns capítulos dependem intrinsecamente dos anteriores, variando essa dependência de caso para caso. A parte IV, por exemplo, embora não dependa significativamente da parte III, é constituída por capítulos que, na sua generalidade, dependem sequencialmente uns dos outros. Com base nestas relações de dependência entre capítulos, para facilitar o estudo e para permitir uma leitura mais apropriada à formação pretendida e à respectiva maturidade matemática, seguem-se algumas sugestões para percursos alternativos.

Aos leitores que pretendem iniciar a sua formação matemática pós-secundária e detêm uma cultura matemática que se baseia, unicamente, na aprendizagem conseguida até ao 12º ano de escolaridade, para uma primeira leitura, recomenda-se o seguinte percurso: capítulos 1 a 6 (ou seja, as partes I e II) e os capítulos 12 a 15 da parte IV. Em leituras subsequentes, porém, já se recomenda uma passagem gradual por um cada vez maior número de capítulos da parte III e restantes capítulos da parte IV.

Aos leitores que frequentam disciplinas de matemática discreta nos primeiros anos da universidade, embora possam ignorar os primeiros dois capítulos, chama-se a atenção para o facto de uma revisão dos conceitos e metodologias ali abordados poder vir a fortalecer a sua capacidade de compreensão da matemática. Os capítulos das partes II, III e IV, devem ser percorridos de acordo com os tópicos estudados na disciplina, sem desrespeitar as regras de precedência anteriormente referidas. É claro que este livro pode servir de base ao programa da disciplina de matemática discreta a leccionar a diferentes cursos universitários de ciências e engenharia, como sejam, os cursos de matemática, ciências da computação, informática, etc. Neste caso, se a disciplina é leccionada num único semestre, sugere-se que os capítulos 1, 2 e 3 sejam abordados com uma cadência mais rápida, de modo que o tempo restante seja devidamente aproveitado para um estudo mais pausado dos capítulos 4, 5 e 6 e dos capítulos 12 a 15. Se a disciplina é leccionada durante dois semestres, dependendo dos seus objectivos, sugere-se que se acrescentem alguns capítulos das partes III e IV.

Os alunos de pós-graduação podem estudar grande parte dos capítulos deste livro numa disciplina anual (ou semestral, mas nesse caso, com ritmo muito elevado) que inclua todos os capítulos das partes III e IV, com demonstrações detalhadas.

Agradecimentos.

Os dois primeiros autores desejam expressar o seu agradecimento ao Centro de Estudos em Optimização e Controlo - CEOC, da Fundação para a Ciéncia e Tecnologia - FCT, co-financiado pela Comunidade Europeia FEDER/POCI 2010, o apoio financeiro por diversas vezes concedido nas múltiplas actividades realizadas ao longo de todo o período de preparação deste livro. Ao colega Marian Dondajewski pela preciosa ajuda que nos deu na preparação de muitas das figuras. Aos Professores do Departamento de Matemática Discreta da Universidade de Adam Mickiewicz, especialmente Jerzy Jaworski, Michał Karoński, Zbigniew Palka e Andrzej Ruciński, uma vez que muito dos exemplos e

exercícios deste livro são utilizados por todos eles e é quase impossível determinar o autor. A vários colegas do Departamento de Matemática da Universidade de Aveiro, entre os quais: Agostinho Agra, Paula Rama, Paula Carvalho e Rosa Amélia Martins, pela leitura cuidada que fizeram de todo ou parte do livro, e pelas correções e sugestões de vária ordem que melhoraram a apresentação final deste texto. Apesar disso, ainda é possível que existam alguns erros até ao momento não detectados, relativamente aos quais, naturalmente, assumimos a inteira responsabilidade.

Às nossas companheiras Manela, Maria e Simin.

DMC, JS, MR

Aveiro, Fevereiro de 2008

Parte I

Conceitos e Resultados Gerais



1

Linguagem Matemática e Lógica Informal

Usualmente refere-se que a actividade matemática começa quando, a partir da percepção de um certo número de objectos nos separamos desses objectos particulares e, em vez deles, consideramos o inteiro correspondente. Mais geralmente, elevando o nível de abstracção, os desenvolvimentos matemáticos passam pela criação de diferentes entidades que representamos por variáveis, as quais, por sua vez, denotamos usualmente por letras. Embora se utilizem, indiscriminadamente, os vários alfabetos, é comum recorrer-se ao alfabeto grego na representação de variáveis com significado especial. Seguem-se as letras minúsculas e maiúsculas do alfabeto grego.

α	A	alfa	ν	N	niu
β	B	beta	ξ	Ξ	xi
γ	Γ	gama	\omicron	O	omicron
δ	Δ	delta	π	Π	pi
ϵ (ε)	E	epsilon	ρ (ϱ)	P	ró
ζ	Z	zeta	σ (ς)	Σ	sigma
η	H	eta	τ	T	tau
θ (ϑ)	Θ	teta	υ	Υ	upsilon
ι	I	iota	ϕ (φ)	Φ	fi
κ	K	kapa	χ	X	chi
λ	Λ	lambda	ψ	Ψ	psi
μ	M	miu	ω	Ω	ómega

O entendimento da matemática exige a compreensão da sua linguagem e das estruturas lógicas que suportam as respectivas conclusões. Com esse objectivo, neste capítulo introduzem-se os principais conceitos envolvidos, quer utilizando as *definições* formais que os caracterizam rigorosamente, quer recorrendo a descrições informais que permitem o estabelecimento de um primeiro contacto, nomeadamente com alguns dos objectos e instrumentos essenciais ao estudo da matemática discreta. Antes, porém, convém analisar, ainda que brevemente, o conceito mais geral de sistema matemático.

1.1. Sistemas matemáticos

Tendo em conta que dois conjuntos A e B são iguais quando têm os mesmos elementos, podemos concluir que se $A \subseteq B$ e $B \subseteq A$ então $A = B$. Em matemática, este tipo de afirmações, que muitas vezes tomam a forma: *se certas suposições (hipóteses) são verdadeiras, então uma dada conclusão (tese) é também verdadeira*, designam-se por *teoremas*. Por sua vez, designam-se por proposições as afirmações

que podem ser verdadeiras ou falsas. As proposições evidentes ou que, no contexto matemático em que se está a trabalhar, aceitamos como verdadeiras, são chamadas *axiomas*. Os *teoremas* são as proposições verdadeiras que decorrem dos axiomas por aplicação de certas regras, que se designam por *regras de produção*, ou dos desenvolvimentos determinados pela lógica. Alguns resultados com características idênticas às dos teoremas, mas eventualmente mais simples (sendo esta qualificação subjectiva), designam-se por *lemas*. Adicionalmente, é usual designar por *corolários* os teoremas que são consequência imediata de outros teoremas. O conjunto dos axiomas, regras de produção e teoremas (onde se incluem lemas e corolários) constituem o que designamos por *teoria* ou *sistema matemático*.

Exemplo 1.1. Considere um sistema matemático onde as proposições são palavras do alfabeto de símbolos pertencentes ao conjunto $\{x, y, z\}$, com um único axioma xyz e cujas regras de produção são as seguintes:

- (RP1) Proposições obtidas a partir de uma proposição verdadeira, substituindo x por xyz , são proposições verdadeiras.
- (RP2) Proposições obtidas a partir de uma proposição verdadeira, substituindo xyz por yxz , são proposições verdadeiras.

Vamos mostrar que, no contexto deste sistema matemático, a proposição $yyxzz$ é um teorema.

Solução.

Teorema. $yyxzz$.

Demonstração. Do axioma xyz , por aplicação de (RP2), tem-se yxz . De yxz , aplicando (RP1), tem-se $yxyzz$. Finalmente, da aplicação de (RP2) a $yxyzz$, decorre $yyxzz$. \square

Mais geralmente, é possível mostrar que qualquer proposição da forma

$$\underbrace{y \dots y}_n \underbrace{x z \dots z}_n,$$

onde n é um inteiro positivo, é um teorema da teoria definida neste exemplo. \square

A escolha dos axiomas de um determinado sistema matemático pode ser uma tarefa difícil. Em particular, o sistema de axiomas deve ser *consistente*, isto é, não deve permitir a dedução de um teorema e da sua negação. Também é conveniente que o sistema de axiomas seja *independente*, isto é, que não inclua axiomas que sejam consequência de outros axiomas. Com efeito, se um axioma é consequência de outros axiomas, ou seja, se um axioma pode ser obtido como teorema a partir de outros axiomas, a teoria que se obtém do sistema de axiomas, com ou sem esse axioma, é a mesma. Sendo assim, esse axioma é redundante e pode ser retirado. Outra condição que o sistema de axiomas deve satisfazer é a de ser constituído por proposições evidentes que não estejam, por isso, em contradição com a intuição matemática.

Como exemplo de sistema axiomático, pode indicar-se uma das primeiras teorias definidas axiomaticamente, a *geometria euclideana*, publicada nos *Elementos* de Euclides (c. 300 a.C.) que é o primeiro livro matemático com o objectivo de fundamentar uma área da matemática, neste caso a geometria, como teoria matemática. Os axiomas que Euclides escolheu para a geometria foram os seguintes postulados e noções comuns:

Postulado 1. Dados dois pontos existe uma única recta que os contém.

Postulado 2. Todo o segmento de recta está contido numa única recta.

Postulado 3. Dado um ponto C e um número real $r > 0$, existe uma única circunferência de centro C e raio r .

Postulado 4. Todos os ângulos rectos são iguais.

Postulado 5. *Axioma das paralelas:* dada uma recta e um ponto não pertencente a essa recta, existe uma única recta que contém o ponto e é paralela à recta dada.

Noção comum 1. Duas quantidades iguais a uma terceira são iguais.

Noção comum 2. Se a quantidades iguais adicionarmos a mesma quantidade, as somas obtidas são iguais.

Noção comum 3. Se a quantidades iguais subtrairmos a mesma quantidade, as diferenças obtidas são iguais.

Noção comum 4. Objectos coincidentes são iguais.

Noção comum 5. O todo é maior do que a parte.

Estes axiomas de Euclides foram aceites como intuitivamente evidentes pela maioria dos matemáticos da sua época e de épocas posteriores, com a excepção do *axioma das paralelas*. Com efeito, alguns matemáticos tentaram substituir o axioma das paralelas por outro que fosse mais evidente. Outros tentaram mostrar, sem sucesso, que este axioma era consequência dos outros nove axiomas da geometria de Euclides. Porém, só 2 100 anos após a publicação dos Elementos de Euclides é que os matemáticos tomaram consciência do facto que a geometria proposta por Euclides era uma das possíveis definições de geometria. Substituindo o axioma das paralelas por outro(s) axioma(s) definiram-se outras geometrias. As teorias decorrentes das novas definições foram catalogadas sob o nome de geometrias não-euclidianas. Uma teoria diz-se *completa* se, para toda a proposição p , correctamente formulada no contexto dessa teoria, " p " ou "não p " é um teorema. Caso contrário diz-se que a teoria é *incompleta*. O teorema de incompletude de Gödel¹ mostra que existem teorias incompletas.

As iniciais **qed** (iniciais de *quod erat demonstrandum*) ou **cqd** (iniciais de *como se queria demonstrar*), classicamente utilizadas para indicarem o fim da demonstração, são modernamente substituídas por outros símbolos como, por exemplo \square , o qual será adoptado ao longo deste texto.

Como exemplo, segue-se um teorema que estabelece uma propriedade do valor médio relativamente a um majorante.

Teorema 1.1. *Dados $x, y, z \in \mathbb{R}$. Se $x \leq z$ e $y \leq z$ então $\frac{x+y}{2} \leq z$ (isto é, o valor medio não é maior do que um majorante destes números).*

Demonstração. Uma vez que $x \leq z$, então $x + y \leq z + y$. Mas $y \leq z$, então $z + y \leq z + z$. Logo,

$$x + y \leq z + y \leq z + z = 2z$$

implica $\frac{x+y}{2} \leq z$. □

Em matemática, as afirmações não provadas, relativamente às quais existe a expectativa de se vir a encontrar uma prova, designam-se por *conjecturas* e, tais afirmações, enquanto não se provam ou refutam, fazem parte dos desafios da investigação matemática corrente.

Uma conjectura famosa que se tem revelado difícil de provar ou refutar (constituindo um dos maiores desafios matemáticos contemporâneos) é a conjectura de Goldbach² onde se afirma que *todo o inteiro par superior a 2 é soma de dois primos*. É fácil ver que $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$,

¹Kurt Gödel (1906–1978), matemático austríaco que trabalhou em lógica e filosofia da matemática.

²Christian Goldbach (1690–1764), matemático russo que trabalhou em teoria dos números.

$12 = 7 + 5$, $14 = 7 + 7$, etc. Porém, como o número de inteiros positivos pares é infinito, é impossível proceder à verificação exaustiva de todos eles³. Assim, a prova (ou refutação) desta conjectura deverá recorrer aos conceitos abstractos de número par maior do que 2 (ou seja, $2k$, com k natural maior do que 1) e de número primo. Deve observa-se que para se refutar esta conjectura "basta" encontrar um *contra-exemplo*, isto é, um número natural $k > 1$ tal que para todo o número primo arbitrário menor que $2k$, p , se verifica que $2k - p$ é um número composto (ou seja, é tal que entre os seus divisores consta, pelo menos, um inteiro maior do que 1 e menor do que $2k - p$).

1.2. Noção de conjunto

A noção de conjunto é, aparentemente, bem conhecida, mas, em geral, de um modo muito subjectivo, tanto mais que a necessária abrangência deste conceito coloca algumas dificuldades ao seu entendimento (ver Secção 1.8). No entanto, sem tais preocupações, vamos considerar um conjunto como sendo uma colecção de objectos que designamos por elementos do conjunto. Um conjunto sem elementos designa-se por *conjunto vazio* e denota-se por \emptyset .

Ao longo deste texto vamos denotar os conjuntos por letras maiúsculas e os seus possíveis elementos por letras minúsculas. Para se indicar que α é um elemento de A , escrevemos $\alpha \in A$, o que significa que α pertence a A . Muitas vezes estamos interessados em estudar conjuntos cujos elementos pertencem a um mesmo conjunto que designamos por *conjunto universal*. Neste caso, sendo \mathcal{U} o conjunto universal e sendo A um conjunto de elementos de \mathcal{U} também dizemos que A é um subconjunto de \mathcal{U} e escrevemos $A \subseteq \mathcal{U}$.

Definição 1.1 (Conjuntos iguais). *Dados dois conjuntos A e B de elementos do conjunto universal \mathcal{U} , diz-se que A é igual a B e escreve-se $A = B$, se A e B têm exactamente os mesmos elementos.*

Definição 1.2 (Subconjunto). *Dados dois conjuntos A e B de elementos do conjunto universal \mathcal{U} , diz-se que A é um subconjunto de B (ou que está contido em B) e escreve-se $A \subseteq B$, se todos os elementos de A pertencem a B . Adicionalmente, diz-se que A é um subconjunto próprio de B (ou que A está contido estritamente em B) e escreve-se $A \subsetneq B$ (ou $A \subset B$), se A é um subconjunto de B diferente de B .*

Assim, enquanto na inclusão em sentido lato é irrelevante se A é ou não igual a B , na inclusão em sentido estrito a igualdade dos conjuntos A e B está completamente posta de parte.

Existem dois modos de definir um conjunto particular. Em extensão, com a indicação exaustiva de todos os seus elementos (por exemplo, $A = \{1, 10, x, 9, y\}$) ou em compreensão, com indicação do predicado⁴ a satisfazer por todos os elementos do conjunto universal (por exemplo, $B = \{x : P(x)\}$ que se deve ler " B é o conjunto dos elementos x do conjunto universal, implicitamente assumido, que verificam o predicado $P(x)$ "). Em ambos os casos, quer a descrição exaustiva, quer o predicado caracterizador, são usualmente limitados pelas chavetas $\{ \text{ e } \}$.

Existem conjuntos particularmente importantes, com os quais, pelo menos informalmente, já todos tomaram contacto, como sejam, o *conjunto dos números naturais* que denotamos por \mathbb{N} , o conjunto dos números inteiros que denotamos por \mathbb{Z} , o conjunto dos números racionais que denotamos por \mathbb{Q} , o conjunto dos números reais que denotamos por \mathbb{R} , etc. É claro que podemos definir conjuntos à custa de outros conjuntos, por exemplo,

$$C = \{x \in \mathbb{Z} : -5 < x \leq 3\}. \quad (1.1)$$

³Uma verificação muito exaustiva desta conjectura foi realizada por Tomás Oliveira e Silva da Universidade de Aveiro que, com recurso ao computador, verificou a sua validade para todos os números não superiores a $2 \cdot 10^{17}$ (Fevereiro 2005).

⁴Por agora, pode entender-se um predicado como sendo uma ou várias propriedades ou condições, que podem (ou não) ser satisfeitas pelos elementos abrangidos.

Neste caso, o conjunto C é definido em compreensão, ou seja, na forma $C = \{x : P(x)\}$, com $P(x)$ significando que x deve ser inteiro, não superior a 3 e superior a -5.

Note-se que a definição de um conjunto em compreensão obriga à utilização de variáveis cujos valores percorrem um certo conjunto universal implicitamente assumido.

Tendo em conta que os conjuntos e subconjuntos são colecções de objectos com determinadas propriedades ou que satisfazem determinadas condições, as questões matemáticas, de um modo geral, podem reduzir-se ao reconhecimento de objectos (ou conjuntos de objectos) enquanto elementos (subconjuntos) de um determinado conjunto. Assim, sendo $X = \{x : P(x)\}$, se todos os objectos que satisfazem o predicado $P(x)$ também satisfazem o predicado $Q(x)$, podemos concluir que sendo $Y = \{y : Q(y)\}$, então $X \subseteq Y$. Nestes casos, em linguagem matemática, dizemos que $P(x)$ implica $Q(x)$ ou, de modo semelhante, se um objecto x satisfaz a propriedade ou condição P então também satisfaz a propriedade ou condição Q e escrevemos

$$P(x) \Rightarrow Q(x).$$

Esta implicação significa, então, que o conjunto dos objectos com a propriedade P está contido no conjunto dos objectos com a propriedade Q .

Exemplo 1.2. Seja $Y = \{y : y \text{ é inteiro múltiplo de } 4\}$ e seja $X = \{x : x \text{ é inteiro par}\}$. Vamos verificar que $Y \subsetneq X$.

Solução. É claro que

$$z \text{ inteiro múltiplo de } 4 \Rightarrow z \text{ inteiro par},$$

onde podemos concluir que $Y \subseteq X$. Adicionalmente, dado que, por exemplo, $2 \in X$ e $2 \notin Y$, concluímos que $Y \subsetneq X$. \square

Quando $P(x) \Rightarrow Q(x)$ e $Q(x) \Rightarrow P(x)$, diz-se que $P(x)$ é equivalente a $Q(x)$ e escreve-se

$$P(x) \Leftrightarrow Q(x).$$

Nestas condições, $P(x) \Leftrightarrow Q(x)$ significa, por um lado que

$$X = \{x : P(x)\} \subseteq \{y : Q(y)\} = Y \tag{1.2}$$

e por outro que

$$Y = \{y : Q(y)\} \subseteq \{x : P(x)\} = X. \tag{1.3}$$

Como consequência,

$$X = \{x : P(x)\} = \{y : Q(y)\} = Y.$$

Com efeito, de acordo com (1.2), todos os elementos de X são elementos de Y e, de acordo com (1.3), não existe um elemento de Y que não seja elemento de X .

Se o conjunto $Z = \{z : S(z)\}$ é vazio, tal significa que nenhum objecto verifica a propriedade ou condição S . Por outro lado, sendo $X = \{x : P(x)\}$ e $Y = \{y : Q(y)\}$, se X não está contido em Y (escrevendo-se $X \not\subseteq Y$), tal significa que a implicação $P(x) \Rightarrow Q(x)$ é falsa.

1.3. Linguagem proposicional

As afirmações que são verdadeiras ou falsas, designam-se, em linguagem matemática, por proposições. Segue-se a definição formal de proposição.

Definição 1.3 (Proposição). Uma proposição é uma afirmação que é verdadeira ou falsa.

Exemplo 1.3. As declarações:

- (a) a equação $x^2 - 4 = 0$ tem duas soluções inteiros;
 - (b) se $n \in \mathbb{N}$ então $n^5 - n$ é divisível por 30;
 - (c) nenhum número primo é par;
- são exemplos de proposições.

Note-se que embora (a), (b) e (c) sejam proposições, apenas (a) e (b) são proposições verdadeiras.

Quando se define $C = \{x : P(x)\}$, onde x é uma variável que percorre o conjunto universal implicitamente considerado, embora $P(x)$ possa tomar valores verdadeiros ou falsos, não se pode dizer que $P(x)$ é uma proposição. Com efeito, assumindo que para certos valores da variável x , $P(x)$ é verdadeiro e para outros falso, sem se concretizar x não faz sentido atribuir o valor verdadeiro ou falso a $P(x)$. Porém, fixando $P(x)$ para um valor particular de x , já se pode afirmar que se trata de uma proposição. Por exemplo, admitindo que $P(x)$ significa x é par (onde x é uma variável que toma valores inteiros), fazendo $x = 5$, $P(5)$ (que significa 5 é par) é uma proposição (que no caso é falsa).

Para evitar ambiguidades passaremos a denotar as proposições por letras minúsculas. Assim, no caso anterior, podemos denotar a proposição $P(5)$ simplesmente por p .

Exemplo 1.4. A igualdade e as declarações:

- (d) $x^2 - 4 = 0$;
 - (e) apreciem a paisagem;
 - (f) x é maior do que y ;
- não são proposições.

Uma proposição diz-se *atómica* quando não se pode decompor noutras proposições e diz-se *composta* no caso contrário. Por exemplo, dadas duas proposições atómicas p e q , podemos combiná-las de modo a obter a proposição composta

$$p \Rightarrow q$$

que se designa por *proposição condicional* ou *implicação* e se lê *se p então q* ou *p implica q* . Esta proposição significa que se p é verdadeira então q também é verdadeira.

Exemplo 1.5. Considerando a proposição "se o cão tem fome então o cão come muito" como uma proposição condicional na forma $p \Rightarrow q$, vamos identificar as proposições atómicas p e q .

Solução. A variável proposicional p representa a proposição atómica *o cão tem fome* e a variável proposicional q a proposição atómica *o cão come muito*. Neste caso, *o cão tem fome* é uma condição suficiente para a proposição *o cão come muito* e esta, por sua vez, é uma condição necessária para a proposição *o cão tem fome*. \square

Uma proposição composta caracteriza-se completamente à custa da tabela dos valores lógicos que adquire, *verdadeiro* (1) ou *falso* (0), quando se percorrem todos os possíveis valores lógicos das proposições atómicas que a constituem, a qual se designa por *tabela de verdade*. No caso da proposição composta $p \Rightarrow q$ (que é falsa apenas quando p é verdadeira e q é falsa), a tabela de verdade que lhe corresponde é a que a seguir se indica.

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

Tabela 1.1: Tabela de verdade para a implicação.

Por vezes presumimos um conjunto de proposições todas verdadeiras, noutras casos supomos que pelo menos uma, de entre um conjunto delas, o seja, e, noutras situações ainda, interessa-nos negar o valor lógico de uma certa proposição. Para traduzir todos estes contextos e obter proposições compostas mais complexas, a linguagem proposicional faz uso das conjunções, disjunções e negações.

A Tabela 1.2-(A) explicita as tabelas de verdade da negação **não** p (que denotaremos por $\neg p$), da disjunção p **ou** q (que denotaremos por $p \vee q$) e da conjunção p **e** q (que denotaremos por $p \wedge q$).

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

(A)

p	q	$\neg p$	$\neg p \vee q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

(B)

Tabela 1.2: (A) – tabela de verdade para a negação, disjunção e conjunção; (B) – tabela de verdade para $\neg p \vee q$.

A partir das tabelas de verdade da negação, disjunção e conjunção, com facilidade se determinam tabelas de verdade de proposições compostas mais complexas, que também designaremos por expressões proposicionais (ou lógicas). Para tal, torna-se conveniente a identificação das variáveis proposicionais que, por sua vez, denotam outras proposições (atómicas ou compostas) e a determinação dos valores lógicos de subexpressões sucessivamente mais complexas. Por exemplo, para se determinar a tabela de verdade da expressão lógica $\neg p \vee q$, poderemos adoptar o procedimento associado à Tabela 1.2-(B).

Segue-se um exemplo um pouco mais complexo que o anterior, onde apenas se apresentam os valores lógicos de algumas subexpressões da expressão proposicional cuja tabela de verdade se pretende determinar.

Exemplo 1.6. Vamos determinar a tabela de verdade da expressão lógica

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

Solução. Ver Tabela 1.3. □

p	q	r	$(p \wedge q) \vee r$	$\neg(p \wedge r)$	$((p \wedge q) \vee r) \wedge (\neg(p \wedge r))$
1	1	1	1	0	0
1	1	0	1	1	1
1	0	1	1	0	0
1	0	0	0	1	0
0	1	1	1	1	1
0	1	0	0	1	0
0	0	1	1	1	1
0	0	0	0	1	0

Tabela 1.3: Tabela de verdade para $((p \wedge q) \vee r) \wedge (\neg(p \wedge r))$.

Dadas duas proposições p e q , a proposição composta $(p \Rightarrow q) \wedge (q \Rightarrow p)$ denota-se por $p \Leftrightarrow q$ e designa-se por *equivalência* entre p e q (ver Tabela 1.4). Neste caso lê-se p se e só se (sse) q para significar que as proposições p e q têm exactamente os mesmos valores lógicos. Consequentemente, $p \Leftrightarrow q$ é uma proposição composta que toma o valor lógico verdadeiro quando e apenas quando as

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

Tabela 1.4: Tabela de verdade para $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

proposições p e q têm os mesmos valores lógicos. Com efeito, esta conclusão pode ser retirada da respectiva tabela de verdade.

Deve observar-se que uma variável proposicional não denota, necessariamente, uma proposição atómica. Com efeito, pode tornar-se conveniente denotar uma proposição composta por uma certa variável proposicional, pelo que todas as conclusões que obtivermos acerca de expressões lógicas se mantêm válidas quando qualquer das variáveis é substituída por uma proposição composta (assumindo-se, obviamente, que essa proposição composta toma os mesmos valores lógicos da variável que a representa).

O que acabamos de referir leva-nos a introduzir o conceito de *fórmula bem formada* da linguagem proposicional, uma vez que, embora estas fórmulas sejam sequências de símbolos de um determinado conjunto, nem todas as sequências de símbolos fazem sentido do ponto de vista da linguagem proposicional. No nosso caso, o conjunto de símbolos adoptado inclui as letras minúsculas de um qualquer alfabeto (que representam variáveis proposicionais) e, por agora, o conjunto de símbolos especiais $\{\cdot, \cdot, \neg, \wedge, \vee, \Rightarrow, \Leftarrow, \Leftrightarrow\}$. Os parêntesis são utilizados apenas para tornar clara uma determinada subexpressão (note-se que, por exemplo, $\neg p \wedge q$ é diferente de $\neg(p \wedge q)$). Uma fórmula bem formada da linguagem proposicional pode definir-se do seguinte modo:

Definição 1.4 (Fórmula bem formada⁵). *Qualquer variável representando uma proposição atómica é uma fórmula bem formada. Se r é uma fórmula bem formada então (r) é também uma fórmula bem formada. Por outro lado, admitindo que p e q representam fórmulas bem formadas, $\neg p$, $p \vee q$, $p \wedge q$, $p \Rightarrow q$, $p \Leftarrow q$ e $p \Leftrightarrow q$ são ainda fórmulas bem formadas.*

Por exemplo, a fórmula $p \neg \vee q$ não é uma fórmula bem formada. Neste texto, as fórmulas bem formadas da linguagem proposicional são designadas, simplesmente, por fórmulas da linguagem proposicional.

Existem certas fórmulas da linguagem proposicional que são sempre verdadeiras quaisquer que sejam os valores lógicos das suas variáveis (por exemplo, $p \vee \neg p$) e outras que são sempre falsas (por exemplo, $p \wedge \neg p$). As primeiras designam-se por *tautologias* e as segundas por *contradições*.

Definição 1.5 (Expressões lógicas equivalentes). *Duas expressões lógicas, r e s , dizem-se equivalentes se $r \Leftrightarrow s$ é uma tautologia.*

Com base nesta definição, podemos concluir que duas expressões lógicas, com as mesmas variáveis, são equivalentes quando têm a mesma tabela de verdade. Adicionalmente, podemos afirmar que tanto a conjunção como a disjunção são comutativas, no sentido em que $p \vee q$ é equivalente a $q \vee p$ (ou seja, $(p \vee q) \Leftrightarrow (q \vee p)$) e $p \wedge q$ é equivalente a $q \wedge p$ (ou seja, $(p \wedge q) \Leftrightarrow (q \wedge p)$), conforme decorre das respectivas tabelas de verdade.

De igual modo se conclui que $p \Rightarrow q$ é equivalente a $\neg p \vee q$, bem como as propriedades do *cálculo proposicional* que a seguir se indicam.

- $(\neg(p \wedge q)) \Leftrightarrow (\neg p \vee \neg q)$ e $(\neg(p \vee q)) \Leftrightarrow (\neg p \wedge \neg q)$ *(leis de De Morgan)*

⁵ Esta definição pressupõe a existência de uma relação de precedência entre os diferentes operadores, a qual é necessário utilizar na leitura de certas fórmulas.

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

Tabela 1.5: Tabela de verdade onde se evidencia a comutatividade da disjunção e da conjunção.

- $(p \wedge (q \wedge r)) \Leftrightarrow ((p \wedge q) \wedge r)$ e $(p \vee (q \vee r)) \Leftrightarrow ((p \vee q) \vee r)$ *(associatividade)*
- $(p \wedge p) \Leftrightarrow p$ e $(q \vee q) \Leftrightarrow q$ *(idempotência)*
- $(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$ e $(p \vee (q \wedge r)) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ *(distributividade)*
- $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ *(lei de contraposição)*
- $\neg(\neg p) \Leftrightarrow p$ *(lei de dupla negação)*

Tendo presente os conceitos de tautologia e contradição, e assumindo p como uma proposição arbitrária, podemos concluir ainda que

- $p \wedge$ (tautologia) é equivalente a p ,
- $p \vee$ (tautologia) é uma tautologia,
- \neg (tautologia) é uma contradição,
- $p \wedge$ (contradição) é uma contradição,
- $p \vee$ (contradição) é equivalente a p ,
- \neg (contradição) é uma tautologia.

Recorrendo a estas últimas propriedades, poderemos simplificar algumas fórmulas de modo a obter fórmulas equivalentes com menor número de variáveis proposicionais. Por exemplo, em vez de $p \vee (q \wedge \neg p)$ podemos considerar a fórmula equivalente $p \vee q$ (dado que $p \vee (q \wedge \neg p) \Leftrightarrow (p \vee q) \wedge (p \vee \neg p)$ a qual, por sua vez, é equivalente a $p \vee q$, tendo em conta que, $p \vee \neg p$ é uma tautologia).

Para além do conectivo *ou* (que se designa também por *ou inclusivo*), por vezes adopta-se o *ou exclusivo* (ou *rejeição*) que se denota por $\dot{\vee}$. Este *ou exclusivo* aplicado às proposições p e q , produz a proposição $p \dot{\vee} q$ que significa *p ou q mas não ambos*. Assim, a proposição $p \dot{\vee} q$ é verdadeira quando uma e apenas uma das proposições p ou q é verdadeira.

1.4. Operações sobre conjuntos

Com base nos conectivos lógicos anteriormente introduzidos estamos em condições de avançar um pouco mais no estudo dos conjuntos, particularmente no estudo das operações sobre conjuntos.

É muito comum representar os conjuntos de uma forma pictórica, por intermédio de diagramas, conhecidos por *diagramas de Venn*⁶. A Figura 1.1 ilustra este tipo de representação, denotando dois conjuntos A e B com intersecção não vazia.

Vamos começar por definir formalmente as principais operações sobre conjuntos, ou seja, a intersecção, a união, a diferença, a diferença simétrica e a complementação.

⁶John Venn (1834–1923) foi um lógico inglês que utilizou este tipo de representação pictórica num livro, com o título *Symbolic Logic*, publicado em 1894.

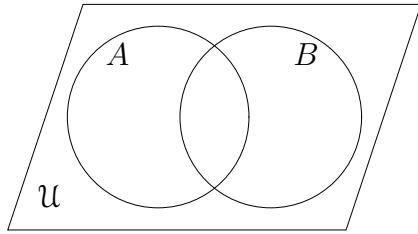


Figura 1.1: Diagrama de Venn de dois conjuntos A e B com intersecção não vazia.

Definição 1.6 (Operações sobre conjuntos). *Sejam A e B dois subconjuntos de um certo universo \mathcal{U} .*

A intersecção de A e B denota-se por $A \cap B$ e é definida pelo conjunto

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}. \quad (1.4)$$

A união de A e B denota-se por $A \cup B$ e é definida pelo conjunto

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}. \quad (1.5)$$

A diferença entre A e B denota-se por $A \setminus B$ e é definida pelo conjunto

$$A \setminus B = \{x : (x \in A) \wedge (x \notin B)\}. \quad (1.6)$$

A diferença simétrica entre A e B denota-se por $A \Delta B$ e é definida pelo conjunto

$$A \Delta B = \{x : (x \in A) \dot{\vee} (x \in B)\}. \quad (1.7)$$

O complementar de A denota-se por A^c e é definido pelo conjunto

$$A^c = \{x : x \notin A\}. \quad (1.8)$$

Na Figura 1.2 exemplificam-se as operações de intersecção, união, diferença e diferença simétrica, com recurso a diagramas de Venn.

Exemplo 1.7. *Dados dois conjuntos arbitrários A e B de um universo \mathcal{U} , vamos mostrar que se verificam as seguintes propriedades:*

1. $A = B$ se e só se $A \subseteq B$ e $B \subseteq A$, *(princípio de inclusão mútua)*
2. $\emptyset \subseteq A$,
3. $A \cap A^c = \emptyset$,
4. $A \setminus B = A \cap B^c$,
5. $(A \setminus B) \cap (B \setminus A) = \emptyset$.

Solução.

1. Vamos dividir esta prova em duas partes. Primeiro provando a implicação (a) $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$ e, posteriormente, a implicação (b) $A = B \Rightarrow (A \subseteq B \wedge B \subseteq A)$.

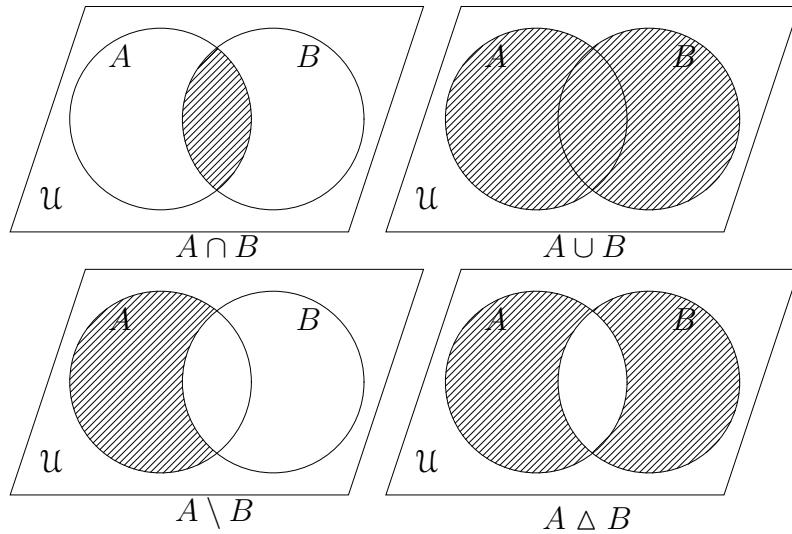


Figura 1.2: Diagramas de Venn de algumas operações sobre os conjuntos A e B .

- (a) Tendo em conta que, de acordo com a lei de contraposição, a implicação $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$ é equivalente à implicação $A \neq B \Rightarrow \neg(A \subseteq B \wedge B \subseteq A)$, vamos demonstrar esta última.
Suponha $A \neq B$, o que significa que existe $x \in A$ tal que $x \notin B$ ou existe $y \in B$ tal que $y \notin A$. Logo, $A \not\subseteq B$ ou $B \not\subseteq A$, pelo que concluímos que a proposição $\neg(A \subseteq B \wedge B \subseteq A)$ é verdadeira.
- (b) Suponha $A = B$. Então cada elemento de A é também elemento de B (isto é, $A \subseteq B$) e cada elemento de B é também o elemento de A (isto é, $B \subseteq A$). Logo, $A = B \Rightarrow (A \subseteq B \wedge B \subseteq A)$.
2. A proposição $\emptyset \subseteq A$ significa, por definição, que dado um elemento arbitrário x , $x \in \emptyset \Rightarrow x \in A$. Porém, esta implicação é equivalente à proposição $x \notin \emptyset \vee x \in A$ que, por sua vez, é uma tautologia.
3. Para demonstrar $A \cap A^c = \emptyset$, recorrendo ao princípio de inclusão mútua, vamos dividir a prova em duas partes. Primeiro provamos a inclusão (a) $\emptyset \subseteq A \cap A^c$ e, posteriormente, a inclusão (b) $A \cap A^c \subseteq \emptyset$.
 - (a) A inclusão $\emptyset \subseteq A \cap A^c$ é consequência directa do item 2.;
 - (b) Se $x \in A \cap A^c$, então $x \in A$ e $x \in A^c$, ou seja, $x \in A$ e $x \notin A$, o que constitui uma contradição. Logo, $A \cap A^c$ não tem elementos e, consequentemente, $A \cap A^c = \emptyset$.
4. Com efeito, $x \in A \setminus B$ é equivalente a $x \in A \wedge x \notin B$ que, por sua vez, é equivalente a $x \in A \cap B^c$.
5. Com efeito, $x \in (A \setminus B) \cap (B \setminus A)$ é equivalente a $x \in A \setminus B$ e $x \in B \setminus A$ que, por sua vez, é equivalente a $(x \in A \wedge x \notin B) \wedge (x \in B \wedge x \notin A)$, o que constitui uma contradição. \square

Exemplo 1.8. Vamos mostrar que se A , B e C são três conjuntos arbitrários de um certo universo, U , então

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{e} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Estas propriedades são conhecidas por propriedades de distributividade.

Solução. Observe-se que

$$\begin{aligned} A \cap (B \cup C) &= \{x : x \in A \wedge x \in B \cup C\} = \{x : x \in A \wedge (x \in B \vee x \in C)\} \\ &= \{x : (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\} \\ &= \{x : x \in A \cap B \vee x \in A \cap C\} = \{x : x \in (A \cap B) \cup (A \cap C)\} \\ &= (A \cap B) \cup (A \cap C). \end{aligned}$$

Similarmente,

$$\begin{aligned} A \cup (B \cap C) &= \{x : x \in A \vee x \in B \cap C\} = \{x : x \in A \vee (x \in B \wedge x \in C)\} \\ &= \{x : (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\} \\ &= \{x : x \in A \cup B \wedge x \in A \cup C\} = \{x : x \in (A \cup B) \cap (A \cup C)\} \\ &= (A \cup B) \cap (A \cup C). \end{aligned}$$

□

Sendo A , B e C três conjuntos arbitrários de um certo universo, \mathcal{U} , com facilidade se concluem as seguintes propriedades, a seguir indicadas, das operações sobre conjuntos, cujas provas são semelhantes às anteriormente apresentadas.

- $A \setminus A = \emptyset = \emptyset \setminus A$
- $A \setminus \emptyset = A$
- $A \setminus B = B \setminus A \Leftrightarrow A = B$
- $\emptyset^c = \mathcal{U}$ e $\mathcal{U}^c = \emptyset$
- $(A^c)^c = A$ (dupla complementaridade)
- $A \cap B = B \cap A$ e $A \cup B = B \cup A$ (comutatividade)
- $A \cap (B \cap C) = (A \cap B) \cap C$ e $A \cup (B \cup C) = (A \cup B) \cup C$ (associatividade)
- $(A \cup B)^c = A^c \cap B^c$ e $(A \cap B)^c = A^c \cup B^c$ (leis de De Morgan)

1.5. União e intersecção generalizadas e quantificadores

A união e a intersecção podem estender-se, de um modo natural, a famílias finitas ou infinitas de conjuntos. Com efeito, considerando a família de conjuntos $\mathcal{A} = \{A_i\}_{i \in I}$, onde I denota um conjunto de índices, vem

$$\bigcap \mathcal{A} = \bigcap_{i \in I} A_i = \{x : x \in A_i, \text{ para todo } i \in I\}, \quad (1.9)$$

$$\bigcup \mathcal{A} = \bigcup_{i \in I} A_i = \{x : x \in A_i, \text{ para algum } i \in I\}. \quad (1.10)$$

Uma família de conjuntos $\{A_i\}_{i \in I}$ diz-se *disjunta* se $\bigcap_{i \in I} A_i = \emptyset$ e diz-se *dois a dois disjunta* se $i \neq j \Rightarrow A_i \cap A_j = \emptyset$. Por exemplo, dada a família de conjuntos $\mathcal{A} = \{[\frac{1}{i}, i]\}_{i \in \mathbb{N}}$ que corresponde à

família de intervalos $[1, 1]$, $[\frac{1}{2}, 2]$, $[\frac{1}{3}, 3]$, etc, podemos concluir que dados dois índices p e q tais que $p < q$, se verifica $[\frac{1}{p}, p] \cap [\frac{1}{q}, q] = [\frac{1}{p}, p]$ e ainda

$$\begin{aligned}\bigcap_{i \in \mathbb{N}} \left[\frac{1}{i}, i \right] &= \{1\}, \\ \bigcup_{i \in \mathbb{N}} \left[\frac{1}{i}, i \right] &= (0, +\infty),\end{aligned}$$

onde $(0, +\infty)$ denota o intervalo dos números reais maiores do que zero. Nestas condições, a família \mathcal{A} não é disjunta, nem dois a dois disjunta.

A união e intersecção generalizadas gozam de propriedades análogas às anteriormente demonstradas para a união e intersecção de dois conjuntos. Como exemplo, seguem-se as leis de De Morgan generalizadas (cuja demonstração fica como exercício).

Leis de De Morgan generalizadas:

$$A \setminus \bigcap_{i \in I} B_i = \bigcup_{i \in I} (A \setminus B_i), \quad (1.11)$$

$$A \setminus \bigcup_{i \in I} B_i = \bigcap_{i \in I} (A \setminus B_i), \quad (1.12)$$

$$\left(\bigcap_{i \in I} B_i \right)^c = \bigcup_{i \in I} B_i^c, \quad (1.13)$$

$$\left(\bigcup_{i \in I} B_i \right)^c = \bigcap_{i \in I} B_i^c. \quad (1.14)$$

Os conjuntos definidos em (1.10) e (1.9) sugerem a introdução de símbolos matemáticos adequados a estas situações, os quais se designam por quantificadores. Assim, em linguagem simbólica, em vez de (1.10) poderia escrever-se

$$\bigcup_{i \in I} A_i = \{x : \exists_{i \in I} x \in A_i\},$$

onde $\exists_{i \in I}$ (ou $\exists i \in I$), significa *existe i pertencente a I*. Este quantificador designa-se por quantificador existencial⁷.

Quando se pretende indicar que existe um único elemento que satisfaz determinada propriedade (ou condição), por exemplo, que dado $x \in \mathbb{R} \setminus \{0\}$ existe um único $y \in \mathbb{R}$ tal que $xy = yx = 1$, escreve-se $\exists!_{y \in \mathbb{R}} xy = yx = 1$. Por sua vez, para se indicar que não existe um número real que satisfaz uma determinado predicado, por exemplo $x^2 < 0$, escreve-se $\nexists_{x \in \mathbb{R}} x^2 < 0$.

Por outro lado, em linguagem simbólica, em vez de (1.9) poderia escrever-se

$$\bigcap_{i \in I} A_i = \{x : \forall_{i \in I} x \in A_i\},$$

onde $\forall_{i \in I}$ (ou $\forall i \in I$), significa *para todo i pertencente a I ou qualquer que seja i pertencente a I*. Este quantificador designa-se por quantificador universal⁸. Os quantificadores existenciais e universais são utilizados em fórmulas que envolvem variáveis, para limitarem ou estenderem o âmbito em que se

⁷Note-se que $\exists_{y \in Y} Q(y)$ significa, em linguagem simbólica mais precisa, $\exists_y (y \in Y \wedge Q(y))$.

⁸Note-se que $\forall_{x \in X} P(x)$ significa, em linguagem simbólica mais precisa, $\forall_x (x \in X \Rightarrow P(x))$.

verifica(m) determinada(s) propriedade(s). Os quantificadores podem agrupar-se, de modo adequado, numa mesma fórmula. A seguir, exemplificam-se algumas fórmulas que envolvem mais do que um quantificador.

Exemplo 1.9. Fórmulas que incluem vários quantificadores:

$$1. \forall_{n \in \mathbb{N} \setminus \{1\}} \exists_{p \in \mathbb{N}} (p \text{ é primo}) \wedge (n < p < 2n),$$

$$2. \forall_{x \in \mathbb{R}} \left(x \geq 0 \Rightarrow \exists_{y \in \mathbb{R}} y^2 = x \right).$$

Em fórmulas que envolvem quantificadores é crucial reconhecer o alcance de cada um deles, isto é, a parte da fórmula sobre a qual actua. No caso do Exemplo 1.9-1, o alcance do quantificador universal é a fórmula

$$\exists_{p \in \mathbb{N}} (p \text{ é primo}) \wedge (n < p < 2n)$$

e o alcance do quantificador existencial é a fórmula

$$(p \text{ é primo}) \wedge (n < p < 2n).$$

Por vezes, torna-se conveniente negar expressões que envolvem quantificadores. Após uma análise cuidada das expressões $\forall_x P(x)$ e $\exists_y Q(y)$, concluem-se as seguintes equivalências:

$$\neg(\forall_x P(x)) \Leftrightarrow \exists_x \neg P(x); \quad (1.15)$$

$$\neg(\exists_y Q(y)) \Leftrightarrow \forall_y \neg Q(y). \quad (1.16)$$

A fórmula (1.16) pode também escrever-se na forma $\nexists_y Q(y) \Leftrightarrow \forall_y \neg Q(y)$. A partir de (1.15) e de (1.16) estamos em condições de determinar fórmulas simplificadas equivalentes à negação de fórmulas mais complexas que envolvem vários quantificadores.

Exemplo 1.10. Vamos determinar a negação da expressão

$$\forall_{x_1} \exists_{x_2} \exists_{x_3} \forall_{x_4} P(x_1, x_2, x_3, x_4). \quad (1.17)$$

Solução. Podemos obter a negação da expressão (1.17), procedendo do seguinte modo:

$$\begin{aligned} \neg \left(\forall_{x_1} \exists_{x_2} \exists_{x_3} \forall_{x_4} P(x_1, x_2, x_3, x_4) \right) &\Leftrightarrow \exists_{x_1} \neg \left(\exists_{x_2} \exists_{x_3} \forall_{x_4} P(x_1, x_2, x_3, x_4) \right) \\ &\Leftrightarrow \exists_{x_1} \forall_{x_2} \neg \left(\exists_{x_3} \forall_{x_4} P(x_1, x_2, x_3, x_4) \right) \\ &\Leftrightarrow \exists_{x_1} \forall_{x_2} \forall_{x_3} \neg \left(\forall_{x_4} P(x_1, x_2, x_3, x_4) \right) \\ &\Leftrightarrow \exists_{x_1} \forall_{x_2} \forall_{x_3} \exists_{x_4} \neg P(x_1, x_2, x_3, x_4). \end{aligned} \quad \square$$

1.6. Relações

As relações entre conjuntos desempenham um papel importantíssimo na linguagem matemática e na dedução de muitos resultados, pelo que, antes de mais, convém introduzir o respectivo conceito formal.

Para tal, vamos utilizar outros conceitos, como sejam o de *par ordenado* e o de *produto cartesiano* de conjuntos.

O conceito de par ordenado (mais geralmente, de n -uplo ordenado) é muito intuitivo e esta noção intuitiva é muito utilizada neste texto. Porém, formalmente, podemos definir par ordenado como a seguir se indica.

Definição 1.7 (Par ordenado). *Dados x e y , o par ordenado (x, y) define-se como sendo o conjunto $\{\{x\}, \{x, y\}\}$, ou seja, $(x, y) = \{\{x\}, \{x, y\}\}$. Adicionalmente, diz-se que x é o primeiro elemento e y é o segundo elemento.*

A definição de pares ordenados pode estender-se, recursivamente, aos n -uplos ordenados, com $n \geq 3$, da seguinte forma:

$$\begin{aligned} (x_1, x_2, x_3) &= (x_1, (x_2, x_3)) \\ (x_1, x_2, x_3, x_4) &= (x_1, (x_2, x_3, x_4)) = (x_1, (x_2, (x_3, x_4))) \\ \vdots &\quad \vdots \quad \vdots \quad \vdots \\ (x_1, x_2, \dots, x_n) &= (x_1, (x_2, x_3, \dots, x_n)) = (x_1, (x_2, (x_3, \dots, x_n))). \end{aligned}$$

Definição 1.8 (Produto cartesiano e relação binária). *Dados dois conjuntos arbitrários, A_1 e A_2 , designa-se por produto cartesiano destes conjuntos e denota-se por $A_1 \times A_2$, o conjunto dos pares ordenados (x_1, x_2) tais que $x_1 \in A_1$ e $x_2 \in A_2$, ou mais formalmente*

$$A_1 \times A_2 = \{(x_1, x_2) : x_1 \in A_1 \wedge x_2 \in A_2\}.$$

Por sua vez, designa-se por relação binária entre os conjuntos A_1 e A_2 todo o subconjunto do produto cartesiano $A_1 \times A_2$.

Por economia de escrita denota-se o produto cartesiano $A \times A$ simplesmente por A^2 . Neste caso, uma relação binária $\mathcal{R} \subseteq A^2$ diz-se uma relação binária definida em A ou sobre A . Dada uma relação $\mathcal{R} \subseteq A \times B$, usualmente, escreve-se $a \mathcal{R} b$ para indicar $(a, b) \in \mathcal{R}$.

Por exemplo, de acordo com a Definição 1.8, dados os conjuntos $A = \{1, 2, 3\}$ e $B = \{a, b, c, d, e, f\}$, vem que o conjunto $A \times B$ tem os elementos:

$$\begin{aligned} A \times B = \{&(1, a), (1, b), (1, c), (1, d), (1, e), (1, f), \\ &(2, a), (2, b), (2, c), (2, d), (2, e), (2, f), \\ &(3, a), (3, b), (3, c), (3, d), (3, e), (3, f)\} \end{aligned}$$

e o subconjunto $\mathcal{R} \subset A \times B$ tal que

$$\mathcal{R} = \{(1, a), (1, f), (2, b), (2, d), (2, f)\}$$

é uma relação binária entre A e B .

Exemplo 1.11. Vamos mostrar que a relação de menor ou igual, que se denota por \leq , é uma relação binária sobre o conjunto dos números inteiros.

Solução. Uma vez que podemos escrever $a \leq b$ na forma $(a, b) \in \leq$, vem

$$\leq = \{(a, b) \in \mathbb{Z}^2 : a \leq b\} \subseteq \mathbb{Z}^2.$$

Note-se que embora se possa escrever $(2, 3) \in \leq$ e $(3, 2) \notin \leq$, usualmente, escreve-se $2 \leq 3$ e $3 \not\leq 2$ (ou $3 > 2$). \square

Definição 1.9 (Conjunto potência). *Dado um conjunto X , designa-se por conjunto das partes de X e denota-se por $\mathcal{P}(X)$ o conjunto dos subconjuntos de X , onde se inclui, naturalmente, o conjunto vazio. Este conjunto $\mathcal{P}(X) = \{Y : Y \subseteq X\}$ também se designa por conjunto potência (ou, simplesmente, potência) de X .*

Com estes conceitos, pode encarar-se a relação de pertença dos elementos de um certo conjunto universal, \mathcal{U} , em relação às suas partes, como uma relação binária entre \mathcal{U} e $\mathcal{P}(\mathcal{U})$, ou seja, $\in \subset \mathcal{U} \times \mathcal{P}(\mathcal{U})$.

Exemplo 1.12. Vamos determinar a relação binária de pertença \in , definida entre \mathcal{U} e $\mathcal{P}(\mathcal{U})$, supondo $\mathcal{U} = \{x, y\}$.

Solução. Uma vez que $\mathcal{U} = \{x, y\}$, então $\mathcal{P}(\mathcal{U}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$. Como consequência,

$$\in = \{(x, \{x\}), (x, \{x, y\}), ((y, \{y\}), (y, \{x, y\}))\}. \quad \square$$

Definição 1.10 (Domínio, contradomínio, imagem, imagem recíproca e relação inversa). *Seja \mathcal{R} uma relação binária entre os conjuntos X e Y .*

1. Então, designa-se por

(a) domínio de \mathcal{R} , denotando-se por $\text{dom}(\mathcal{R})$, o conjunto

$$\text{dom}(\mathcal{R}) = \{x \in X : \exists_{y \in Y} (x, y) \in \mathcal{R}\};$$

(b) imagem (ou contradomínio) de \mathcal{R} , denotando-se por $\text{img}(\mathcal{R})$, o conjunto

$$\text{img}(\mathcal{R}) = \{y \in Y : \exists_{x \in X} (x, y) \in \mathcal{R}\}.$$

2. Dado um elemento $x \in X$, designa-se por

(a) imagem de x por \mathcal{R} , denotando-se por $\mathcal{R}(x)$, o conjunto

$$\mathcal{R}(x) = \{y \in Y : (x, y) \in \mathcal{R}\};$$

(b) imagem recíproca por \mathcal{R} de um elemento $y \in Y$, denotando-se por $\mathcal{R}^{-1}(y)$, o conjunto

$$\mathcal{R}^{-1}(y) = \{x \in X : (x, y) \in \mathcal{R}\}.$$

3. Por sua vez, designa-se por relação inversa de \mathcal{R} e denota-se por \mathcal{R}^{-1} o subconjunto de $Y \times X$ definido por

$$\mathcal{R}^{-1} = \{(y, x) \in Y \times X : (x, y) \in \mathcal{R}\}.$$

Definição 1.11 (Reflexividade, simetria, anti-simetria e transitividade). *Dado um conjunto A , uma relação binária \mathcal{R} definida nele (isto é, $\mathcal{R} \subseteq A \times A$) diz-se*

1. reflexiva, se $\forall_{x \in A} (x, x) \in \mathcal{R}$;

2. simétrica, se $\forall_{x, y \in A} (x, y) \in \mathcal{R} \Rightarrow (y, x) \in \mathcal{R}$;

3. anti-simétrica, se $\forall_{x, y \in A} ((x, y) \in \mathcal{R} \wedge (y, x) \in \mathcal{R}) \Rightarrow x = y$;

4. transitiva, se $\forall_{x, y, z \in A} ((x, y) \in \mathcal{R} \wedge (y, z) \in \mathcal{R}) \Rightarrow (x, z) \in \mathcal{R}$.

Exemplo 1.13. Vamos determinar as propriedades da Definição 1.11 que são verificadas pelas relações binárias a seguir indicadas, definidas no conjunto dos números reais.

1. Relação $<$ tal que $x < y$ (ou, de modo equivalente, $(x, y) \in <$) se e só se x é menor do que y .
2. Relação \mathcal{R} tal que $(x, y) \in \mathcal{R}$ se e só se $|x - y| \leq 2$.

Solução.

1. Uma vez que $a < b \wedge b < c \Rightarrow a < c$, conclui-se imediatamente que a relação $<$ é transitiva. Por outro lado, tendo em conta que $(a \neq b) \Rightarrow (a < b \vee b < a)$, também se conclui que a relação $<$ é anti-simétrica. Porém, é fácil verificar que esta relação não é reflexiva nem simétrica.
2. Facilmente se conclui que a relação \mathcal{R} é reflexiva ($|x - x| \leq 2$) e simétrica ($|x - y| \leq 2 \Rightarrow |y - x| \leq 2$), mas não é transitiva nem anti-simétrica. \square

1.6.1 Relações de ordem

As relações de ordem são relações muito utilizadas em matemática e na vida prática em geral, pelo que, neste texto, vão ser alvo de atenção muito particular. Nesta secção, porém, vamos introduzir apenas alguns conceitos básicos.

Definição 1.12 (Relação de ordem parcial). *Uma relação binária diz-se uma relação de ordem parcial se é reflexiva, anti-simétrica e transitiva.*

Exemplo 1.14. Tendo em conta que dado um inteiro n , $d \neq 0$ é um divisor de n (ou divide n) se existe um inteiro z tal que $dz = n$, vamos considerar o conjunto $D_{18} = \{1, 2, 3, 6, 9, 18\}$ de todos os divisores positivos de 18 e vamos mostrar que a relação $|$, definida por $x|y$ se e só se x divide y , é uma relação de ordem parcial em D_{18} .

Solução. Por definição

$$| = \{(1, 1), (1, 2), (1, 3), (1, 6), (1, 9), (1, 18), (2, 2), (2, 6), (2, 18), (3, 3), (3, 6), (3, 9), (3, 18), (6, 6), (6, 18), (9, 9), (9, 18), (18, 18)\}.$$

Logo, por observação, verifica-se que esta relação é reflexiva, anti-simétrica e transitiva. Idêntica conclusão pode ser obtida utilizando as propriedades da divisibilidade, a estudar no Capítulo 8. \square

Sendo \mathcal{R} uma relação de ordem parcial sobre um conjunto A , então o par (A, \mathcal{R}) designa-se por *conjunto parcialmente ordenado*. No Capítulo 7 faz-se um estudo detalhado dos conjuntos parcialmente ordenados.

Definição 1.13 (Relação de ordem total e conjunto totalmente ordenado). *Uma relação \mathcal{R} de ordem parcial definida num conjunto A diz-se uma relação de ordem total (ou relação de ordem linear) se para cada $a, b \in A$ se verifica que $(a, b) \in \mathcal{R}$ ou $(b, a) \in \mathcal{R}$. Neste caso diz-se que o par (A, \mathcal{R}) é um conjunto totalmente ordenado.*

Seguem-se alguns exemplos de conjuntos totalmente ordenados.

1. O conjunto \mathbb{N} com relação \leq , ou seja, o par (\mathbb{N}, \leq) .
2. O conjunto $D_{32} = \{1, 2, 4, 8, 16, 32\}$ dos divisores positivos de 32 com a relação de divisibilidade $|$, ou seja, o par $(D_{32}, |)$.
3. O conjunto de entradas de um dicionário com a ordem lexicográfica (alfabética).

1.6.2 Relações de equivalência

Pode considerar-se o conceito de relação de equivalência como uma generalização do conceito de igualdade entre objectos, relativamente a certos aspectos (ou características) que consideramos fundamentais.

Definição 1.14 (Relação de equivalência). *Uma relação binária diz-se uma relação de equivalência se é reflexiva, simétrica e transitiva.*

Se \mathcal{R} é uma relação de equivalência definida em X , então para cada $x \in X$, o conjunto $[x]_{\mathcal{R}} = \{y \in X : (x, y) \in \mathcal{R}\}$ designa-se por *classe de equivalência* de x . Quando não existem dúvidas em relação a \mathcal{R} , a classe de equivalência de x também se denota por $[x]$.

Exemplo 1.15. *Sendo \mathcal{R} é uma relação de equivalência definida num conjunto A , vamos demonstrar que*

1. $\forall a \in [a] \text{ e, como consequência, } [a] \neq \emptyset;$
2. $\forall a, b \in A \text{ s.t. } a \mathcal{R} b \Leftrightarrow [a] = [b];$
3. $\forall a, b \in A \text{ s.t. } [a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset;$
4. $A = \bigcup_{a \in A} [a].$

Solução.

1. A relação \mathcal{R} , por definição, é reflexiva, isto é $a \mathcal{R} a$, o que implica $a \in [a]$.
2. Se $a, b \in A$ e $[a] = [b]$, então, pelo item 1, $a \in [a] = [b]$ implica $a \mathcal{R} b$. Reciprocamente, supondo que $a, b \in A$ e $a \mathcal{R} b$ vamos demonstrar $[a] = [b]$ utilizando inclusão mútua. Se $x \in [a]$ então $x \mathcal{R} a$ e como $a \mathcal{R} b$, pela transitividade de \mathcal{R} vem que $x \mathcal{R} b$ ou, por definição de \mathcal{R} , $x \in [b]$. Logo $[a] \subseteq [b]$. Analogamente se conclui que $[b] \subseteq [a]$ e, consequentemente, $[a] = [b]$.
3. Vamos provar a implicação equivalente $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$. Suponha que $x \in [a] \cap [b]$, pelo que $x \mathcal{R} a$ e $x \mathcal{R} b$. Logo, pela simetria e transitividade de \mathcal{R} vem que $a \mathcal{R} b$. Como consequência, de acordo com o item 2, $[a] = [b]$.
4. Por definição, $\forall a \in A \text{ s.t. } [a] \subseteq A$, donde $\bigcup_{a \in A} [a] \subseteq A$. Por outro lado, uma vez que $a \in [a]$ vem $\bigcup_{a \in A} [a] \supseteq A$. Logo, $A = \bigcup_{a \in A} [a]$. \square

Definição 1.15 (Partição de um conjunto). *Se A é um conjunto não vazio, então uma coleção $P \subseteq \mathcal{P}(A)$ tal que*

- (a) $\forall S \in P \text{ s.t. } S \neq \emptyset,$
- (b) $\forall S_1, S_2 \in P \text{ s.t. } S_1 \neq S_2 \Rightarrow S_1 \cap S_2 = \emptyset,$
- (c) $A = \bigcup_{S \in P} S.$

designa-se por partição do conjunto A .

Algumas vezes os elementos de uma partição P designam-se por *blocos da partição P* ou (quando não existem dúvidas relativamente à partição), simplesmente, *blocos*.

Exemplo 1.16. Sendo $A = \{n \in \mathbb{N} : 1 \leq n \leq 10\}$ e dados os subconjuntos $A_1 = \{1, 3, 5, 7, 9\}$, $A_2 = \{1, 2, 3, 4, 5, 6\}$, $A_3 = \{6, 7, 8, 9, 10\}$ e $A_4 = \{2, 4, 6, 8, 10\}$, vamos determinar aqueles que formam os blocos de uma partição de A .

Solução. Uma vez que quaisquer três conjuntos têm pelo menos dois com intersecção não vazia, a partição de A , a existir, tem apenas dois blocos de entre os subconjuntos A_1, \dots, A_4 . Porém, $A_1 \cap A_2 = \{1, 3, 5\} \neq \emptyset$, $A_1 \cap A_3 = \{7, 9\} \neq \emptyset$, $A_2 \cap A_3 = \{6\} \neq \emptyset$, $A_2 \cap A_4 = \{2, 4, 6\} \neq \emptyset$ e $1 \notin A_3 \cup A_4$. Logo, restam apenas A_1 e A_4 como candidatos a blocos de uma partição, com os quais, efectivamente, se obtém a partição $P = \{A_1, A_4\}$. \square

Note-se que uma partição não é necessariamente finita (no sentido em que o número de subconjuntos disjuntos é finito). Por exemplo, sendo $S_n = [n, n+1)$ para cada $n \in \mathbb{Z}$, verifica-se facilmente que a família de intervalos $\{S_n : n \in \mathbb{Z}\}$ constitui uma partição de \mathbb{R} numa infinidade de subconjuntos.

Como consequência do Exemplo 1.15 e tendo em conta a Definição 1.15, é claro que uma relação de equivalência \mathcal{R} , definida num conjunto X , determina a *partição* de X nas respectivas classes de equivalência. O conjunto de tais classes designa-se por *conjunto quociente* e denota-se por X/\mathcal{R} , isto é,

$$X/\mathcal{R} = \{[x] : x \in X\}.$$

Exemplo 1.17. Considere a relação binária sobre o conjunto \mathbb{Z} , $\equiv (\text{mod } 5)$ definida por $x \equiv y (\text{mod } 5)$ se e só se 5 divide $x - y$ ou, de modo equivalente, $x \equiv y (\text{mod } 5)$ se e só se x e y quando divididos por 5 têm o mesmo resto. Vamos demonstrar que $\equiv (\text{mod } 5)$ é uma relação de equivalência e vamos determinar todas as classes de equivalência do conjunto quociente $\mathbb{Z}/\equiv (\text{mod } 5)$.

Solução. Para demonstrar que $\equiv (\text{mod } 5)$ é uma relação de equivalência em \mathbb{Z} basta provar cada uma das propriedades que se seguem.

Reflexividade: Para cada $z \in \mathbb{Z}$ vem que 5 divide $z - z = 0$, logo $z \equiv z (\text{mod } 5)$.

Simetria: Se $x \equiv y (\text{mod } 5)$, então existe $k \in \mathbb{Z}$ tal que $x - y = 5k$. Porém, neste caso, $y - x = 5(-k)$ e, uma vez que $-k \in \mathbb{Z}$, podemos concluir que $y \equiv x (\text{mod } 5)$.

Transitividade: Se $x \equiv y (\text{mod } 5)$ e $y \equiv z (\text{mod } 5)$, então $x - y = 5k'$ e $y - z = 5k''$, com $k', k'' \in \mathbb{Z}$. Assim, $x - z = (x - y) + (y - z) = 5(k' + k'')$, pelo que $x \equiv z (\text{mod } 5)$.

Tendo em conta que cada classe de equivalência pode ser representada pelos restos da divisão inteira por 5, conclui-se imediatamente que

$$\begin{aligned}[0] &= \{x \in \mathbb{Z} : x \equiv 0 (\text{mod } 5)\} = \{\dots, -10, -5, 0, 5, 10, \dots\}, \\ [1] &= \{x \in \mathbb{Z} : x \equiv 1 (\text{mod } 5)\} = \{\dots, -9, -4, 1, 6, 11, \dots\}, \\ [2] &= \{x \in \mathbb{Z} : x \equiv 2 (\text{mod } 5)\} = \{\dots, -8, -3, 2, 7, 12, \dots\}, \\ [3] &= \{x \in \mathbb{Z} : x \equiv 3 (\text{mod } 5)\} = \{\dots, -7, -2, 3, 8, 13, \dots\}, \\ [4] &= \{x \in \mathbb{Z} : x \equiv 4 (\text{mod } 5)\} = \{\dots, -6, -1, 4, 9, 14, \dots\}, \end{aligned}$$

onde decorre a igualdade $\mathbb{Z}/\equiv (\text{mod } 5) = \{[0], [1], [2], [3], [4]\}$.

Deve observar-se que, por exemplo, $[-9] = [1]$, $[8] = [3]$, etc. \square

Mais geralmente, a relação *quando dividido por p tem o mesmo resto que*, com $p \in \mathbb{N}$, designa-se por *relação de congruência módulo p* e denota-se por $\equiv (\text{mod } p)$. Assim, $x \equiv y (\text{mod } p)$ designa que x é congruente com y módulo p e significa que $x - y$ é divisível por p (ou seja, existe $k \in \mathbb{Z}$ tal que $x = pk + y$). Denotando-se, como usualmente, o resto da divisão inteira de z por p , por $z (\text{mod } p)$, vem

$$x \equiv y (\text{mod } p) \Leftrightarrow x (\text{mod } p) = y (\text{mod } p). \quad (1.18)$$

Estes conceitos são analisados no Capítulo 8.

Exemplo 1.18. Vamos demonstrar que os conceitos de relação de equivalência e de partição de um conjunto são idênticos. Mais precisamente, vamos demonstrar que uma relação de equivalência definida num conjunto A define um conjunto de classes de equivalência que determinam uma partição de A e, reciprocamente, uma partição de um conjunto A determina uma relação de equivalência \mathcal{R} definida por $x\mathcal{R}y$ se e só se x e y pertencem a um mesmo subconjunto da partição.

Solução. Observe-se que das propriedades das classes de equivalência de uma relação de equivalência definida num conjunto A , demonstradas no Exemplo 1.15, decorre que tais classes formam uma partição de A . Assim, resta provar que dada uma partição $P = \{S_i : i \in I\}$ de um conjunto A , então a relação \mathcal{R} definida por

$$x\mathcal{R}y \Leftrightarrow \exists_{i \in I} x \in S_i \wedge y \in S_i$$

é (1) reflexiva, (2) simétrica e (3) transitiva. Com efeito,

- (1) pela Definição 1.15 (c), para cada $x \in A$ existe $i \in I$ tal que $x \in S_i$, pelo que \mathcal{R} é reflexiva;
- (2) uma vez que $x\mathcal{R}y \Rightarrow \exists_{i \in I} x \in S_i \wedge y \in S_i \Leftrightarrow \exists_{i \in I} y \in S_i \wedge x \in S_i \Rightarrow y\mathcal{R}x$, logo \mathcal{R} é simétrica;
- (3) uma vez que se x e y pertencem ao mesmo subconjunto da partição tal como y e z , então x , y e z pertencem todos ao mesmo subconjunto, podemos concluir que \mathcal{R} é transitiva. \square

1.6.3 Funções

As funções são casos particulares de relações com utilização muito frequente em matemática. Porém, a sua utilização geral, associada a razões de ordem histórica, conduziram a uma notação distinta da usualmente utilizada nas relações.

Definição 1.16 (Função, conjunto de partida e conjunto de chegada). *Uma função (ou aplicação) definida num conjunto A e com imagem em B é uma relação unívoca $f \subseteq A \times B$, ou seja, tal que se $(\alpha, \beta), (a, b) \in f \wedge \alpha = a \text{ então } \beta = b$. O conjunto A designa-se por conjunto de partida e o conjunto B por conjunto de chegada. Usualmente, escreve-se $f(\alpha) = \beta$ em vez de $(\alpha, \beta) \in f$.*

Como as funções são casos particulares de relações, os conceitos de *domínio*, *imagem* (ou *contradomínio*), *imagem recíproca*, *inversa*, etc, de funções, são idênticos aos das relações. Porém, dada uma função f , quando se escreve $f : A \rightarrow B$ ou

$$\begin{aligned} f : A &\rightarrow B \\ x &\rightsquigarrow f(x), \end{aligned} \tag{1.19}$$

tal significa que $\text{dom}(f) = A$ e que $\text{img}(f) = f(A) \subseteq B$.

Como consequência da Definição 1.16, se $A \neq \emptyset$ e $B \neq \emptyset$, então podemos concluir que uma relação binária $f \subseteq A \times B$ é uma função se e só se

$$\forall_{x \in \text{dom}(f)} \exists!_{y \in B} (x, y) \in f.$$

Adicionalmente, se $A = \emptyset$, então a única função entre A e B é o conjunto vazio.

Por exemplo, se $A = \{1, 2, 3\}$ e $B = \{a, b, c, d\}$, então a relação $f = \{(1, a), (2, a), (3, b)\}$ é uma função $f : A \rightarrow B$, a relação $g = \{(1, a), (2, c), (3, d), (2, b)\}$ não é uma função, e a relação $h = \{(1, a), (2, b)\}$ não é uma função cujo domínio é A , mas é uma função $h : \{1, 2\} \rightarrow B$.

Definição 1.17 (Função injectiva, sobrejectiva e bijectiva). *Considere a função $f : X \rightarrow Y$.*

1. Diz-se que f é injectiva se

$$\forall_{x, y \in X} f(x) = f(y) \Rightarrow x = y.$$

2. Diz-se que f é sobrejectiva se

$$\forall_{y \in Y} \exists_{x \in X} f(x) = y.$$

3. Diz-se que f é bijectiva se é injectiva e sobrejectiva.

Exemplo 1.19. Vamos verificar qual (ou quais) das funções, a seguir indicadas, é (ou são) injectiva(s), sobrejectiva(s) ou bijectiva(s):

1. $f : \mathbb{N} \rightarrow \mathbb{N}$, definida por $f(n) = 2n$;

2. $g : \mathbb{Z} \rightarrow \mathbb{N}$, definida por $g(n) = n^2$;

3. $h : \mathbb{R} \rightarrow \mathbb{R}$, definida por $g(x) = x^3$;

4. $i : \mathbb{Z} \rightarrow \mathbb{N}$, definida por $i(n) = \begin{cases} 2n + 1, & \text{se } n \geq 0; \\ -2n, & \text{se } n < 0. \end{cases}$

Solução.

1. Uma vez que $2m = 2n \Rightarrow m = n$, a função f é injectiva. Por outro lado, dado que $\nexists_{n \in \mathbb{N}} 2n = 3$, podemos concluir que f não é sobrejectiva.

2. Uma vez que $g(-2) = g(2)$, a função g não é injectiva. Adicionalmente, tendo em conta que $\nexists_{n \in \mathbb{Z}} n^2 = 3$, podemos concluir que g não é sobrejectiva.

3. A função h é bijectiva. Com efeito, $x^3 = y^3 \Rightarrow x = y$ e $\forall_{x \in \mathbb{R}} \exists_{\tilde{x} \in \mathbb{R}} (\sqrt[3]{x})^3 = x$.

4. A prova que a função i é bijectiva é imediata, considerando separadamente as imagens pares e ímpares. \square

Duas funções f e g são iguais (isto é, $f = g$) se têm o mesmo domínio $\text{dom}(f) = \text{dom}(g) = D$ e $\forall_{x \in D} f(x) = g(x)$.

Exemplo 1.20. Vamos verificar quais as funções que são iguais e as que são diferentes, de entre as a seguir indicadas.

$$\begin{aligned} f(x) &= x^3 + x^2 - x - 1, & x \in \mathbb{Z} \\ g(x) &= x^3 + x^2 - x - 1, & x \in \mathbb{R} \\ h(x) &= (x^2 - 1)(x + 1), & x \in \mathbb{R} \end{aligned}$$

Solução. Com facilidade se conclui que $g = h$ e, tendo em conta que f e g não têm o mesmo domínio, $f \neq g$. \square

Dada uma função $f : A \rightarrow B$, $X \subseteq A$ e $Y \subseteq B$, usualmente, designa-se por *imagem de X por f* , e denota-se por $f(X)$, o conjunto

$$f(X) = \{b \in B : \exists_{x \in X} f(x) = b\}$$

e por *imagem recíproca de Y por f* , e denota-se por $f^{-1}(Y)$, o conjunto

$$f^{-1}(Y) = \{a \in A : f(a) \in Y\}.$$

Quando se trata de um conjunto singular $Y = \{y\}$, por simplicidade, escreve-se $f^{-1}(y)$ em vez de $f^{-1}(\{y\})$.

Exemplo 1.21. Dada uma função $f : A \rightarrow B$, vamos demonstrar que

- (i) f é injectiva se e só se $f^{-1}(f(X)) = X$, para cada $X \subseteq A$;
- (ii) f é sobrejectiva se e só se $f(f^{-1}(B)) = B$.

Solução.

- (i) Suponha que f é injectiva e seja $X \subseteq A$.

- (a) Se $x \in f^{-1}(f(X))$, então $f(x) \in f(X)$. Pela injectividade de f , $f(x') = f(x) \Rightarrow x' = x$, donde $f(x) \in f(X) \Rightarrow x \in X$. Consequentemente, $f^{-1}(f(X)) \subseteq X$.
- (b) Se $x \in X$, então $f(x) \in f(X)$ e, pela a definição de imagem recíproca, $x \in f^{-1}(f(X))$, pelo que $X \subseteq f^{-1}(f(X))$.

Logo, $f^{-1}(f(X)) = X$.

Reciprocamente, suponha que $\bigvee_{X \subseteq A} f^{-1}(f(X)) = X$. Seja $f(x) = f(y)$, com $x, y \in A$, então $\{x\} = f^{-1}(f(\{x\})) = f^{-1}(f(\{y\})) = \{y\}$, donde f é injectiva.

- (ii) A prova é imediata. □

De agora em diante, vamos denotar por $[k]$ o conjuntos dos primeiros k naturais, isto é, $[k] = \{1, 2, \dots, k\}$.

Definição 1.18 (Sequência finita). Uma sequência finita de um conjunto A é uma função

$$\begin{aligned} a : [k] &\rightarrow A \\ n &\rightsquigarrow a(n). \end{aligned}$$

Por razões de tradição, escrevemos a_n em vez de $a(n)$ (isto é, $a(n) = a_n$, para $n = 1, \dots, k$), dizendo-se, neste caso, que se trata de uma sequência de comprimento k .

Uma sequência a de elementos de um conjunto A , de comprimento n , denota-se, usualmente, pelo n -uplo ordenado de elementos do conjunto A , ou seja, $a = (a_1, \dots, a_n)$.

Definição 1.19 (Sucessão). Uma sucessão de elementos de um conjunto A é uma sequência com uma infinidade de elementos do conjunto A , cada um dos quais se designa por termo.

Tendo em conta esta definição, podemos dizer que uma sucessão de elementos de A é uma função $a : \mathbb{N} \rightarrow A$.

A sucessão (a_1, a_2, \dots) denota-se, habitualmente, por $(a_n)_{n \in \mathbb{N}}$.

Definição 1.20 (Composição de relações). Dadas duas relações \mathcal{R}_1 entre A e B e \mathcal{R}_2 entre B e C , designa-se por composição de \mathcal{R}_1 com \mathcal{R}_2 , a relação que se denota por $\mathcal{R}_2 \circ \mathcal{R}_1$ (e, usualmente, se lê \mathcal{R}_2 após \mathcal{R}_1) definida por

$$\mathcal{R}_2 \circ \mathcal{R}_1 = \{(a, c) \in A \times C : \exists_{b \in B} (a, b) \in \mathcal{R}_1 \wedge (b, c) \in \mathcal{R}_2\}.$$

No caso particular das funções, considerando-se $f : A \rightarrow B$ e $g : B \rightarrow C$, a composição $g \circ f$ corresponde à função

$$\begin{aligned} g \circ f : A &\rightarrow C \\ x &\rightsquigarrow (g \circ f)(x) = g(f(x)). \end{aligned}$$

O diagrama da Figura 1.3 ilustra esta composição de funções.

Exemplo 1.22. Sendo $g : \mathbb{Z} \rightarrow \mathbb{R}$ tal que $g(x) = \frac{x}{2} + 3$, e $f : \mathbb{Z} \rightarrow \mathbb{Z}$ tal que $f(n) = n^2 - 4n + 2$, vamos determinar a função composta $g \circ f$.

Solução. A função composta $g \circ f$ tem por domínio o domínio de f e contradomínio contido no contradomínio de g , ou seja, $g \circ f : \mathbb{Z} \rightarrow \mathbb{R}$. Adicionalmente,

$$(g \circ f)(n) = g(f(n)) = g(n^2 - 4n + 2) = \frac{n^2 - 4n + 2}{2} + 3 = \frac{1}{2}n^2 - 2n + 4.$$

□

Exemplo 1.23. Sendo $f : A \rightarrow B$ e $g : B \rightarrow C$ duas funções, vamos demonstrar que

1. se f e g são sobrejectivas então $g \circ f$ também é sobrejectiva,
2. se f e g são injectivas então $g \circ f$ também é injectiva.

Solução.

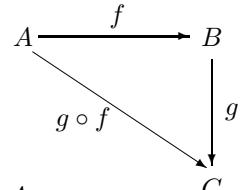
1. Suponha que f e g são funções sobrejectivas e que $c \in C$. Então existe $b \in B$ tal que $g(b) = c$ e existe $a \in A$ tal que $f(a) = b$. Logo, $g \circ f(a) = g(f(a)) = g(b) = c$, o que significa que $g \circ f$ é sobrejectiva.
2. Suponha que f e g são injectivas. Se $a_1, a_2 \in A$ e $a_1 \neq a_2$, então $b_1 = f(a_1) \neq f(a_2) = b_2$ e $g \circ f(a_1) = g(f(a_1)) = g(b_1) \neq g(b_2) = g(f(a_2)) = g \circ f(a_2)$. Logo, $g \circ f(a_1) \neq g \circ f(a_2)$ e, consequentemente, $g \circ f$ é injectiva.

□

A composição de duas funções pode estender-se (de um modo natural) a três ou mais funções. Com efeito, dada a família de funções $f_i : A_i \rightarrow A_{i+1}$, para $i = 1, \dots, p$, a função composta $f_p \circ f_{p-1} \circ \dots \circ f_1 : A_1 \rightarrow A_{p+1}$ corresponde à função

$$\begin{array}{ccccccc} A_1 & \xrightarrow{f_1} & A_2 & \dots & A_p & \xrightarrow{f_p} & A_{p+1} \\ x & \rightsquigarrow & f_1(x) & \dots & f_{p-1}(\dots f_1(x)\dots) & \rightsquigarrow & F\text{figura-1}(3;\text{Diagrama}) \end{array}$$

das funções $f : A \rightarrow B$ e $g : B \rightarrow C$.



Definição 1.21 (Restrição e extensão de uma função). Dada uma função $f : A \rightarrow B$ e um subconjunto $X \subseteq A$, designa-se por restrição de f a X e denota-se por $f|_X$ a função $f|_X : X \rightarrow B$ definida por

$$\forall_{x \in X} f|_X(x) = f(x).$$

Nestas condições, sendo $g = f|_X$, diz-se que f é uma extensão de g a A .

Uma função $id_X : X \rightarrow X$ tal que $\forall_{x \in X} id_X(x) = x$ diz-se a função identidade sobre X . É claro que a função identidade é uma bijecção.

Exemplo 1.24. Vamos apresentar a restrição de uma função como composição de funções.

Solução. Considere uma função $f : A \rightarrow B$ e um subconjunto $X \subseteq A$ e seja $i : X \rightarrow A$ a função definida por $\forall_{x \in X} i(x) = x$ (observe que a função i é a restrição ao conjunto X da função identidade definida em A). Uma vez que, definindo-se a composição de funções $f \circ i : X \rightarrow B$, se verifica que $\forall_{x \in X} f \circ i(x) = f(i(x)) = f(x)$, obtém-se $f|_X = f \circ i$.

□

Exemplo 1.25. Vamos demonstrar que se $f : X \rightarrow Y$ é uma função sobrejectiva, então

- (a) a relação $\sim \subseteq X \times X$, definida por $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$ para $x_1, x_2 \in X$ é uma relação de equivalência sobre X ;

- (b) considerando o conjunto quociente $X/\sim = \{[x] : x \in X\}$ e uma função quociente $\kappa : X \rightarrow X/\sim$, definida por $\kappa(x) = [x]$, para $x \in X$, então existe uma função $\varphi : X/\sim \rightarrow Y$ tal que φ é bijectiva.

Solução. Uma vez que (a) é trivialmente verdadeiro, apenas vamos demonstrar (b). Defina-se a função φ de tal forma que $\varphi([x]) = \varphi(\kappa(x)) = f(x)$. Uma vez que $\varphi([x_1]) = \varphi([x_2]) \Leftrightarrow f(x_1) = f(x_2) \Leftrightarrow x_1 \sim x_2 \Leftrightarrow [x_1] = [x_2]$, a função φ está bem definida e é injectiva. Por outro lado, uma vez que as funções f e κ são sobrejectivas, então a função φ também é sobrejectiva.

□

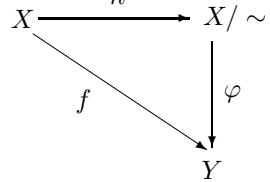


Figura 1.5: Diagrama da bijecção $\varphi : X/\sim \rightarrow Y$.

Definição 1.22 (Função inversa). *Uma função $f : X \rightarrow Y$ diz-se invertível se existe uma função $f^{-1} : Y \rightarrow X$ tal que*

$$f^{-1} \circ f = id_X \quad \text{e} \quad f \circ f^{-1} = id_Y.$$

A função f^{-1} designa-se por função inversa de f .

Como consequência desta definição, a função f é invertível se e só se f é uma bijecção. Observe que se a função f é invertível, então a função f^{-1} é também invertível e $(f^{-1})^{-1} = f$.

Exemplo 1.26. Vamos determinar (caso existam) as funções inversas das seguintes funções:

1. $f : \mathbb{R} \rightarrow \mathbb{R}$ tal que $f(x) = ax + b$ onde $a \neq 0$;
2. $g : \mathbb{R} \rightarrow (0, \infty)$ tal que $g(x) = e^x$;
3. $h : \mathbb{Z} \rightarrow \mathbb{N}$ tal que $h(n) = \begin{cases} 2n+1, & \text{para } n \geq 0; \\ -2n, & \text{para } n < 0. \end{cases}$

Solução. Recorrendo à definição, facilmente se verifica que as funções a seguir indicadas correspondem às funções inversas pretendidas.

1. $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$ tal que $f^{-1}(x) = \frac{x-b}{a}$,
2. $g^{-1} : (0, \infty) \rightarrow \mathbb{R}$ tal que $g^{-1}(x) = \ln x$,
3. $h^{-1} : \mathbb{N} \rightarrow \mathbb{Z}$ tal que $h^{-1}(n) = \begin{cases} -\frac{n}{2}, & \text{para } n \text{ par;} \\ \frac{n-1}{2}, & \text{para } n \text{ ímpar.} \end{cases}$

□

1.7. Cardinalidade

Para caracterizar o "tamanho" de um conjunto e estudar com rigor os conjuntos com uma "infinitude" de elementos, Georg Cantor⁹ introduziu a noção de *equipotência* entre conjuntos.

Definição 1.23 (Conjuntos equipotentes). *Dois conjuntos A e B dizem-se equipotentes (ou numericamente equivalentes) se e só se existe uma bijecção $f : A \rightarrow B$.*

É imediato concluir que a relação de equipotência é uma relação de equivalência entre conjuntos. As classes de equivalência da relação de equipotência correspondem aos conjuntos com o mesmo "tamanho" ou, mais precisamente, com a mesma *cardinalidade*, ou com o mesmo *número cardinal*. A cardinalidade de um conjunto X denota-se por $|X|$ (utilizando-se, também, outras notações para cardinalidade, como sejam $\text{card}(X)$ ou $\#X$).

⁹Georg Cantor (1845–1918), matemático russo nascido em S. Petersburgo, filho de pais dinamarqueses, que estudou em Zurique, Göttingen e Berlin, onde recebeu a influência de Weierstrass (1815–1897). Desenvolveu uma longa carreira académica na Universidade de Halle.

Exemplo 1.27. Vamos demonstrar que os pares de conjuntos a seguir indicados são equipotentes:

1. \mathbb{N} e \mathbb{Z} ;
2. \mathbb{N} e $2\mathbb{N}$, onde $2\mathbb{N}$ denota o conjunto de números naturais pares;
3. \mathbb{N} e \aleph_0 , onde $\aleph_0 = \mathbb{N} \cup \{0\}$.

Solução.

1. No Exemplo 1.26 já demonstramos que a função $h : \mathbb{Z} \rightarrow \mathbb{Z}$ definida por

$$h(n) = \begin{cases} 2n + 1, & \text{se } n \geq 0, \\ -2n, & \text{se } n < 0, \end{cases}$$

é uma bijecção entre \mathbb{Z} e \mathbb{N} .

2. A função $f : \mathbb{N} \rightarrow 2\mathbb{N}$, definida por $f(n) = 2n$, é uma bijecção entre \mathbb{N} e $2\mathbb{N}$.
3. A função $g : \mathbb{N} \rightarrow \aleph_0$, definida por $g(n) = n - 1$, é uma bijecção entre \mathbb{N} e \aleph_0 .

Logo, todos os conjuntos \mathbb{N} , \mathbb{Z} , $2\mathbb{N}$ e \aleph_0 têm a mesma cardinalidade a qual, usualmente, se denotada por \aleph_0 (onde \aleph é a primeira letra do alfabeto hebraico que se designa por *alefe*). Consequentemente,

$$|\mathbb{N}| = |\mathbb{Z}| = |2\mathbb{N}| = |\aleph_0| = \aleph_0.$$

□

Podemos introduzir uma relação de ordem parcial no conjunto das cardinalidades dos conjuntos.

Definição 1.24. Sejam A e B dois conjuntos. Diz-se que a cardinalidade do conjunto A é não superior à cardinalidade do conjunto B , e escreve-se $|A| \leq |B|$, se existe uma função injectiva $f : A \rightarrow B$. Se $|A| \leq |B|$ e os conjuntos A e B não são equipotentes, então diz-se que a cardinalidade do conjunto A é menor do que a cardinalidade do conjunto B , e escreve-se $|A| < |B|$.

Teorema 1.2 (Teorema de Cantor). Dado um conjunto X , verifica-se a desigualdade $|X| < |\mathcal{P}(X)|$.

Demonstração. Uma vez que a função $f : X \rightarrow \mathcal{P}(X)$, definida por $f(x) = \{x\}$ é injectiva, podemos concluir que $|X| \leq |\mathcal{P}(X)|$. Assim, resta provar que não existe nenhuma função sobrejectiva entre X e $\mathcal{P}(X)$, uma vez que tal implica a inexistência de uma função bijectiva. Vamos fazer esta prova por redução ao absurdo.

Seja $g : X \rightarrow \mathcal{P}(X)$ uma função sobrejectiva e considere-se o conjunto A definido por $A = \{x \in X : x \notin g(x)\}$. Uma vez que $A \in \mathcal{P}(X)$ e a função g é sobrejectiva, existe $x_0 \in X$ tal que $g(x_0) = A$ e temos duas possibilidades: $x_0 \in A$ ou $x_0 \notin A$. Porém,

- se $x_0 \in A$ então, por definição de A , $x_0 \notin g(x_0) = A$,
- se $x_0 \notin A$ então, por definição de A , $x_0 \in g(x_0) = A$.

Em ambos os casos se obtém uma contradição e, consequentemente, não existe nenhuma função sobrejectiva entre X e $\mathcal{P}(X)$. □

Definição 1.25 (Conjuntos finitos e infinitos). Um conjunto A diz-se *finito* (ou que tem cardinalidade finita) se é vazio ou existe $n \in \mathbb{N}$ tal que $|A| = |[n]|$, onde $[n] = \{1, \dots, n\}$. Caso contrário, diz-se *infinito* (ou que tem cardinalidade infinita).

Como consequência imediata do teorema de Cantor, uma vez que $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$, podemos afirmar que existe uma infinidade de números cardinais infinitos. Adicionalmente, podemos concluir que não existe o conjunto de todos os conjuntos.

No caso de conjuntos finitos, se $|A| = |[n]|$, diz-se que a cardinalidade do conjunto A é igual n , ou seja, $|A| = n$ e interpreta-se a cardinalidade como sendo o número de elementos do conjunto A . Como consequência desta definição, pode concluir-se, por exemplo, que a cardinalidade do conjunto vazio é zero, isto é, $|\emptyset| = 0$ e que, sendo C o conjunto definido em (1.1), $|C| = 8$.

Seja $f : [n] \rightarrow \mathbb{N}$ uma função arbitrária de $[n]$ em \mathbb{N} , com $n \in \mathbb{N}$. Se $k = 1 + \max\{f(1), \dots, f(n)\}$, então $k \in \mathbb{N}$ e $\nexists_{i \in [n]} f(i) = k$, ou seja, f não é sobrejectiva. Logo, \mathbb{N} é um conjunto infinito. Por outro lado, a função $i : [n] \rightarrow \mathbb{N}$ tal que $i(k) = k$, para todo o $k \in [n]$, é injectiva, donde podemos concluir que qualquer conjunto finito tem cardinalidade inferior à cardinalidade \mathbb{N} .

Definição 1.26 (Conjunto numerável). *Um conjunto X diz-se numerável (ou enumerável, ou contável) se X é finito ou equipotente ao conjunto \mathbb{N} . Caso contrário, diz-se que X é não numerável.*

De acordo com o Exemplo 1.27, os conjuntos \mathbb{N} , \mathbb{Z} , $2\mathbb{N}$ e \mathbb{N}_0 são conjuntos numeráveis.

Exemplo 1.28. *Sendo A um conjunto não vazio, vamos mostrar que as proposições a seguir indicadas são equivalentes.*

- (a) A é numerável;
- (b) existe uma função $f : \mathbb{N} \rightarrow A$ que é sobrejectiva;
- (c) existe uma função $g : A \rightarrow \mathbb{N}$ que é injectiva.

Solução.

(a) \Rightarrow (b) Seja A um conjunto numerável. Se A é infinito então, por definição, é equipotente ao conjunto \mathbb{N} , isto é, existe uma bijecção entre A e \mathbb{N} (cuja inversa é sobrejectiva). Se A é finito, então existe uma bijecção $\alpha : [n] \rightarrow A$ para um certo $n \in \mathbb{N}$. Sendo $\beta : \mathbb{N} \rightarrow [n]$ uma função definida por

$$\beta(i) = \begin{cases} i, & \text{para } i \leq n, \\ n, & \text{para } i > n, \end{cases}$$

vem que β é sobrejectiva. Logo, a função $f = \alpha \circ \beta : \mathbb{N} \rightarrow A$ é sobrejectiva.

(b) \Rightarrow (c) Se $f : \mathbb{N} \rightarrow A$ é uma função sobrejectiva, então a função $g : A \rightarrow \mathbb{N}$, definida por $g(a) = \min(f^{-1}(a))$ é injectiva.

(c) \Rightarrow (a) Se o conjunto A é finito, então A é numerável. Se A não é finito, uma vez que a função $g : A \rightarrow \mathbb{N}$ é injectiva, fazendo $B = g(A)$, vem $|A| = |B|$. Dado que $B \subseteq \mathbb{N}$, podemos escrever o conjunto B na forma $\{b_1, b_2, \dots\}$, com $b_i < b_{i+1}$. A função $\gamma : B \rightarrow \mathbb{N}$, definida por $\gamma(b_n) = n$, é uma bijecção. Logo, $|B| = |\mathbb{N}|$ e, consequentemente, A é numerável. \square

Como consequência deste exemplo, pode concluir-se que cada subconjunto de um conjunto numerável é também numerável.

Exemplo 1.29. *Vamos demonstrar que*

- (a) o conjunto $\mathbb{N} \times \mathbb{N}$ é numerável;
- (b) se A e B são numeráveis, então $A \times B$ é também numerável.

Solução. Considere-se a função injectiva $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, definida por $f(n, m) = 2^n 3^m$.

(a) Uma vez que f é injectiva, recorrendo ao Exemplo 1.28, conclui-se que o conjunto $\mathbb{N} \times \mathbb{N}$ é numerável.

Como exercício, pode demonstrar que a função $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, definida por $g(n, m) = 2^{n-1}(2m - 1)$, é uma bijecção.

(b) Se algum dos conjuntos A ou B é vazio, então $A \times B$ também é vazio e, portanto, numerável.

Suponha que A e B são conjuntos não vazios numeráveis. Utilizando o Exemplo 1.28, podemos concluir que existem duas funções injectivas $\alpha : A \rightarrow \mathbb{N}$ e $\beta : B \rightarrow \mathbb{N}$. Como consequência, a função $g : A \times B \rightarrow \mathbb{N} \times \mathbb{N}$, definida por $g(a, b) = (\alpha(a), \beta(b))$, é também injectiva. Finalmente, a função $f \circ g : A \times B \rightarrow \mathbb{N}$ é injectiva e, utilizando o Exemplo 1.28, conclui-se que o conjunto $A \times B$ é numerável. \square

Este último exemplo permite concluir que o conjunto \mathbb{Q} de todos os números racionais é enumerável (uma vez que qualquer número racional $\frac{p}{q}$ pode ser interpretado como um par $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ e $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = \aleph_0$).

Exemplo 1.30. *Vamos mostrar que qualquer conjunto infinito A contém um subconjunto infinito numerável, ou seja, que existe uma função injectiva $f : \mathbb{N} \rightarrow A$.*

Solução. Seja A um conjunto infinito. Vamos utilizar uma função de escolha¹⁰ $\xi : \mathcal{P}(A) \setminus \emptyset \rightarrow A$ tal que $a_1 = \xi(A)$, $a_2 = \xi(A \setminus \{a_1\})$, $a_3 = \xi(A \setminus \{a_1, a_2\})$, etc. Uma vez que A é infinito, então $A \setminus \{a_1, \dots, a_n\} \neq \emptyset$, para cada $n \in \mathbb{N}$. Por outro lado, é claro que $a_p \neq a_q$ se $p \neq q$, donde se conclui que o conjunto $\{a_1, a_2, \dots\} \subseteq A$ é infinito numerável (deve observar-se que a sucessão (a_1, a_2, \dots) corresponde à função f pretendida). \square

A primeira definição formal de conjunto infinito, dada por Dedekind¹¹ e Cantor, é uma consequência deste exemplo.

Teorema 1.3 (Dedekind e Cantor). *Um conjunto é infinito se e só se é equipotente a um subconjunto próprio.*

Demonstração. Se X é um conjunto infinito, então (de acordo com o Exemplo 1.30) existe um conjunto $A = \{a_1, a_2, \dots\}$ tal que $A \subseteq X$ e A é infinito numerável. Sendo $Y = X \setminus \{a_1\} \subsetneq X$ e $f : X \rightarrow Y$ tal que

$$f(x) = \begin{cases} x, & \text{se } x \in X \setminus A, \\ a_{n+1}, & \text{se } x = a_n \in A, \end{cases}$$

conclui-se que f é uma bijecção.

Por outro lado, tendo em conta que a existência de uma bijecção entre conjuntos finitos implica que eles tenham o mesmo número de elementos, a existência de uma bijecção entre X e um seu subconjunto próprio permite-nos concluir que X é infinito. \square

Deve observar-se que nem todos os conjuntos infinitos são numeráveis. Por exemplo, utilizando um processo de *diagonalização*, idêntico ao que se descreve no Exemplo 1.31, Cantor mostrou que os conjuntos \mathbb{N} e \mathbb{R} não são equipotentes.

Exemplo 1.31. *Vamos demonstrar que o intervalo $(0, 1)$ não é numerável.*

¹⁰Note-se que sendo $\mathcal{A} = \{A_i : i \in I\}$ uma família de conjuntos não vazios, então existe uma função $\xi : \mathcal{A} \rightarrow \bigcup_{i \in I} A_i$ tal que $\xi(A_i) \in A_i$.

¹¹Richard Dedekind (1831–1916), matemático alemão que trabalhou em teoria dos números.

Solução. Sabe-se que todo o número $x \in (0, 1)$ tem uma representação única na forma decimal $x = 0, x_1 x_2 \dots$, onde $x_i \in \{0, 1, \dots, 9\}$ (por exemplo, o número 0,5 é representável pela dízima infinita periódica 0,4999...). Suponha que o intervalo $(0, 1)$ é numerável e que os seus elementos se podem listar conforme, a seguir, se indica.

$$x_1 = 0, x_{11} x_{12} x_{13} \dots x_{1n} \dots$$

$$x_2 = 0, x_{21} x_{22} x_{23} \dots x_{2n} \dots$$

 \vdots

$$x_n = 0, x_{n1} x_{n2} x_{n3} \dots x_{nn} \dots$$

 \vdots

Considerando $a = 0, a_1 a_2 \dots$, com

$$a_i = \begin{cases} 1, & \text{se } x_{ii} \neq 1, \\ 2, & \text{se } x_{ii} = 1, \end{cases}$$

conclui-se que $\forall_{n \in \mathbb{N}} a_n \neq x_{nn}$ e, consequentemente, $\forall_{n \in \mathbb{N}} a \neq x_n$, ou seja, a não faz parte da lista. Porém, $a \in (0, 1)$, o que constitui uma contradição. Logo, o intervalo $(0, 1)$ não é numerável. \square

Segue-se o teorema de ponto fixo de Tarski¹² e uma aplicação deste teorema.

Teorema 1.4 (Teorema de ponto fixo de Tarski). *Considere um conjunto X e uma função $f : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$. Se, para quaisquer subconjuntos $A, B \subseteq X$, $A \subseteq B \Rightarrow f(A) \subseteq f(B)$, então existe $C \subseteq X$ tal que $f(C) = C$.*

Demonstração. Seja \mathcal{A} a família de todos os subconjuntos A de X , tais que $f(A) \subseteq A$. Uma vez que $f(X) \subseteq X$ a família \mathcal{A} não é vazia. Definindo $C = \bigcap_{A \in \mathcal{A}} A$, vamos mostrar que $f(C) = C$.

Com efeito, pela definição de C , $\forall_{A \in \mathcal{A}} C \subseteq A$ e, consequentemente, $\forall_{A \in \mathcal{A}} f(C) \subseteq f(A) \subseteq A$. Logo, $f(C) \subseteq C$ e, tendo em conta a hipótese, $f(f(C)) \subseteq f(C)$, pelo que $f(C) \in \mathcal{A}$. Assim, atendendo novamente à definição de C , vem que $C \subseteq f(C)$ e, consequentemente, $f(C) = C$. \square

Segue-se a aplicação do teorema de Tarski na demonstração do teorema de Schröder e Bernstein¹³.

Teorema 1.5 (Schröder-Bernstein). *Sejam X e Y dois conjuntos. Se $f : X \rightarrow Y$ e $g : Y \rightarrow X$ são funções injectivas, então existe uma bijecção $h : X \rightarrow Y$.*

Demonstração. Considere a função $\varphi : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$, definida por $\varphi(A) = X \setminus g(Y \setminus f(A))$, com $A \subseteq X$. Vamos mostrar que φ verifica as hipóteses do teorema de Tarski.

Com efeito, se $A \subseteq B \subseteq X$, então $g(Y \setminus f(B)) \subseteq g(Y \setminus f(A))$ e, consequentemente, $\varphi(A) \subseteq \varphi(B)$. Logo, por aplicação do teorema de Tarski, existe $C \subseteq X$ tal que $\varphi(C) = X \setminus g(Y \setminus f(C)) = C$, o que implica que se obtenha $X \setminus C = g(Y \setminus f(C))$ e $Y \setminus f(C) = g^{-1}(X \setminus C)$. Uma vez que, por hipótese, g é injectiva, então a sua restrição $g|_{Y \setminus f(C)}$ é uma bijecção entre $X \setminus C$ e $Y \setminus f(C)$, pelo que existe a bijecção inversa $g^{-1}|_{X \setminus C}$. Adicionalmente, é claro que a restrição $f|_C$ da função injectiva f é uma bijecção entre C e $f(C)$. Como consequência, considerando a função $h : X \rightarrow Y$, definida por

$$h(x) = \begin{cases} f(x), & \text{se } x \in C, \\ g^{-1}(x), & \text{se } x \in X \setminus C, \end{cases}$$

vem que h é uma bijecção entre X e Y . \square

¹² Alfred Tarski (1901–1983), matemático polaco que trabalhou em lógica.

¹³ Ernst Schröder (1841–1902) e Felix Bernstein (1878–1956) foram matemáticos alemães que trabalharam em álgebra e lógica, o primeiro, e matemática aplicada, o segundo.

1.8. Algumas notas históricas

Relativamente à conjectura de Goldbach, referida na Secção 1.1, deve acrescentar-se que numa carta datada de 1742, Goldbach conjecturou que

| todo o inteiro superior a 5 se pode exprimir como soma de três primos.

Logo (tendo em conta que um primo é um inteiro maior do que 1, sem divisores menores do que ele e maiores do que 1) conclui-se que, se a conjectura for verdadeira, sendo k um inteiro par maior do que 5 tal que $k = x + y + z$, com x, y e z primos, então um deles é 2 (que é o único primo par). Assim, supondo $x = 2$, conclui-se que $k - x = y + z$, o que implica que todo o inteiro par superior a 3 seja soma de dois primos. Note-se também que no caso do inteiro k maior do que 5 ser ímpar, $k - 3$ é um inteiro par maior do que 2. A conjectura de Goldbach foi reescrita, tal como hoje se apresenta, por Leonhard Euler¹⁴. Já se verificou que a conjectura de Goldbach é verdadeira até 100 milhões. Porém, no caso geral, até agora, o melhor que se conseguiu foi o resultado obtido pelo matemático russo I. M. Vinogradoff (nascido em 1891) que provou a existência de um número natural n^* (cuja ordem de grandeza se desconhece), relativamente ao qual todo o inteiro $n > n^*$ se pode exprimir como soma de no máximo quatro primos.

A noção de conjunto, apesar de intuitivamente simples, foi responsável por vários problemas ao longo da história do desenvolvimento da matemática. Com efeito, intuitivamente, um conjunto é *uma coleção de objectos* pelo que, praticamente, tudo é um conjunto. Esta abrangência, porém, deu origem ao aparecimento de alguns paradoxos, os quais, por sua vez, chegaram mesmo a provocar uma crise profunda nos fundamentos da matemática no princípio do século XX. Na verdade, desde a antiguidade grega até aos nossos dias, existiram três crises profundas sobre os fundamentos da matemática. A primeira ocorreu no século V a. C., com a descoberta de que a diagonal e o lado de um quadrado não se podem dividir em segmentos com igual comprimento, contrariando a convicção dos pitagóricos de que as grandezas da mesma espécie seriam comensuráveis. Esta crise, embora ficasse resolvida com os estudos de Eudoxo de Cnido¹⁵ (370 a. C.) sobre os incomensuráveis, os quais aparecem no quinto livro dos Elementos de Euclides (300 a. C.), só bastante mais tarde foi definitivamente superada com a moderna teoria dos números irracionais desenvolvida por Richard Dedekind (em 1872). A segunda crise teve lugar no final do século XVII (embora o paradoxo de Zenão de Eléia (c. 450 a. C.), da impossibilidade do movimento (450 a. C.), constituísse já um seu prenúncio) na sequência dos trabalhos de Isaac Newton e Gottfried Leibnitz¹⁶ sobre os infinitésimos e só veio a ser resolvida no século XIX, com a introdução dos limites por Augustin-Louis Cauchy¹⁷ e a subsequente aritmética da análise desenvolvida por Karl Weierstrass¹⁸ e seus seguidores. Finalmente, a terceira crise eclodiu com os paradoxos ou antinomias descobertos na sequência do desenvolvimento da teoria dos conjuntos de Georg Cantor (para mais detalhes consultar, por exemplo, [35]). O paradoxo mais famoso é o paradoxo de Bertrand Russel¹⁹ que foi escrito numa carta enviada a Gottlob Frege²⁰, em 1902, na

¹⁴Leonhard Euler (1707–1783), matemático suíço, nascido em Basileia, aluno de Johan Bernoulli, passou a maior parte da sua vida como membro da Academia de S. Petersburgo (14 anos), Berlin (25 anos) e S. Petersburgo novamente (nos seus últimos 17 anos).

¹⁵Eudoxo (408–355 a. C) filósofo que estudou com Platão (c. 427–347 a. C) e fundou uma escola em Cizico no norte da Ásia Menor.

¹⁶Isaac Newton (1642–1727) e Gottfried Leibnitz (1646–1716), foram dois grandes génios matemáticos. O primeiro nasceu em Woolsthorpe em Inglaterra e o segundo em Leipzig na Alemanha.

¹⁷Agustin-Louis Cauchy (1789–1857), matemático francês nascido em Paris.

¹⁸Karl Theodor Wilhelm Weierstrass (1815–1897), matemático alemão nascido em Ostenfeld que iniciou a sua carreira universitária, na Universidade de Berlin, aos 40 anos de idade.

¹⁹Bertrand Arthur William Russel (1872–1970), nasceu no País de Gales e, depois de se formar no Trinity College em Cambridge, dividiu a sua actividade entre a matemática e a filosofia, tendo escrito, juntamente com Whitehead (1861–1947), a monumental obra os *Principia Mathematica*.

²⁰Gottlob Frege (1848–1925), lógico alemão cujas obras mais marcantes são *Begriffsschrift*, publicado em 1879 e *Grundgesetze der Arithmetik*, publicado em dois volumes (1893 e 1903).

seguinte forma:

Seja C o conjunto de todos os conjuntos que são membros de si próprios e seja D o conjunto de todos os conjuntos que não são membros de si próprios. A pergunta que se coloca é: o conjunto D é ou não membro de si próprio.

Se D é membro de si próprio, então pertence a C e não a D pelo que não é membro de si próprio. Por outro lado, se D não é membro de si próprio então pertence a D pelo que é membro de si próprio. O paradoxo consiste no facto de ambas as situações (uma delas inevitável) produzirem uma contradição. Outra versão deste paradoxo é designada por paradoxo do barbeiro, onde se questiona

| quem barbeia o barbeiro que barbeia todos os que não se barbeiam a si próprios (e apenas estes)?

Esta crise, embora não totalmente superada, esbateu-se com as contribuições de Ernst Zermelo em 1908, Abraham Fraenkel e Thoralf Skolem em 1922 e John von Neumann²¹ em 1924, entre outros, os quais, de um modo geral, procuraram evitar as antinomias à custa de certas restrições impostas a um conjunto para ser considerado como tal.

Os teoremas são resultados matemáticos demonstrados com argumentos lógico-dedutivos, aceites como válidos para fundamentar as respectivas conclusões. Porém, embora esta aceitabilidade dos argumentos utilizados nas demonstrações dos teoremas tenha hoje um tratamento relativamente homogéneo, nem sempre foi assim. Particularmente, no princípio do século XX, apareceram duas correntes de pensamento matemático (os *intuicionistas* e os *formalistas*) com concepções completamente distintas do que deveria ser uma demonstração. A escola (ou corrente) intuicionista, que nasceu com Brouwer²², defende que a matemática deve ser desenvolvida apenas por métodos construtivos finitos, enquanto a escola formalista, criada por David Hilbert²³ encara a matemática como estudo de sistemas simbólicos formais. A concepção matemática dos intuicionistas tem como consequência que a prova da existência de uma certa entidade só é aceite quando se mostra que ela é construtível num número finito de passos, não bastando mostrar, por exemplo, que a não existência da entidade em causa implica uma contradição. Esta limitação significa que muitas das demonstrações da matemática contemporânea não são aceites pelos intuicionistas. Outra consequência importante da exigência da construtibilidade finita é a não aceitação universal da *lei do terceiro excluído* que, para os intuicionistas, só é válida em conjuntos finitos. Este facto implica a não aceitação (no caso geral) da demonstração por *reductio ad absurdum*. A seu favor, porém, tudo aponta, na *matemática intuicionista*, para a ausência de contradições internas (o que não acontece nas abordagens clássicas²⁴). Por sua vez, os formalistas consideram a matemática como um jogo de desenvolvimentos abstractos onde se vão produzindo novas fórmulas de símbolos a partir das anteriores, segundo regras muito precisas. Hilbert acreditava que, a partir de um conjunto de certas regras e procedimentos com os quais se obteriam as novas fórmulas que traduziriam os novos resultados, se construiria um sistema não contraditório, isto é, onde não fosse possível produzir uma contradição (fórmula do tipo $p \wedge \neg p$). Porém, tal revelou-se impossível, conforme veio a provar Kurt Gödel em 1931 (por métodos aceites por todas as principais correntes matemáticas). Existe ainda uma terceira escola, a *logicista*, que reduz a matemática a um ramo da lógica. Segundo esta corrente, a lógica em vez de ser um instrumento da matemática passa a ser a sua génese. Os principais impulsionadores desta filosofia foram Whitehead e Russel os quais, nos *Principia Mathematica*, estabeleceram as bases para o estudo da matemática segundo os modelos e desenvolvimentos

²¹ Ernst Zermelo (1871–1953), Abraham Fraenkel (1891–1965), Thoralf Skolem (n. 1887), John von Neumann (1903–1957)

²² L.E.J. Brouwer (1881–1966), matemático holandês que desenvolveu a sua carreira académica na Universidade de Amsterdam.

²³ David Hilbert (1862–1943), matemático marcante que nasceu, obteve o doutoramento e, nos primeiros anos, lecionou em Königsberg, na Prússia. Em 1895 tornou-se professor da Universidade de Göttingen, onde permaneceu até se aposentar em 1930.

²⁴ Apesar do esforço de vários investigadores no sentido de reconstruir toda a matemática dentro das limitações da *matemática intuicionista*, o seu desenvolvimento tem-se revelado pouco produtivo e, muitas vezes, mais complicado que as abordagens clássicas.

determinados pela lógica. A demonstração, apresentada por Gödel, de que o sistema de Hilbert não é completo (isto é, contém proposições indecidíveis, entre as quais a sua própria consistência) tornaram visíveis limitações, até então insuspeitas, dos métodos matemáticos formais e vieram estabelecer a separação entre *verdadeiro* e *demonstrável*.

1.9. Exercícios.

1.1. Determine as tabelas de verdade das proposições

- (a) $(p \Rightarrow q) \Rightarrow r$.
- (b) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.
- (c) $(r \Rightarrow (\neg q \vee p)) \Leftarrow (p \Rightarrow \neg q)$.
- (d) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$.
- (e) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$.
- (f) $\neg(p \wedge q) \wedge (\neg p \vee \neg(\neg q \vee (\neg p \vee q)))$.

1.2. Verifique quais os pares de expressões lógicas a seguir indicadas que incluem expressões lógicas equivalentes.

- (a) $(p \Rightarrow q)$ e $\neg p \Leftarrow \neg q$.
- (b) $\neg(p \wedge \neg q)$ e $\neg p \vee q$.
- (c) $\neg(\neg p)$ e p .
- (d) $\neg(p \vee \neg q)$ e $\neg p \wedge q$.
- (e) $((p \wedge q) \vee (p \wedge \neg q)) \wedge (r \vee \neg r)$ e p .
- (f) $(p \wedge q) \Leftarrow p$ e $(p \wedge q) \vee \neg p$.

1.3. Indique qual ou quais das expressões a seguir indicadas são tautologias, contradições ou nem uma coisa nem outra.

- (a) $p \Rightarrow (\neg p \Rightarrow q)$.
- (b) $(p \wedge q) \Rightarrow (p \vee q)$.
- (c) $p \Rightarrow (q \Rightarrow (q \Rightarrow p))$.
- (d) $p \vee (q \vee \neg p)$.
- (e) $p \wedge \neg(q \vee \neg q)$.
- (f) $p \vee \neg(q \vee \neg q)$.

1.4. Simplifique (se possível) as fórmulas proposicionais a seguir indicadas.

- (a) $\neg(p \vee (q \wedge (\neg r)) \wedge q)$.
- (b) $\neg(\neg p \wedge \neg q)$.
- (c) $\neg(\neg p \vee q) \vee (p \wedge \neg r)$.
- (d) $(p \wedge q) \vee (p \wedge \neg q)$.
- (e) $(p \wedge r) \vee [\neg r \wedge (p \vee q)]$.
- (f) $(\neg p \vee q) \wedge (p \wedge \neg q)$.

1.5. Tendo em conta que a proposição *p ou q mas não ambos*, que se designa por *ou exclusivo*, se denota por $p \dot{\vee} q$, responda às questões a seguir indicadas.

- (a) Determine a tabela de verdade de $p \dot{\vee} q$.
 (b) Encontre uma fórmula equivalente a $p \dot{\vee} q$, utilizando apenas os conectivos lógicos \wedge , \vee e \neg .
 (c) Justifique a resposta da alínea anterior com recurso às respectivas tabelas de verdade.
 (d) Verifique se a fórmula proposicional $(p \dot{\vee} q) \Leftrightarrow (\neg p \dot{\vee} \neg q)$ é (ou não) uma tautologia.
 (e) Conclua que $(p \dot{\vee} \neg q) \wedge (\neg p \dot{\vee} q)$ é equivalente a $(p \wedge q) \vee (\neg p \wedge \neg q)$.
 (f) Simplifique a expressão lógica $(p \dot{\vee} \neg q) \dot{\vee} (\neg p \vee q)$.
- 1.6. Dados os conjuntos X , Y e Z , prove que se $Z \subseteq X$ e $Z \subseteq Y$ então $Z \subseteq X \cap Y$.
- 1.7. Prove que uma família de conjuntos dois a dois disjunta é uma família disjunta.
- 1.8. Prove as leis de De Morgan generalizadas (1.11), (1.12), (1.13) e (1.14).
- 1.9. Considere as funções a seguir indicadas e diga quais as que são injectivas, sobrejectivas e biyectivas.
- (a) $f : \mathbb{N} \rightarrow \mathbb{N}$ tal que $f(n) = n^3$.
 (b) $g : \{a, b, c\} \rightarrow \{1, 2, 3\}$ tal que $g = \{(a, 2), (b, 1), (c, 3)\}$
 (c) $h : \mathbb{R}^+ \rightarrow \mathbb{R}$ tal que $h(x) = \log(x)$, onde \mathbb{R}^+ denota o conjunto dos números reais positivos.
- 1.10. Considerando os conjuntos A e B , tais que $|A| = 3$ e $|B| = 3$, responda às questões a seguir indicadas.
- (a) Quantas funções distintas se podem definir entre o conjunto de partida A e o conjunto de chegada B ?
 (b) Quantas das funções referidas na alínea a) são injectivas?
 (c) Quantas das funções referidas na alínea a) são sobrejectivas?
- 1.11. Dadas as funções
- $$\begin{array}{ccc} f : \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \rightsquigarrow & f(x) = \frac{1}{x^2 + 2}, \end{array} \quad \text{e} \quad \begin{array}{ccc} g : \mathbb{R} & \rightarrow & \mathbb{R} \\ y & \rightsquigarrow & g(y) = 2y - 1, \end{array}$$
- determine as funções compostas $f \circ g$ e $g \circ f$.
- 1.12. Considerando a função $f : A \rightarrow B$ e os subconjuntos de A , X e Y , prove as seguintes proposições:
- (a) $f(X \cap Y) \subseteq f(X) \cap f(Y)$.
 (b) Se f é injectiva, então $f(X \cap Y) = f(X) \cap f(Y)$.
- 1.13. Dados os conjuntos A , B e C , prove as seguintes igualdades e proposições.
- (a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
 (b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
 (c) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.
 (d) Se A e B são conjuntos não vazios então $A \times B = B \times A \Leftrightarrow A = B$.
 (e) Se $A_1 \in \mathcal{P}(A)$ e $B_1 \in \mathcal{P}(B)$, então $A_1 \times B_1 \in \mathcal{P}(A \times B)$.
 (f) $\emptyset \times A = \emptyset$.

- 1.14. Dados os subconjuntos A , B e C de um mesmo universo e tendo em conta que B^A denota o conjunto das funções com conjunto de partida A e conjunto de chegada B , responda às seguintes questões.
- Explicite os elementos do conjunto $\{a, b\}^{\{1,2,3\}}$
 - Prove que se $A \subseteq B$ então $A^C \subseteq B^C$.
 - Prove que se $B \neq C$ então $A^B \cap A^C = \emptyset$.
- 1.15. Prove que $A \times B = \emptyset \Leftrightarrow A = \emptyset$ ou $B = \emptyset$.
- 1.16. A partir da Definição 1.7, prove a implicação
- $$(x_1, x_2, x_3) = (y_1, y_2, y_3) \Rightarrow \forall_{i \in \{1,2,3\}} x_i = y_i .$$
- 1.17. Sendo $X = \{1, 2, 5, 6, 7, 9, 11\}$ e definindo-se a relação $x \sim y$ se e só se $x - y$ é divisível por 5, determine as classes de equivalência X/\sim .
- 1.18. Dados os conjuntos A , B e C , mostre que $(A \cup (B \cap C))^c = A^c \cap (B^c \cup C^c)$.
- 1.19. Sendo $A_n = \{n, n+1, n+2, \dots\}$, para $n \in \mathbb{N}$, determine os conjuntos $\bigcup_{i=1}^k A_i$ e $\bigcap_{i=1}^k A_i$.
- 1.20. Sendo $f : \mathbb{R} \rightarrow \mathbb{R}$ uma função tal que $f(x) = 3x^2 + 2$ para cada $x \in \mathbb{R}$, determine $f^{-1}(f([0, 1]))$ e $f(f^{-1}([0, 5]))$.
- 1.21. Mostre que os intervalos (a, b) e (c, d) , com $a < b$ e $c < d$, são conjuntos equipotentes.
- 1.22. Mostre que \mathbb{R} e o intervalo $(-1, 1)$ são conjuntos equipotentes.
- 1.23. Dada a família de conjuntos $A_n = \{x \in \mathbb{R} : x < 1 + \frac{1}{n}\}$, com $n \in \mathbb{N}$, determine o conjunto $\bigcap_{i=1}^{\infty} A_i$.
- 1.24. Denotando o conjunto dos números racionais positivos por \mathbb{Q}_+ e, para cada $k \in \mathbb{Z}$, sendo
- $$\mathbb{Q}_k = \{2^k \cdot \frac{a}{b} : a, b \in \mathbb{N} \wedge \text{mdc}(a, b) = 1\},$$
- onde $\text{mdc}(a, b)$ denota o máximo divisor comum entre a e b , mostre que $\mathcal{P} = \{\mathbb{Q}_k : k \in \mathbb{Z}\}$ é uma partição do conjunto \mathbb{Q}_+ (em subconjuntos não vazios).
- 1.25. Sendo $f : A \rightarrow B$ e $g : B \rightarrow C$ duas bijeções, mostre que $(g \circ f)^{-1}$ existe e $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- 1.26. Dadas duas funções $f : X \rightarrow Y$ e $g : Y \rightarrow Z$, mostre que
- se f e g são sobrejectivas, então $g \circ f$ é sobrejectiva;
 - se $g \circ f$ é injectiva, então f é injectiva;
 - se f é sobrejectiva e $g \circ f$ é injectiva, então $g \circ f$ é sobrejectiva;
 - se f e g são injectivas, então $g \circ f$ é injectiva;
 - se $g \circ f$ é sobrejectiva, então g é sobrejectiva;
 - se $g \circ f$ é sobrejectiva, então f é sobrejectiva e g é injectiva.
- 1.27. Mostre que se $f : X \rightarrow Y$, $g : X \rightarrow Y$ e $h : Y \rightarrow Z$ são funções tais que $h \circ f = h \circ g$ e h é injectiva, então $f = g$.

- 1.28. Sendo $f : X \rightarrow Y$ uma função e $A \subseteq X$, mostre que
- $f(X) \setminus f(A) \subseteq f(X \setminus A)$;
 - f é injectiva se e só se $\forall_{A \subseteq X} f(X \setminus A) = f(X) \setminus f(A)$.
- 1.29. Seja X um conjunto, $\mathcal{R} \subseteq X \times X$ uma relação reflexiva e transitiva e defina-se $[a] = \{x \in X : a \mathcal{R} x\}$, onde, como é usual, $a \mathcal{R} b \Leftrightarrow (a, b) \in \mathcal{R}$. Mostre que, para quaisquer $a, b \in X$, $a \mathcal{R} b \Leftrightarrow [b] \subseteq [a]$.
- 1.30. Sabendo que $A \preceq B$ significa que existe uma aplicação injectiva de A para B ($A \rightarrow B$) e que $A \prec B$ significa que $A \preceq B$ mas A e B não são equipotentes, prove que se $A \prec B \prec C$, então $A \prec C$.
- 1.31. Utilizando o teorema de Schröder-Bernstein mostre que \mathbb{N} e $\mathbb{N} \times \mathbb{N}$ são conjuntos equipotentes.
- 1.32. Sendo $P(x)$ e $Q(x)$ duas funções proposicionais (ou seja, duas funções cujas imagens são proposições), mostre que
- $\neg \left(\forall_x P(x) \right) \Leftrightarrow \exists_x \neg P(x)$;
 - $\neg \left(\exists_x P(x) \right) \Leftrightarrow \forall_x \neg P(x)$;
 - $\forall_x (P(x) \wedge Q(x)) \Leftrightarrow (\forall_x P(x)) \wedge (\forall_x Q(x))$;
 - $\exists_x (P(x) \vee Q(x)) \Leftrightarrow (\exists_x P(x)) \vee (\exists_x Q(x))$.
- 1.33. Sabendo que X é um conjunto de cardinalidade n (ou seja, $|X| = n$), determine o número de relações reflexivas sobre X .

2

Contextos e Estratégias de Demonstração

Não existe matemática sem demonstração, com a qual, recorrendo a métodos e técnicas desenvolvidos ao longo de milénios, se fundamentam as respectivas conclusões. Embora no capítulo anterior já se tenham feito algumas demonstrações, convém agora dedicar uma atenção mais detalhada aos principais contextos e estratégias de demonstração.

2.1. Estratégias de demonstração da implicação

A expressão proposicional que se designa por *implicação* e se denota por $p \Rightarrow q$ significa que se a proposição p é verdadeira então q também é uma proposição verdadeira. Como consequência, também se diz *q se p ou p somente se q*, sendo ainda usual dizer-se que p é suficiente (ou uma condição suficiente) para q e que q é necessária (ou uma condição necessária) para p . Usualmente, dada a implicação $p \Rightarrow q$, a proposição p designa-se por hipótese ou antecedente e a proposição q designa-se por tese ou consequente. Observe-se que a implicação $p \Rightarrow q$ é falsa se e somente se p é verdadeiro e q é falso (ver Tabela 2.1). Usualmente, os teoremas escrevem-se na forma de implicações deste tipo, onde p denota a hipótese do teorema e q denota a tese do teorema.

Seguem-se três estratégias básicas para a demonstração da implicação.

2.1.1 Prova directa

Como o seu nome indica, a prova directa da implicação $p \Rightarrow q$, consiste em admitir que o antecedente p é verdadeiro e considerando apenas esse facto como adquirido na respectiva fundamentação da prova (para além, naturalmente, dos axiomas e teoremas já conhecidos), mostrar que o consequente q é verdadeiro. Seguem-se dois exemplos que ilustram a utilização desta estratégia de demonstração.

Exemplo 2.1. Vamos utilizar a prova directa para demonstrar que, sendo α um número inteiro, se $\alpha - 2$ é divisível por 3 então $\alpha^2 - 1$ é divisível por 3.

Solução. Vamos admitir como verdadeiro que $\alpha - 2$ é divisível por 3 (proposição p), o que é equivalente a afirmar que $\alpha - 2$ é um múltiplo de 3 ou que existe um inteiro k tal que $\alpha - 2 = 3k$. Como consequência, vem que

$$\alpha + 1 = (\alpha - 2) + 3 = 3(k + 1)$$

o que, por sua vez, implica

$$\alpha^2 - 1 = (\alpha - 1)(\alpha + 1) = 3(\alpha - 1)(k + 1).$$

A última igualdade permite concluir, finalmente, que $\alpha^2 - 1$ é um múltiplo de 3, ou seja, que $\alpha^2 - 1$ é divisível por 3 (proposição q). \square

Exemplo 2.2. Vamos mostrar, directamente, que se x é um número tal que $x^2 - 5x + 6 = 0$ então $x = 2$ ou $x = 3$.

Solução. Primeiramente, note-se que

$$x^2 - 5x + 6 = (x - 2)(x - 3)$$

pelo que, o primeiro membro é igual a zero se e somente se o segundo membro é igual a zero. Assim, se x é um número tal que $x^2 - 5x + 6 = 0$ (proposição p) o que é equivalente a afirmar que x é tal que $(x - 2)(x - 3) = 0$, então podemos concluir que $x - 2 = 0$ ou que $x - 3 = 0$. Por outras palavras, podemos concluir que $x = 2$ ou $x = 3$ (proposição q). \square

Segue-se um teorema demonstrado directamente.

Teorema 2.1. $\forall n ((n \in \mathbb{N} \setminus \{1\} \text{ é ímpar}) \Rightarrow \exists k (k \in \mathbb{N} \wedge n^2 = 8k + 1))$.

Demonstração. Qualquer número natural ímpar, $n > 1$, se pode escrever na forma $n = 2p + 1$, para algum $p \in \mathbb{N}$. Logo, vem que

$$(2p + 1)^2 = 4p(p + 1) + 1. \quad (2.1)$$

É claro que $p(p + 1)$ é um número par e, consequentemente, $p(p + 1) = 2k$ para algum $k \in \mathbb{N}$. Substituindo em (2.1) $p(p + 1)$ por $2k$, obtém-se $n^2 = 8k + 1$. \square

A prova directa da equivalência consiste em demonstrar directamente as implicações nos dois sentidos. Como exemplo, vamos considerar o teorema a seguir, cuja demonstração é feita directamente.

Teorema 2.2. $(x, y) = (u, v) \Leftrightarrow (x = u \wedge y = v)$.

Demonstração. Primeiramente, deve ter-se em conta que, de acordo com a Definição 1.7, $(x, y) = \{\{x\}, \{x, y\}\}$.

(\Leftarrow) Suponha-se $x = u$ e $y = v$, então $\{x\} = \{u\}$ e $\{x, y\} = \{u, v\}$ e, consequentemente, $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$, o que significa que $(x, y) = (u, v)$.

(\Rightarrow) Suponha-se $(x, y) = (u, v)$, ou seja,

$$\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}. \quad (2.2)$$

- Se $x = y$ então, da igualdade (2.2), obtém-se $\{\{x\}\} = \{\{u\}, \{u, v\}\}$. Como consequência $|\{\{x\}\}| = |\{\{u\}, \{u, v\}\}|$, pelo que $\{u\} = \{u, v\}$, ou seja, $u = v$. Logo, mais uma vez, tendo em conta (2.2), concluem-se as igualdades $x = y = u = v$.
- Se $x \neq y$ então a igualdade (2.2) implica que se tenha $\{x\} \in \{\{u\}, \{u, v\}\}$ e $\{x, y\} \in \{\{u\}, \{u, v\}\}$.
 - Uma vez que $|\{x\}| < |\{u, v\}|$, então $\{x\} \neq \{u, v\}$ e, consequentemente, $\{x\} \in \{\{u\}, \{u, v\}\} \setminus \{\{u, v\}\} \Leftrightarrow \{x\} \in \{\{u\}\} \Leftrightarrow \{x\} = \{u\} \Leftrightarrow x = u$.
 - Uma vez que $|\{x, y\}| > |\{u\}|$, então $\{x, y\} \neq \{u\}$ e, consequentemente, $\{x, y\} \in \{\{u\}, \{u, v\}\} \setminus \{\{u\}\} \Leftrightarrow \{x, y\} \in \{\{u, v\}\} \Leftrightarrow \{x, y\} = \{u, v\}$. Por outro lado, uma vez que $x = u$ podemos concluir que $\{x, y\} \setminus \{x\} = \{u, v\} \setminus \{u\}$ o que significa $\{y\} = \{v\} \Leftrightarrow y = v$. \square

Segue-se um corolário do Teorema 2.2, cuja prova fica como exercício.

Corolário 2.3. $(x, y) = (y, x) \Leftrightarrow x = y$.

2.1.2 Demonstração por contraposição

Este método de demonstração baseia-se na tautologia do cálculo proposicional, conhecida como lei de contraposição, (ver Tabela 2.1)

$$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$$

e consiste em demonstrar a implicação $\neg q \Rightarrow \neg p$ para provar a implicação equivalente $p \Rightarrow q$. Neste caso, admite-se que q é falso e, utilizando este facto na fundamentação da prova, conclui-se que p também é falso.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$	$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	1	0	0	1	1

Tabela 2.1: Tabela de verdade para a lei de contraposição $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.

Seguem-se alguns exemplos de utilização da demonstração por contraposição.

Exemplo 2.3. Vamos mostrar, por contraposição, que se o produto de dois inteiros α e β é par então pelo menos um deles é par.

Solução. Denotando por p a proposição *o produto $\alpha\beta$ é par* e por q a proposição *α é par ou β é par*, para provarmos a implicação $p \Rightarrow q$, vamos provar a implicação equivalente $\neg q \Rightarrow \neg p$. Denotando por q_1 a afirmação α é par e por q_2 a afirmação β é par, obtém-se $q = q_1 \vee q_2$. Por aplicação de uma das leis de De Morgan, sabe-se que

$$\neg(q_1 \vee q_2) \Leftrightarrow \neg q_1 \wedge \neg q_2,$$

onde, decorre que a proposição $\neg q$ é equivalente à afirmação α é ímpar e β é ímpar. Assim, admitir que $\neg q$ se verifica equivale a admitir que existem números inteiros m e n tais que

$$\alpha = 2m + 1 \quad \text{e} \quad \beta = 2n + 1.$$

Nestas condições,

$$\alpha\beta = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1,$$

onde decorre que o produto $\alpha\beta$ é ímpar, ou seja, que a proposição $\neg p$ é verdadeira. \square

Exemplo 2.4. Vamos mostrar, por contraposição, que se n é o produto de dois números inteiros positivos α e β então $\alpha \leq \sqrt{n}$ ou $\beta \leq \sqrt{n}$.

Solução. Suponhamos que a tese da proposição é falsa, isto é, que a proposição

$$\neg(\alpha \leq \sqrt{n} \vee \beta \leq \sqrt{n}) \tag{2.3}$$

é verdadeira. Por aplicação de uma das leis de De Morgan, (2.3) é equivalente à proposição

$$\alpha > \sqrt{n} \wedge \beta > \sqrt{n},$$

a qual, por sua vez, implica que se tenha $\alpha\beta > \sqrt{n}\sqrt{n} = n$ e, como consequência, que a proposição

$$\neg(\alpha\beta = n)$$

seja verdadeira. Desta forma, mostramos que se a tese da proposição é falsa, então a hipótese também é falsa. \square

Exemplo 2.5. Dados os conjuntos A e B , vamos provar, por contraposição, que se $A \subseteq B$ e $B \subseteq A$ então $A = B$.

Solução. Tendo em conta que $(A \subseteq B) \wedge (B \subseteq A) \Rightarrow (A = B)$ é equivalente a $(A \neq B) \Rightarrow \neg((A \subseteq B) \wedge (B \subseteq A))$, suponha-se $A \neq B$, o que significa que ou existe $x \in A$ tal que $x \notin B$ ou existe $y \in B$ tal que $y \notin A$. Logo, ou $A \not\subseteq B$ ou $B \not\subseteq A$, pelo que concluímos que a proposição $\neg(A \subseteq B) \vee \neg(B \subseteq A)$ é verdadeira. \square

Segue-se um teorema cuja prova é feita por contraposição.

Teorema 2.4. Seja \sim uma relação de equivalência definida num conjunto X e $x, y \in X$. Se $[x] \neq [y]$ então $[x] \cap [y] = \emptyset$.

Demonstração. Em vez de provarmos a implicação $[x] \neq [y] \Rightarrow [x] \cap [y] = \emptyset$, vamos provar a implicação equivalente $[x] \cap [y] \neq \emptyset \Rightarrow [x] = [y]$.

Se $[x] \cap [y] \neq \emptyset$ então existe $z \in [x] \cap [y]$, o que significa que $x \sim z \wedge y \sim z$ ou ainda $x \sim z \wedge z \sim y$ (uma vez que, sendo \sim uma relação simétrica, $y \sim z \Leftrightarrow z \sim y$). Consequentemente,

$$\begin{aligned} \alpha \in [x] &\Leftrightarrow x \sim \alpha \text{ (pela definição de } [x]) \\ &\Leftrightarrow \alpha \sim x \text{ (pela simetria de } \sim) \\ &\Leftrightarrow \alpha \sim z \text{ (pela transitividade de } \sim \text{ e uma vez que } \alpha \sim x \sim z) \\ &\Leftrightarrow \alpha \sim y \text{ (pela transitividade de } \sim \text{ e uma vez que } \alpha \sim z \sim y) \\ &\Leftrightarrow \alpha \in [y] \text{ (pela definição de } [y]). \end{aligned}$$

\square

2.1.3 Demonstração por redução ao absurdo

A demonstração *por redução ao absurdo* (ou *por absurdo*) tem por base a tautologia do cálculo proposicional

$$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q),$$

a partir da qual, por aplicação das leis de De Morgan, se obtém a tautologia (ver Tabela 2.2) $(p \Rightarrow q) \Leftrightarrow \neg(p \wedge \neg q)$ ou a tautologia

$$\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q).$$

Com este método de prova, para se demonstrar a implicação $p \Rightarrow q$, admite-se que p é verdadeiro e que q é falso (ou seja, nega-se a implicação) e procura-se obter uma contradição (por exemplo, o valor falso de uma dada proposição intrinsecamente verdadeira no contexto da teoria em que nos encontramos).

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

Tabela 2.2: Tabela de verdade para tautologia $(p \Rightarrow q) \Leftrightarrow \neg(p \wedge \neg q)$.

Seguem-se dois exemplos de utilização da prova por redução ao absurdo.

Exemplo 2.6. Vamos mostrar, por redução ao absurdo, que entre treze pessoas pelo menos duas têm o seu aniversário no mesmo mês.

Solução. Vamos provar a implicação $p \Rightarrow q$ onde p é a proposição *existem treze pessoas num dado agrupamento* e q a proposição *pelo menos duas dessas pessoas têm o seu aniversário no mesmo mês*. Suponhamos que existem treze pessoas num dado agrupamento e que não existe nenhum par dessas pessoas com aniversário no mesmo mês (isto é, que a proposição $p \wedge \neg q$ é verdadeira). Porém, marcando cada uma das treze pessoas com o número do respectivo mês de aniversário, para que estes números sejam todos distintos têm de existir pelo menos treze meses, o que constitui uma contradição (ou absurdo). Esta contradição resultou de se ter negado a proposição $p \Rightarrow q$, pelo que a implicação é verdadeira. \square

Exemplo 2.7. Suponha que se escolhem 41 bolas de entre as existentes em cinco caixas, a primeira das quais tem apenas bolas vermelhas, a segunda apenas brancas, a terceira apenas azuis, a quarta apenas verdes e a quinta apenas amarelas. Então pelo menos 12 bolas são vermelhas ou pelo menos 15 bolas são brancas ou pelo menos 4 bolas são azuis ou pelo menos 10 bolas são verdes ou pelo menos 4 bolas são amarelas. Vamos fazer a prova desta afirmação por redução ao absurdo.

Solução. Seja x_1, x_2, x_3, x_4, x_5 o número de bolas escolhidas de cor vermelha, branca, azul, verde e amarela, respectivamente. Vamos provar a implicação

$$x_1 + x_2 + x_3 + x_4 + x_5 = 41 \Rightarrow x_1 \geq 12 \vee x_2 \geq 15 \vee x_3 \geq 4 \vee x_4 \geq 10 \vee x_5 \geq 4$$

por redução ao absurdo. Suponhamos que a igualdade $x_1 + x_2 + x_3 + x_4 + x_5 = 41$ se verifica mas a tese não, isto é, por aplicação de uma das leis de De Morgan, vamos supor que

$$x_1 \leq 11 \wedge x_2 \leq 14 \wedge x_3 \leq 3 \wedge x_4 \leq 9 \wedge x_5 \leq 3.$$

Porém, a negação da tese implica que se tenha

$$x_1 + x_2 + x_3 + x_4 + x_5 \leq 40,$$

o que contraria a hipótese, segundo a qual a igualdade

$$x_1 + x_2 + x_3 + x_4 + x_5 = 41$$

é verdadeira. \square

2.2. Princípio de indução

Antes de introduzirmos a prova por indução, vamos considerar a família de proposições $P(n)$ que, para cada $n \in \mathbb{N}$, denota a desigualdade

$$1 \cdot 2 \cdot \dots \cdot n > 2^n \tag{2.4}$$

É fácil verificar que as proposições $P(1)$, $P(2)$ e $P(3)$ são falsas, enquanto as proposições $P(4)$, $P(5)$ e $P(6)$ são verdadeiros. Será que a proposição $P(n)$ é verdadeira para todos os inteiros $n \geq 4$? Tudo indica que sim, uma vez que a parte esquerda da desigualdade (2.4) ($n!$) cresce mais rapidamente do que a parte direita (2^n). Porém, para a resposta ter validade matemática, é necessário uma prova formal (não bastando afirmar *tudo indica que ...*, *parece que ...*, etc). Um dos métodos mais utilizados na demonstração de teoremas deste tipo, designa-se por método de indução. Este método de indução baseia-se no princípio com o mesmo nome que, por sua vez, decorre da seguinte regra de inferência:

$$\left(P(n_0) \wedge \forall_{n \geq n_0} (P(n) \Rightarrow P(n+1)) \right) \Rightarrow \forall_{n \geq n_0} P(n)$$

onde n é uma variável inteira e

$$\forall_{n \geq n_0} (P(n) \Rightarrow P(n+1))$$

denota a conjunção das proposições $P(n) \Rightarrow P(n+1)$, quando n percorre todos os valores inteiros não inferiores a n_0 .

Note-se que uma expressão lógica do tipo $P(n) \Rightarrow P(n+1)$, para cada valor particular de n , toma um dos valores verdadeiro ou falso, pelo que, para cada n , constitui uma proposição. Porém, tal como se referiu no Capítulo 1, considerando uma expressão deste tipo como função de n , não se pode afirmar que se trata de uma proposição, uma vez que o respectivo valor lógico pode depender dos valores particulares de n . Nestes casos, dada uma expressão lógica cujo valor lógico depende dos valores particulares das variáveis x_1, \dots, x_m , a qual podemos denotar por $Q(x_1, \dots, x_m)$, dizemos que $Q(x_1, \dots, x_m)$ é um *predicado*. Mais formalmente, um predicado é uma aplicação que, para uma dada lista de constantes se transforma numa proposição (ou seja, faz corresponder o valor verdadeiro ou falso).

Assim, para mostrar que o predicado $\forall_{n \geq n_0} P(n)$ é verdadeiro, utilizando o método de indução, é necessário mostrar que a proposição $P(n_0)$ é verdadeira e que o predicado $\forall_{n \geq n_0} (P(n) \Rightarrow P(n+1))$ é também verdadeiro. Logo, podemos descrever o princípio de indução conforme a seguir se indica.

Para cada inteiro positivo n , seja $P(n)$ uma proposição. Para mostrar que a proposição $P(n)$ é verdadeira para todo o inteiro $n \geq n_0$, basta mostrar que

- (a) *a proposição $P(n_0)$ é verdadeira;*
- (b) *para cada inteiro $k \geq n_0$, a implicação*

$$P(k) \Rightarrow P(k+1) \tag{2.5}$$

é também verdadeira (o que significa que a proposição $P(k+1)$ é verdadeiro se a proposição $P(k)$ é verdadeira).

A condição (a) $P(n_0)$ é verdadeira designa-se por *condição inicial* e a implicação (2.5) designa-se por *passo de indução*, onde $P(k)$ constitui a *hipótese de indução*.

Voltando ao nosso exemplo inicial, seja $n_0 = 4$. Já sabemos que a proposição $P(4)$ é verdadeira (isto é, a condição inicial verifica-se). Para completar a demonstração, resta provar o passo de indução, para $k \geq 4$, ou seja, resta provar que a implicação

$$k! > 2^k \Rightarrow (k+1)! > 2^{k+1}$$

é verdadeira, para $k \geq 4$. Com efeito, supondo que a desigualdade $k! > 2^k$ é verdadeira, vem que

$$(k+1)! = k!(k+1) > 2^k \cdot (k+1) > 2^k \cdot 2,$$

uma vez que $k+1 \geq 5 > 2$. Então, pelo princípio de indução, podemos concluir que a desigualdade

$$n! > 2^n$$

é verdadeira para cada inteiro $n \geq 4$.

A primeira prova por indução que se conhece foi publicada no ano de 1575 no livro *Arithmetoricorum Libri Duo*, e é atribuída ao frade beneditino italiano Francesco Maurolico (1494–1575). Maurolico mostrou, por indução, que a soma dos n primeiros números ímpares é igual n^2 (ver Exercício 2.5 (b)).

Seguem-se mais alguns exemplos, onde se utiliza o princípio de indução.

Exemplo 2.8. *Vamos proceder à determinação (e mostrar a respectiva validade) de uma fórmula para a soma dos n primeiros números inteiros positivos.*

Solução. Seja

$$S(n) = 1 + 2 + \cdots + n.$$

Calculando alguns valores de $S(n)$, por exemplo $S(1) = 1$, $S(2) = 3$, $S(3) = 6$, $S(4) = 10$ e $S(5) = 15$, podemos observar que

$$\begin{aligned} 2 \cdot S(1) &= 2 = 1 \cdot 2, \\ 2 \cdot S(2) &= 6 = 2 \cdot 3, \\ 2 \cdot S(3) &= 12 = 3 \cdot 4, \\ 2 \cdot S(4) &= 20 = 4 \cdot 5, \\ 2 \cdot S(5) &= 30 = 5 \cdot 6. \end{aligned}$$

As igualdades anteriores parecem indicar que, para cada inteiro positivo n , se verifica a igualdade

$$2 \cdot S(n) = n(n + 1)$$

ou, equivalentemente, que $S(n) = n(n + 1)/2$. Vamos mostrar que esta última igualdade é verdadeira para todo o inteiro positivo n . Assim, para cada inteiro positivo n considere-se a proposição $p(n)$ definida pela igualdade

$$S(n) = \frac{n(n + 1)}{2}. \quad (2.6)$$

Já sabemos que condição inicial $P(1)$ é verdadeira. Supondo que a proposição $P(k)$ é verdadeira, para um k arbitrariamente escolhido, vamos provar que a proposição $P(k + 1)$ é também verdadeira, ou seja, que a igualdade

$$S(k + 1) = \frac{(k + 1)(k + 2)}{2} \quad (2.7)$$

se verifica.

Demonstração do passo de indução:

$$\begin{aligned} S(k + 1) &= 1 + 2 + \cdots + k + (k + 1) \\ &= S(k) + (k + 1) \\ &= \frac{k(k + 1)}{2} + (k + 1) = \frac{(k + 1)(k + 2)}{2}. \end{aligned}$$

Logo, pelo princípio de indução, a proposição $P(n)$ é verdadeira para todo o inteiro $n \geq 1$. □

Gauss¹, com a idade de nove anos, quando questionado pelo seu professor para calcular $S(n)$, chegou à respectiva fórmula somando duas vezes as parcelas de $S(n)$, dispondo-as por ordem crescente e por ordem decrescente, conforme a seguir se indica.

$$\begin{array}{rcl} S(n) & = & 1 + 2 + \cdots + (n - 1) + n \\ + S(n) & = & n + (n - 1) + \cdots + 2 + 1 \\ \hline 2 S(n) & = & (n + 1) + (n + 1) + \cdots + (n + 1) + (n + 1) \end{array}$$

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

É claro que a última igualdade obtida é equivalente à formula (2.6).

¹Carl Friedrich Gauss (1777–1855), foi o maior matemático de século XIX e um dos maiores de todos os tempos. Nasceu em Brunswick, na Alemanha, e doutorou-se aos 20 anos na Universidade de Helmstedt. Um dos seus trabalhos mais relevantes é a obra *Disquisitiones arithmeticæ* sobre teoria dos números.

Exemplo 2.9. Vamos determinar (e mostrar a respectiva validade) uma fórmula para a soma dos cubos dos n primeiros de números inteiros positivos,

$$1^3 + 2^3 + \cdots + n^3.$$

Solução. Calculando alguns casos particulares, obtém-se

$$1^3 = 1 = 1^2,$$

$$1^3 + 2^3 = 9 = 3^2,$$

$$1^3 + 2^3 + 3^3 = 36 = 6^2,$$

$$1^3 + 2^3 + 3^3 + 4^3 = 100 = 10^2,$$

$$1^3 + 2^3 + 3^3 + 4^3 + 5^3 = 225 = 15^2.$$

Uma vez que, de acordo com o Exemplo 2.8, $S(1) = 1$, $S(2) = 3$, $S(3) = 6$, $S(4) = 10$, $S(5) = 15$, os cálculos anteriores parecem indicar que, para $n \geq 1$, se obtém a fórmula

$$1^3 + 2^3 + \cdots + n^3 = (S(n))^2 = \left(\frac{n(n+1)}{2}\right)^2. \quad (2.8)$$

Vamos fazer a prova por indução.

1. Verificando a condição inicial, vem que

$$1^3 = 1 = \left(\frac{1 \cdot 2}{2}\right)^2.$$

2. Suponhamos que a formula (2.8) é válida para $n = k$ (hipótese de indução), ou seja,

$$1^3 + 2^3 + \cdots + k^3 = \left(\frac{k(k+1)}{2}\right)^2.$$

Então podemos concluir que

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\ &= \left(\frac{k+1}{2}\right)^2 (k^2 + 4(k+1)) \\ &= \left(\frac{(k+1)(k+2)}{2}\right)^2. \end{aligned}$$

Como consequência, a formula (2.8) é válida para todo o inteiro positivo n . □

Exemplo 2.10. Vamos mostrar que, para todos os inteiros $n \geq 0$, o número que se obtém da expressão

$$6^{n+2} + 7^{2n+1}$$

é divisível por 43.

Solução.

1. Verificando a condição inicial, para $n = 0$, obtém-se $6^2 + 7^1 = 43$ que é, claramente, divisível por 43.

2. Supondo que existe um número inteiro p tal que

$$6^{k+2} + 7^{2k+1} = 43p,$$

para k arbitrariamente escolhido, vamos provar que existe um número inteiro q tal que

$$6^{k+1+2} + 7^{2(k+1)+1} = 43q.$$

Com efeito,

$$\begin{aligned} 6^{k+3} + 7^{2k+3} &= 6(6^{k+2} + 7^{2k+1}) - 6 \cdot 7^{2k+1} + 7^{2k+3} \\ &= 6(6^{k+2} + 7^{2k+1}) + 7^{2k+1}(7^2 - 6) \\ &= 6 \cdot 43 \cdot p + 43 \cdot 7^{2k+1} = 43(6p + 7^{2k+1}). \end{aligned}$$

Consequentemente, uma vez que o número $6p + 7^{2k+1}$ é um numero inteiro, a demonstração do passo de indução fica completa, podendo concluir-se que o resultado pretendido se verifica para todos os inteiros $n \geq 0$. \square

Exemplo 2.11. Vamos mostrar que para todos os inteiros $n \geq 4$

$$3^n > n^3. \quad (2.9)$$

Solução.

1. Verificando a condição inicial, para $n = 4$, obtém-se $3^4 = 81 > 64 = 4^3$ pelo que, a desigualdade (2.9) é verdadeira para $n = 4$.
2. Por hipótese de indução, supondo que para $k \geq 4$, a desigualdade

$$3^k > k^3$$

se verifica, resta provar que a desigualdade

$$3^{k+1} > (k+1)^3$$

é verdadeira, o que constitui o passo de indução.

Demonstração do passo de indução. Uma vez que

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1 = k^3 \left(1 + \frac{3}{k} + \frac{3}{k^2} + \frac{1}{k^3}\right)$$

e, por hipótese de indução, $k^3 < 3^k$, então basta mostrar que, para $k \geq 4$,

$$1 + \frac{3}{k} + \frac{3}{k^2} + \frac{1}{k^3} \leq 3.$$

Porém, uma vez que o máximo de $1 + \frac{3}{k} + \frac{3}{k^2} + \frac{1}{k^3}$, para os inteiros $k \geq 4$, é atingido para $k = 4$, com o qual se obtém

$$1 + \frac{3}{4} + \frac{3}{16} + \frac{1}{64} = \frac{125}{64} \leq 3,$$

conclui-se o pretendido. \square

Exemplo 2.12. (Desigualdade de Chebyshev). Dada a sequência de números reais z_1, z_2, \dots, z_n , com $n \in \mathbb{N}$, vamos mostrar que se verifica desigualdade

$$\left(\sum_{k=1}^n z_k\right)^2 \leq n \sum_{k=1}^n z_k^2, \quad (2.10)$$

conhecida por desigualdade de Chebyshev.

Solução. Prova por indução sobre n .

Uma vez que para $n = 1$,

$$\left(\sum_{k=1}^1 z_k \right)^2 = z_1^2 = 1 \sum_{k=1}^1 z_k^2,$$

a desigualdade (2.10) verifica-se para $n = 1$.

Vamos mostrar que para $n \geq 2$,

$$\left(\sum_{k=1}^{n-1} z_k \right)^2 \leq (n-1) \sum_{k=1}^{n-1} z_k^2 \Rightarrow \left(\sum_{k=1}^n z_k \right)^2 \leq n \sum_{k=1}^n z_k^2.$$

Como efeito, admitindo que a desigualdade $\left(\sum_{k=1}^{n-1} z_k \right)^2 \leq (n-1) \sum_{k=1}^{n-1} z_k^2$ se verifica, vem que

$$\begin{aligned} \left(\sum_{k=1}^n z_k \right)^2 &= \left(\sum_{k=1}^{n-1} z_k \right)^2 + z_n^2 + 2z_n \sum_{k=1}^{n-1} z_k \leq (n-1) \sum_{k=1}^{n-1} z_k^2 + z_n^2 + \sum_{k=1}^{n-1} 2z_n z_k \\ &\leq (n-1) \sum_{k=1}^{n-1} z_k^2 + z_n^2 + \sum_{k=1}^{n-1} (z_n^2 + z_k^2) = n \sum_{k=1}^n z_k^2 \end{aligned}$$

uma vez que $(z_n - z_k)^2 \geq 0 \Rightarrow 2z_n z_k \leq z_n^2 + z_k^2$. Logo, por indução, conclui-se que desigualdade de Chebyshev é verdadeira para qualquer $n \in \mathbb{N}$. \square

Exemplo 2.13. Vamos mostrar, por indução, que a soma dos n primeiros termos da progressão aritmética, com primeiro termo α e razão δ , é igual a

$$\frac{1}{2}n(2\alpha + (n-1)\delta). \quad (2.11)$$

Solução. Note-se que se $\alpha_1, \alpha_2, \dots, \alpha_n, \dots$ é uma progressão aritmética cujo primeiro termo é α e a razão é δ , então $\alpha_1 = \alpha$ e, para $n \geq 2$, vem que

$$\alpha_n = \alpha_{n-1} + \delta.$$

Como consequência, para $n \geq 1$, o n -ésimo termo da progressão pode ser determinado por intermédio da equação

$$\alpha_n = \alpha + (n-1)\delta. \quad (2.12)$$

Vamos utilizar esta igualdade para mostrar, por indução, a validade da formula 2.11.

1. Verificando a condição inicial, para $n = 1$, obtém-se

$$\alpha_1 = \alpha = \frac{1}{2} \cdot 1 (2\alpha + 0 \cdot \delta),$$

pelo que o resultado é verdadeiro para $n = 1$.

2. Supondo que, para $k \geq 1$, a hipótese de indução se verifica, ou seja, que a igualdade

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k = \frac{1}{2}k(2\alpha + (k-1)\delta)$$

é verdadeira, vamos provar que a igualdade

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k + \alpha_{k+1} = \frac{1}{2}(k+1)(2\alpha + k\delta)$$

também é verdadeira (passo de indução).

Demonstração do passo de indução. Por hipótese de indução

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k + \alpha_{k+1} = \frac{1}{2}k(2\alpha + (k-1)\delta) + \alpha_{k+1}$$

e, tendo em conta (2.12), sabemos que $\alpha_{k+1} = \alpha + k\delta$. Então

$$\begin{aligned}\alpha_1 + \alpha_2 + \cdots + \alpha_k + \alpha_{k+1} &= k\alpha + \frac{1}{2}k(k-1)\delta + \alpha + k\delta \\ &= (k+1)\alpha + \frac{1}{2}k(k+1)\delta \\ &= \frac{1}{2}(k+1)(2\alpha + k\delta).\end{aligned}$$

□

No exemplo a seguir vamos utilizar uma variante do princípio de indução, designada por *princípio de indução completa*, com o qual, admitindo que a condição inicial $P(n_0)$ se verifica e que, para todo o $k \geq n_0$, a implicação

$$\forall_{n \in [n_0, k]} P(n) \Rightarrow P(k+1)$$

é verdadeira, se conclui que a proposição $P(n)$ é verdadeira para todo o $n \geq n_0$ (onde $[n_0, k]$ denota o conjunto $\{n \in \mathbb{N} : n_0 \leq n \leq k\}$).

Exemplo 2.14. Vamos mostrar, utilizando o princípio de indução completa, que se $\alpha_0 = 12$, $\alpha_1 = 29$ e, para $n \geq 2$, a igualdade

$$\alpha_n = 5\alpha_{n-1} - 6\alpha_{n-2} \quad (2.13)$$

é verdadeira, então pode concluir-se que

$$\alpha_n = 5 \cdot 3^n + 7 \cdot 2^n, \quad (2.14)$$

para todo o inteiro $n \geq 0$.

Solução.

- Verificando a condição inicial, para $n = 0$ e $n = 1$, obtém-se

$$\alpha_0 = 12 = 5 \cdot 3^0 + 7 \cdot 2^0, \quad \alpha_1 = 29 = 5 \cdot 3^1 + 7 \cdot 2^1.$$

- Admitindo, por hipótese de indução, que a igualdade (2.14) se verifica para todo o $n \in [0, k]$, onde k é um número inteiro tal que $k \geq 1$, vamos provar que a igualdade

$$\alpha_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$$

é verdadeira. Com efeito, tendo em conta (2.13) e a hipótese de indução, vem que

$$\begin{aligned}\alpha_{k+1} &= 5\alpha_k - 6\alpha_{k-1} = 5(5 \cdot 3^k + 7 \cdot 2^k) - 6(5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}) \\ &= 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}.\end{aligned}$$

□

Observe-se que, na prova por indução, todos os elementos definidos à custa do argumento de indução, com valores não inferiores ao que define a condição inicial, são importantes. Não se considerando um deles, a prova deixa de ser válida e, mais grave do que isso, o resultado concluído pode estar completamente errado. Seguem-se dois exemplos de utilização incorrecta do princípio de indução que implicaram a obtenção de provas e conclusões erradas.

Exemplo 2.15. Vamos detectar os erros que estão na base da (pseudo)prova por indução, a seguir indicada, de que $P(n)$ é verdadeiro qualquer que seja o inteiro positivo n , onde $P(n)$ denota o predicado: em qualquer conjunto de n pessoas não existem duas pessoas de sexo diferente.

A (pseudo)prova por indução é feita do seguinte modo:

1. Verificando a condição inicial com um conjunto singular, obtém-se a conclusão evidente que não existem duas pessoas com sexo diferente (uma vez que o conjunto é constituído por uma única pessoa). Logo a proposição $P(1)$ é verdadeira.
2. Admitindo, por hipótese de indução, que $P(n)$ é verdadeiro, onde n é um número natural arbitrário fixo, vamos provar (passo de indução) que $P(n+1)$ é também verdadeiro. Assim, sendo $A = \{a_1, a_2, \dots, a_{n+1}\}$ um conjunto com $n+1$ pessoas, então $B = A \setminus \{a_1\}$ e $C = A \setminus \{a_2\}$ são conjuntos com n pessoas. Por hipótese de indução, todas as pessoas em B e todas as pessoas em C têm o mesmo sexo. Como a_3 pertence tanto a B como a C , podemos concluir que todas as pessoas em $B \cup C = A$ têm o mesmo sexo de a_3 . Uma vez que A é arbitrário, conclui-se assim que $P(n) \Rightarrow P(n+1)$ e, consequentemente, que $\forall n (P(n) \Rightarrow P(n+1))$.

Pelo princípio de indução (neste caso incorrectamente concluído) tem-se então que $P(n)$ é verdadeiro $\forall n \in \mathbb{N}$.

Solução. Aparentemente, a demonstração parece correcta. Porém, num certo ponto da demonstração, assumimos a existência de um elemento $a_3 \in A$, ou seja, assumimos que $n+1 = |A| \geq 3$. Na prática provamos $P(1)$ e que $\forall n \geq 2 P(n) \Rightarrow P(n+1)$, faltando, portanto, provar a implicação $P(1) \Rightarrow P(2)$. Porém, uma vez que a implicação $P(1) \Rightarrow P(2)$ é falsa, como é fácil provar com um contra-exemplo, é claro que nem todas as pessoas têm o mesmo sexo. \square

Exemplo 2.16. Vamos determinar os erros da seguinte (pseudo)prova, com a qual se conclui que uma mala pode conter qualquer número de lenços de mão, ou seja, dada uma mala particular e sendo $P(n)$ o predicado: “a mala tem capacidade para n lenços de mão,” então qualquer que seja o número inteiro positivo n , $P(n)$ é verdadeiro.

A (pseudo)prova por indução é feita do seguinte modo:

1. Verificando a condição inicial, é claro que um lenço de mão cabe dentro da mala, pelo que a proposição $P(1)$ é verdadeira.
2. Admitindo, por hipótese de indução, que $P(n)$ é verdadeiro, onde n é um número natural arbitrário, vamos provar (passo de indução) que $P(n+1)$ é também verdadeiro. Na verdade, por experiência própria, sabemos que quando fazemos uma mala, se a mala tem n lenços de mão (hipótese de indução) então podemos acrescentar mais um, pelo que $P(n+1)$ é verdadeiro.

Logo, pelo princípio de indução (mais uma vez, incorrectamente concluído), decorre que a mala contém qualquer número de lenços de mão.

Solução. O erro desta (pseudo)prova reside na utilização errada da nossa experiência, uma vez que não estamos habituados a lidar com situações em que a mala está próxima do seu limite de capacidade. \square

2.3. Princípio da gaiola dos pombos

O princípio da gaiola dos pombos consiste na conclusão evidente de que, dadas n bolas para serem introduzidas em m caixas, onde $n > m$, pelo menos uma das caixas terá de conter duas ou mais bolas. Mais geralmente, o princípio da gaiola dos pombos estabelece o seguinte:

Dadas n bolas para serem introduzidas em m caixas, onde $n > km$, pelo menos uma das caixas terá de conter $k + 1$ ou mais bolas.

Alguns autores designam este princípio por *Princípio de Dirichlet*², por lhe ser atribuída a sua primeira utilização explícita como argumento de demonstração. Com efeito, Dirichlet utilizou este tipo de argumentação combinatória na prova do resultado de *teoria dos números* que a seguir se apresenta (onde \mathbb{R}^+ denota o conjunto dos números reais positivos).

Teorema 2.5 (Dirichlet). $\forall \alpha \in \mathbb{R}^+ \text{ e } \forall n \in \mathbb{N} \exists p \in \mathbb{N} \cup \{0\} \text{ e } \exists q \in [n], \text{ tal que}$

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qn} \leq \frac{1}{q^2},$$

onde $[n]$ denota o conjunto dos primeiros n números naturais.

Demonstração. Tendo em conta que

$$[0, 1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \dots \cup \left[\frac{n-1}{n}, 1\right),$$

seja $f : [n+1] \mapsto [0, 1)$ uma função, tal que $f(i) = i\alpha - \lfloor i\alpha \rfloor$ (onde o símbolo $\lfloor x \rfloor$ denota o maior inteiro não superior a x). Dado que existem n subintervalos e $\lvert [n+1] \rvert = n+1$, pode concluir-se que $\exists j, k \in [n+1]$, com $j > k$, tais que $f(j)$ e $f(k)$ pertencem ao mesmo subintervalo. Logo $\exists r \in \{0, 1, \dots, n-1\}$ tal que $j\alpha - \lfloor j\alpha \rfloor, k\alpha - \lfloor k\alpha \rfloor \in [\frac{r}{n}, \frac{r+1}{n})$ e, consequentemente,

$$\begin{aligned} |j\alpha - \lfloor j\alpha \rfloor - k\alpha + \lfloor k\alpha \rfloor| &= |j\alpha - k\alpha - (\lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor)| \\ &= |(j-k)\alpha - (\lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor)| \\ &< \frac{1}{n}. \end{aligned}$$

Assim, existe $p \in \mathbb{N} \cup \{0\}$ ($p = \lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor$) tal que $|(j-k)\alpha - p| < \frac{1}{n}$, donde vem que

$$\left| \alpha - \frac{p}{j-k} \right| < \frac{1}{n(j-k)} \Leftrightarrow \left| \alpha - \frac{p}{q} \right| < \frac{1}{qn} \leq \frac{1}{q^2},$$

com $q = j - k$ (note-se que, nestas condições, $q \in [n]$). □

Matematicamente, o princípio da gaiola dos pombos pode ser apresentado de dois modos distintos:

A. *Seja X um conjunto finito tal que $|X| = n$,*

$$X = X_1 \cup X_2 \cup \dots \cup X_m,$$

onde $X_i \cap X_j = \emptyset$ para $i \neq j$. Se $n > m$ então existe $i \in \{1, \dots, m\}$ tal que $|X_i| > 1$.

²Lejeune Dirichlet (1805–1859), algebrista alemão nascido em Düren. Foi aluno de Gauss, tendo-lhe sucedido em Göttingen depois da sua morte.

- B. Sejam X e Y dois conjuntos arbitrários tais que $|X| = n$ e $|Y| = m$. Se $n > m$ então não existe uma função $f : X \mapsto Y$ tal que

$$f(x) = f(y) \Rightarrow x = y,$$

ou seja, não existe nenhuma função injetiva de X em Y .

Seguem-se alguns exemplos de questões que podem ser resolvidas por aplicação do princípio da gaiola dos pombos.

Exemplo 2.17. Vamos provar que em qualquer cidade com pelo menos 1,5 milhões de habitantes existem pelo menos quatro pessoas com o mesmo número de cabelos (tendo em conta que um homem tem no máximo 400.000 cabelos).

Solução. Considere que existem 400.001 caixas marcadas, respectivamente, com os inteiros $0, 1, \dots, 400.000$ e que introduzimos um cartão de identificação de cada habitante na caixa marcada com o número de cabelos que lhe corresponde. Podemos supor que, na melhor das hipóteses, os primeiros 400.001 habitantes têm todos um número de cabelos diferente. Porém, na melhor das hipóteses, os cartões de identificação dos primeiros 800.002 habitantes, ficarão distribuídos dois por cada caixa. Por sua vez, os primeiros 1.200.003, na melhor das hipóteses terão os seus cartões de identificação distribuídos três por cada caixa. Em tais condições, qualquer que seja o número de cabelos do habitante ordenado na posição 1.200.004, a caixa que incluir a sua identificação terá, necessariamente, quatro cartões de identificação. Esta conclusão pode ser imediatamente obtida, tendo em conta que

$$1.500.000 > 3 \times 400.001.$$

□

Exemplo 2.18. Sabendo que num torneio em que participam n equipas de futebol, todas jogam umas com as outras, prove que em cada jornada deste torneio existem pelo menos duas equipas que jogam o mesmo número de jogos.

Solução. Em qualquer das jornadas do torneio, cada equipa pode fazer entre 0 e $n - 1$ jogos. Tal como anteriormente, consideramos n caixas marcadas com os números $0, 1, \dots, n - 1$ e introduzimos um cartão de identificação de cada equipa na caixa correspondente ao número de jogos que faz. Nestas condições, numa mesma jornada utiliza-se uma e apenas uma das caixas marcadas com 0 ou $n - 1$ (com efeito, se existe uma equipa que não joga com nenhuma outra então não existe nenhuma equipa que joga com todas as outras, por outro lado, se existe uma equipa que joga com todas as outras então não existe uma equipa que não joga com nenhuma). Logo, numa mesma jornada, ou se utilizam apenas as caixas $0, \dots, n - 2$ ou se utilizam apenas as caixas $1, \dots, n - 1$, mas não ambas as situações. Como consequência, temos apenas $n - 1$ caixas para introduzir n cartões de identificação de outras tantas equipas. Logo, pelo princípio da gaiola dos pombos, pelo menos uma das caixas terá de conter dois ou mais cartões de identificação.

Vamos apresentar outra prova deste mesmo resultado, utilizando a versão B do princípio da gaiola dos pombos.

Seja $E = \{e_1, e_2, \dots, e_n\}$ o conjunto de equipas e seja $f : E \mapsto \{0, \dots, n - 1\}$ uma função tal que $f(e_i)$ é igual ao número de equipas com que a equipa e_i joga numa dada jornada. Tendo em conta a justificação anterior, é claro que $|\{0, n - 1\} \cap f(E)| \leq 1$. Então a versão B do princípio da gaiola dos pombos implica que f não seja injetiva. □

Exemplo 2.19. Prove que se marcarmos, arbitrariamente, 17 pontos num triângulo equilátero com lados de comprimento 4, então existem pelo menos dois pontos a uma distância máxima de 1.

Solução. Considere-se a partição do triângulo inicial em 16 triângulos equiláteros, com lados de comprimento 1, conforme se indica na Figura 2.1. Com recurso ao princípio da gaiola dos pombos concluímos que pelo menos um dos 16 triângulos da partição contém dois ou mais pontos. Como consequência, é claro que tais pontos estarão a uma distância máxima de 1. □

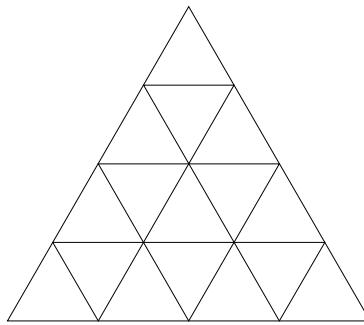


Figura 2.1: Partição de um triângulo em 16 triângulos.

Exemplo 2.20. Prove que num conjunto de $n + 1$ números inteiros existem (pelo menos) dois cuja diferença é divisível por n .

Solução. Sejam $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ números inteiros arbitrários. Introduza-se o número α_i na caixa marcada com $\alpha_i \pmod n$ que denota o resto da divisão inteira de α_i por n (ver (1.18)). Logo, temos n caixas possíveis (dado que os restos pertencem ao conjunto $\{0, 1, \dots, n - 1\}$) para $n + 1$ números. Assim, temos pelo menos dois restos iguais que correspondem a dois números introduzidos na mesma caixa e, consequentemente, a diferença entre esses números é divisível por n . \square

Exemplo 2.21. Prove que num conjunto de dez números inteiros não negativos todos distintos e inferiores a 107 existem dois subconjuntos disjuntos cujas somas dos respectivos elementos são iguais.

Solução. O conjunto de dez números inteiros não negativos todos distintos e inferiores a 107, cuja soma dos elementos é máxima, é o conjunto $\{97, \dots, 106\}$ com soma 1.015. Considerem-se 1.016 caixas marcadas com os números $0, \dots, 1.015$ e considere-se que cada subconjunto de números é introduzido na caixa marcada com a soma dos seus elementos. Sabe-se que existem $2^{10} = 1.024$ subconjuntos de um conjunto com 10 elementos e 1.016 caixas. Logo, existe pelo menos uma caixa com pelo menos dois subconjuntos A e B . Como consequência, para se obterem dois subconjuntos disjuntos nas condições requeridas, basta considerar os subconjuntos $A \setminus B$ e $B \setminus A$. \square

Exemplo 2.22. Seja X um conjunto de n elementos e sejam X_1, X_2, \dots, X_{n+1} subconjuntos de X não vazios. Prove que existem dois subconjuntos distintos $I_p, I_q \subseteq I = \{1, 2, \dots, n + 1\}$, tais que

$$\bigcup_{k \in I_p} X_k = \bigcup_{k \in I_q} X_k.$$

Solução. A cada subconjunto não vazio $I_j \subseteq I$, corresponde o subconjunto $\bigcup_{k \in I_j} X_k$ não vazio de X . Por outro lado, existem $2^{n+1} - 1$ subconjuntos não vazios de I , a cada um dos quais corresponde uma parte não vazia de X , de entre as $2^n - 1$ partes possíveis. Dado que

$$2^n - 1 < 2^{n+1} - 1,$$

podemos concluir que existem pelo menos dois subconjuntos de índices nas condições referidas. \square

2.4. Exercícios.

2.1. Mostre, com uma prova directa, que sendo a e b dois inteiros ímpares então $a + b$ é par.

- 2.2. Mostre, por contraposição, que se n^2 é ímpar então n é ímpar.
- 2.3. Mostre que se $n \in \mathbb{N}$, então existe um e um só par (a, b) de números inteiros não negativos tais que $n = 2^a(2b + 1)$.
- 2.4. Mostre, por redução ao absurdo, a seguinte proposição:

Sejam m_1, m_2, \dots, m_n inteiros positivos. Se colocarmos

$$m_1 + m_2 + \dots + m_n - n + 1$$

bolas em n caixas então a primeira caixa contém pelo menos m_1 bolas ou a segunda caixa contém pelo menos m_2 bolas ou ... ou a n -ésima caixa contém pelo menos m_n bolas.

- 2.5. Mostre que qualquer que seja o inteiro positivo n se verificam as igualdades:

- (a) $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$;
- (b) $1 + 3 + 5 + \dots + (2n-1) = n^2$;
- (c) $1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$;
- (d) $1^3 + 3^3 + 5^3 + \dots + (2n-1)^3 = n^2(2n^2 - 1)$;
- (e) $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \dots + n \cdot (n+1) \cdot (n+2) = \frac{n(n+1)(n+2)(n+3)}{4}$.

- 2.6. Mostre que para todo o $n \geq 2$ se verifica a igualdade

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{(n-1) \cdot n} = 1 - \frac{1}{n}.$$

- 2.7. Mostre que para todo o inteiro $n \geq 0$, o número que se obtém da expressão

$$11^{n+2} + 12^{2n+1}$$

é divisível por 133.

- 2.8. Mostre que para todo o inteiro $n \geq 0$ o número que decorre da expressão

$$4^{2n+1} + 3^{n+2}$$

é um múltiplo de 13.

- 2.9. Mostre que para todo o inteiro $n \geq 0$ o número que se obtém da expressão

$$n^4 - 4n^2$$

é divisível por 3.

- 2.10. Mostre que para todo o inteiro $n \geq 17$ a desigualdade

$$2^n > n^4$$

é verdadeira.

- 2.11. Mostre que para todo o inteiro $n \geq 9$,

$$n! > 4^n$$

é uma desigualdade válida.

- 2.12. Mostre, por indução sobre n , que para todos os números reais $x > -1$ e para todos os inteiros positivos n a desigualdade

$$(1 + x)^n \geq 1 + nx$$

é verdadeira.

- 2.13. Mostre que a soma dos n primeiros termos da progressão geométrica cujo primeiro termo é a e a razão é q (com $q \neq 1$) é igual a

$$\frac{a(1 - q^n)}{1 - q}.$$

- 2.14. Mostre que se $a_0 = 6$, $a_1 = 11$ e, qualquer que seja $n \geq 2$

$$a_n = 3a_{n-1} - 2a_{n-2},$$

então para todo o inteiro positivo n

$$a_n = 5 \cdot 2^n + 1.$$

- 2.15. Sabendo que num encontro existem várias pessoas que se cumprimentam, prove que existem pelo menos duas pessoas que cumprimentam exactamente o mesmo número de pessoas.

- 2.16. Dado um conjunto de dez números inteiros positivos com dois algarismos. Mostre que existem dois subconjuntos diferentes não vazios cujas somas dos respectivos elementos são iguais.

- 2.17. Mostre que para qualquer conjunto de 12 números inteiros positivos inferiores a 120 existem quatro subconjuntos cujas somas dos respectivos elementos são iguais.

- 2.18. Suponha que se escreve em cada uma das $n \times n$ entradas de uma tabela um dos números do conjunto $\{-1, 0, 1\}$ e que, posteriormente, se adiciona os elementos obtidos em cada linha, coluna e cada uma das duas diagonais. Prove que pelo menos duas destas somas são iguais.

- 2.19. Mostre que dados $n + 1$ números inteiros positivos distintos não superiores a $2n$ existem dois números com soma igual a $2n + 1$.

- 2.20. Supondo que se liga cada par de vértices de um hexágono regular com um segmento vermelho ou azul, prove que existe pelo menos um triângulo formado por segmentos da mesma cor.

- 2.21. Seja $n \in \mathbb{N}$, tal que $n > 1$ e n não é primo. Mostre, por redução ao absurdo, que n admite pelo menos um factor primo p tal que $p \leq \sqrt{n}$.

- 2.22. Utilizando o Exercício 2.21, mostre directamente, que o numero 101 é primo.

- 2.23. Mostre, por indução, que

- (a) $(1 + \sqrt{2})^n + (1 - \sqrt{2})^n$ é um inteiro par, para $n \in \mathbb{N}$,
- (b) $(1 + \sqrt{2})^n - (1 - \sqrt{2})^n = b_n \sqrt{2}$, onde $b_n \in \mathbb{N}$, para $n \in \mathbb{N}$.

- 2.24. Seja A um subconjunto de cardinalidade 20 do conjunto $\{1, 4, 7, 10, 13, \dots, 100\}$. Mostre que A contém dois números distintos cuja soma é igual 104.

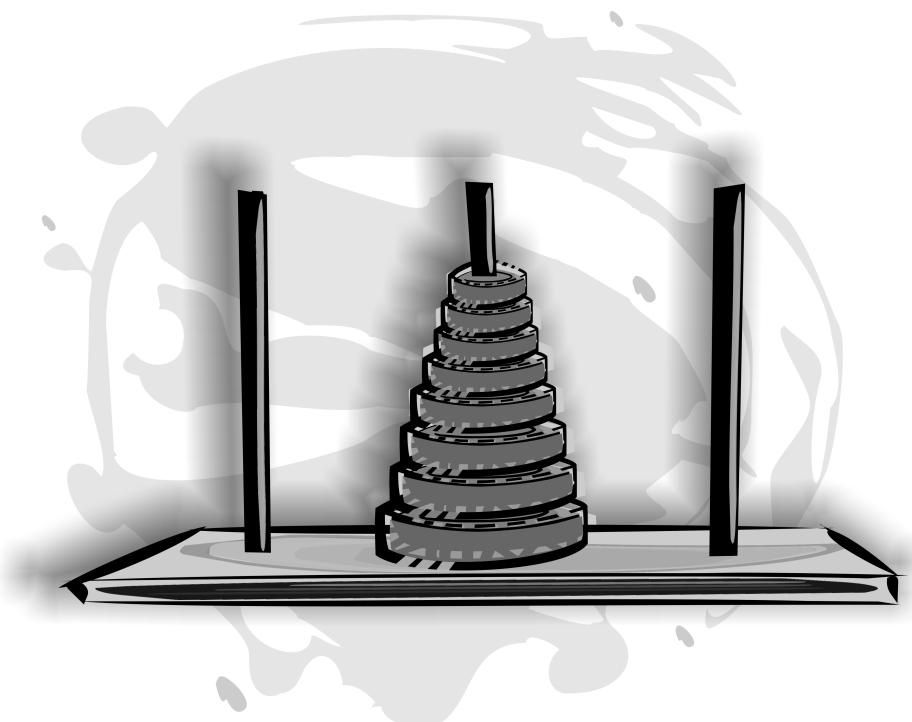
- 2.25. Seja A um subconjunto de cardinalidade $n + 1$ do conjunto $[2n]$, onde $n \in \mathbb{N}$. Mostre que A contém dois números a e b distintos tais que a divide b .

- 2.26. Quantas diagonais tem um n -ágono convexo?

- 2.27. Mostre, por indução, que $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$, para todo $n \in \mathbb{N}$.
- 2.28. Mostre, por indução, que $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$, para todo $n \in \mathbb{N}$.
- 2.29. Mostre, por indução, que para todo o $n \in \mathbb{N}$, se A é um conjunto finito, então $|A \times [n]| = n|A|$.
- 2.30. Mostre, por indução e também por prova directa, que para todo $n \in \mathbb{N}$, o número $n(n+1)$ é par.

Parte II

Combinatória



3

Princípios de Enumeração Combinatória

A enumeração de objectos combinatórios, identificados por um determinado padrão, é um dos tópicos relevantes da matemática discreta. Neste capítulo, vamos abordar vários métodos de contagem de elementos de um conjunto finito, desde os muito básicos até aos que utilizam métodos matemáticos sofisticados. Todos eles, porém, muito poderosos quando utilizados em contextos adequados.

Começamos pelo princípio da bijecção que permite a enumeração e/ou contagem de objectos de um conjunto a partir da enumeração e/ou contagem dos elementos de outro conjunto, com o qual (em geral) é mais simples trabalhar. Seguem-se as leis da adição e da multiplicação, depois das quais continuamos com uma generalização da lei da adição – o princípio de inclusão-exclusão.

3.1. Princípio da bijecção

O *princípio da bijecção* consiste na identificação dos objectos de um conjunto com os elementos de outro conjunto com o qual é mais fácil trabalhar. Assim, de acordo com este princípio, dados os conjuntos A e B , se existe uma bijecção

$$f : A \rightarrow B,$$

isto é, tal que $x \neq y \Rightarrow f(x) \neq f(y)$ e $f(A) = B$ (ver Definição 1.17), conhecida a cardinalidade do conjunto A , ficamos a conhecer a cardinalidade do conjunto B . Seguem-se alguns exemplos, aos quais vamos recorrer ao longo do capítulo.

Exemplo 3.1. Seja \mathbb{B}^n o conjunto dos n -uplos de componentes binárias e seja $\mathcal{P}(X)$ o conjunto de todos os subconjuntos do conjunto $X = \{x_1, x_2, \dots, x_n\}$. Pretende-se definir uma bijecção entre $\mathcal{P}(X)$ e \mathbb{B}^n .

Solução. Considere-se a função

$$\begin{aligned} f : \mathcal{P}(X) &\mapsto \mathbb{B}^n \\ A &\rightsquigarrow f(A) = (b_1, b_2, \dots, b_n), \end{aligned}$$

tal que $b_i = 1$ se e só se $x_i \in A$. Por exemplo, supondo $X = \{1, 2, 3, 4, 5\}$ e $A = \{1, 3, 4\}$, vem que $f(A) = (1, 0, 1, 1, 0)$. Nestas condições, é claro que se $A = \emptyset$ então $f(A)$ é o n -uplo de componentes

todas nulas e se $A = X$ então $f(A)$ é o n -uplo de componentes todas unitárias. Resta mostrar que f é uma bijecção entre $\mathcal{P}(X)$ e \mathbb{B}^n .

- Sejam $A, B \in \mathcal{P}(X)$ tais que $A \neq B$. Logo, sem perda de generalidade, podemos admitir que $\exists x_i \in A \setminus B$. Consequentemente, vem que a i -ésima componente de $f(A)$ é igual a 1 e a i -ésima componente de $f(B)$ é igual a zero, pelo que $f(A) \neq f(B)$. Assim, concluímos que f é injetiva.
- Seja $b = (b_1, \dots, b_n) \in \mathbb{B}^n$. Então o conjunto $C = \{x_i \in X : b_i = 1\}$ pertence a $\mathcal{P}(X)$ e é tal que $f(C) = b$. Logo, conclui-se que f é sobrejectiva. \square

Exemplo 3.2. Vamos mostrar que existe uma bijecção entre os diferentes modos de colocar k bolas iguais em n caixas distintas e o conjunto de sequências binárias com k zeros e $n - 1$ uns.

Solução. Vamos recorrer a uma representação pictórica de uma colocação arbitrária das k bolas nas n caixas. Assim, utilizando o símbolo $|$ para separar as caixas umas das outras e supondo que se colocam k_1 bolas na primeira caixa, k_2 bolas na segunda e assim sucessivamente, até se colocarem k_n bolas na n -ésima caixa (pelo que $k = k_1 + k_2 + \dots + k_n$), obtém-se:

$$\underbrace{\overbrace{o \dots o}^{k_1 \text{ bolas}}}_{k \text{ bolas}} | \underbrace{\overbrace{o \dots o}^{k_2 \text{ bolas}}}_{k \text{ bolas}} | \dots | \underbrace{\overbrace{o \dots o}^{k_n \text{ bolas}}}_{k \text{ bolas}}$$

A partir desta representação pictórica, substituindo $|$ por "1" e o por "0", produz-se a sequência binária

$$\underbrace{\overbrace{0 \dots 0}^{k_1 \text{ zeros}}}_{k \text{ zeros}} \underbrace{\overbrace{1 0 \dots 0}^{k_2 \text{ zeros}}}_{k \text{ zeros}} \dots \underbrace{\overbrace{1 \dots 1 0 \dots 0}^{k_n \text{ zeros}}}_{k \text{ zeros}}$$

Para o caso particular de $k = 7$ e $n = 6$, uma possibilidade de colocação das 7 bolas nas 6 caixas é a que a seguir se representa.

$$\underbrace{\overbrace{o o}^{2 \text{ bolas}}}_{7 \text{ bolas}} | \underbrace{\overbrace{}^{0 \text{ bolas}}}_{7 \text{ bolas}} | \underbrace{\overbrace{o}^{1 \text{ bola}}}_{7 \text{ bolas}} | \underbrace{\overbrace{}^{0 \text{ bolas}}}_{7 \text{ bolas}} | \underbrace{\overbrace{o}^{1 \text{ bola}}}_{7 \text{ bolas}} | \underbrace{\overbrace{o o o}^{3 \text{ bolas}}}_{7 \text{ bolas}}$$

Nesta condições, a sequência binária

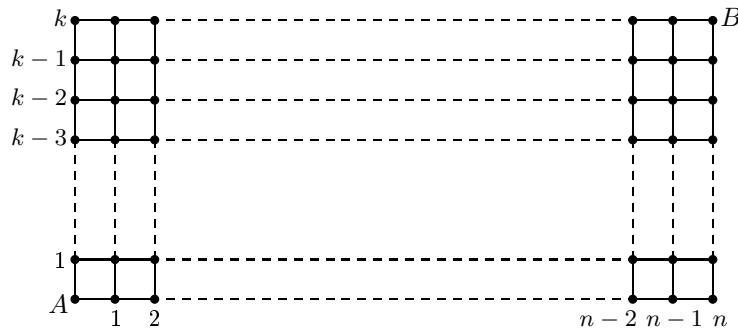
$$001101101000$$

com $k = 7$ zeros e $n - 1 = 5$ uns corresponde à referida colocação particular das bolas nas caixas.

Conclui-se assim que as sequências binárias de k zeros e $n - 1$ uns estão biunivocamente relacionadas com as diferentes possibilidades de colocação das k bolas nas n caixas, conforme se pretendia. \square

Exemplo 3.3. Considerando a grelha de dimensão $k \times n$, onde k denota o número de segmentos verticais e n o número de segmentos horizontais (ver Figura 3.1), suponha-se que qualquer caminho entre A e B se faz percorrendo apenas segmentos de recta, verticais e horizontais, que unem os pontos representados. Neste exemplo, vamos mostrar que existe uma bijecção entre o conjunto de caminhos mais curtos de A para B e o conjunto de sequências binárias com n uns e k zeros.

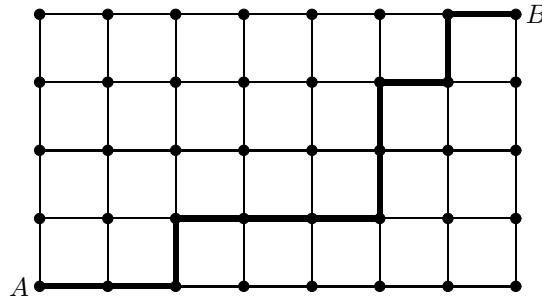
Solução. Note-se que ao percorrer qualquer dos caminhos mais curtos entre o ponto A e o ponto B , não existem deslocamentos da direita para a esquerda, nem de cima para baixo. Consequentemente, qualquer dos caminhos mais curtos entre A e B tem k segmentos verticais e n segmentos horizontais. Assim, representando por "0" cada um dos segmentos verticais do caminho e por "1" cada um dos segmentos horizontais, obtém-se uma sequência binária, com n uns e k zeros que identifica (de modo

Figura 3.1: Grelha de dimensão $k \times n$.

único) o caminho em causa. Reciprocamente, cada sequência binária com n uns e k zeros determina um dos caminhos mais curtos entre A e B . Por exemplo, a sucessão

$$11011100101 \quad (3.1)$$

determina o caminho da grelha de dimensão 4×7 representado na Figura 3.2. \square

Figura 3.2: Um dos caminhos mais curtos entre A e B .

Exemplo 3.4. O exemplo anterior vai facilitar o estabelecimento de uma bijecção entre todas as sequências binárias de n uns e $k - 1$ zeros e o conjunto de soluções inteiras não negativas da equação

$$x_1 + x_2 + \dots + x_k = n. \quad (3.2)$$

Solução. Com efeito, considere uma grelha de dimensão $(k-1) \times n$ e dois pontos A e B representados, respectivamente, no canto inferior esquerdo e no canto superior direito, tal como se indica no Exemplo 3.3. Para cada um dos caminhos mais curtos entre A e B , seja x_i , para $i = 1, 2, \dots, k$, o número de segmentos horizontais que constituem o caminho e pertencem à $(i-1)$ -ésima linha (contando as linhas de baixo para cima). É claro que a soma destes inteiros x_i (para todas as linhas) é precisamente igual a n . Consequentemente, cada um destes caminhos está biunivocamente relacionado com uma solução inteira não negativa da equação (3.2). Por outro lado, uma vez que também existe uma bijecção entre os caminhos mais curtos de A para B numa grelha de dimensão $k \times n$ e as sequências binárias com n uns e k zeros, por composição das duas bijecções conclui-se que existe uma bijecção entre as soluções inteiras não negativas da equação (3.2) e as sequências binárias com n uns e $k - 1$ zeros. No caso particular de $k = 5$ e $n = 7$, uma solução inteira não negativa da equação (3.2) é

$$x_1 = 2, \quad x_2 = 3, \quad x_3 = 0, \quad x_4 = 1, \quad x_5 = 1$$

que corresponde ao caminho mais curto entre A e B representado na Figura 3.2, o qual, por sua vez, corresponde à sequência binária (3.1) com $n = 7$ uns e $k - 1 = 4$ zeros. \square

Mais tarde, voltaremos a estes exemplos para calcularmos o número de objectos em causa.

3.2. Princípios da adição e da multiplicação

Muitos problemas de enumeração combinatória podem resolver-se com recurso a dois princípios básicos, conhecidos por *princípio da adição* e *princípio da multiplicação*. Vamos iniciar este estudo pelo segundo que é o mais conhecido.

Teorema 3.1 (Princípio da multiplicação). *Se A_1, A_2, \dots, A_n são conjuntos não vazios finitos, então o conjunto dos n -uplos (a_1, a_2, \dots, a_n) , onde $a_i \in A_i$, $i = 1, 2, \dots, n$, o qual vamos denotar por $A_1 \times A_2 \times \dots \times A_n$, é tal que*

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|.$$

Demonstração. Por indução sobre n . Seja $A_i = \{a_1^{(i)}, a_2^{(i)}, \dots, a_{|A_i|}^{(i)}\}$.

Claro que para $n = 1$ temos $|A_1|$ sequências do comprimento 1: $(a_1^{(1)}), (a_2^{(1)}), \dots, (a_{|A_1|}^{(1)})$.

Suponhamos que o resultado se verifica para a cardinalidade de qualquer conjunto de p -uplos, com $p < n$ e $n > 1$. Então, fazendo $m = |A_1| \cdot |A_2| \cdot \dots \cdot |A_{n-1}|$, por hipótese de indução, existem m $(n-1)$ -uplos, $(a_1, a_2, \dots, a_{n-1})$, tais que $a_i \in A_i$, para $i = 1, 2, \dots, n-1$. Cada um destes $(n-1)$ -uplos pode estender-se aos n -uplos com elementos $a_1^{(n)}, a_2^{(n)}, \dots, a_{|A_n|}^{(n)}$, considerando $(x_1), (x_2), \dots, (x_m)$ como sendo os $(n-1)$ -uplos obtidos de A_1, A_2, \dots, A_{n-1} e escrevendo todos os possíveis n -uplos na forma

$$\begin{array}{cccc} (x_1, a_1^{(n)}) & (x_1, a_2^{(n)}) & \cdots & (x_1, a_{|A_n|}^{(n)}) \\ (x_2, a_1^{(n)}) & (x_2, a_2^{(n)}) & \cdots & (x_2, a_{|A_n|}^{(n)}) \\ \cdots & \cdots & \cdots & \cdots \\ (x_m, a_1^{(n)}) & (x_m, a_2^{(n)}) & \cdots & (x_m, a_{|A_n|}^{(n)}). \end{array}$$

Por este processo, conclui-se que a cardinalidade de $A_1 \times A_2 \times \dots \times A_n$ é igual a $m \cdot |A_n|$ e que, por sua vez,

$$m \cdot |A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|. \quad \square$$

Exemplo 3.5. *Vamos calcular o número de números de 4 algarismos que se podem escrever com os dígitos pertencentes $\{1, 2, \dots, 9\}$?*

Solução. Cada número de 4 algarismos corresponde a um 4-uplo da forma (a_1, a_2, a_3, a_4) , onde $a_i \in A_i = \{1, \dots, 9\}$, para $i = 1, 2, 3, 4$. Aplicando o princípio da multiplicação conclui-se que o número destes 4-uplos é igual

$$|A_1| \cdot |A_2| \cdot |A_3| \cdot |A_4| = 9^4 = 6.561. \quad \square$$

Em certos problemas, verifica-se que cada conjunto A_i , com $i > 1$, depende da escolha das componentes anteriores. O teorema a seguir estende o princípio da multiplicação aos casos em que, para cada n -uplo (a_1, a_2, \dots, a_n) , A_i depende das componentes a_1, a_2, \dots, a_{i-1} .

Teorema 3.2 (Princípio da multiplicação generalizada). *Admitindo que um processo de escolha das componentes de um n -uplo se pode partir em n passos sucessivos, de tal forma que existem r_1 escolhas possíveis no primeiro passo, para a primeira componente, r_2 escolhas possíveis no segundo, para a segunda componente, ..., r_n escolhas possíveis no último, para a n -ésima componente, então podem escolher-se $r_1 \cdot r_2 \cdot \dots \cdot r_n$ n -uplos distintos.*

Demonstração. Por indução sobre n . Para $n = 1$ o resultado é evidente.

Suponhamos que o resultado se verifica para todos os p -uplos, tais que $p < n$, com $n > 1$. Então, por hipótese de indução, sabe-se que existem $r_1 \cdot r_2 \cdot \dots \cdot r_{n-1}$ ($n - 1$)-uplos distintos, cada um dos quais se pode estender aos n -uplos cuja última componente é escolhida no n -ésimo passo, de entre r_n escolhas possíveis. Consequentemente, pelo princípio da multiplicação, o número de escolhas possíveis para um dado n -uplo é igual a

$$(r_1 \cdot r_2 \cdot \dots \cdot r_{n-1}) \cdot r_n = r_1 \cdot r_2 \cdot \dots \cdot r_n.$$

□

Seguem-se alguns exemplos de aplicação do teorema anterior.

Exemplo 3.6. Vamos calcular o número de números com 4 algarismos pertencentes ao conjunto $\{1, 2, \dots, 9\}$ de tal forma que nenhum número tenha dois dígitos iguais.

Solução. Note-se que a utilização do princípio da multiplicação não nos permite efectuar o cálculo pretendido. Com efeito, embora se conheça o conjunto $A_1 = \{1, 2, \dots, 9\}$, não podemos determinar os conjuntos A_2 , A_3 e A_4 , uma vez que A_2 depende da escolha do primeiro algarismo, por sua vez, o conjunto A_3 depende da escolha dos dois primeiros algarismos e, finalmente, A_4 depende da escolha dos três primeiros algarismos. Por outras palavras, os conjuntos A_2 , A_3 e A_4 não são previamente conhecidos.

A resolução deste problema passa pela utilização do princípio da multiplicação generalizada, com o qual, tendo em conta que $r_1 = 9$, $r_2 = 8$, $r_3 = 7$ e $r_4 = 6$, se obtém o resultado

$$9 \cdot 8 \cdot 7 \cdot 6 = 3.024.$$

□

Exemplo 3.7. Vamos calcular o número de números com 4 algarismos, pertencentes ao conjunto $\{1, 2, \dots, 9\}$, tais que nenhum deles tem dígitos repetidos e todos contêm o algarismo 5.

Solução. Vamos considerar o procedimento a seguir.

1. Começamos por escolher a posição do dígito 5, de entre as quatro possíveis, pelo que $r_1 = 4$.
2. Escolhemos um dos dígitos entre 1 e 9 diferente de 5 (dado que o dígito 5 consta na posição escolhida no passo 1) para a primeira posição não ocupada, donde se conclui que $r_2 = 8$.
3. Escolhemos um novo algarismo (diferente de 5 e do escolhido no passo 2) para a primeira posição não ocupada em nenhum dos passos anteriores, pelo que $r_3 = 7$.
4. Escolhemos o quarto algarismo distinto de qualquer dos algarismos anteriormente considerados para a única posição ainda disponível, pelo que $r_4 = 6$.

Como consequência, aplicando o princípio da multiplicação generalizada, concluímos que existem $4 \cdot 8 \cdot 7 \cdot 6 = 1.344$ quádruplos da forma (i, x, y, z) , cujas as componentes foram determinadas pelos passos 1, ..., 4, ou seja, são tais que

$$\begin{aligned} i &\in \{1, 2, 3, 4\}, \\ x &\in \{1, 2, \dots, 9\} \setminus \{5\}, \\ y &\in \{1, 2, \dots, 9\} \setminus \{5, x\}, \\ z &\in \{1, 2, \dots, 9\} \setminus \{5, x, y\}. \end{aligned}$$

Note-se que aplicando o princípio da bijecção se conclui que existem tantos números nas condições requeridas quantos os quádruplos determinados pelo procedimento definido pelos passos 1, 2, 3 e 4. □

Exemplo 3.8. Vamos determinar o número de subconjuntos de um conjunto com n elementos.

Solução. Aplicando o princípio da bijecção, verifica-se que o número de subconjuntos de um conjunto de cardinalidade n é igual ao número de n -uplos binários (compare com o Exemplo 3.1) o qual, por aplicação do princípio da multiplicação, é igual a 2^n . \square

Segue-se um outro princípio combinatório básico, muito utilizado em enumeração combinatória conjuntamente com o princípio da multiplicação.

Princípio da adição. *Sejam A_1, A_2, \dots, A_n conjuntos finitos, dois a dois disjuntos (ou seja, tais que $A_i \cap A_j = \emptyset$ para $i \neq j$), então*

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i|.$$

O problema, porém, é mais complicado, quando os conjuntos não são necessariamente disjuntos. Por exemplo, para dois conjuntos A e B (ver a Figura 3.3), vem que

$$|A \cup B| = |A| + |B| - |A \cap B|. \quad (3.3)$$

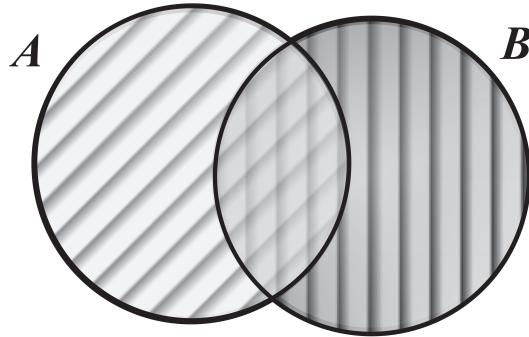


Figura 3.3: União de dois conjuntos com intersecção não vazia.

No caso mais geral, da união de n conjuntos finitos (com intersecção arbitrária), utilizaremos o princípio de inclusão-exclusão que se apresentará na próxima secção.

Seguem-se alguns exemplos de aplicação do princípio da adição.

Exemplo 3.9. *Vamos calcular o número de números com 4 algarismos pertencentes ao conjunto $\{1, 2, \dots, 9\}$ que contêm o algarismo 5.*

Solução. Observe-se que o método utilizado no Exemplo 3.7, neste caso, não funciona. Com efeito, adoptando a notação seguida no Exemplo 3.7, concluímos que, embora existam $r_1 = 4$ possibilidades para a localização do dígito 5, existem $9 \cdot 9 \cdot 9 = 729$ possibilidades para os restantes dígitos (uma vez que o dígito 5 pode voltar a aparecer em qualquer das restantes posições). Assim, o resultado $4 \cdot 729 = 2.916$ que se obteria, adoptando o procedimento seguido no Exemplo 3.7, não é o correcto, uma vez que alguns dos 2.916 quádruplos do tipo (i, x, y, z) correspondem, neste caso, a um mesmo número. Por exemplo, qualquer dos quádruplos $(1, 3, 5, 2)$ e $(3, 5, 3, 2)$ obtidos no Exemplo 3.7, neste caso, correspondem ao número 5.352 (note que o primeiro elemento do quádruplo indica a posição de dígito 5, enquanto os restantes elementos correspondem aos dígitos que ocupam as posições que ainda estão livres, pela ordem com que aparecem).

Como resolver este problema? Partimos o conjunto destes números em quatro subconjuntos disjuntos que dependem, unicamente, da posição do primeiro dígito 5 (a contar da esquerda para a direita). Sejam $A_1 = \{1, 2, \dots, 9\}$, $A_2 = A_1 \setminus \{5\}$ e

$$\begin{aligned}E_1 &= \{(5, x, y, z) : x, y, z \in A_1\}, \\E_2 &= \{(x, 5, y, z) : x \in A_2, y, z \in A_1\}, \\E_3 &= \{(x, y, 5, z) : x, y \in A_2, z \in A_1\}, \\E_4 &= \{x, y, z, 5\} : x, y, z \in A_2\}.\end{aligned}$$

Claro que os conjuntos E_i , $i = 1, 2, 3, 4$ são dois a dois disjuntos e a sua união cobre todas as possibilidades. Por outro lado, a cardinalidade de cada um destes conjuntos pode ser determinada por aplicação do princípio da multiplicação. Logo, vem que

$$\begin{aligned}|E_1 \cup E_2 \cup E_3 \cup E_4| &= |E_1| + |E_2| + |E_3| + |E_4| \\&= 9^3 + 8 \cdot 9^2 + 8^2 \cdot 9 + 8^3 \\&= 2.465.\end{aligned}$$

Um modo mais simples de resolver este problema (sem recorrer ao princípio da adição) seria calcular primeiro o número de números de quatro dígitos pertencentes ao conjunto $\{1, 2, \dots, 9\}$ (cujo valor é $9^4 = 6.561$) e depois subtrair o número de números de quatro dígitos pertencentes ao conjunto $\{1, 2, \dots, 9\} \setminus \{5\}$ (cujo valor é $8^4 = 4.096$). Nestas condições obtém-se o resultado

$$6.561 - 4.096 = 2.465,$$

que, naturalmente, é igual ao obtido pelo procedimento anterior. \square

Os próximos exemplos ilustram a aplicação de todos os princípios apresentados.

Exemplo 3.10. Vamos determinar o número de partições do conjunto $\{1, 2, \dots, n\}$ em dois subconjuntos, nenhum dos quais vazio.

Solução. A ordem dos subconjuntos não é importante. Um dos subconjuntos da partição contém o elemento n (e o outro não), pelo que o número de partições é igual ao número de subconjuntos do conjunto $\{1, 2, \dots, n-1\}$ com excepção do vazio (note que qualquer um destes subconjuntos não vazios, juntamente com o seu complementar em $\{1, 2, \dots, n\}$, define uma das partições pretendidas). Como consequência, concluí-se que este número é igual a $2^{n-1} - 1$. \square

Exemplo 3.11. Vamos calcular o maior número de pacotes distintos não vazios de fruta, supondo que cada pacote tem no máximo n maçãs e no máximo m laranjas.

Solução. Cada pacote é determinado por um par (x, y) , onde x é o número de maçãs e y é o número de laranjas. Uma vez que $0 \leq x \leq n$ e $0 \leq y \leq m$, por aplicação do princípio da multiplicação, vem que o número destes pares é igual a $(n+1)(m+1)$. Porém, dado que temos de subtrair o par $(0, 0)$, de entre os pares admissíveis, concluímos que existem

$$(n+1)(m+1) - 1$$

pacotes diferentes. \square

Exemplo 3.12. Vamos calcular o número de números maiores do que 666 e com 3 algarismos, tais que o primeiro algarismo é diferente do último.

Solução. Seja A o conjunto dos números nas condições indicadas e seja

- A_6 – o subconjunto de A relativo aos números que começam com algarismo 6;
- A_7 – o subconjunto de A relativo aos números que começam com algarismo 7;
- A_8 – o subconjunto de A relativo aos números que começam com algarismo 8;
- A_9 – o subconjunto de A relativo aos números que começam com algarismo 9.

Então

$$A = A_6 \cup A_7 \cup A_8 \cup A_9$$

e, uma vez que estes subconjuntos são disjuntos, por aplicação do princípio da adição, vem que

$$|A| = |A_6| + |A_7| + |A_8| + |A_9|.$$

Podemos observar que

$$A_7 = \{(7, x, y) : x \in \{0, 1, 2, \dots, 9\}, y \in \{0, 1, 2, \dots, 9\} \setminus \{7\}\},$$

onde, por aplicação do princípio da multiplicação, se conclui que $|A_7| = 10 \cdot 9 = 90$. De modo idêntico se conclui que $|A_8| = 90$ e $|A_9| = 90$. Resta calcular a cardinalidade do subconjunto A_6 , para o que vamos considerar a partição de A_6 nos subconjuntos B_1 e B_2 tais que

$$B_1 = \{(6, 6, y) : y \in \{7, 8, 9\}\}$$

e

$$B_2 = \{(6, x, y) : x \in \{7, 8, 9\}, y \in \{0, 1, 2, \dots, 9\} \setminus \{6\}\}.$$

Aplicando os princípios da adição e da multiplicação, vem que

$$|A_6| = |B_1| + |B_2| = 3 + 3 \cdot 9 = 30.$$

Nestas condições, o resultado final vem dado por $|A| = 30 + 3 \cdot 90 = 300$. □

3.3. Princípio de inclusão-exclusão

A determinação do número de elementos da união finita de conjuntos finitos poder ser feita com recurso ao princípio da adição apenas quando os conjuntos são disjuntos. Quando tal não acontece temos de utilizar o *princípio de inclusão-exclusão* que vamos abordar, inicialmente, com alguns exemplos.

Exemplo 3.13. Vamos calcular o número de inteiros positivos não superiores a 500 que não são divisíveis por 3 nem por 5.

Solução. Seja A_i o conjunto dos inteiros positivos não superiores a 500 divisíveis por i . Então, o conjunto dos inteiros positivos não superiores a 500 que não são divisíveis por 3 nem por 5 é determinado pela intersecção

$$A_3^c \cap A_5^c$$

onde $A_i^c = \{1, 2, \dots, 500\} \setminus A_i$. Utilizando uma das leis de De Morgan vem que

$$A_3^c \cap A_5^c = (A_3 \cup A_5)^c.$$

Calculando o número de elementos de $A_3 \cup A_5$, utilizando (3.3), obtém-se

$$|A_3 \cup A_5| = |A_3| + |A_5| - |A_3 \cap A_5| = \left\lfloor \frac{500}{3} \right\rfloor + \left\lfloor \frac{500}{5} \right\rfloor - \left\lfloor \frac{500}{15} \right\rfloor,$$

onde $\lfloor x \rfloor$ é o maior número inteiro não superior a x . Nestas condições, vem que

$$|A_3 \cup A_5| = 166 + 100 - 33 = 233.$$

Como consequência, o resultado final é $|A_3^c \cap A_5^c| = 500 - 233 = 267$. □

Segue-se a fórmula geral da determinação da cardinalidade da união finita de conjuntos finitos que foi primeiro publicada pelo matemático português Daniel Augusto da Silva¹ (1814–1878) e, posteriormente, estudada por James J. Sylvester (1814–1897) que mais tarde a apresentou numa publicação datada de 1883. O desconhecimento da primeira publicação tem implicado que, algumas vezes, se designe esta fórmula por fórmula de Sylvester.

Teorema 3.3 (Fórmula de Daniel da Silva). *Dados os conjuntos finitos arbitrários A_1, A_2, \dots, A_n*

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k-1} S_k^{(n)}$$

onde $S_k^{(n)} = \sum_{I \in [n]^k} \left| \bigcap_{i \in I} A_i \right|$ e $[n]^k$ é conjunto de subconjuntos de $[n] = \{1, 2, \dots, n\}$ com k elementos.

Demonstração. Por indução sobre n .

Para $n = 1$, $|A_1| = |A_1|$.

Para $n = 2$, o resultado é equivalente à fórmula (3.3).

Suponha-se que o resultado é verdadeiro para menos do que n conjuntos, com $n \geq 3$, fazendo $A = \bigcup_{i=1}^{n-1} A_i$ e $B = A_n$ e utilizando a fórmula (3.3), vem que

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n| - \left| \bigcup_{i=1}^{n-1} A_i \cap A_n \right| \\ &= \sum_{k=1}^{n-1} (-1)^{k-1} S_k^{(n-1)} + |A_n| - \sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in [n-1]^k} \left| \bigcap_{i \in I} A_i \cap A_n \right| \\ &= \sum_{k=1}^{n-1} (-1)^{k-1} \sum_{n \notin I \in [n]^k} \left| \bigcap_{i \in I} A_i \right| + \sum_{k=1}^n (-1)^{k-1} \sum_{n \in I \in [n]^k} \left| \bigcap_{i \in I} A_i \right|, \end{aligned}$$

uma vez que para $k = 1$, $(-1)^{k-1} \sum_{n \in I \in [n]^k} \left| \bigcap_{i \in I} A_i \right| = |A_n|$. Tendo em conta que, para $k = n$, $(-1)^{k-1} \sum_{n \notin I \in [n]^k} \left| \bigcap_{i \in I} A_i \right| = 0$, finalmente, vem que

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k-1} \left(\sum_{n \in I \in [n]^k} \left| \bigcap_{i \in I} A_i \right| + \sum_{n \notin I \in [n]^k} \left| \bigcap_{i \in I} A_i \right| \right) = \sum_{k=1}^n (-1)^{k-1} S_k^{(n)}.$$

□

Seguem-se alguns exemplos de aplicação desta fórmula.

Exemplo 3.14. Entre 200 alunos do segundo ano de matemática, 80 inscrevem-se no curso de análise, 80 no curso de álgebra e 80 em probabilidades. O número de alunos que se inscrevem simultaneamente em quaisquer dois cursos é igual a 30 e o número de alunos que se inscrevem simultaneamente nos três cursos é igual a 15. Pretende saber-se:

- (1) qual o número total de alunos que não se inscreveram em nenhum destes cursos?

¹Daniel Augusto da Silva nasceu em Lisboa e formou-se em Matemática na Universidade de Coimbra, em 1839. Foi oficial da marinha e lente da Escola Naval. A fórmula em causa foi publicada em 1854 no J. de l'Ecole Polytechnique, cah. 30, num artigo com o título *Propriétades gerales*.

(2) qual o número de alunos que apenas se inscreveram em probabilidades?

Solução. Sejam A_1 , A_2 e A_3 os conjuntos de alunos que se inscreveram em análise, álgebra e probabilidade, respectivamente. Então, sabemos que

$$\begin{aligned}|A_1| &= |A_2| = |A_3| = 80, \\ |A_1 \cap A_2| &= |A_1 \cap A_3| = |A_2 \cap A_3| = 30\end{aligned}$$

e

$$|A_1 \cap A_2 \cap A_3| = 15.$$

Com recurso à notação da fórmula de Daniel da Silva, obtém-se

$$\begin{aligned}S_1^{(3)} &= |A_1| + |A_2| + |A_3| = 240, \\ S_2^{(3)} &= |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| = 90, \\ S_3^{(3)} &= |A_1 \cap A_2 \cap A_3| = 15.\end{aligned}$$

Logo, por aplicação da fórmula de Daniel da Silva, podemos concluir que

$$|A_1 \cup A_2 \cup A_3| = S_1^{(3)} - S_2^{(3)} + S_3^{(3)} = 240 - 90 + 15 = 165.$$

Para resolver o problema (1), podemos calcular o número de alunos que se inscreveram pelo menos num curso e subtrair esse número à totalidade dos alunos. Nestas condições, vem que

$$200 - |A_1 \cup A_2 \cup A_3| = 200 - 165 = 35.$$

No caso (2), se aos 165 alunos que se inscreveram pelo menos num curso subtraímos o número de alunos que se inscreveram em álgebra ou análise, obtém-se

$$165 - |A_1 \cup A_2| = 165 - (160 - 30) = 35,$$

que corresponde, precisamente, à solução pretendida. \square

Exemplo 3.15. Suponha que numa competição de atletismo estão inscritos 80 atletas em quatro provas, a saber:

1. maratona;
2. 10.000 metros;
3. 5.000 metros;
4. 3.000 metros.

Entre estes atletas, 52 estão inscritos na maratona, 27 nos 10.000 metros e 22 nos 5.000 metros. Existem 18 que estão inscritos na maratona e nos 10.000 metros. Existem 13 atletas que estão inscritos na maratona e nos 5.000 metros e 8 estão inscritos nos 10.000 e 5.000 metros. Existem 3 atletas inscritos na maratona, 10.000 e 5.000 metros. Por sua vez, de entre os atletas inscritos nos 3.000 metros apenas 5 estão inscritos também nos 5.000 metros, os restantes são atletas que se inscreveram numa única prova. Vamos calcular quantos atletas estão inscritos na prova de 3.000 metros?

Solução. Seja A_M o conjunto dos atletas inscritos na maratona, A_{10} o conjunto dos inscritos nos 10.000 metros, A_5 o conjunto dos inscritos nos 5.000 metros e A_3 o conjunto dos inscritos nos 3.000 metros.

$$\begin{aligned}|A_M \cup A_{10} \cup A_5 \cup A_3| &= 80 \\ |A_M| + |A_{10}| + |A_5| + |A_3| &= 52 + 27 + 22 + |A_3| \\ |A_M \cap A_{10}| + |A_M \cap A_5| + |A_{10} \cap A_5| + |A_5 \cap A_3| &= 18 + 13 + 8 + 5 \\ |A_M \cap A_{10} \cap A_5| &= 3.\end{aligned}$$

Logo, vem que

$$80 = 101 + |A_3| - 44 + 3 \Leftrightarrow 124 - 104 = |A_3| \Leftrightarrow |A_3| = 20.$$

\square

Exemplo 3.16. Vamos calcular o número de números com quatro algarismos que não são divisíveis nem por 2, nem por 3, nem por 5, nem por 7.

Solução. Sendo A_i o conjunto dos números com quatro algarismos que são divisíveis por i , pretendemos calcular a cardinalidade do conjunto

$$A_2^c \cap A_3^c \cap A_5^c \cap A_7^c = (A_2 \cup A_3 \cup A_5 \cup A_7)^c.$$

Primeiro, vamos calcular o número de elementos do conjunto $A_2 \cup A_3 \cup A_5 \cup A_7$, utilizando fórmula de Daniel da Silva, ou seja,

$$\begin{aligned} |A_2 \cup A_3 \cup A_5 \cup A_7| &= |A_2| + |A_3| + |A_5| + |A_7| - |A_2 \cap A_3| - |A_2 \cap A_5| \\ &\quad - |A_2 \cap A_7| - |A_3 \cap A_5| - |A_3 \cap A_7| - |A_5 \cap A_7| \\ &\quad + |A_2 \cap A_3 \cap A_5| + |A_2 \cap A_3 \cap A_7| + |A_2 \cap A_5 \cap A_7| \\ &\quad + |A_3 \cap A_5 \cap A_7| - |A_2 \cap A_3 \cap A_5 \cap A_7| \\ &= 4.500 + 3.000 + 1.800 + 1.286 - 1.500 - 900 - 643 \\ &\quad - 600 - 429 - 257 + 300 + 215 + 128 + 86 - 43 \\ &= 6.943. \end{aligned}$$

Logo, uma vez que existem $9.000 = 9.999 - 999$ números com quatro dígitos, finalmente conclui-se que o resultado final é igual a $9.000 - 6.943 = 2.057$. \square

Com recurso à fórmula de Daniel da Silva, podemos generalizar o método utilizado no Exemplo 3.14 e no Exemplo 3.16, conforme a seguir se indica.

Se N_0 é o número de elementos que não pertencem a nenhum dos conjuntos $A_i \subseteq X$, $i = 1, 2, \dots, n$ e $S_0^{(n)} = |X|$, então

$$N_0 = \left| X \setminus \bigcup_{i=1}^n A_i \right| = \sum_{k=0}^n (-1)^k S_k^{(n)}. \quad (3.4)$$

Note-se que $N_0 = |X| - |A_1 \cup \dots \cup A_n|$ e, para a determinação de $|A_1 \cup \dots \cup A_n|$, podemos utilizar a fórmula de Daniel da Silva.

A fórmula de Daniel da Silva é conhecida em linguagem corrente por princípio de inclusão-exclusão, o qual vamos formular do seguinte modo.

Teorema 3.4 (Princípio de inclusão-exclusão). *Dado um conjunto finito de objectos, cada um dos quais pode ter ou não a propriedade $1, 2, \dots, n$, seja $N(i_1, i_2, \dots, i_k)$ o número de objectos que têm pelo menos as propriedades i_1, i_2, \dots, i_k . Então o número de objectos que têm pelo menos uma destas propriedades é igual a*

$$\begin{aligned} &N(1) + N(2) + \dots + N(n) \\ &- N(1, 2) - N(1, 3) - \dots - N(n-1, n) \\ &+ N(1, 2, 3) + N(1, 2, 4) + \dots + N(n-2, n-1, n) \\ &- \dots + (-1)^{n-1} N(1, 2, \dots, n) \end{aligned}$$

O exemplo a seguir ilustra a aplicação deste princípio.

Exemplo 3.17. Vamos calcular o número de números inteiros entre 2 e 1.000 que têm pelo menos uma raiz (quadrada, cúbica ou de maior grau) inteira.

Solução. Os objectos em causa são números do conjunto $\{2, 3, \dots, 1.000\}$. Considere-se que um objecto tem a propriedade i se é um número inteiro elevado à potencia i . Uma vez que $2^{10} > 1.000$ e $2^9 < 1.000$, concluir-se que as propriedades dos nossos objectos se resumem às propriedades $2, 3, \dots, 9$. Como consequência, o número N_1 de objectos com pelo menos uma destas propriedades pode ser determinado, por aplicação do princípio de inclusão-exclusão, conforme a seguir se indica.

$$\begin{aligned} N_1 = & N(2) + N(3) + \dots + N(9) \\ & - N(2, 3) - N(2, 4) - \dots - N(8, 9) \\ & + N(2, 3, 4) + N(2, 3, 5) + \dots + N(7, 8, 9) \\ & - \dots - N(2, 3, \dots, 9). \end{aligned}$$

Com facilidade se calculam estes números. Por exemplo, $N(2) = 30$, $N(3) = 9$, $N(4) = 4$, $N(5) = N(6) = 2$, $N(7) = N(8) = N(9) = 1$, $N(2, 3) = N(6) = 2$, $N(2, 4) = N(4) = 4$, $N(2, 3, 4) = 0$, $N(2, 3, 6) = N(6) = 2$, etc. Logo, com facilidade se conclui que $N_1 = 40$. \square

3.4. Exercícios

- 3.1. Procure uma bijecção entre os seguintes conjuntos de objectos combinatórios:
 - (a) conjunto das diferentes colocações de k bolas iguais em n caixas distintas, sem que haja caixas vazias;
 - (b) conjunto das diferentes partições do número k em n parcelas ordenadas de soma k ;
 - (c) conjunto das sequências binárias de $n - 1$ uns e $k - n$ zeros.
- 3.2. Qual o número de pares homem mulher não casados de entre um conjunto de n pares casados?
- 3.3. Existem quatro caminhos da cidade A para a cidade B , três de B para C e dois de A para C .
 - (a) De quantos modos diferentes podemos ir da cidade A para a cidade C ?
 - (b) De quantos modos diferentes podemos ir da cidade A para a cidade B e voltar?
 - (c) De quantos modos diferentes podemos ir da cidade A para a cidade B e voltar, sem repetir qualquer dos caminhos entre pares de cidades?
- 3.4. Qual o número de subconjuntos de dois elementos do conjunto $\{0, \dots, n\}$ cuja diferença é k ?
- 3.5. De quantos modos se podem colocar k bolas diferentes em n caixas distintas, supondo que cada caixa tem no máximo uma bola?
- 3.6. Qual o número de números naturais com cinco algarismos nos quais o dígito 3 aparece exactamente uma vez?
- 3.7. Qual o número de pares de cartas que é possível retirar ordenadamente de um baralho de 52 de tal forma que a primeira é uma espada (\spadesuit) e a segunda é uma dama?
- 3.8. Qual o número de números divisíveis por 5 com três algarismos, onde o primeiro algarismo é maior do que o último?
- 3.9. Qual o número de inteiros positivos não superiores a 10^n sem algarismos vizinhos iguais?
- 3.10. Quantos pacotes (não vazios) distintos se podem fazer com um máximo de cinco maçãs e oito laranjas?

- 3.11. Mostre que dados $n + 1$ números inteiros positivos distintos não superiores a $2n$ existem pelo menos dois que são relativamente primos.
- 3.12. Mostre que dado um conjunto de n números inteiros positivos distintos existe um subconjunto cuja soma dos elementos é divisível por n .
- 3.13. Sabendo que num conjunto de 100 alunos, 50 estudam francês, 40 estudam inglês e 20 estudam ambas as línguas, quantos alunos não estudam nenhuma das línguas?
- 3.14. Indique o número de inteiros que descrevem palindromas (isto é, cuja leitura da esquerda para a direita e da direita para a esquerda produz a mesma sequência de dígitos) de entre os seguintes números:
 - (a) naturais com cinco dígitos,
 - (b) naturais com $2k + 1$ dígitos ($k \in \mathbb{N}$),
 - (c) naturais com $2k$ dígitos ($k \in \mathbb{N}$).
- 3.15. Utilizando um alfabeto com m letras, quantos palindromas com n letras (ou seja, de comprimento n) se podem escrever?
- 3.16. Qual o número de números naturais divisíveis por 3, com cinco dígitos cujo dígito do meio é igual a d , para $d = 0, 1, \dots, 9$?
- 3.17. Qual o número de números naturais divisíveis por 3, com cinco dígitos que contêm (pelo menos) um dígito igual a d , para $d = 0, 1, \dots, 9$?
- 3.18. Qual o número de números naturais divisíveis por 3, com cinco dígitos que não contêm nenhum dígito igual a d , para $d = 0, 1, \dots, 9$?
- 3.19. Qual o número de números naturais inferiores a 1.000 que não são divisíveis por 3, nem por 7, nem por 11?
- 3.20. Qual o número de números naturais inferiores a 1.000 que não são divisíveis por 4, nem por 6, nem por 9?
- 3.21. Qual o número de números naturais inferiores a 1.000 que não são divisíveis por nenhum número natural superior a um elevado ao quadrado?
- 3.22. Qual o número de números naturais inferiores a 1.000 que não são divisíveis por nenhum número natural superior a um elevado ao cubo?
- 3.23. Qual o número de colocações de oito torres num tabuleiro de xadrez (de dimensão 8×8) de tal modo que nenhuma torre está em posição de atacar outra.
- 3.24. Qual o número de sequências de números de $[n]$ de comprimento $2n$ que contém cada um dos números de $[n]$ em duplicado, nas quais não existem números iguais em posições consecutivas?
- 3.25. Qual o número de submulticonjuntos de cardinalidade 11 do "multiconjunto" que contém quatro elementos a , três elementos b e onze elementos c ?
- 3.26. Qual o número de números naturais com cinco dígitos cuja soma dos seus dígitos é não superior a 43?
- 3.27. Qual o número de números naturais com seis dígitos cuja soma dos seus dígitos é não superior a 51?

- 3.28. Qual o número de números naturais com sete dígitos cuja soma dos seus dígitos pertence ao conjunto $\{3, 4, \dots, 60\}$?
- 3.29. A Ana e o Bruno jogam com dados lançando, em cada jogada, quatro dados ao mesmo tempo. De acordo com as regras estabelecidas, se sair pelo menos um 6 a Ana ganha, caso contrário ganha o Bruno. Qual dos jogadores tem a maior chance de ganhar?
- 3.30. Quantos pares de equipas, sedo uma de futebol (com 11 jogadores) e outra de basquetebol (com 5 jogadores) se podem formar, a partir de uma classe de 30 estudantes, se
- nenhum estudante participa em ambas as equipas,
 - no máximo um estudante participa em ambas as equipas,
 - qualquer estudante pode participar em ambas as equipas.

4

Agrupamentos e Identidades Combinatórias

A *Análise Combinatória* deve grande parte do seu desenvolvimento aos jogos de sorte ou azar e, neste contexto, à necessidade de contar o número de possibilidades de ocorrência de certas configurações que correspondem a outras tantas jogadas. O estudo de tais contagens está na base dos métodos de enumeração que atraíram grandes matemáticos, como sejam, o italiano Niccollo Fontana (1500–1557), conhecido por Tartaglia, e os franceses Pierre de Fermat (1601–1665) e Blaise Pascal (1623–1662). A Análise Combinatória tem por objectivo o desenvolvimento de métodos que facilitem a contagem – de forma prática e indirecta – do número de ocorrências de certos subconjuntos definidos à custa de condições de agrupamento.

4.1. Arranjos com repetição

Dados n tipos de objectos, podemos formar diferentes configurações de k objectos, em certos casos assumindo que essas configurações podem conter mais do que um objecto do mesmo tipo. Duas configurações dizem-se distintas se contêm diferente número de objectos de determinado tipo ou se são determinadas por diferentes ordenações dos objectos que as constituem.

Dados n tipos diferentes de objectos, as configurações de k objectos que dependem da ordem e podem conter mais do que um objecto do mesmo tipo designam-se por *arranjos com repetição de n elementos k a k* . Nestes casos, duas configurações dizem-se distintas se existe pelo menos um tipo de objectos que ocorre mais vezes numa configuração do que na outra ou se a ordem de ocorrência dos diferentes objectos não é igual nas duas configurações. Por exemplo, supondo que dispomos de bolas pretas (p), brancas (b) e verdes (v), podemos obter sequências de $k = 5$ bolas, cada uma das quais corresponde a um arranjo. Por outro lado, podemos concluir que o arranjo (p, p, b, p, b) é diferente do arranjo (p, p, b, p, v) (dado que contém bolas diferentes) e ainda que este último, por sua vez, é diferente do arranjo (p, p, b, v, p) (uma vez que as bolas de diferentes tipos ocorrem segundo uma ordem distinta).

O número de arranjos com repetição de um conjunto de n elementos k a k denota-se por $A_n^{(k)}$ e, pelo princípio da multiplicação, é igual a

$$A_n^{(k)} = n^k. \quad (4.1)$$

Exemplo 4.1. Perguntando a seis pessoas, escolhidas aleatoriamente, o dia da semana do seu aniversário, quantas respostas distintas se podem obter, considerando que uma resposta é uma informação

relativa às seis pessoas?

Solução. Cada uma das seis pessoas pode ter nascido em qualquer dos sete dias da semana. Logo, cada resposta pode ser representada pela sequência de seis elementos $(D_1, D_2, D_3, D_4, D_5, D_6)$, onde D_i denota o dia da semana em que a i -ésima pessoa faz anos (com $i = 1, 2, \dots, 6$), pelo que D_i é um elemento do conjunto de sete elementos $\{\text{Do, Se, Te, Qu, Qi, Se, Sa}\}$. Uma vez que a repetição é possível (com efeito, duas pessoas podem ter nascido no mesmo dia da semana), cada sequência de 6 respostas corresponde a um arranjo com repetição do conjunto de 7 elementos 6 a 6. Assim, o número de respostas possíveis é igual a $A_7^{(6)} = 7^6 = 117.649$. \square

Observe-se que os arranjos com repetição foram anteriormente referidos nos Exemplos 3.5 e 3.9.

4.2. Arranjos e combinações simples

Se na definição de arranjo não considerarmos a hipótese de repetição de qualquer elemento dizemos que se trata de *arranjo simples* (ou *arranjo sem repetição* ou simplesmente *arranjo*). Aplicando o princípio da multiplicação generalizada, concluímos que o número de arranjos simples de n elementos k a k , denotado por $A_{n,k}$, é igual

$$A_{n,k} = (n)_k = n(n-1)\dots(n-k+1). \quad (4.2)$$

Em particular, os arranjos simples com $k = n$ designam-se por *permutações* (*permutações simples*). Como consequência, o número de permutações de n elementos vem dado por

$$P_n = n! = n(n-1)(n-2)\dots3\cdot2\cdot1, \quad (4.3)$$

convencionando-se que existe uma única permutação com 0 elementos e, consequentemente, que $0! = 1$.

O número $(n)_k$ é também conhecido como *coeficiente factorial* (*falling factorial* na terminologia inglesa). Casos particulares de arranjos simples foram apresentados nos Exemplos 3.6 e 3.7.

Exemplo 4.2. Vamos calcular o número de alinhamentos possíveis de doze escuteiros de tal modo que dois deles sejam sempre vizinhos um do outro.

Solução. Vamos começar por substituir os dois escuteiros (que vamos designar por gémeos) por uma única escuteira. Com esta nova equipa de escuteiros obtém-se $P_{11} = 11!$ alinhamentos possíveis. Para cada um destes alinhamentos, podemos substituir a escuteira pelos gémeos segundo $P_2 = 2!$ maneiras diferentes. Aplicando o princípio da multiplicação obtém-se um resultado final de $2 \cdot 11! = 79.833.600$ alinhamentos possíveis. \square

Dado um conjunto Y com n elementos, as escolhas de k elementos sem repetição e sem que a ordem segundo a qual os k elementos são escolhidos tenha qualquer importância (por outras palavras, as escolhas de subconjuntos de cardinalidade k), designam-se por *combinações simples* ou, simplesmente, *combinações* de n elementos k a k . O número destas combinações simples denota-se por $\binom{n}{k}$ e designa-se por *número binomial*.

Tendo em vista a determinação dos números binomiais, vamos considerar dois exemplos simples.

Exemplo 4.3. Supondo que se pretendem comprar 2 bilhetes da lotaria de entre 16 bilhetes disponíveis, vamos calcular o número de possibilidades para se efectuar uma tal compra.

Solução. Considere-se a lista de todos os pares ordenados de diferentes números de 1 até 16 (ou seja, arranjos simples de 2 elementos do conjunto $\{1, 2, \dots, 16\}$):

$$(1, 2), (1, 3), (1, 4), \dots, (1, 16), (2, 1), (2, 3), \dots, (16, 14), (16, 15).$$

Esta lista tem $(16)_2 = 16 \cdot 15$ elementos (comparar com a formula 4.2). Porém, dado que cada par de elementos aparece duas vezes (por exemplo $(1, 2)$ e $(2, 1)$), o resultado final é obtido dividindo-se o número de elementos da lista por 2, isto é,

$$\binom{16}{2} = \frac{16 \cdot 15}{2} = 120. \quad (4.4)$$

Alternativamente, para evitar as repetições na lista, podemos assumir que em cada par o primeiro elemento é menor do que o segundo. Então, temos 15 pares cujo primeiro elemento é 1, 14 pares cujo primeiro elemento é 2, etc. Como consequência,

$$\binom{16}{2} = 15 + 14 + \dots + 2 + 1 = 120. \quad \square$$

Podemos generalizar (4.4) escrevendo

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

Exemplo 4.4. Supondo que se pretendem comprar 3 bilhetes da lotaria de entre 16 bilhetes disponíveis, vamos calcular o número de possibilidades para uma tal compra.

Solução. Seguindo uma técnica semelhante à utilizada no exemplo anterior, vamos considerar a lista de todos os triplos de diferentes números de 1 até 16 (ou seja, os arranjos simples de 3 elementos do conjunto $\{1, 2, \dots, 16\}$). Esta lista tem $(16)_3 = 16 \cdot 15 \cdot 14 = 3.360$ elementos (comparar com a formula (4.2)). Porém, uma vez que cada triplo de elementos aparece $3! = 6$ vezes na lista (por exemplo $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$ e $(3, 2, 1)$), o resultado pretendido é igual a um sexto do número de elementos na lista, ou seja,

$$\binom{16}{3} = \frac{(16)_3}{3!} = 560.$$

Em alternativa, para evitar a repetição de triplos, podemos assumir que em cada triplo as componentes aparecem segundo a ordem crescente. Nesta condições, tendo em conta o Exemplo 4.3, obtém-se $\binom{15}{2}$ triplos começados com 1, $\binom{14}{2}$ triplos começados com 2, etc. Como consequência,

$$\binom{16}{3} = \binom{15}{2} + \binom{14}{2} + \binom{13}{2} + \dots + \binom{3}{2} + \binom{2}{2} = 560. \quad \square$$

Como generalização imediata dos Exemplos 4.3 e 4.4, temos o seguinte teorema.

Teorema 4.1. Se n e k são inteiros positivos tais que $1 \leq k \leq n$, então

$$\binom{n}{k} = \frac{A_{n,k}}{k!} = \frac{(n)_k}{k!} \quad (4.5)$$

e

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \dots + \binom{k-1}{k-1}. \quad (4.6)$$

Demonstração. Considerando que temos disponíveis n bilhetes da lotaria, dos quais pretendemos escolher apenas k , tendo em conta a fórmula (4.2), concluímos que o número de elementos da lista de todos os k -uplos cujas componentes são números distintos entre 1 e n , é igual ao número de arranjos de n elementos k a k , isto é, $(n)_k$. Porém, cada conjunto de elementos definido pelas componentes

dos k -uplos da lista, aparece $k!$ vezes (tendo em conta as ordenações possíveis de cada k -uplo). Como consequência, o número de combinações de n elementos k a k vem dado por

$$\binom{n}{k} = \frac{(n)_k}{k!}.$$

Em alternativa, novamente para evitar as referidas repetições, podemos assumir que em cada k -uplo os elementos aparecem segundo uma ordem crescente. Consequentemente, obtém-se $\binom{n-1}{k-1}$ k -uplos cuja primeira componente é igual a 1, $\binom{n-2}{k-1}$ k -uplos cuja primeira componente é igual a 2, etc. Logo,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \dots + \binom{k}{k-1} + \binom{k-1}{k-1} = \sum_{m=k}^n \binom{m-1}{k-1}.$$

□

Reformulando (4.5) obtém-se

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \quad (4.7)$$

Exemplo 4.5. Vamos calcular o número de caminhos mais curtos entre A e B na grelha de ordem $k \times n$ (compare com o Exemplo 3.3).

Solução. Sabemos que cada um dos caminhos mais curtos entre A e B corresponde a uma sequência binária de n uns e k zeros. O número destas sucessões é igual ao número de escolhas de n posições para os dígitos um (ou das k posições para os dígitos zeros) de entre $n+k$ posições. Este número é igual $\binom{n+k}{k} = \binom{n+k}{n}$. □

Exemplo 4.6. Suponha que são dadas n rectas no plano, sem que haja um par de rectas paralelas e sem que existam três rectas que se intersectem num único ponto. Vamos calcular o número total de pontos definidos pelas intersecções das rectas.

Solução. Uma vez que não existem três rectas que se intersectem num ponto, os pontos são determinados por pares de rectas e como não existem rectas paralelas, cada par de rectas determina um ponto dos definidos pelas intersecções das rectas. Como consequência, o número de pontos de intersecção das rectas é igual ao número de pares de rectas, isto é, é igual a $\binom{n}{2}$. □

Exemplo 4.7. Sabendo que uma classe tem 16 raparigas e 15 rapazes, vamos calcular o número de grupos de 5 alunos que podemos formar com pelo menos 3 rapazes.

Solução. Podemos considerar três tipos de grupos:

1. grupos com três rapazes;
2. grupos com quatro rapazes;
3. grupos com cinco rapazes.

Vamos proceder ao cálculo do número de grupos de cada um destes tipos.

1. Nos grupos do primeiro tipo, existem $\binom{15}{3}$ possibilidades para a escolha dos três rapazes e $\binom{16}{2}$ possibilidades de escolha das duas raparigas. Logo, de acordo com o princípio da multiplicação, podemos obter $\binom{15}{3}\binom{16}{2} = 54.600$ grupos do primeiro tipo.
2. Nos grupos do segundo tipo, existem $\binom{15}{4}$ possibilidades de escolha dos 4 rapazes e $\binom{16}{1}$ possibilidades de escolha da rapariga. Como consequência, aplicando novamente o princípio da multiplicação, podemos obter $\binom{15}{4}\binom{16}{1} = 21.840$ grupos do segundo tipo.

3. Finalmente, a ausência de raparigas nos grupos do terceiro tipo implica que se possam escolher apenas $\binom{15}{5} = 3.003$ grupos deste tipo.

Aplicando o princípio da adição, concluímos que, na sua totalidade, podemos formar

$$\binom{15}{3} \binom{16}{2} + \binom{15}{4} \binom{16}{1} + \binom{15}{5} = 79.443$$

grupos diferentes. \square

Exemplo 4.8. Num concurso sobre um torneio de ténis em que participam 10 jogadores, existem dois tipos de apostas. O primeiro tipo consiste em indicar os três primeiros jogadores do torneio pela respectiva ordem, e o segundo consiste em indicar o conjunto dos três jogadores melhor classificados (sem referir a sua ordem). Vamos calcular, para cada tipo, o número de apostas que é necessário fazer para termos a certeza que ganhamos.

Solução.

- No primeiro tipo, são necessárias todas as sequências de três jogadores pertencentes ao conjunto de participantes, cujo número é igual ao número de arranjos de 10 elementos 3 a 3, ou seja, são necessários $(10)_3 = 720$ apostas.
- No segundo tipo, precisamos de apostar em todos os conjuntos distintos de 3 jogadores pertencentes ao conjunto de participantes. Logo, neste caso, são necessárias $\binom{10}{3} = 120$ apostas. \square

Exemplo 4.9. Vamos determinar o número de soluções da equação

$$x_1 + x_2 + \dots + x_k = n,$$

onde x_i , para $i = 1, \dots, k$, são números inteiros positivos.

Solução. Colocando n bolas em linha, vamos dividi-las em k conjuntos não vazios (o i -ésimo conjunto corresponde à variável x_i). Estes conjuntos podem ser obtidos colocando $k - 1$ separadores entre eles, existindo $n - 1$ posições possíveis para os colocar. Como consequência, existem $\binom{n-1}{k-1}$ possibilidades de colocação dos separadores ou (equivalentemente) igual número de soluções para a equação em causa. Um outro método para determinar o número de soluções, consiste em definir as variáveis y_i , $y_i = x_i - 1$, $i = 1, 2, \dots, k$ e proceder à respectiva substituição de variáveis, obtendo-se a equação:

$$y_1 + y_2 + \dots + y_k = n - k$$

onde as variáveis y_i , para $i = 1, \dots, k$ tomam valores inteiros não negativos. Tendo em conta o Exemplo 3.4 sabemos que o número de soluções inteiras não negativas desta equação é igual ao número de sequências binárias com $n - k$ uns e $k - 1$ zeros. Por sua vez, o número destas sequências é igual ao número de escolhas de $k - 1$ posições para os zeros de entre as $(n - k) + (k - 1) = n - 1$ posições, ou seja, $\binom{n-1}{k-1}$. \square

Exemplo 4.10. Vamos calcular o número de rectângulos diferentes que podemos formar na grelha de ordem $n \times n$.

Solução. Primeiramente, deve observar-se que um rectângulo fica definido pelos dois pares de coeficientes que determinam dois vértices opostos, (x_1, y_1) e (x_2, y_2) , podendo admitir-se, sem perda de generalidade que $x_1 < x_2$ e $y_1 < y_2$. Uma vez que existem $\binom{n+1}{2}$ possibilidades de escolher os conjuntos $\{x_1, x_2\}$ e o mesmo número para os conjuntos $\{y_1, y_2\}$, aplicando o princípio da multiplicação, conclui-se que o número de rectângulos da grelha de ordem $n \times n$ é igual a $\binom{n+1}{2}^2$. \square

Exemplo 4.11. Vamos mostrar que o número de rectângulos que se podem representar na grelha $n \times n$ com pelo menos um dos seus lados no bordo direito ou no bordo inferior da grelha é igual a n^3 .

Solução. Os rectângulos que "tocam" o bordo direito e não tocam o bordo inferior da grelha são determinados pelos pares (compare com o Exemplo 4.10) (x_1, y_1) e (n, y_2) , onde x_1 tem n valores possíveis em $\{0, \dots, n-1\}$ e nem y_1 nem y_2 podem tomar o valor 0. Logo, uma vez que para o conjunto $\{y_1, y_2\}$ existem $\binom{n}{2}$ escolhas possíveis, por aplicação do princípio da multiplicação, o número de rectângulos que "tocam" o bordo direito mas não o bordo inferior da grelha é igual $n\binom{n}{2}$.

De modo semelhante se conclui que o número de rectângulos que "tocam" o bordo inferior e não tocam o bordo direito da grelha é igual $n\binom{n}{2}$.

Finalmente, o número de rectângulos que "tocam" ambos os bordos (direito e inferior) da grelha, são determinados pelos pares $(x_1, 0)$ e (n, y_1) , com $x_1 \in \{0, \dots, n-1\}$ e $y_1 \in \{1, \dots, n\}$ os quais podem ser escolhidos de n^2 modos distintos.

Consequentemente, a totalidade dos rectângulos vem dada por

$$n\binom{n}{2} + n\binom{n}{2} + n^2 = n^2 \left(\frac{n-1}{2} + \frac{n-1}{2} + 1 \right) = n^3.$$

Alternativamente, este número poderia ser obtido calculando o número de rectângulos que se podem representar na grelha $n \times n$ e subtraindo a esse número o número de rectângulos que se podem representar na grelha $(n-1) \times (n-1)$ (que corresponde à grelha obtida da grelha inicial, retirando o bordo direito e o bordo inferior) o qual, por sua vez, é igual a $\binom{n}{2}^2$. Desta forma, obtém-se o valor

$$\binom{n+1}{2}^2 - \binom{n}{2}^2 = n^3$$

que, naturalmente, coincide com o anterior. \square

Exemplo 4.12. Vamos calcular o número de funções sobrejectivas definidas no conjunto D com m elementos e com imagem no conjunto $R = \{y_1, \dots, y_n\}$.

Solução. Seja $X = \{f : D \rightarrow R\}$ o conjunto de todas as funções de D em R e, para $i = 1, 2, \dots, n$,

$$A_i = \{f \in X : y_i \notin f(D)\}.$$

Então o conjunto de todos as funções sobrejectivas de D em R coincide com o subconjunto de X constituído pelas funções que não pertencem a nenhum dos conjuntos A_1, A_2, \dots, A_n . Assim, é necessário calcular N_0 , de acordo com a fórmula (3.4). Antes porém, dado um subconjunto arbitrário de índices $I \subseteq \{1, \dots, n\}$, podemos concluir que

$$|\bigcap_{i \in I} A_i| = (n - |I|)^m$$

e, consequentemente, que

$$S_k^{(n)} = \binom{n}{k} (n - k)^m.$$

Logo, utilizando a fórmula (3.4), vem que

$$N_0 = \sum_{k=0}^n (-1)^k \binom{n}{k} (n - k)^m = \sum_{k=1}^n (-1)^{n-k} \binom{n}{k} k^m. \quad (4.8)$$

\square

4.3. Combinações e permutações com repetição

Considere-se, mais uma vez, o Exemplo 3.2. Se $Y = \{y_1, y_2, \dots, y_n\}$ é um conjunto de caixas, então cada colocação de k bolas iguais nas n caixas corresponde a uma das *combinações com repetição* de n caixas k a k . No Exemplo 3.2, no caso particular de $k = 7$, o agrupamento apresentado corresponde à colocação $[y_1, y_1, y_3, y_5, y_6, y_6, y_6]$. Note-se que esta notação não identifica nem uma sequência (uma vez que a ordem dos elementos é irrelevante) nem um conjunto (uma vez que aparecem elementos repetidos). Este objecto é designado, em muitas publicações, por conjunto com repetição, pseudoconjunto, colecção, multiconjunto, etc.

No caso do Exemplo 3.2 sabemos que o número de combinações com repetição de n elementos k a k é igual ao número de sequências binárias com k zeros e $n - 1$ uns, ou seja,

$$\binom{n+k-1}{k}.$$

Exemplo 4.13. Vamos calcular o número de possibilidades de colocação de 20 bolas iguais em cinco caixas, com pelo menos duas bolas em cada caixa.

Solução. A obrigatoriedade de colocação de pelo menos duas bolas em cada caixa implica que à partida se distribuam 10 bolas igualmente pelas cinco caixas, pelo que restam outras 10 bolas para distribuir arbitrariamente pelas caixas. Como consequência, o número de possibilidades de colocação de todas as bolas nas caixas (com a condicionante referida) é igual ao número de possibilidades de colocação de 10 bolas nas cinco caixas, o qual corresponde ao número de combinações com repetição de 5 caixas 10 a 10. Logo, o resultado final é

$$\binom{5+10-1}{10} = 1.001.$$

□

Exemplo 4.14. Vamos calcular o número de possibilidades de escolha de dez bolas de um número ilimitado de bolas vermelhas, azuis e verdes, de tal forma que

- (1) pelo menos cinco bolas são vermelhas;
- (2) no máximo cinco bolas são vermelhas.

Solução.

- (1) Note-se, primeiramente, que o número de possibilidades de escolha de dez bolas de um número ilimitado de bolas vermelhas, azuis e verdes, de tal forma que pelo menos cinco bolas são vermelhas, é igual ao número de possibilidades de atribuição de três cores a cinco bolas que é, precisamente, o número de possibilidades de colocação de cinco bolas em três caixas. Este número, por sua vez, é igual ao número de combinações com repetição de 3 caixas 5 a 5, ou seja,

$$\binom{3+5-1}{5} = \binom{7}{5} = 21.$$

- (2) O número de possibilidades de escolha de dez bolas de um número ilimitado de bolas vermelhas, azuis e verdes é igual ao número de combinações com repetição das 3 cores 10 a 10, ou seja,

$$\binom{3+10-1}{10} = \binom{12}{10} = 66.$$

Por outro lado, este número é também igual ao número de possibilidades de escolha de dez bolas de um número ilimitado de bolas vermelhas, azuis e verdes de tal forma que no máximo 5

bolas são vermelhas mais o número de possibilidades de escolha das dez bolas com pelo menos 6 bolas vermelhas. Tendo em conta que (utilizando uma argumentação idêntica à anterior) este último número é igual ao número de combinações com repetição de 3 cores 4 a 4, ou seja, $\binom{3+4-1}{4} = \binom{6}{4} = 15$, podemos concluir que o resultado pretendido é igual a $66 - 15 = 51$. \square

Vamos iniciar o estudo das permutações com repetição com um exemplo.

Exemplo 4.15. Admitindo que dispomos dos algarismos: 4, 4, 4, 4, 3, 3, 3, 2, 2, 1, vamos calcular o número de números de dez dígitos que podemos explicitar utilizando estes (e apenas estes) algarismos.

Solução. Assumindo que cada um dos dez algarismos tem uma cor distinta (que é independente do seu valor), é possível obter $10!$ sequências cromáticas. Por outro lado, tendo em conta que em qualquer das sequências cromáticas existem quatro dígitos 4, três dígitos 3, dois dígitos 2 e um díxito 1, podemos concluir que para qualquer dos números que lhe corresponde existem $4! \cdot 3! \cdot 2!$ sequências cromáticas distintas que o representam. Como consequência, o número de números que se podem explicitar utilizando estes (e apenas estes) dez dígitos é igual a

$$\frac{10!}{4! 3! 2!} = 12.600.$$

\square

Este exemplo ilustra o conceito de *permutação com repetição*, a qual também pode ser vista como uma permutação dos elementos de um pseudoconjunto (com elementos repetidos).

O Exemplo 4.15 pode resolver-se com recurso a outro método. Com efeito, a escolha de cada um dos números representáveis pelos dez algarismos pode fazer-se pela seguinte sequência de procedimentos:

1. Escolher quatro posições para os dígitos 4, de entre as dez posições possíveis, para o que existem $\binom{10}{4}$ possibilidades;
2. Escolher três posições para os dígitos 3, de entre as seis posições que restam após o passo anterior, para o que existem $\binom{6}{3}$ possibilidades;
3. Escolher duas posições para os dígitos 2, de entre as três posições que restam após os passos anteriores, para o que existem $\binom{3}{2}$ possibilidades;
4. Colocar o díxito 1 na única posição que resta (ou seja, nas $\binom{1}{1}$ posições que restam).

Como consequência, por aplicação do princípio da multiplicação generalizada, obtém-se

$$\binom{10}{4} \binom{6}{3} \binom{3}{2} \binom{1}{1} = 12.600$$

de números distintos.

Note-se que neste caso, partimos um conjunto de dez elementos (as posições dos dígitos) em quatro subconjuntos, sendo um deles de cardinalidade quatro (relativo às posições do algarismo 4), outro de cardinalidade três (relativo às posições do algarismo 3), outro de cardinalidade dois (relativo às posições do algarismo 2) e finalmente um subconjunto de cardinalidade um (relativo à posição do algarismo 1). O teorema a seguir, que recorre ao conceito de número multinomial, que é um número da forma

$$\binom{n}{n_1, \dots, n_r} = \frac{n!}{n_1! n_2! \dots n_r!},$$

onde $\sum_{j=1}^r n_j = n$, generaliza a metodologia anterior.

Teorema 4.2 (Números multinomiais). *Dado um conjunto finito A de cardinalidade n existem*

$$\binom{n}{n_1, \dots, n_r} = \frac{n!}{n_1! n_2! \dots n_r!}$$

possibilidades de partir A em r subconjuntos A_1, A_2, \dots, A_r , com cardinalidade n_1, n_2, \dots, n_r , respectivamente.

Demonastração. Podemos começar pela escolha dos elementos do subconjunto A_1 , para o que existem $\binom{n}{n_1}$ possibilidades. Seguidamente, podemos escolher os elementos do subconjunto A_2 de entre os $n - n_1$ elementos que restam, para o que existem $\binom{n-n_1}{n_2}$ possibilidades, etc. Como consequência, aplicando o princípio da multiplicação generalizada, obtém-se

$$\binom{n}{n_1} \binom{n-n_1}{n_2} \binom{n-n_1-n_2}{n_3} \dots \binom{n-n_1-n_2-\dots-n_{r-1}}{n_r} = \frac{n!}{n_1! n_2! \dots n_r!}$$

possibilidades para a partição de A em r subconjuntos de cardinalidade n_1, n_2, \dots, n_r , respectivamente. \square

Note-se que, no caso particular de $r = 2$, $n_1 + n_2 = n$ e o número multinomial correspondente é igual ao número binomial de combinações de n elementos n_1 a n_1 que, por sua vez, é igual ao número de combinações de n elementos n_2 a n_2 (comparar com (4.7)). Com efeito,

$$\binom{n}{n_1, n_2} = \frac{n!}{n_1! n_2!} = \frac{n!}{n_1!(n - n_1)!} = \binom{n}{n_1}.$$

Seguem-se mais alguns exemplos de aplicação.

Exemplo 4.16. *Vamos calcular o número de possibilidades de distribuição das cartas por quatro jogadores de uma partida de bridge.*

Solução. É claro que para um jogador de bridge, o importante é saber quais as suas cartas e quais as cartas que cada um dos restantes três jogadores tem, independentemente da ordem segundo a qual as cartas foram distribuídas. Porém, tendo em conta que o baralho contém 52 cartas, sabemos que existem $52!$ possíveis diferentes ordenações para a distribuição das cartas pelos jogadores. Assim, a distribuição das cartas consiste na partição das 52 cartas em 4 subconjuntos de 13 cartas cada. Logo, o número de possibilidades de distribuição das cartas pelos quatro jogadores é igual a

$$\begin{aligned} \binom{52}{13, 13, 13, 13} &= \frac{52!}{13! \cdot 13! \cdot 13! \cdot 13!} \\ &= 53\,644\,737\,765\,488\,792\,839\,237\,440\,000. \end{aligned} \quad \square$$

Exemplo 4.17. *Suponha que durante uma investigação se chegou à conclusão que se deve identificar uma pessoa que tem um telefone cujo número (com nove dígitos) contém exactamente os dígitos (segundo uma ordem desconhecida) que constam no número*

232 757 223.

Supondo ainda que uma vez contactada pelo telefone a pessoa em causa fica identificada e que não existe qualquer limitação para o posicionamento dos dígitos, vamos determinar o número máximo de números de telefone que devem ser testados para se garantir a respectiva identificação.

Solução. Como apenas estão disponíveis quatro dígitos 2, dois dígitos 3, dois dígitos 7 e um dígito 5, cada número a testar vai corresponder a uma partição das 9 posições possíveis para os dígitos nos subconjuntos A_j , para cada dígito $j \in \{2, 3, 5, 7\}$, ou seja, nos subconjuntos A_2 com cardinalidade

quatro, A_3 com cardinalidade dois, A_5 com cardinalidade um e A_7 com cardinalidade dois. Logo, o número máximo de números a testar é igual ao número multinomial

$$\binom{9}{4, 2, 2, 1} = \frac{9!}{4! \cdot 2! \cdot 2! \cdot 1!} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5}{2 \cdot 2} = 3.780.$$

□

Exemplo 4.18. Vamos calcular o número D_n de permutações de uma sequência de n elementos sem pontos fixos relativamente a essa sequência (as quais são conhecidas como desencontros de comprimento n).

Solução. Sem perda de generalidade, vamos assumir que a sequência é $\pi = (1, 2, \dots, n)$. É claro que existem $n!$ permutações destes elementos das quais (tendo em vista o cálculo pretendido) se devem retirar as permutações σ com pontos fixos em relação π (ou seja, tais que $\sigma(i) = i = \pi(i)$). Este último número pode ser determinado com recurso ao princípio da inclusão-exclusão.

Vamos designar por "propriedade i ", com $1 \leq i \leq n$, a verificação da condição de i ser ponto fixo de uma permutação σ (isto é, para a qual $\sigma(i) = i$) e, dados $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$, vamos denotar por $N(i_1, \dots, i_k)$ o número de permutações com pelo menos os k pontos fixos i_1, i_2, \dots, i_k . Assim, vem que

$$N(i_1, \dots, i_k) = (n - k)!$$

e, por aplicação do princípio de inclusão-exclusão, obtém-se

$$\begin{aligned} D_n &= n! - N(1) - N(2) - \dots - N(n) + N(1, 2) + \dots + N(n-1, n) \\ &\quad - N(1, 2, 3) - \dots - N(n-2, n-1, n) + \dots + (-1)^n N(1, 2, \dots, n) \\ &= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \dots + (-1)^n \binom{n}{n}(n-n)! \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \dots + (-1)^n \frac{n!}{n!} = n! \left(\frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right) \\ &= n! \sum_{k=2}^n (-1)^k \frac{1}{k!}. \end{aligned}$$

Alternativamente, este problema pode resolver-se com utilização da fórmula (3.4). Com efeito, seja X o conjunto de todas as permutações dos elementos do conjunto $\{1, 2, \dots, n\}$, isto é,

$$X = \{f : [n] \rightarrow [n] : f \text{ é uma bijecção}\}$$

e, para $i = 1, 2, \dots, n$, seja

$$A_i = \{f \in X : f(i) = i\}.$$

Dado que

$$S_k^{(n)} = \binom{n}{k}(n-k)! = \frac{n!}{k!},$$

vem que

$$D_n = n! + \sum_{k=1}^n (-1)^k S_k^{(n)} = n! \sum_{k=0}^n (-1)^k \frac{1}{k!}.$$

Note-se que para n suficientemente grande, $\sum_{k=0}^n (-1)^k \frac{1}{k!}$ tem um valor muito próximo de e^{-1} (ver Tabela 4.1). □

n	D_n	$D_n/n!$
1	0	0,0000000000
2	1	0,5000000000
3	2	0,3333333333
4	9	0,3750000000
5	44	0,3666666667
6	265	0,3680555556
7	1 854	0,3678571429
8	14 833	0,3678819444
9	133 496	0,3678791887
10	1 334 961	0,3678794643

Tabela 4.1: Valores de D_n e de $D_n/n!$ (observe-se que $e^{-1} = 0,3678794411\dots$).

4.4. Permutações

Na Secção 4.2 concluímos que as permutações de n elementos são casos particulares de arranjos simples de n elementos k a k com $k = n$ e que o número de permutações dos elementos de um conjunto com cardinalidade n é igual $n!$. Sem perda de generalidade, nesta secção, vamos centrar o estudo das permutações no conjunto das permutações de elementos do conjunto $[n] = \{1, 2, \dots, n\}$, o qual se denota por S_n .

É claro que cada permutação π dos elementos do conjunto $[n]$ pode ser interpretada como uma bijecção $\pi : [n] \rightarrow [n]$. Neste caso, usualmente, escreve-se π_i em vez de $\pi(i)$. Por outro lado, é muito comum denotar uma permutação π por

$$\pi = \begin{pmatrix} a & b & \cdots & z \\ \pi_a & \pi_b & \cdots & \pi_z \end{pmatrix}, \quad (4.9)$$

onde na primeira linha aparecem os elementos de $[n]$, segundo uma ordem arbitrária, e na segunda aparecem as correspondentes imagens por π (note-se que $\pi(a) = \pi_a$, $\pi(b) = \pi_b$, ..., $\pi(z) = \pi_z$). No caso particular em que os elementos de $[n]$ aparecem na primeira linha de (4.9) segundo a ordem natural, ou seja,

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_n \end{pmatrix}, \quad (4.10)$$

esta permutação pode escrever-se na forma mais compacta $\pi = (\pi_1 \ \pi_2 \ \dots \ \pi_n)$ ou, quando no contexto não há lugar a qualquer dúvida em relação à permutação em causa, simplesmente $(\pi_1 \ \pi_2 \ \dots \ \pi_n)$.

Definição 4.1 (Permutação identidade). *Para cada inteiro $n \geq 1$ a permutação $\pi \in S_n$ tal que $\forall_{i \in [n]} \pi(i) = i$ designa-se por permutação identidade e denota-se por π_{id} .*

Tendo em conta as observações anteriores, podemos ainda representar a permutação identidade por $\pi_{id} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ ou $\pi_{id} = (1 \ 2 \ \dots \ n)$.

Uma vez que as permutações são bijecções, a composição de permutações define-se em coerência com a composição de bijecções. Como consequência, se $\pi, \rho \in S_n$ então $\pi \circ \rho \in S_n$ e $\rho \circ \pi \in S_n$.

Exemplo 4.19. Vamos determinar as composições $\pi \circ \rho$ e $\rho \circ \pi$ das permutações $\pi = (3 \ 4 \ 1 \ 5 \ 2)$ e $\rho = (4 \ 3 \ 2 \ 5 \ 1)$ (do conjunto $\{1, 2, 3, 4, 5\}$).

Solução. Uma vez que $\pi \circ \rho(1) = \pi(\rho(1)) = \pi(4) = 5$, $\pi \circ \rho(2) = \pi(\rho(2)) = \pi(3) = 1$, etc., vem que $\pi \circ \rho = (5 \ 1 \ 4 \ 2 \ 3)$. Analogamente $\rho \circ \pi(1) = \rho(\pi(1)) = \rho(3) = 2$, $\rho \circ \pi(2) = \rho(\pi(2)) = \rho(4) = 5$, etc., logo $\rho \circ \pi = (2 \ 5 \ 4 \ 1 \ 3)$. \square

É claro que dada uma permutação $\pi = (\pi_1 \ \pi_2 \ \dots \ \pi_n)$, existe a respectiva permutação inversa π^{-1} , a qual podemos determinar trocando as linhas da notação (4.9), isto é,

$$\pi^{-1} = \begin{pmatrix} \pi_1 & \pi_2 & \cdots & \pi_n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Observe-se que $\forall_{i \in \{1, \dots, n\}} \pi^{-1} \circ \pi(i) = \pi^{-1}(\pi(i)) = \pi^{-1}(\pi_i) = i$.

Por outro lado, para cada permutação $\pi \in S_n$ existe uma única partição do conjunto $[n]$ em subconjuntos não vazios X_1, \dots, X_k tal que

$$\forall_{j \in \{1, \dots, k\}} \forall_{x \in \{1, \dots, n\}} x \in X_j \Rightarrow \pi(x) \in X_j$$

e nenhum X_j se pode partir em dois subconjuntos não vazios com a mesma propriedade. Uma tal partição é única para cada permutação π e designa-se por *partição cíclica* de π .

Exemplo 4.20. Vamos determinar a partição cíclica da permutação

$$\pi = (2 \ 8 \ 1 \ 3 \ 9 \ 6 \ 5 \ 4 \ 7).$$

Solução. Uma vez que $\pi(1) = 2$ os elementos 1 e 2 pertencem ao mesmo subconjunto da partição. Analogamente, uma vez que $\pi(2) = 8$, $\pi(8) = 4$, $\pi(4) = 3$, $\pi(3) = 1$, concluímos que os elementos 1, 2, 3, 4 e 8 estão contidos no mesmo subconjunto da partição. Por outro lado, dado que $\pi(5) = 9$, $\pi(9) = 7$ e $\pi(7) = 5$, concluímos que 5, 7 e 9 ficam noutro subconjunto. Finalmente, $\pi(6) = 6$ implica que o elemento 6 constitui um subconjunto singular da partição cíclica de π . Logo, a partição cíclica de π tem a forma $\{\{1, 2, 3, 4, 8\}, \{5, 7, 9\}, \{6\}\}$. \square

Dado um subconjunto $\{x_1, \dots, x_s\}$ da partição cíclica de uma permutação π , podemos ordenar os respectivos elementos, apresentando-os de acordo com a ordenação definida simbolicamente por $[x_{i_1}, \dots, x_{i_s}]$, de tal forma que $\pi(x_{i_1}) = x_{i_2}$, $\pi(x_{i_2}) = x_{i_3}, \dots, \pi(x_{i_{s-1}}) = x_{i_s}$, $\pi(x_{i_s}) = x_{i_1}$. Por exemplo, os elementos do subconjunto $\{1, 2, 3, 4, 8\}$ da partição cíclica do Exemplo 4.20 podem apresentar-se segundo a ordenação definida por $[1, 2, 8, 4, 3]$. Note-se que a representação desta ordenação não é única, dependendo da escolha do primeiro elemento. Assim, no exemplo que estamos a analisar, a ordenação $[1, 2, 8, 4, 3]$ é idêntica a qualquer das ordenações $[2, 8, 4, 3, 1]$, $[8, 4, 3, 1, 2]$, $[4, 3, 1, 2, 8]$ e $[3, 1, 2, 8, 4]$. Cada uma das ordenações associadas a um subconjunto da partição cíclica de uma permutação π , $X = [x_{i_1}, \dots, x_{i_s}]$, designa-se por *ciclo da permutação* π e interpreta-se como sendo uma permutação π_X tal que

$$\pi_X(x) = \begin{cases} x, & \text{se } x \notin X, \\ x_{i_{k+1}}, & \text{se } x = x_{i_k}, \text{ com } k \in \{1, \dots, s-1\}, \\ x_{i_1}, & \text{se } x = x_{i_s}. \end{cases}$$

Por sua vez, o número de elementos do ciclo X designa-se por *comprimento do ciclo*. Observe-se que se o comprimento de um ciclo X é igual 1, então a permutação π_X é a permutação identidade.

Exemplo 4.21. Seja $\pi \in S_n$ e sejam X_1, \dots, X_k os subconjuntos de $[n]$ da correspondente partição cíclica. Vamos demonstrar que

$$\pi = \pi_{X_1} \circ \pi_{X_2} \circ \cdots \circ \pi_{X_k}. \quad (4.11)$$

Solução. Se $x \in \{1, \dots, n\}$ então existe um único j tal que $x \in X_j$ (e também $\pi_x \in X_j$). Por definição,

$$\forall_{i \in [k] \setminus \{j\}} \pi_{X_i}(x) = x \wedge \pi_{X_j}(x) = \pi_x$$

o que implica $\pi_{X_1} \circ \pi_{X_2} \circ \cdots \circ \pi_{X_k}(x) = \pi_{X_j}(x) = \pi(x)$. \square

Dada uma permutação $\pi \in S_n$, a factorização (4.11), obtida tal como no Exemplo 4.21, designa-se por *decomposição de π num produto de ciclos*. Deve observar-se que uma decomposição de uma permutação num produto de ciclos goza das seguintes propriedades:

1. Por definição de partição cíclica, a decomposição de uma permutação num produto de ciclos não depende da ordem com que são considerados os diversos ciclos.
2. Uma vez que para cada ciclo X de comprimento 1 a permutação π_X é a permutação identidade, na decomposição num produto de ciclos podemos omitir todos os ciclos de comprimento 1.
3. A decomposição num produto de ciclos é única a menos da ordem dos ciclos e da representação de cada ciclo.

Logo, considerando novamente a permutação π do Exemplo 4.20, podemos representá-la na forma cíclica $\pi = [1, 2, 8, 4, 3] \circ [5, 9, 7] \circ [6]$. Uma vez que, por convenção, usualmente, se omitem os símbolos \circ e os ciclos de comprimento 1, a decomposição de π num produto de ciclos pode apresentar a forma

$$\pi = [1, 2, 8, 4, 3][5, 9, 7].$$

De modo equivalente, também se pode escrever $\pi = [5, 9, 7][1, 2, 8, 4, 3]$, $\pi = [2, 8, 4, 3, 1][5, 9, 7]$, etc.

Se a decomposição de uma permutação $\pi \in S_n$ num produto de ciclos contém λ_i ciclos de comprimento i , para $i = 1, \dots, n$, então diz-se que a permutação é do tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$. É claro, que $\sum_{i=1}^n i\lambda_i = n$. Com esta notação, em geral, omitem-se todos os símbolos da forma i^{λ_i} , com $\lambda_i = 0$. Logo, podemos concluir que a permutação π do Exemplo 4.20 é do tipo $1^1 3^1 5^1$.

Exemplo 4.22. Vamos calcular o número de permutações do tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$.

Solução. Uma representação da permutação π de tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ designa-se por *normalizada* se

$$\pi = [x_1^1, x_2^1, \dots, x_{n_1}^1] \cdots [x_1^k, x_2^k, \dots, x_{n_k}^k], \quad (4.12)$$

onde os ciclos aparecem por ordem não decrescente dos seus comprimentos, ou seja, $n_1 \leq \dots \leq n_k$. Existem $n!$ possíveis ordenações dos elementos da representação normalizada (4.12), alguns dos quais representam a mesma permutação. Com efeito, cada ciclo de comprimento i pode representar-se de i modos equivalentes (dependendo da escolha do primeiro elemento), pelo que existem i^{λ_i} representações para os ciclos de comprimento i . Adicionalmente, os blocos que constituem os ciclos de comprimento i podem ser ordenados de $\lambda_i!$ maneiras distintas. Como consequência, cada permutação do tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ admite $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} \lambda_1! \lambda_2! \dots \lambda_n!$ representações normalizadas, donde podemos concluir que existem¹

$$\frac{n!}{1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} \lambda_1! \lambda_2! \dots \lambda_n!} \quad (4.13)$$

permutações do tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$. □

Definição 4.2 (Transposição). Uma permutação $\tau \in S_n$ diz-se uma transposição se é um ciclo de comprimento dois. Em particular, os ciclos com dois elementos sucessivos, ou seja, tais que $\tau = [i, i+1]$, para $i \in \{1, \dots, n-1\}$, são transposições que se designam por transposições simples.

Observe-se que cada transposição τ é igual à sua inversa, isto é, $\tau^{-1} = \tau$ ou de modo equivalente $\tau \circ \tau = \pi_{id}$. Mais geralmente, cada permutação π tal que $\pi \circ \pi = \pi_{id}$ diz-se uma *involução*, logo, cada transposição é uma involução. Por outro lado, sendo $\pi = (\pi_1 \dots \pi_n) \in S_n$ uma permutação, se $\tau = [i, i+1] \in S_n$ então

$$\pi \circ \tau = (\pi_1 \pi_2 \dots \pi_{i-1} \pi_{i+1} \pi_i \pi_{i+2} \pi_{i+3} \dots \pi_n). \quad (4.14)$$

¹A fórmula (4.13) para o número das permutações do tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ é conhecida como fórmula de Cauchy.

Definição 4.3 (Inversão). Dada a permutação $\pi = (x_1, x_2, \dots, x_n) \in S_n$, o par (x_i, x_j) , com $i < j$, designa-se por inversão de π se $x_i > x_j$. O número de todas as inversões da permutação π denota-se por $I(\pi)$.

Exemplo 4.23. Vamos demonstrar que cada permutação $\pi \in S_n$ se pode representar como produto (composição) de $I(\pi)$ transposições.

Solução. Observe-se que, considerando a transposição simples $\tau = [i, i + 1] \in S_n$,

$$I(\pi \circ \tau) = \begin{cases} I(\pi) + 1, & \text{se } \pi_i < \pi_{i+1}, \\ I(\pi) - 1, & \text{se } \pi_i > \pi_{i+1}. \end{cases} \quad (4.15)$$

Logo, escolhendo i tal que $\pi_i > \pi_{i+1}$ (i existe se $\pi \neq \pi_{id}$ ou, de modo equivalente, se $I(\pi) > 0$) e $\tau_1 = [i, i + 1]$ vem que $I(\pi \circ \tau_1) = I(\pi) - 1$. Seguidamente, escolhendo $\tau_2 = [j, j + 1]$ de tal modo que $\pi \circ \tau_1(j) > \pi \circ \tau_1(j + 1)$, vem que $I(\pi \circ \tau_1 \circ \tau_2) = I(\pi) - 2$, etc. Finalmente, obtém-se $I(\pi \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_{I(\pi)}) = I(\pi) - I(\pi) = 0$ o que implica $\pi \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_{I(\pi)} = \pi_{id}$. Uma vez que $\tau_i^{-1} = \tau_i$, conclui-se que

$$\pi = \tau_{I(\pi)} \circ \tau_{I(\pi)-1} \circ \dots \circ \tau_2 \circ \tau_1.$$

Esta representação designa-se por *decomposição da permutação π num produto de transposições*. \square

Definição 4.4 (Sinal de uma permutação). Dada uma permutação $\pi \in S_n$, o número $(-1)^{I(\pi)}$ designa-se por sinal da permutação π e denota-se por $\text{sgn}(\pi)$.

Uma vez que $I(\pi_{id}) = 0$, deve observar-se que $\text{sgn}(\pi_{id}) = 1$ e, para cada transposição τ , $I(\tau) = 1$ implica $\text{sgn}(\tau) = -1$.

Exemplo 4.24. Vamos demonstrar as seguintes propriedades de sinal duma permutação:

1. se $\pi, \rho \in S_n$ então $\text{sgn}(\pi \circ \rho) = \text{sgn}(\pi) \text{sgn}(\rho)$;
2. se uma permutação π é um ciclo de comprimento k então $\text{sgn}(\pi) = (-1)^{k-1}$;
3. se uma permutação π é do tipo $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ então

$$\text{sgn}(\pi) = (-1)^{\lambda_2 + \lambda_4 + \lambda_6 + \dots}. \quad (4.16)$$

A fórmula (4.16) pode ser utilizada para definir o sinal de uma permutação de elementos de um conjunto X onde o conceito de inversão não faça sentido.

Solução.

1. Utilizando a decomposição das permutações π e ρ numa composição de transposições, vem que $\rho = \tau_1 \circ \dots \circ \tau_{I(\rho)}$, $\pi = \tau'_1 \circ \dots \circ \tau'_{I(\pi)}$ e, como consequência,

$$\pi \circ \rho = \tau'_1 \circ \dots \circ \tau'_{I(\pi)} \circ \tau_1 \circ \dots \circ \tau_{I(\rho)}, \quad (4.17)$$

ou seja, $\pi \circ \rho$ pode representar-se como composição de $I(\pi) + I(\rho)$ transposições. Note-se que a fórmula (4.15) implica que a composição das k transposições $\rho_1 \circ \dots \circ \rho_k$ tenha sinal -1 , para $k = 1$, sinal 1 , para $k = 2$, sinal -1 , para $k = 3$, etc. Como consequência, podemos concluir que a composição de $I(\pi) + I(\rho)$ transposições tem sinal $(-1)^{I(\pi)+I(\rho)} = (-1)^{I(\pi)}(-1)^{I(\rho)} = \text{sgn}(\pi) \text{sgn}(\rho)$. Porém, não se sabendo se a representação (4.17) é composição do menor número possível de transposições, embora os números $I(\pi \circ \rho)$ e $I(\pi) + I(\rho)$ tenham a mesma paridade, não são necessariamente iguais.

2. Resta provar que um ciclo $[x_1, \dots, x_k]$ se pode representar como composição de $k - 1$ transposições. Assim, vamos demonstrar a igualdade

$$[x_1, \dots, x_k] = [x_1, x_2][x_2, x_3] \cdots [x_{k-1}, x_k].$$

Sendo $i \in \{1, \dots, n\}$ vem que:

- se $i \notin \{x_1, \dots, x_k\}$, então $[x_1, \dots, x_k](i) = i$ e $[x_1, x_2] \circ [x_2, x_3] \circ \cdots \circ [x_{k-1}, x_k](i) = i$;
- se $i = x_k$ então $[x_1, \dots, x_k](i) = x_1$ e $[x_1, x_2] \circ \cdots \circ [x_{k-1}, x_k](i) = [x_1, x_2] \circ \cdots \circ [x_{k-2}, x_{k-1}](x_{k-1}) = [x_1, x_2] \circ \cdots \circ [x_{k-3}, x_{k-2}](x_{k-2}) = \cdots = [x_1, x_2](x_2) = x_1$;
- se $i = x_j$ com $j \in \{1, \dots, k-1\}$, então $[x_1, \dots, x_k](i) = x_{j+1}$ e $[x_1, x_2] \circ \cdots \circ [x_{k-1}, x_k](i) = [x_1, x_2] \circ \cdots \circ [x_j, x_{j+1}](x_j) = [x_1, x_2] \circ \cdots \circ [x_{j-1}, x_j](x_{j+1}) = x_{j+1}$.

Logo, $\forall j \in \{1, \dots, n\} [x_1, \dots, x_k](j) = [x_1, x_2][x_2, x_3] \cdots [x_{k-1}, x_k](j)$.

3. Esta propriedade é consequência directa de pontos 1 e 2 e da decomposição de uma permutação em ciclos.

□

Definição 4.5 (Paridade de uma permutação). A permutação $\pi \in S_n$ diz-se par se $\text{sgn}(\pi) = 1$ e diz-se ímpar no caso contrário.

Denotando o conjunto das permutações pares do conjunto $[n]$ por P_n , ou seja, $P_n = \{\pi \in S_n : \text{sgn}(\pi) = 1\}$, pode concluir-se que se $\pi, \rho \in P_n$ então $\pi \circ \rho \in P_n$ e $\pi^{-1} \in P_n$.

Exemplo 4.25. Vamos demonstrar que $|P_n| = \frac{1}{2}n!$.

Solução. Se $\pi \in P_n$ então $\pi \circ [1, 2]$ é ímpar e se $\rho \in S_n \setminus P_n$ então $\rho \circ [1, 2]$ é par. Por outro lado, se $\pi, \rho \in S_n$ e $\pi \neq \rho$ então $\pi \circ [1, 2] \neq \rho \circ [1, 2]$. Como consequência, a função $\Phi : P_n \rightarrow S_n \setminus P_n$ tal que $\Phi(\pi) = \pi \circ [1, 2]$ é uma bijecção. Logo, pela princípio da bijecção, $|P_n| = |S_n \setminus P_n| = \frac{1}{2}n!$. □

4.5. Identidades combinatórias

Considerando o desenvolvimento de $(1+x)^n$, ou seja, o desenvolvimento do produto de n factores

$$(1+x)(1+x) \cdots (1+x),$$

obtém-se um polinómio em x de grau n onde, para $0 \leq k \leq n$, o coeficiente de x^k é $\binom{n}{k}$. Com efeito, no desenvolvimento do produto $(1+x)(1+x) \cdots (1+x)$, o número de parcelas da forma $x^k 1^{n-k}$, com $k \in \{0, 1, \dots, n\}$, é igual ao número de possibilidades de escolher x em k dos n factores e este número é igual a $\binom{n}{k}$. Como consequência, vem que

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k. \quad (4.18)$$

Em particular, para $x = 1$, obtém-se a equação

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}, \quad (4.19)$$

a qual também se pode concluir, tendo em conta que o número de subconjuntos de um conjunto de cardinalidade n é igual a 2^n , mas também é igual à soma dos números de subconjuntos de cardinalidade k , $\binom{n}{k}$, para $k = 0, 1, \dots, n$.

O teorema a seguir generaliza a fórmula (4.18).

Teorema 4.3 (Fórmula binomial de Newton). *Se a e b são dois números reais e n é um número inteiro positivo, então*

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}. \quad (4.20)$$

Esta fórmula é conhecida por *fórmula binomial de Newton* ou *fórmula do binómio de Newton*. A fórmula binomial de Newton é um caso particular da fórmula multinomial.

Teorema 4.4 (Fórmula multinomial). *Se a_1, a_2, \dots, a_r são números reais e n é um número inteiro positivo, então*

$$(a_1 + a_2 + \dots + a_r)^n = \sum_{\substack{t_1, \dots, t_r \in \mathbb{N} \\ t_1 + t_2 + \dots + t_r = n}} \binom{n}{t_1, \dots, t_r} a_1^{t_1} a_2^{t_2} \dots a_r^{t_r}.$$

Demonstração. Desenvolvendo o produto de n factores

$$(a_1 + a_2 + \dots + a_r)(a_1 + a_2 + \dots + a_r) \dots (a_1 + a_2 + \dots + a_r)$$

obtém-se termos da forma $a_1^{t_1} a_2^{t_2} \dots a_r^{t_r}$, com $t_1 + t_2 + \dots + t_r = n$, os quais correspondem à escolha de a_1 em t_1 dos factores, à escolha de a_2 em t_2 dos restantes factores e assim sucessivamente. Nestas condições, pela definição de número multinomial, concluímos que existem $\binom{n}{t_1, t_2, \dots, t_r}$ termos da forma $a_1^{t_1} a_2^{t_2} \dots a_r^{t_r}$. \square

Seguem-se alguns exemplos de identidades que demonstraremos com argumentos combinatórios.

Exemplo 4.26. *Dados os números inteiros positivos k e n tais que $1 \leq k \leq n$, vamos mostrar que*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \quad (4.21)$$

Solução. Vamos partir o conjunto de todos os caminhos mais curtos entre A e B (ver Figura 4.1) no subconjunto dos caminhos mais curtos que contêm B_1 e no subconjunto dos caminhos mais curtos que contêm B_2 (no primeiro caso chega-se a B percorrendo em último lugar o segmento horizontal situado o mais acima e mais à direita possível, e no segundo caso chega-se a B percorrendo em último lugar o segmento vertical situado o mais acima e mais à direita possível).

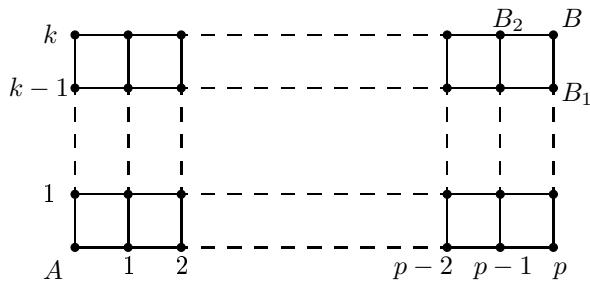


Figura 4.1: Partição do conjunto dos caminhos mais curtos entre A e B .

É claro que estes dois subconjuntos formam uma partição do conjunto de todos os caminhos mais curtos entre A e B . Por outro lado, o número de caminhos do primeiro tipo é $\binom{p+k-1}{k-1}$ (compare com o Exemplo 4.5) e o número de caminhos do segundo tipo é igual a $\binom{p+k-1}{k}$. Por sua vez, o número de caminhos de A para B é igual a $\binom{p+k}{k}$. Como consequência, por aplicação do princípio da adição, fazendo $n = p + k$, obtém-se a igualdade (4.21). \square

Tendo em conta que $\forall_{n,k \in \mathbb{N}} \binom{n}{n+k} = 0$, $\binom{n}{0} = \binom{n}{n} = 1$ e convencionando que $\binom{0}{0} = 1$, a igualdade (4.21) estabelece um método recursivo para a determinação dos números binomiais. Usualmente, este procedimento de cálculo representa-se na forma do triângulo a seguir indicado, conhecido por *triângulo de Pascal*² (ver Figura 4.2), no qual a j -ésima entrada (contada da esquerda para a direita entre 0 e i) da i -esima linha (contada de cima para baixo a partir de 0) vem dada por

$$\binom{i}{j} = \binom{i-1}{j-1} + \binom{i-1}{j},$$

para $i > 2$ e $0 < j < i$.

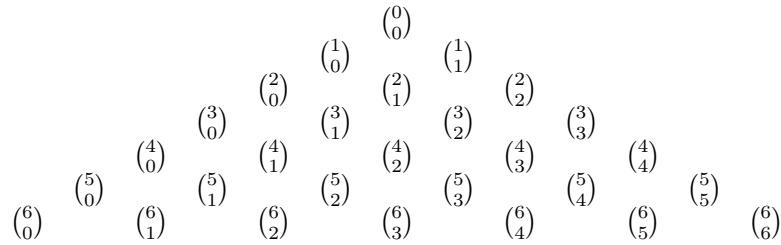


Figura 4.2: Triângulo de Pascal.

Exemplo 4.27. Vamos mostrar que para cada inteiro positivo n se verifica a igualdade

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

Solução. Considerando a grelha $n \times n$, sabemos que existem

$$\binom{n+n}{n}$$

caminhos mais curtos de A para B . Por outro lado, partindo o conjunto de todos os caminhos mais curtos entre A e B nos $n+1$ subconjuntos disjuntos:

$$\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_k, \dots, \mathcal{A}_n$$

onde \mathcal{A}_k (para $k \in \{0, 1, \dots, n\}$) é o conjunto de todos caminhos mais curtos de A para B que passam no ponto $(k, n-k)$, por aplicação do princípio da adição vem que

$$|\mathcal{A}_0| + |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| + \cdots + |\mathcal{A}_n| = \binom{2n}{n}.$$

Logo, para concluir a prova, basta demonstrar a igualdade

$$|\mathcal{A}_k| = \binom{n}{k}^2. \quad (4.22)$$

Porém, esta igualdade é consequência do facto de cada caminho de \mathcal{A}_k ser a concatenação de um caminho mais curto entre A e $(k, n-k)$ na grelha $k \times (n-k)$, cujo número é igual a

$$\binom{n-k+k}{k}$$

²O triângulo de Pascal foi introduzido por Blasie Pascal (1623–1666). Porém, já era do conhecimento do poeta e matemático persa Omar Khayyam (عمر خیام) (1048–1131) e do matemático chinês Yang Hui (1238–1298).

com um caminho mais curto entre $(k, n - k)$ e B na grelha $(n - k) \times k$, cujo número é igual a

$$\binom{k+n-k}{n-k}.$$

Por aplicação do princípio da multiplicação obtém-se, finalmente a fórmula (4.22). \square

Exemplo 4.28. *Vamos mostrar a igualdade*

$$\binom{n}{t_1, t_2, \dots, t_r} = \sum_{i=1}^r \binom{n-1}{t_1, \dots, t_i-1, \dots, t_r}, \quad (4.23)$$

que é uma generalização da igualdade (4.21), uma vez que $\binom{n}{k} = \binom{n}{k, n-k}$.

Solução. A parte esquerda da igualdade é o número multinomial que corresponde ao número de partições de $\{1, 2, \dots, n\}$ nos subconjuntos A_1, A_2, \dots, A_r , com cardinalidade t_1, t_2, \dots, t_r , respectivamente. Podemos dividir estas partições nos seguinte r tipos de partições distintas:

- (1) aquelas em que $n \in A_1$, cuja cardinalidade corresponde ao número de partições de $n-1$ elementos em r subconjuntos, com cardinalidades t_1-1, t_2, \dots, t_r , respectivamente;
- (2) aquelas em que $n \in A_2$, cuja cardinalidade corresponde ao número de partições de $n-1$ elementos em r subconjuntos, com cardinalidades t_1, t_2-1, \dots, t_r , respectivamente;
- (.) etc;
- (r) aquelas em que $n \in A_r$, cuja cardinalidade corresponde ao número de partições de $n-1$ elementos em r subconjuntos, com cardinalidades t_1, t_2, \dots, t_r-1 , respectivamente.

Logo, para $i = 1, 2, \dots, r$, o número de partições do tipo i é igual a

$$\binom{n-1}{t_1, \dots, t_i-1, \dots, t_r}$$

e, aplicando o princípio da adição, obtém-s a identidade (4.23). \square

Exemplo 4.29. *Vamos demonstrar as seguintes igualdades*

$$\sum_{k=0}^m \binom{k}{n} = \binom{m+1}{n+1}, \quad (4.24)$$

$$\sum_{k=0}^l \binom{n}{k} \binom{m}{l-k} = \binom{n+m}{l}, \quad (4.25)$$

$$\sum_{k=1}^n k^2 \binom{n}{k}^2 = n^2 \binom{2n-2}{n-1}. \quad (4.26)$$

Solução.

- (4.24) Sendo $\mathcal{X} = \{X \in \mathcal{P}([m+1]) : |X| = n+1\}$, podemos concluir que a parte direita da igualdade (4.24) corresponde à cardinalidade de \mathcal{X} . Vamos partir \mathcal{X} nos subconjuntos

$$\mathcal{X}_k = \{Y \in \mathcal{X} : \max Y = k+1\},$$

para $k = n, \dots, m$. É claro que $|\mathcal{X}_k| = \binom{k}{n}$, uma vez que para se obterem os subconjuntos de \mathcal{X}_k , basta fixar o número $k+1$ e determinar todas as combinações de n elementos do conjunto $\{1, \dots, k\}$. Tendo em conta que $k < n \Rightarrow \binom{k}{n} = 0$, podemos finalmente concluir a igualdade (4.24).

- (4.25) É claro que a parte direita da equação (4.25) corresponde ao número de subconjuntos de cardinalidade l de um conjunto X de cardinalidade $n+m$. Considerando que o conjunto X é constituído por n elementos de cor vermelha e m elementos de cor azul, podemos classificar os subconjuntos de cardinalidade l de X nos subconjuntos com k elementos vermelhos e $l-k$ elementos azuis, para $k = 0, 1, \dots, \min\{l, n\}$. Assim, para cada $k \in \{0, 1, \dots, \min\{l, n\}\}$ existem $\binom{n}{k} \binom{m}{l-k}$ subconjuntos de cardinalidade l com k elementos vermelhos e $l-k$ azuis. Aplicando o princípio da adição obtém-se a igualdade (4.25).
- (4.26) Para provar a igualdade (4.26) vamos, primeiramente, considerar um conjunto de m homens e m mulheres, a partir do qual se escolhem subconjuntos com igual número (possivelmente zero) de homens e mulheres. O número de tais subconjuntos é, naturalmente, igual a $\sum_{k=0}^m \binom{m}{k}^2$ e a igualdade do Exemplo 4.27 implica que se obtenha

$$\sum_{k=0}^m \binom{m}{k}^2 = \binom{2m}{m}. \quad (4.27)$$

Suponha-se agora que a partir de um conjunto de n homens e n mulheres, em cada subconjunto (com igual número de homens e mulheres) se escolhe um líder para os homens e uma líder para as mulheres. Como consequência, para cada subconjunto com k homens e k mulheres existem k^2 possíveis pares de líderes e por aplicação do princípio da multiplicação $k^2 \binom{n}{k}^2$ subconjuntos com k homens e k mulheres com um par de líderes cada. Como consequência, para os diferentes valores de k obtém-se o lado esquerdo da equação (4.26). Em alternativa, vamos supor que se escolhem primeiramente os (as) líderes dos (das) homens (mulheres) para o que existem n^2 possibilidades. Logo, completando os subconjuntos com o mesmo número de homens e mulheres, utilizando a igualdade (4.27) com $m = n - 1$ obtém-se

$$n^2 \sum_{k=0}^{n-1} \binom{n-1}{k}^2 = n^2 \binom{2(n-1)}{n-1}$$

e, consequentemente, a igualdade pretendida.

Note-se que qualquer das igualdades (4.24)–(4.26) poderia ser obtida algebricamente. Por exemplo, a igualdade (4.26) pode demonstrar-se algebricamente, conforme a seguir se indica.

$$\begin{aligned} \sum_{k=1}^n k^2 \binom{n}{k}^2 &= \sum_{k=1}^n k^2 \left(\frac{n!}{k!(n-k)!} \right)^2 = \sum_{k=1}^n n^2 \left(\frac{(n-1)!}{(k-1)!(n-k)!} \right)^2 \\ &= n^2 \sum_{k=1}^n \binom{n-1}{k-1}^2 = n^2 \sum_{k=0}^{n-1} \binom{n-1}{k}^2 = n^2 \binom{2n-2}{n-1}. \end{aligned}$$

Note-se que a última igualdade se obtém tendo em conta o Exemplo 4.27. □

Exemplo 4.30. *Vamos demonstrar as igualdades*

$$\left(\sum_{k=0}^n \binom{n}{k} \right)^2 = \sum_{k=0}^{2n} \binom{2n}{k}, \quad (4.28)$$

$$(n-r) \binom{n+r-1}{r} \binom{n}{r} = n \binom{n+r-1}{2r} \binom{2r}{r}, \quad (4.29)$$

$$\sum_{k=0}^m \binom{n+k}{k} = \binom{n+m+1}{m}. \quad (4.30)$$

Solução.

- (4.28) Tendo em conta que o número de elementos do conjunto das partes de um conjunto de cardinalidade n é igual a 2^n (que por sua vez é igual a $\sum_{k=0}^n \binom{n}{k}$), podemos concluir que dado um conjunto com $2n$ elementos, a cardinalidade do conjunto das suas partes é igual a

$$2^{2n} = \left(\sum_{k=0}^n \binom{n}{k} \right)^2 = \sum_{k=0}^{2n} \binom{2n}{k}.$$

- (4.29) Usando formula (4.7) para simplificar igualdade (4.29) temos

$$\frac{n(n+r-1)!}{r!r!(n-r-1)!} = \frac{n(n+r-1)!}{r!r!(n-r-1)!}.$$

- (4.30) Dado que

$$\sum_{k=0}^m \binom{n+k}{k} = \sum_{k=0}^m \binom{n+k}{n} = \sum_{j=n}^{n+m} \binom{j}{n} = \sum_{j=0}^{n+m} \binom{j}{n},$$

aplicando a igualdade (4.24), obtém-se a igualdade (4.30). \square

4.6. Exercícios

- 4.1. Determine o número de permutações de elementos do conjunto $\{0, 1, \dots, 9\}$, nas quais os dígitos 2, 6 e 9 (não necessariamente por esta ordem) ocupam posições de vizinhança mútua.
- 4.2. Dados dez pares de sapatos, de quantas maneiras podemos escolher quatro sapatos de tal forma que dois deles constituam um dos pares originais?
- 4.3. Prove a igualdade (4.1), por indução sobre k .
- 4.4. Prove que de entre os resultados que é possível obter, lançando doze dados e somando os doze números que aparecem nas faces voltadas para cima, precisamente metade têm valor par.
- 4.5. Quantos pares de dança (homem-mulher) se podem formar com 10 homens e 10 mulheres?
- 4.6. Num conjunto de 20 pessoas quantos pares de pessoas se podem formar?
- 4.7. Qual o número de possibilidades de se colocarem em linha n bolas brancas (iguais) e m bolas pretas (iguais)?
- 4.8. Ao preencher um boletim do totobola o objectivo consiste em prever os resultados (vitória, empate ou derrota) de 12 jogos. Quantos boletins se devem preencher para se ter a garantia de se acertar em pelo menos 11 resultados?
- 4.9. Qual o número de possibilidades de colocar quatro laranjas iguais e seis maçãs diferentes em cinco caixas numeradas?
- 4.10. Qual o número de possibilidades de colocação de 25 cartas iguais em 10 caixas do correio, sabendo que se coloca pelo menos uma carta em cada caixa?

4.11. Quantas soluções inteiras não negativas tem a equação

$$x_1 + x_2 + \dots + x_9 = 90,$$

onde todas as variáveis x_i tomam valores não inferiores a 3?

4.12. Quantos quadrados existem no conjunto de todos os rectângulos da grelha $n \times n$?

4.13. Desenvolva a expressão $(a + b + c)^4$ (utilizando fórmula multinomial).

4.14. Demonstre a igualdade

$$\binom{n}{0} \binom{n}{k} + \binom{n}{1} \binom{n-1}{k-1} + \dots + \binom{n}{k} \binom{n-k}{0} = \binom{n}{k} 2^k.$$

contando de dois modos distintos o número de colorações de k bolas escolhidas de um conjunto de n bolas (todas diferentes), utilizando apenas duas cores.

4.15. Demonstre a igualdade a seguir indicada, utilizando argumentos combinatórios

$$1^3 + 2^3 + \dots + n^3 = \binom{n+1}{2}^2.$$

4.16. Utilizando argumentos combinatórios, prove as seguintes igualdades:

$$(a) \sum_{k=0}^n k \binom{n}{k} = n 2^{n-1},$$

$$(b) \sum_{k=1}^n k(n+1-k) = \binom{n+2}{3},$$

$$(c) \sum_{k=0}^n \binom{n}{k} (m-1)^{n-k} = m^n.$$

4.17. Com recurso a argumentos combinatórios e algébricos, prove a igualdade:

$$\sum_{k=0}^n \frac{(2n)!}{(k!)^2 (n-k)!^2} = \binom{2n}{n}^2.$$

4.18. Utilizando argumentos combinatórios e algébricos, prove a igualdade:

$$\binom{2n}{n} = 2 \binom{n}{2} + n^2.$$

4.19. Prove a igualdade

$$\sum_{k=m}^n \binom{k}{r} = \binom{n+1}{r+1} - \binom{m}{r+1}.$$

4.20. Prove a igualdade

$$\sum_{k=1}^n \binom{m+k-1}{k} = \sum_{k=1}^m \binom{n+k-1}{k}.$$

4.21. Indique o número de números naturais "monótonos" com n dígitos, $d_1 d_2 \dots d_n$, onde "monótono" significa que, para $j = 1, \dots, n-1$,

- (a) $d_j < d_{j+1}$,
 (b) $d_j \leq d_{j+1}$,
 (c) $d_j \leq d_{j+1}$ e $\exists k \in \{1, \dots, n-1\}$ tal que $d_k < d_{k+1}$.
- 4.22. Suponha que $n+k$ pessoas querem comprar gelados que custam 1€, e que, entre elas, n pessoas têm uma moeda de 1€ e k pessoas têm uma moeda de 2€. Qual o número de maneiras de ordenar as pessoas na fila de tal forma que o vendedor de gelados arranje sempre uma moeda para dar de troco quando tal é necessário (assumindo-se que, inicialmente, o vendedor não tem qualquer moeda).
- 4.23. Prove a igualdade
- $$\sum_{k=1}^n k^2 \binom{n}{k} = n(n+1)2^{n-2}.$$
- 4.24. Determine os valores de n e k tais que $\binom{n}{k+1} = 3\binom{n}{k}$.
- 4.25. Mostre que
- $$\frac{n^k}{k^k} \leq \binom{n}{k} \leq \frac{n^k}{k!}.$$
- 4.26. Utilizando argumentos combinatórios, prove que
- $$\sum_{k=0}^n 2^k \binom{n}{k} = 3^n.$$
- 4.27. Mostre que todo $n \in \mathbb{N}$
- $$\binom{n}{0} < \binom{n}{1} < \dots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \dots > \binom{n}{n},$$
- (onde o símbolo $\lceil x \rceil$ denota menor número inteiro não inferior a x).
- 4.28. Demonstre, de duas maneiras distintas, a igualdade
- $$\binom{n}{2} + \binom{n+1}{2} = n^2,$$
- num caso utilizando argumentos combinatórios e no outro recorrendo às expressões de cálculo.
- 4.29. Demonstre, de duas maneiras distintas, a igualdade
- $$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1},$$
- num caso utilizando argumentos combinatórios e no outro recorrendo às expressões de cálculo.
- 4.30. Demonstre, de duas maneiras distintas, que para $0 \leq k \leq n \leq m$ se verifica a igualdade
- $$\binom{m}{n} \binom{n}{k} = \binom{m}{m-k} \binom{m-k}{n-k},$$
- num caso utilizando argumentos combinatórios e no outro recorrendo às expressões de cálculo.

5

Recorrência e Funções Geradoras

A solução de muitos problemas de natureza combinatória pode ser obtida recursivamente ou, por outras palavras, utilizando uma relação de recorrência (que também se pode designar por relação recursiva). Em traços gerais, a resolução recursiva consiste em expressar a solução de um problema de certa ordem à custa da solução de um problema idêntico, mas de ordem inferior. Um exemplo típico de resolução recursiva é o da determinação do factorial de um número $n \in \mathbb{N}$. Com efeito, é imediato concluir que

$$n! = n(n - 1)!$$

e esta relação é, claramente, uma relação de recorrência.

Em termos de aplicações, é frequente a utilização de relações recursivas em informática, com vista à simplificação de algoritmos. Por outro lado, a análise de complexidade de algoritmos (com a qual se procura medir o esforço computacional exigido na respectiva execução) é feita, em muitos casos, utilizando relações de recorrência.

5.1. Dependências recursivas simples

Vamos iniciar o estudo das relações de recorrência com um método "ingénuo" para a dedução de fórmulas de recorrência de determinação dos termos de sucessões, admitindo que tais termos possam ser determinados recursivamente. Assim, dada uma sucessão, o método "ingénuo" consiste no seguinte:

1. Propor uma fórmula de dependência simples entre os termos da sucessão, a partir da observação de alguns termos;
2. Provar (por exemplo, por indução) que a fórmula proposta no passo 1 é válida.

Com este método, chegar a uma proposta de relação de dependência entre elementos de uma sucessão pode não ser uma tarefa fácil e depende muito da capacidade de observação e detecção dos relacionamentos existentes entre alguns dos termos. Porém, a não existência de um método geral que garanta a obtenção das relações de recorrência, leva a que, frequentemente, se adopte esta metodologia.

Exemplo 5.1. *Vamos determinar recursivamente o número de permutações do conjunto $[n] = \{1, 2, \dots, n\}$.*

Solução. Denote-se por a_n o número de permutações de conjunto $[n]$. Cada uma destas permutações pode obter-se a partir das permutações de elementos do conjunto $[n - 1]$, inserindo o elemento n em

todas as posições possíveis de cada uma das permutações desse conjunto (ou seja, antes do primeiro elemento, entre os dois primeiros elementos, depois do último elemento, etc). Assim, uma vez que existem a_{n-1} permutações de elementos do conjunto $[n - 1]$ e n posições possíveis para inserir o elemento n , aplicando o princípio da multiplicação obtém-se a equação recursiva

$$a_n = n a_{n-1}, \quad n \geq 2. \quad (5.1)$$

É claro que existe uma única permutação dos elementos do conjunto $\{1\}$, pelo que, a condição inicial é $a_1 = 1$. Tendo em vista obter uma fórmula para a_n , repetindo sucessivamente a aplicação da fórmula (5.1), vem

$$a_n = n a_{n-1} = n(n-1)a_{n-2} = \dots = n(n-1) \cdot \dots \cdot 2 \cdot a_1.$$

Assim, obtém-se a fórmula para o número de permutações de n elementos (idêntica à igualdade (4.3))

$$a_n = n!. \quad (5.2)$$

Vamos fazer a prova da igualdade (5.2) por indução sobre n , tendo em conta que a igualdade (5.2) se verifica para $n = 1$. Supondo que a igualdade (5.2) se verifica para $n - 1$, com $n \geq 2$, aplicando a relação de recorrência (5.1) vem

$$a_n = n a_{n-1} = n(n-1)! = n!,$$

o que permite concluir a prova desejada. \square

Exemplo 5.2. Considerando que dispomos de n rectas num plano, de tal modo que não existe um par de rectas paralelas e não existem três rectas que se intersectem num ponto, vamos determinar o número de regiões do plano definidas por essas rectas.

Solução. Denotando por a_n o número de regiões do plano definidas pelas n rectas, podemos concluir que $a_0 = 1$ e $a_1 = 2$. Ao traçarmos a recta número n , de acordo com as hipóteses, estamos a intersectar todas as $n - 1$ rectas já traçadas e também a dividir n regiões do plano, de entre as definidas por $n - 1$ rectas, em duas partes (note-se que os pontos de intersecção da n -ésima recta com cada uma das restantes rectas, são pontos da fronteira de n regiões de entre as criadas pelas $n - 1$ rectas, tal como se apresenta na Figura 5.1). Como consequência, depois de traçada a n -ésima recta, além das a_{n-1} regiões, passam a existir mais n , ou seja,

$$a_n = a_{n-1} + n, \quad n \geq 1. \quad (5.3)$$

Repetindo a igualdade (5.3) (entre 1 e n) obtém-se

$$a_n = a_{n-1} + n = a_{n-2} + n - 1 + n = \dots = a_0 + 1 + 2 + \dots + n.$$

Uma vez que $1 + 2 + \dots + n = \binom{n+1}{2}$, conclui-se finalmente que

$$a_n = 1 + \binom{n+1}{2}. \quad (5.4)$$

Tal como anteriormente, vamos fazer a prova formal da fórmula (5.4). Em primeiro lugar, é imediato que a formula (5.4) se verifica para $n = 1$ e $n = 2$. Assumindo que a fórmula (5.4) se verifica-se para $n - 1$, tendo em conta a igualdade (5.3), podemos concluir que

$$a_n = a_{n-1} + n = 1 + \binom{n}{2} + n = 1 + \binom{n+1}{2},$$

o que completa a prova por indução sobre n da validade da formula (5.4). \square

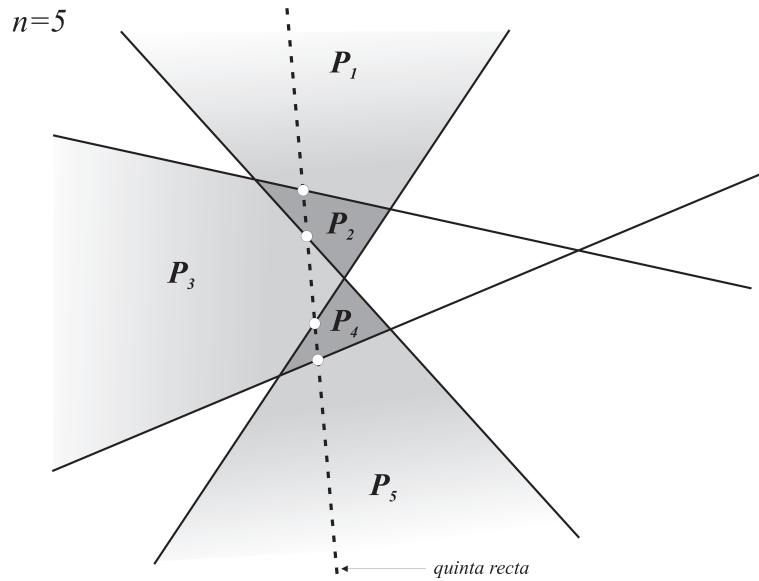


Figura 5.1: Representação das divisões em duas partes provocadas pela quinta recta nas regiões P_1 , P_2 , P_3 , P_4 e P_5 .

Nos casos em que a relação de recorrência determina o termo a_n em função de a_{n-1} (ou seja, os termos anteriores não aparecem, directamente, na relação), como é o caso das igualdades recursivas (5.1) e (5.3), dizemos que a relação de recorrência tem *profundidade* ou *ordem* 1. Mais geralmente:

Definição 5.1 (Profundidade da relação de recorrência). *Quando a relação de recorrência toma a forma*

$$a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-k}),$$

diz-se que se trata de uma relação de recorrência com profundidade ou ordem k.

Dado uma equação de recorrência $a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-k})$, a sua *resolução* consiste na determinação de uma fórmula não recursiva para a_n . No caso da equação de recorrência ter profundidade k , para a sua resolução são necessárias k condições iniciais.

Observe-se que uma equação de recorrência pode ter mais do que uma solução. A forma geral desta solução, a partir da qual se obtém cada uma das soluções particulares (de acordo com os valores escolhidos para as respectivas constantes), designa-se por *solução geral*. Uma solução obtida da solução geral, atribuindo-se valores às constantes, designa-se por *solução particular*. Por exemplo, dado a equação de recorrência $a_n = na_{n-1}$, cuja solução geral é $a_n = Cn!$, se $C = 1$, então obtém-se a solução particular $a_n = n!$ (note-se que $a_1 = 1$ é uma condição inicial para esta solução particular).

5.2. Equações de recorrência homogéneas

Uma equação de recorrência linear é uma equação onde o termo de ordem n depende linearmente dos termos de ordem inferior e diz-se homogénea quando a equação não tem termo independente. Mais formalmente, temos a seguinte definição.

Definição 5.2 (Equação de recorrência linear homogénea). *Designa-se por equação de recorrência linear homogénea toda a equação da forma:*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r}, \quad (5.5)$$

onde c_i , para $i = 1, 2, \dots, r$, são constantes que não dependem de n .

Uma vez que esta equação recursiva tem profundidade r , são necessárias r condições iniciais (tal como já foi referido).

Definição 5.3 (Equação característica). *Dada uma equação de recorrência da forma (5.5), define-se a equação característica que lhe corresponde como sendo a equação da forma:*

$$x^r - c_1 x^{r-1} - c_2 x^{r-2} - \cdots - c_r = 0. \quad (5.6)$$

Observe-se que a equação (5.6) decorre da equação (5.5), substituindo a_k por x^k , para $k = n-r, \dots, n-1, n$, e dividindo a equação obtida pela menor potência de x . Conforme se verá, mais adiante, a solução da equação (5.5) depende das raízes da equação característica (5.6). Em particular, se a equação de recorrência (5.5) tem profundidade dois, então a equação característica que lhe corresponde é uma equação quadrática cujas raízes se determinam, facilmente, por aplicação da respectiva fórmula resolvente.

Lema 5.1. *Sejam α e β as raízes (não necessariamente reais mas que se supõem ambas não nulas¹) da equação característica*

$$x^2 - Ax - B = 0, \quad (5.7)$$

que corresponde à equação de recorrência

$$a_n = Aa_{n-1} + Ba_{n-2}. \quad (5.8)$$

Se $\alpha \neq \beta$ então a respectiva solução geral vem dada por

$$a_n = C_1\alpha^n + C_2\beta^n, \quad (5.9)$$

caso contrário, vem dada por

$$a_n = (C_1 + C_2n)\alpha^n. \quad (5.10)$$

Em ambos os casos, os coeficientes C_1 e C_2 são determinados pelas condições iniciais.

Demonstração. Vamos dividir esta prova em três partes.

1. Na primeira parte vamos provar os seguintes resultados:
 - (a) A sucessão γ^k , $k = 1, 2, \dots$, satisfaz a relação de recorrência (5.8) se e só se γ é solução da equação característica (5.7).
 - (b) Adicionalmente, se (5.7) tem uma única raiz ρ , então a sucessão $k\rho^k$, para $k = 1, 2, \dots$, satisfaz também a relação de recorrência (5.8).
2. Na segunda parte vamos provar, por indução sobre n , que a fórmula (5.9) é válida quando $\alpha \neq \beta$.
3. Finalmente, na terceira parte provaremos, por indução sobre n , a validade da fórmula (5.10) quando $\alpha = \beta$.

Seguem-se as respectivas provas.

1. (a) Com efeito, se $\gamma^n = A\gamma^{n-1} + B\gamma^{n-2}$ então, dividindo esta equação por γ^{n-2} , obtém-se a equação quadrática $\gamma^2 - A\gamma - B = 0$. Reciprocamente, supondo que $\gamma \neq 0$ satisfaz a equação característica (5.7), para $k \geq 2$, vem $\gamma^{k-2}(\gamma^2 - A\gamma - B) = 0 \Leftrightarrow \gamma^k = A\gamma^{k-1} + B\gamma^{k-2}$.

¹Deve observar-se que as raízes da equação quadrática (5.7) são ambas não nulas se e só se $B \neq 0$.

- (b) Uma vez que a equação característica (5.7) tem uma única raiz ρ , vem $x^2 - Ax - B = (x - \rho)^2 = x^2 - 2\rho x + \rho^2$ e, consequentemente, $A = 2\rho$ e $B = -\rho^2$. Logo, considerando a sucessão $0, 1\rho^1, 2\rho^2, \dots, k\rho^k$, podemos concluir que, para $k \geq 2$,

$$\begin{aligned} A(k-1)\rho^{k-1} + B(k-2)\rho^{k-2} &= 2\rho(k-1)\rho^{k-1} - \rho^2(k-2)\rho^{k-2} \\ &= (2k-2-k+2)\rho^k = k\rho^k. \end{aligned}$$

2. Tendo em conta as condições iniciais, é claro que a fórmula (5.9) é válida para $n \in \{0, 1\}$. Suponha-se que a fórmula $a_k = C_1\alpha^k + C_2\beta^k$ é válida para $0 \leq k < n$. Então, para $n \geq 2$,

$$\begin{aligned} a_n &= Aa_{n-1} + Ba_{n-2} \\ &= A(C_1\alpha^{n-1} + C_2\beta^{n-1}) + B(C_1\alpha^{n-2} + C_2\beta^{n-2}) \\ &= C_1(A\alpha^{n-1} + B\alpha^{n-2}) + C_2(A\beta^{n-1} + B\beta^{n-2}) \\ &= C_1\alpha^n + C_2\beta^n \text{ (tendo em conta o ponto 1a).} \end{aligned}$$

3. Tendo em conta as condições iniciais, é claro que a fórmula (5.10) é válida para $n \in \{0, 1\}$. Suponha-se que a fórmula $a_k = (C_1 + C_2k)\alpha^k$ é válida para $0 \leq k < n$. Então, para $n \geq 2$,

$$\begin{aligned} a_n &= Aa_{n-1} + Ba_{n-2} \\ &= A(C_1 + C_2(n-1))\alpha^{n-1} + B(C_1 + C_2(n-2))\alpha^{n-2} \\ &= C_1(A\alpha^{n-1} + B\alpha^{n-2}) + C_2(A(n-1)\alpha^{n-1} + B(n-2)\alpha^{n-2}) \\ &= C_1\alpha^n + C_2n\alpha^n \text{ (tendo em conta os pontos 1a e 1b).} \end{aligned}$$

□

Seguem-se alguns exemplos que ilustram a aplicação deste resultado.

Exemplo 5.3. Suponha que um concurso está dividido em n etapas com cinco obstáculos possíveis em cada uma. Na n -ésima etapa existem dois obstáculos, a partir dos quais, ultrapassado um deles, se passa à etapa $n-1$ e existem outros três, a partir dos quais, ultrapassado um deles, se passa directamente da etapa n à etapa $n-2$. Sendo a_n o número de possibilidades de se ultrapassarem diferentes obstáculos, a partir da etapa n e supondo $a_1 = 5$ e $a_2 = 13$, vamos determinar uma fórmula para a_n .

Solução. A formulação do problema conduz-nos à seguinte equação de recorrência

$$a_n = 2a_{n-1} + 3a_{n-2},$$

para a qual se obtém a equação característica $x^2 = 2x + 3$. Uma vez que

$$x^2 - 2x - 3 = (x+1)(x-3),$$

por aplicação da fórmula (5.9), obtém-se

$$a_n = C_1(-1)^n + C_23^n.$$

Por sua vez, das condições iniciais decorre o sistema de equações

$$\begin{cases} -C_1 + 3C_2 = 5 \\ C_1 + 9C_2 = 13 \end{cases}$$

cuja resolução conduz à solução final:

$$a_n = -\frac{1}{2}(-1)^n + \frac{3}{2}3^n, \quad n \geq 1.$$

□

Exemplo 5.4. Vamos resolver a seguinte equação de recorrência

$$a_n = -6a_{n-1} - 9a_{n-2},$$

com condições iniciais $a_0 = 1$, $a_1 = -9$.

Solução. Uma vez que a equação característica é

$$x^2 + 6x + 9 = (x + 3)^2,$$

por aplicação da formula (5.10), obtém-se a solução

$$a_n = (C_1 + C_2 n)(-3)^n.$$

Considerando as condições iniciais, vem

$$\begin{cases} C_1 &= a_0 = 1 \\ -3C_1 - 3C_2 &= a_1 = -9 \end{cases}$$

onde, determinados C_1 e C_2 , se obtém finalmente a solução:

$$a_n = (1 + 2n)(-3)^n.$$

□

Exemplo 5.5. Vamos calcular o número de maneiras de subir uma escada com n degraus, sabendo que em cada passo podemos avançar um ou dois degraus.

Solução. Sendo F_n o número de maneiras de subir $n - 1$ degraus, vamos dividi-las em dois conjuntos, o que corresponde às subidas da escada admitindo que no último passo se avança um degrau, cuja cardinalidade é então F_{n-1} , e o que corresponde às subidas em que se admite que no último passo se avançam dois degraus, cuja cardinalidade é F_{n-2} . Logo, aplicando o princípio da adição, vem

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 3, \tag{5.11}$$

com as condições iniciais $F_1 = 1$ e $F_2 = 1$. A equação de recorrência (5.11) é conhecida por *equação de Fibonacci* e a sucessão de números $1, 1, 2, 3, 5, 8, 13, 21, \dots$ que se obtém com a sua aplicação é conhecida por *sequência de Fibonacci*² ou *números de Fibonacci*. Para determinar F_n , considerando a equação característica $x^2 - x - 1 = 0$, cujas raízes são $(1 \pm \sqrt{5})/2$, por aplicação da fórmula (5.9), vem

$$F_n = C_1 \left(\frac{1 + \sqrt{5}}{2} \right)^n + C_2 \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

Considerando as condições iniciais, obtém-se

$$C_1 = \frac{1}{\sqrt{5}}, \quad C_2 = -\frac{1}{\sqrt{5}}$$

e, consequentemente, a solução

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n. \tag{5.12}$$

□

²Fibonacci, também conhecido por Leonardo de Pisa, em "Liber abaci", publicado em 1202, introduziu estes números, tendo ainda divulgado na Europa o sistema decimal hindu/árabe e a numeração árabe.

Exemplo 5.6. Vamos calcular o número de n -uplos b_n com componente pertencentes ao conjunto $\{0, 1, 2\}$, nos quais não existem componentes vizinhas com valor igual e pertencente ao subconjunto $\{1, 2\}$.

Solução. Seja $\mathcal{B}_k^{(i)}$ o conjunto dos k -uplos com componentes pertencentes ao conjunto $\{0, 1, 2\}$ nos quais não existem componentes vizinhas com o mesmo valor pertencente ao subconjunto $\{1, 2\}$ e cuja primeira componente é i . Note-se, por um lado que

$$|\mathcal{B}_k^{(0)}| = b_{k-1} \quad (5.13)$$

e por outro lado que se o primeiro elemento é 1 então o segundo é 0 ou 2 e se o primeiro elemento é 2 então o segundo é 0 ou 1. Logo,

$$b_n = |\mathcal{B}_n^{(0)}| + |\mathcal{B}_n^{(1)}| + |\mathcal{B}_n^{(2)}| \quad (5.14)$$

$$\begin{aligned} &= |\mathcal{B}_n^{(0)}| + \left(|\mathcal{B}_{n-1}^{(2)}| + |\mathcal{B}_{n-1}^{(0)}| \right) + \left(|\mathcal{B}_{n-1}^{(1)}| + |\mathcal{B}_{n-1}^{(0)}| \right) \\ &= |\mathcal{B}_n^{(0)}| + \left(|\mathcal{B}_{n-1}^{(2)}| + |\mathcal{B}_{n-1}^{(0)}| + |\mathcal{B}_{n-1}^{(1)}| \right) + |\mathcal{B}_{n-1}^{(0)}| \end{aligned} \quad (5.15)$$

$$\begin{aligned} &= |\mathcal{B}_n^{(0)}| + b_{n-1} + |\mathcal{B}_{n-1}^{(0)}| \\ &= 2b_{n-1} + b_{n-2}. \end{aligned} \quad (5.16)$$

Note-se que a igualdade (5.14) decorre da definição de $\mathcal{B}_n^{(i)}$, para $i = 0, 1, 2$, a igualdade (5.15) é consequência de se ter $b_{n-1} = |\mathcal{B}_{n-1}^{(0)}| + |\mathcal{B}_{n-1}^{(1)}| + |\mathcal{B}_{n-1}^{(2)}|$ e a igualdade (5.16) decorre de (5.13).

Procedendo ao cálculo das condições iniciais, obtém-se:

- $b_1 = 3$ (uma vez que os 1-uplos possíveis são da forma: 0, 1, 2),
- $b_2 = 7$ (uma vez que os 2-uplos possíveis são da forma: 00, 01, 02, 10, 12, 20, 21).

Para determinar b_n , considerando a equação característica $x^2 = 2x+1$ cujas raízes são $1 \pm \sqrt{2}$, obtém-se a solução geral:

$$b_n = C_1 \left(1 + \sqrt{2} \right)^n + C_2 \left(1 - \sqrt{2} \right)^n.$$

Finalmente, determinando as constantes a partir das condições iniciais, vem

$$C_1 = \frac{1 + \sqrt{2}}{2}, \quad C_2 = \frac{1 - \sqrt{2}}{2}$$

e, consequentemente, chega-se à solução

$$b_n = \frac{1}{2} \left(1 + \sqrt{2} \right)^{n+1} + \frac{1}{2} \left(1 - \sqrt{2} \right)^{n+1}.$$

□

O Lema 5.1 é um caso particular do Lema 5.2 que se apresenta a seguir.

Lema 5.2. Se $\alpha_1, \alpha_2, \dots, \alpha_r$ são raízes distintas (não necessariamente reais) da equação característica

$$x^r - c_1 x^{r-1} - c_2 x^{r-2} - \dots - c_r = 0$$

da equação de recorrência

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_r a_{n-r},$$

então a equação de recorrência tem como solução

$$a_n = C_1 \alpha_1^n + C_2 \alpha_2^n + \dots + C_r \alpha_r^n.$$

Mais geralmente, se

$$\begin{aligned} x^r - c_1x^{r-1} - c_2x^{r-2} - \dots - c_r \\ = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdots (x - \alpha_k)^{m_k}, \end{aligned}$$

onde $m_i \geq 1$, $i = 1, 2, \dots, k$ e $m_1 + m_2 + \dots + m_k = r$ (pelo que cada α_i é uma raiz com multiplicidade m_i), então

$$\begin{aligned} a_n &= (D_1 + D_2n + \dots + D_{m_1}n^{m_1-1})\alpha_1^n \\ &\quad + (E_1 + E_2n + \dots + E_{m_2}n^{m_2-1})\alpha_2^n \\ &\quad \vdots \\ &\quad + (Z_1 + Z_2n + \dots + Z_{m_k}n^{m_k-1})\alpha_k^n \end{aligned}$$

é a solução da equação de recorrência, onde as constantes D_1, \dots, Z_{m_k} são determinadas pelas condições iniciais.

Exemplo 5.7. Suponha que um organismo primitivo necessita de duas horas para se desenvolver, após as quais produz quatro descendentes e, posteriormente, mais seis descendentes no final de cada hora subsequente. Admitindo que todos os descendentes têm o mesmo comportamento, vamos determinar o número a_n de organismos obtidos após n horas, supondo que o processo se inicia com um único organismo acabado de nascer.

Solução. Note-se que a população destes organismos pode ser dividida nos seguintes grupos:

- (a) Organismos com tempo de vida de uma hora, cujo o número é $a_{n-1} - a_{n-2}$;
- (b) Organismos com tempo de vida de duas horas, cujo número é $a_{n-2} - a_{n-3}$, e respectivos descendentes, cujo número é $4(a_{n-2} - a_{n-3})$;
- (c) Organismos com tempo de vida de pelo menos três horas, cujo número é a_{n-3} , e seus descendentes, cujo número é $6a_{n-3}$.

Como consequência,

$$\begin{aligned} a_n &= a_{n-1} - a_{n-2} + 5(a_{n-2} - a_{n-3}) + 7a_{n-3} \\ &= a_{n-1} + 4a_{n-2} + 2a_{n-3}, \end{aligned}$$

onde se obtém a equação característica

$$x^3 - x^2 - 4x - 2 = 0$$

cujas três raízes são

$$\alpha_1 = -1, \quad \alpha_2 = 1 - \sqrt{3}, \quad \alpha_3 = 1 + \sqrt{3}.$$

A aplicação do Lema 5.2 conduz-nos à solução geral

$$a_n = C_1(-1)^n + C_2(1 - \sqrt{3})^n + C_3(1 + \sqrt{3})^n.$$

Dado que as condições iniciais são $a_0 = 1$, $a_1 = 1$ e $a_2 = 5$, obtém-se o sistema de equações lineares:

$$\begin{cases} 1 = C_1 + C_2 + C_3 \\ 1 = -C_1 + C_2(1 - \sqrt{3}) + C_3(1 + \sqrt{3}) \\ 5 = C_1 + C_2(1 - \sqrt{3})^2 + C_3(1 + \sqrt{3})^2 \end{cases}$$

cuja solução é

$$C_1 = 1, \quad C_2 = -\frac{1}{\sqrt{3}}, \quad C_3 = \frac{1}{\sqrt{3}}.$$

Logo, podemos concluir, finalmente, que após n horas de desenvolvimento, a população de organismos atinge o número

$$a_n = \frac{(1 + \sqrt{3})^n - (1 - \sqrt{3})^n}{\sqrt{3}} + (-1)^n.$$

□

Exemplo 5.8. Vamos resolver a equação de recorrência

$$a_n = 2a_{n-1} + 15a_{n-2} + 4a_{n-3} - 20a_{n-4},$$

cujas condições iniciais são

$$a_0 = 6, \quad a_1 = 3, \quad a_2 = 71 \quad e \quad a_3 = 203.$$

Solução. Uma vez que

$$x^4 - 2x^3 - 15x^2 - 4x + 20 = (x + 2)^2(x - 1)(x - 5),$$

podemos concluir que a equação característica tem as raízes

- $\alpha_1 = -2$ de multiplicidade dois,
- $\alpha_2 = 1$ de multiplicidade um,
- $\alpha_3 = 5$ de multiplicidade um.

A aplicação do Lema 5.2 implica que a solução geral da equação de recorrência tome a forma

$$a_n = (C_1 + C_2 n)(-2)^n + C_3 + C_4 5^n.$$

Determinando as constantes, a partir das condições iniciais, conclui-se que $C_1 = 3$, $C_2 = 1$, $C_3 = 1$ e $C_4 = 2$. Logo, procedendo à respectiva substituição, obtém-se a solução pretendida, ou seja,

$$a_n = (3 + n)(-2)^n + 1 + 2 \cdot 5^n.$$

□

Atenção! No exemplo a seguir utilizam-se números complexos. Se o leitor não teve ainda contacto com estes números, sugere-se que avance para o próximo exemplo.

Exemplo 5.9. Vamos resolver a equação de recorrência

$$a_n = 2a_{n-1} - 2a_{n-2} + a_{n-3}$$

cujas condições iniciais são: $a_0 = 0$, $a_1 = 1$ e $a_2 = 2$.

Solução. Tendo em conta a fórmula obtida para a equação característica

$$x^3 - 2x^2 + 2x - 1 = (x - 1)(x^2 - x + 1)$$

conclui-se que as raízes são um número real e dois números complexos conjugados, ou seja,

$$\alpha_1 = 1, \quad \alpha_2 = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \alpha_3 = \frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

As raízes complexas podem apresentar-se na forma trigonométrica:

$$\alpha_{2,3} = 1 \left(\cos \frac{\pi}{3} \pm i \sin \frac{\pi}{3} \right)$$

ou, ainda, na forma de Moivre:

$$\alpha_{2,3}^n = \rho^n \left(\cos \frac{n\pi}{3} \pm i \sin \frac{n\pi}{3} \right),$$

com $\rho = 1$. Como consequência, a solução geral da equação de recorrência toma a forma

$$\begin{aligned} a_n &= C_1 \alpha_1^n + C_2 \rho^n (\cos \frac{n\pi}{3} + i \sin \frac{n\pi}{3}) + C_3 \rho^n (\cos \frac{n\pi}{3} - i \sin \frac{n\pi}{3}) \\ &= C_1 \alpha_1^n + (C_2 + C_3) \rho^n \cos \frac{n\pi}{3} + (C_2 - C_3) i \rho^n \sin \frac{n\pi}{3} \\ &= C_1 \alpha_1^n + C_{23}^+ \rho^n \cos \frac{n\pi}{3} + C_{23}^- \rho^n \sin \frac{n\pi}{3} \\ &= C_1 + C_{23}^+ \cos \frac{n\pi}{3} + C_{23}^- \sin \frac{n\pi}{3}, \end{aligned}$$

onde $C_{23}^+ = C_2 + C_3$ e $C_{23}^- = (C_2 - C_3)i$.

Tendo em conta as condições iniciais, podemos calcular as constantes resolvendo o sistema de equações lineares:

$$\begin{cases} 0 = C_1 + C_{23}^+ \\ 1 = C_1 + \frac{1}{2}C_{23}^+ + \frac{\sqrt{3}}{2}C_{23}^- \\ 2 = C_1 - \frac{1}{2}C_{23}^+ + \frac{\sqrt{3}}{2}C_{23}^- \end{cases}$$

a partir do qual se obtém $C_1 = 1$, $C_{23}^+ = -1$ e $C_{23}^- = \frac{\sqrt{3}}{3}$. Logo, podemos concluir que a solução final é

$$a_n = 1 - \cos \frac{n\pi}{3} + \frac{\sqrt{3}}{3} \sin \frac{n\pi}{3}.$$

□

5.3. Equações de recorrência lineares não homogéneas

Definição 5.4 (Equação de recorrência linear não homogénea). *As equações de recorrência lineares não homogéneas são da forma*

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \cdots - c_r a_{n-r} = f(n), \quad (5.17)$$

onde $f(n)$, que se designa por segundo membro, é uma função não nula, ou seja, é tal que $f(n) \neq 0$, para pelo menos um número natural n .

Neste caso, a solução geral toma a forma

$$a_n = a_n^{(1)} + a_n^{(2)},$$

onde $a_n^{(1)}$ é a solução geral da equação de recorrência homogénea

$$a_n^{(1)} = c_1 a_{n-1}^{(1)} + c_2 a_{n-2}^{(1)} + \cdots + c_r a_{n-r}^{(1)}, \quad (5.18)$$

a qual pode ser resolvida pelos métodos apresentados na secção anterior.

A função $a_n^{(2)}$ é uma solução particular da equação (5.17). Porém, infelizmente, não existe um método geral para a determinação de soluções particulares, restando algumas técnicas que se podem aplicar com êxito a certos casos específicos. No que se segue, apresenta-se o designado *método de previsão* da solução (aplicável com êxito em certos casos), o qual decorre da dependência da solução particular em relação ao segundo membro. Esta descrição será feita, unicamente, para os casos mais importantes.

- Se o segundo membro é um polinómio (na variável n) de grau k e a solução geral da equação homogénea não tem um termo polinomial (o que equivale a afirmar que 1 não é raiz da equação característica correspondente a (5.18)) então existe uma solução particular que também é um polinómio de grau k (note-se que uma constante é um polinómio de grau 0). A determinação de uma solução particular é um pouco mais complicada quando a solução geral da equação homogénea tem um termo polinomial (em n) de grau $s - 1$ (o que significa que 1 é raiz de multiplicidade s da equação característica). Neste caso, existe uma solução particular que é o produto de x^s por um polinómio de ordem k . Em qualquer dos casos, sendo $f(n)$ um polinómio de ordem $k \in \mathbb{N}_0$, uma solução particular da equação de recorrência linear não homogénea vem dada por

$$a_n^{(2)} = A_0 n^s + A_1 n^{s+1} + \cdots + A_k n^{s+k},$$

onde $s \in \mathbb{N}_0$ é a multiplicidade de 1 enquanto raiz da equação característica (caso não seja raiz a multiplicidade é $s = 0$) e A_0, \dots, A_k , são constantes a determinar pelas condições iniciais.

- Se $f(n)$ é uma função exponencial na base b , $b \neq 1$ e não é uma raiz da equação característica correspondente a (5.18), então existe uma solução particular que é o produto de uma constante por uma função exponencial com a mesma base (por exemplo, se $f(n) = 2 \cdot 3^n$, então $a_n^{(2)} = A 3^n$, em que A é uma constante a determinar pelas condições iniciais, é uma solução particular). No caso geral, em que $f(n) = cb^n$, c é uma constante não nula e se admite que a base b da função exponencial (com $b \neq 1$) é uma raiz de multiplicidade p da equação característica (caso não seja raiz, a multiplicidade é $p = 0$), existe uma solução particular da forma

$$a_n^{(2)} = A n^p b^n.$$

- Se o segundo membro é soma de várias funções para as quais é possível prever as respectivas soluções particulares, ou seja, se $f(n) = f_1(n) + \cdots + f_k(n)$ e $a_{n,j}^{(2)}, j = 1, \dots, k$ são soluções particulares das equações de recorrência lineares não homogéneas $a_n - c_1 a_{n-1} - \cdots - c_r a_{n-r} = f_j(n), j = 1, \dots, k$, então

$$a_n^{(2)} = a_{n,1}^{(2)} + \cdots + a_{n,k}^{(2)},$$

é uma solução particular da equação (5.17).

Conhecem-se outras formas para a solução particular de outros tipos de segundo membro (por exemplo funções trigonométricas), porém, neste texto apenas abordaremos os tipos anteriormente referidos.

Seguem-se alguns exemplos de aplicação.

Exemplo 5.10. Vamos resolver a equação de recorrência

$$a_n = 7a_{n-1} - 10a_{n-2} + 3^n, \quad (5.19)$$

cujas condições iniciais são $a_0 = 0$ e $a_1 = 1$.

Solução. Em primeiro lugar, conclui-se que a equação homogénea

$$a_n^{(1)} = 7a_{n-1}^{(1)} - 10a_{n-2}^{(1)},$$

tem a equação característica

$$x^2 - 7x + 10 = 0.$$

Esta equação tem duas raízes $\alpha_1 = 2$ e $\alpha_2 = 5$, pelo que a solução geral da equação homogénea é

$$a_n^{(1)} = C_1 2^n + C_2 5^n.$$

Uma vez que o segundo membro da equação de recorrência linear não homogénea que corresponde à equação (5.19) é igual a 3^n e 3 não é uma raiz da equação característica, podemos prever a existência da solução particular

$$a_n^{(2)} = A 3^n.$$

Posteriormente, procedendo à substituição de a_k , para $k = n, n-1, n-2$, na equação (5.19), de acordo com a igualdade anterior, obtém-se

$$A 3^n = 7A 3^{n-1} - 10A 3^{n-2} + 3^n.$$

Dividindo esta equação por 3^n , vem

$$A = \frac{7}{3}A - \frac{10}{9}A + 1,$$

onde, finalmente, se conclui que $A = -9/2$ e que a solução particular é

$$a_n^{(2)} = -\frac{9}{2} 3^n.$$

Logo, podemos concluir que a solução geral da equação (5.19) toma a forma

$$a_n = a_n^{(1)} + a_n^{(2)} = C_1 2^n + C_2 5^n - \frac{9}{2} 3^n,$$

onde as constantes têm os valores $C_1 = 8/3$ e $C_2 = 11/6$ que foram determinados a partir das condições iniciais. Assim, chegamos à solução final

$$a_n = \frac{8}{3} 2^n + \frac{11}{6} 5^n - \frac{9}{2} 3^n. \quad \square$$

Exemplo 5.11. Vamos determinar a solução geral da equação de recorrência

$$a_n = 3a_{n-1} - 2a_{n-2} + 2^n. \quad (5.20)$$

Solução. Considerando a equação homogénea associada a (5.20)

$$a_n^{(1)} = 3a_{n-1}^{(1)} - 2a_{n-2}^{(1)},$$

obtém-se a equação característica

$$x^2 - 3x + 2 = 0,$$

cujas raízes são $\alpha_1 = 1$ e $\alpha_2 = 2$. Como consequência, conclui-se que a solução geral da equação homogénea é

$$a_n^{(1)} = C_1 + C_2 2^n.$$

No que diz respeito à determinação das soluções particulares, tendo em conta que o segundo membro da equação de recorrência linear não homogénea que corresponde à equação (5.20) é a função exponencial 2^n , cuja base 2 é uma raiz de multiplicidade um da equação característica, podemos prever a existência da solução particular

$$a_n^{(2)} = An 2^n.$$

Procedendo à respectiva substituição na equação (5.20), obtém-se a equação

$$An 2^n = 3A(n-1) 2^{n-1} - 2A(n-2) 2^{n-2} + 2^n$$

que, dividida por 2^n , toma a forma

$$An = An - \frac{1}{2}A + 1.$$

Como consequência, obtém-se $A = 2$ e conclui-se, finalmente, que a solução geral da equação (5.20) é

$$a_n = C_1 + C_2 2^n + 2n 2^n. \quad \square$$

Exemplo 5.12. Vamos determinar a solução geral da equação

$$a_n = 2a_{n-1} + 7n^2. \quad (5.21)$$

Solução. A solução geral da equação homogénea $a_n^{(1)} = 2a_{n-1}^{(1)}$ vem dada, imediatamente, por

$$a_n^{(1)} = C_1 2^n.$$

No que diz respeito à determinação de uma solução particular, porém, o trabalho necessário é maior. Com efeito, tendo em conta que o segundo membro da equação de recorrência linear não homogénea que corresponde à equação (5.21) é $7n^2$, podemos prever a existência da solução particular

$$a_n^{(2)} = An^2 + Bn + C.$$

Procedendo à respectiva substituição na equação (5.21), obtém-se

$$An^2 + Bn + C = 2A(n-1)^2 + 2B(n-1) + 2C + 7n^2.$$

Logo, a comparação dos coeficientes das diferentes potências de n conduz-nos ao sistema de equações lineares

$$\begin{cases} A = 2A + 7 \\ B = -4A + 2B \\ C = 2A - 2B + 2C \end{cases}$$

cuja solução é $A = -7$, $B = -28$ e $C = -42$, e da qual decorre, finalmente, a solução geral de equação (5.21), ou seja,

$$a_n = C_1 2^n - 7n^2 - 28n - 42. \quad \square$$

Exemplo 5.13. Sabendo que o número de partições de um conjunto de cardinalidade n em dois subconjuntos não vazios é igual $2^{n-1} - 1$ (de acordo com o Exemplo 3.10), vamos mostrar que o número a_n de partições do conjunto $\{1, 2, \dots, n\}$ em três subconjuntos não vazios é

$$a_n = \frac{1}{6}3^n - \frac{1}{2}2^n + \frac{1}{2},$$

para $n \geq 1$.

Solução. Seja \mathcal{P}_1 o conjunto de partições do conjunto $\{1, 2, \dots, n\}$ tal que um elemento da partição contém o elemento "n" e não contém quaisquer outros elementos e seja \mathcal{P}_2 o conjunto de todas as outras partições. Note-se que existe uma bijecção entre o \mathcal{P}_1 e o conjunto das partições do conjunto $\{1, 2, \dots, n-1\}$ em dois subconjuntos não vazios. Logo, por aplicação do princípio da bijecção, conclui-se que

$$|\mathcal{P}_1| = 2^{n-2} - 1.$$

As partições pertencentes a \mathcal{P}_2 podem ser obtidas a partir das partições do conjunto $\{1, 2, \dots, n-1\}$ em três subconjuntos não vazios, adicionando o elemento n a cada um dos elementos da partição. Como consequência, conclui-se que

$$a_n = |\mathcal{P}_2| + |\mathcal{P}_1| = 3a_{n-1} + 2^{n-2} - 1. \quad (5.22)$$

É claro que $a_1 = a_2 = 0$ e que a equação de recorrência é linear não homogénea. Começando por resolver a equação homogénea que tem a forma

$$a_n^{(1)} = 3a_{n-1}^{(1)},$$

e equação característica $x = 3$, obtém-se a solução geral

$$a_n^{(1)} = C_1 3^n.$$

Uma vez que o segundo membro da equação de recorrência é a soma de uma função exponencial com um polinómio de grau 0, podemos prever que existe uma solução particular da forma

$$a_n^{(2)} = A 2^n + B.$$

Depois da respectiva substituição na equação (5.22) obtém-se a equação

$$A 2^n + B = 3A 2^{n-1} + 3B + 2^{n-2} - 1,$$

que pode tomar a forma

$$A = \frac{3}{2}A + \frac{1}{4}, \quad B = 3B - 1.$$

Logo, conclui-se que $A = -1/2$, $B = 1/2$ e que a solução geral da equação (5.22) é

$$a_n = a_n^{(1)} + a_n^{(2)} = C_1 3^n - \frac{1}{2} 2^n + \frac{1}{2}.$$

Finalmente, a condição inicial $a_1 = 0$ implica $C_1 = 1/6$. □

Deve observar-se que as equações de recorrência desta secção podem também ser resolvidas por outros métodos, utilizando, por exemplo, as funções geradoras a estudar no Capítulo 5.5.

5.4. Equações de recorrência não lineares

As equações de recorrência que não são lineares (homogéneas ou não homogéneas) designam-se por *equações de recorrência não lineares*. Nesta secção, apresentam-se alguns exemplos de equações de recorrência não lineares e respectivos métodos de resolução. Porém, deve observar-se que, tal como anteriormente, não existe nenhum método de aplicação geral para a resolução de equações de recorrência deste tipo.

Exemplo 5.14. Sendo D_n o número de desencontros de uma dada sequência de comprimento n (ver Exemplo 4.18), vamos deduzir uma equação de recorrência para D_n .

Solução. Sem perda de generalidade, vamos determinar o número de desencontros da sequência $(1, 2, \dots, n)$ de comprimento n , começando por partir o conjunto de todos os desencontros em dois subconjuntos.

1. O primeiro conjunto é constituído pelas permutações em que n ocupa a i -ésima posição e i ocupa a n -ésima, para $i = 1, 2, \dots, n-1$. É claro que, fixando i , existem D_{n-2} desencontros deste tipo e existem $n-1$ possibilidades para fixar i . Logo, por aplicação do princípio da multiplicação, o número de desencontros deste conjunto é igual a $(n-1)D_{n-2}$.
2. O segundo conjunto contém os restantes desencontros, nos quais i ocupa a n -ésima posição e n não ocupa a posição i . Logo, fixando i , deste conjunto fazem parte todos os desencontros da sequência $(1, 2, \dots, i-1, n, i+1, \dots, n-1)$ aos quais se deve acrescentar i na n -ésima posição. Logo, temos D_{n-1} desencontros deste tipo e, uma vez que existem $n-1$ possibilidades para a escolha de i , neste conjunto existem $(n-1)D_{n-1}$ desencontros.

Assim, temos uma equação de recorrência da forma

$$D_n = (n-1)D_{n-2} + (n-1)D_{n-1}.$$

Para simplificar um pouco, note-se que a equação anterior pode apresentar-se na forma

$$D_n - nD_{n-1} = (n-1)D_{n-2} - D_{n-1},$$

a partir da qual, fazendo

$$a_n = D_n - nD_{n-1}$$

se obtém a equação de recorrência

$$a_n = -a_{n-1}, \quad \text{com} \quad a_2 = D_2 - 2D_1 = 1.$$

Por outro lado, tendo em conta que $a_n = (-1)^n$, para $n \geq 2$, obtém-se a relação final

$$D_n = nD_{n-1} + (-1)^n$$

cuja condição inicial é $D_1 = 0$.

Esta equação será resolvida, utilizando as funções geradoras (ver o Exemplo 5.32). \square

Exemplo 5.15. Seja B_n o número de todas as partições de um conjunto de cardinalidade n em subconjuntos não vazios. Estes números B_n são conhecidos por números de Bell. Vamos deduzir uma equação de recorrência para os números de Bell.

Solução. Para facilitar a notação, vamos determinar uma relação de recorrência para B_{n+1} . Considerando todas as partições do conjunto $\{1, 2, \dots, n+1\}$, é claro que para cada partição existe um subconjunto que contém o elemento $n+1$ e, eventualmente, mais i elementos, com $0 \leq i \leq n$. Assim, fixando i existem $\binom{n}{i}$ subconjuntos do conjunto $\{1, 2, \dots, n\}$ que pertencem ao tipo de subconjuntos anteriormente referidos. Logo, para cada i , o número de partições em que o subconjunto que contém $n+1$ tem cardinalidade $i+1$ é igual a $\binom{n}{i}B_{n-i}$. Como consequência, procedendo à contagem de todas as partições vem

$$B_{n+1} = \sum_{i=0}^n \binom{n}{i} B_{n-i}, \quad \text{para } n \geq 0, \tag{5.23}$$

com condição inicial $B_0 = 1$. Uma vez que, $\binom{n}{i} = \binom{n}{n-i}$, a equação (5.23) pode tomar a forma

$$B_{n+1} = \sum_{i=0}^n \binom{n}{i} B_i.$$

Tal como no Exemplo 5.14, esta equação será resolvida na Capítulo 5.5 (ver o Exemplo 5.34). \square

Um dos métodos muito utilizados para a resolução de equações de recorrência não lineares consiste numa mudança adequada de variáveis, tendo em vista a simplificação da respectiva equação. Seguem-se alguns exemplos de aplicação deste método.

Exemplo 5.16. Vamos resolver a equação de recorrência não linear

$$a_n^2 = 2a_{n-1}^2 + 1, \tag{5.24}$$

com a condição inicial $a_0 = 2$ (assumindo-se $a_n \geq 0$, para todo o n).

Solução. Note-se que, procedendo à substituição de variáveis $b_n = a_n^2$, a equação de recorrência não linear (5.24) transforma-se na equação de recorrência linear não homogénea definida pela equação

$$b_n = 2b_{n-1} + 1, \quad (5.25)$$

com condição inicial $b_0 = a_0^2 = 4$. Utilizando os métodos da Secção 5.3 podemos resolver a equação homogénea associada $b_n^{(1)} = 2b_{n-1}^{(1)}$, cuja solução geral é

$$b_n^{(1)} = C_1 2^n.$$

Uma vez que o segundo membro da equação de recorrência linear não homogénea que corresponde à equação (5.25) é igual 1 (que é um polinómio de grau 0), podemos concluir que existe uma solução particular da forma $b_n^{(2)} = A$. Logo, tendo em conta a equação (5.25), vem

$$A = 2A + 1 \Leftrightarrow A = -1.$$

Finalmente, obtém-se a solução geral da equação (5.25) na forma

$$b_n = C_1 2^n - 1,$$

a partir da qual, tendo em conta que a condição inicial implica $C_1 = 5$, se obtém a solução final

$$a_n = \sqrt{5 \cdot 2^n - 1}. \quad \square$$

Exemplo 5.17. Vamos resolver a equação de recorrência não linear

$$a_n^2 - 2a_{n-1} = 0,$$

com condição inicial $a_0 = 4$ (assumindo-se $a_n > 0$, para todo o n).

Solução. Aplicando logaritmos (na base 2) a ambos os lados da equação $a_n^2 = 2a_{n-1}$, obtém-se

$$\log_2 a_n^2 = \log_2 (2a_{n-1}) \Leftrightarrow 2 \log_2 a_n = 1 + \log_2 a_{n-1}.$$

Procedendo à mudança de variável $b_n = \log_2 a_n$, obtém-se a equação de recorrência linear não homogénea definida pela equação

$$2b_n = b_{n-1} + 1, \quad (5.26)$$

com condição inicial $b_0 = \log_2 a_0 = 2$. Logo, a equação homogénea associada $2b_n^{(1)} = b_{n-1}^{(1)}$ tem a solução geral

$$b_n^{(1)} = C_1 2^{-n}.$$

Uma vez que o segundo membro da equação de recorrência linear não homogénea que corresponde à equação (5.26) é igual 1 (que é um polinómio de grau 0), existe uma solução particular da equação (5.26) da forma $b_n^{(2)} = A$, a partir da qual se obtém

$$2A = A + 1 \Leftrightarrow A = 1.$$

Como consequência, a solução geral da equação (5.26) toma a forma

$$b_n = C_1 2^{-n} + 1,$$

onde a condição inicial implica $C_1 = 1$. Finalmente, vem

$$b_n = 2^{-n} + 1$$

onde, voltando às variáveis iniciais, se obtém a solução final

$$a_n = 2^{b_n} = 2 \cdot 2^{-n}. \quad \square$$

Exemplo 5.18. Vamos resolver a equação de recorrência não linear

$$a_n = \sqrt{a_{n-1} + \sqrt{a_{n-2} + \sqrt{a_{n-3} + \sqrt{\dots \sqrt{a_0}}}}}, \quad (5.27)$$

com condição inicial $a_0 = 4$.

Solução. Elevando ao quadrado ambos os membros da equação (5.27), para $n \geq 2$, obtém-se

$$a_n^2 = a_{n-1} + \sqrt{a_{n-2} + \sqrt{a_{n-3} + \sqrt{\dots \sqrt{a_0}}}} = a_{n-1} + a_{n-1} = 2a_{n-1}$$

e, para $n = 1$, obtém-se $a_1^2 = a_0$. Uma vez que é imediato concluir que $a_1 = 2$, vamos considerar apenas os casos em que $n \geq 2$, para os quais se obtém a equação de recorrência

$$a_n^2 = 2a_{n-1},$$

com condição inicial $a_1 = 2$. Tendo em conta que esta equação de recorrência é idêntica à equação de recorrência do Exemplo 5.17, embora com uma condição inicial distinta, vamos proceder à respectiva resolução sem detalhes.

Efectuando a mudança de variável $b_n = \log_2 a_n$, obtém-se a equação de recorrência linear

$$2b_n = b_{n-1} + 1,$$

com condição inicial $b_1 = \log_2 a_1 = 1$, cuja solução geral vem dada por

$$b_n = C_1 2^{-n} + 1.$$

Uma vez que a condição inicial implica $C_1 = 0$, conclui-se que

$$b_n = 1,$$

ou seja, voltando às variáveis iniciais,

$$a_n = 2^{b_n} = 2.$$

Como consequência, para todos os valores de $n \geq 0$, a solução final é $a_0 = 4$ e $a_n = 2$ para $n \geq 1$. \square

5.5. Funções geradoras

Trabalhar com sucessões de números inteiros e com relações de recorrência é uma tarefa, muitas vezes, difícil que requer a utilização de várias ferramentas específicas. Algumas destas ferramentas são disponibilizadas pela análise matemática, como são o caso das usualmente utilizadas no estudo das funções reais e complexas. Nesta secção, introduz-se o conceito de função geradora, com o objectivo de se obterem conclusões de natureza combinatória a partir de certas propriedades analíticas. Para tal, vamos recorrer ao estudo de funções de *variável formal*, entendendo-se por variável formal todo o símbolo, sem significado específico, utilizado, simplesmente, para manipulação algébrica.

Por exemplo, a determinação do número de escolhas de quatro letras de um conjunto com uma letra A , duas letras B , três letras C e quatro letras D (independentemente da ordem com que as letras são escolhidas), pode ser feita recorrendo ao produto

$$(1 + A)(1 + B + B^2)(1 + C + C^2 + C^3)(1 + D + D^2 + D^3 + D^4), \quad (5.28)$$

tendo em conta que no respectivo desenvolvimento o número destas escolhas corresponde ao número de termos do tipo $A^i B^j C^k D^l$, com $i + j + k + l = 4$. Note-se que o termo AC^2D corresponde à escolha da letra A , duas letras C e uma letra D . Logo, substituindo em (5.28) as letras A , B , C e D pela variável x e desenvolvendo o produto de factores obtido, podemos concluir que o coeficiente de x^4 corresponde precisamente ao número pretendido.

Para facilitar a multiplicação de polinómios podemos trabalhar directamente com os seus coeficientes, conforme a seguir se exemplifica.

Exemplo 5.19. Vamos multiplicar o polinómio $2 + 3x + x^2$ pelo polinómio $1 + 5x$.

Solução.

$$\begin{array}{r} & 2 & 3 & 1 \\ \times & 1 & 5 \\ \hline & 2 & 3 & 1 \\ & 10 & 15 & 5 \\ \hline & 2 & 13 & 16 & 5 \end{array}$$

Como consequência,

$$(1 + 5x)(2 + 3x + x^2) = 2 + 13x + 16x^2 + 5x^3.$$

□

Aplicando o procedimento utilizado no Exemplo 5.19 ao produto de factores

$$(1 + x)(1 + x + x^2)(1 + x + x^2 + x^3)(1 + x + x^2 + x^3 + x^4),$$

vem

$$\begin{array}{r} & 1 & 1 & 1 \\ \times & 1 & 1 \\ \hline & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ \hline & 1 & 2 & 2 & 1 \end{array} \quad \begin{array}{r} & 1 & 2 & 2 & 1 \\ \times & 1 & 1 & 1 & 1 \\ \hline & 1 & 2 & 2 & 1 \\ & 1 & 2 & 2 & 1 \\ & 1 & 2 & 2 & 1 \\ \hline & 1 & 3 & 5 & 6 & 5 & 3 & 1 \end{array}$$

$$\begin{array}{r} & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ \times & 1 & 1 & 1 & 1 & 1 \\ \hline & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ & 1 & 3 & 5 & 6 & 5 & 3 & 1 \\ \hline & 1 & 4 & 9 & 15 & 20 & 23 & 24 & 23 & 20 & 15 & 9 & 4 & 1 \end{array}$$

obtendo-se o polinómio

$$1 + 4x + 9x^2 + 15x^3 + 20x^4 + 23x^5 + 24x^6 + 23x^7 + 20x^8 + 15x^9 + 9x^{10} + 4x^{11} + x^{12}.$$

5.5.1 Séries formais de potências

Definição 5.5 (Série formal de potências). Seja a_0, a_1, a_2, \dots uma sucessão de números e x um variável formal. Então a expressão

$$\mathcal{A}(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{n=0}^{\infty} a_n x^n \tag{5.29}$$

designa-se por série formal de potências de x com coeficientes a_0, a_1, a_2, \dots .

Note-se que, em geral, $\mathcal{A}(x)$ não só não é uma função como não se pode determinar para certos valores de x . Porém, quando o *raio de convergência da série* $R_{\mathcal{A}}$ é positivo (isto é, $R_{\mathcal{A}} > 0$), encarando x como uma variável real (ou complexa) podemos concluir que a série converge para todo o x tal que $|x| < R_{\mathcal{A}}$. Nesse caso, podemos considerar $\mathcal{A}(x)$ como uma função de variável real (ou complexa). Se tal acontece, então todas as operações sobre séries formais de potências (a definir mais adiante) são coerentes com as respectivas operações sobre séries de potências, bem como com as respectivas operações sobre funções.

No entanto, convém realçar que o recurso à utilização de séries formais em combinatória não pressupõe a utilização dos valores que eventualmente estas funções possam tomar, tratando-se apenas de escrever as sucessões e as operações sobre sucessões de modo mais expediente.

No que se segue, vamos utilizar algumas séries de potências bem conhecidas da análise matemática, como sejam,

$$1 + x + x^2 + \dots = \sum_{k=0}^{\infty} x^k = \frac{1}{1-x}, \quad (5.30)$$

$$1 + nx + \frac{n(n+1)}{2}x^2 + \dots = \sum_{k=0}^{\infty} \binom{k+n-1}{k} x^k = \frac{1}{(1-x)^n}, \quad (5.31)$$

$$1 + \alpha x + \frac{(\alpha)_2}{2}x^2 + \dots = \sum_{k=0}^{\infty} \frac{(\alpha)_k}{k!} x^k = (1+x)^\alpha, \quad (5.32)$$

$$1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x. \quad (5.33)$$

Note-se que o coeficiente factorial $(\alpha)_k$ que aparece na expressão (5.32) corresponde à sua forma mais geral, com $\alpha \in \mathbb{R}$, a qual será definida no capítulo seguinte. Note-se ainda que as expressões obtidas pressupõem que a variável x toma valores dentro dos respectivos domínios de convergência. Nestas condições, em particular, considerando os primeiros n termos da série (5.30), obtém-se

$$1 + x + x^2 + \dots + x^n = \sum_{k=0}^n x^k = \frac{1 - x^{n+1}}{1 - x}. \quad (5.34)$$

Exemplo 5.20. Vamos analisar as séries formais de potências associadas às sucessões $(a_n)_{n \in \mathbb{N}_0}$, $(b_n)_{n \in \mathbb{N}_0}$ e $(c_n)_{n \in \mathbb{N}_0}$, tais que $a_n = n!$, $b_n = 2^n$ e $c_n = 1/n!$, para $n \in \mathbb{N}_0$.

Solução. Designem-se por \mathcal{A} , \mathcal{B} e \mathcal{C} as séries formais de potências associadas, respectivamente, às sucessões $(a_n)_{n \in \mathbb{N}_0}$, $(b_n)_{n \in \mathbb{N}_0}$ e $(c_n)_{n \in \mathbb{N}_0}$. Para cada uma destas sucessões, vamos determinar a respectiva série formal de potências, bem como o seu raio de convergência.

(a) Uma vez que

$$\mathcal{A}(x) = 1 + x + 2x^2 + \dots = \sum_{n=0}^{\infty} n!x^n,$$

o raio de convergência desta série é $R_{\mathcal{A}} = 0$. Então a função $\mathcal{A}(x)$ tem significado, apenas, para $x = 0$ e $\mathcal{A}(0) = 1$. Note-se, porém, que considerando $\mathcal{A}(x)$ como uma função, perdemos toda a informação sobre os termos de $(a_n)_{n \in \mathbb{N}_0}$. Logo, torna-se conveniente interpretar $\mathcal{A}(x)$ como uma série formal de potências.

(b) Uma vez que

$$\mathcal{B}(x) = 1 + 2x + 4x^2 + \dots = \sum_{n=0}^{\infty} 2^n x^n,$$

o raio de convergência desta série é $R_B = \frac{1}{2}$ (compare com a fórmula (5.30)). Então $\mathcal{B}(x)$ pode ser interpretada como uma função no intervalo $|x| < \frac{1}{2}$, no qual se obtém

$$\mathcal{B}(x) = \frac{1}{1-2x}.$$

Assim, neste caso, podemos interpretar $\mathcal{B}(x)$ como uma função ou como uma série formal de potências.

(c) Uma vez que

$$\mathcal{C}(x) = 1 + x + \frac{1}{2}x^2 + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

o raio de convergência desta série é $R_C = \infty$. Então, pela fórmula (5.33), podemos interpretar $\mathcal{C}(x)$ como uma função definida em \mathbb{R} (ou em \mathbb{C}), para a qual se obtém a expressão

$$\mathcal{C}(x) = e^x.$$

Assim, tal como anteriormente, podemos interpretar $\mathcal{C}(x)$ como uma função ou como uma série formal de potências. \square

Seguem-se algumas definições de operações sobre séries formais de potências que são coerentes com as respectivas operações sobre funções, quando as séries formais podem ser interpretadas como tal.

Definição 5.6 (Soma e produto de séries formais de potências). *Dadas as séries formais de potências*

$$\begin{aligned}\mathcal{A}(x) &= a_0 + a_1x + a_2x^2 + \dots = \sum_{n=0}^{\infty} a_n x^n, \\ \mathcal{B}(x) &= b_0 + b_1x + b_2x^2 + \dots = \sum_{n=0}^{\infty} b_n x^n,\end{aligned}$$

designa-se por soma destas séries a série formal de potências

$$\mathcal{A}(x) + \mathcal{B}(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots = \sum_{n=0}^{\infty} (a_n + b_n)x^n$$

e designa-se por produto a série formal de potências

$$\mathcal{A}(x)\mathcal{B}(x) = c_0 + c_1x + c_2x^2 + \dots = \sum_{n=0}^{\infty} c_n x^n,$$

$$\text{onde } c_n = a_0b_n + a_1b_{n-1} + \dots + a_{n-1}b_1 + a_nb_0 = \sum_{k=0}^n a_k b_{n-k}.$$

É claro que as operações de soma e produto de séries formais de potências são operações comutativas e associativas. Vamos mostrar que a multiplicação de uma série formal de potências por um número é um caso particular do produto de séries formais.

Exemplo 5.21. *Vamos calcular o produto $c\mathcal{A}(x)$, onde c é um número fixo e $\mathcal{A}(x)$ é uma série formal de potências definida por*

$$\mathcal{A}(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{n=0}^{\infty} a_n x^n.$$

Solução. Uma vez que podemos interpretar a constante c como sendo a série formal de potências

$$c = \mathcal{B}(x) = \sum_{n=0}^{\infty} b_n x^n, \quad \text{com } b_0 = c \text{ e } b_k = 0, \text{ para } k > 0,$$

então, de acordo com a Definição 5.6,

$$c\mathcal{A}(x) = \mathcal{A}(x)\mathcal{B}(x) = \sum_{n=0}^{\infty} c_n x^n,$$

onde $c_n = a_0 \cdot 0 + a_1 \cdot 0 + \cdots + a_{n-1} \cdot 0 + a_n \cdot c = ca_n$. Como consequência,

$$c\mathcal{A}(x) = ca_0 + ca_1 x + ca_2 x^2 + \cdots = \sum_{n=0}^{\infty} ca_n x^n. \quad \square$$

Definição 5.7 (Substituição de séries formais de potências). *Dadas as séries formais de potências*

$$\begin{aligned} \mathcal{A}(x) &= a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n, \\ \mathcal{B}(x) &= b_0 + b_1 x + b_2 x^2 + \cdots = \sum_{n=0}^{\infty} b_n x^n, \end{aligned}$$

a última das quais é tal que $\mathcal{B}(0) = b_0 = 0$, designa-se por substituição de x por $\mathcal{B}(x)$ na série $\mathcal{A}(x)$, a série formal de potências

$$\mathcal{A}(\mathcal{B}(x)) = c_0 + c_1 x + c_2 x^2 + \cdots = \sum_{n=0}^{\infty} c_n x^n,$$

onde os coeficientes c_n são definidos por

$$\mathcal{A}(\mathcal{B}(x)) = a_0 + a_1 \mathcal{B}(x) + a_2 \mathcal{B}^2(x) + \cdots = \sum_{n=0}^{\infty} a_n \mathcal{B}^n(x).$$

o que implica que se tenha

$$\begin{aligned} c_0 &= a_0, \\ c_1 &= a_1 b_1, \\ c_2 &= a_1 b_2 + a_2 b_1^2, \\ c_3 &= a_1 b_3 + 2a_2 b_1 b_2 + a_3 b_1^3, \end{aligned}$$

etc.

Exemplo 5.22. Dada a série formal de potências

$$\mathcal{A}(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n,$$

vamos calcular $\mathcal{A}(-x)$.

Solução. Interpretando $-x$ como uma série formal de potências, ou seja,

$$-x = \mathcal{B}(x) = \sum_{n=0}^{\infty} b_n x^n, \quad \text{com } b_1 = -1 \text{ e } b_k = 0, \text{ para } k \neq 1,$$

de acordo com a Definição 5.7, vem

$$\mathcal{A}(-x) = \mathcal{A}(\mathcal{B}(x)) = \sum_{n=0}^{\infty} c_n x^n,$$

onde $a_n \mathcal{B}^n(x) = (-1)^n a_n x^n$. Finalmente, conclui-se que

$$\mathcal{A}(-x) = a_0 - a_1 x + a_2 x^2 - \cdots = \sum_{n=0}^{\infty} (-1)^n a_n x^n.$$

□

Definição 5.8 (Derivada e integral de uma série formal de potências). *Dada a série formal de potências*

$$\mathcal{A}(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n,$$

designa-se por derivada de $\mathcal{A}(x)$ a série formal de potências

$$\mathcal{A}'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n,$$

e designa-se por integral de $\mathcal{A}(x)$, a série formal de potências

$$\int \mathcal{A}(x) = a_0 x + \frac{a_1}{2} x^2 + \frac{a_2}{3} x^3 + \cdots = \sum_{n=1}^{\infty} \frac{a_{n-1}}{n} x^n.$$

Note-se que se a série formal de potências converge, então o seu integral é coerente com o integral usual, tal como a seguir se indica

$$\int \mathcal{A}(x) = \int_0^x \mathcal{A}(t) dt.$$

Por outro lado, as operações de derivação e integração de séries formais de potências são operações inversas uma da outra, ou seja,

$$\left(\int \mathcal{A}(x) \right)' = \mathcal{A}(x).$$

Exemplo 5.23. Vamos determinar as séries formais de potências para as sucessões $(a_k)_{k \in \mathbb{N}}$ e $(b_k)_{k \in \mathbb{N}}$, tais que $a_k = k$ e $b_k = \frac{1}{k}$, para $k \in \mathbb{N}$.

Solução. Tendo em conta a definição de série formal de potências

$$\mathcal{A}(x) = \sum_{k=1}^{\infty} k x^k = x \sum_{k=1}^{\infty} k x^{k-1} = x \left(\sum_{k=1}^{\infty} x^k \right)'$$

e utilizando fórmula (5.30), vem

$$\mathcal{A}(x) = x \left(\frac{x}{1-x} \right)' = \frac{x}{(1-x)^2}.$$

De um modo semelhante se conclui que

$$\mathcal{B}(x) = \sum_{k=1}^{\infty} \frac{1}{k} x^k = \int \left(\sum_{k=1}^{\infty} x^{k-1} \right) = \int \left(\sum_{k=0}^{\infty} x^k \right).$$

Logo, de acordo com a fórmula (5.30),

$$\mathcal{B}(x) = \int \frac{1}{1-x} = \int_0^x \frac{dt}{1-t} = -\ln(1-x).$$

□

5.5.2 Funções geradoras ordinária e exponencial

Seguem-se algumas definições e propriedades básicas associadas às funções geradoras. Observe-se que cada sequência finita a_1, a_2, \dots, a_n pode ser também considerada como uma sucessão infinita $a_1, a_2, \dots, a_n, 0, 0, \dots$

Definição 5.9 (Função geradora ordinária). *Se a_0, a_1, a_2, \dots é uma sucessão de números, então designa-se por função geradora ou função geradora ordinária da sucessão $(a_k)_{k \in \mathbb{N}_0}$, a série formal de potências*

$$f(x) = \sum_{k=0}^{\infty} a_k x^k. \quad (5.35)$$

Por exemplo, considerando a função geradora ordinária da sucessão de Fibonacci 1, 1, 2, 3, 5, 8, ..., ou seja, $f(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 \dots$, uma vez que

$$\begin{aligned} (x + x^2)f(x) &= x^2 + x^3 + 2x^4 + 3x^5 + 5x^6 + 8x^7 + \dots \\ &\quad + x^3 + x^4 + 2x^5 + 3x^6 + 5x^7 + \dots \\ &= x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + \dots \end{aligned}$$

obtém-se $(x + x^2)f(x) = f(x) - x \Leftrightarrow f(x) = \frac{x}{1-x-x^2}$.

Definição 5.10 (Função geradora exponencial). *Se a_0, a_1, a_2, \dots é uma sucessão de números, então designa-se por função geradora exponencial da sucessão $(a_k)_{k \in \mathbb{N}_0}$, a série formal de potências*

$$f(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}. \quad (5.36)$$

Por exemplo, considerando a sucessão n^k , com $k = 0, 1, 2, \dots$, onde cada termo determina o número de arranjos com repetição de n objectos k a k , a correspondente função geradora exponencial vem dada por

$$f(x) = \sum_{k=0}^{\infty} n^k \frac{x^k}{k!} = e^{nx}.$$

Quando, a partir de uma certa ordem, os termos da sucessão são todos iguais a zero, a função geradora ordinária (exponencial) designa-se por *polinómio gerador* ordinário (exponencial). Por exemplo, se $a_k = \binom{n}{k}$, com $k = 0, 1, \dots, n$, e $a_{n+1} = a_{n+2} = \dots = 0$, então obtém-se o polinómio gerador ordinário

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

Assim, podemos concluir que o binómio de Newton $(1+x)^n$ é o polinómio gerador ordinário para a sequência $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}$, onde cada termo é o número de combinações de n objectos k a k , para $k = 0, \dots, n$. Por outro lado, uma vez que

$$(1+x)^n = \sum_{k=0}^n (n)_k \frac{x^k}{k!},$$

$(1+x)^n$ é também o polinómio gerador exponencial para a sequência $(n)_k$, com $k = 0, \dots, n$, onde cada termo determina o número de arranjos de n objectos k a k .

Seguem-se alguns exemplos de utilização de polinómios geradores e de funções geradoras na contagem de objectos combinatórios.

Exemplo 5.24. Vamos determinar o número de possibilidades de colocação de quatro bolas iguais em cinco caixas numeradas, de tal forma que cada uma das três primeiras caixas tem no máximo uma bola e cada uma das restantes contém no máximo duas bolas.

Solução. Considere o polinómio $f(x) = (1+x)^3(1+x+x^2)^2$, o qual pode apresentar a forma:

$$f(x) = (x^0 + x^1)(x^0 + x^1)(x^0 + x^1)(x^0 + x^1 + x^2)(x^0 + x^1 + x^2). \quad (5.37)$$

Note-se que, desenvolvendo a expressão obtida para $f(x)$, se obtém uma soma onde cada termo é um produto com factores pertencentes a cada uma das adições (entre parêntesis) de (5.37). Como consequência, o coeficiente do termo obtido para x^4 é igual ao número de soluções inteiras não negativas da equação:

$$e_1 + e_2 + e_3 + e_4 + e_5 = 4,$$

onde e_i denota a potência da variável escolhida no i -ésimo factor na determinação de um dos termos relativos a x^4 . Isto implica que se tenha $e_1, e_2, e_3 \in \{0, 1\}$ e $e_4, e_5 \in \{0, 1, 2\}$. Logo, podemos concluir que existe uma bijecção entre as possíveis colocações das bolas nas caixas e as soluções desta equação. Assim, uma vez que o coeficiente de x^4 no desenvolvimento obtido para $f(x)$ é igual ao número de possibilidades de colocação das bolas nas caixas, sendo

$$f(x) = 1 + 5x + 12x^2 + 18x^3 + 18x^4 + 12x^5 + 5x^6 + x^7,$$

conclui-se que existem 18 possibilidades para as colocações pretendidas. \square

Exemplo 5.25. Vamos determinar o polinómio gerador ordinário para a sequência $(a_r)_{1 \leq r \leq 12}$, onde a_r é o número de possibilidades de escolha de r bolas de entre três bolas verdes, três brancas, três azuis e três pretas.

Solução. É imediato concluir que a_r corresponde ao número de soluções inteiras não negativas da equação

$$e_1 + e_2 + e_3 + e_4 = r,$$

onde e_i denota o número de bolas escolhidas com a cor i . Logo, $0 \leq e_i \leq 3$ e, tal como anteriormente, o número de soluções é igual ao coeficiente de x^r na expressão

$$(x^0 + x^1 + x^2 + x^3)(x^0 + x^1 + x^2 + x^3)(x^0 + x^1 + x^2 + x^3)(x^0 + x^1 + x^2 + x^3).$$

Como consequência, o polinómio gerador da sequência (a_r) é igual

$$f(x) = (1 + x + x^2 + x^3)^4. \quad \square$$

Exemplo 5.26. Vamos determinar a função geradora para a sucessão $(a_k)_{k \in \mathbb{N}}$, onde a_k é o número de possibilidades de colocação de k bolas iguais em cinco caixas numeradas, de tal forma que cada uma das duas primeiras caixas contém um número par de bolas e cada uma das restantes contém entre três e cinco bolas.

Solução. Uma vez que a_k é igual ao número de soluções inteiras não negativas da equação

$$e_1 + e_2 + e_3 + e_4 + e_5 = k,$$

onde e_1, e_2 tomam apenas valores pares e $3 \leq e_3, e_4, e_5 \leq 5$, pode concluir-se que

$$f(x) = (1 + x^2 + x^4 + x^6 + \dots)^2(x^3 + x^4 + x^5)^3. \quad \square$$

Exemplo 5.27. Vamos calcular o número de possibilidade de colocação de 25 bolas idênticas em sete caixas numeradas, de tal forma que a primeira caixa tenha no máximo dez bolas.

Solução. Para efectuar este cálculo basta determinar o coeficiente de x^{25} na função geradora

$$h(x) = (1 + x + x^2 + \dots + x^{10})(1 + x + x^2 + \dots)^6.$$

Tendo em conta a expressão (5.34), vem

$$\begin{aligned} f(x) &= 1 + x + x^2 + \dots + x^{10} = \frac{1 - x^{11}}{1 - x}, \\ g(x) &= (1 + x + x^2 + \dots)^6 = \frac{1}{(1 - x)^6} \end{aligned}$$

e, consequentemente,

$$h(x) = f(x)g(x) = (1 - x)^{-7}(1 - x^{11}).$$

Utilizando a expressão (5.31) para $(1 - x)^{-7}$, obtém-se

$$h(x) = \left(1 + \binom{1+7-1}{1}x + \dots + \binom{k+7-1}{k}x^k + \dots\right)(1 - x^{11}).$$

Fazendo $(1 - x)^{-7} = \sum_{n=1}^{\infty} a_n x^n$ e $1 - x^{11} = \sum_{n=1}^{\infty} b_n x^n$, pode concluir-se que o coeficiente de x^{25} em $h(x)$, vem dado por

$$\begin{aligned} \sum_{i=0}^{25} a_i b_{25-i} &= a_{25}b_0 + a_{14}b_{11} \\ &= \binom{25+7-1}{25} \cdot 1 + \binom{14+7-1}{14} \cdot (-1) \\ &= \binom{31}{25} - \binom{20}{14} = 697.521. \end{aligned}$$

□

O exemplo anterior pode ser resolvido sem utilização da função geradora. Com efeito, o número de possibilidades de colocação (sem restrições) de 25 bolas idênticas em sete caixas numeradas é igual a $\binom{25+7-1}{25}$ (compare com o Exemplo 4.13). Porém, a este número é necessário retirar o número de colocações não permitidas que são aquelas que contemplam pelo menos 11 bolas na primeira caixa. Para o cálculo deste número de colocações não permitidas, basta fixar 11 bolas na primeira caixa e distribuir (de todas as maneiras possíveis) as restantes $25 - 11 = 14$ bolas pelas sete caixas, para o que existem $\binom{14+7-1}{14}$ possibilidades.

Muitas vezes, porém, é difícil determinar directamente uma fórmula explícita para os termos de uma sucessão. Em tais casos, a utilização da função geradora ordinária ou exponencial transforma o problema combinatório num problema de análise matemática, o que possibilita o recurso a resultados bem conhecidos da teoria das séries de funções e que, muitas vezes, simplifica o cálculo. Tal como se referiu, embora se possa utilizar tanto a função geradora ordinária como a função geradora exponencial, frequentemente, escolhe-se a função geradora ordinária, uma vez que, geralmente, os seus coeficientes são mais fáceis de manipular. Em certos casos, porém, principalmente quando o raio de convergência da série definida pela função geradora ordinária é zero ou quando não apresenta uma forma compacta conhecida, recorre-se à função geradora exponencial.

Exemplo 5.28. Vamos determinar a função geradora da sucessão $(a_n)_{n \in \mathbb{N}}$, com a_n denotando o número de partições de n em parcelas inteiras positivas (onde a ordem das parcelas não é importante).

Solução. Neste caso, é necessário determinar o número de soluções inteiras positivas da equação

$$1 \cdot x_1 + 2 \cdot x_2 + \dots + k \cdot x_k + \dots + n \cdot x_n = n,$$

para o qual se obtém a função geradora $f(x)$, definida pela expressão:

$$\begin{aligned} f(x) &= (1 + x + x^2 + \dots)(1 + (x^1)^2 + (x^2)^2 + (x^3)^2 + \dots) \\ &\quad \cdots (1 + (x^1)^k + (x^2)^k + (x^3)^k + \dots) \cdots \\ &= \prod_{k=1}^{\infty} (1 + x^k + x^{2k} + x^{3k} + \dots) = \prod_{k=1}^{\infty} \frac{1}{1 - x^k}. \end{aligned}$$

□

5.6. Equações de recorrência e funções geradoras

Seguem-se alguns exemplos de utilização da função geradora para a determinação de soluções de equações de recorrência.

Exemplo 5.29. (Torre de Hanoi) Suponha que tem n discos com diâmetros distintos que se podem colocar em três pilhas e que, inicialmente, todos os discos se encontram numa única pilha dispostos por ordem decrescente dos respectivos diâmetros desde a base até ao topo (ver Figura 5.2). Suponha ainda que os discos só podem ser deslocados para outra pilha desde que se respeitem as seguintes restrições:

1. em cada passo só se pode deslocar um disco;
2. não pode haver discos com diâmetro superior colocados em cima de discos com diâmetro inferior.

Vamos determinar o menor número de passos necessários para transportar os n discos da pilha inicial para outra. (Este problema foi proposto por Edouard Lucas em 1883.)

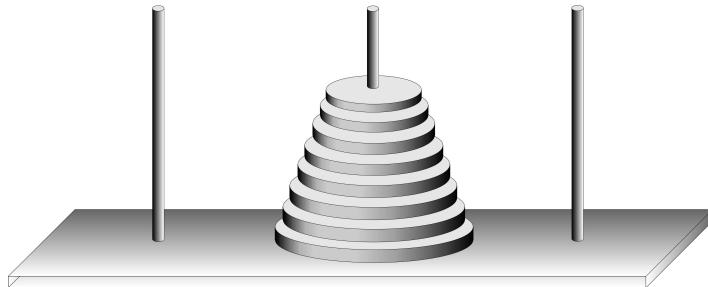


Figura 5.2: Torre de Hanoi.

Solução. Denote-se por a_n o menor número de passos para transportar n discos de uma pilha para outra. Note-se que antes de se transportar o n -ésimo disco (cujo diâmetro é máximo) é necessário transportar o disco de ordem $n - 1$, ou seja, temos de resolver o problema de ordem $n - 1$ que corresponde à determinação de a_{n-1} . Assim, uma vez transportados $n - 1$ discos no menor número de passos a_{n-1} , transportamos o disco com diâmetro máximo para a pilha vazia (num único passo) e, posteriormente, transportamos os restantes $n - 1$ discos para cima dele (em a_{n-1} passos). Logo, para $n \geq 2$, obtém-se a equação de recorrência

$$a_n = 2a_{n-1} + 1,$$

cuja condição inicial é $a_1 = 1$.

Sendo $f(x)$ a função geradora da sucessão $(a_n)_{n \in \mathbb{N}}$, utilizando esta equação de recorrência e a expressão (5.30), vem

$$f(x) = \sum_{n=1}^{\infty} a_n x^n = x + \sum_{n=2}^{\infty} 2a_{n-1} x^n + \sum_{n=2}^{\infty} x^n = 2xf(x) + \frac{x}{1-x}.$$

Tendo em conta a expressão obtida, conclui-se que

$$\begin{aligned} f(x) &= \frac{x}{(1-x)(1-2x)} = \frac{1}{1-2x} - \frac{1}{1-x} = \sum_{n=0}^{\infty} ((2x)^n - x^n) \\ &= \sum_{n=1}^{\infty} (2^n - 1) x^n \end{aligned}$$

e, finalmente, que $a_n = 2^n - 1$. \square

Exemplo 5.30. Vamos utilizar o método da função geradora para resolver a equação de recorrência

$$a_n = a_{n-1} + 6a_{n-2}$$

cujas condições iniciais são $a_0 = 3$ e $a_1 = 4$.

Solução. Considerando que $f(x)$ é a função geradora para a sucessão $(a_n)_{n \in \mathbb{N}_0}$, tendo em conta a equação de recorrência, vem

$$\begin{aligned} f(x) &= \sum_{n=0}^{\infty} a_n x^n = 3 + 4x + \sum_{n=2}^{\infty} a_{n-1} x^n + 6 \sum_{n=2}^{\infty} a_{n-2} x^n \\ &= 3 + 4x + x(f(x) - 3) + 6x^2 f(x) \\ &= (6x^2 + x)f(x) + x + 3. \end{aligned}$$

A partir da expressão obtida, conclui-se que a função geradora fica definida pela expressão

$$f(x) = \frac{x+3}{-6x^2 - x + 1} = \frac{x+3}{(1-3x)(1+2x)}.$$

A representação desta função como soma de frações simples, pode obter-se fazendo

$$\frac{1}{(1-3x)(1+2x)} = \frac{A}{1-3x} + \frac{B}{1+2x},$$

onde se obtém a igualdade

$$1 = A + 2xA + B - 3xB,$$

a qual equivale ao sistema de equações

$$A + B = 1, \quad 2A - 3B = 0.$$

Resolvendo este sistema, obtém-se a solução $A = 3/5$ e $B = 2/5$ e, consequentemente,

$$\frac{1}{(1-3x)(1+2x)} = \frac{3}{5} \frac{1}{1-3x} + \frac{2}{5} \frac{1}{1+2x},$$

pelo que a função geradora $f(x)$ toma a forma

$$\begin{aligned} f(x) &= \frac{3}{5} \frac{x+3}{1-3x} + \frac{2}{5} \frac{x+3}{1+2x} \\ &= \frac{3}{5} x \sum_{k=0}^{\infty} (3x)^k + \frac{9}{5} \sum_{k=0}^{\infty} (3x)^k + \frac{2}{5} x \sum_{k=0}^{\infty} (-2x)^k + \frac{6}{5} \sum_{k=0}^{\infty} (-2x)^k. \end{aligned}$$

Finalmente, determina-se o coeficiente de x^n em $f(x)$, ou seja,

$$a_n = 2 \cdot 3^n + (-2)^n.$$

□

Exemplo 5.31. Vamos resolver a equação de recorrência obtida no Exemplo 5.4 aplicando o método da função geradora.

Solução. Note-se que a equação de recorrência do Exemplo 5.4 tem a forma

$$a_n = -6a_{n-1} - 9a_{n-2}$$

e as condições iniciais $a_0 = 1$ e $a_1 = -9$. Como consequência, a função geradora que lhe corresponde satisfaz as igualdades

$$\begin{aligned} f(x) &= 1 - 9x - 6x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} - 9x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} \\ &= 1 - 9x - 6x(f(x) - 1) - 9x^2 f(x) \\ &= (-9x^2 - 6x)f(x) - 3x + 1, \end{aligned}$$

pelo que

$$f(x) = \frac{-3x + 1}{9x^2 + 6x + 1} = \frac{1 - 3x}{(1 + 3x)^2}.$$

Tendo em conta a igualdade (5.31), vem

$$f(x) = (1 - 3x) \sum_{k=0}^{\infty} (k+1)(-3x)^k = \sum_{k=0}^{\infty} (k+1)(-3x)^k + \sum_{k=0}^{\infty} (k+1)(-3x)^{k+1}$$

e, consequentemente, que o coeficiente de x^n em $f(x)$ é

$$a_n = (n+1) \cdot (-3)^n + n(-3)^n = (2n+1) \cdot (-3)^n,$$

ao qual, naturalmente, corresponde um valor idêntico ao obtido no Exemplo 5.4. □

Exemplo 5.32. Seja D_n o número de desencontros de comprimento n (ou seja, o número de permutações sem pontos fixos apresentado nos Exemplos 5.14 e 4.18). Vamos utilizar equação de recorrência obtida no Exemplo 5.14, na determinação de uma expressão para D_n .

Solução. Note-se (ver Exemplo 5.14) que a equação de recorrência para os números D_n tem a forma

$$D_n = nD_{n-1} + (-1)^n,$$

e a condição inicial $D_1 = 0$. Utilizando esta equação de recorrência na função geradora exponencial, vem

$$\begin{aligned} f(x) &= \sum_{n=2}^{\infty} \frac{D_n}{n!} x^n = \sum_{n=2}^{\infty} \frac{nD_{n-1} + (-1)^n}{n!} x^n \\ &= x \sum_{n=2}^{\infty} \frac{D_{n-1}}{(n-1)!} x^{n-1} + \sum_{n=2}^{\infty} \frac{(-1)^n}{n!} x^n \\ &= xf(x) + e^{-x}. \end{aligned}$$

Consequentemente,

$$f(x) = \frac{e^{-x}}{1-x} = \sum_{k=0}^{\infty} x^k \sum_{l=0}^{\infty} \frac{(-1)^l}{l!} x^l = \sum_{t=0}^{\infty} x^t \sum_{l=0}^t \frac{(-1)^l}{l!}$$

e, uma vez que $\frac{D_n}{n!}$ é o coeficiente de x^n em $f(x)$, podemos concluir que

$$\frac{D_n}{n!} = \sum_{l=0}^n \frac{(-1)^l}{l!}.$$

Deve observar-se ainda que, para n suficientemente grande, $\sum_{l=0}^n \frac{(-1)^l}{l!} \approx \frac{1}{e}$. \square

Exemplo 5.33. Sendo a_n o número de partições de um conjunto de cardinalidade n em três subconjuntos não vazios, vamos utilizar a equação de recorrência obtida no Exemplo 5.13 na determinação de uma expressão para a_n .

Solução. Note-se que a_n satisfaz a equação de recorrência linear não homogénea, resolvida no Exemplo 5.13,

$$a_n = 3a_{n-1} + 2^{n-2} - 1,$$

com condições iniciais $a_1 = a_2 = 0$. Agora, vamos voltar a resolvê-la, mas desta vez utilizando o método da função geradora.

Denotando a função geradora da sucessão $(a_n)_{n \in \mathbb{N}}$ por $f(x)$ e tendo em conta que

$$\begin{aligned} f(x) &= \sum_{n=2}^{\infty} a_n x^n = 3 \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} (2)^{n-2} x^n - \sum_{n=2}^{\infty} x^n \\ &= 3x \sum_{k=1}^{\infty} a_k x^k + x^2 \sum_{k=0}^{\infty} (2x)^k - x^2 \sum_{k=0}^{\infty} x^n \\ &= 3xf(x) + \frac{x^2}{1-2x} - \frac{x^2}{1-x}, \end{aligned}$$

conclui-se a expressão

$$f(x) = \frac{x^2}{(1-3x)(1-2x)} - \frac{x^2}{(1-3x)(1-x)}.$$

Recorrendo ao desenvolvimento em frações simples, obtém-se

$$\frac{1}{(1-3x)(1-2x)} = \frac{A}{1-3x} + \frac{B}{1-2x},$$

onde decorre a equação

$$1 = A - 2xA + B - 3xB$$

e o sistema

$$A + B = 1, \quad -2A - 3B = 0,$$

cuja solução é $A = 3$ e $B = -2$. Logo,

$$\frac{1}{(1-3x)(1-2x)} = \frac{3}{1-3x} + \frac{-2}{1-2x}.$$

De modo idêntico se conclui a igualdade

$$\frac{1}{(1-3x)(1-x)} = \frac{3}{2} \cdot \frac{1}{1-3x} - \frac{1}{2} \cdot \frac{1}{1-x}.$$

Assim, obtém-se

$$\begin{aligned} f(x) &= \frac{3x^2}{1-3x} - \frac{2x^2}{1-2x} - \frac{1}{2} \cdot \frac{3x^2}{1-3x} + \frac{1}{2} \cdot \frac{x^2}{1-x} \\ &= \frac{3}{2}x^2 \sum_{k=0}^{\infty} (3x)^k - 2x^2 \sum_{k=0}^{\infty} (2x)^k + \frac{1}{2}x^2 \sum_{k=0}^{\infty} x^k \end{aligned}$$

e, finalmente,

$$a_n = \frac{1}{2}3^{n-1} - 2^{n-1} + \frac{1}{2}.$$

□

Exemplo 5.34. Vamos determinar os números de Bell que denotamos por B_n .

Solução. A equação de recorrência para os números de Bell, obtida no Exemplo 5.15, tem a forma

$$B_{n+1} = \sum_{i=0}^n \binom{n}{i} B_i$$

e a condição inicial $B_0 = 1$. Sendo $f(x)$ a função geradora exponencial dos números de Bell, isto é, sendo

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n,$$

a derivada de primeira ordem conduz-nos às igualdades $f'(x) = \sum_{n=1}^{\infty} \frac{B_n}{(n-1)!} x^{n-1} = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{i=0}^n \binom{n}{i} B_i$.

Escrevendo cada um dos termos desta série na Tabela 5.1, com entradas $n \setminus i$, onde os termos de $\frac{x^n}{n!} \sum_{i=0}^n \binom{n}{i} B_i$ aparecem na n -ésima linha,

$n \setminus i$	$i = 0$	$i = 1$	$i = 2$	$i = 3$	$i = 4$	\dots	$i = k$	\dots
$n = 0$	$\frac{x^0}{0!} \binom{0}{0} B_0$							
$n = 1$	$\frac{x^1}{1!} \binom{1}{0} B_0$	$\frac{x^1}{1!} \binom{1}{1} B_1$						
$n = 2$	$\frac{x^2}{2!} \binom{2}{0} B_0$	$\frac{x^2}{2!} \binom{2}{1} B_1$	$\frac{x^2}{2!} \binom{2}{2} B_2$					
$n = 3$	$\frac{x^3}{3!} \binom{3}{0} B_0$	$\frac{x^3}{3!} \binom{3}{1} B_1$	$\frac{x^3}{3!} \binom{3}{2} B_2$	$\frac{x^3}{3!} \binom{3}{3} B_3$				
$n = 4$	$\frac{x^4}{4!} \binom{4}{0} B_0$	$\frac{x^4}{4!} \binom{4}{1} B_1$	$\frac{x^4}{4!} \binom{4}{2} B_2$	$\frac{x^4}{4!} \binom{4}{3} B_3$	$\frac{x^4}{4!} \binom{4}{4} B_4$			
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\dots		
$n = k$	$\frac{x^k}{k!} \binom{k}{0} B_0$	$\frac{x^k}{k!} \binom{k}{1} B_1$	$\frac{x^k}{k!} \binom{k}{2} B_2$	$\frac{x^k}{k!} \binom{k}{3} B_3$	$\frac{x^k}{k!} \binom{k}{4} B_4$	\dots	$\frac{x^k}{k!} \binom{k}{k} B_k$	
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\dots	\vdots	

Tabela 5.1: Tabela de termos de $f'(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{i=0}^n \binom{n}{i} B_i$.

podemos calcular $f'(x)$, somando todos os termos coluna a coluna. Desta forma, obtém-se

$$\begin{aligned} f'(x) &= \sum_{i=0}^{\infty} \frac{B_i}{i!} \sum_{n=i}^{\infty} \frac{x^n}{(n-i)!} = \sum_{i=0}^{\infty} \frac{B_i}{i!} x^i e^x \\ &= f(x)e^x. \end{aligned}$$

Logo, $(\ln f(x))' = \frac{f'(x)}{f(x)} = e^x$, o que significa $\ln f(x) = \int e^x dx$ e que $f(x) = \exp(e^x + C)$. Uma vez que $f(0) = B_0 = 1$, conclui-se que $C = -1$ e, finalmente, que a função geradora exponencial dos números de Bell é

$$f(x) = e^{e^x - 1}.$$

Utilizando a expressão (5.33), para o cálculo do coeficiente de x^n no desenvolvimento de $f(x)$, obtém-se

$$f(x) = \frac{1}{e} \sum_{k=0}^{\infty} \frac{1}{k!} e^{xk} = \frac{1}{e} \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=0}^{\infty} \frac{(xk)^n}{n!},$$

onde podemos, finalmente, concluir que B_n (que, neste desenvolvimento, corresponde ao coeficiente de $\frac{x^n}{n!}$) fica definido pela expressão

$$B_n = \frac{1}{e} \sum_{k=1}^{\infty} \frac{k^n}{k!}.$$

□

Exemplo 5.35. Utilizando funções geradoras, vamos resolver o sistema de equações de recorrência

$$\begin{cases} a_n = 2a_{n-1} + b_{n-1} + 1, \\ b_n = a_{n-1} + 2b_{n-1} + 2^{n-1}, \end{cases} \quad (5.38)$$

com condições iniciais $a_0 = b_0 = 0$.

Solução. Sendo

$$\mathcal{A}(x) = \sum_{n=0}^{\infty} a_n x^n \quad \text{e} \quad \mathcal{B}(x) = \sum_{n=0}^{\infty} b_n x^n$$

as funções geradoras das sucessões (a_n) e (b_n) , multiplicando ambos membros do sistema (5.38) por x^n e procedendo à respectiva soma, para $n = 1, 2, \dots$, vem

$$\begin{cases} \sum_{n=1}^{\infty} a_n x^n = 2 \sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} b_{n-1} x^n + \sum_{n=1}^{\infty} x^n \\ \sum_{n=1}^{\infty} b_n x^n = \sum_{n=1}^{\infty} a_{n-1} x^n + 2 \sum_{n=1}^{\infty} b_{n-1} x^n + x \sum_{n=0}^{\infty} (2x)^n. \end{cases}$$

Utilizando as definições de \mathcal{A} e \mathcal{B} e as respectivas condições iniciais, obtém-se o sistema

$$\begin{cases} \mathcal{A}(x) = 2x\mathcal{A}(x) + x\mathcal{B}(x) + \frac{x}{1-x}, \\ \mathcal{B}(x) = x\mathcal{A}(x) + 2x\mathcal{B}(x) + \frac{x}{1-2x}, \end{cases}$$

cuja solução é

$$\mathcal{A}(x) = \frac{x - 3x^2 + 3x^3}{(1-x)^2(1-2x)(1-3x)} \quad \text{e} \quad \mathcal{B}(x) = \frac{x}{(1-x)^2(1-3x)},$$

ou seja,

$$\begin{aligned} \mathcal{A}(x) &= -\frac{1}{4} \frac{1}{1-x} + \frac{1}{2} \frac{1}{(1-x)^2} - \frac{1}{1-2x} + \frac{3}{4} \frac{1}{1-3x}, \\ \mathcal{B}(x) &= -\frac{1}{4} \frac{1}{1-x} - \frac{1}{2} \frac{1}{(1-x)^2} + \frac{3}{4} \frac{1}{1-3x}. \end{aligned}$$

Após o desenvolvimento destas frações em séries de potências, obtém-se a solução final

$$a_n = \frac{3}{4}3^n - 2^n + \frac{1}{2}n + \frac{1}{4} \quad \text{e} \quad b_n = \frac{3}{4}3^n - \frac{1}{2}n - \frac{3}{4}.$$

□

5.7. Funções geradoras de várias variáveis

As funções geradoras podem também ser utilizadas nos casos multidimensionais e, embora nesta secção, apenas se defina função geradora com duas variáveis, a respectiva extensão aos casos com mais do que duas variáveis é imediata.

Definição 5.11 (Função geradora ordinária com duas variáveis). *Dada a sucessão bidimensional de números $(a_{n,k})_{n,k \in \mathbb{N}_0}$, designa-se por função geradora (ordinária) bidimensional desta sucessão a série formal de potências*

$$\mathcal{A}(x, y) = \sum_{n,k \in \mathbb{N}_0} a_{nk} x^n y^k \quad (5.39)$$

Seguem-se alguns exemplos de funções geradoras bidimensionais.

Exemplo 5.36. Vamos determinar a função geradora para a sucessão de números binomiais $(b_{n,k})_{n,k \in \mathbb{N}_0}$, tal que $b_{n,k} = \binom{n}{k}$.

Solução. Uma vez que $\binom{n}{k} = 0$, quando $k > n$, vem

$$\mathcal{B}(x, y) = \sum_{n,k \in \mathbb{N}_0} b_{n,k} x^n y^k = \sum_{n=0}^{\infty} \sum_{k=0}^n \binom{n}{k} x^n y^k.$$

Logo,

$$\mathcal{B}(x, y) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n \binom{n}{k} y^k \right) x^n = \sum_{n=0}^{\infty} (1+y)^n x^n = \sum_{n=0}^{\infty} (x+xy)^n$$

e, consequentemente,

$$\mathcal{B}(x, y) = \frac{1}{1-x-xy}. \quad \square$$

Exemplo 5.37. Vamos determinar a função geradora para a sucessão $(b_{n,k})_{n,k \in \mathbb{N}_0}$, tal que $b_{nk} = \frac{n^k}{k!}$, convencionando que $0^0 = 1$.

Solução. Uma vez que

$$\mathcal{B}(x, y) = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{n^k}{k!} x^n y^k = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\infty} \frac{n^k}{k!} y^k \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\infty} \frac{(ny)^k}{k!} \right) x^n,$$

utilizando (5.33), vem

$$\mathcal{B}(x, y) = \sum_{n=0}^{\infty} e^{ny} x^n = \sum_{n=0}^{\infty} (xe^y)^n$$

e, por (5.30),

$$\mathcal{B}(x, y) = \frac{1}{1-xe^y}. \quad \square$$

Os capítulos a seguir contêm vários exemplos de aplicação das funções geradoras na resolução de problemas combinatórios.

5.8. Exercícios

5.1. Resolver a equação de recorrência

$$a_n = n^2 a_{n-1},$$

com condição inicial $a_1 = 1$.

5.2. Sabendo que uma dada população de coelhos duplica de ano para ano, quantos coelhos existem após n anos, a partir de uma população inicial de seis coelhos?

- 5.3. Sendo b_n o número de n -uplos de componentes binárias nos quais não existem duas componentes vizinhas com valor zero, deduza uma relação de recorrência para b_n .
- 5.4. Sendo $h(k, n)$ o número de possibilidades de colocação de k pacientes numa sala de espera com n cadeiras em linha, de tal forma que os pacientes não se sentam em cadeiras vizinhas, deduza uma relação de recorrência para $h(k, n)$.
- 5.5. Sendo p_n o número de partições de um conjunto de cardinalidade n em dois subconjuntos não vazios, deduza uma relação de recorrência para p_n e encontre a respectiva solução.
- 5.6. Sendo s_n o número de subconjuntos do conjunto $\{1, 2, \dots, n\}$ (onde se inclui o conjunto vazio) que não contêm números consecutivos, deduza uma relação de recorrência para s_n e determine a respectiva solução.
- 5.7. Suponha que um par de coelhos tem o primeiro par de descendentes após dois meses de estarem juntos e que, posteriormente, no final de cada mês têm mais um par de descendentes. Começando com um par de coelhos, deduza uma relação de recorrência para o número c_n de coelhos existentes depois de n meses.
- 5.8. Resolva as seguintes equações de recorrência com condições iniciais:
- $a_n = 2a_{n-1} + 3a_{n-2}$, $a_0 = a_1 = 1$.
 - $a_n = 2a_{n-1} - a_{n-2}$, $a_0 = a_1 = 2$.
 - $a_n = 6a_{n-1} - 9a_{n-2} - 4a_{n-3} + 12a_{n-4}$, $a_i = i$ para $i \in \{0, 1, 2, 3\}$ (sabendo que $x^4 - 6x^3 + 9x^2 + 4x - 12 = (x-2)^2(x+1)(x-3)$).
- 5.9. Resolva a equação de recorrência

$$a_n = a_{n-1} + 6a_{n-2},$$

com condições iniciais $a_0 = 4$, $a_1 = 4$.
- 5.10. Resolva as equações de recorrência com condições iniciais:
- $a_n + 6a_{n-1} + 9a_{n-2} = 3$, $a_0 = 0$, $a_1 = 1$.
 - $a_n = 4a_{n-1} - 4a_{n-2} + 2^n$, $a_0 = a_1 = 2$.
 - $a_n = a_{n-1} + 7n$, $a_0 = 0$.
- 5.11. Resolva a equação de recorrência

$$a_n + 5a_{n-1} + 6a_{n-2} = 3n^2,$$

com condições iniciais $a_0 = 1$ e $a_1 = 4$.
- 5.12. Resolva a equação de recorrência

$$a_n + 3a_{n-1} + 2a_{n-2} = f(n),$$

onde

$$f(n) = \begin{cases} 1, & \text{para } n = 5, \\ 0, & \text{para } n \neq 5, \end{cases}$$

com condições iniciais $a_0 = a_1 = 0$.
- 5.13. Suponha que não existem três diagonais de um n -ágono convexo que se intersectem num ponto e que a_n é o número de regiões do n -ágono determinadas por todas as possíveis diagonais.

(a) Mostre que

$$a_n = a_{n-1} + \frac{(n-1)(n-2)(n-3)}{6} + n - 2, \quad \text{para } n \geq 3,$$

com $a_0 = a_1 = a_2 = 0$.

(b) Determine a_n .

5.14. Resolva a equação de recorrência

$$na_n + na_{n-1} - a_{n-1} = 2^n,$$

com condição inicial $a_0 = 3.456$.

5.15. Resolva a equação de recorrência

$$a_n = na_{n-1} + n!,$$

com condição inicial $a_0 = 2$.

5.16. Defina a função geradora para a sucessão $(a_n)_{n \in \mathbb{N}}$, onde (a_n) é o número de soluções inteiras da equação

$$x_1 + x_2 + x_3 + x_4 = n,$$

nos casos em que

- (a) $0 \leq x_1 \leq 5$, $0 \leq x_2 \leq 3$, $2 \leq x_3 \leq 8$, $0 \leq x_4 \leq 4$;
- (b) $2 \leq x_i \leq 8$, para $i = 1, 2, 3, 4$, x_1 é par e x_2 é ímpar.

5.17. Resolva a equação (5.1), com condição inicial $a_0 = 1$, utilizando o método da função geradora.

5.18. Resolva a equação (5.3), com condição inicial $a_0 = 1$, utilizando o método da função geradora.

5.19. Resolva a equação de recorrência para os números Fibonacci (5.11), com condições iniciais $a_0 = a_1 = 1$, utilizando o método da função geradora.

5.20. Resolva o sistema de equações de recorrência

$$\begin{aligned} a_n &= 3a_{n-1} + 2b_{n-1} \\ b_n &= a_{n-1} + b_{n-1} \end{aligned}$$

com condições iniciais $a_0 = b_0 = 1$, utilizando o método da função geradora.

5.21. Calcule o número de possibilidades de troca de 50€ em notas de 20€, 10€ e 5€ e moedas de 2€ e 1€, sabendo que dispõe no máximo de cinco moedas de 1€, cinco moedas de 2€ e cinco notas de 5€ (não havendo qualquer limitação em relação às restantes notas).

5.22. Determine a função geradora da sucessão $(a_n)_{n \in \mathbb{N}}$, onde a_n é o número de n -uplos contendo as letras A, B e C, nos quais a letra A aparece pelo menos duas vezes.

6

Números Combinatórios

Existem certas sucessões de números inteiros que desempenham um papel muito importante na matemática e suas aplicações. Estão neste caso, os números primos, números binomiais, números binomiais generalizados, número de Fibonacci, números triangulares¹, etc. No caso particular da matemática discreta, são especialmente relevantes, não só os números anteriormente referidos, como ainda outros números muito utilizados na resolução de problemas de contagem de permutações ou de partições de conjuntos como, por exemplo, os números de Stirling, Euler, Bell e Catalan que serão estudados neste capítulo.

6.1. Factoriais e números binomiais

Anteriormente, definimos factorial de n como sendo $n! = n(n - 1) \cdots 2 \cdot 1$ (ver fórmula (4.3)). Agora, mais formalmente, vamos definir $n!$ de um modo recursivo, conforme a seguir se indica.

Definição 6.1 (Factorial). *Se n é um inteiro não negativo, então*

$$n! = \begin{cases} 1, & \text{se } n = 0, \\ n(n-1)!, & \text{se } n \geq 1. \end{cases}$$

A definição recursiva, embora elegante, não simplifica a determinação do factorial de um número n a qual, para valores elevados de n , exige um considerável esforço cálculo. Por este motivo, desenvolveram-se várias fórmulas de aproximação de $n!$, entre as quais se destacam as obtidas pelo matemático escocês James Stirling (1692–1770) e que são as seguintes:

$$n! \approx \sqrt{2\pi n} n^n e^{-n}, \quad (6.1)$$

$$n! \approx \sqrt{2\pi n} n^n e^{-n + \frac{1}{12n}}. \quad (6.2)$$

Observando os valores da Tabela 6.1, verifica-se que a fórmula (6.2) é mais precisa do que a fórmula (6.1). Por outro lado, conclui-se também que as fórmulas (6.1) e (6.2) determinam, respectivamente, um minorante e um majorante para $n!$. O Teorema 6.1 estabelece a validade desta última conclusão para todos os valores de n .

Teorema 6.1 (Fórmula de Stirling). *Para cada inteiro $n \geq 1$ verificam-se as desigualdades*

$$\sqrt{2\pi n} n^n e^{-n} < n! < \sqrt{2\pi n} n^n e^{-n + \frac{1}{12n}}. \quad (6.3)$$

¹ Assim designados porque o n -ésimo número corresponde ao número de pontos distribuídos por n linhas de modo a formarem um triângulo.

n	$n!$	$\sqrt{2\pi n} n^n e^{-n}$	% erro	$\sqrt{2\pi n} n^n e^{-n + \frac{1}{12n}}$	% erro
1	1	0,922	7,7863	1,002	0,2274
2	2	1,919	4,0498	2,001	0,0326
3	6	5,836	2,7298	6,001	0,0100
4	24	23,506	2,0576	24,001	0,0043
5	120	118,019	1,6507	120,003	0,0022
6	720	710,078	1,3780	720,009	0,0013
7	5 040	4 980,396	1,1826	5 040,040	0,0008
8	40 320	39 902,395	1,0357	40 320,218	0,0005
9	362 880	359 536,873	0,9213	362 881,378	0,0004
10	3 628 800	3 598 695,619	0,8296	3 628 810,051	0,0003

Tabela 6.1: Aproximações de Stirling para $n \leq 10$ (com erro em %).

A demonstração deste teorema, bem como das fórmulas (6.1) e (6.3), aparecem em vários livros de análise matemática e são aqui omitidas pelo facto das técnicas utilizadas saírem fora do âmbito da matemática discreta.

Para alguns problemas combinatórios torna-se útil considerar o conceito de factorial duplo que a seguir se define.

Definição 6.2 (Factorial duplo). *Se n é um inteiro não negativo, então*

$$n!! = \begin{cases} 1, & \text{se } n \in \{0, 1\}, \\ n(n-2)!! , & \text{se } n \geq 2. \end{cases}$$

Com base nesta definição podemos concluir que o factorial duplo de n é igual ao produto de todos os números naturais não superiores a n e com a paridade de n . Como consequência,

$$\forall_{n \in \mathbb{N}} n!!(n-1)!! = n!. \quad (6.4)$$

Exemplo 6.1. Vamos explicitar $n!!$ a partir de funções já conhecidas.

Solução. Considere-se cada uma das paridades possíveis de n .

- Considerando $n = 2k$, vem que

$$\begin{aligned} n!! &= 2 \cdot 4 \cdot 6 \cdots (n-2) \cdot n \\ &= (2 \cdot 1)(2 \cdot 2)(2 \cdot 3) \cdots (2 \cdot (k-1))(2 \cdot k) \\ &= 2^k(1 \cdot 2 \cdot 3 \cdots (k-1) \cdot k) \\ &= 2^k k!. \end{aligned}$$

- Considerando $n = 2k+1$, e tendo em conta (6.4), vem que

$$n!! = \frac{n!}{(n-1)!!} = \frac{n!}{(2k)!!} = \frac{n!}{2^k k!}. \quad \square$$

Os números binomiais $\binom{n}{k}$ foram definidos e estudados nos capítulos anteriores. Com efeito, estes números foram definidos com as fórmulas (4.5), (4.7) e (4.21) (a última das quais corresponde à definição recursiva), foram utilizados na função geradora definida em (4.18) e na fórmula do binómio de Newton (4.20) e as suas propriedades foram analisadas nos Exemplos 4.27, 4.29, 4.30 e Exercícios 4.14, ..., 4.20.

	k	0	1	2	3	4	5	6	7	8	9	10	11	12
$n = 0$	0	1												
$n = 1$	1	1	1											
$n = 2$	2	1	2	1										
$n = 3$	3	1	3	3	1									
$n = 4$	4	1	4	6	4	1								
$n = 5$	5	1	5	10	10	5	1							
$n = 6$	6	1	6	15	20	15	6	1						
$n = 7$	7	1	7	21	35	35	21	7	1					
$n = 8$	8	1	8	28	56	70	56	28	8	1				
$n = 9$	9	1	9	36	84	126	126	84	36	9	1			
$n = 10$	10	1	10	45	120	210	252	210	120	45	10	1		
$n = 11$	11	1	11	55	165	330	462	462	330	165	55	11	1	
$n = 12$	12	1	12	66	220	495	792	924	792	495	220	66	12	1

Tabela 6.2: Triângulo de Pascal.

A Figura 4.2 do capítulo 4, descreve uma versão moderna do triângulo de Pascal. Porém, na sua forma original, este triângulo foi introduzido por Blaise Pascal com o aspecto da Tabela 6.2. Adiante, apresentaremos mais alguns triângulos de números com propriedades especiais.

Observe-se que, de acordo com a fórmula (4.5), os números binomiais podem generalizar-se conforme a seguir se indica.

Definição 6.3 (Número binomial generalizado). *Para cada número real x e cada número inteiro não negativo k*

$$\binom{x}{k} = \frac{(x)_k}{k!},$$

onde $(x)_k$ se designa por coeficiente factorial e é tal que $(x)_0 = 1$ e $(x)_k = x(x - 1)\dots(x - k + 1)$, para $k \geq 1$.

Exemplo 6.2. Vamos calcular $\binom{-1}{k}$, $\binom{-1/2}{k}$ e $\binom{1/2}{k}$.

Solução.

1. Cálculo de $\binom{-1}{k}$. Uma vez que

$$(-1)_k = (-1)(-2)(-3)\dots(-k) = (-1)^k k!$$

então

$$\binom{-1}{k} = (-1)^k.$$

2. Cálculo de $\binom{-1/2}{k}$.

$$\begin{aligned} \left(\frac{-1}{2}\right)_k &= \left(-\frac{1}{2}\right) \left(-\frac{3}{2}\right) \left(-\frac{5}{2}\right) \dots \left(-\frac{2k-1}{2}\right) \\ &= \frac{(-1)^k}{2^k} 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k-1) = \frac{(-1)^k}{2^k} (2k-1)!! . \end{aligned}$$

Tendo em conta o Exemplo 6.1, sabe-se que $(2k-1)!! = \frac{(2k-1)!}{2^{k-1}(k-1)!}$, uma vez que $2k-1 = 2(k-1)+1$. Logo,

$$\left(\frac{-1}{2}\right)_k = \frac{(-1)^k}{2^{2k-1}} \frac{(2k-1)!}{(k-1)!}$$

e, finalmente,

$$\binom{-1/2}{k} = \frac{(-1)^k}{2^{2k-1}} \binom{2k-1}{k}.$$

3. *Cálculo de $\binom{1/2}{k}$.*

$$\begin{aligned} \left(\frac{1}{2}\right)_k &= \left(\frac{1}{2}\right) \left(-\frac{1}{2}\right) \left(-\frac{3}{2}\right) \left(-\frac{5}{2}\right) \cdots \left(-\frac{2k-3}{2}\right) \\ &= \frac{(-1)^{k-1}}{2^k} 1 \cdot 1 \cdot 3 \cdot 5 \cdots (2k-3) = \frac{(-1)^{k-1}}{2^k} (2k-3)!! . \end{aligned}$$

Tendo em conta o Exemplo 6.1 e a igualdade $2k-3 = 2(k-2)+1$, vem que $(2k-3)!! = \frac{(2k-3)!}{2^{k-2}(k-2)!}$.
Logo, uma vez que $\frac{1}{k-2} \binom{2k-3}{k} = \frac{1}{2k} \binom{2k-2}{k-1}$,

$$\left(\frac{1}{2}\right)_k = \frac{(-1)^{k-1}}{2^{2k-2}} \frac{(2k-3)!}{(k-2)!} = \frac{(-1)^{k-1} k!}{4^{k-1} (k-2)} \binom{2k-3}{k}$$

e, finalmente,

$$\binom{1/2}{k} = \frac{(-1)^{k-1}}{4^{k-1} \cdot 2k} \binom{2k-2}{k-1}. \quad (6.5)$$

□

6.2. Números de Fibonacci e o número de ouro

Os números de Fibonacci foram definidos pela fórmula recursiva (5.11) do Exemplo 5.5 (alternativamente, a fórmula explícita (5.12) define também estes números). Na Tabela 6.3 apresentam-se os primeiros 18 números de Fibonacci.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584

Tabela 6.3: Números de Fibonacci.

Considerando a função geradora dos números de Fibonacci

$$\mathcal{F}(x) = \sum_{n=1}^{\infty} F_n x^n = x F_1 + x^2 F_2 + \dots \quad (6.6)$$

podemos concluir o resultado que se segue.

Teorema 6.2. *Se $\mathcal{F}(x)$ é a função geradora (6.6) dos números de Fibonacci, então*

$$\mathcal{F}(x) = \frac{x}{1-x-x^2}.$$

Demonstração. Tendo em conta (5.11), $F_n - F_{n-1} - F_{n-2} = 0$, $F_1 = 1$ e $F_2 = 2$. Logo,

$$\begin{aligned} \mathcal{F}(x) &= x F_1 + x^2 F_2 + x^3 F_3 + x^4 F_4 + x^5 F_5 + \dots \\ -x\mathcal{F}(x) &= -x^2 F_1 - x^3 F_2 - x^4 F_3 - x^5 F_4 - \dots \\ -x^2\mathcal{F}(x) &= -x^3 F_1 - x^4 F_2 - x^5 F_3 - \dots \\ (1-x-x^2)\mathcal{F}(x) &= x + 0 + 0 + 0 + 0 + 0 + \dots \end{aligned}$$

e, consequentemente, $(1-x-x^2)\mathcal{F}(x) = x$. □

Uma das características dos números de Fibonacci é sua soma telescópica, a qual se torna evidente nos exemplos a seguir, onde se apresentam algumas propriedades combinatórias adicionais destes números.

Exemplo 6.3. Vamos calcular a soma dos n primeiros números de Fibonacci $\sum_{k=1}^n F_k$.

Solução. Escrevendo a relação (5.11) na forma

$$F_n = F_{n+1} - F_{n-1} \quad (6.7)$$

obtém-se o somatório

$$\begin{array}{rcl} F_2 & = & F_3 - F_1 \\ F_3 & = & F_4 - F_2 \\ F_4 & = & F_5 - F_3 \\ \dots & = & \dots - \dots \\ F_{n-1} & = & F_n - F_{n-2} \\ \hline F_n & = & F_{n+1} - F_{n-1} \\ \hline \sum_{k=2}^n F_k & = & F_n + F_{n+1} - (F_1 + F_2) \end{array}$$

Note-se que no somatório do lado direito existem muitas parcelas canceladas ($F_3 - F_3$, $F_4 - F_4$, ..., $F_{n-1} - F_{n-1}$) e, por outro lado,

$$F_n + F_{n+1} = F_{n+2} \quad \text{e} \quad F_1 + F_2 = 1 + 1 = 2.$$

Como consequência, finalmente, vem

$$\sum_{k=2}^n F_k = F_{n+2} - 2 \Leftrightarrow \sum_{k=1}^n F_k = F_{n+2} - 1. \quad (6.8)$$

□

Exemplo 6.4. Vamos calcular a soma dos n primeiros números de Fibonacci com índice par e com índice ímpar, respectivamente, ou seja,

$$\begin{aligned} P_n &= F_2 + F_4 + \dots + F_{2n} &= \sum_{k=1}^n F_{2k}, \\ I_n &= F_1 + F_3 + \dots + F_{2n-1} &= \sum_{k=1}^n F_{2k-1}. \end{aligned}$$

Solução. Utilizando a equação (6.7), obtém-se o somatório telescópico

$$\begin{array}{rcl} F_2 & = & F_3 - F_1 \\ F_4 & = & F_5 - F_3 \\ F_6 & = & F_7 - F_5 \\ \dots & = & \dots - \dots \\ F_{2n} & = & F_{2n+1} - F_{2n-1} \\ \hline P_n & = & F_{2n+1} - F_1 \end{array}$$

Assim, procedendo aos respectivos cancelamentos, podemos concluir a igualdade

$$F_2 + F_4 + \dots + F_{2n} = F_{2n+1} - 1. \quad (6.9)$$

Por outro lado, tendo em conta (6.8), vem

$$P_n + I_n = F_1 + F_2 + \dots + F_{2n-1} + F_{2n} = F_{2n+2} - 1$$

onde, utilizando (6.9), se obtém

$$I_n = F_{2n+2} - 1 - P_n = F_{2n+2} - 1 - F_{2n+1} + 1 = F_{2n+2} - F_{2n+1}.$$

Finalmente, tendo em conta que, de acordo com (6.7), $F_{2n+2} - F_{2n+1} = F_{2n}$,

$$F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}. \quad (6.10)$$

□

Exemplo 6.5. Vamos calcular o somatório

$$-F_1 + F_2 - F_3 + \cdots + (-1)^n F_n = \sum_{k=1}^n (-1)^k F_k.$$

Solução. Este cálculo vai ser feito considerando o caso em que n é par e o caso em que n é ímpar, recorrendo à notação do Exemplo 6.4.

- Caso em que n é par ($n = 2k$). Tendo em conta que

$$\begin{aligned} -F_1 + F_2 - F_3 + \cdots + (-1)^n F_n &= P_k - I_k \\ &= F_{2k+1} - 1 - F_{2k} \\ &= F_{n+1} - F_n - 1 \end{aligned}$$

e que, de acordo com (6.7), $F_{n+1} - F_n = F_{n-1}$, se n é par, então

$$-F_1 + F_2 - F_3 + \cdots + (-1)^n F_n = F_{n-1} - 1. \quad (6.11)$$

- Caso em que n é ímpar ($n = 2k - 1$). Tendo em conta que

$$\begin{aligned} -F_1 + F_2 - F_3 + \cdots + (-1)^n F_n &= P_{k-1} - I_k \\ &= F_{2k-1} - 1 - F_{2k} \\ &= F_n - F_{n+1} - 1 \end{aligned}$$

e que, de acordo com (6.7), $F_n - F_{n+1} = -F_{n-1}$, se n é ímpar, então

$$-F_1 + F_2 - F_3 + \cdots + (-1)^n F_n = -F_{n-1} - 1. \quad (6.12)$$

Considerando as equações (6.11) e (6.12) conjuntamente, para cada $n \geq 1$, obtém-se

$$-F_1 + F_2 - F_3 + \cdots + (-1)^n F_n = (-1)^n F_{n-1} - 1. \quad (6.13)$$

□

Segue-se mais um exemplo (um pouco mais complicado) de soma telescópica, desta vez relativa à soma dos quadrados dos n primeiros números de Fibonacci.

Exemplo 6.6. Vamos calcular o somatório dos quadrados dos n primeiros números de Fibonacci

$$F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = \sum_{k=1}^n F_k^2.$$

Solução. Uma vez que, tendo em conta (5.11), $F_k = F_{k+1} - F_{k-1}$, vem

$$F_k^2 = F_k(F_{k+1} - F_{k-1}) = F_k F_{k+1} - F_{k-1} F_k.$$

Como consequência, obtém-se o somatório

$$\begin{array}{rcl} F_2^2 & = & F_2 F_3 - F_1 F_2 \\ F_3^2 & = & F_3 F_4 - F_2 F_3 \\ F_4^2 & = & F_4 F_5 - F_3 F_4 \\ \dots & = & \dots - \dots \\ F_n^2 & = & F_n F_{n+1} - F_{n-1} F_n \\ \hline \sum_{k=2}^n F_k^2 & = & F_n F_{n+1} - F_1 F_2 \end{array}$$

Logo,

$$\sum_{k=1}^n F_k^2 = F_n F_{n+1}. \quad (6.14)$$

□

O próximo exemplo relaciona os números de Fibonacci com os números binomiais, provando-se que os números de Fibonacci são somas de elementos diagonais do triângulo de Pascal.

Exemplo 6.7. Vamos mostrar a igualdade

$$F_{n+1} = \sum_{k=0}^n \binom{n-k}{k}. \quad (6.15)$$

Solução. Para demonstrar a igualdade (6.15), vamos considerar o código de Morse, introduzido por Samuel Morse que, em 1840, inventou o telégrafo e o código, com o seu nome, para comunicações telegráficas.

O código de Morse é constituído por sequências de pontos e traços, as quais definem caracteres alfanuméricos e caracteres especiais. Designa-se por *comprimento do código de um carácter* o número que se obtém somando uma unidade por cada ponto e duas unidades por cada traço. Por exemplo, as sequências de pontos e traços de comprimento 4 do código de Morse são as seguintes:

· · · · - - - - . - - - - - - -

Seja a_n o número de sequências de pontos e traços de comprimento n . Vamos calcular a_n , utilizando dois métodos distintos.

- Convém observar que $a_1 = 1$ (·) e $a_2 = 2$ (·· e -). Sendo $n > 2$, para se determinar o número de sequências de comprimento n podemos partir o conjunto destas sequências S em dois subconjuntos, S_1 e S_2 , tais que S_1 é constituído pelas sequências cujo primeiro símbolo é um ponto e S_2 é constituído pelas sequências cujo primeiro símbolo é um traço. Logo, $|S| = |S_1| + |S_2|$ e, uma vez que $|S_1| = a_{n-1}$ e $|S_2| = a_{n-2}$, conclui-se a igualdade

$$a_n = a_{n-1} + a_{n-2},$$

ou seja, obtém-se a equação de recorrência para os números de Fibonacci, pelo que, pela unicidade da solução e tendo conta as condições iniciais,

$$a_n = F_{n+1}. \quad (6.16)$$

2. Em alternativa ao método anterior, tendo em vista a determinação de a_n , vamos começar por calcular o número de sequências do código de Morse de comprimento n , com precisamente k traços. Assim, neste caso, as sequências são constituídas por $n - 2k$ pontos e k traços, ou seja, são constituídas por $n - k$ elementos (pontos ou traços). De entre estes $n - k$ elementos existem $\binom{n-k}{k}$ (combinações) modos de escolher as k posições para os traços. Logo, existem $\binom{n-k}{k}$ sequências de comprimento n com k traços. Somando os valores obtidos para os diferentes números de traços, obtém-se

$$a_n = \sum_{k=0}^n \binom{n-k}{k}. \quad (6.17)$$

Tendo em conta as igualdades (6.16) e (6.17), conclui-se a igualdade (6.15). \square

Voltando ao Exemplo 5.5, vamos analisar novamente a equação característica dos números de Fibonacci, $x^2 - x - 1 = 0$, tendo em conta que as suas raízes são os números $\frac{1+\sqrt{5}}{2}$. Uma destas raízes, $\frac{1+\sqrt{5}}{2}$, é conhecida por *número de ouro* e denotada por Φ (inicial do escultor e arquitecto grego do século V a.C. Fídias que utilizou frequentemente o número de ouro nas suas obras). É claro que o número de ouro

$$\Phi = \frac{1 + \sqrt{5}}{2} = 1,6180339887498948482\dots$$

é um número irracional e, denotando a segunda raiz, $\frac{1-\sqrt{5}}{2} = -\frac{1}{\Phi}$, por $\widehat{\Phi}$, vem

$$\widehat{\Phi} = -\Phi^{-1} = \frac{1 - \sqrt{5}}{2} = -0,61803398874989484820\dots$$

Como consequência, utilizando a fórmula (5.12), podemos expressar o número de Fibonacci em função do número de ouro, conforme se indica.

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - \widehat{\Phi}^n).$$

Tendo em conta que F_n é inteiro e, para cada inteiro positivo n , $\left| \frac{1}{\sqrt{5}}\widehat{\Phi}^n \right| < \frac{1}{2}$, podemos concluir que o número de Fibonacci F_n vem determinado pelo arredondamento de $\frac{1}{\sqrt{5}}\Phi^n$ ou, mais precisamente, por

$$F_n = \left\lfloor \frac{1}{\sqrt{5}}\Phi^n + \frac{1}{2} \right\rfloor. \quad (6.18)$$

Observe-se que, de acordo com o Exemplo 5.5, a equação de recorrência $a_n = a_{n-1} + a_{n-2}$ tem como solução geral

$$a_n = C_1\Phi^n + C_2\widehat{\Phi}^n, \quad (6.19)$$

onde as constantes C_1 e C_2 dependem dos valores iniciais.

Exemplo 6.8. Vamos determinar uma fórmula para os números de Lucas² que se definem pela expressão

$$L_n = F_{n+1} + F_{n-1},$$

onde F_k denota o k -ésimo número de Fibonacci e se assume $F_0 = 0$.

²Edouard Lucas (1842–1891) foi um matemático francês que investigou diferentes versões da sucessão de Fibonacci.

Solução. Uma vez que

$$\begin{aligned} L_{n-1} + L_{n-2} &= F_n + F_{n-2} + F_{n-1} + F_{n-3} \\ &= F_{n+1} + F_{n-1} \\ &= L_n, \end{aligned}$$

aplicando a solução geral para este tipo de equações de recorrência, vem

$$L_n = C_1 \Phi^n + C_2 \hat{\Phi}^n. \quad (6.20)$$

A partir da determinação dos valores iniciais

$$\begin{aligned} L_1 &= F_2 + F_0 = 1, \\ L_2 &= F_3 + F_1 = 3, \end{aligned}$$

e, uma vez que $L_2 = L_1 + L_0$, vem

$$L_0 = L_2 - L_1 = 2.$$

Logo, tendo em conta (6.20), obtém-se o sistema de equações lineares

$$\begin{cases} C_1 + C_2 = 2 \\ C_1 \Phi + C_2 \hat{\Phi} = 1 \end{cases}$$

cuja solução é $C_1 = C_2 = 1$. Finalmente, substituindo em (6.20) os valores das constantes, vem

$$L_n = \Phi^n + \hat{\Phi}^n.$$

□

Com o próximo exemplo, vamos concluir que o quociente de dois números de Fibonacci consecutivos tende, assintoticamente, para o número de ouro.

Exemplo 6.9. Vamos determinar

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n}. \quad (6.21)$$

Solução. Começamos por provar que a sucessão $a_n = \frac{F_{n+1}}{F_n}$ tem limite, quando n tende para infinito. Para tal basta provar que a_n é uma sucessão de Cauchy, ou seja, que satisfaz as condições:

$$a_{n+1} - a_n \rightarrow 0 \text{ e } a_{n+1} - a_n \text{ alterna em sinal,} \quad (6.22)$$

$$\exists M > 0 \quad \forall n \in \mathbb{N} \quad |a_n| < M. \quad (6.23)$$

- *Prova de (6.22).* Utilizando a equação de Cassini (ver Exercício 6.3),

$$\frac{F_{n+2}}{F_{n+1}} - \frac{F_{n+1}}{F_n} = \frac{F_{n+2}F_n - F_{n+1}^2}{F_{n+1}F_n} = \frac{(-1)^{n+1}}{F_{n+1}F_n} \rightarrow 0.$$

- *Prova de (6.23).* Utilizando a equação (6.18), para $n \geq 1$, vem

$$\frac{F_{n+1}}{F_n} < \frac{\frac{1}{\sqrt{5}}\Phi^{n+1} + \frac{1}{2}}{\frac{1}{\sqrt{5}}\Phi^n - \frac{1}{2}} = \frac{\Phi + \frac{\sqrt{5}}{2\Phi^n}}{1 - \frac{\sqrt{5}}{2\Phi^n}} < \frac{\Phi + \frac{\sqrt{5}}{2\Phi}}{1 - \frac{\sqrt{5}}{2\Phi}} = 3 + 2\sqrt{5} < 7,5.$$

Uma vez que já sabemos que o limite da sucessão a_n existe, vamos calcula-lo, denotando-o por x e utilizando as igualdades

$$\frac{F_{n+1}}{F_n} = \frac{F_n + F_{n-1}}{F_n} = 1 + \frac{F_{n-1}}{F_n}.$$

Assim, quando $n \rightarrow \infty$, vem

$$\begin{array}{rcl} \frac{F_{n+1}}{F_n} & = & 1 + \frac{F_{n-1}}{F_n} \\ \downarrow & & \downarrow \\ x & = & 1 + \frac{1}{x}. \end{array}$$

Logo, obtém-se a equação quadrática $x^2 - x - 1 = 0$, cujas raízes são Φ e $\widehat{\Phi}$. Porém, dado que $\widehat{\Phi} < 0$, podemos concluir que

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \Phi.$$

□

6.3. Números de Stirling

Nesta secção estudam-se os números de Stirling de primeira e segunda espécie. Os primeiros relacionam-se com a contagem do número de permutações com um número fixo de ciclos (ver secção 4.4) e o segundo com a contagem das partições de um conjunto num número fixo de subconjuntos não vazios.

Definição 6.4 (Números de Stirling de primeira espécie). *Designa-se por número de Stirling de primeira espécie e denota-se por $[n]_k$, com $n, k \geq 0$, o número de permutações de n elementos com exactamente k ciclos. Por convenção, assume-se $[0]_0 = 1$ e $[0]_k = 0$, para $k > 0$.*

Desta definição decorre directamente a seguinte igualdade:

$$\sum_{k=1}^n [n]_k = n!.$$

Por exemplo, para $n = 3$ temos as seguintes permutações do conjunto $\{1, 2, 3\}$:

- Duas permutações com um ciclo: $[1, 2, 3]$ e $[1, 3, 2]$, pelo que $[3]_1 = 2$.
- Três permutações com dois ciclos: $[1][2, 3]$, $[2][1, 3]$ e $[3][1, 2]$, donde $[3]_2 = 3$.
- Uma permutação com três ciclos: $[1][2][3]$ e, consequentemente, $[3]_3 = 1$.

Na Tabela 6.4, representa-se o triângulo dos números não nulos de Stirling de primeira espécie.

Algumas autores definem os números de Stirling de primeiro espécie como números que alternam de sinal. Vamos denotar esta versão de números de Stirling por $s(n, k)$, onde

$$s(n, k) = (-1)^{n-k} [n]_k.$$

Para além da notação $[n]_k$ (utilizada em [61, 47]) e $s(n, k)$ (utilizada em [80, 81, 87, 90, 91]), existem outras notações para os números de Stirling de primeira espécie, como são o caso, por exemplo, de s_n^k (utilizada em [1]) e σ_n^k (utilizada em [58]). Neste texto optou-se por utilizar a notação $[n]_k$ por ser a que mais se aproxima da notação usualmente utilizada na caracterização de ciclos de permutações.

Exemplo 6.10. *Vamos determinar os casos particulares de números de Stirling de primeira espécie: $[n]_0$, $[n]_k$, com $k > n$, $[n]_1$, $[n]_{n-1}$ e $[n]_n$.*

k	0	1	2	3	4	5	6	7	8	9
$n = 0$	1									
$n = 1$		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	1.764	1624	735	175	21	1		
$n = 8$		5.040	13.068	13.132	6.769	1.960	322	28	1	
$n = 9$		40.320	109.584	118.124	67.284	22.449	4.536	546	36	1

Tabela 6.4: Triângulo de números de Stirling de primeira espécie $\begin{bmatrix} n \\ k \end{bmatrix}$.**Solução.**

- É claro que, dado um conjunto de $n > 0$ elementos, não existem permutações sem ciclos, nem permutações com mais do que n ciclos. Logo,

$$\begin{aligned} \begin{bmatrix} n \\ 0 \end{bmatrix} &= 0, & \text{para } n > 0, \\ \begin{bmatrix} n \\ k \end{bmatrix} &= 0, & \text{para } k > n. \end{aligned}$$

- Tendo em conta que, por definição, $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$ e que, por outro lado, existe uma única permutação de n elementos com n ciclos (permutação identidade), podemos concluir que

$$\begin{bmatrix} n \\ n \end{bmatrix} = 1, \quad \text{para } n \geq 0.$$

- Podemos escrever qualquer permutação com um único ciclo na forma $[1, \dots]$, onde "... " denota uma permutação arbitrária dos elementos do conjunto $\{2, \dots, n\}$. Então

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!, \quad \text{para } n > 0.$$

- Finalmente, observando que as permutações de n elementos com $n-1$ ciclos contêm um ciclo de comprimento 2 e os restantes ciclos de comprimento 1, podemos concluir que existem $\binom{n}{2}$ maneiras de escolher os dois elementos do ciclo de comprimento 2, donde se obtém

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2}, \quad \text{para } n > 0.$$

□

Segue-se uma relação de recorrência para a determinação dos números de Stirling de primeira espécie.

Teorema 6.3. Se $1 \leq k \leq n$, então

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}. \quad (6.24)$$

Demonstração. Observe-se que todas as permutações do conjunto $\{1, \dots, n\}$, com k ciclos, se podem dividir em dois tipos:

1. *Permutações que contêm o ciclo $[n]$ (ou que têm n como ponto fixo).* Neste caso, estamos na presença de permutações de elementos do conjunto $\{1, \dots, n-1\}$, com $k-1$ ciclos, com as quais, adicionando o ciclo $[n]$, se obtém permutações de n elementos com k ciclos (em que n é ponto fixo). Logo, podemos concluir que existem $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ permutações deste tipo.
2. *Permutações sem o ciclo $[n]$ (ou que não têm n como ponto fixo).* Neste caso, estamos na presença de permutações de elementos do conjunto $\{1, \dots, n-1\}$, com k ciclos, (cujo número é igual a $\begin{bmatrix} n-1 \\ k \end{bmatrix}$), em cada uma das quais podemos inserir n de modo a obter permutações de n elementos com k ciclos sem que n seja um ponto fixo. Uma vez que existem $n-1$ possibilidades de inserir n , podemos concluir que existem $(n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}$ permutações deste tipo.

Tendo em conta 1 e 2, obtém-se a igualdade pretendida, ou seja,

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

□

Seguem-se os números de Stirling de segunda espécie.

Definição 6.5 (Números de Stirling de segunda espécie). *Designa-se por número de Stirling de segunda espécie e denota-se por $\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \}$, com $n, k \geq 0$, o número de partições de um conjunto de cardinalidade n em k subconjuntos (não vazios). Por convenção, assume-se que $\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \} = 1$ e que $\{ \begin{smallmatrix} 0 \\ k \end{smallmatrix} \} = 0$, para $k > 0$.*

Por exemplo, para $n = 3$, temos as seguintes partições do conjunto $\{1, 2, 3\}$:

- Uma partição num único subconjunto $\{\{1, 2, 3\}\}$, pelo que $\{ \begin{smallmatrix} 3 \\ 1 \end{smallmatrix} \} = 1$.
- Três partições em dois subconjuntos $\{\{1\}, \{2, 3\}\}, \{\{2\}, \{1, 3\}\}, \{\{3\}, \{1, 2\}\}$, pelo que $\{ \begin{smallmatrix} 3 \\ 2 \end{smallmatrix} \} = 3$.
- Uma partição em três subconjuntos $\{\{1\}, \{2\}, \{3\}\}$, pelo que $\{ \begin{smallmatrix} 3 \\ 3 \end{smallmatrix} \} = 1$.

Na Tabela 6.5 representa-se o triângulo dos números não nulos de Stirling de segunda espécie.

	k	0	1	2	3	4	5	6	7	8	9	10
$n = 0$	0	1										
$n = 1$	1		1									
$n = 2$	2	1		1								
$n = 3$	3	1	3		1							
$n = 4$	4	1	7	6		1						
$n = 5$	5	1	15	25	10		1					
$n = 6$	6	1	31	90	65	15		1				
$n = 7$	7	1	63	301	350	140	21		1			
$n = 8$	8	1	127	966	1.701	1.050	266	28		1		
$n = 9$	9	1	255	3.025	7.770	6.951	2.646	462	36		1	
$n = 10$	10	1	511	9.330	34.105	42.525	22.827	5.880	750	45		1

Tabela 6.5: Números de Stirling de segunda espécie $\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \}$.

Tal como anteriormente, para além da notação $\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \}$ (utilizada em [61, 47]), existem outras notações para os números de Stirling de segunda espécie, como são o caso, por exemplo, de $S(n, k)$ (utilizada em [1]), σ_n^k (utilizada em [58]) e $\sigma(n, k)$ (utilizada em [90, 91]). Neste texto optou-se por utilizar a notação $\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \}$, por estar mais próxima da notação associada a conjuntos.

Exemplo 6.11. Vamos determinar os casos particulares de números de Stirling de segunda espécie: $\{ \begin{smallmatrix} n \\ 0 \end{smallmatrix} \}$, $\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \}$, com $k > n$, $\{ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \}$, $\{ \begin{smallmatrix} n \\ n \end{smallmatrix} \}$, $\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \}$ e $\{ \begin{smallmatrix} n \\ n-1 \end{smallmatrix} \}$.

Solução.

- É claro que dado um conjunto de cardinalidade $n > 0$, não é possível parti-lo em 0 subconjuntos e também não é possível parti-lo em mais do que n subconjuntos. Logo,

$$\begin{aligned}\{ \begin{smallmatrix} n \\ 0 \end{smallmatrix} \} &= 0, && \text{para } n > 0, \\ \{ \begin{smallmatrix} n \\ k \end{smallmatrix} \} &= 0, && \text{para } k > n.\end{aligned}$$

- Tendo em conta que, por definição, $\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \} = 1$ e, uma vez que, dado um conjunto de cardinalidade $n > 0$, existe uma única maneira de o partir num único subconjunto e uma única maneira de o partir em n subconjuntos, então

$$\begin{aligned}\{ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \} &= 1, && \text{para } n > 0, \\ \{ \begin{smallmatrix} n \\ n \end{smallmatrix} \} &= 1, && \text{para } n \geq 0.\end{aligned}$$

- Para determinar $\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \}$, observe-se que quando partimos o conjunto $[n]$ em dois subconjuntos, podemos concluir que apenas um dos subconjuntos fica com o elemento n . Então, existem $2^{n-1}-1$ possibilidades de escolher o subconjunto que não contém n . Logo,

$$\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \} = 2^{n-1} - 1, \quad \text{para } n > 0.$$

- Finalmente, observe-se que as partições do conjunto $[n]$ em $n-1$ subconjuntos consiste num único subconjunto de cardinalidade 2 e $n-2$ subconjuntos de cardinalidade 1. Uma vez que existem $\binom{n}{2}$ modos de escolher o subconjunto de cardinalidade 2,

$$\{ \begin{smallmatrix} n \\ n-1 \end{smallmatrix} \} = \binom{n}{2}, \quad \text{para } n > 0.$$

□

Segue-se uma relação de recorrência para a determinação dos números de Stirling de segunda espécie.

Teorema 6.4. Se $1 \leq k \leq n$, então

$$\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \} = \{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \} + k \{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \}. \quad (6.25)$$

Demonstração. Observe-se que todas as partições do conjunto $\{1, \dots, n\}$ em k subconjuntos se podem dividir em dois tipos:

1. *Partições tais que $\{n\}$ é um dos subconjuntos da partição.* Neste caso, estamos na presença de partições do conjunto $\{1, \dots, n-1\}$ em $k-1$ subconjuntos, cujo número é $\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \}$ e com as quais, adicionando o conjunto $\{n\}$, se obtêm todas as partições deste tipo, .
2. *Partições tais que n está contido num subconjunto de cardinalidade superior de 1.* Neste caso, estamos na presença de partições do conjunto $\{1, \dots, n-1\}$ em k subconjuntos (cujo número é $\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \}$), num dos quais devemos inserir o elemento n (para o que existem k possibilidades) para se obterem as partições pretendidas. Como consequência, existem $k \{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \}$ partições deste tipo.

Tendo em conta 1 e 2, obtém-se a igualdade pretendida, ou seja,

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = \begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix} + k \begin{Bmatrix} n-1 \\ k \end{Bmatrix}. \quad \square$$

No Exemplo 4.12, utilizando a fórmula de Daniel da Silva, determinámos o número de funções sobrejectivas definidas num conjunto de cardinalidade n e com imagem num conjunto de cardinalidade k . No exemplo a seguir, vamos determinar este mesmo número recorrendo aos números de Stirling.

Exemplo 6.12. Vamos calcular o número de funções sobrejectivas definidas no conjunto $\{1, 2, \dots, n\}$ e com imagem no conjunto $\{1, 2, \dots, k\}$.

Solução. Observe-se que para cada função sobrejectiva $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, k\}$, os conjuntos $f^{-1}(1), f^{-1}(2), \dots, f^{-1}(k)$, constituem uma partição do conjunto $\{1, 2, \dots, n\}$ em k subconjuntos não vazios. Por outro lado, a cada partição do conjunto $\{1, 2, \dots, n\}$ em k subconjuntos não vazios correspondem $k!$ funções sobrejectivas distintas. Como consequência, podemos concluir que o número de funções sobrejectivas definidas no conjunto $\{1, 2, \dots, n\}$ e com imagens no conjunto $\{1, 2, \dots, k\}$, é a igual a

$$k! \begin{Bmatrix} n \\ k \end{Bmatrix}. \quad (6.26) \quad \square$$

Tendo em conta os resultados obtidos para o número de funções sobrejectivas definidas num conjunto de cardinalidade n e imagem num conjunto de cardinalidade k , respectivamente, no Exemplo 4.12 e no Exemplo 6.12 (ver (4.8) e (6.26)), podemos concluir a seguinte fórmula para os números de Stirling de segunda espécie:

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = \frac{1}{k!} \sum_{i=0}^{k-1} (-1)^i \binom{k}{i} (k-i)^n.$$

Sabe-se que qualquer dos conjuntos³ $B_1 = \{x^0, x^1, \dots, x^n\}$ ou $B_2 = \{(x)_0, (x)_1, \dots, (x)_n\}$ constitui uma base para os espaços de polinómios de grau não superior a n , ou seja, qualquer polinómio de grau não superior a n , $p_n(x)$, pode ser obtido, de forma única, como combinação linear de elementos de B_1 ou como combinação linear de elementos de B_2 , respectivamente.⁴ Em muitos casos, porém, tem interesse passar da base B_1 para a base B_2 ou, reciprocamente, da base B_2 para a base B_1 . No exemplo a seguir, determinam-se os escalares que permitem estas mudanças de base.

Exemplo 6.13. Vamos mostrar as igualdades

$$x^n = \sum_{k=0}^n \begin{Bmatrix} n \\ k \end{Bmatrix} (x)_k, \quad (6.27)$$

$$(x)_n = \sum_{k=0}^n (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} x^k. \quad (6.28)$$

Solução.

1. *Demonstração da fórmula (6.27).* Inicialmente, vamos assumir que $x \in \mathbb{N}$ e calcular o número de funções $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, x\}$, recorrendo a dois métodos distintos. É claro que o número destas funções é igual a x^n . Por outro lado, podemos partir o conjunto de todas estas funções em subconjuntos de funções cujas imagens têm a mesma cardinalidade k . Uma vez

³Note-se que, de acordo com a definição, $(x)_i = x(x-1)\dots(x-(i-1))$.

⁴Dizer que $p_n(x)$ é combinação linear de elementos da base B_1 (B_2), significa que $\exists \alpha_1, \dots, \alpha_n \in \mathbb{R}$ tais que $p_n(x) = \sum_{i=0}^n \alpha_i b_i(x)$, com $b_i(x) = x^i$ ($b_i(x) = (x)_i$).

que, para cada k , existem $\binom{x}{k}$ maneiras de escolher a imagem destas funções e existem $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ funções sobrejectivas definidas num conjunto de cardinalidade n e com imagem num conjunto de cardinalidade k , então o número de funções $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, x\}$ é igual a

$$\sum_{k=1}^n \binom{x}{k} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}.$$

Como consequência, tendo em conta que, por definição de número binomial generalizado, $\binom{x}{k} k! = (x)_k$, obtém-se a igualdade

$$x^n = \sum_{k=1}^n (x)_k \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}, \quad (6.29)$$

quando $x \in \mathbb{N}$. Porém, umas vez que para n fixo os polinómios de grau n obtidos em ambos os lados da equação são únicos, podemos concluir que a equação polinomial (6.29) se verifica $\forall x \in \mathbb{R}$.

2. *Demonstração da fórmula (6.28).* Considerando a igualdade

$$(x)_n = \sum_{k=0}^n (-1)^{n-k} a_{n,k} x^k,$$

vamos mostrar que os coeficientes $a_{n,k}$ verificam a equação de recorrência para os números de Stirling de primeira espécie. Com efeito, observe-se que $(x)_n = (x)_{n-1}(x - n + 1)$ implica

$$\begin{aligned} (x)_n &= \sum_{k=0}^n (-1)^{n-k} a_{n,k} x^k = (x - n + 1) \sum_{k=0}^{n-1} (-1)^{n-k-1} a_{n-1,k} x^k \\ &= \sum_{k=0}^{n-1} (-1)^{n-k-1} a_{n-1,k} x^{k+1} - (n-1) \sum_{k=0}^{n-1} (-1)^{n-k-1} a_{n-1,k} x^k \\ &= \sum_{k=0}^n \left((-1)^{n-k} a_{n-1,k-1} - (n-1)(-1)^{n-k-1} a_{n-1,k} \right) x^k \\ &= \sum_{k=0}^n (-1)^{n-k} (a_{n-1,k-1} + (n-1)a_{n-1,k}) x^k \end{aligned}$$

Logo,

$$a_{n,k} = a_{n-1,k-1} + (n-1)a_{n-1,k},$$

e conclui-se que $a_{nn} = 1$ e $a_{n0} = 0$. Nestas condições, obtém-se uma equação de recorrência, com condições iniciais $a_{nn} = 1$ e $a_{n0} = 0$, cujos números de Stirling de primeira espécie são a única solução (ver (6.24)). \square

6.4. Números de Euler

Dada a permutação $\pi = (p_1, p_2, \dots, p_n)$ dos elementos do conjunto $\{1, \dots, n\}$, vamos designar por posição de crescimento, todo o índice $i < n$ tal que $p_i < p_{i+1}$.

Definição 6.6 (Número de Euler de primeira ordem). *Designa-se por número de Euler de primeira ordem, e denota-se por $\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle$, o número de permutações dos elementos do conjunto $\{1, \dots, n\}$, com k posições de crescimento.*

k	0	1	2	3	4	5	6	7	8	9
$n = 0$	1									
$n = 1$	1									
$n = 2$	1	1								
$n = 3$	1	4	1							
$n = 4$	1	11	11	1						
$n = 5$	1	26	66	26	1					
$n = 6$	1	57	302	302	57	1				
$n = 7$	1	120	1.191	2.416	1.191	120	1			
$n = 8$	1	247	4.293	15.619	15.619	4.293	247	1		
$n = 9$	1	502	14.608	88.234	15.6190	88.234	14.608	502	1	

Tabela 6.6: Números de Euler de primeira ordem, $\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle$.

Na Tabela 6.6, indicam-se todos os números de Euler de primeira ordem, para $n \leq 9$.

É claro que a soma dos números de permutações dos elementos do conjunto $\{1, \dots, n\}$, para todos os números de posições de crescimento possíveis é igual ao número de todas as permutações dos elementos deste conjunto, ou seja,

$$\sum_{k=0}^n \langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle = n!.$$

Teorema 6.5. Se $1 \leq k \leq n$, então os números de Euler de primeira ordem verificam a equação de recorrência

$$\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle = (n-k) \langle \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \rangle + (k+1) \langle \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \rangle, \quad (6.30)$$

com valores iniciais $\langle \begin{smallmatrix} n \\ 0 \end{smallmatrix} \rangle = 1$ e $\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle = 0$, para $k > n$.

Demonstração. Observe que as permutações dos elementos do conjunto $\{1, \dots, n\}$, com k posições de crescimento, podem ser obtidas a partir das permutações dos elementos do conjunto $\{1, \dots, n-1\}$, de duas maneiras distintas.

1. *A partir das permutações de $\{1, \dots, n-1\}$ com k posições de crescimento.* Note-se que, dada uma permutação de elementos do conjunto $\{1, \dots, n-1\}$, com k posições de crescimento, se inserirmos n à esquerda do primeiro elemento da permutação ou imediatamente após uma posição de crescimento, então a permutação permanece uma permutação com k posições de crescimento. Logo, desta forma, podemos construir $(k+1) \langle \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \rangle$ permutações de elementos do conjunto $\{1, \dots, n\}$, com k posições de crescimento.
2. *A partir de permutações de $\{1, \dots, n-1\}$ com $k-1$ posições de crescimento.* Note-se que, dada uma permutação de elementos do conjunto $\{1, \dots, n-1\}$, com $k-1$ posições de crescimento, se inserirmos n imediatamente após qualquer posição que não seja de crescimento, obtém-se uma permutação com k posições de crescimento. Logo, desta forma, podemos construir $(n-k) \langle \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \rangle$ permutações de elementos do conjunto $\{1, \dots, n\}$, com k posições de crescimento.

Tendo em conta 1 e 2, podemos concluir que existem

$$(n-k) \langle \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \rangle + (k+1) \langle \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \rangle$$

permutações de elementos do conjunto $\{1, \dots, n\}$, com k posições de crescimento. □

Considerem-se os conjuntos com repetições, $S_n^{(2)} = \{1, 1, 2, 2, 3, 3, \dots, n, n\}$, nos quais cada elemento aparece repetido, exactamente, uma vez e, para cada um destes conjuntos, denote-se o conjunto das permutações $\pi = (p_1, p_2, \dots, p_{2n})$ dos respectivos elementos, para as quais

$$\forall_{i < j} \left(p_i = p_j \Rightarrow \forall_{k \in \{i+1, \dots, j-1\}} p_i < p_k \right)$$

por $\Pi_n^{(2)}$.

Exemplo 6.14. Vamos provar por indução que $\forall_{n \in \mathbb{N}} |\Pi_n^{(2)}| = (2n - 1)!!$.

Solução. É claro que, para $n = 1$, existe unicamente a permutação $(1, 1)$, pelo que $|\Pi_1^{(2)}| = 1$. Suponha que o resultado é verdadeiro para $1 \leq n \leq k$. Assim, sabendo que $|\Pi_k^{(2)}| = (2k - 1)!!$, tendo em vista inserir os dois elementos $k + 1$ do conjunto $S_{k+1}^{(2)}$ em cada uma das permutações $\pi \in \Pi_k^{(2)}$, de modo a obter permutações $\pi' \in \Pi_{k+1}^{(2)}$, é imediato concluir que estes elementos são necessariamente vizinhos em π' . Logo, existem $2k + 1$ posições válidas para a respectiva inserção e, consequentemente,

$$|\Pi_{k+1}^{(2)}| = (2k + 1) |\Pi_k^{(2)}| = (2k + 1)(2k - 1)!! = (2k + 1)!!.$$

Deste modo, por indução, conclui-se que $\forall_{n \in \mathbb{N}} |\Pi_n^{(2)}| = (2n - 1)!!$. \square

Definição 6.7 (Número de Euler de segunda ordem). Designa-se por número de Euler de segunda ordem e denota-se por $\langle\!\langle n \rangle\!\rangle_k$, o número de permutações do conjunto $\Pi_n^{(2)}$, com k posições de crescimento.

Na Tabela 6.7 apresentam-se todos os números de Euler de segunda ordem não nulos, para $n \leq 8$, onde, por convenção, $\langle\!\langle 0 \rangle\!\rangle_0 = 1$.

k	0	1	2	3	4	5	6	7
$n = 0$	1							
$n = 1$	1							
$n = 2$	1	2						
$n = 3$	1	8	6					
$n = 4$	1	22	58	24				
$n = 5$	1	52	328	444	120			
$n = 6$	1	114	1.452	4.400	3.708	720		
$n = 7$	1	240	5.610	32.120	58.140	33.984	5.040	
$n = 8$	1	494	19.950	195.800	644.020	78.5304	341.136	40.320

Tabela 6.7: Números de Euler de segunda ordem $\langle\!\langle n \rangle\!\rangle_k$.

Uma vez que

$$|\Pi_n^{(2)}| = \sum_{k=0}^n \left| \{\pi \in \Pi_n^{(2)} : \text{número de posições de crescimento é } k\} \right|$$

e $\left| \{\pi \in \Pi_n^{(2)} : \text{número de posições de crescimento é } k\} \right| = \langle\!\langle n \rangle\!\rangle_k$, podemos concluir que

$$\sum_{k=0}^n \langle\!\langle n \rangle\!\rangle_k = |\Pi_n^{(2)}| = (2n - 1)!!.$$

Teorema 6.6. Se $1 \leq k \leq n$, então os números de Euler de segunda ordem verificam a equação de recorrência

$$\left\langle\!\left\langle \frac{n}{k} \right\rangle\!\right\rangle = (2n - 1 - k) \left\langle\!\left\langle \frac{n-1}{k-1} \right\rangle\!\right\rangle + (k+1) \left\langle\!\left\langle \frac{n-1}{k} \right\rangle\!\right\rangle, \quad (6.31)$$

com valores iniciais $\left\langle\!\left\langle \frac{n}{0} \right\rangle\!\right\rangle = 1$ e $\left\langle\!\left\langle \frac{n}{k} \right\rangle\!\right\rangle = 0$, para $k > n$.

Demonstração. Observe-se que as permutações dos elementos do conjunto $S_n^{(2)}$, com k posições de crescimento, podem ser obtidas a partir de permutações dos elementos do conjunto $S_{n-1}^{(2)}$, inserindo o par de elementos n e n , desde que estes ocupem posições sucessivas. Por outro lado, temos dois casos distintos a considerar.

1. *A partir de permutações de $S_{n-1}^{(2)}$, com k posições de crescimento.* Neste caso, dada uma permutação arbitrária $\pi \in \Pi_{n-1}^{(2)}$, com k posições de crescimento, ou inserimos os elementos sucessivos n e n à esquerda do primeiro elemento da permutação π , ou os inserimos imediatamente após uma posição de crescimento. Deste modo, o número de posições de crescimento que existia em π permanece o mesmo. Logo, com este tipo de construção, obtém-se $(k+1) \left\langle\!\left\langle \frac{n-1}{k} \right\rangle\!\right\rangle$ permutações de elementos do conjunto $S_n^{(2)}$, com k posições de crescimento.
2. *A partir de permutações de $S_{n-1}^{(2)}$, com $k-1$ posições de crescimento.* Neste caso, dada uma permutação $\pi \in \Pi_{n-1}^{(2)}$, com $k-1$ posições de crescimento, inserindo os elementos sucessivos n e n após qualquer posição que não seja de crescimento, obtém-se uma permutação com k posições de crescimento. Logo, com este tipo de construção, obtém-se $(2n - 1 - k) \left\langle\!\left\langle \frac{n-1}{k-1} \right\rangle\!\right\rangle$ permutações de elementos do conjunto $S_n^{(2)}$, com k posições de crescimento.

Tendo em conta 1 e 2, podemos concluir que existem

$$(2n - 1 - k) \left\langle\!\left\langle \frac{n-1}{k-1} \right\rangle\!\right\rangle + (k+1) \left\langle\!\left\langle \frac{n-1}{k} \right\rangle\!\right\rangle$$

permutações de elementos do conjunto $S_n^{(2)}$, com k posições de crescimento. □

6.5. Números de Bell

Definição 6.8 (Números de Bell). Designa-se por número de Bell e denota-se por B_n , com $n \geq 0$, o número de todas as partições de um conjunto de cardinalidade n em subconjuntos não vazios. Por convenção, assume-se $B_0 = 1$.

Por exemplo, para $n = 3$, tendo em conta que

$$\{\{1\}, \{2\}, \{3\}\}, \{\{1, 2\}, \{3\}\}, \{\{1, 3\}, \{2\}\}, \{\{2, 3\}, \{1\}\} \text{ e } \{\{1, 2, 3\}\},$$

é o conjunto de todas as partições do conjunto $\{1, 2, 3\}$, em subconjuntos não vazios, $B_3 = 5$. Na Tabela 6.8 apresentam-se os primeiros 13 números de Bell.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
B_n	1	1	2	5	15	52	203	877	4.140	21.147	115.975	678.570	4.213.597

Tabela 6.8: Números de Bell B_n , para $n \leq 12$.

No Exemplo 5.15 deduziu-se a equação de recorrência para os números de Bell:

$$B_{n+1} = \sum_{i=0}^n \binom{n}{i} B_i, \quad (6.32)$$

cuja solução, obtida no Exemplo 5.34, tem a forma:

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}. \quad (6.33)$$

Uma vez que B_n é inteiro (por definição) e a parte da série (6.33) obtida para termos de ordem superior a $2n$ tem soma inferior a 1, conclui-se a igualdade

$$B_n = \left\lceil \frac{1}{e} \sum_{k=1}^{2n} \frac{k^n}{k!} \right\rceil.$$

Tendo presente a definição de número de Stirling de segunda espécie, imediatamente se conclui a seguinte expressão para a determinação dos números de Bell:

$$B_n = \sum_{k=0}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}. \quad (6.34)$$

Verifica-se que alguns números de Bell são primos. Os primeiros primos de Bell (e únicos conhecidos), são $B_2, B_3, B_7, B_{13}, B_{42}, B_{55}$ e B_{2841} . O último destes primos foi obtido por I. L. Canistro, em 2004, depois de 17 meses de cálculos em computador.

Exemplo 6.15. Vamos determinar a função geradora exponencial dos números de Bell.

Solução. Por definição de função geradora exponencial vem que

$$\mathcal{B}(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n.$$

Logo, utilizando a fórmula (6.33), obtém-se

$$\begin{aligned} \mathcal{B}(x) &= \frac{1}{e} \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{k^n}{k!} \frac{x^n}{n!} = \frac{1}{e} \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=0}^{\infty} \frac{(kx)^n}{n!} \\ &= \frac{1}{e} \sum_{k=0}^{\infty} \frac{1}{k!} e^{kx} = \frac{1}{e} \sum_{k=0}^{\infty} \frac{(e^x)^k}{k!} = \frac{1}{e} e^{e^x} \end{aligned}$$

e, consequentemente,

$$\mathcal{B}(x) = e^{e^x - 1}$$

é a função geradora exponencial dos números de Bell. □

6.6. Números de Catalan

Os números de Catalan, embora pareçam ter uma definição abstracta, têm várias aplicações em problemas combinatórios.

Definição 6.9. Designa-se por n -ésimo número de Catalan e denota-se por C_n , com $n \geq 0$, o número que se obtém pela expressão:

$$C_n = \frac{1}{n+1} \binom{2n}{n}. \quad (6.35)$$

Na Tabela 6.9, apresentam-se os primeiros 13 números de Catalan. Observe-se que, tendo em conta várias relações conhecidas entre números binomiais, as expressões para os números de Catalan podem apresentar formas distintas mas equivalentes, conforme a seguir se exemplifica.

$$C_n = \frac{(2n)!}{(n+1)!n!} = \frac{(2n)_n}{(n+1)!} = \frac{2^n(2n-1)!!}{(n+1)!}.$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
C_n	1	1	2	5	14	42	132	429	1430	4.862	16.796	58.786	208.012

Tabela 6.9: Números de Catalan.

Os números de Catalan têm o nome do matemático belga Eugène Charles Catalan (1814–1894) que investigou algumas propriedades deste números. Sabe-se porém que, antes dele, o matemático alemão Johann Andreas von Segner (1704–1777), estudou estes números, tendo publicado em 1777 a equação de recorrência (6.36).

Exemplo 6.16. Vamos mostrar que os números de Catalan satisfazem a equação de recorrência

$$\begin{aligned} C_n &= \sum_{k=0}^{n-1} C_k C_{n-1-k} \\ &= C_0 C_{n-1} + C_1 C_{n-2} + \cdots + C_{n-2} C_1 + C_{n-1} C_0, \end{aligned} \quad (6.36)$$

com valor inicial $C_0 = 1$. Note-se que esta equação de recorrência também pode ser utilizada para definir números de Catalan.

Solução. Seja a_n a solução da equação de recorrência (6.36). Então $a_0 = 1$ e $a_n = \sum_{k=0}^{n-1} a_k a_{n-1-k}$, para $n \geq 1$. Assim, sendo $\mathcal{C}(x)$ a função geradora para os números a_n que satisfazem a equação de recorrência (6.36), vem

$$\begin{aligned} \mathcal{C}(x) &= \sum_{n=0}^{\infty} a_n x^n \\ &= 1 + \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} a_k a_{n-1-k} x^n \\ &= 1 + x \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} (a_k x^k)(a_{n-1-k} x^{n-1-k}) \\ &= 1 + x \sum_{k=0}^{\infty} a_k x^k \sum_{n=k+1}^{\infty} a_{n-1-k} x^{n-1-k}. \end{aligned}$$

Fazendo $i = n - 1 - k$, obtém-se

$$\mathcal{C}(x) = 1 + x \sum_{k=0}^{\infty} a_k x^k \sum_{i=0}^{\infty} a_i x^i = 1 + x \mathcal{C}^2(x),$$

onde se retira a equação funcional $x\mathcal{C}^2(x) - \mathcal{C}(x) + 1 = 0$, cujas soluções são

$$\mathcal{C}_1(x) = \frac{1 - \sqrt{1 - 4x}}{2x} \quad \text{e} \quad \mathcal{C}_2(x) = \frac{1 + \sqrt{1 - 4x}}{2x},$$

uma das quais é a função geradora dos números a_n . Tendo em conta que $\mathcal{C}(0) = a_0 = 1$, $\lim_{x \rightarrow 0} \mathcal{C}_1(x) = 1$ e $\lim_{x \rightarrow 0} \mathcal{C}_2(x)$ não existe, podemos concluir as igualdades

$$\mathcal{C}(x) = \mathcal{C}_1(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

Tendo em vista a determinação dos coeficientes da função geradora $\mathcal{C}(x)$, utilizando (5.32), obtém-se

$$\sqrt{1 - 4x} = (1 - 4x)^{1/2} = \sum_{k=0}^{\infty} \frac{(1/2)_k}{k!} (-4x)^k = \sum_{k=0}^{\infty} \binom{1/2}{k} (-4x)^k,$$

onde, por (6.5), se conclui que

$$\sqrt{1 - 4x} = 1 + \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{4^{k-1} \cdot 2k} \binom{2k-2}{k-1} (-4x)^k = 1 - 2 \sum_{k=1}^{\infty} \frac{1}{k} \binom{2k-2}{k-1} x^k.$$

Finalmente,

$$\mathcal{C}(x) = \sum_{k=1}^{\infty} \frac{1}{k} \binom{2k-2}{k-1} x^{k-1} = \sum_{k=0}^{\infty} \frac{1}{k+1} \binom{2k}{k} x^k,$$

onde decorre que $a_k = \frac{1}{k+1} \binom{2k}{k} = C_k$. □

Como consequência dos desenvolvimentos anteriores, podemos concluir que a função geradora dos números de Catalan pode tomar a forma

$$\mathcal{C}(x) = \sum_{n=0}^{\infty} C_n x^n = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

Seguem-se alguns exemplos de aplicação dos números de Catalan.

Exemplo 6.17. Considerando o produto de $n+1$ números $x_0 x_1 \dots x_n$, suponha que se pretende inserir parêntesis nesta expressão de tal forma que se defnam rigorosamente todos os produtos de pares de factores. Suponha ainda que estamos interessados em saber o número de possibilidades de inserção dos parêntesis em tais condições. Por exemplo,

- para $n = 2$, existem duas possibilidades de inserção de parêntesis:

$$(x_0 x_1) x_2 \text{ e } x_0 (x_1 x_2);$$

- para $n = 3$, existem cinco possibilidades:

$$x_0((x_1 x_2) x_3), x_0(x_1(x_2 x_3)), (x_0 x_1)(x_2 x_3), ((x_0 x_1) x_2) x_3 \text{ e } (x_0(x_1 x_2)) x_3.$$

Vamos mostrar que o número de possibilidades de inserir parêntesis no produto de $n+1$ números é igual ao número de Catalan C_n .

Solução. Denotando o número de possibilidades de inserção de parêntesis no produto de $n + 1$ números por a_n , uma vez que $a_0 = a_1 = 1$, basta mostrar que os números a_n satisfazem a equação de recorrência (6.36).

Observe-se que cada par de parêntesis externos (ou seja, aqueles que não estão contidos noutras parêntesis) divide o produto em duas partes, a primeira de x_0 até x_k e a segunda de x_{k+1} até x_n , para um certo k . Por exemplo, em $(x_0x_1)(x_2x_3)$, considerando um dos pares de parêntesis externos, obtém-se $k = 1$, e em $x_0((x_1x_2)x_3)$ considerando o único par de parêntesis externos, obtém-se $k = 0$. Como consequência, podemos determinar o número de possibilidades de inserção de parêntesis, para cada valor de k , multiplicando o número de possibilidades de inserção de parêntesis no produto $x_0 \cdots x_k$ (que é a_k) pelo número de possibilidades de inserção de parêntesis no produto $x_{k+1} \cdots x_n$ (que é a_{n-k-1}). Logo, obtém-se a equação de recorrência

$$a_n = \sum_{k=0}^{n-1} a_k a_{n-k-1}$$

que é equivalente à equação (6.36). Finalmente, dada a unicidade de solução e as condições iniciais desta equação, conclui-se que $a_k = C_k$, para $k \geq 0$. \square

Exemplo 6.18. Considerem-se as sequências binárias de comprimento $2n$, com n zeros e n uns, as quais se designam por totalmente equilibradas quando, para cada k ($1 \leq k \leq 2n$), nos k primeiros dígitos binários o número de zeros é não inferior ao número de uns. Por exemplo,

- para $n = 1$, existe uma única sequência binária totalmente equilibrada (01);
- para $n = 2$, existem duas sequências binárias totalmente equilibradas (0011 e 0101);
- para $n = 3$, existem cinco sequências binárias totalmente equilibradas (000111, 001011, 001101, 010011 e 010101).

Vamos mostrar que o número de sequências binárias totalmente equilibradas de comprimento $2n$ é igual ao número de Catalan C_n .

Solução. Denotando o número de sequências binárias totalmente equilibradas de comprimento $2n$ por a_n , conforme se referiu, sabe-se que $a_1 = 1$, $a_2 = 2$ e $a_3 = 5$. Por outro lado, uma vez que a sequência vazia é única, $a_0 = 1$.

Observando que o número total de sequências binárias (não necessariamente totalmente equilibradas) com n zeros e n uns é igual $\binom{2n}{n}$ (ver Exemplo 4.5), vamos determinar o número de sequências binárias com n zeros e n uns que não são totalmente equilibradas. Por simplicidade, vamos designar estas sequências por sequências complementares.

Assim, se (a_1, \dots, a_{2n}) é uma sequência complementar, então existe um índice i relativamente ao qual, na subsequência (a_1, \dots, a_i) o número de zeros é inferior ao número de uns. Sendo k o menor destes índices i , é claro que é ímpar e é tal que $1 \leq k \leq 2n - 1$. Considere-se a função φ definida no conjunto das sequências complementares, tal que

$$\varphi(a_1, \dots, a_{2n}) = (1 - a_1, \dots, 1 - a_k, a_{k+1}, \dots, a_{2n}).$$

Por exemplo, dada a sequência complementar 011010, vem que $k = 3$ e $\varphi(011010) = 100010$.

Vamos mostrar que função φ é uma bijecção entre o conjunto das sequências complementares e o conjunto S_{2n} de todas as sequências com $n + 1$ zeros e $n - 1$ uns. Para tal, basta provar (1) que a imagem de uma sequência complementar pertence a S_{2n} (2) que φ é injectiva e (3) que φ é sobrejectiva.

1. Seja $a = a_1, \dots, a_{2n}$, uma sequência complementar e $k = 2j - 1$, com $j \in \mathbb{N}$, pelo que nos primeiros k dígitos binários de a existem j uns e $j - 1$ zeros. Então, nos primeiros k dígitos binários de $\varphi(a)$, existem $j - 1$ uns e j zeros. Como consequência, na imagem por φ de qualquer sequência complementar, o número de uns decresce de uma unidade e o número de zeros cresce de uma unidade. Logo, $\varphi(a)$ tem $n + 1$ zeros e $n - 1$ uns, ou seja, $\varphi(a) \in S_{2n}$.
2. Sejam $a = (a_1, \dots, a_{2n})$ e $b = (b_1, \dots, b_{2n})$ duas sequências complementares distintas e sejam k_a e k_b os valores de k , respectivamente, para a e para b . Sem perda de generalidade, podemos assumir que $k_a \leq k_b$. Dado que $a \neq b$, existe um índice i tal que $a_i \neq b_i$ e, adicionalmente,
 - se $k_a = k_b$, então $\varphi(a)_i \neq \varphi(b)_i$;
 - se $k_a < k_b$ então podemos admitir que $i \leq k_a$ e, consequentemente, que $\varphi(a)_i \neq \varphi(b)_i$.

Logo, em ambos os casos se conclui que $a \neq b \Rightarrow \varphi(a) \neq \varphi(b)$.

3. Seja $a = (a_1, \dots, a_{2n}) \in S_{2n}$, ou seja, a é uma sequência com $n + 1$ zeros e $n - 1$ uns. Seja r o menor índice, para o qual nos r primeiros dígitos binários de a o número de zeros é superior ao número de uns. Então $(1 - a_1, \dots, 1 - a_r, a_{r+1}, \dots, a_{2n})$ é uma sequência complementar e

$$\varphi(1 - a_1, \dots, 1 - a_r, a_{r+1}, \dots, a_{2n}) = (a_1, \dots, a_{2n}),$$

pelo que φ é sobrejectiva.

Logo, o número de sequências complementares é igual a $|S_{2n}|$. Finalmente, uma vez que o número de sequências de comprimento $2n$, com n uns é $\binom{2n}{n}$ e $|S_{2n}| = \binom{2n}{n-1} = \frac{n}{n+1} \binom{2n}{n}$, podemos concluir que o número de sequências binárias totalmente equilibradas de comprimento $2n$ vem dado por

$$\binom{2n}{n} - \frac{n}{n+1} \binom{2n}{n} = \frac{1}{n+1} \binom{2n}{n} = C_n.$$

□

Exemplo 6.19. Considerem-se as tabelas com duas linhas e n colunas. Nestas tabelas estamos interessados em escrever os números do conjunto $[2n]$, de tal forma que, quer em linha (da esquerda para a direita), quer em coluna (de cima para baixo), os números cresçam. Por exemplo,

- para $n = 1$, existe uma única tabela: $\begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline \end{array}$;
- para $n = 2$, existem apenas duas tabelas distintas: $\begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array}$ e $\begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array}$;
- para $n = 3$, existem apenas cinco tabelas distintas:
 $\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline \end{array}$, $\begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 3 & 5 & 6 \\ \hline \end{array}$, $\begin{array}{|c|c|c|} \hline 1 & 2 & 5 \\ \hline 3 & 4 & 6 \\ \hline \end{array}$, $\begin{array}{|c|c|c|} \hline 1 & 3 & 4 \\ \hline 2 & 5 & 6 \\ \hline \end{array}$ e $\begin{array}{|c|c|c|} \hline 1 & 3 & 5 \\ \hline 2 & 4 & 6 \\ \hline \end{array}$.

Vamos mostrar que o número destas tabelas de ordem $2 \times n$ é igual ao número de Catalan C_n .

Solução. Para fazer esta prova, basta definir uma bijecção entre o conjunto das sequências binárias totalmente equilibradas de comprimento $2n$ e o conjunto destes tabelas de ordem $2 \times n$ (ver Exemplo 6.18). Com efeito, dada uma sequência binária totalmente equilibrada $a = a_1, \dots, a_{2n}$ definindo-se a função φ cujo domínio é o conjunto das sequências binárias totalmente equilibradas, tal que $\varphi(a)$ é uma tabela de ordem $2 \times n$, onde a primeira linha contém, por ordem crescente, os índices dos dígitos binários da sequência a com valor zero e a segunda linha contém, por ordem crescente, os índices dos dígitos binários com valor 1. Por exemplo,

$$\varphi(0010011101) = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 4 & 5 & 9 \\ \hline 3 & 6 & 7 & 8 & 10 \\ \hline \end{array}.$$

Nestas condições, verifica-se que φ é uma bijecção entre o conjunto das sequências binárias totalmente equilibradas de comprimento $2n$ e o conjunto das tabelas de ordem $2 \times n$ acima referidas. \square

6.7. Exercícios

6.1. Mostre que para os números $(x)_n$ se verifica equação de tipo binomial

$$(x+y)_n = \sum_{k=0}^n \binom{n}{k} (x)_k (y)_{n-k}$$

(observe-se que, por definição, $(x)_0 = 1$).

6.2. Mostre que o número de ouro Φ pode ser determinado pelas expressões:

(a)

$$\Phi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}},$$

(b)

$$\Phi = \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{\dots}}}}}.$$

6.3. Mostre que os números de Fibonacci satisfazem a igualdade

$$F_{n+1} F_{n-1} - F_n^2 = (-1)^n, \quad (6.37)$$

designada por igualdade de Cassini (Jean-Dominique Cassini, demonstrou esta igualdade em 1680).

6.4. Mostre que os números de Lucas verificam as igualdades

(a) $L_0 + L_1 + L_2 + \dots + L_n = L_{n+2} - 1,$

(b) $L_1 + L_3 + L_5 + \dots + L_{2n+1} = L_{2n+2} - 2.$

6.5. Considerem-se os perfis montanhosos ("mountain ranges") desenhados com pontos e segmentos de recta, entre $(0,0)$ e $(2n,0)$, de tal forma que qualquer segmento de recta com coeficiente angular positivo é determinado por um par de pontos consecutivos $((x,y), (x+1, y+1))$ e qualquer segmento de recta com coeficiente angular negativo é determinado por um par de pontos consecutivos $((x,y), (x+1, y-1))$. Adicionalmente, a coordenada y nunca é negativa. Nestas condições, mostre que o número destes perfis é igual ao número de Catalan C_n .

6.6. Mostre que o número de modos de dividir um polígono regular de $n+2$ lados em n triângulos, com diagonais que não se intersectam, é igual ao número de Catalan C_n . Este problema é conhecido por *problema de Euler da divisão do polígono* ("Euler polygon division problem").

6.7. Considerando uma área reticular de dimensão $2 \times n$ que dispõe de azulejos de dimensão 1×2 , mostre que existem F_{n+1} maneiras de cobrir a área com os azulejos (onde F_n denota o n -ésimo número de Fibanacci).

6.8. Mostre que para $n, m \in \mathbb{N}$, $F_{n+m-1} = F_n F_m + F_{n-1} F_{m-1}$.

6.9. Mostre que

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix},$$

onde $n \in \mathbb{N}$ e se supõe $F_0 = 0$.

6.10. Prove que F_{3n} é par.

6.11. Prove que F_{5n} é divisível por 5.

6.12. Prove que para todo $n \in \mathbb{N}$

- (a) $F_n^2 + F_{n-1}^2 = F_{2n-1}$;
- (b) $F_n^2 - F_{n-1}^2 = F_{n-2} F_{n+1}$.

6.13. Prove que para todo $n \in \mathbb{N}$

- (a) $\sum_{k=0}^n \binom{n}{k} F_k = F_{2n}$;
- (b) $\sum_{k=0}^n \binom{n}{k} F_{k+1} = F_{2n+1}$.

6.14. Prove que para todo $n \in \mathbb{N}$

- (a) $F_{2n} = F_n L_n$;
- (b) $2F_{n+k} = F_n L_k + F_k L_n$;
- (c) $2L_{n+k} = 5F_n F_k + L_n L_k$;
- (d) $L_{4n} = L_{2n}^2 - 2$;
- (e) $L_{4n+2} = L_{2n+1}^2 + 2$.

6.15. Mostre que o número de colocações de n pessoas em k mesas redondas é igual $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$.

6.16. Determine formulas para $\left[\begin{smallmatrix} n \\ 2 \end{smallmatrix} \right]$, $\left[\begin{smallmatrix} n \\ 3 \end{smallmatrix} \right]$, $\left[\begin{smallmatrix} n \\ n-3 \end{smallmatrix} \right]$ e $\left[\begin{smallmatrix} n \\ n-2 \end{smallmatrix} \right]$.

6.17. Mostre que o número de colocações de n pessoas em k quartos de tal modo que nenhum quarto fique vazio é igual a $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$.

6.18. Mostre que o número de números que são produto de n primos e podem ser representados como um produto de k factores superiores a um é igual $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$.

6.19. Determine formulas para $\left\{ \begin{smallmatrix} n \\ 3 \end{smallmatrix} \right\}$, $\left\{ \begin{smallmatrix} n \\ n-3 \end{smallmatrix} \right\}$, $\left\{ \begin{smallmatrix} n \\ n-2 \end{smallmatrix} \right\}$.

6.20. Demonstre a desigualdade $n! \leq \left\{ \begin{smallmatrix} 2n \\ n \end{smallmatrix} \right\} \leq (2n)!$.

6.21. Demonstre a igualdade

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} i^n.$$

6.22. Demonstre que o número de números que são produto de n primos e podem ser representado como um produto de diferentes factores é igual a B_n .

6.23. Demonstre que o número de relações de equivalência que se podem definir num conjunto de cardinalidade n é igual a B_n .

6.24. Demonstre a desigualdade $B_n \leq n!$.

6.25. Demonstre a igualdade $\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle = \left\langle \begin{smallmatrix} n \\ n-k-1 \end{smallmatrix} \right\rangle$.

6.26. Demonstre as igualdades

$$(a) \sum_{k=0}^n \langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle \binom{m+k}{n} = m^n;$$

$$(b) \sum_{k=0}^n \langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle \binom{k}{n-m} = m! \left\{ \begin{smallmatrix} n \\ m \end{smallmatrix} \right\}.$$

6.27. Demonstre que o número de caminhos mais curtos na grelha de dimensão $n \times n$ entre os pontos $A = (0, 0)$ e $B = (n, n)$, sem cruzarem a diagonal principal (que liga A e B) é igual C_n .

6.28. Demonstre as igualdades

$$(a) \left\{ \begin{smallmatrix} x \\ x-n \end{smallmatrix} \right\} = \sum_{k=0}^n \langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle \binom{x+n-1-k}{2n};$$

$$(b) \left[\begin{smallmatrix} x \\ x-n \end{smallmatrix} \right] = \sum_{k=0}^n \langle \begin{smallmatrix} n \\ k \end{smallmatrix} \rangle \binom{x+k}{2n}.$$

6.29. Demonstre a igualdade $\text{mdc}(F_n, F_m) = F_{\text{mdc}(m,n)}$, onde $\text{mdc}(x, y)$ denota o máximo divisor comum entre x e y .

6.30. Demonstre a seguinte lei de inversão para os números de Stirling

$$g(n) = \sum_{k=0}^n \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} (-1)^k f(k) \iff f(n) = \sum_{k=0}^n \left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] (-1)^k g(k).$$

6.31. Demonstre as igualdades $\langle \begin{smallmatrix} n \\ 0 \end{smallmatrix} \rangle = 1$, $\langle \begin{smallmatrix} n \\ 1 \end{smallmatrix} \rangle = 2^n - n - 1$ e $\langle \begin{smallmatrix} n \\ 2 \end{smallmatrix} \rangle = 3^n - (n+1)2^n + \binom{n}{2}$.

6.32. Estendendo aos inteiros negativos as equações de recorrência que definem os números de Stirling, demonstre a igualdade $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = \left\{ \begin{smallmatrix} -n \\ -k \end{smallmatrix} \right\}$.

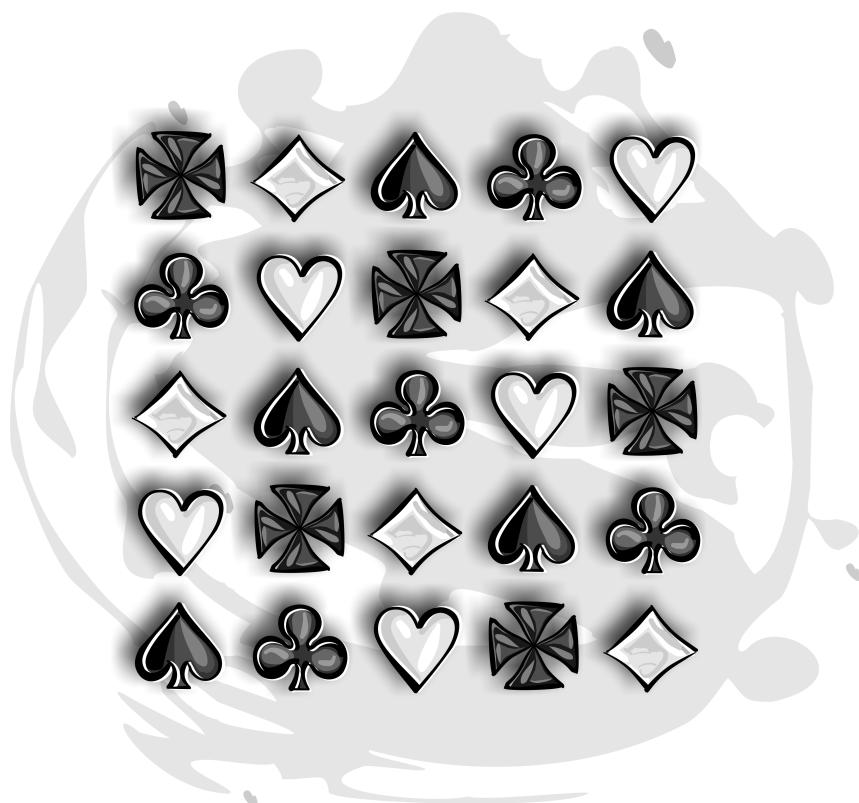
6.33. Demonstre a igualdade

$$\sum_k \left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] \left\{ \begin{smallmatrix} k \\ m \end{smallmatrix} \right\} (-1)^{n-k} = \sum_k \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} \left[\begin{smallmatrix} k \\ m \end{smallmatrix} \right] (-1)^{n-k} = \delta_{m,k},$$

onde $\delta_{m,k}$ denota a função delta de Kronecker (ou seja, $\delta_{m,k} = 1$ se $m = k$ e $\delta_{m,k} = 0$ no caso contrário).

Parte III

Abordagens Algébricas da Combinatória



7

Conjuntos Parcialmente Ordenados e Reticulados

A *teoria dos conjuntos parcialmente ordenados* é um instrumento essencial em *combinatória*. Com efeito, verifica-se que muitas questões de natureza combinatória podem ser resolvidas, com vantagem, recorrendo a resultados decorrentes da teoria dos conjuntos parcialmente ordenados. Trata-se de uma teoria que é crucial para a *teoria dos reticulados*, *teoria dos grafos*, *álgebras de Boole*, *topologia digital*, etc.

7.1. Conjuntos ordenados – definições básicas

Tal com se referiu na Secção 1.6.1, uma relação binária diz-se uma relação de ordem parcial se e só se é reflexiva, anti-simétrica e transitiva.

Definição 7.1 (Conjunto parcialmente ordenado). *Dada uma relação de ordem parcial \mathcal{R} (que também vamos denotar por \preceq) definida num conjunto X , o par (X, \mathcal{R}) (ou (X, \preceq)) designa-se por conjunto parcialmente ordenado (poset na terminologia inglesa¹) que se abrevia por cpo.*

Dados dois elementos $x, y \in X$, algumas vezes escrevemos $x \prec y$ para indicar que $x \preceq y$ e $x \neq y$. Escreve-se também $x \not\preceq y$ para indicar que $x \preceq y$ é falso.

Para distinguir as diferentes relações de ordem parcial definidas num conjunto X , representamos cada conjunto parcialmente ordenado por $P = (X, \mathcal{R}_P)$, onde \mathcal{R}_P denota a relação de ordem parcial que em X define P . Quando não existem dúvidas, o conjunto parcialmente ordenado $P = (X, \mathcal{R}_P)$ denota-se, simplesmente, por $P = (X, \mathcal{R})$.

Definição 7.2 (Elementos comparáveis). *Dado o conjunto parcialmente ordenado $P = (X, \preceq)$, dois elementos $x, y \in X$ dizem-se elementos \preceq -comparáveis (ou, simplesmente, comparáveis, quando não há lugar a confusão) se $x \preceq y$ ou $y \preceq x$.*

De modo equivalente, uma vez que uma relação é um subconjunto do produto cartesiano X^2 , x e y são \preceq -comparáveis se e só se

$$\{(x, y), (y, x)\} \cap \mathcal{R} \neq \emptyset.$$

Exemplo 7.1. Considerando o conjunto parcialmente ordenado $(\mathcal{P}(\mathbb{N}), \subseteq)$ vamos indicar alguns elementos comparáveis e alguns elementos não comparáveis.

¹"Poset" é a abreviatura de *Partially Ordered Set*.

Solução. Sendo $A = \{1, 2, 3\} \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9\} = B$, os conjuntos A e B são comparáveis. Considerando $C = \{5, 10, 15, 20\}$, vem que $A \not\subseteq C$ e $C \not\subseteq A$, pelo que A e C não são comparáveis. Analogamente, dado que $B \not\subseteq C$ e $C \not\subseteq B$, conclui-se que B e C também não são comparáveis. \square

Uma relação de ordem parcial \preceq definida num conjunto Y diz-se uma relação de ordem *total* (ou *linear*) se quaisquer dois elementos de Y são \preceq -comparáveis (ver Definição 7.2), ou seja, se

$$\forall_{x,y \in Y} \{(x,y), (y,x)\} \cap \preceq \neq \emptyset.$$

Considerando um conjunto parcialmente ordenado (X, \preceq) e dados dois elementos $x, y \in X$, diz-se que y *cobre* x se $x \prec y$ e $\nexists z \in X$ tal que $x \prec z \prec y$.

Os conjuntos parcialmente ordenados, representam-se, graficamente, por *diagramas de Hasse*² que são grafos não orientados nos quais a existência de uma aresta entre os vértices x e y , representada de modo ascendente, denota que y cobre x . Como consequência, a existência de um caminho entre os vértices x e y , constituído unicamente por arestas representadas de modo ascendente, significa $x \prec y$. A Figura 7.1 exemplifica a representação de um conjunto parcialmente ordenado por intermédio do respectivo diagrama de Hasse.

Definição 7.3 (Elemento maximal e elemento minimal). *Designa-se por elemento maximal de um conjunto parcialmente ordenado $P = (X, \preceq)$, todo o elemento $x \in X$ tal que $\forall_{y \in X} x \preceq y \Rightarrow x = y$. Os elementos mínimos em P são definidos do modo dual.*

Teorema 7.1. *Todo o subconjunto não vazio de um conjunto parcialmente ordenado finito tem um elemento maximal e um elemento minimal.*

Demonstração. Considere-se o conjunto parcialmente ordenado finito $P = (X, \preceq)$ e seja $Y \subseteq X$. Uma vez que $Y \neq \emptyset$, existe $y_1 \in Y$. Se $y_1 \in Y$ não é um elemento maximal em Y , então existe $y_2 \in Y$ tal que $y_1 \prec y_2$. Continuando este processo, uma vez que Y é finito (dado ser um subconjunto do conjunto finito X), ao fim de um número finito de passos obtém-se um elemento maximal. A prova da existência de um elemento minimal no subconjunto Y faz-se de modo análogo. \square

Definição 7.4 (Majorante, minorante, supremo, ínfimo). *Sejam (X, \preceq) um conjunto parcialmente ordenado e $A \subseteq X$. Diz-se que $a \in X$ é um majorante (minorante) para A se $\forall_{x \in A} x \preceq a$ (respectivamente, $\forall_{x \in A} a \preceq x$). Designa-se por supremo (ínfimo) de A e denota-se por $\sup A$ ($\inf A$) o menor (maior) dos majorantes (minorantes) de A , quando existem.*

No caso particular em que $|A| = 2$, escreve-se

$$x \vee y = \sup\{x, y\} \quad \text{e} \quad x \wedge y = \inf\{x, y\}.$$

Exemplo 7.2. Considerando o cpo $(D_{36}, |)$, constituído pelo conjunto de todos os divisores positivos de 36, $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, munido da relação de divisibilidade, vamos determinar o supremo e o ínfimo dos conjuntos $A = \{1, 2, 3, 4, 6\}$ e $B = \{2, 6, 12, 18\}$.

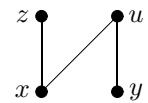


Figura 7.1: Diagrama de Hasse do conjunto parcialmente ordenado (X, \preceq) , com $X = \{u, x, y, z\}$ e $\preceq = \{(u,u), (x,x), (x,u), (x,z), (y,y), (y,u), (z,z)\}$.

²Helmut Hasse (1898–1979), matemático alemão que trabalhou em álgebra e que obteve resultados especialmente importantes para a teoria algébrica dos números.

Solução. Na Figura 7.2 representa-se o diagrama de Hasse do cpo $(D_{36}, |)$. Por definição, o conjunto dos majorantes de A é $\{12, 36\}$ e como consequência $\sup A = 12$. Analogamente, o conjunto dos majorantes de B é $\{36\}$, pelo que $\sup B = 36$.

Por sua vez, o conjunto dos minorantes de A é $\{1\}$, o que implica $\inf A = 1$ e o conjunto dos minorantes de B é $\{1, 2\}$, donde $\inf B = 2$. \square

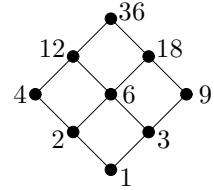


Figura 7.2: Diagrama de Hasse de $(D_{36}, |)$.

Exemplo 7.3. Vamos determinar o supremo e o ínfimo de cada um dos seguintes conjuntos parcialmente ordenados:

- (a) (X, \subseteq) , onde $X = \mathcal{P}(\{a, b, c\}) \setminus \{\emptyset\}$ (ver Figura 7.3-(a)),
- (b) (Y, \preceq) , onde $Y = \{a, b, c, d, e, f, g, h, i\}$ e a relação \preceq é definida pelo diagrama de Hasse representado na Figura 7.3-(b).

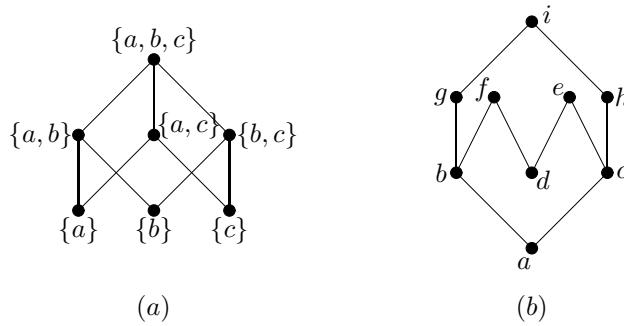


Figura 7.3: Diagramas de Hasse dos conjuntos parcialmente ordenados definidos no Exemplo 7.3.

Solução.

- (a) O conjunto de todos os elementos minimais de X é $\{\{a\}, \{b\}, \{c\}\}$. Uma vez que não existe o maior elemento minimal, também não existe $\inf X$. Por sua vez, o conjunto de elementos maximais de X é $\{\{a, b, c\}\}$, logo $\sup X = \{a, b, c\}$.
- (b) Uma vez que o conjunto de todos os elementos minimais de Y é $\{a, d\}$ e os elementos a e d não são comparáveis, não existe $\inf Y$. Por sua vez, o conjunto de elementos maximais de Y é o conjunto de elementos não comparáveis $\{e, f, i\}$, pelo que também não existe $\sup Y$. \square

Em geral, o conjunto de todos os subconjuntos próprios não vazios dum conjunto A de cardinalidade n tem n elementos minimais (todos os subconjuntos de cardinalidade 1) e n elementos maximais (todos os subconjuntos de cardinalidade $n - 1$), relativamente à relação de inclusão. Porém, como tanto os elementos minimais como os maximais não são comparáveis, não existe nem supremo nem ínfimo para o conjunto de subconjuntos próprios não vazios, munido da relação de inclusão.

Note-se que se um subconjunto A de um conjunto parcialmente ordenado $(\mathcal{P}(A) \setminus \{A, \emptyset\}, \subseteq)$ tem supremo (ínfimo), então $\sup A$ ($\inf A$) é único.

Exemplo 7.4. Seja $(\mathbb{N}, |)$ o conjunto parcialmente ordenado dos números naturais munido da relação de divisibilidade. Vamos determinar o supremo e o ínfimo de um subconjunto arbitrário, finito e não vazio, $A \subset \mathbb{N}$.

Solução. Por definição, os majorantes de A são todos os múltiplos comuns dos elementos de A e, como consequência, $\sup A = \text{mmc } A$ (onde mmc denota mínimo múltiplo comum). Analogamente, uma vez que os minorantes de A são todos os divisores comuns dos elementos de A , $\inf A = \text{mdc } A$ (onde mdc denota máximo divisor comum). \square

Exemplo 7.5. Seja $X = \{1, 2, 3\}$. Vamos determinar todos os conjuntos parcialmente ordenados que é possível definir em X .

Solução. Na Figura 7.4 apresentam-se os diagramas de Hasse de todos os conjuntos parcialmente ordenados definidos no conjunto $X = \{1, 2, 3\}$. \square

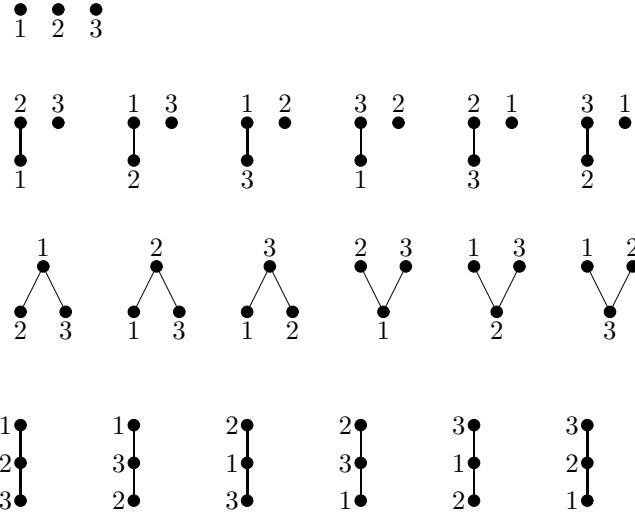


Figura 7.4: Diagramas de Hasse dos conjuntos parcialmente ordenados definidos em $\{1, 2, 3\}$.

Dado um cpo (X, \preceq) , a relação \succeq definida por $a \succeq b \Leftrightarrow b \preceq a$ designa-se por relação inversa de \preceq . Por sua vez, o conjunto parcialmente ordenado (X, \succeq) designa-se por conjunto parcialmente ordenado dual de (X, \preceq) . Na Figura 7.5 faz-se a representação de um conjunto parcialmente ordenado (X, \preceq) e do seu dual.

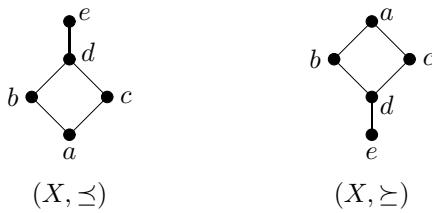


Figura 7.5: Diagramas de Hasse de conjuntos parcialmente ordenados duals.

7.2. Funções entre conjuntos parcialmente ordenados

Dados os conjuntos X e Y , onde estão definidas as relações binárias \mathcal{R}_X e \mathcal{R}_Y , respectivamente, diz-se que a função $f : X \rightarrow Y$ preserva as relações \mathcal{R}_X e \mathcal{R}_Y se

$$\forall_{x_1, x_2 \in X} (x_1, x_2) \in \mathcal{R}_X \Rightarrow (f(x_1), f(x_2)) \in \mathcal{R}_Y.$$

No caso particular das relações de ordem parcial temos a seguinte definição:

Definição 7.5 (Função isótona e isomorfismo). *Considerem-se os conjuntos parcialmente ordenados $\mathcal{P} = (P, \preceq_P)$ e $\mathcal{Q} = (Q, \preceq_Q)$ e uma função $f : P \rightarrow Q$.*

(1) *Diz-se que f preserva as ordens (ou é isótona) se*

$$\forall_{x,y \in P} x \preceq_P y \Rightarrow f(x) \preceq_Q f(y).$$

(2) *Diz-se que f é um isomorfismo entre P e Q se f é uma bijecção e*

$$\forall_{x,y \in P} x \preceq_P y \Leftrightarrow f(x) \preceq_Q f(y).$$

Quando existe um isomorfismo entre os conjuntos parcialmente ordenados \mathcal{P} e \mathcal{Q} diz-se que \mathcal{P} e \mathcal{Q} são isomorfos.

De modo equivalente, pode afirmar-se que a função $f : P \rightarrow Q$ é um isomorfismo entre os conjuntos parcialmente ordenado $\mathcal{P} = (P, \preceq_P)$ e $\mathcal{Q} = (Q, \preceq_Q)$ se e só se verifica as seguintes propriedades:

1. preserva as relações de ordem \preceq_P e \preceq_Q ,
2. admite inversa f^{-1} ,
3. e f^{-1} preserva as relações de ordem \preceq_Q e \preceq_P .

Exemplo 7.6. *Dados os conjuntos parcialmente ordenados $\mathcal{A} = (A, \preceq_A)$, $\mathcal{B} = (B, \preceq_B)$, $\mathcal{C} = (C, \preceq_C)$ e $\mathcal{Y} = (Y, \leq)$ representados pelos diagramas de Hasse da Figura 7.6. Vamos determinar quais das seguintes funções são isótomas e quais as que são isomorfismos.*

1. $f_1 : A \rightarrow Y$ tal que $f_1(a) = 3$, $f_1(b) = f_1(c) = 1$ e $f_1(d) = 2$;
2. $f_2 : B \rightarrow Y$ tal que $f_2(x) = 1$, $f_2(y) = f_2(u) = 2$ e $f_2(v) = f_2(w) = 3$;
3. $f_3 : C \rightarrow Y$ tal que $f_3(p) = 3$, $f_3(q) = 1$ e $f_3(r) = 2$.

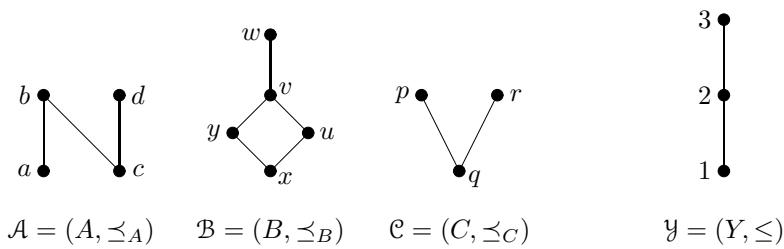


Figura 7.6: Diagramas de Hasse dos conjuntos parcialmente ordenados $\mathcal{A} = (A, \preceq_A)$, $\mathcal{B} = (B, \preceq_B)$, $\mathcal{C} = (C, \preceq_C)$ e $\mathcal{Y} = (Y, \leq)$.

Solução.

1. Uma vez que $a \preceq_A b$ e $f_1(a) = 3 \not\leq 1 = f_1(b)$ a função f_1 não é isótona e, como consequência, não é um isomorfismo.
2. Por verificação exaustiva conclui-se que f_2 preserva a ordem. Porém, uma vez que $|B| = 5$ e $|Y| = 3$, a função f_2 não é uma bijecção. Logo, f_2 é isótona mas não é um isomorfismo.

3. A função f_3 é isótoma e é uma bijecção mas não é um isomorfismo de ordem, uma vez que f_3^{-1} não é isótona (com efeito, $f_3(r) \leq f_3(p)$, mas p e q não são \preceq_C -comparáveis). \square

Exemplo 7.7. Dados os conjuntos parcialmente ordenados $(D_{30}, |)$ (onde D_{30} denota o conjunto dos divisores positivos de 30 e $|$ a relação de divisibilidade) e $(\mathcal{P}(Y), \subseteq)$, com $Y = \{2, 3, 5\}$, vamos demonstrar que são isomorfos.

Solução. Definindo a função $\Phi : D_{30} \rightarrow \mathcal{P}(Y)$ por $\Phi(n) = \{m \in Y : m|n\}$, é fácil verificar que Φ é um isomorfismo (ver Figura 7.7) \square

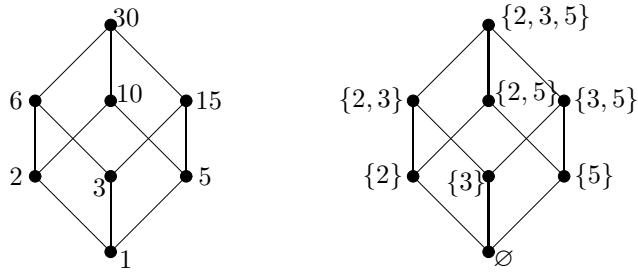


Figura 7.7: Diagramas de Hasse dos conjuntos parcialmente ordenados $(D_{30}, |)$ e $(\mathcal{P}(\{2, 3, 5\}), \subseteq)$.

Exemplo 7.8. Vamos demonstrar que os seguintes pares de conjuntos parcialmente ordenados são isomorfos

1. (\mathbb{N}, \leq) e $(2\mathbb{N}, \leq)$,
2. $(\mathcal{P}(X), \subseteq)$ e $(\mathcal{P}(X), \supseteq)$, onde X é um conjunto finito não vazio.

Solução.

1. Considerando a função $\Phi : \mathbb{N} \rightarrow 2\mathbb{N}$ tal que $\Phi(n) = 2n$, vem:
 - (a) $n \leq m \Leftrightarrow 2n \leq 2m \Leftrightarrow \Phi(n) \leq \Phi(m)$. Logo, Φ preserva a relação \leq .
 - (b) Existe a função inversa $\Phi^{-1} : 2\mathbb{N} \rightarrow \mathbb{N}$, definida por $\Phi^{-1}(n) = \frac{n}{2}$.
 - (c) Adicionalmente, uma vez que $n \leq m \Leftrightarrow \frac{n}{2} \leq \frac{m}{2} \Leftrightarrow \Phi^{-1}(n) \leq \Phi^{-1}(m)$, então Φ^{-1} preserva a relação \leq .

Logo, Φ é um isomorfismo e os conjuntos (\mathbb{N}, \leq) e $(2\mathbb{N}, \leq)$ são isomorfos.

2. Considerando a função $\Psi : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$, definida por $\Psi(A) = A^c$, onde $A^c = X \setminus A$, vem:
 - (a) $A \subseteq B \Leftrightarrow A^c \supseteq B^c \Leftrightarrow \Psi(A) \supseteq \Psi(B)$, pelo que Ψ preserva as relações \subseteq e \supseteq .
 - (b) Existe a função inversa $\Psi^{-1} : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ definida por $\Psi^{-1} = \Psi$,
 - (c) Utilizando o item 1, podemos concluir que $\Psi^{-1} = \Psi$ preserva as relações \supseteq e \subseteq .

Logo, Ψ é um isomorfismo e os conjuntos $(\mathcal{P}(X), \subseteq)$ e $(\mathcal{P}(X), \supseteq)$ são isomorfos. \square

Exemplo 7.9. Considerem-se três conjuntos totalmente ordenados $A = \{1 - \frac{1}{n} : n \in \mathbb{N}\}$, $B = A \cup \{1\}$ e \mathbb{N} relativamente à relação de ordem usual \leq . Vamos demonstrar que os conjuntos totalmente ordenados A e \mathbb{N} são isomorfos e que B e \mathbb{N} não são isomorfos.

Solução. Definindo-se a função $\Phi : \mathbb{N} \rightarrow A$ por $\Phi(n) = 1 - \frac{1}{n}$, por um lado conclui-se que Φ é uma bijecção e por outro lado que $m \leq n \Leftrightarrow 1 - \frac{1}{m} \leq 1 - \frac{1}{n} \Leftrightarrow \Phi(m) \leq \Phi(n)$. Logo, Φ e Φ^{-1} são funções isótonas e, consequentemente, Φ é um isomorfismo.

Vamos supor que a função $\Psi : B \rightarrow \mathbb{N}$ é um isomorfismo. Uma vez que 1 é um elemento maximal do B , vem que $\Psi(1)$ é um elemento maximal de \mathbb{N} o que, obviamente, constitui uma contradição. Como consequência, os conjuntos B e \mathbb{N} não são isomorfos. \square

Definição 7.6. Sendo (X, \preceq) um conjunto parcialmente ordenado, para $A \subseteq X$ e $x \in X$, define-se

$$1. \downarrow x = \{y \in X : y \preceq x\} \quad e \quad \uparrow x = \{y \in X : x \preceq y\},$$

$$2. \downarrow A = \bigcup_{a \in A} \downarrow a \quad e \quad \uparrow A = \bigcup_{a \in A} \uparrow a.$$

De modo equivalente, $\downarrow A$ e $\uparrow A$ podem definir-se, directamente, pelas igualdades

$$\downarrow A = \{y \in X : \exists_{a \in A} y \preceq a\} \quad e \quad \uparrow A = \{y \in X : \exists_{a \in A} a \preceq y\}.$$

Adicionalmente, deve observar-se que $A \subseteq X \Rightarrow A \subseteq \downarrow A \wedge A \subseteq \uparrow A$ e, tendo em conta a Definição 7.6, podemos concluir as igualdades

$$\downarrow(\downarrow A) = \downarrow A \text{ e } \uparrow(\uparrow A) = \uparrow A.$$

Se $A = \downarrow A$ diz-se que A é um conjunto *inferior* e se $A = \uparrow A$ diz-se que A é um conjunto *superior*. Denotando por $\mathcal{J}(X)$ o conjunto de todos subconjuntos inferiores de X , é claro que $(\mathcal{J}(X), \subseteq)$ é um conjunto parcialmente ordenado.

Exemplo 7.10. Dados os conjuntos parcialmente ordenados (X, \preceq_X) , (Y, \preceq_Y) e (Z, \preceq_Z) , definidos pelos diagramas de Hasse apresentados na Figura 7.8, vamos determinar os conjuntos parcialmente ordenados $(\mathcal{J}(X), \subseteq)$, $(\mathcal{J}(Y), \subseteq)$ e $(\mathcal{J}(Z), \subseteq)$.

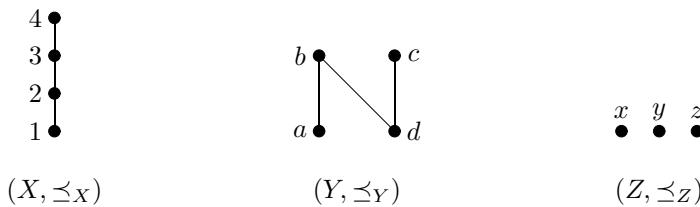


Figura 7.8: Diagramas de Hasse dos conjuntos parcialmente ordenados (X, \preceq_X) , (Y, \preceq_Y) e (Z, \preceq_Z) .

Solução. Tendo em conta que

$$\mathcal{J}(X) = \{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}\},$$

$$\mathcal{J}(Y) = \{\emptyset, \{a\}, \{d\}, \{a, d\}, \{c, d\}, \{a, b, d\}, \{a, c, d\}, \{a, b, c, d\}\} \text{ e}$$

$$\mathcal{J}(Z) = \mathcal{P}(Z),$$

obtém-se os conjuntos parcialmente ordenados representados pelos diagramas de Hasse da Figura 7.9. \square

7.3. Reticulados

Muitas das propriedades de um conjunto parcialmente ordenado (X, \preceq) podem ser expressas em termos da existências de supremo e/ou ínfimo para subconjuntos de X . Nesta secção, vamos estudar as propriedades dos conjuntos parcialmente ordenados, onde cada par de elementos tem um ínfimo e um supremo, os quais se designam por *reticulados*.

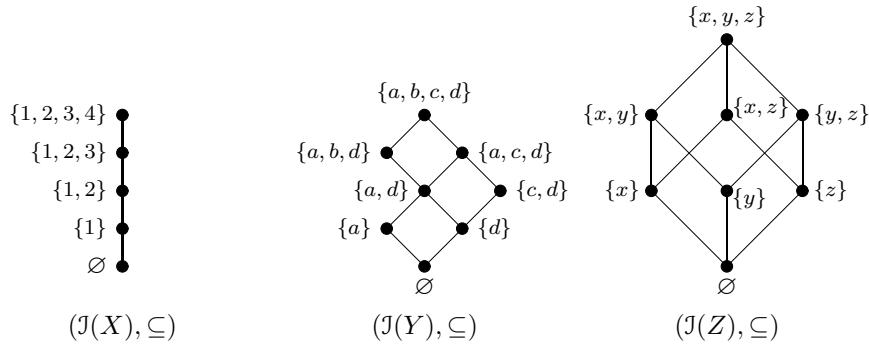


Figura 7.9: Diagramas de Hasse dos conjuntos parcialmente ordenados $(\mathcal{J}(X), \subseteq)$, $(\mathcal{J}(Y), \subseteq)$ e $(\mathcal{J}(Z), \subseteq)$.

7.3.1 Definições e conceitos básicos

Definição 7.7 (Reticulado). Um conjunto parcialmente ordenado (R, \preceq) diz-se um reticulado se para todo o par x, y de elementos de R existe o ínfimo $x \wedge y$ e o supremo $x \vee y$.

Antes da apresentação de alguns exemplos e propriedades dos reticulados, vamos introduzir o conceito de dualidade.

Propriedade de dualidade. O dual de qualquer proposição ou fórmula sobre um reticulado é a proposição ou fórmula que se obtém substituindo \vee por \wedge , \wedge por \vee , \preceq por \succeq e \succeq por \preceq . Neste condições, o dual de qualquer teorema da teoria dos reticulados é também uma teorema dessa mesma teoria.

Exemplo 7.11. Vamos determinar quais dos conjuntos parcialmente ordenados representados na Figura 7.10 são reticulados.

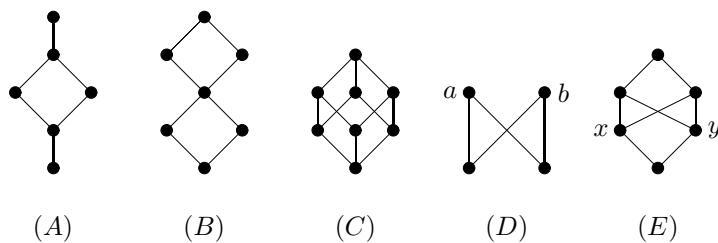


Figura 7.10: Diagramas de Hasse de alguns conjuntos parcialmente ordenados.

Solução. Pela verificação de cada par de elementos podemos concluir que os conjuntos parcialmente ordenados (A), (B) e (C) são reticulados e que (D) e (E) não são (note-se que em (D) não existe $a \vee b$ e em (E) não existe $x \vee y$). \square

Teorema 7.2. Seja (R, \preceq) um reticulado, então para $x, y \in R$ as seguintes afirmações são equivalentes:

1. $x \preceq y$,
2. $x \vee y = y$,
3. $x \wedge y = x$.

Demonstração.

1 ⇒ 2 Seja $x \preceq y$. Como, por definição de ordem parcial, \preceq é reflexiva, então $y \preceq y$ e, consequentemente, y é majorante tanto de x como de y , ou seja, $x \vee y = \sup\{x, y\} \preceq y$. Por outro lado, dado que por definição do supremo, $y \preceq x \vee y$, podemos concluir que $y = x \vee y$.

$2 \Rightarrow 1$ Seja $x \vee y = y$. Então y é majorante para o conjunto $\{x, y\}$ e, como consequência, é majorante para cada elemento deste conjunto, pelo que $x \preceq y$.

$1 \Leftrightarrow 3$ Esta prova é idêntica à anterior. \square

Teorema 7.3. *Seja (R, \preceq) um reticulado, então $\forall x, y, z \in R$ as operações binárias \vee e \wedge satisfazem as seguintes propriedades:*

- $x \vee (y \vee z) = (x \vee y) \vee z$ e $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, *(associatividade)*
- $x \vee y = y \vee x$ e $x \wedge y = y \wedge x$, *(comutatividade)*
- $x \vee (x \wedge y) = x$ e $x \wedge (x \vee y) = x$, *(absorção)*
- $x \vee x = x$ e $x \wedge x = x$. *(idempotência)*

Demonstração. As propriedades de comutatividade e de idempotência são consequência directa das definições de supremo e de ínfimo, pelo que resta demonstrar as propriedades de associatividades e de absorção (tendo em conta que cada uma delas se apresenta com a respectiva propriedade dual).

Absorção: Por definição, $x \vee (x \wedge y) = \sup\{x, \inf\{x, y\}\}$ e, uma vez que $\inf\{x, y\} \preceq x$, então $\sup\{x, \inf\{x, y\}\} = x$. Logo, $x \vee (x \wedge y) = x$.

Associatividade: Uma vez que $x \vee (y \vee z) = x \vee \sup\{y, z\} = \sup\{x, y, z\}$ e $(x \vee y) \vee z = \sup\{x, y\} \vee z = \sup\{x, y, z\}$, vem que $x \vee (y \vee z) = (x \vee y) \vee z$. \square

Sabe-se que um conjunto parcialmente ordenado é um reticulado quando existem o ínfimo e o supremo de todo o subconjunto de dois elementos. O Teorema 7.4, a seguir, estabelece um outro modo (equivalente) para se definir reticulado (enquanto estrutura algébrica), a partir das operações binárias \vee e \wedge que satisfazem as propriedades do Teorema 7.3.

Teorema 7.4. *Seja (R, \vee, \wedge) um conjunto não vazio R com duas operações binárias $\vee : R \times R \rightarrow R$ e $\wedge : R \times R \rightarrow R$ que satisfazem as propriedades de associatividade, comutatividade, absorção e idempotência (do Teorema 7.3). Se uma relação \preceq sobre R é definida por*

$$\forall_{x, y \in R} x \preceq y \Leftrightarrow x \vee y = y, \quad (7.1)$$

então (X, \preceq) é um reticulado em que as operações \vee e \wedge coincidem com o supremo e o ínfimo.

Demonstração. Primeiramente vamos mostrar que a relação binária \preceq é uma relação de ordem parcial sobre R . Com efeito, para cada $x, y, z \in R$ verificam-se as seguintes propriedades.

Reflexividade de \preceq : A idempotência de \vee (isto é, $x \vee x = x$) implica $x \preceq x$.

Anti-simetria de \preceq : Se $x \preceq y$ e $y \preceq x$, então $x \vee y = y$ e $y \vee x = x$. Logo, pela comutatividade de \vee , vem $x = y$.

Transitividade de \preceq : Se $x \preceq y$ e $y \preceq z$, então $x \vee y = y$ e $y \vee z = z$. Assim, $x \vee z = x \vee (y \vee z) = (x \vee y) \vee z = y \vee z = z$, pelo que $x \preceq z$.

Resta mostrar que $x \vee y = \sup\{x, y\}$ e $x \wedge y = \inf\{x, y\}$. Como efeito, $x \vee y = (x \vee x) \vee y = x \vee (x \vee y)$, pelo que (tendo em conta a definição de \preceq) $x \preceq x \vee y$. Analogamente se conclui que $y \preceq x \vee y$. Logo, $x \vee y$ é um majorante de $\{x, y\}$. Para provarmos que $x \vee y$ é o supremo (isto é, o menor dos majorantes) suponha-se que z é também um majorante de $\{x, y\}$. Então $x \preceq z$ e $y \preceq z$ e, consequentemente, $x \vee z = z$ e $y \vee z = z$. Logo, $(x \vee y) \vee z = x \vee (y \vee z) = x \vee z = z$, o que prova a desigualdade $x \vee y \preceq z$. Assim, $x \vee y$ é o menor majorante de $\{x, y\}$, pelo que $x \vee y = \sup\{x, y\}$.

Analogamente se demonstra que $x \wedge y = \inf\{x, y\}$. \square

Exemplo 7.12. Vamos demonstrar que as condições $x \vee y = y$ e $x \wedge y = x$ são equivalentes. Como consequência, a condição (7.1) pode ser escrita na seguinte forma:

$$\forall_{x,y \in R} x \preceq y \Leftrightarrow x \wedge y = x.$$

Solução. Se $x \vee y = y$, então $x \wedge y = x \wedge (x \vee y) = x$ (pela propriedade de absorção). Por outro lado, sendo $x \wedge y = x$, vem que $x \vee y = (x \wedge y) \vee y = y$ (pela propriedade de absorção). \square

Tendo em conta a equivalência das definições de um reticulado, respectivamente, pela relação \preceq e pelas operações binárias \vee e \wedge , muitas vezes denota-se um reticulado pelo quádruplo $(R, \preceq, \vee, \wedge)$. Por exemplo, se X é um conjunto não vazio, então para cada $A, B \subseteq X$ as operações $A \vee B = A \cup B$ e $A \wedge B = A \cap B$ verificam todas as propriedades do Teorema 7.3 e, por conseguinte, $(\mathcal{P}(X), \subseteq, \cup, \cap)$ denota um reticulado. Analogamente, tendo em conta o Exemplo 7.4, $(\mathbb{N}, |, \text{mmc}, \text{mdc})$ é também um reticulado.

Exemplo 7.13. Vamos definir o reticulado representado pelo dia-

grama de Hasse de Figura 7.11 por intermédio das tabelas das operações \vee e \wedge .

Solução. Pela Figura 7.11 vem que $R = \{0, a, b, c, 1\}$. Por sua vez, o resultado da operação $x \vee y$ corresponde ao menor elemento de R que é comum aos caminhos ascendentes percorridos a partir de x e de y . De modo análogo se define $x \wedge y$. Assim, podemos determinar as seguintes tabelas das operações \vee e \wedge :

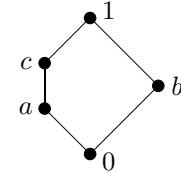


Figura 7.11: Diagrama de Hasse de um reticulado.

\vee	0	a	b	c	1	
0	0	a	b	c	1	
a	a	a	1	c	1	
b	b	1	b	1	1	
c	c	c	1	c	1	
1	1	1	1	1	1	

\wedge	0	a	b	c	1	
0	0	0	0	0	0	
a	0	a	0	a	a	
b	0	0	b	0	b	
c	0	a	0	c	c	
1	0	a	b	c	1	

\square

7.3.2 Subreticulados e isomorfismos

Definição 7.8 (Subreticulado). Seja $(R, \preceq, \vee, \wedge)$ um reticulado e M um subconjunto de R (ou seja, $M \subseteq R$), então M é um subreticulado de R se M é um reticulado para a restrição a M das operações \vee e \wedge (ou seja, se $a, b \in M$ então $a \vee b \in M$ and $a \wedge b \in M$).

Exemplo 7.14. Dado o reticulado $(D_{12}, |)$ de divisores positivos do número 12 com a relação de divisibilidade. Vamos verificar se os subconjuntos $M_1 = \{1, 2, 3, 6\}$ e $M_2 = \{1, 2, 3, 4\}$ são (ou não) subreticulados.

Solução. Por verificação exaustiva dos pares de elementos do conjunto M_1 vem que o supremo e o ínfimo de cada um deles pertencem ao conjunto M_1 . Como consequência, o conjunto M_1 constitui um subreticulado de D_{12} (ver Figura 7.12). No que diz respeito a M_2 , porém, uma vez que $3 \in M_2$ e $4 \in M_2$, mas $3 \vee 4 = \text{mmc}\{3, 4\} = 12 \notin M_2$, podemos concluir que não é um subreticulado. \square

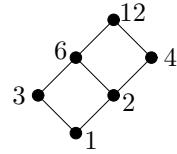


Figura 7.12: Diagrama de Hasse de $(D_{12}, |)$.

Definição 7.9 (Intervalo). Seja $(R, \preceq, \vee, \wedge)$ um reticulado e sejam $a, b \in R$ tais que $a \preceq b$, então o conjunto $[a, b] = \{x \in R : a \preceq x \preceq b\}$ designa-se por intervalo.

Exemplo 7.15. Vamos demonstrar que cada intervalo $[a, b]$ de um reticulado $(R, \preceq, \vee, \wedge)$ é um subreticulado e, considerando novamente o reticulado $(D_{12}, |)$, (ver Exemplo 7.14) vamos determinar o intervalo $[1, 6]$.

Solução. Se $x, y \in [a, b]$ então, pela definição de intervalo, $x \preceq b$ e $y \preceq b$. Logo, b é um majorante do conjunto $\{x, y\}$ e, como consequência, $x \vee y \preceq b$. Por outro lado, $a \preceq x \preceq x \vee y$, donde $a \preceq x \vee y \preceq b$, o que significa que $x \vee y \in [a, b]$. Analogamente se demonstra que $x \wedge y \in [a, b]$. Assim, uma vez que $x \vee y \in [a, b]$ e $x \wedge y \in [a, b]$, podemos concluir que $[a, b]$ é um subreticulado.

Por verificação exaustiva de todos os elementos de D_{12} , verifica-se que $[1, 6] = \{1, 2, 3, 6\}$ e, consequentemente, de acordo com o Exemplo 7.14, trata-se de um subreticulado.

Note-se que nem todos os elementos de um intervalo são comparáveis. Por exemplo, os elementos 2 e 3 do intervalo $[1, 6]$ não são comparáveis. \square

Definição 7.10 (Produto de reticulados). Sejam $(R_1, \preceq_1, \vee_1, \wedge_1)$ e $(R_2, \preceq_2, \vee_2, \wedge_2)$ dois reticulados. Considerando o produto cartesiano $R = R_1 \times R_2$, as operações binárias \vee e \wedge definem-se em R do seguinte modo. Quaisquer que sejam $a_1, b_1 \in R_1$ e quaisquer que sejam $a_2, b_2 \in R_2$

$$(1) \quad (a_1, a_2) \vee (b_1, b_2) = (a_1 \vee_1 b_1, a_2 \vee_2 b_2),$$

$$(2) \quad (a_1, a_2) \wedge (b_1, b_2) = (a_1 \wedge_1 b_1, a_2 \wedge_2 b_2).$$

O reticulado $(R, \preceq, \vee, \wedge)$ designa-se por produto dos reticulados $(R_1, \preceq_1, \vee_1, \wedge_1)$ e $(R_2, \preceq_2, \vee_2, \wedge_2)$ e as definições das operações \vee e \wedge implicam que a relação de ordem \preceq seja definida por

$$(a_1, a_2) \preceq (b_1, b_2) \Leftrightarrow a_1 \preceq_1 b_1 \text{ e } a_2 \preceq_2 b_2.$$

Na Figura 7.13 dão-se dois exemplos de produtos de reticulados.

Exemplo 7.16. Considerando o reticulado \mathbb{B} de algarismos binários (com a relação de ordem natural $0 \leq 1$) vamos determinar o reticulado $\mathbb{B}^n = \underbrace{\mathbb{B} \times \cdots \times \mathbb{B}}_n$.

Solução. É claro que $\mathbb{B}^n = \{(a_1, \dots, a_n) : a_i \in \mathbb{B}, \text{ para } i = 1, \dots, n\}$. Por outras palavras, \mathbb{B}^n é o conjunto dos n -uplos com componentes binárias. As operações \vee e \wedge são definidas por

$$(a_1, a_2, \dots, a_n) \vee (b_1, b_2, \dots, b_n) = (a_1 \vee b_1, a_2 \vee b_2, \dots, a_n \vee b_n),$$

$$(a_1, a_2, \dots, a_n) \wedge (b_1, b_2, \dots, b_n) = (a_1 \wedge b_1, a_2 \wedge b_2, \dots, a_n \wedge b_n).$$

Como consequência, $(a_1, a_2, \dots, a_n) \preceq (b_1, b_2, \dots, b_n) \Leftrightarrow \forall_{i \in \{1, \dots, n\}} a_i \leq b_i$. \square

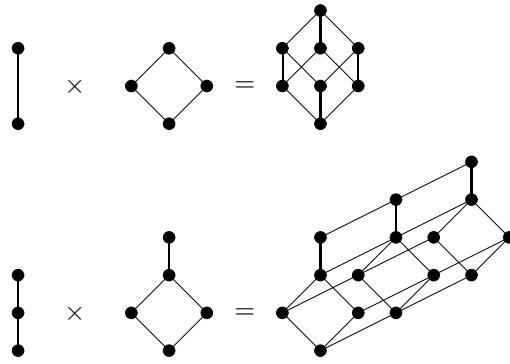


Figura 7.13: Produto de reticulados.

Embora os reticulados sejam também conjuntos parcialmente ordenados e, consequentemente, a Definição 7.5 de conjuntos parcialmente ordenados isomorfos se particularize ao caso dos reticulados, o teorema a seguir sugere outro modo de definir isomorfismos entre reticulados.

Teorema 7.5. *Dois reticulados $\mathcal{R}_1 = (R_1, \preceq_1, \vee_1, \wedge_1)$ e $\mathcal{R}_2 = (R_2, \preceq_2, \vee_2, \wedge_2)$ são isomorfos se e só se existe uma bijecção $\Phi : R_1 \rightarrow R_2$ para a qual, quaisquer que sejam $a, b \in R_1$, se verificam as seguintes propriedades:*

$$(1) \quad \Phi(a \vee_1 b) = \Phi(a) \vee_2 \Phi(b),$$

$$(2) \quad \Phi(a \wedge_1 b) = \Phi(a) \wedge_2 \Phi(b).$$

Demonstração. Seja $\Phi : R_1 \rightarrow R_2$ um isomorfismo entre os reticulados \mathcal{R}_1 e \mathcal{R}_2 , isto é, Φ é uma bijecção e as funções Φ e Φ^{-1} preservam as relações de ordem. Tendo em conta que para $a, b \in R_1$ se verifica $a \preceq_1 a \vee_1 b$ e $b \preceq_1 a \vee_1 b$ e ainda que Φ preserva a relação de ordem, podemos concluir que $\Phi(a) \preceq_2 \Phi(a \vee_1 b)$ e $\Phi(b) \preceq_2 \Phi(a \vee_1 b)$. Como consequência, $\Phi(a) \vee_2 \Phi(b) \preceq_2 \Phi(a \vee_1 b)$. Adicionalmente, se $\Phi(a) \vee_2 \Phi(b) \preceq_2 \mu$, com $\mu \in R_2$, então $\Phi(a) \preceq_2 \mu$ e $\Phi(b) \preceq_2 \mu$. Uma vez que Φ^{-1} preserva a relação de ordem vem que $a \preceq_1 \Phi^{-1}(\mu)$ e $b \preceq_1 \Phi^{-1}(\mu)$. Assim, $a \vee_1 b \preceq_1 \Phi^{-1}(\mu)$ ou, de modo equivalente, $\Phi(a \vee_1 b) \preceq_2 \mu$. Fazendo $\mu = \Phi(a) \vee_2 \Phi(b)$, vem que $\Phi(a \vee_1 b) = \Phi(a) \vee_2 \Phi(b)$. Analogamente se prova que $\Phi(a \wedge_1 b) = \Phi(a) \wedge_2 \Phi(b)$.

Reciprocamente, se $\Phi : R_1 \rightarrow R_2$ é uma bijecção para a qual (1) e (2) se verificam e se $a, b \in R_1$ são tais que $a \preceq_1 b$, então $a = a \wedge_1 b$. Assim, $\Phi(a) = \Phi(a \wedge_1 b) = \Phi(a) \wedge_2 \Phi(b)$, pelo que $\Phi(a) \preceq_2 \Phi(b)$, o que significa que Φ preserva a relação de ordem. De modo análogo se prova que Φ^{-1} preserva a relação de ordem. \square

Se o reticulado $(R, \preceq, \vee, \wedge)$ é finito, então a relação de ordem \preceq e as operações binárias \vee e \wedge ficam completamente determinadas pelo diagrama de Hasse. Mais precisamente, podemos concluir o seguinte teorema.

Teorema 7.6. *Dois reticulados finitos $\mathcal{R}_1 = (R_1, \preceq_1, \vee_1, \wedge_1)$ e $\mathcal{R}_2 = (R_2, \preceq_2, \vee_2, \wedge_2)$ são isomorfos se e só se \mathcal{R}_1 e \mathcal{R}_2 têm o mesmo diagrama de Hasse (a menos da etiquetação dos vértices).*

Demonstração. Para $a, b \in R_1$, se b cobre a (o que, no diagrama de Hasse, significa a existência de uma aresta ascendente de a para b), então $a \prec_1 b$ e não existe $x \in R_1$ tal que $a \prec_1 x \prec_1 b$.

- Vamos supor que os reticulados $\mathcal{R}_1 = (R_1, \preceq_1, \vee_1, \wedge_1)$ e $\mathcal{R}_2 = (R_2, \preceq_2, \vee_2, \wedge_2)$ são isomorfos. Então existe um isomorfismo $\Phi : R_1 \rightarrow R_2$ que preserva a relação de ordem, donde se conclui que $\Phi(a) \prec_2 \Phi(b)$. Suponhamos que existe $w \in R_2$ tal que $\Phi(a) \prec_2 w \prec_2 \Phi(b)$. Uma vez que

Φ^{-1} preserva a relação de ordem, vem que $a \prec_1 \Phi^{-1}(w) \prec_1 b$ e $\Phi^{-1}(w) \in R_1$, o que entra em contradição com a hipótese de b cobrir a . Como consequência, $\Phi(b)$ cobre $\Phi(a)$ e, no diagrama de Hasse, existe uma aresta ascendente de $\Phi(a)$ para $\Phi(b)$. Analogamente se mostra que para $x, y \in R_2$, se y cobre x então $\Phi^{-1}(y)$ cobre $\Phi^{-1}(x)$. Logo \mathcal{R}_1 e \mathcal{R}_2 têm o mesmo diagrama de Hasse.

- Reciprocamente, se \mathcal{R}_1 e \mathcal{R}_2 têm o mesmo diagrama de Hasse, vamos definir uma bijecção $\Phi : R_1 \rightarrow R_2$ tal que, para $a \in R_1$, $\Phi(a)$ é igual ao elemento de R_2 que ocupa a mesma posição no diagrama. Uma vez que as operações binárias \vee e \wedge são determinadas pelo diagrama de Hasse (ver Exemplo 7.13), então Φ preserva estas operações e, pelo Teorema 7.5, é um isomorfismo. \square

Exemplo 7.17. Vamos determinar todos os reticulados com cardinalidade não superior de cinco (a menos de um isomorfismo).

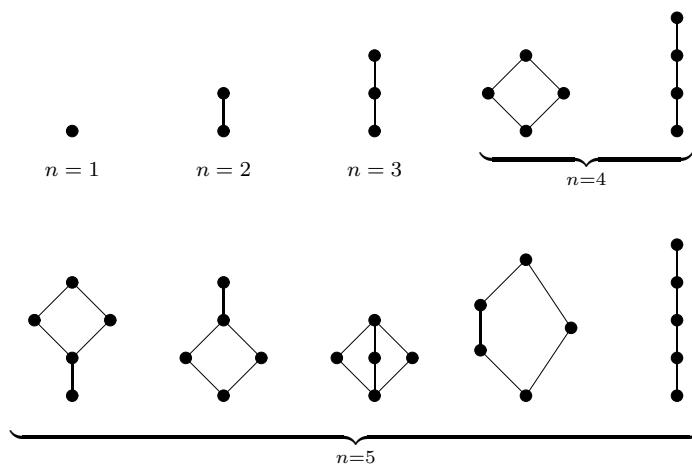


Figura 7.14: Todos os reticulados com n elementos, para $n \leq 5$.

Solução. Ver Figura 7.14. Note-se que os reticulados com um, dois e três elementos são únicos e que existem dois reticulados com quatro elementos e cinco reticulados com cinco elementos. \square

7.3.3 Reticulados distributivos

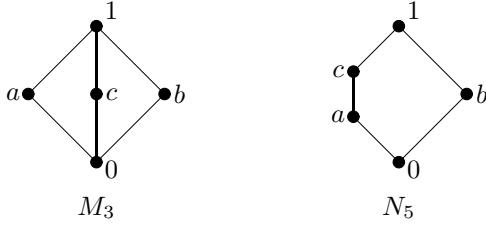
Definição 7.11 (Reticulado distributivo). Um reticulado $(R, \preceq, \vee, \wedge)$ diz-se distributivo se as operações binárias \vee e \wedge são distributivas, isto é, se para $a, b, c \in R$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad \text{e} \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Observe-se que, tendo em conta o princípio da dualidade, as duas condições da Definição 7.11 são equivalentes. Logo, para demonstrar que um reticulado é distributivo basta mostrar apenas uma delas.

Por exemplo, qualquer reticulado $(\mathcal{P}(X), \subseteq, \cup, \cap)$, com $X \neq \emptyset$, é distributivo. Também qualquer um dos reticulados $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ com a relação de ordem usual \leq é distributivo.

Exemplo 7.18. Vamos provar que entre todos os reticulados com cinco elementos (ver Figura 7.14), os que se denotam, respectivamente, por M_3 (e se designa por "diamante") e por N_5 (e se designa por "pentágono"), não são distributivos.

Figura 7.15: Reticulados M_3 "diamante" e N_5 "pentágono".

Solução. Com recurso à notação utilizada na Figura 7.15, podemos tirar as seguintes conclusões:

- Para o diamante: $a \vee (b \wedge c) = a \vee 0 = a$ e $(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$. Logo, uma vez que $1 \neq a$, o diamante é um reticulado não distributivo.
- Para o pentágono temos: $a \vee (b \wedge c) = a \vee 0 = a$ e $(a \vee b) \wedge (a \vee c) = 1 \wedge c = c$. Logo, dado que $a \neq c$, o pentágono é um reticulado não distributivo. \square

Definição 7.12 (Reticulado modular). *Um reticulado $(R, \preceq, \vee, \wedge)$ diz-se modular se*

$$\forall_{a,b,c \in R} a \preceq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$$

(ou, pelo princípio da dualidade, $a \succeq c \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c$).

Deve observar-se que sendo $(R, \preceq, \vee, \wedge)$ um reticulado distributivo então, para $a, b, c \in R$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Adicionalmente, se $a \preceq c$, então $a \vee c = c$ e, como consequência, $a \vee (b \wedge c) = (a \vee b) \wedge c$. Logo, podemos concluir que todo o reticulado distributivo é modular.

Exemplo 7.19. Vamos demonstrar que um dos reticulados com cinco elementos (ver Figura 7.14), mais precisamente N_5 ("pentágono"), não é modular.

Solução. Com recurso à notação utilizada na Figura 7.15 para o pentágono, vem que $a \vee (b \wedge c) = a \vee 0 = a$ e $(a \vee b) \wedge c = 1 \wedge c = c$. Dado que $a \neq c$, podemos concluir que o pentágono não é um reticulado modular. \square

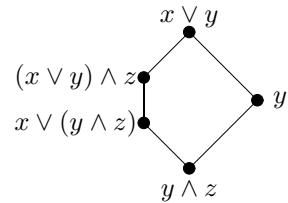
Este último exemplo é um exemplo muito representativo dos reticulados não modulares, conforme decorre do teorema a seguir.

Teorema 7.7. Seja $\mathcal{R} = (R, \preceq, \vee, \wedge)$ um reticulado. Então \mathcal{R} é modular se e só se \mathcal{R} não contém qualquer subreticulado isomorfo a N_5 (ou seja, ao pentágono).

Demonstração. É claro que se N_5 é um subreticulado de \mathcal{R} , então \mathcal{R} não pode ser modular, pelo que basta provar o recíproco, ou seja, que se \mathcal{R} não é modular então contém N_5 como subreticulado.

Suponhamos que \mathcal{R} não é modular. Então por definição existem elementos $x, y, z \in \mathcal{R}$, tais que $x \prec z$, mas $x \vee (y \wedge z) \prec (x \vee y) \wedge z$. Agora vamos provar que o conjunto parcialmente ordenado representado pelo diagrama de Hasse da Figura 7.16 é um subreticulado de \mathcal{R} .

É evidente que $y \wedge z \preceq x \vee (y \wedge z) \prec (x \vee y) \wedge z \preceq x \vee y$, $((x \vee (y \wedge z)) \vee y = (x \vee (y \wedge z)) \vee y = x \vee y$ e $((x \vee y) \wedge z) \wedge y = (x \vee y) \wedge (z \wedge y) = y \wedge z$. Por outro lado, se $y \wedge z = x \vee (y \wedge z)$ então $x \preceq y \wedge z$ e $(x \vee y) \wedge z = x \vee (y \wedge z)$, o que é impossível. Logo, $y \wedge z \neq x \vee (y \wedge z)$ e, consequentemente, \mathcal{R} contém um subreticulado isomorfo a N_5 . \square

Figura 7.16: Diagrama de Hasse de N_5 .

Teorema 7.8. Seja $\mathcal{R} = (R, \preceq, \vee, \wedge)$ um reticulado distributivo. Se $a, b, c \in R$, então

$$c \wedge a = c \wedge b \quad e \quad c \vee a = c \vee b \quad \Rightarrow \quad a = b.$$

Demonstração. Observe-se que $a = a \wedge (c \vee a) = a \wedge (c \vee b) = (a \wedge c) \vee (a \wedge b) = (c \wedge b) \vee (a \wedge b) = (c \vee a) \wedge b = (c \vee b) \wedge b = b$. \square

Definição 7.13 (Reticulado complementado). Seja $(R, \preceq, \vee, \wedge)$ um reticulado. Denotando por 1 o elemento máximo e por 0 o elemento mínimo de R , quanto existem (note-se que os elementos máximo e mínimo existem pelo menos para os reticulados finitos). O reticulado $(R, \preceq, \vee, \wedge)$ com 0 e 1 diz-se complementado se todo o elemento $x \in R$ possui um complemento, isto é,

$$\forall_{x \in R} \exists_{y \in R} x \vee y = y \vee x = 1 \quad e \quad x \wedge y = y \wedge x = 0.$$

O complemento de x (se existe e é único) denota-se por x' .

Exemplo 7.20. Vamos determinar quais dos reticulados $(\mathcal{P}(X), \subseteq, \cup, \cap)$ com $X \neq \emptyset$, $(D_{12}, |)$ (ver Exemplo 7.14) e M_3 "diamante" (ver Exemplo 7.18) são complementados.

Solução. Para o reticulado $(\mathcal{P}(X), \subseteq, \cup, \cap)$, com $X \neq \emptyset$, podemos concluir que $0 = \emptyset$, $1 = X$, e

$$\forall_{A \subseteq X} \exists_{A' = X \setminus A} A \cap A' = \emptyset \quad e \quad A \cup A' = X.$$

Como consequência, $(\mathcal{P}(X), \subseteq, \cup, \cap)$ é um reticulado complementado.

Uma vez que o elemento 6 do reticulado $(D_{12}, |)$ não tem complemento (isto é, não existe $x \in D_{12}$ tal que $\text{mdc}(6, x) = 1$ e $\text{mmc}(6, x) = 12$), o reticulado $(D_{12}, |)$ não é complementado.

O reticulado M_3 diamante é complementado mas o elemento c tem dois complementos: a e b (ver Figura 7.15). \square

Teorema 7.9. Num reticulado distributivo $(R, \preceq, \vee, \wedge)$, com 0 e 1 , qualquer elemento $a \in R$ não tem mais do que um complemento.

Demonstração. Supondo que b_1 e b_2 são complementos de a vem que

$$a \vee b_1 = a \vee b_2 = 1 \quad e \quad a \wedge b_1 = a \wedge b_2 = 0.$$

Como consequência, $b_1 = b_1 \vee 0 = b_1 \vee (a \wedge b_2) = (b_1 \vee a) \wedge (b_1 \vee b_2) = (b_2 \vee a) \wedge (b_2 \vee b_1) = b_2 \vee (a \wedge b_1) = b_2 \vee 0 = b_2$. \square

Definição 7.14 (Reticulado de Boole). Um reticulado distributivo e complementado designa-se por reticulado (álgebra) de Boole.

O Capítulo 10 é dedicado completamente ao estudo das álgebras de Boole. Segue-se a definição de uma outra classe de reticulados.

Definição 7.15 (Reticulado completo). Um reticulado $(R, \preceq, \vee, \wedge)$ diz-se completo, se para todo o subconjunto $M \subseteq R$ existe o supremo $\sup M$ e o ínfimo $\inf M$ (neste caso, denota-se também $\sup M$ por $\bigvee M$ e $\inf M$ por $\bigwedge M$).

Por definição, um reticulado completo tem os elementos 0 e 1 (uma vez que $0 = \bigwedge R$ e $1 = \bigvee R$). Seguem-se alguns exemplos de reticulados completos:

1. Todos os reticulados finitos são completos.
2. Se \mathcal{R}_1 e \mathcal{R}_2 são reticulados completos, então o reticulado $\mathcal{R}_1 \times \mathcal{R}_2$ também é completo.

3. O reticulado $(\mathcal{P}(X), \subseteq, \cup, \cap)$, com $X \neq \emptyset$, é completo. Observe-se que, neste reticulado, para qualquer família de subconjuntos de X , $\{A_i : i \in I\}$, $\sup\{A_i : i \in I\} = \bigcup_{i \in I} A_i$ e $\inf\{A_i : i \in I\} = \bigcap_{i \in I} A_i$.
4. Seja (P, \preceq) um conjunto parcialmente ordenado, considerando $\mathcal{J}(P) \subseteq \mathcal{P}(P)$ o conjunto de todos os subconjuntos inferiores de P (ver Exemplo 7.10). Se $\{A_i : i \in I\} \subseteq \mathcal{J}(P)$, então $\bigcup_{i \in I} A_i \in \mathcal{J}(P)$ e $\bigcap_{i \in I} A_i \in \mathcal{J}(P)$. Como consequência, $(\mathcal{J}(P), \subseteq, \cup, \cap)$ é um reticulado completo.

Alguns exemplos de reticulados que não são completos:

1. Uma vez que não existe $\sup \mathbb{N}$, nenhum dos reticulados \mathbb{N} , \mathbb{Z} , \mathbb{Q} e \mathbb{R} , munidos da ordem usual (\leq), é completo.
2. Se um reticulado não tem 0 ou 1 então não é completo.

Teorema 7.10. *Um reticulado $(R, \preceq, \vee, \wedge)$ é completo se e só se para todo o subconjunto $M \subseteq R$ existe o supremo $\bigvee M$.*

Demonstração. Se R é completo então, por definição, todo o subconjunto $M \subseteq R$ tem supremo e ínfimo e, em particular, existe o supremo $\bigvee M$. Para provar o recíproco, basta provar que para todo o subconjunto $M \subseteq R$ existe o ínfimo $\bigwedge M$. Assim, seja $M \subseteq R$. Uma vez que

$$\bigwedge M = \bigvee \{x \in R : x \text{ é um minorante de } M\},$$

se $M \neq \emptyset$, então $\bigwedge M$ existe, caso contrário $\bigwedge \emptyset = \bigvee R$. □

7.3.4 Representação de reticulados distributivos

Neste secção vamos demonstrar que qualquer reticulado finito e distributivo é isomorfo ao reticulado dos subconjuntos inferiores de um conjunto parcialmente ordenado.

Definição 7.16 (Átomo e elemento irredutível). *Seja $(R, \preceq, \vee, \wedge)$ um reticulado, então*

- (a) *um elemento $a \in R$ diz-se um átomo se a cobre 0, ou seja, $\forall_{y \in R} y \prec a \Rightarrow y = 0$;*
- (b) *um elemento $x \in R \setminus \{0\}$ diz-se \vee -irredutível se*

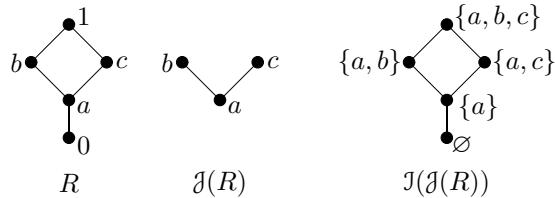
$$\forall_{y,z \in R} (x = y \vee z) \Rightarrow (x = y \text{ ou } x = z).$$

Denota-se por $\mathcal{J}(R)$ o conjunto de todos os elementos \vee -irredutíveis de R .

Na Figura 7.17 apresenta-se o exemplo de um reticulado R e dos correspondentes cpo $\mathcal{J}(R)$ e reticulado $\mathcal{J}(\mathcal{J}(R))$.

Teorema 7.11. *Se $(R, \preceq, \vee, \wedge)$ é um reticulado finito e os elementos $a, b \in R$ são tais que $a \not\preceq b$, então existe um elemento x , \vee -irredutível (ou seja, $x \in \mathcal{J}(R)$) tal que $x \preceq a$ e $x \not\preceq b$.*

Demonstração. Seja $A = \{x \in R : x \preceq a \text{ e } x \not\preceq b\}$. Uma vez que $a \in A$, então $A \neq \emptyset$. Logo, existe um elemento mínimo $y = \inf A$ e basta mostrar que y é \vee -irredutível. Suponha que $y = c \vee d$, com $y \neq c$ e $y \neq d$. Nestas condições, $c \prec y$ e $d \prec y$ e, por definição de A , $y \preceq a$, o que implica $c \prec a$ e $d \prec a$. Uma vez que y é o elemento mínimo de A , c e d não pertencem a A . Assim, $c \preceq b$ e $d \preceq b$ e, como consequência, $y = c \vee d \preceq b$, o que constitui uma contradição. Logo, $y = c$ ou $y = d$, ou seja, $y \in \mathcal{J}(R)$. □

Figura 7.17: Reticulado R e correspondentes $J(R)$ e $I(J(R))$.

Note-se que se R é um reticulado, então $J(R)$ é um conjunto parcialmente ordenado (cuja relação de ordem parcial é a induzida pela relação de ordem parcial de R). Este facto, por sua vez, dá origem ao reticulado distributivo $I(J(R))$.

Teorema 7.12 (da representação de Birkhoff³). *Se $(R, \preceq, \vee, \wedge)$ é um reticulado finito e distributivo, então a função $\Phi : R \rightarrow I(J(R))$ definida por $\Phi(a) = \{x \in J(R) : x \preceq a\}$ é um isomorfismo.*

Demonstração. Inicialmente vamos demonstrar que Φ preserva a relação de ordem parcial. Sejam $a, b \in R$ tais que $a \preceq b$, então $\downarrow a \subseteq \downarrow b$ e, como consequência, $\Phi(a) \subseteq \Phi(b)$. Suponhamos agora que $\Phi(a) \subseteq \Phi(b)$ e $a \not\preceq b$. Pelo Teorema 7.11, existe $x \in J(R)$ tal que $x \preceq a$ e $x \not\preceq b$. Consequentemente, $x \in \Phi(a)$ e $x \notin \Phi(b)$, o que contradiz a hipótese. Logo, $a \preceq b$. Por outro lado, uma vez que para $c \in R$, $c = \sup\{x \in J(R) : x \preceq c\}$, então $\Phi(a) = \Phi(b)$ implica $a = \sup \Phi(a) = \sup \Phi(b) = b$ e, por conseguinte, Φ é uma aplicação injetiva.

Resta provar que Φ é uma aplicação sobrejectiva. Seja $A \in I(J(R)) = \{X \subseteq J(R) : X = \downarrow X\}$. Uma vez que A é um conjunto finito então $A = \{a_1, a_2, \dots, a_n\}$ e, sendo $a = \sup A = a_1 \vee a_2 \vee \dots \vee a_n$, podemos provar que $\Phi(a) = A$.

- Se $x \in A$, então $x = a_i \in J(R)$, para algum $i \in \{1, \dots, n\}$. Logo, $a_i \in \Phi(a)$, ou seja, $\Phi(a) \supseteq A$.
- Se $y \in \Phi(a)$, então $y \preceq a = a_1 \vee a_2 \vee \dots \vee a_n$ e $y \in J(R)$. Como consequência, $y = y \wedge (a_1 \vee a_2 \vee \dots \vee a_n) = (y \wedge a_1) \vee (y \wedge a_2) \vee \dots \vee (y \wedge a_n)$ e, uma vez que y é \vee -irredutível, então existe $i \in \{1, \dots, n\}$ tal que $y = y \wedge a_i \preceq a_i$. Porém, dado que $A \subseteq J(R)$ é um conjunto inferior, $y \in A$ e, consequentemente, $\Phi(a) \subseteq A$. \square

Com base neste teorema podemos concluir que um reticulado finito é distributivo se e só se é isomorfo a um subreticulado de $\mathcal{P}(X)$, onde X é um conjunto finito.

7.3.5 Topologias finitas e reticulados

Neste secção, vamos relacionar os espaços topológicos (finitos) com certas relações de ordem parcial. Dada a sua natureza discreta e as suas múltiplas aplicações, será dada especial atenção aos espaços topológicos digitais.

Definição 7.17 (Topologia). *Seja X um conjunto não vazio. Uma parte τ de $\mathcal{P}(X)$ diz-se uma estrutura topológica (ou topologia) em X se se verificam os seguintes axiomas:*

1. $\emptyset \in \tau$ e $X \in \tau$,
2. a intersecção finita de elementos de τ é um elemento de τ ,
3. a união de uma família arbitrária de elementos de τ é um elemento de τ .

³Garret Birkhoff (1911–1996), matemático americano que foi autor do primeiro livro sobre reticulados.

Os elementos de τ designam-se por *conjuntos abertos* (ou, simplesmente, *abertos*). Um subconjunto de X diz-se um *fechado* se é o complementar de um aberto de X . O par (X, τ) designa-se por *espaço topológico*. Se X é um conjunto finito, então (X, τ) diz-se *espaço topológico finito*.

Exemplo 7.21. Vamos determinar todas as topologias sobre o conjunto $X = \{0, 1\}$.

Solução. Existem quatro topologias sobre X :

$$\begin{aligned}\tau_1 &= \{\emptyset, X\}, \\ \tau_2 &= \{\emptyset, \{0\}, X\}, \\ \tau_3 &= \{\emptyset, \{1\}, X\} \text{ e} \\ \tau_4 &= \{\emptyset, \{0\}, \{1\}, X\}.\end{aligned}$$

Na Figura 7.18 faz-se uma representação pictórica das abertos destas topologias. □

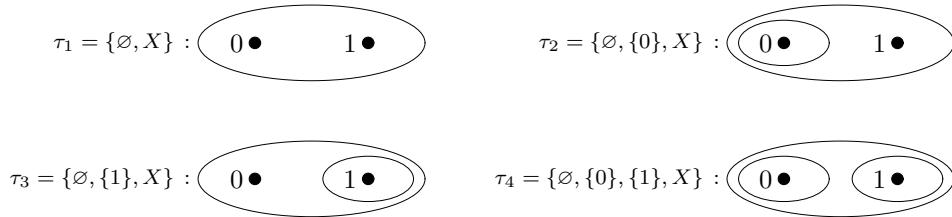


Figura 7.18: Representação pictórica de todas as topologias sobre $X = \{0, 1\}$.

Dado um espaço topológico $\mathcal{X} = (X, \tau)$ e um elemento $x \in X$, designa-se por *vizinhança mínima de x* e denota-se por V_x a intersecção de todos os vizinhâncias abertas de x , ou seja,

$$V_x = \bigcap \{A \in \tau : x \in A\}. \quad (7.2)$$

Se X não é finito, então V_x não é necessariamente aberto.

Definição 7.18 (Interior de um conjunto). *Seja $\mathcal{X} = (X, \tau)$ um espaço topológico e $Y \subseteq X$. Designa-se por *interior de Y* , e denota-se por Y° , a união de todos os abertos contidos em Y , isto é, $\bigcup \{A \in \tau : A \subseteq Y\}$.*

Por outras palavras, Y° é maior aberto contido em Y . É claro que Y° é um conjunto aberto (isto é, $Y^\circ \in \tau$) e $Y^\circ \subseteq Y$. Deve observar-se que $A \subseteq X$ é aberto se e só se $A^\circ = A$.

Definição 7.19 (Fecho de um conjunto). *Seja $\mathcal{X} = (X, \tau)$ um espaço topológico e $Y \subseteq X$. Designa-se por *fecho de Y* , e denota-se por \overline{Y} , a intersecção de todos os fechados que contêm Y , isto é, $\bigcap \{F : X \setminus F \in \tau, Y \subseteq F\}$.*

Por outras palavras, \overline{Y} é menor fechado que contém Y . É claro que \overline{Y} é um conjunto fechado (isto é, $X \setminus \overline{Y} \in \tau$) e que $Y \subseteq \overline{Y}$. Observe-se que um subconjunto $F \subseteq X$ é fechado se e só se $F = \overline{F}$. Em particular, $\{x\}$ denota o fecho de um elemento $x \in X$.

Segue-se a definição dos axiomas de separação (de Alexandroff⁴) T_0 e T_1 . Note-se que existem mais axiomas de separação (como sejam, T_2 , T_3 e T_4). Porém, neste texto, apenas precisaremos dos dois primeiros.

Definição 7.20 (Axiomas de separação (de Alexandroff)). *Dado um espaço topológico $\mathcal{X} = (X, \tau)$. Diz-se que \mathcal{X} é um espaço T_0 (ou que satisfaz o axioma de separação T_0) se para qualquer par de elementos distintos existe um aberto que apenas contém um dos pontos, ou seja,*

⁴Pavel Sergeevich Alexandroff (ou Aleksandrov), 1896–1982, matemático russo que trabalhou em topologia

$$\forall_{x,y \in X} \exists_{A \in \tau} x \in A \wedge y \notin A \vee y \in A \wedge x \notin A.$$

$x \neq y$

Diz-se que X é um espaço T_1 (ou que satisfaz o axioma de separação T_1) se para cada par de elementos distintos x e y de X , existem dois abertos, o primeiro contendo x mas não y e o segundo contendo y mas não x , ou seja, cada ponto pertence a um conjunto aberto que não contém o outro, isto é,

$$\forall_{x,y \in X} \exists_{A,B \in \tau} x \in A \wedge y \notin A \wedge x \notin B \wedge y \in B.$$

$x \neq y$

Os espaços T_0 também se designam por *espaços de Kolmogorov* e os espaços T_1 por *espaços de Fréchet*.

É fácil verificar que X é um espaço T_1 se e só se os seus pontos são fechados, isto é, se e só se $\forall_{x \in X} \overline{\{x\}} = \{x\}$.

Em geral, dado um espaço topológico (X, τ) e dois elementos distintos $x, y \in X$, dizemos que τ separa x e y se $\exists A \in \tau$ tal que $|\{x, y\} \cap A| = 1$.

Exemplo 7.22. Seja $X = \{x, y, z\}$ e considerem-se os espaços topológicos (X, τ_i) , para $i = 1, \dots, 6$, com

$$\begin{aligned} \tau_1 &= \{\emptyset, \{x\}, \{y\}, \{x, y\}, X\}, \\ \tau_2 &= \{\emptyset, \{x\}, X\}, \\ \tau_3 &= \{\emptyset, \{x\}, \{x, y\}, X\}, \\ \tau_4 &= \{\emptyset, \{x\}, \{x, y\}, \{x, z\}, X\}, \\ \tau_5 &= \{\emptyset, \{x, y\}, X\} \text{ e} \\ \tau_6 &= \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, X\} = \mathcal{P}(X). \end{aligned}$$

Vamos determinar quais os que são espaços T_0 e/ou espaços T_1 .

Solução. Uma vez que a topologia τ_2 não separa os pontos y e z e a topologia τ_5 não separa os pontos x e y , podemos concluir que as topologias τ_2 e τ_5 não são espaços T_0 e (uma vez que uma topologia T_1 é também uma topologia T_0) também não são espaços T_1 .

As topologias τ_1 , τ_3 , τ_4 e τ_6 são topologias T_0 .

Na topologia τ_1 , para o par x e z , não existe um aberto que contenha z e não contenha x e, como consequência, τ_1 não é um espaço T_1 . Analogamente, podemos mostrar que apenas a topologia τ_6 é um espaço T_1 . \square

Definição 7.21 (Espaço de Alexandroff). Um espaço topológico $X = (X, \tau)$ diz-se um espaço de Alexandroff se, para cada elemento $x \in X$, existe a mais pequena das suas vizinhanças abertas ou, de modo equivalente, se a intersecção arbitrária de abertos é um aberto e, consequentemente, a união arbitrária de fechados é um fechado.

Exemplo 7.23. Considere o espaço topológico $\mathcal{N} = (\mathbb{N}, \tau)$, onde τ consiste nos intervalos $[n, \infty)$, com $n \in \mathbb{N}$, mais o conjunto vazio (ou seja, $\tau = \{[n, \infty) : n \in \mathbb{N}\} \cup \{\emptyset\}$). Vamos verificar que \mathcal{N} é um espaço T_0 e um espaço de Alexandroff, mas não é um espaço T_1 .

Solução. A intersecção de todos os abertos que contêm n , V_n , é igual ao intervalo $[n, \infty)$, o qual, por definição, é um aberto. Logo, \mathcal{N} é um espaço de Alexandroff.

Note-se que dados dois elementos arbitrários $n, m \in \mathbb{N}$, com $n < m$, então $m \in V_m$ e $n \notin V_m$, logo \mathcal{N} é um espaço topológico T_0 . Por outro lado, todo o aberto que contém n também contém m , donde podemos concluir que \mathcal{N} não é um espaço topológico T_1 . \square

Observe-se que todos os espaços topológicos finitos são espaços de Alexandroff. Como consequência, os espaços topológicos finitos T_1 são muito simples, uma vez que, nestes espaços, cada subconjunto

é simultaneamente aberto e fechado. Por outro lado, os espaços que não são T_0 não separam alguns dos seus pontos. Por este motivo, neste texto, apenas vamos considerar os espaços finitos com uma topologia T_0 que não é T_1 .

A um espaço topológico finito (X, τ) podemos associar duas estruturas de ordenação, a saber, um reticulado e um conjunto parcialmente ordenado. No que se segue, vamos estudar uma relação de ordem parcial entre os elementos de X que, usualmente, se designa por *ordem de especialização* e uma relação de ordem parcial entre os elementos de τ que, usualmente, se designa por *ordem das frames*. A ordem de especialização e a ordem das *frames* desempenham papel de relevo em teoria da computação, particularmente em topologia digital.

Seja (X, τ) um espaço topológico, então a topologia τ , que pode ser parcialmente ordenada pela inclusão, é um reticulado (uma vez que, para $A_1, A_2 \in \tau$, se verifica $A_1 \vee A_2 = A_1 \cup A_2 \in \tau$ e $A_1 \wedge A_2 = A_1 \cap A_2 \in \tau$). Para ilustração, a partir dos espaços topológicos (X, τ_i) do Exemplo 7.22, obtém-se os reticulados representados pelos diagramas de Hasse da Figura 7.19.

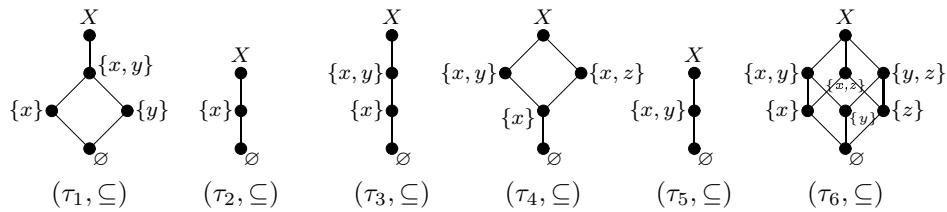


Figura 7.19: Reticulados associados aos espaços (X, τ_i) , para $i = 1, \dots, 6$.

Seja (X, τ) um espaço de Alexandroff. Então, para qualquer família de abertos $\{A_\alpha : A_\alpha \in \tau, \alpha \in I\}$ verifica-se que $\bigcap_{\alpha \in I} A_\alpha \in \tau$. Como consequência, uma vez que, tal como acontece para qualquer espaço topológico, também se verifica que $\bigcup_{\alpha \in I} A_\alpha \in \tau$, podemos concluir que (τ, \subseteq) é um reticulado completo⁵.

Assim, como a relação de inclusão entre os abertos de uma topologia produz um reticulado, uma relação de *pré-ordem*⁶, que é uma relação reflexiva e transitiva (pelo que as relações de ordem parcial são também pré-ordens), entre os pontos do espaço topológico, produz uma relação de ordem parcial directamente relacionada com as propriedades da topologia.

Definição 7.22 (Ordem de especialização). *Seja $\mathcal{X} = (X, \tau)$ um espaço topológico. Denota-se por \leq a relação binária definida em X tal que, para $x, y \in X$,*

$$x \leq y \quad \text{se e só se} \quad x \in \overline{\{y\}}$$

(ou seja, $x \leq y \Leftrightarrow \overline{\{x\}} \subseteq \overline{\{y\}}$). Trata-se de uma relação de pré-ordem em X que, no entanto, é anti-simétrica quando \mathcal{X} é um espaço T_0 . Neste último caso, a relação \leq diz-se uma ordem de especialização (ou ordem de especialização de Alexandroff).

Recorde-se que se X é um espaço de Alexandroff, então cada um dos seus pontos x tem uma vizinhança aberta mínima V_x (ver (7.2)). Como consequência,

$$\forall_{x,y \in X} x \leq y \Leftrightarrow x \in \overline{\{y\}} \Leftrightarrow y \in V_x.$$

⁵ Note-se que, no caso geral, sendo (X, τ) um espaço topológico arbitrário, embora a topologia τ não seja, necessariamente, fechada para a intersecção, definindo

$$\bigvee \{A_\alpha : \alpha \in I\} = \bigcup_{\alpha \in I} A_\alpha \quad \text{e} \quad \bigwedge \{A_\alpha : \alpha \in I\} = \left(\bigcap_{\alpha \in I} A_\alpha \right)^o,$$

onde $\{A_\alpha : \alpha \in I\} \subseteq \tau$, de acordo com o Teorema 7.10, podemos concluir que (τ, \subseteq) constitui um reticulado completo.

⁶ Na terminologia inglesa designa-se por *quasi-order*.

Logo, a ordem de especialização transforma qualquer espaço que seja T_0 e de Alexandroff, X , num conjunto parcialmente ordenado (X, \leq) tal que

$$\overline{\{y\}} = \{x \in X : x \leq y\} = \downarrow y \quad \text{e} \quad V_x = \{y \in X : x \leq y\} = \uparrow x.$$

Para ilustrar estas últimas afirmações, podemos considerar os seguintes espaços topológicos do Exemplo 7.22:

1. No espaço (X, τ_2) , $V_x = \{x\}$, $V_y = \{y\}$ e $V_z = X$.
2. No espaço (X, τ_4) , $V_x = V_y = \{x, y\}$ e $V_z = X$.

Deve observar-se que se o espaço de Alexandroff é T_1 , então cada ponto é fechado e, consequentemente, $x \leq y \Leftrightarrow x = y$. Logo, neste caso, a ordem de especialização que se obtém é trivial. Porém, conforme já se referiu, em matemática discreta, o nosso interesse incide essencialmente sobre espaços topológicos T_0 que não são T_1 . Em tais espaços, a ordem de especialização constitui uma ferramenta muito poderosa para o estudo das respectivas propriedades.

Teorema 7.13. *Seja (X, τ) um espaço T_0 e de Alexandroff e $A \subseteq X$. Então*

$$\begin{aligned} A &= \downarrow A && \text{se e só se } A \text{ é fechado,} \\ A &= \uparrow A && \text{se e só se } A \text{ é aberto.} \end{aligned}$$

Demonstração. Basta mostrar que $\downarrow A = \overline{A}$ e $\uparrow A = A^\circ$. Porém, como as demonstrações das duas igualdades são semelhantes, apenas vamos demonstrar a primeira.

Por definição $\downarrow A = \bigcup_{y \in A} \downarrow y = \bigcup_{y \in A} \overline{\{y\}}$. Logo, tendo em conta que num espaço de Alexandroff a união de fechados é um fechado, podemos concluir que $\downarrow A$ é um fechado. Por outro lado, se $y \in A$ então $\overline{\{y\}} \subseteq \overline{A}$, donde vem que $\bigcup_{y \in A} \overline{\{y\}} \subseteq \overline{A}$. Assim, $A \subseteq \downarrow A \subseteq \overline{A}$ e, uma vez que \overline{A} é o menor fechado que contém A , conclui-se que $\downarrow A = \overline{A}$. \square

Como consequência directa deste teorema, podemos concluir que a topologia de um espaço T_0 e de Alexandroff fica completamente determinada pela sua ordem de especialização.

Teorema 7.14. *Se (X, τ) um espaço topológico T_0 finito, então os conjuntos singulares que são abertos (fechados) para a topologia τ contêm elementos maximais (minimais) para a respectiva ordem de especialização.*

Demonstração. Seja $\{x\}$ um aberto, pelo que $\{x\} = V_x$. Se $x \leq y$, então $y \in V_x$ e, como consequência, $y = x$. Logo, x é um elemento maximal em (X, \leq) . De um modo semelhante, sendo $\{x\}$ um fechado, pelo que $\{x\} = \overline{\{x\}}$, se $z \leq x$, então $z \in \overline{\{x\}} = \{x\}$ e, como consequência, $z = x$. Logo, x é um elemento minimal em (X, \leq) . \square

Exemplo 7.24. *Sendo (X, τ) um espaço topológico, com $X = \{a, b, c\}$ e $\tau = \{\emptyset, \{a\}, \{a, b\}, \{a, c\}, X\}$, vamos determinar a correspondente ordem de especialização.*

Solução. Uma vez que o conjunto $\{a\}$ é aberto, o elemento a é maximal. Por sua vez, o conjunto $\{b\}$ é fechado (dado que $\{a, c\}$ é aberto) e, consequentemente, b é minimal. Analogamente se conclui que c é também um elemento minimal. A Figura 7.20 apresenta o diagrama de Hasse desta ordem de especialização. \square

Exemplo 7.25. *Seja (X, τ_6) o espaço topológico definido no Exemplo 7.22, ou seja, $X = \{x, y, z\}$ e $\tau_6 = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, X\} = \mathcal{P}(X)$. Vamos determinar a respectiva ordem de especialização.*

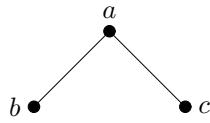


Figura 7.20: Diagrama de Hasse da ordem de especialização do espaço topológico do Exemplo 7.24.

Solução. Observe-se que nesta ordem de especialização, $x \leq y \Leftrightarrow x = y$. Logo, $\overline{\{x\}} = \{x\}$, $\overline{\{y\}} = \{y\}$ e $\overline{\{z\}} = \{z\}$. O diagrama de Hasse desta ordem de especialização é o apresentado na Figura 7.21. \square

$$x \bullet \quad y \bullet \quad z \bullet$$

Figura 7.21: Diagrama de Hasse da ordem de especialização do espaço topológico do Exemplo 7.25.

Definição 7.23 (Base de uma topologia). *Seja (X, τ) um espaço topológico. Uma família $\mathcal{B} \subseteq \tau$ de abertos é uma base para τ quando cada aberto não vazio de τ é a união de elementos de \mathcal{B} .*

Exemplo 7.26. *Seja X um conjunto não vazio e $a \in X$. Considerando as topologias sobre X definidas pelas bases*

1. $\mathcal{B} = \{\{a, x\} : x \in X\}$, ou seja, \mathcal{B} é formado por $\{a\}$ e pelos subconjuntos $\{a, x\}$, com $x \in X \setminus \{a\}$,
2. $\mathcal{B}' = \{\{x\} : x \in X, x \neq a\} \cup \{X\}$, ou seja, \mathcal{B}' é formado por X e pelos subconjuntos $\{x\}$, com $x \in X \setminus \{a\}$,

vamos determinar as respectivas ordens de especialização.

Solução.

1. Note-se que, por definição, o conjunto $\{a\}$ é aberto. Por outro lado, qualquer que seja $x \neq a$, $\bigcup_{y \neq x} \{a, y\} = X \setminus \{x\}$ é aberto e, consequentemente, $\{x\}$ é fechado. Adicionalmente, o fecho de $\{a\}$ é todo o espaço, isto é, $\overline{\{a\}} = X$. A Figura 7.22 (A) apresenta o diagrama de Hasse da ordem de especialização desta topologia.
2. Neste caso, os conjuntos $\{x\}$, para $x \neq a$, são abertos e $\{a\}$ é fechado (uma vez que $X \setminus \{a\}$ é aberto), donde vem que o diagrama de Hasse da correspondente ordem de especialização é o que se apresenta na Figura 7.22 (B).

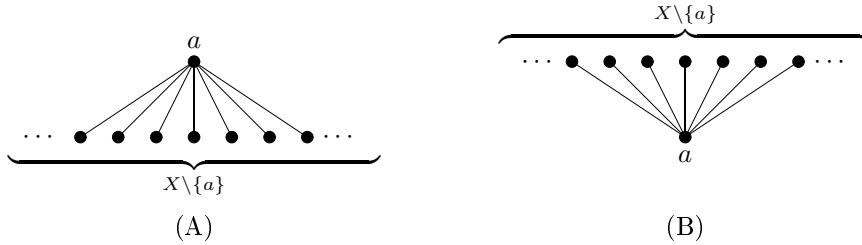


Figura 7.22: Diagramas de Hasse das ordens de especialização dos espaços topológicos do Exemplo 7.26.

Uma aplicação interessante dos espaços topológicos finitos em matemática discreta (e em computação) diz respeito à análise das propriedades topológicas de imagens representadas em computador ou por uma grelha finita de pontos. Neste contexto, os espaços topológicos associados designam-se por *topologias digitais*. Como exemplo de topologia digital, vamos introduzir o conceito de *recta digital*.

Exemplo 7.27. (Recta digital). Considere-se o conjunto \mathbb{Z} dos números inteiros munido da topologia gerada pela base constituída pelos conjuntos da forma $\{2k+1\}$ e $\{2k-1, 2k, 2k+1\}$, com $k \in \mathbb{Z}$. O conjunto \mathbb{Z} , com esta topologia que é T_0 e de Alexandroff, designa-se por recta digital (ou por recta de Khalimsky, ou ainda por espaço de Khalimsky). Vamos determinar a ordem de especialização da recta digital.

Solução. Observe-se que todos os conjuntos singulares com inteiros ímpares são abertos, logo $V_{2k+1} = \{2k+1\}$. Por outro lado, os números pares têm vizinhanças abertas mínimas que são os conjuntos da forma $V_{2k} = \{2k-1, 2k, 2k+1\}$. Na Figura 7.23 faz-se uma representação pictórica de parte destas vizinhanças.

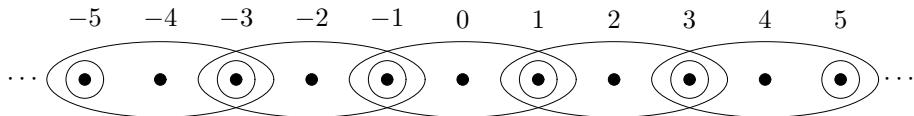


Figura 7.23: Vizinhanças mínimas dos elementos da recta digital.

Uma vez que os conjuntos singulares que incluem números ímpares são abertos, podemos concluir que estes números são elementos maximais da ordem de especialização. Por outro lado, uma vez que para qualquer número par $2k$, a união de todas as vizinhanças mínimas V_x , para $x \neq 2k$, é o aberto

$$\bigcup_{x \neq 2k} V_x = \mathbb{Z} \setminus \{2k\},$$

podemos concluir que $\{2k\}$ é um fechado e, consequentemente, $2k$ é elemento minimal da ordem de especialização. Logo, o diagrama de Hasse da ordem de especialização da recta digital tem o aspecto apresentado na Figura 7.24. \square

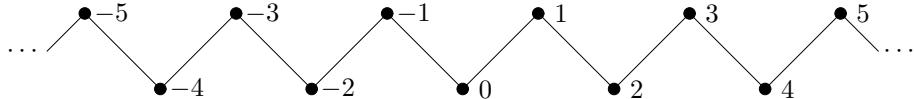


Figura 7.24: Diagrama de Hasse da ordem de especialização de uma recta digital.

Sendo (X, τ) um espaço topológico de Alexandroff, para cada $x \in X$, existe a vizinhança mínima V_x e esta vizinhança é um aberto. Assim, considerando a família de abertos $\mathcal{B} = \{V_x : x \in X\}$, verifica-se que \mathcal{B} é uma base para o espaço (X, τ) . Deve observar-se que $\forall x, y \in X, y \in V_x \Leftrightarrow V_y \subseteq V_x$, ou seja, se y é um elemento da vizinhança mínima de x então qualquer aberto que contenha x contém também y .

Exemplo 7.28. Seja (X, τ) um espaço topológico, com $X = \{a, b, c, d\}$ e

$$\tau = \{\emptyset, \{a\}, \{c\}, \{a, c\}, \{c, d\}, \{a, b, c\}, \{a, c, d\}, X\}.$$

Vamos determinar os conjuntos parcialmente ordenados (X, \leq) , (\mathcal{B}, \subseteq) e (τ, \subseteq) , onde \mathcal{B} é uma base mínima da topologia τ .

Solução. Note-se que, por definição, os conjuntos $\{a\}$ e $\{c\}$ são abertos e, como consequência, os elementos a e c são elementos maximais para a ordem de especialização \leq . Uma vez que os conjuntos $\{a, b, c\}$ e $\{a, c, d\}$ são abertos, os complementos deles, $\{b\}$ e $\{d\}$, são fechados, donde os elementos b

e d são elementos minimais para a ordem de especialização \leq . A Figura 7.25 apresenta o diagrama de Hasse desta ordem de especialização.

A base \mathcal{B} da topologia τ contém os subconjuntos $\{a\}$ e $\{c\}$, não contém o subconjunto $\{a, c\}$ (porque $\{a, c\} = \{a\} \cup \{c\}$), contém $\{c, d\}$ e $\{a, b, c\}$, não contém $\{a, c, d\}$ e X (porque $\{a, c, d\} = \{a\} \cup \{c, d\}$ e $X = \{a, b, c\} \cup \{c, d\}$). Logo, $\mathcal{B} = \{\{a\}, \{c\}, \{c, d\}, \{a, b, c\}\}$ e o diagrama de Hasse do conjunto parcialmente ordenado (\mathcal{B}, \subseteq) é o que se apresenta na Figura 7.25. De modo equivalente, pode definir-se \mathcal{B} como sendo o conjunto das vizinhanças mínimas de elementos de X , ou seja, $\mathcal{B} = \{V_x : x \in X\}$.

Finalmente, o diagrama de Hasse do conjunto parcialmente ordenado (τ, \subseteq) é o apresentado na Figura 7.25. De modo equivalente, pode definir-se \mathcal{B} como sendo o conjunto das vizinhanças mínimas de elementos de X , ou seja, $\mathcal{B} = \{V_x : x \in X\}$. \square

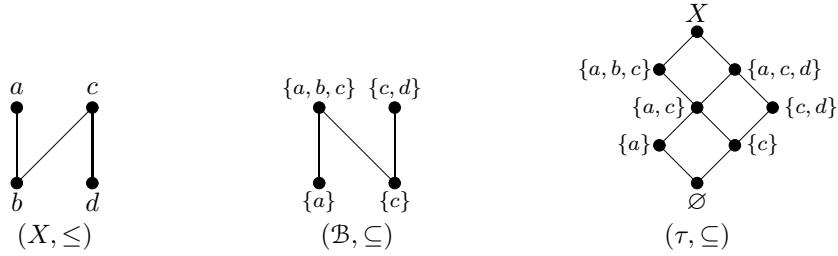


Figura 7.25: Diagramas de Hasse dos conjuntos parcialmente ordenados associados ao espaço topológico do Exemplo 7.28.

Definição 7.24 (Base \vee -irreduzível). *Uma base \mathcal{B} para um espaço topológico T_0 e finito diz-se \vee -irreduzível, ou simplesmente irreduzível, se cada membro B de \mathcal{B} é \vee -irreduzível no reticulado da topologia τ .*

Se (X, τ) é um espaço topológico T_0 e de Alexandoff, então $\mathcal{B} = \{V_x : x \in X\}$ é uma base \vee -irreduzível.

Exemplo 7.29. Vamos determinar uma base irreduzível e as diferentes relações de ordem parcial do espaço topológico (X, τ) , com $X = \{a, b, c, d\}$ e $\tau = \{\emptyset, \{a\}, \{c\}, \{a, b\}, \{a, c\}, \{c, d\}, \{a, b, c\}, \{a, c, d\}, \{a, b, c, d\}\}$.

Solução. A partir da definição da topologia τ , vem que $V_a = \{a\}$, $V_b = \{a, b\}$, $V_c = \{c\}$ e $V_d = \{c, d\}$. Logo, $\mathcal{B} = \{\{a\}, \{a, b\}, \{c\}, \{c, d\}\}$ é uma base \vee -irreduzível para a topologia τ . Na Figura 7.26 apresentam-se os diagramas de Hasse para as respectivas relações de ordem parcial.

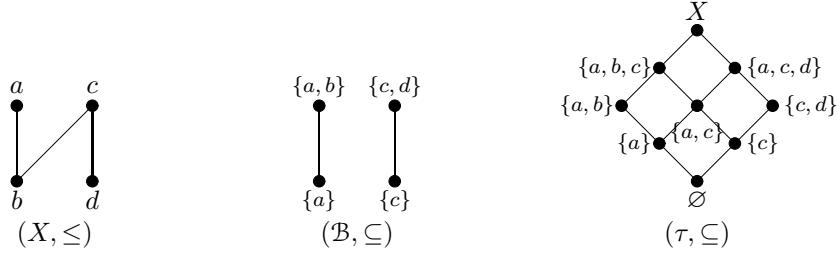


Figura 7.26: Diagramas de Hasse dos conjuntos parcialmente ordenados associados ao espaço topológico do Exemplo 7.29.

Definição 7.25 (Função continua). *Sejam (X, τ) e (X', τ') espaços topológicos e $f : X \rightarrow X'$ uma função. Diz-se que f é continua se e só se para cada subconjunto A aberto (fechado) de X' , $f^{-1}(A)$ é aberto (fechado) em X .*

Exemplo 7.30. Considerem-se os espaços topológicos (X, τ) e (X', τ') , com $X = X' = \{x, y, z\}$, $\tau = \{\emptyset, \{x\}, \{y\}, \{x, y\}, X\}$ e $\tau' = \{\emptyset, \{x\}, \{x, y\}, X'\}$ (ou seja, utilizando notação do Exemplo 7.22, $\tau = \tau_1$ e $\tau' = \tau_3$). Dada a função $f : X \rightarrow X'$, definida por $f(x) = x$, $f(y) = z$ e $f(z) = y$, vamos verificar se f é continua e se preserva a ordem de especialização.

Solução. Uma vez que as imagens recíprocas dos abertos de τ' são, respectivamente, $f^{-1}(\{x\}) = \{x\} \in \tau$, $f^{-1}(\{x, y\}) = \{x, z\} \notin \tau$ e $f^{-1}(X') = X \in \tau$, conclui-se que f não é continua.

No que diz respeito à preservação da ordem de especialização, vamos analisar cada um dos fechos dos conjuntos singulares de (X, τ) e de (X', τ') .

1. Em (X, τ) , $\overline{\{x\}} = \{x, z\}$, $\overline{\{y\}} = \{y, z\}$ e $\overline{\{z\}} = \{z\}$ (ver Figura 7.27), donde podemos concluir que $z \leq x$ e $z \leq y$.
2. Em (X', τ') , $\overline{\{x\}} = X'$, $\overline{\{y\}} = \{y, z\}$ e $\overline{\{z\}} = \{z\}$ (ver Figura 7.27), pelo que $z \leq' x$, $z \leq' y$ e $y \leq' x$.

Assim, uma vez que $z \leq y$, $f(z) = y \not\leq' f(y) = z$, conclui-se que f não preserva as ordem de especialização. \square



Figura 7.27: Diagrama de Hasse das ordens de especialização do Exemplo 7.30.

Teorema 7.15. Sejam (X, τ) e (X', τ') espaços topológicos T₀ e de Alexandroff e $f : X \rightarrow X'$ uma função. Então f é continua se e só se f preserva a ordem de especialização (ou seja, $\forall_{x, y \in X} x \leq y \Rightarrow f(x) \leq' f(y)$).

Demonstração. Assumindo que f preserva ordem de especialização, vamos mostrar que f é continua. Seja $A \subseteq X'$ um aberto arbitrário de (X', τ') . Então, pelo Teorema 7.13, verifica-se a igualdade $A = \uparrow A$ e basta provar a igualdade $f^{-1}(A) = \uparrow f^{-1}(A)$, o que é equivalente a afirmar que $f^{-1}(A)$ é um aberto. Se $x \in f^{-1}(A)$ e $y \in X$ é tal que $x \leq y$, então $f(x) \leq' f(y)$ e, consequentemente, $f(y) \in A$. Logo, $y \in f^{-1}(A)$, donde $f^{-1}(A) = \uparrow f^{-1}(A)$, ou seja, $f^{-1}(A)$ é aberto em (X, τ) .

Reciprocamente, assumindo que f é contínua, vamos mostrar que f preserva ordem de especialização. Sejam $x, y \in X$ tais que $x \leq y$. Uma vez que f é continua, $f^{-1}(\{f(y)\})$ é fechado em (X, τ) e, como consequência, $f^{-1}(\{f(y)\}) = \downarrow f^{-1}(\{f(y)\})$ e $x \in \downarrow f^{-1}(\{f(y)\})$. Logo,

$$x \in f^{-1}(\overline{\{f(y)\}}) \Rightarrow f(x) \in \overline{\{f(y)\}} \Rightarrow f(x) \leq' f(y). \quad \square$$

Sendo (X, τ) um espaço topológico arbitrário, sabe-se que (τ, \subseteq) é um reticulado distributivo. De modo semelhante, por dualidade, pode concluir-se que o conjunto dos fechados relativamente a τ , com a relação de ordem de inclusão, constitui outro reticulado. Reciprocamente, no que se segue, vamos introduzir um procedimento para a obtenção de uma topologia a partir de um reticulado finito e distributivo.

Seja $\mathcal{R} = (R, \preceq)$ um reticulado finito e distributivo e considere-se o conjunto $X = \mathcal{J}(\mathcal{R})$ dos elementos V-irredutíveis de \mathcal{R} , munido da relação de ordem parcial induzida por \preceq . Seja τ a família de todos os subconjuntos superiores de (X, \preceq) , isto é, $\tau = \{A \subseteq X : A = \uparrow A\}$. Logo, $A \subseteq X$, $A \in \tau$ se e só se $A = \bigcup \{\uparrow x : x \in A\}$, o que é equivalente a afirmar que qualquer conjunto $A \in \tau$ admite uma única

representação definida pela união dos conjuntos $\uparrow x = \{y \in X : x \preceq y\}$ (ver Teorema 7.13). Assim, podemos afirmar que τ é uma topologia sobre X gerada pela base minimal $\mathcal{B} = \{V_x = \uparrow x : x \in X\}$ e, consequentemente, que $A \subseteq X$ é um aberto desta topologia se e só se, para cada $x \in A$ e para cada $y \in X$, $x \preceq y$ implica $y \in A$, ou seja, A é aberto se e só se $\bigvee_{x \in A} V_x = \uparrow x \subseteq A$. Como consequência, os conjuntos \vee -irreduíveis de R e τ são dualmente isomorfos. O teorema a seguir estabelece precisamente estas conclusões.

Teorema 7.16. *Todo o reticulado finito e distributivo é isomorfo ao conjunto de subconjuntos fechados do espaço topológico dos seus elementos \vee -irreduíveis munido da relação de inclusão.*

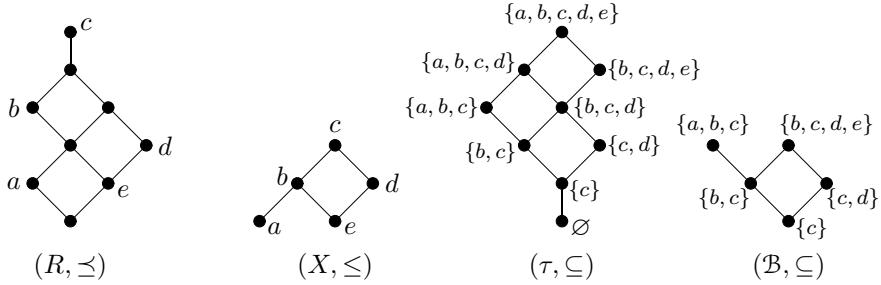


Figura 7.28: Diagramas de Hasse de um reticulado e dos conjuntos parcialmente ordenados que decorrem dele.

Na Figura 7.28 apresenta-se um exemplo de um reticulado (R, \preceq) , a partir do qual se obtém o conjunto parcialmente ordenado (X, \leq) , onde X é o conjunto dos elementos \vee -irreduíveis (ou seja, $X = \mathcal{I}(R)$), o espaço topológico (X, τ) e o correspondente reticulado, e ainda o reticulado determinado pela base minimal \mathcal{B} de τ , tal como anteriormente se referiu.

7.4. Cadeias e anticadeias

Definição 7.26 (Cadeia e anticadeia). *Dado um conjunto parcialmente ordenado $P = (X, \preceq)$, designa-se por cadeia (de X) todo o subconjunto $Y \subseteq X$ no qual todos os elementos são comparáveis. Por sua vez, designa-se por anticadeia (de X) todo o subconjunto $Z \subseteq X$ no qual não existem dois elementos distintos comparáveis.*

Exemplo 7.31. Considerando o conjunto $X = \{1, 2, 3, 4\}$ munido da relação de ordem parcial $|$ (onde $x|y$ significa "x divide y") vamos determinar as cadeias, anticadeias e os subconjuntos que não são cadeias nem anticadeias de conjunto parcialmente ordenado $(X, |)$.

Solução.

1. As cadeias de $(X, |)$ são: $\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 4\}, \{1, 2, 4\}$.
2. As anticadeias de $(X, |)$ são: $\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{2, 3\}, \{3, 4\}$.
3. Os subconjuntos de X que não são cadeias nem anticadeias de $(X, |)$ são: $\{1, 2, 3\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$.

Observe que os subconjuntos $\emptyset, \{1\}, \{2\}, \{3\}$ e $\{4\}$ são simultaneamente cadeias e anticadeias. \square

O resultado que se segue foi publicado por Robert P. Dilworth em 1950.

Teorema 7.17 (Lema de Dilworth). *Em qualquer conjunto parcialmente ordenado $P = (X, \preceq)$ de $mn + 1$ elementos, existe uma cadeia de cardinalidade $m + 1$ ou uma anticadeia de cardinalidade $n + 1$.*

Demonstração. Suponha-se que em P não existe qualquer cadeia de cardinalidade $m + 1$. Então, podemos definir a função $f : X \rightarrow \{1, \dots, m\}$, com $f(x)$ igual à cardinalidade da cadeia de máxima cardinalidade, de entre as cadeias para as quais x é um elemento maximal, ou seja,

$$f(x) = \max\{|Y| : Y \text{ é uma cadeia de } P \text{ e } x \text{ é elemento maximal de } Y\}.$$

Observe-se que $\exists_{j \in [m]} |f^{-1}(j)| \geq \frac{|X|}{m}$. Caso contrário, vem que

$$|X| = \left| \bigcup_{j=1}^m f^{-1}(j) \right| \leq \sum_{j=1}^m |f^{-1}(j)| < m \frac{|X|}{m} = |X|$$

o que constitui uma contradição. Logo, uma vez que a existência de $j \in [m]$ tal que $|f^{-1}(j)| \geq \frac{|X|}{m} = \frac{mn+1}{m} = n + \frac{1}{m}$ implica $|f^{-1}(j)| \geq n + 1$ (ou seja, existem $n + 1$ elementos de X com a mesma imagem por f), pela definição de f , estes elementos não são comparáveis, isto é, formam uma anticadeia de cardinalidade $n + 1$. \square

Uma das consequências imediatas do lema de Dilworth sobre subsequências monótonas de um conjunto totalmente ordenado é o resultado que se segue, atribuído aos matemáticos húngaros Paul Erdős (1913–1996) e George Szekeres (1911–2005).

Corolário 7.18 (Teorema de Erdős-Szekeres). *Sejam $m, n \in \mathbb{N}$ e $S = (\alpha_1, \dots, \alpha_{mn+1})$ uma sequência de $mn + 1$ elementos de um conjunto Z munido de uma relação de ordem total \preceq . Então S contém uma subsequência não decrescente de $m + 1$ termos ou uma subsequência não crescente de $n + 1$ termos (ou ambas).*

Demonstração. Com efeito, considerando-se o conjunto X dos termos da sequência S (que, por sua vez, são elementos do conjunto totalmente ordenado $L = (Z, \preceq)$) de tal forma que, em X , dois quaisquer termos de S são distinguidos pelos seus índices e definindo-se em X a relação de ordem parcial \preceq_S tal que $x_i \preceq_S x_j$ se $x_i \preceq x_j$ e $i \leq j$ (da qual decorre que toda a cadeia em S é uma subsequência não decrescente e toda a anticadeia é uma subsequência não crescente), obtém-se o resultado pretendido. \square

Exemplo 7.32. Considere-se a sequência $S = (3, -2, 4, 6, 10, 1, 2, -4, 0, 3, 2, 0, 8)$ de inteiros com a relação de ordem usual \leq . Vamos demonstrar que existe uma subsequência monótona cujo número de termos não é inferior de 4.

Solução. Uma vez que $|S| = mn + 1 = 13$, podemos escolher $m = 4$ e $n = 3$. Por teorema de Erdős-Szekeres, existe uma subsequência não decrescente de 5 termos ou uma subsequência não crescente de 4 e como consequência uma subsequência monótona de 4 termos. Com efeito, com facilidade se constata a existência da subsequência não decrescente de 5 termos $(-2, 1, 2, 3, 8)$. \square

Tal como no teorema de Erdős-Szekeres, também no lema de Dilworth, $mn + 1$ é a cardinalidade mínima de X para se garantir a existência de uma cadeia de cardinalidade $m + 1$ ou uma anticadeia de cardinalidade $n + 1$. Com efeito, relativamente ao teorema de Erdős-Szekeres, deve observar-se que se $|S| = mn$, então é possível determinar uma sequência de mn termos, relativamente à qual não existe qualquer subsequência de $m + 1$ termos não decrescentes, nem qualquer subsequência de $n + 1$ termos não crescentes. Para tal basta considerar $m = n$ e a sequência obtida concatenando n sequências de m termos crescentes, do seguinte modo: para cada $j \in [n]$, seja $S_j = (\alpha_{1j}, \dots, \alpha_{mj})$ tal que $\forall i \in \{1, \dots, m - 1\} \quad \alpha_{ij} < \alpha_{(i+1)j}$ e tal que $\alpha_{pj_1} > \alpha_{qj_2}$ se $j_1 < j_2$. Nestas condições, na sequência

$$S = (\alpha_{11}, \dots, \alpha_{m1}, \alpha_{12}, \dots, \alpha_{m2}, \dots, \alpha_{1n}, \dots, \alpha_{mn}),$$

não existe qualquer subsequência de $m + 1$ termos não decrescentes, nem qualquer subsequência de $n + 1$ termos não crescentes.

Definição 7.27 (Comprimento e largura de um cpo). *Dado o conjunto parcialmente ordenado $P = (X, \preceq)$, denotando por Cadeias(P) e Anticadeias(P) os conjuntos de subconjuntos de X que determinam, respectivamente, cadeias e anticadeias, os números*

$$p = \max\{|Y| : Y \in \text{Cadeias}(X)\} - 1 \quad (7.3)$$

e

$$q = \max\{|Z| : Z \in \text{Anticadeias}(X)\} \quad (7.4)$$

designam-se, respectivamente, por comprimento e largura de P .

Como consequência, quando todos os elementos do conjunto parcialmente ordenado $P = (X, \preceq)$ são comparáveis P tem comprimento $|X| - 1$ e largura 1 e quando todos são incomparáveis o comprimento é 0 e a largura $|X|$. A título de exemplo, sendo X o conjunto de participantes num determinado congresso onde a cada congressista é atribuído um número de identificação e definindo-se em X a relação \mathcal{R} tal que $(x, y) \in \mathcal{R}$ se e só se x e y têm a mesma nacionalidade e o número de identificação de x é inferior ao número de identificação de y , pode concluir-se que o comprimento de \mathcal{R} é igual ao número de participantes da nacionalidade que é maioritária no congresso menos uma unidade e a respectiva largura é igual ao número das diferentes nacionalidades representadas (por pelo menos um participante). Embora este exemplo ilustre os conceitos de comprimento e largura de uma relação de ordem parcial, deve observar-se, porém, que a respectiva determinação nem sempre é tão imediata. Conhecido, no entanto, um destes valores (o comprimento ou a largura), o corolário do lema de Dilworth, que a seguir se apresenta, permite a obtenção de um menorante para o valor que se desconhece.

Corolário 7.19. *Se $P = (X, \preceq)$ é um conjunto parcialmente ordenado com comprimento p e largura q , então $|X| \leq (p + 1)q$.*

Demonstração. Suponha-se que, apesar das hipóteses se verificarem, $|X| > (p + 1)q \Leftrightarrow |X| \geq (p + 1)q + 1$. Então, por aplicação do lema de Dilworth, ou existe uma cadeia de cardinalidade $p + 2$ ou uma anticadeia de cardinalidade $q + 1$, o que contraria os valores adoptados na hipótese para o comprimento e largura. \square

Deve observar-se que se C é uma cadeia e A uma anticadeia, de um dado conjunto parcialmente ordenado, então $|C \cap A| \leq 1$, uma vez que nesta intersecção não podem existir dois elementos que são comparáveis e não comparáveis.

Teorema 7.20. *Seja $P = (X, \preceq)$ um conjunto parcialmente ordenado com comprimento p e largura q . Então X não pode ser partido em menos de q cadeias nem em menos de $p + 1$ anticadeias.*

Demonstração. Tendo em conta que dois elementos de uma mesma cadeia têm, necessariamente, que pertencer a diferentes anticadeias da partição a considerar, conclui-se que cada elemento de uma cadeia de $p + 1$ elementos (cuja existência está garantida pelo facto de P ter comprimento p) pertence a uma anticadeia distinta de qualquer conjunto de anticadeias que forme uma partição de X . Logo, qualquer partição de X em anticadeias tem, pelo menos, $p + 1$ subconjuntos.

Analogamente se prova a minimalidade de q relativamente ao número de cadeias em que se pode partir X . \square

Relativamente à partição de um conjunto parcialmente ordenado em cadeias e anticadeias é possível obter resultados ainda mais fortes do que o anterior, como é o caso (relativamente à partição em cadeias) do teorema a seguir (conhecido por *teorema de Dilworth*⁷) que é de grande relevância para a teoria dos conjuntos parcialmente ordenados.

⁷ De acordo com [22], Gallai e Milgram concluíram o resultado em causa alguns anos antes de Dilworth o ter publicado (em 1950). Porém, a vontade de Gallai de o ver traduzido em inglês e a indiferença de Milgram em relação a essa particularidade, provocaram o adiamento da sua divulgação.

Teorema 7.21 (de Dilworth). *Se o conjunto parcialmente ordenado $P = (X, \preceq)$ tem largura q então X pode partir-se em q cadeias.*

Demonstração. Vamos fazer a prova por indução sobre a cardinalidade de X , tendo em conta que para $X = \emptyset$ ($|X| = 0$) o resultado é (trivialmente) verdadeiro. Assim, suponha $|X| > 0$ e que o resultado é verdadeiro para qualquer conjunto parcialmente ordenado com menos do que $|X|$ elementos.

Considere-se uma cadeia, C , de máxima cardinalidade em X (pelo que (X, \preceq) tem comprimento $|C| - 1$).

- Se $X \setminus C$ não tem qualquer anticadeia de q elementos, então cada anticadeia de cardinalidade q em X têm exactamente um elemento comum com C . Logo em $X \setminus C$ existem anticadeias de cardinalidade $q - 1$, e, por hipótese de indução, existem $q - 1$ cadeias que partem $X \setminus C$, as quais, conjuntamente com C , formam q cadeias que partem X .
- Suponha-se que em $X \setminus C$ existe uma anticadeia $A = \{\alpha_1, \dots, \alpha_q\}$ e considerem-se o conjunto inferior $\downarrow A$ e o conjunto superior $\uparrow A$ (os quais, por sua vez, são subconjuntos de X). É claro que $X = \downarrow A \cup \uparrow A$, caso contrário existiria $y \in X$ não comparável com qualquer dos elementos de A e, consequentemente, ter-se-ia $|A \cup \{y\}| = q + 1$, contrariando a hipótese.

Tendo em conta que ambos os subconjuntos de X , $\downarrow A$ e $\uparrow A$, contêm A e qualquer deles tem cardinalidade inferior⁸ a X , por hipótese de indução, podemos concluir que o subconjunto $\downarrow A$ se parte nas q cadeias $\downarrow C_1, \dots, \downarrow C_q$ e que o subconjunto $\uparrow A$ se parte nas q cadeias $\uparrow C_1, \dots, \uparrow C_q$. Tendo em conta ainda que cada α_i pertence a uma única cadeia da partição $\downarrow C_1, \dots, \downarrow C_q$ e a uma única cadeia da partição $\uparrow C_1, \dots, \uparrow C_q$ vamos denotar por $\downarrow C_j$ e por $\uparrow C_j$ as cadeias que contêm α_j (pelo que $\alpha_j \in \downarrow C_j \cap \uparrow C_j$).

A prova completa-se mostrando que (a) para cada $i \in [q]$, α_i é um elemento maximal para $\downarrow C_i$ e um elemento minimal para $\uparrow C_i$, que (b) $C_i = \downarrow C_i \cup \uparrow C_i$, é uma cadeia, para $i = 1, \dots, q$ e ainda que (c) C_i para $i = 1, \dots, q$, constitui uma partição de X .

- Suponha-se que α_i não é elemento maximal para $\downarrow C_i$. Então $\exists x \in \downarrow C_i$ tal que $(\alpha_i, x) \in \preceq$. Por outro lado, uma vez que $x \in \downarrow A$, $\exists \alpha_j \in A$ tal que $(x, \alpha_j) \in \preceq$. Logo, pela transitividade de \preceq , $(\alpha_i, \alpha_j) \in \preceq$, o que é absurdo, tendo em conta que $\alpha_i, \alpha_j \in A$. A prova de que α_i é um elemento minimal para $\uparrow C_i$ é análoga.
- Dado que $\forall i \in [q]$, de acordo com (a), α_i é um elemento maximal da cadeia $\downarrow C_i$ e um elemento minimal da cadeia $\uparrow C_i$, vem que $\forall_{x \in \downarrow C_i} (x, \alpha_i) \in \preceq$ e $\forall_{y \in \uparrow C_i} (\alpha_i, y) \in \preceq$. Consequentemente, todos os elementos em $C_i = \downarrow C_i \cup \uparrow C_i$ são comparáveis, pelo que C_i é uma cadeia.
- Tendo em conta que os subconjuntos $\downarrow C_1, \dots, \downarrow C_q$ partem $\downarrow A$ e os subconjuntos $\uparrow C_1, \dots, \uparrow C_q$ partem $\uparrow A$, que $X = \downarrow A \cup \uparrow A$, que os elementos de A são os únicos elementos que pertencem⁹ a $\downarrow A \cap \uparrow A$ e ainda que cada α_i pertence a um único C_i , concluímos que os subconjuntos de X , C_1, \dots, C_q constituem uma partição de X em q cadeias. \square

O resultado dual do Teorema 7.21 foi publicado por L. Mirsky em 1971.

Teorema 7.22 (de Mirsky). *Se no conjunto parcialmente ordenado $P = (X, \preceq)$ a cadeia de maior cardinalidade tem p elementos, então X pode partir-se em p anticadeias.*

⁸Caso contrário, pelo facto de A ser uma anticadeia de máxima cardinalidade, ou A é o conjunto dos elementos minimais (e, nesse caso, $\uparrow A = X$) ou A é o conjunto dos elementos maximais (e, nesse caso $\downarrow A = X$). Em qualquer dos casos, porém, um dos extremos de C (o elemento maximal ou o elemento minimal) tem de pertencer a A , o que não se verifica (uma vez que $A \subseteq X \setminus C$).

⁹Caso contrário, existiria $x \in A$ tal que $(\alpha_i, x) \in \preceq$, para algum $\alpha_i \in A$ e $(x, \alpha_j) \in \preceq$, para algum $\alpha_j \in A$, donde, pela transitividade de \preceq , se concluiria que $(\alpha_i, \alpha_j) \in \preceq$.

Demonstração. Considere-se a aplicação $f : X \mapsto \{1, \dots, |X|\}$, onde $f(x)$ é igual à cardinalidade de uma cadeia de máxima cardinalidade que admite x como elemento maximal. Seja $A_i = \{x \in X : f(x) = i\}$, então (tendo em conta a hipótese) $A_i = \emptyset$ para $i > p$. Adicionalmente, dado existir em X uma cadeia, C , de p elementos, ou seja, um subconjunto $\{x_1, \dots, x_p\} \subseteq X$, cujos elementos são tais que $x_1 \prec_P \dots \prec_P x_p$, pode concluir-se o seguinte:

- por um lado que $A_i \neq \emptyset$, $\forall i \leq p$, uma vez que, para cada $i \in \{1, 2, \dots, p\}$, $x_i \in C \cap A_i$ (no caso contrário, $f(x_i) < i$ entra em contradição com o facto de x_i ser o elemento maximal dos primeiros i elementos da cadeia C e $f(x_i) > i$ entra em contradição com o facto de $|C| = p$);
- por outro lado que $X = A_1 \cup A_2 \cup \dots \cup A_p$, uma vez que $\forall x \in X$, x é o elemento maximal de algum subconjunto de X e, consequentemente, o elemento maximal de alguma das cadeias a que pertence.

Sendo claro que $\bigvee_{i \neq j} A_i \cap A_j = \emptyset$ (caso contrário, existiria $x \in A_i \cap A_j$, com $i < j$, tal que $f(x) = i$ e $f(x) = j$), resta provar que $\forall i \in \{1, \dots, p\}$ o conjunto A_i é uma anticadeia. Com efeito, se existirem dois elementos distintos de A_i comparáveis, por exemplo $x, y \in A_i$ com $x \prec_P y$, então $f(x) = i \Rightarrow f(y) \geq i + 1$, o que contradiz o facto de y ser um elemento de A_i . \square

Definição 7.28 (Restrição, subrelação e extensão linear). *Dada uma relação de ordem parcial, \mathcal{R} , definida em X , se $Y \subset X$ então $\mathcal{R}_Y = \mathcal{R} \cap (Y \times Y)$ designa-se por restrição de \mathcal{R} a Y . Sendo $P_1 = (X, \preceq_{P_1})$ e $P_2 = (X, \preceq_{P_2})$ dois conjuntos parcialmente ordenados tais que $\preceq_{P_1} \subset \preceq_{P_2}$, diz-se que \preceq_{P_2} é uma extensão de \preceq_{P_1} e que \preceq_{P_1} é uma subrelação de \preceq_{P_2} . Se \preceq_{P_2} é uma ordem linear em X , então P_2 diz-se uma extensão linear de P_1 .*

O teorema de Szpilrajn (de 1930) estabelece que todo o conjunto parcialmente ordenado admite uma extensão linear. O teorema que se segue é uma versão mais fraca onde se consideram apenas conjuntos finitos. A demonstração da versão geral, baseia-se no lema de Zorn (que não foi considerado neste texto) e pode ser consultada, por exemplo, em [37].

Teorema 7.23 (Szpilrajn). *Todo o conjunto parcialmente ordenado finito tem uma extensão linear.*

Demonstração. Denotando por P_0 o conjunto parcialmente ordenado finito $P = (X, \preceq_P)$ e por $P_{i+1} = (X_{i+1}, \preceq_{P_{i+1}})$ o conjunto parcialmente ordenado obtido de $P_i = (X_i, \preceq_{P_i})$ fazendo $X_{i+1} = X_i \setminus \{x_i\}$, onde x_i é um elemento minimal para P_i , obtém-se a extensão linear $L(P) = (X, \preceq_{L(P)})$ tal que $x_i \preceq_{L(P)} x_j$, para $1 \leq i \leq j \leq |X|$. \square

A partir de agora apenas vamos considerar conjuntos parcialmente ordenados finitos, os quais designaremos, simplesmente, por conjuntos parcialmente ordenados. O teorema a seguir sugere uma metodologia distinta da anterior para a obtenção de extensões lineares de conjuntos parcialmente ordenados.

Teorema 7.24. *Dado um conjunto parcialmente ordenado (X, \mathcal{R}) se $\alpha, \beta \in X$ são não comparáveis relativamente a \mathcal{R} , então a relação \mathcal{R}' tal que $\alpha \mathcal{R}' \beta$ e*

$$\mathcal{R}' = \mathcal{R} \cup (\downarrow \alpha \times \uparrow \beta),$$

é também uma relação de ordem parcial.

Demonstração. Antes de se iniciar a prova, convém notar que $\downarrow \alpha \cap \uparrow \beta = \emptyset$ (dado que se existe x nesta intersecção, então $(\beta, x), (x, \alpha) \in \mathcal{R}$ e, pela transitividade de \mathcal{R} , $(\beta, \alpha) \in \mathcal{R}$, o que contradiz a hipótese).

- Uma vez que \mathcal{R} é reflexiva, é claro que \mathcal{R}' também é reflexiva.

- Suponha-se que $(x, y), (y, x) \in \mathcal{R}'$. Se ambos os pares pertencem a \mathcal{R} então, pela anti-simetria de \mathcal{R} , $x = y$. Tendo em conta que $\downarrow\alpha \cap \uparrow\beta = \emptyset$, sabe-se que não existem $(x, y), (y, x) \in \downarrow\alpha \times \uparrow\beta$, pelo que resta o caso em que (sem perda de generalidade) $(x, y) \in \mathcal{R}$ e $(y, x) \in \downarrow\alpha \times \uparrow\beta$. Então $(\beta, x), (x, y), (y, \alpha) \in \mathcal{R}$ o que, pela transitividade de \mathcal{R} , contraria novamente a \mathcal{R} -incomparabilidade de α e β .
- A demonstração da transitividade é idêntica à anterior. Se $(x, y), (y, z) \in \mathcal{R}$ então $(x, z) \in \mathcal{R}$. Uma vez que não existem $(x, y), (y, z) \in \downarrow\alpha \times \uparrow\beta$, resta considerar o caso em que $(x, y) \in \mathcal{R}$ e $(y, z) \in \downarrow\alpha \times \uparrow\beta$, o qual implica que $x \in \downarrow\alpha$ e, consequentemente, que $(x, z) \in \mathcal{R}'$. \square

Com este resultado, uma vez que $\mathcal{R} \subset \mathcal{R}'$ e \mathcal{R}' é, ainda, uma relação de ordem parcial, escolhendo, sucessivamente, pares de pontos não comparáveis, até que não exista nenhum em tais condições, obtém-se uma relação de ordem total, ou seja, uma extensão linear de \mathcal{R} .

Os diagramas de Hasse das extensões lineares do conjunto parcialmente ordenado P , da Figura 7.1, estão representados na Figura 7.29.

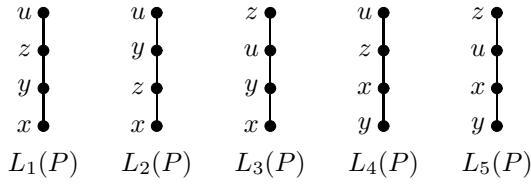


Figura 7.29: Extensões lineares do conjunto parcialmente ordenado da Figura 7.1.

7.5. Relações de ordem fraca, intervalar e semi-transitivas

Definição 7.29 (Relações de ordem fraca, intervalar, semi-transitiva e quase-ordem). *Dado um conjunto parcialmente ordenado, $P = (X, \preceq_P)$, a relação de ordem parcial \preceq_P designa-se por*

- *ordem fraca quando*

$$x \prec_P y \Rightarrow \forall_{z \in X} x \preceq_P z \vee z \preceq_P y$$

(de um modo equivalente pode afirmar-se que \preceq_P é uma ordem fraca se existe uma função $f : X \rightarrow \mathbb{R}$ tal que $x \prec_P y$ se e só se $f(x) < f(y)$);

- *ordem intervalar quando*

$$x \prec_P y \wedge z \prec_P u \Rightarrow x \prec_P u \vee z \prec_P y;$$

- *ordem semi-transitiva quando*

$$x \prec_P y \wedge y \prec_P z \Rightarrow \forall_{u \in X} u \preceq_P z \vee x \preceq_P u;$$

- *quase-ordem ("semiorder" na terminologia inglesa) quando é intervalar e semi-transitiva.*

É fácil concluir que uma ordem fraca é também intervalar e semi-transitiva e, consequentemente, uma quase-ordem. Na Figura 7.30 representam-se os diagramas de Hasse dos conjuntos parcialmente ordenados usualmente denotados por $1 \oplus 2$, $2 \oplus 2$ e $1 \oplus 3$.

Em alternativa às definições anteriores pode concluir-se que uma relação de ordem parcial é uma ordem fraca se e só se nenhuma das suas restrições é isomorfa a um conjunto parcialmente ordenado

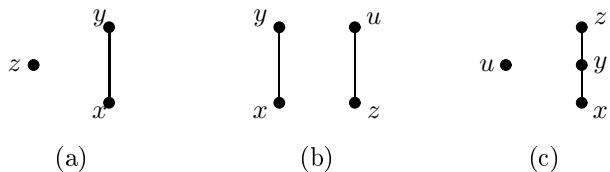


Figura 7.30: Diagramas de Hasse de $1 \oplus 2$, $2 \oplus 2$ e $1 \oplus 3$.

com o diagrama de Hasse da Figura 7.30-(a) (i.e., $1 \oplus 2$). Uma relação de ordem parcial é uma ordem intervalar se e só se nenhuma das suas restrições é isomorfa a um conjunto parcialmente ordenado com o diagrama de Hasse da Figura 7.30-(b) (isto é, $2 \oplus 2$). Uma relação de ordem parcial é semi-transitiva se e só se nenhuma das suas restrições é isomorfa a um conjunto parcialmente ordenado com o diagrama de Hasse da Figura 7.30-(c) (isto é, $1 \oplus 3$). Finalmente, uma relação de ordem parcial é uma quase-ordem (*semiorder* na terminologia inglesa) se e só se nenhuma das suas restrições é isomorfa nem ao conjunto parcialmente ordenado com o diagrama de Hasse da Figura 7.30-(b) nem ao conjunto parcialmente ordenado com o diagrama de Hasse da Figura 7.30-(c).

Na Figura 7.31 representam-se todas as extensões fracas do conjunto parcialmente ordenado representado na Figura 7.1.

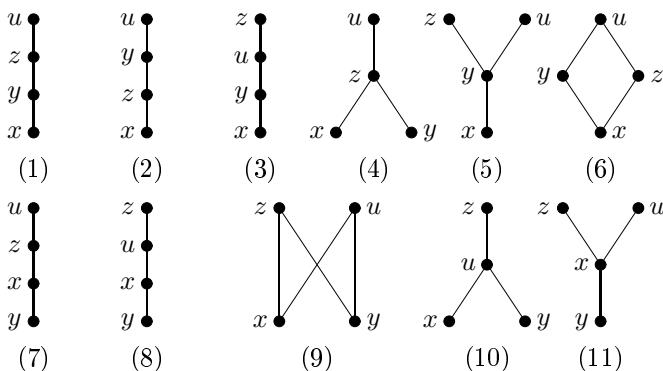


Figura 7.31: Extensões fracas do conjunto parcialmente ordenado da Figura 7.1.

Uma vez que toda a ordem linear é também uma ordem fraca, toda a extensão linear é também uma extensão fraca e, consequentemente, as extensões lineares estão contidas no conjunto das extensões fracas. Na Figura 7.31, os diagramas de Hasse assinalados por (1), (2), (3), (7) e (8) referem-se às extensões lineares do conjunto parcialmente ordenado da Figura 7.1.

Seja AM_P o conjunto de todas as anticadeias maximais do conjunto parcialmente ordenado $P = (X, \preceq_P)$ e seja $AM(P) = (AM_P, \preceq_{AM(P)})$ tal que

$$\forall_{A_i, A_j \in AM_P} A_i \prec_{AM(P)} A_j \Leftrightarrow \forall_{x \in A_i} \exists_{y \in A_j} x \prec_P y.$$

Então é fácil concluir que $AM(P)$ é uma ordem parcial (sabendo-se até que é um reticulado). Como exemplo, considerando o conjunto parcialmente ordenado, P , representado na Figura 7.1, conclui-se que $AM_P = \{\{u, z\}, \{x, y\}, \{y, z\}\}$ e que $\{x, y\}$ e $\{u, z\}$ são os únicos elementos comparáveis em $AM(P)$.

Teorema 7.25. Uma ordem parcial em $P = (X, \preceq_P)$ é uma ordem fraca se e só se

$$\forall_{A,B \in AM_P} A \neq B \Rightarrow A \cap B = \emptyset.$$

Demonstração. Assumindo-se que \preceq_P é uma ordem fraca em X , sejam A_i e A_j duas anticadeias maximais distintas em P e suponha-se que $\exists z \in A_i \cap A_j$. Uma vez que A_i e A_j são distintas e maximais então $\exists x \in A_i \setminus A_j$ e $\exists y \in A_j \setminus A_i$ tais que x e y são comparáveis. Contudo z não é comparável nem com x nem com y e, consequentemente, existe uma restrição de P isomorfa a $1 \oplus 2$, o que é uma contradição.

Reciprocamente, suponha que \preceq_P não é uma ordem fraca em X , isto é, $\exists x, y, z \in X$ tais que x é comparável com y mas z não é comparável nem com x nem com y . Se A_{xz} e A_{yz} são as anticadeias maximais que incluem $\{x, z\}$ e $\{y, z\}$, respectivamente, então $A_{xz} \neq A_{yz}$ e $A_{xz} \cap A_{yz} \neq \emptyset$. \square

Com base neste resultado, é imediato concluir que no conjunto parcialmente ordenado representado na Figura 7.1 não está definida uma relação de ordem fraca, uma vez que $A_1 = \{x, y\}$ e $A_2 = \{y, z\}$ são duas anticadeias maximais distintas com intersecção não vazia.

O Teorema 7.25 permite-nos representar uma ordem fraca como uma sequência de anticadeias,

$$A_1 \prec_{AM(P)} A_2 \prec_{AM(P)} \cdots \prec_{AM(P)} A_q.$$

Logo, ordenando os elementos de cada anticadeia, de modo arbitrário, obtém-se uma extensão linear.

Dados dois intervalos $[a, b]$ e $[\alpha, \beta]$, diz-se que $[a, b] \triangleleft [\alpha, \beta]$ se $b < \alpha$ e dado um conjunto parcialmente ordenado $P = (X, \preceq_P)$, supondo que a partir dele é possível determinar um conjunto de intervalos $\{I_x = [\alpha_x, \beta_x] : x \in X\}$, tais que

$$\forall_{x_i, x_j \in X} x_i \prec_P x_j \Leftrightarrow I_{x_i} \triangleleft I_{x_j},$$

então \preceq_P é uma ordem intervalar.

Nem todas as ordens intervalares são semi-transitivas. Por exemplo, a ordem intervalar representada na Figura 7.32 não é semi-transitiva (uma vez que a sua restrição aos intervalos x, y, z e v é isomorfa a $1 \oplus 3$).

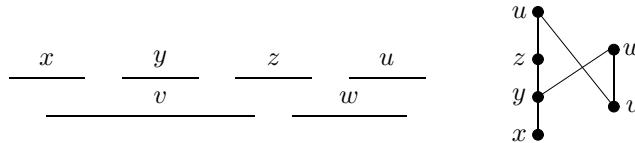


Figura 7.32: Exemplo de ordem intervalar não semi-transitiva.

Teorema 7.26. Seja $\{I_x = [\alpha_x, \beta_x] : x \in X\}$ uma família de intervalos tais que $\forall_{x \in X} \beta_x - \alpha_x = \epsilon > 0$.

Então $P = (X, \preceq_P)$ tal que

$$\forall_{x_i, x_j \in X} x_i \prec_P x_j \Leftrightarrow I_{x_i} \triangleleft I_{x_j}$$

é uma quase-ordem.

Demonstração. Suponha-se que $P = (X, \preceq_P)$ não é uma quase-ordem. Uma vez que \preceq_P é uma ordem intervalar, então \preceq_P não é semi-transitiva, isto é, existe um subconjunto de X , $Y = \{x, y, z, u\}$, onde a restrição de \preceq_P é tal que $x \prec_P y \prec_P z$, mas u não é comparável com nenhum dos elementos x, y e z . Sejam $[\alpha_x, \beta_x], [\alpha_y, \beta_y], [\alpha_z, \beta_z]$ e $[\alpha_u, \beta_u]$ os intervalos associados, respectivamente, a x, y, z e u . Então

$$\beta_x < \alpha_y, \beta_y < \alpha_z, \alpha_u \leq \beta_x \text{ e } \alpha_z \leq \beta_u,$$

e, consequentemente,

$$\epsilon = \beta_u - \alpha_u \geq \alpha_z - \beta_x > \beta_y - \alpha_y + \alpha_y - \beta_x = \epsilon + \alpha_y - \beta_x,$$

o que constitui uma contradição, uma vez que $\alpha_y - \beta_x > 0$. \square

Denotando o conjunto das pré-ordens definidas em X por $PO(X)$, o das ordens parciais por $OP(X)$, o das ordens intervalares por $OI(X)$, o das semi-transitivas por $ST(X)$, o das quase-ordens por $QO(X)$, o das ordens fracas por $OF(X)$ e o das ordens lineares por $OL(X)$, vem que

$$OL(X) \subset OF(X) \subset QO(X) = OI(X) \cap ST(X).$$

Por outro lado

$$OI(X) \subset OP(X) \subset PO(X) \text{ e } ST(X) \subset OP(X) \subset PO(X).$$

A Figura 7.33 ilustra estas relações de inclusão e intersecção entre as referidas extensões e subrelações de ordens parciais.

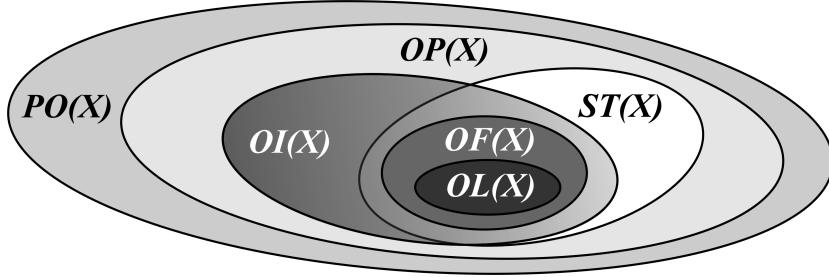


Figura 7.33: Inclusão e intersecção de diferentes relações de ordem.

Sejam $\{L_1(P), \dots, L_k(P)\}$ um conjunto de extensões lineares do conjunto parcialmente ordenado $P = (X, \preceq_P)$. Então $\bigcap_{j=1}^k L_j(P)$ denota a ordem parcial definida em X , onde dois elementos de X são comparáveis se e só se são comparáveis, segundo a mesma direcção, para todas as extensões lineares do conjunto $\{L_j(P) : j \in [k]\}$. É claro que se o conjunto $\{L_j(P) : j \in [k]\}$ contém todas as extensões lineares de P , então $P = \bigcap_{j=1}^k L_j(P)$.

Definição 7.30 (Dimensão). *O menor número de extensões lineares dum conjunto parcialmente ordenado $P = (X, \preceq_P)$ cuja intersecção é P designa-se por dimensão de P e denota-se por $\dim(P)$, isto é,*

$$\dim(P) = \min\{|J| : J \subseteq [k], P = \bigcap_{j \in J} L_j(P)\}, \quad (7.5)$$

onde k é o número de extensões lineares de P .

Desta definição decorre que se P é linear então $\dim(P) = 1$.

O conceito de dimensão de um conjunto parcialmente ordenado foi introduzido por B. Dushnik e E. Miller em 1941 e é conhecido também como dimensão de Dushnik-Miller.

Relativamente ao conjunto parcialmente ordenado P representado na Figura 7.1, obtém-se $P = L_2(P) \cap L_5(P)$, donde (tendo em conta que \preceq_P não é linear e, consequentemente, $\dim(P) \geq 2$) se conclui que $\dim(P) = 2$.

Note-se que, de acordo com a definição de dimensão de um conjunto parcialmente ordenado, se Q é uma extensão de P , então $\dim(P) \geq \dim(Q)$.

Exemplo 7.33. Vamos apresentar uma aplicação das ordens intervalares na resolução de problemas de sequenciamento de tarefas que podem ser executadas em qualquer máquina de um certo conjunto.

Solução. Seja $T = \{\tau_j : 1 \leq j \leq n\}$ um conjunto de tarefas que podem ser executadas em qualquer máquina de um conjunto de m máquinas idênticas (cada uma das quais executa uma única tarefa de cada vez), com limites bem definidos em relação ao instante em que se deve iniciar a sua execução (i_j) e relativamente ao instante em que deve findar (f_j). Deste modo, cada tarefa τ_j fica definida pelo intervalo $[i_j, f_j]$.

O objectivo é utilizar o menor número de máquinas na execução de todas as tarefas. Assim, definindo-se a ordem intervalar no conjunto das tarefas, $\mathcal{T} = (T, \triangleleft_T)$, de tal modo que $\tau_p \triangleleft_T \tau_q \Leftrightarrow f_p < i_q$, conclui-se que uma cadeia de tarefas pode ser executada consecutivamente na mesma máquina e, reciprocamente, cada sequência de tarefas processadas numa dada máquina corresponde a uma cadeia. Logo, o menor número de máquinas necessárias para a execução das n tarefas é igual ao menor número de cadeias em que se pode partir o conjunto parcialmente ordenado T .

Invocando o teorema de Dilworth (Theorema 7.21), onde se afirma que *num conjunto parcialmente ordenado o menor número de cadeias em que se pode partir o conjunto é igual à cardinalidade da maior anticadeia* conclui-se que o menor número de máquinas necessárias para executar todas as tarefas é igual à largura de \mathcal{T} . \square

7.6. Teorema da inversão de Möbius

Ao longo desta secção vamos considerar o cpo $P = (X, \preceq)$, o qual podemos representar pela função $\zeta : X \times X \rightarrow \mathbb{C}$, tal que

$$\zeta(x, y) = \begin{cases} 1, & \text{se } x \preceq_P y \\ 0, & \text{caso contrário.} \end{cases}$$

Com efeito, esta função ζ , conhecida por *função zeta* de P , contém toda a informação necessária para representar P , ou seja, contém informação sobre todos os pares de elementos $x, y \in X$ tais que $x \preceq_P y$.

Considerando $\mathcal{F}(X)$ como sendo o conjunto de todas as funções $f : X \times X \rightarrow \mathbb{C}$, tais que $f(x, y) = 0$ se $x \not\preceq y$ (é claro que $\zeta \in \mathcal{F}(X)$), dadas duas funções $f, g \in \mathcal{F}(X)$, define-se o *produto de convolução* $f * g$ como sendo a função $h \in \mathcal{F}(X)$ tal que $\forall x, y \in X$

$$h(x, y) = \begin{cases} \sum_{x \preceq z \preceq y} f(x, z)g(z, y), & \text{se } x \preceq y \\ 0, & \text{caso contrário.} \end{cases}$$

Outra função bem conhecida pertencente a $\mathcal{F}(X)$ é a função delta de Kronecker, δ , definida por

$$\delta(x, y) = \begin{cases} 1, & \text{se } x = y \\ 0, & \text{caso contrário.} \end{cases}$$

Esta função δ comporta-se como elemento unidade, relativamente ao produto de convolução. Com efeito, dada uma função arbitrária $f \in \mathcal{F}(X)$ e $x, y \in X$, podemos concluir o seguinte:

- Se $x \not\preceq y$, então $f(x, y) = 0$, $(\delta * f)(x, y) = \sum_{x \preceq z \preceq y} \delta(x, z)f(z, y) = 0$ e $(f * \delta)(x, y) = \sum_{x \preceq z \preceq y} f(x, z)\delta(z, y) = 0$, donde $(\delta * f)(x, y) = (f * \delta)(x, y) = f(x, y)$.
- Se $x \preceq_P y$, então

$$(\delta * f)(x, y) = \sum_{x \preceq z \preceq y} \delta(x, z)f(z, y) = f(x, y) = \sum_{x \preceq z \preceq y} f(x, z)\delta(z, y) = (f * \delta)(x, y).$$

Logo, $\forall f \in \mathcal{F}(X)$

$$\delta * f = f * \delta = f. \quad (7.6)$$

Exemplo 7.34. Considerando o cpo $P = (X, \preceq)$, vamos provar que o produto de convolução das funções pertencentes a $\mathcal{F}(X)$ é associativo.

Solução. Considere as funções $f, g, h \in \mathcal{F}(X)$ e $x, y \in X$. Se $x \not\leq y$, é imediato que $(f * (g * h))(x, y) = 0 = ((f * g) * h)(x, y)$. Se $x \preceq y$, então

$$\begin{aligned} (f * (g * h))(x, y) &= \sum_{x \preceq z \preceq y} f(x, z)(g * h)(z, y) \\ &= \sum_{x \preceq z \preceq y} f(x, z) \left(\sum_{z \preceq z' \preceq y} g(z, z')h(z', y) \right) \\ &= \sum_{x \preceq z' \preceq y} \left(\sum_{x \preceq z \preceq z'} f(x, z)g(z, z') \right) h(z', y) \\ &= \sum_{x \preceq z' \preceq y} (f * g)(x, z')h(z', y) \\ &= ((f * g) * h)(x, y). \end{aligned}$$

□

Qualquer função $f \in \mathcal{F}(X)$ tal que $f(x, x) \neq 0 \forall x \in X$, admite como inversa à esquerda, relativamente ao produto de convolução, a função $g \in \mathcal{F}(X)$ definida por

$$g(x, x) = \frac{1}{f(x, x)}, \quad \forall x \in X, \tag{7.7}$$

$$g(x, y) = - \sum_{x \preceq z \prec y} g(x, z) \frac{f(z, y)}{f(y, y)}, \quad \forall x, y \in X \text{ tal que } x \prec_P y. \tag{7.8}$$

Com efeito, de (7.7) e (7.8), decorre a igualdade $\sum_{x \preceq z \preceq y} g(x, z)f(z, y) = \delta(x, y)$, ou seja, $g * f = \delta$. De modo semelhante se pode concluir que existe uma função $h \in \mathcal{F}(X)$ que é a inversa à direita de f , ou seja, $f * h = \delta$. Porém, tendo em conta (7.6) e a associatividade do produto de convolução,

$$g = g * \delta = g * (f * h) = (g * f) * h = \delta * h = h.$$

Consequentemente, $g * f = f * g = \delta$, pelo que g é a inversa de f relativamente ao produto de convolução.

Tendo em conta que a função zeta de P , ζ , pertence a $\mathcal{F}(X)$ e é tal que $\zeta(x, x) \neq 0 \forall x \in X$, podemos introduzir a *função de Möbius*¹⁰ (que desempenha papel de relevo, quer na *Combinatória*, quer na *Teoria dos Números*) como sendo a função inversa de ζ . Logo,

$$\mu * \zeta = \delta = \zeta * \mu \tag{7.9}$$

e, consequentemente, $\sum_{x \preceq z \preceq y} \mu(x, z)\zeta(z, y) = \delta(x, y) \Leftrightarrow \sum_{x \preceq z \preceq y} \mu(x, z) = \delta(x, y)$. Desta última igualdade, decorre a seguinte definição recursiva da função de Möbius:

$$\mu(x, y) = \begin{cases} 1, & \text{se } x = y \\ -\sum_{x \preceq z \prec y} \mu(x, z), & \text{se } x \prec y. \end{cases} \tag{7.10}$$

Exemplo 7.35. Vamos determinar a função de Möbius de um conjunto totalmente ordenado $P = (X, \leq)$, tal que $X = \{x_1, \dots, x_n\}$ e $x_1 < \dots < x_n$.

¹⁰ August Ferdinand Möbius (1790–1868), matemático e astrónomo alemão que introduziu pela primeira vez o conceito de coordenadas homogéneas em geometria projectiva.

Solução. Sabemos que $\mu(x_i, x_i) = 1$, para $i = 1, \dots, n$, e $\mu(x_j, x_i) = 0$, para $1 \leq i < j \leq n$. Sendo $j = i + i$, com $1 \leq i \leq n - 1$, de acordo com (7.10), $\sum_{i \leq j \leq i+1} \mu(x_i, x_j) = 0$ e, consequentemente, $\mu(x_i, x_i) + \mu(x_i, x_{i+1}) = 0$. Logo, $\mu(x_i, x_{i+1}) = -1$. Por sua vez, tendo em conta que $\mu(x_i, x_i) + \mu(x_i, x_{i+1}) + \mu(x_i, x_{i+2}) = 0$, para $1 \leq i \leq n - 2$, vem $\mu(x_i, x_{i+2}) = -(1 + (-1)) = 0$. No caso geral, por indução, concluímos que a função de Möbius de P fica determinada pela expressão

$$\mu(x_i, x_j) = \begin{cases} 1, & \text{se } j = i, \\ -1, & \text{se } j = i + 1, \\ 0, & \text{caso contrário.} \end{cases}$$

□

Considerando os conjuntos parcialmente ordenados $P_1 = (X_1, \preceq_1), \dots, P_r = (X_r, \preceq_r)$ e definindo-se a relação binária \preceq no produto cartesiano $X_1 \times \dots \times X_r$, como sendo

$$(x_1, \dots, x_r) \preceq (y_1, \dots, y_r) \text{ se e só se } x_i \preceq_i y_i, \forall i \in \{1, \dots, r\},$$

prova-se (ver Exercício 7.34) que $P_1 \times \dots \times P_r = (X_1 \times \dots \times X_r, \preceq)$ é um cpo. Este cpo designa-se por *produto directo* dos conjuntos parcialmente ordenados P_1, \dots, P_r . O Teorema a seguir, mostra como obter a função de Möbius do produto directo de conjuntos parcialmente ordenados, a partir da função de Möbius de cada um deles.

Teorema 7.27. *Sejam $P = (X_1, \preceq_P)$ e $Q = (X_2, \preceq_Q)$ dois conjuntos parcialmente ordenados com funções de Möbius μ_P e μ_Q , respectivamente, e seja $\mu_{P \times Q}$ a função de Möbius do produto directo $P \times Q = (X_1 \times X_2, \preceq_{P \times Q})$. Então, $\forall (x_1, x_2), (y_1, y_2) \in X_1 \times X_2$*

$$\mu_{P \times Q}((x_1, x_2), (y_1, y_2)) = \mu_P(x_1, y_1)\mu_Q(x_2, y_2).$$

Demonstração. Sendo $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$ tais que $(x_1, x_2) \preceq_{P \times Q} (y_1, y_2)$, vem

$$\begin{aligned} \sum_{(x_1, x_2) \preceq_{P \times Q} (z_1, z_2) \preceq_{P \times Q} (y_1, y_2)} \mu_P(x_1, z_1)\mu_Q(x_2, z_2) &= \left(\sum_{x_1 \preceq_P z_1 \preceq_P y_1} \mu_P(x_1, z_1) \right) \left(\sum_{x_2 \preceq_Q z_2 \preceq_Q y_2} \mu_Q(x_2, z_2) \right) \\ &= \delta(x_1, y_1)\delta(x_2, y_2) \\ &= \delta((x_1, x_2), (y_1, y_2)). \end{aligned}$$

Com base na fórmula recursiva (7.10) que determina de modo único a função de Möbius, a demonstração fica completa. □

Este resultado pode estender-se imediatamente ao produto arbitrário de conjuntos totalmente ordenados, obtendo-se o seguinte corolário.

Corolário 7.28. *Considerando os conjuntos totalmente ordenados $P_1 = (X_1, \preceq_1), \dots, P_r = (X_r, \preceq_r)$, cujas funções de Möbius são, respectivamente, μ_1, \dots, μ_r , se μ é a função de Möbius do produto directo $P_1 \times \dots \times P_r$, então*

$$\mu((x_1, \dots, x_r), (y_1, \dots, y_r)) = \prod_{i=1}^r \mu_i(x_i, y_i).$$

Exemplo 7.36. Tendo em conta que a relação de divisibilidade: x divide y , que significa y é múltiplo de x e se denota por $x|y$, é uma relação de ordem parcial no subconjunto de números naturais $X = \{1, \dots, n\}$, considerando o cpo $P = (X, |)$ e sendo μ a função de Möbius de P , vamos determinar $\mu(1, d)$, para $d \in P$ tal que $d|n$.¹¹

¹¹No caso particular desta relação de divisibilidade, em geral, escreve-se simplesmente $\mu(d)$ (em vez de $\mu(1, d)$), sendo esta a versão clássica da função de Möbius.

Solução. Sabe-se que n admite uma factorização em números primos $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (que é única a menos da ordem dos factores), onde p_1, \dots, p_k são primos distintos e $\alpha_1, \dots, \alpha_k$ são inteiros positivos. Seja $X^* \subseteq X$, o subconjunto dos inteiros $d \in X$ que dividem n , ou seja, $X^* = \{d \in X : d|n\}$. Assim, podemos considerar o cpo $Q = (X^*, |)$ no qual, se $q, r \in X^*$, então $q = p_1^{\beta_1} \cdots p_k^{\beta_k}$ e $r = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, com $0 \leq \beta_j, \gamma_j \leq \alpha_j$, para $j = 1, \dots, k$ e, adicionalmente, $q|r$ se e só se $\beta_i \leq \gamma_i$, para $i = 1, \dots, k$. Considerando os conjuntos parcialmente ordenados $P_1 = (X_1^*, |), \dots, P_k = (X_k^*, |)$, onde $X_i^* = \{p_i^j, j = 0, \dots, \alpha_i\}$, podemos concluir que o cpo Q é precisamente o produto directo dos conjuntos totalmente ordenados P_1, \dots, P_k , com $\alpha_1 + 1, \dots, \alpha_k + 1$ elementos, respectivamente. Logo, considerando $d = p_1^{\lambda_1} \cdots p_k^{\lambda_k} \in X^*$ e aplicando o Corolário 7.28, obtém-se

$$\mu_Q(1, d) = \prod_{i=1}^k \mu_i(1, p_i^{\lambda_i}),$$

onde μ_i denota a função de Möbius do cpo P_i , para $i = 1, \dots, k$. Tendo em conta o Exemplo 7.35, sabemos que

$$\mu_i(1, p_i^{\lambda_i}) = \begin{cases} 1, & \text{se } \lambda_i = 0, \\ -1, & \text{se } \lambda_i = 1, \\ 0, & \text{se } \lambda_i \geq 2 \end{cases}$$

Como consequência, dado que $\mu(1, d) = \mu_Q(1, d)$, vem

$$\mu(1, d) = \begin{cases} 1, & \text{se } d = 1, \\ (-1)^k, & \text{se } d \text{ é o produto de } k \text{ primos distintos,} \\ 0, & \text{caso contrário.} \end{cases}$$

□

Teorema 7.29 (da inversão de Möbius). *Considerando o cpo $P = (X, \preceq)$ e as funções $f, g : X \rightarrow \mathbb{C}$, se X é finito, então*

$$g(y) = \sum_{z \preceq y} f(z) \quad \forall y \in X \quad \Leftrightarrow \quad f(y) = \sum_{z \preceq y} g(z) \mu(z, y) \quad \forall y \in X. \quad (7.11)$$

Demonstração. Vamos definir o cpo $Q = (X', \preceq_Q)$, a partir do cpo P , da seguinte forma: se P tem elemento mínimo $\hat{0}$, então $Q = P$; caso contrário $X' = X \cup \{\hat{0}\}$, onde $\hat{0}$ é elemento mínimo de Q (ou seja, é tal que $\hat{0} \prec_Q x \forall x \in X$).

- Supondo que $\forall y \in X$ se verifica a igualdade $g(y) = \sum_{x \preceq y} f(x)$, a partir das funções f e g , vamos definir $f' : X' \times X' \rightarrow \mathbb{C}$ e $g' : X' \times X' \rightarrow \mathbb{C}$, respectivamente, da seguinte forma: $\forall (z, x) \in X' \times X'$,

$$f'(z, x) = \begin{cases} f(x), & \text{se } z \preceq_Q x \text{ e } x \in X \\ 0, & \text{caso contrário,} \end{cases}$$

e $g' = f' * \zeta$. Então, $\forall y \in X$

$$g(y) = \sum_{x \preceq y} f(x) = \sum_{\hat{0} \preceq_Q x \preceq_Q y} f'(\hat{0}, x) = \sum_{\hat{0} \preceq_Q x \preceq_Q y} f'(\hat{0}, x) \zeta(x, y) = (f' * \zeta)(\hat{0}, y) = g'(\hat{0}, y).$$

Adicionalmente, tendo em conta (7.9) e $\zeta * \mu = \delta$, vem $f' * \zeta = g' \Leftrightarrow f' = g' * \mu$. Logo, $\forall y \in X$

$$f(y) = f'(\hat{0}, y) = (g' * \mu)(\hat{0}, y) = \sum_{\hat{0} \preceq_Q x \preceq_Q y} g'(\hat{0}, x) \mu(x, y) = \sum_{x \preceq y} g(x) \mu(x, y).$$

- Reciprocamente, supondo que $\forall y \in X$ se verifica a igualdade $f(y) = \sum_{x \preceq y} g(x)\mu(x, y)$, a partir das funções f e g , vamos definir $g' : X' \times X' \rightarrow \mathbb{C}$ e $f' : X' \times X' \rightarrow \mathbb{C}$, respectivamente, da seguinte forma: $\forall (z, x) \in X' \times X'$,

$$g'(z, x) = \begin{cases} g(x), & \text{se } z \preceq_Q x \text{ e } x \in X \\ 0, & \text{caso contrário,} \end{cases}$$

e $f' = g' * \mu$. Então, $\forall y \in X$

$$f(y) = \sum_{x \preceq y} g(x)\mu(x, y) = \sum_{\hat{0} \preceq_Q x \preceq_Q y} g'(\hat{0}, x)\mu(x, y) = (g' * \mu)(\hat{0}, y) = f'(\hat{0}, y).$$

Adicionalmente, $g' * \mu = f' \Leftrightarrow g' = f' * \zeta$ e, consequentemente, $\forall y \in X$

$$g(y) = g'(\hat{0}, y) = (f' * \zeta)(\hat{0}, y) = \sum_{\hat{0} \preceq_Q x \preceq_Q y} f'(\hat{0}, x)\zeta(x, y) = \sum_{x \preceq y} f(x).$$

□

Exemplo 7.37. Recorrendo à fórmula da inversão de Möbius (7.11), vamos provar a fórmula de Daniel da Silva para a determinação da cardinalidade da reunião dos conjuntos finitos A_1, \dots, A_n (Teorema 3.3).

Solução. Seja $Q = (\mathcal{A}; \subseteq)$ o cpo definido pelo conjunto de todas as intersecções dos conjuntos A_1, \dots, A_n , incluindo a intersecção de zero conjuntos que vamos denotar por $\cap_{i \in \emptyset} A_i = A_1 \cup \dots \cup A_n$, e pela relação de inclusão em sentido lato \subseteq . Por facilidade, vamos denotar $\cap_{i \in I} A_i$, simplesmente pelo respectivo conjunto de índices I e $\cap_{i \in I} A_i \subseteq \cap_{j \in J} A_j$, por $I \preceq J$. Assim, considere-se a função $f : \mathcal{A} \rightarrow \mathbb{C}$, tal que para cada elemento I de \mathcal{A} , $f(I)$ é igual ao número de elementos em I (ou seja, em $\cap_{i \in I} A_i$) que não pertencem $J \prec I$ (ou seja, a $\cap_{j \in J} A_j \subset \cap_{i \in I} A_i$) em Q e seja $g : \mathcal{A} \rightarrow \mathbb{C}$ tal que $g(J) = |\cap_{i \in J} A_i|$. Nestas condições, $g(\emptyset) = |A_1 \cup \dots \cup A_n| = \sum_{J \preceq I} f(J)$. Logo, aplicando a fórmula da inversão de Möbius, vem $0 = f(\emptyset) = \sum_{J \preceq \emptyset} g(J)\mu(J, \emptyset) \Leftrightarrow g(\emptyset) = -\sum_{J \prec \emptyset} g(J)\mu(J, \emptyset)$ e esta última igualdade é equivalente à igualdade

$$|A_1 \cup \dots \cup A_n| = -\sum_{J \prec \emptyset} \mu(J, \emptyset) |\cap_{j \in J} A_j|,$$

onde $\mu(J, \emptyset) = (-1)^{|J|}$.

□

Exemplo 7.38. Dados três conjuntos finitos A_1, A_2, A_3 , com recurso à fórmula da inversão de Möbius, vamos determinar a cardinalidade do conjunto $A_1 \cup A_2 \cup A_3$.

Solução. Considerando o cpo $Q = (\mathcal{A}; \subseteq)$, tal que $\mathcal{A} = \{A_1 \cup A_2 \cup A_3, A_1, A_2, A_3, A_1 \cap A_2, A_1 \cap A_3, A_2 \cap A_3, A_1 \cap A_2 \cap A_3\}$ e a relação de ordem parcial definida pelo diagrama de Hasse da Figura 7.34, vem

$$\begin{aligned} |A \cup B \cup C| &= -(\mu(\{1\}, \emptyset)|A_1| + \mu(\{2\}, \emptyset)|A_2| + \mu(\{3\}, \emptyset)|A_3| \\ &\quad + \mu(\{1, 2\}, \emptyset)|A_1 \cap A_2| + \mu(\{1, 3\}, \emptyset)|A_1 \cap A_3| + \mu(\{2, 3\}, \emptyset)|A_2 \cap A_3| \\ &\quad + \mu(\{1, 2, 3\}, \emptyset)|A_1 \cap A_2 \cap A_3|). \end{aligned}$$

Logo, $|A \cup B \cup C| = -(-|A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|)$.

□

Com uma técnica idêntica à utilizada na demonstração do Teorema 7.29, igualmente se prova (ver Exercício 7.35) a formulação dual do teorema da inversão de Möbius.

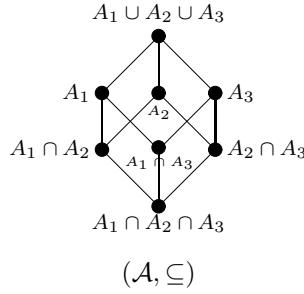


Figura 7.34: Diagrama de Hasse do cpo do Exemplo 7.38.

Teorema 7.30 (da inversão de Möbius na formulação dual). *Considerando o cpo $P = (X, \preceq)$ e as funções $f, g : X \rightarrow \mathbb{C}$, se X é finito, então*

$$g(x) = \sum_{x \preceq z} f(z) \quad \forall x \in X \quad \Leftrightarrow \quad f(x) = \sum_{x \preceq z} \mu(x, z)g(z) \quad \forall x \in X. \quad (7.12)$$

7.7. Conjuntos extremais

Um conjunto parcialmente ordenado de utilização corrente é o conjunto das partes de um conjunto finito X , $\mathcal{P}(X)$, munido da relação de ordem parcial \subseteq . Considerando $X = \{x_1, x_2, \dots, x_n\}$, é imediato concluir que o conjunto de subconjuntos de X , $C = \{\emptyset, \{x_1\}, \{x_1, x_2\}, \dots, X\}$ constitui uma cadeia de $P = (\mathcal{P}(X), \subseteq_P)$ de máxima cardinalidade. Consequentemente, P tem comprimento $|X|$ e, por aplicação do Teorema 7.22, $\mathcal{P}(X)$ pode partir-se em $|X| + 1$ anticadeias. No que diz respeito à largura de P , a sua avaliação é, porém, mais complicada.

Definição 7.31 (Família de Sperner). *Dado o conjunto parcialmente ordenado $P = (\mathcal{P}(X), \subseteq_P)$, uma família $\mathcal{F} \subseteq \mathcal{P}(X)$, diz-se uma família de Sperner, se nenhum elemento de \mathcal{F} contém qualquer outro, isto é, se*

$$\forall_{A, B \in \mathcal{F}} A \neq B \Rightarrow \{(A, B), (B, A)\} \cap \subseteq_P = \emptyset.$$

Assim, pode afirmar-se que \mathcal{F} constitui uma anticadeia de $\mathcal{P}(X)$, pelo que se \mathcal{F} tem máxima cardinalidade então P tem largura $|\mathcal{F}|$.

Dado um número arbitrário $k \leq n$, o conjunto dos subconjuntos de X (com $|X| = n$) de cardinalidade k é uma família de Sperner com $\binom{n}{k}$ elementos. Uma vez que estes coeficientes binomiais crescem até ao ponto médio, pode concluir-se que as famílias de Sperner deste tipo atingem a máxima cardinalidade para

$$k = \begin{cases} \frac{n}{2}, & \text{se } n \text{ é par,} \\ \frac{n-1}{2}, & \text{se } n \text{ é ímpar,} \end{cases}$$

e, como consequência, $k = \lfloor \frac{n}{2} \rfloor$. Relacionado com o número de anticadeias numa família de subconjuntos de $[n]$, onde se define a relação de ordem parcial \subseteq , Emanuel Sperner (1905–1980) introduziu, em 1928, o resultado que o teorema a seguir (com o seu nome) explicita.

Teorema 7.31 (Lema de Sperner). *Se \mathcal{A} é uma anticadeia de máxima cardinalidade do conjunto parcialmente ordenado $P = (\mathcal{P}([n]), \subseteq)$ então*

$$|\mathcal{A}| = \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Demonstração. Considerando uma anticadeia $\mathcal{A} = \{A_1, \dots, A_q\}$ de máxima cardinalidade do conjunto parcialmente ordenado $P = (\mathcal{P}([n]), \subseteq)$ e denotando $\alpha_i = |A_i|$, para cada $i \in [q]$, primeiramente vamos provar que, para cada A_i , existem $\alpha_i!(n - \alpha_i)!$ cadeias de $n + 1$ elementos que contêm A_i .

Com efeito, supondo $A_i = \{\tau_{i1}, \dots, \tau_{i\alpha_i}\}$, então as cadeias de máxima cardinalidade que contêm A_i , começam com o conjunto vazio, depois têm um conjunto singular $\{\tau_{ij}\}$, com $j \in [\alpha_i]$, a seguir um conjunto do tipo $\{\tau_{ij}, \tau_{ik}\}$, com $k \in [\alpha_i] \setminus \{j\}$, e assim sucessivamente, até se atingir o conjunto A_i . Adicionalmente, destas cadeias fazem ainda parte os conjuntos $A_i \cup \{x\}$, para cada $x \in [n] \setminus A_i$, os conjuntos $A_i \cup \{x, y\}$, etc, até ao conjunto $[n]$. Nestas condições, uma vez que cada cadeia que contenha A_i , pode ser identificada por uma sequência definida por uma permutação dos α_i elementos de A_i concatenada com uma permutação dos $n - \alpha_i$ elementos de $[n] \setminus A_i$, conclui-se que, efectivamente, o número de cadeias de $n + 1$ elementos que contêm A_i é igual a $\alpha_i!(n - \alpha_i)!$.

Tendo em conta que existem $n!$ cadeias de comprimento $n + 1$, conclui-se que

$$\sum_{i=1}^q \alpha_i!(n - \alpha_i)! \leq n! \Leftrightarrow \sum_{i=1}^q \frac{\alpha_i!(n - \alpha_i)!}{n!} \leq 1 \Leftrightarrow \sum_{i=1}^q \binom{n}{\alpha_i}^{-1} \leq 1.$$

Por outro lado, tendo em conta que $\binom{n}{k}$ atinge o seu máximo para $k = \lfloor \frac{n}{2} \rfloor$, vem que

$$q \binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} \leq \sum_{i=1}^q \binom{n}{\alpha_i}^{-1} \leq 1 \Leftrightarrow |\mathcal{A}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Finalmente, dado que os $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ subconjuntos de cardinalidade $\lfloor \frac{n}{2} \rfloor$ formam uma anticadeia, podemos concluir que se \mathcal{A} é uma anticadeia de máxima cardinalidade, então $|\mathcal{A}| \geq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. \square

A teoria dos conjuntos extremais também inclui o estudo das famílias intersectantes.

Definição 7.32 (Família intersectante). *Uma família \mathcal{F} de subconjuntos de X designando-se por família intersectante se $\forall_{A, B \in \mathcal{F}} A \cap B \neq \emptyset$.*

Teorema 7.32. *Qualquer família intersectante \mathcal{F} de subconjuntos de $[n]$, é tal que $|\mathcal{F}| \leq 2^{n-1}$. Adicionalmente, pode concluir-se que existe uma destas famílias cuja cardinalidade é precisamente 2^{n-1} .*

Demonstração. Tendo em conta que os 2^n subconjuntos A de $[n]$ se podem dividir em 2^{n-1} pares complementares $(A, [n] \setminus A)$, conclui-se que qualquer família intersectante de $[n]$ contém, no máximo, um conjunto de cada um destes pares. Logo, $|\mathcal{F}| \leq 2^{n-1}$.

Por outro lado, qualquer família de subconjuntos de $[n]$, que contenha um elemento particular x , tem 2^{n-1} elementos e é intersectante. \square

Vamos finalizar este capítulo apresentando um resultado associado às famílias intersectantes, introduzido em [33].

Teorema 7.33 (de Erdős-Ko-Radó). *Seja $\mathcal{F} \subseteq \{A \in \mathcal{P}([n]) : |A| = k\}$ uma família intersectante. Se $k \leq \frac{n}{2}$ então $|\mathcal{F}| \leq \binom{n-1}{k-1}$.*

Demonstração. Considerem-se os números de $[n]$ dispostos consecutivamente ao longo de uma circunferência e seja $C = \{C_1, \dots, C_n\}$ o conjunto de todos os conjuntos cujos elementos são as componentes dos k -uplos consecutivos que se conseguem observar de um modo circular, isto é, $C_j = \{j, j+1, \dots, j+k-1\}$, onde as operações são consideradas módulo n (com n ocupando a posição do elemento nulo).

Consequentemente vem que $|\mathcal{F} \cap C| \leq k$. Com efeito, se $C_j \in \mathcal{F}$, para algum j , então, além de C_j , apenas pertencem a \mathcal{F} , no máximo um conjunto de cada par de conjuntos de cardinalidade k ($\{r, r+1, \dots, r+k-1\}, \{r-k, r-k+1, \dots, r-1\}$), com $j < r \leq j+k$. O mesmo se pode afirmar

para qualquer outra disposição dos números na circunferência, isto é, para qualquer das permutações, π , dos n números de $[n]$.

Denotando por $C^\pi = \{C_1^\pi, \dots, C_n^\pi\}$ cada um dos conjuntos obtidos para as diferentes permutações de $[n]$, $\Pi([n])$, (onde $C_j^\pi = \{\pi(j), \pi(j+1), \pi(j+2), \dots, \pi(j+k-1)\}$) obtém-se

$$\sum_{\pi \in \Pi([n])} |C^\pi \cap \mathcal{F}| \leq kn!. \quad (7.13)$$

Alternativamente, considerando cada um dos conjuntos $A \in \mathcal{F}$ e cada um dos índices $r \in \{1, \dots, n\}$ verifica-se a existência de $k!(n-k)!$ permutações π tais que $C_r^\pi = A$ e, consequentemente, conclui-se que

$$\sum_{\pi \in \Pi([n])} |C^\pi \cap \mathcal{F}| = |\mathcal{F}| k!(n-k)! . \quad (7.14)$$

De (7.13) e (7.14) vem finalmente que

$$|\mathcal{F}| k!(n-k)! \leq kn! \Leftrightarrow |\mathcal{F}| \leq \frac{kn!}{nk!(n-k)!} \Leftrightarrow |\mathcal{F}| \leq \binom{n-1}{k-1} . \quad \square$$

Adicionalmente, podemos concluir que existem famílias, \mathcal{F} , intersectantes de subconjuntos de $[n]$ com cardinalidade k , tais que $|\mathcal{F}| = \binom{n-1}{k-1}$, pelo que este valor constitui um máximo para o conjunto das cardinalidades das famílias intersectantes constituídas por subconjuntos de $[n]$ de k elementos. Com efeito, fixado um determinado elemento $x \in [n]$, existem $|\mathcal{F}| = \binom{n-1}{k-1}$ subconjuntos de $k-1$ elementos de $[n] \setminus \{x\}$. Logo, se a cada um destes subconjuntos acrescentarmos x , obtém-se uma família intersectante de subconjuntos de $[n]$ com k elementos.

Para ilustrar a demonstração do teorema 7.33, considere-se a família intersectante de subconjuntos de $\mathcal{P}(\{1, \dots, 6\})$ de cardinalidade 3,

$$\mathcal{F} = \{\{1, 2, 4\}, \{1, 3, 4\}, \{1, 6, 4\}, \{1, 5, 4\}, \{2, 3, 4\}, \{2, 5, 4\}, \{2, 6, 4\}, \{3, 5, 4\}, \{3, 6, 4\}, \{5, 6, 4\}\}.$$

Para a distribuição circular relativa à permutação identidade, π_1 , dos elementos de $\{1, \dots, 6\}$, tendo em conta a definição dos subconjuntos C_j obtém-se $C_1 = \{1, 2, 3\}$, $C_2 = \{2, 3, 4\}$, $C_3 = \{3, 4, 5\}$, $C_4 = \{4, 5, 6\}$, $C_5 = \{5, 6, 1\}$, $C_6 = \{6, 1, 2\}$. Uma vez que $C_2 \in \mathcal{F}$, tal como se afirma na demonstração, no máximo apenas um dos subconjuntos de cada um dos pares de subconjuntos ($\{3, 4, 5\}, \{6, 1, 2\}$) e ($\{4, 5, 6\}, \{1, 2, 3\}$), pertence à família \mathcal{F} . Com efeito, podem observar-se, a partir do conjunto C_2 representado na Figura 7.35-(a), os pares de conjuntos disjuntos (C_3, C_6) (representado na Figura 7.35-(b)) e (C_4, C_1) (representado na Figura 7.35-(c)) cuja intersecção com C_2 é não vazia.

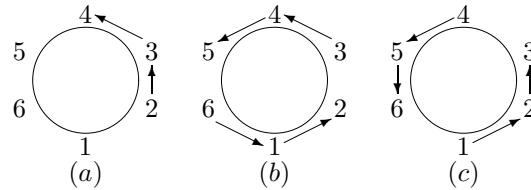


Figura 7.35: Ilustração da prova do teorema de Erdős-Ko-Radó.

Desta observação, com facilidade se conclui que, no primeiro par, apenas $\{3, 4, 5\} \in \mathcal{F}$ e, no segundo, apenas $\{4, 5, 6\} \in \mathcal{F}$. Por sua vez, considerando a distribuição circular da permutação π_2 , representada na Figura 7.36, obtém-se $C_1 = \{2, 1, 3\}$, $C_2 = \{1, 3, 4\}$, $C_3 = \{3, 4, 5\}$, $C_4 = \{4, 5, 6\}$, $C_5 = \{5, 6, 2\}$ e $C_6 = \{6, 2, 1\}$ e verifica-se que $C_4 \in \mathcal{F}$. Nestas condições, considerando os pares de subconjuntos ($\{5, 6, 2\}, \{1, 3, 4\}$) e ($\{6, 2, 1\}, \{3, 4, 5\}$), conclui-se que, no primeiro par, apenas $\{1, 3, 4\} \in \mathcal{F}$ e, no segundo, apenas $\{3, 4, 5\} \in \mathcal{F}$. Repetindo este processo para cada uma das 6! permutações, π , dos

elementos de $\{1, \dots, 6\}$ obtém-se não mais do que $3 \cdot 6!$ subconjuntos C_r^π pertencentes a \mathcal{F} (incluindo nesta contagem todos os que aparecem repetidos para as diferentes permutações).

Em alternativa ao processo acima referido, fixando um dado conjunto da família \mathcal{F} , por exemplo $A = \{1, 3, 4\}$, existem $3!(6 - 3)! = 36$ permutações, π , dos elementos de $\{1, \dots, 6\}$ para as quais se verifica a igualdade $C_r^\pi = A$. Com efeito, por exemplo para $C_1^{\pi_1} = \{1, 3, 4\} \in \mathcal{F}$, obtém-se as permutações $(1, 3, 4)$, $(1, 4, 3)$, $(4, 3, 1)$, $(4, 1, 3)$, $(3, 1, 4)$ e $(3, 4, 1)$ e, para cada uma delas, ainda se obtêm as permutações relativas aos restantes elementos de $\{1, \dots, 6\}$: $(2, 5, 6)$, $(2, 6, 5)$, $(5, 2, 6)$, $(5, 6, 2)$, $(6, 2, 5)$ e $(6, 5, 2)$. Por outro lado, para

$$C_2^{\pi_2} = C_3^{\pi_3} = C_4^{\pi_4} = C_5^{\pi_5} = C_6^{\pi_6} = \{1, 3, 4\},$$

obtém-se as mesmas permutações, pelo que o seu número é igual a 10 (número de elementos de \mathcal{F}) vezes 6 (número dos C_j s) vezes 3! (número de permutações possíveis em cada subconjunto A) vezes $(6 - 3)!$ (número de permutações possíveis para os elementos de $\{1, \dots, 6\} \setminus A$). Consequentemente, tal como na demonstração, pode concluir-se que $|F|nk!(n - k)! = 10 \cdot 6 \cdot 3!(6 - 3) = 2160 \leq 3 \cdot 6! = 2160$.

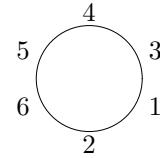


Figura 7.36: Representação da distribuição circular da permutação π_2 .

7.8. Exercícios.

7.1. Prove que o conjunto $X = \{1, 2, 3, 4\}$ munido da relação

$$\preceq = \{(1, 1), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (3, 3), (3, 5), (3, 6), (4, 4), (4, 5), (4, 6), (5, 5), (6, 6)\},$$

é um conjunto parcialmente ordenado.

7.2. Prove que se $P = (X, \preceq_P)$ é um conjunto parcialmente ordenado e existem $x_1, \dots, x_k \in X$ tais que $x_1 \preceq_P \dots \preceq_P x_k \preceq_P x_1$ então $x_1 = x_2 = \dots = x_k$.

7.3. Dada a sequência

$$S = (3, -1, 0, 2, 5, -2, 4, 1, -9, -3, 2, 6, 8, -6, -5, 7, -6, -4, 9, -7, -8, 6, -7, 5, -2, 0),$$

com 25 termos, responda às seguintes questões:

- (a) Verifique se existe ou não uma subsequência monótona com 5 termos.
- (b) Determine uma subsequência monótona com o número máximo de termos.

7.4. Dados os conjuntos parcialmente ordenados $P = (X, \preceq_P)$ e $Q = (Y, \preceq_Q)$, onde $X = \{1, 2, 3, 4\}$, $Y = \{a, b, c, d, e, f\}$,

$$\begin{aligned} \preceq_P &= \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (4, 4)\}, \\ \preceq_Q &= \{(a, a), (a, d), (b, b), (b, d), (b, f), (c, c), (c, e), (d, d), (e, e), (f, f)\}, \end{aligned}$$

determine uma função $f : X \rightarrow Y$ que preserve as relações \preceq_P e \preceq_Q .

7.5. Dados os conjuntos parcialmente ordenados $P = (X, \preceq_P)$, $Q = (Y, \preceq_Q)$ e $R = (Z, \preceq_R)$ e as funções $f : X \rightarrow Y$ e $g : Y \rightarrow Z$ que preservam as respectivas relações de ordem parcial, prove que a composição $g \circ f : P \rightarrow R$ preserva as relações de ordem parcial \preceq_P e \preceq_Q .

- 7.6. Sendo $P = (X, \preceq_P)$ um conjunto parcialmente ordenado e $Q = (Y, \mathcal{R}_Q)$ prove que se existe uma função bijectiva $f : X \rightarrow Y$ que preserva as relações \preceq_P e \mathcal{R}_Q , então Q é um conjunto parcialmente ordenado.

- 7.7. Represente o cpo $P = (X, \preceq_P)$, onde $X = \{1, 2, 3, 4, 5, 6\}$ e

$$\preceq_P = \{(1, 1), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (3, 3), (3, 5), (3, 6), (4, 4), (4, 5), (4, 6), (5, 5), (6, 6)\},$$

através do respectivo diagrama de Hasse.

- ### 7.8. Dados os conjuntos parcialmente ordenados

- (a) $P = (X, \preceq_P)$
 - (b) $Q = (Y, \preceq_Q)$
 - (c) $R = (Z, \preceq_R)$

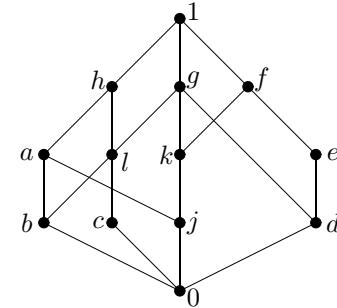
onde $X = \{1, 2, 3, 4, 5, 6\}$, $Y = \{1, 2, 3, 4\}$ e $Z = \{a, b, c, d, e, f\}$, e as respectivas relações de ordem parcial são definidas por

$$\begin{aligned}\preceq_P &= \{(1,1), (1,3), (1,4), (1,5), (1,6), (2,1), (2,2), (2,3), (2,4), (2,5), \\&\quad (2,6), (3,3), (3,5), (3,6), (4,4), (4,5), (4,6), (5,5), (6,6)\}, \\ \preceq_Q &= \{(1,1), (1,2), (1,4), (2,2), (2,3), (2,4), (3,3), (4,4)\}, \\ \preceq_R &= \{(a,a), (a,d), (b,b), (b,d), (b,f), (c,c), (c,e), (d,d), (e,e), (f,f)\},\end{aligned}$$

determine uma extensão linear para cada um deles.

- 7.9. Considerando o cpo representado na figura a seguir pelo respectivo diagrama de Hasse, calcule os seguintes elementos (caso existam):

- | | |
|---------------------------|--------------------------------------|
| (1) $b \vee c$ | (6) $l \wedge d$ |
| (2) $b \vee j$ | (7) $(h \vee g) \wedge f$ |
| (3) $c \vee j$ | (8) $(b \wedge d) \vee g$ |
| (4) $a \vee d$ | (9) $(a \vee l) \wedge (k \vee e)$ |
| (5) $(a \vee k) \wedge g$ | (9) $(a \wedge l) \vee (k \wedge e)$ |

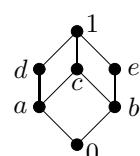


- 7.10. Desenhe os diagramas de Hasse de todos os conjuntos parcialmente ordenados, dois a dois não isomorfos, com quatro elementos.

7.11. Considerando todos os cinco reticulados com cinco elementos (ver Figura 7.14), determine os respectivos duais.

7.12. Desenhe os diagramas de Hasse dos reticulados $(D_{30}, |)$, $(D_{36}, |)$ e $(D_{70}, |)$.

7.13. Sejam $(R, \preceq, \vee, \wedge)$ um reticulado e X um conjunto não vazio. Definindo-se $F(X) = \{f : X \rightarrow R\}$ e, para $f, g \in F(X)$, as funções $f \vee' g$ e $f \wedge' g$ por $(f \vee' g)(x) = f(x) \vee g(x)$ e $(f \wedge' g)(x) = f(x) \wedge g(x)$, prove que $(F(X), \vee', \wedge')$ é um reticulado.



7.15. Seja $(R, \preceq, \vee, \wedge)$ um reticulado e $c \in R$. Demonstre que a função $f : R \rightarrow R$, determinada por $f(x) = c \wedge x$, para $x \in R$, preserva a relação de ordem.

7.16. Determine os produtos dos seguintes conjuntos parcialmente ordenados:



7.17. Sabendo que um subconjunto A de \mathbb{N} diz-se *cofinito* se $\mathbb{N} \setminus A$ é finito, demonstre que

- (a) se $F_c(\mathbb{N}) = \{A \subseteq \mathbb{N} : A \text{ é cofinito}\}$ então $(F_c(\mathbb{N}), \subseteq, \cup, \cap)$ é um reticulado;
- (b) se $FC(\mathbb{N}) = \{A \subseteq \mathbb{N} : A \text{ é finito ou } A \text{ é cofinito}\}$ então $(FC(\mathbb{N}), \subseteq, \cup, \cap)$ é um reticulado;
- (c) nenhum destes reticulados, $F_c(\mathbb{N})$ e $FC(\mathbb{N})$, é completo.

7.18. Seja (X, \preceq) um conjunto parcialmente ordenado finito. Demonstre que se pode escrever X na forma $X = \{x_1, \dots, x_n\}$, de tal forma que $x_i \preceq x_j \Rightarrow i \leq j$.

7.19. Seja $(R, \preceq, \vee, \wedge)$ um reticulado distributivo e $x \in R$. Demonstre que se $x \preceq a_1 \vee \dots \vee a_n$, com $a_1, \dots, a_n \in R$, então $x \preceq a_i$ para alguma $i \in \{1, \dots, n\}$.

7.20. Prove que dois reticulados finitos R_1 e R_2 são isomorfos se e só se os conjuntos parcialmente ordenados $\mathcal{J}(R_1)$ e $\mathcal{J}(R_2)$ são isomorfos.

7.21. Sejam (X, \preceq_X) e (Y, \preceq_Y) dois conjuntos parcialmente ordenados. Mostre que $f : X \rightarrow Y$ é isótona se e só se para, cada $B \in \mathcal{J}(Y)$, $f^{-1}(B) \in \mathcal{J}(X)$.

7.22. Seja (X, \preceq) um conjunto parcialmente ordenado e $x, y \in X$. Mostre que

- (a) $x \preceq y \Leftrightarrow \downarrow x \subseteq \downarrow y$,
- (b) se $\downarrow x = \{x\}$, então x é minimal,
- (c) determine os elementos \vee -irredutíveis do reticulado $\mathcal{J}(X)$,
- (d) se (X, \preceq) é finito, então $\mathcal{J}(\mathcal{J}(X)) = \{\downarrow x : x \in X\}$.

7.23. Mostre que o reticulado $(D_n, |)$ é complementado (é uma álgebra de Boole) se não existe p primo tal que $p^2 | n$.

7.24. Considere as relações de ordem parcial

$$\begin{aligned} \preceq_P &= \{(1, 1), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), \\ &\quad (2, 6), (3, 3), (3, 5), (3, 6), (4, 4), (4, 5), (4, 6), (5, 5), (6, 6)\}, \\ \preceq_Q &= \{(1, 1), (1, 2), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (4, 4)\}, \\ \preceq_R &= \{(a, a), (a, d), (b, b), (b, d), (b, f), (c, c), (c, e), (d, d), (e, e), (f, f)\}, \end{aligned}$$

definidas em $X = \{1, 2, 3, 4, 5, 6\}$, $Y = \{1, 2, 3, 4\}$ e $Z = \{a, b, c, d, e, f\}$, respectivamente e verifique se alguma delas é uma relação de ordem

- (a) fraca;
- (b) intervalar;
- (c) semi-transitiva;
- (d) quase-ordem.

- 7.25. No caso de alguma das relações anteriores ser uma relação de ordem fraca, determine o conjunto parcialmente ordenado AM_P das anticadeias maximais e, a partir dele, obtenha a correspondente extensão linear.
- 7.26. Determine as dimensões dos conjuntos parcialmente ordenados do Exercício 7.24.
- 7.27. Dada uma família de conjuntos parcialmente ordenados $P_i = (X, \preceq_{P_i})$, com $i \in I$, denotando por $\bigcap_{i \in I} P_i$ o par (X, \preceq) , onde $\preceq = \bigcap_{i \in I} \preceq_{P_i}$, prove que $\bigcap_{i \in I} P_i$ é um conjunto parcialmente ordenado.
- 7.28. Sendo $\mathcal{R}(P) = \{L_j(P) : j \in J\}$ o conjunto de todas as extensões lineares do conjunto parcialmente ordenado $P = (X, \preceq_P)$, prove que $P = \bigcap_{j \in J} L_j(P)$.
- 7.29. Considere os inteiros positivos $x_1 < x_2 < \dots < x_{mn+1}$ e prove que ou existe um subconjunto $S \subset \{x_1, x_2, \dots, x_{mn+1}\}$ de $m + 1$ inteiros tais que $\forall x_i, x_j \in S$, com $i < j$, x_i não divide x_j , ou existe um subconjunto $T \subset \{x_1, x_2, \dots, x_{mn+1}\}$ de $n + 1$ inteiros tais que $\forall x_i, x_j \in T$, com $i < j$, x_i divide x_j .
- 7.30. Dados $n^2 + 1$ intervalos arbitrários de \mathbb{R} prove que ou existem $n + 1$ intervalos cuja intersecção é não vazia ou existem $n + 1$ intervalos todos disjuntos.
- 7.31. Dado o conjunto parcialmente ordenado $P = (\mathcal{P}(X), \subseteq_P)$ prove que
- o comprimento de P é igual $|X|$
 - e a largura de P é não inferior a $\frac{2^{|X|}}{|X|+1}$.
- 7.32. Determine o comprimento e a largura do conjunto parcialmente ordenado definido no Exercício 7.1.
- 7.33. Prove a seguinte versão do lema de Dilworth para conjuntos infinitos:
- Teorema** (versão infinita do lema de Dilworth). *Em qualquer conjunto parcialmente ordenado com uma infinidade de elementos ou existe uma anticadeia de cardinalidade infinita ou existe uma cadeia de cardinalidade infinita.*
- 7.34. Dado os conjuntos parcialmente ordenados (X_i, \preceq_i) , $i = 1, \dots, p$, prove que a relação binária \preceq definida no produto directo $\prod_{i=1}^p X_i$ de tal forma que $(x_1, \dots, x_p) \preceq (y_1, \dots, y_p)$ se e somente se $x_i \preceq_i y_i$, para $i = 1, \dots, p$, é uma relação de ordem parcial.
- 7.35. Prove o Teorema 7.30.
- 7.36. Dado o conjunto parcialmente ordenado $P = (\mathcal{P}([n]), \subseteq_P)$, prove que existem $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ subconjuntos de cardinalidade $\lfloor \frac{n}{2} \rfloor$ que constituem uma anticadeia.
- 7.37. Dada a família $\mathcal{F}_k = \{U : U \subseteq X, |U| = k\}$, onde X é um conjunto finito não vazio, prove que se $|X| < 2k$, então \mathcal{F}_k é intersectante.
- 7.38. Prove que o conjunto parcialmente ordenado $P = (\mathcal{P}([n]), \subseteq)$ admite uma partição em $n + 1$ anticadeias e uma partição em $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ cadeias.

8

Divisibilidade e Aritmética Modular

Dado um número inteiro arbitrário, n , um seu *divisor* é um número inteiro não nulo d para o qual existe um inteiro k tal que $n = kd$. Usualmente, escreve-se $d | n$ para denotar que d é um divisor de (*ou divide*) n e escreve-se $x \nmid n$ para denotar que x não é um divisor de (*ou não divide*) n .

O conjunto dos divisores de um inteiro positivo contém números positivos e negativos. Por exemplo, denotando por D_n^* o conjunto dos divisores de n , para $n = 18$ vem

$$D_{18}^* = \{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}.$$

Dados dois inteiros positivos m e n , os divisores comuns a m e n são os elementos do conjunto $D_m^* \cap D_n^*$. Uma vez que 1 divide qualquer inteiro, podemos afirmar que

$$\forall_{m,n \in \mathbb{Z}} D_m^* \cap D_n^* \neq \emptyset.$$

É claro que se $m \neq 0 \neq n$ e $d \in D_m^* \cap D_n^*$, então $d \leq |m|$ e $d \leq |n|$, pelo que o $\max D_m^* \cap D_n^*$ existe. Este máximo designa-se por *máximo divisor comum* entre m e n e denota-se por $\text{mdc}(m, n)$. Note-se ainda que qualquer número inteiro não nulo divide 0, donde se $n \in \mathbb{Z} \setminus \{0\}$ então $\text{mdc}(0, n) = \text{mdc}(n, 0) = |n|$. Nestas condições, podemos afirmar que $d = \text{mdc}(m, n)$ se e só se

$$1. d | n, \quad 2. d | m, \quad 3. \forall_{c \in \mathbb{Z}} c | n \wedge c | m \Rightarrow c \leq d.$$

Um conceito dual de máximo divisor comum é o conceito de *mínimo múltiplo comum* entre dois números m e n que se denota por $\text{mmc}(m, n)$ que é o menor inteiro não negativo s para o qual existem dois inteiros p e q tais que $mp = nq = s$ (ou, de modo equivalente, se m e n são não nulos, $\text{mmc}(m, n)$ é o menor inteiro não negativo s tal que $m | s$ e $n | s$).

Os conceitos de máximo divisor comum e mínimo múltiplo comum têm a seguinte interpretação geométrica: se considerarmos um rectângulo R de lados m e n , então $\text{mdc}(m, n)$ corresponde ao comprimento do lado do quadrado de maior lado (com comprimento inteiro) com réplicas do qual se pode cobrir (sem sobreposições) a área do rectângulo R . Por outro lado, o comprimento do lado do quadrado de menor lado cuja área pode ser coberta (sem sobreposições) com réplicas de R corresponde ao $\text{mmc}(m, n)$.

Note-se que para quaisquer inteiros m e n não simultaneamente nulos verifica-se a igualdade

$$\text{mdc}(m, n) \text{mmc}(m, n) = |mn|.$$

Uma vez que $\text{mdc}(m, n) = \text{mdc}(|m|, |n|)$, na generalidade dos casos, sem perda de generalidade, podemos considerar m e n como sendo inteiros não negativos não simultaneamente nulos. Mais geralmente,

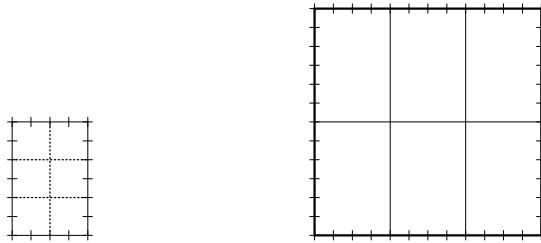


Figura 8.1: Interpretação geométrica de $\text{mdc}(4, 6)$ e $\text{lcm}(4, 6)$.

uma vez que se d é um divisor de n , então $|d|$ é também um divisor de n , no que se segue, apenas vamos considerar divisores positivos, os quais, por abuso de linguagem, designaremos simplesmente por divisores de n , cujo conjunto passaremos a denotar por D_n .

8.1. Algoritmo de Euclides

O mais popular dos métodos para determinação do máximo divisor comum entre dois inteiros m e n é o algoritmo de Euclides que se baseia no seguinte resultado:

$$m = nq + r \text{ com } q \in \mathbb{Z} \Rightarrow D_m \cap D_n = D_n \cap D_r.$$

Com efeito, se $d \in D_m \cap D_n$ então $d|(m - nq) \Leftrightarrow d|r$ e, consequentemente, $d \in D_n \cap D_r$. Reciprocamente, se $d \in D_n \cap D_r$ então $d|(nq + r) \Leftrightarrow d|m$, pelo que $d \in D_m \cap D_n$. Logo, podemos concluir que $\text{mdc}(m, n) = \text{mdc}(n, r)$. Nestas condições, o algoritmo de Euclides para a determinação de máximo divisor comum entre dois números m e n (não simultaneamente nulos) pode formalizar-se conforme a seguir se indica

Algoritmo 8.1: MDC(m, n)

```

 $m \leftarrow |m|$ 
 $n \leftarrow |n|$ 
se  $m < n$  então  $m \leftrightarrow n$ 
enquanto  $n \neq 0$ 
    fazer
        
$$\begin{cases} q \leftarrow \lfloor \frac{m}{n} \rfloor \\ r \leftarrow m - nq \\ m \leftarrow n \\ n \leftarrow r \end{cases}$$

    devolver  $(m)$ 
```

Exemplo 8.1. Utilizando o algoritmo de Euclides, vamos determinar o máximo divisor comum entre 546 e 222.

Solução. A Tabela 8.1 ilustra a aplicação do algoritmo de Euclides. Observe-se que as diferentes iterações do algoritmo correspondem, sucessivamente, às igualdades:

$$\text{mdc}(546, 222) = \text{mdc}(222, 102) = \text{mdc}(102, 18) = \text{mdc}(18, 12) = \text{mdc}(12, 6) = \text{mdc}(6, 0) = 6.$$

□

Como consequência imediata do algoritmo de Euclides, pode concluir-se o resultado que se segue.

passo	q	r	m	n
			546	222
1	2	102	222	102
2	2	18	102	18
3	5	12	18	12
4	1	6	12	6
5	2	0	6	0

Tabela 8.1: Determinação de $\text{mdc}(546, 222)$.

Teorema 8.1. Sejam m e n dois inteiros positivos e seja $d = \text{mdc}(m, n)$. Então existem dois inteiros x e y tais que

$$d = mx + ny.$$

Demonstração. Supondo que, por aplicação do algoritmo de Euclides, se obtém a sequência de igualdades

$$\begin{aligned} r_0 = r_1 q_1 + r_2 &\Leftrightarrow r_2 = r_0 - r_1 q_1, \\ r_1 = r_2 q_2 + r_3 &\Leftrightarrow r_3 = r_1 - r_2 q_2 \\ &\Leftrightarrow r_3 = r_1 - (r_0 - r_1 q_1) q_2 \\ &\Leftrightarrow r_3 = r_1(1 + q_1 q_2) - r_0 q_2, \\ r_2 = r_3 q_3 + r_4 &\Leftrightarrow r_4 = r_2 - r_3 q_3 \\ &\Leftrightarrow r_4 = (r_0 - r_1 q_1) - (r_1(1 + q_1 q_2) - r_0 q_2) q_3 \\ &\Leftrightarrow r_4 = r_0(1 + q_2 q_3) - r_1(q_1 + q_3 + q_1 q_2 q_3), \end{aligned}$$

etc, até se determinar $d = r_k$, conclui-se a igualdade pretendida. \square

Exemplo 8.2. Vamos determinar dois inteiros x e y tais que $546x + 222y = 6$.

Solução. Procedendo como é sugerido na prova do Teorema 8.1, para o caso de $m = 546$ e $n = 222$, obtém-se $r_0 = 546$ e $r_1 = 222$ e a sequência de igualdades

$$\begin{aligned} r_0 = r_1 q_1 + r_2 &\Rightarrow q_1 = 2 \\ &\Rightarrow r_2 = 546 - 222 \cdot 2, \\ r_1 = r_2 q_2 + r_3 &\Rightarrow q_2 = 2 \Rightarrow r_3 = 222 - (546 - 222 \cdot 2) \cdot 2 \\ &\Rightarrow r_3 = 546 \cdot (-2) + 222 \cdot 5, \\ r_2 = r_3 q_3 + r_4 &\Rightarrow q_3 = 5 \Rightarrow r_4 = 546 - 222 \cdot 2 - (546 \cdot (-2) + 222 \cdot 5) \cdot 5, \\ &\Rightarrow r_4 = 546 \cdot 11 + 222 \cdot (-27), \\ r_3 = r_4 q_4 + r_5 &\Rightarrow q_4 = 1 \Rightarrow r_5 = 546 \cdot (-2) + 222 \cdot 5 - (546 \cdot 11 + 222 \cdot (-27)), \\ &\Rightarrow r_5 = 546 \cdot (-13) + 222 \cdot 32. \end{aligned}$$

Assim, uma vez que $r_5 = \text{mdc}(546, 222) = 6$, vem

$$6 = 546 \cdot (-13) + 222 \cdot 32. \quad \square$$

Um número natural diz-se *primo* se é maior do que 1 e apenas é divisível pela unidade e por ele próprio.

Exemplo 8.3. Supondo que p é um número primo e n_1, \dots, n_k são números naturais, vamos provar que se $p|(n_1 \cdots n_k)$, então $p|n_i$, para algum $i \in \{1, \dots, k\}$.

Solução. Vamos fazer a prova por indução sobre k , tendo em conta que o resultado é trivialmente verdadeiro para $k = 1$ e, para $k = 2$ a prova se pode fazer do seguinte modo:

Suponha que $p | (n_1 n_2)$ mas $p \nmid n_1$. Então $\text{mdc}(p, n_1) = 1$ e, consequentemente, existem inteiros x e y tais que $xp + yn_1 = 1$, donde $n_2 = n_2(xp + yn_1) = p(xn_2) + y(n_1 n_2)$. Logo, uma vez que $p | (n_1 n_2)$, podemos concluir que $p | n_2$.

Assim, por hipótese de indução, suponha que o resultado é verdadeiro para produtos de $k - 1$ factores, com $k \geq 3$, e que $p|((n_1 \cdots n_{k-1})n_k)$. Logo, tendo em conta a demonstração anterior, se $p \nmid n_k$, então $p|(n_1 \cdots n_{k-1})$ e, consequentemente, por hipótese de indução, $p | n_j$, para algum $j \in \{1, \dots, k-1\}$. \square

A partir do resultado demonstrado no Exemplo 8.3, estamos em condições de introduzir o *teorema fundamental da aritmética*, cuja prova fica como exercício.

Teorema 8.2 (fundamental da aritmética). *Dado um número natural $n > 1$, existem números primos p_1, \dots, p_r tais que*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \quad (8.1)$$

com $k_1, \dots, k_r \in \mathbb{N}$, e esta factorização é única (a menos da ordem dos factores).

8.2. Funções de Euler e de Möbius

Considerando a factorização (8.1) de $n \in \mathbb{N}$, podemos concluir que d divide n se e somente se d não tem divisores primos distintos dos de n e nenhum dos seus divisores o divide sucessivamente mais vezes do que a n , ou seja, se e somente se d admite a factorização

$$d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r},$$

onde, para $1 \leq i \leq r$, s_i é tal que $0 \leq s_i \leq k_i$.

Como exemplo, considerando $n = 90 = 2 \cdot 3^2 \cdot 5$, conclui-se que os seus divisores são 1, 2, 3, 5, $6 = 2 \cdot 3$, $9 = 3^2$, $10 = 2 \cdot 5$, $15 = 3 \cdot 5$, $18 = 2 \cdot 3^2$, $30 = 2 \cdot 3 \cdot 5$, $45 = 3^2 \cdot 5$ e $90 = 2 \cdot 3^2 \cdot 5$.

Dois números naturais distintos x e y dizem-se *primos entre si* ou *relativamente primos* (ou ainda *primos relativos* ou *coprimos*) se o seu máximo divisor comum é igual a 1 ($\text{mdc}(x, y) = 1$). Tendo em conta o Teorema 8.1, concluímos que dados dois números naturais m e n primos entre si, existem dois inteiros x e y tais que

$$mx + ny = 1.$$

Nesta altura estamos em condições de introduzir a *função de Euler*¹.

Definição 8.1 (Função de Euler). *A função φ tal que*

$$\begin{aligned} \varphi : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\rightsquigarrow \varphi(n) = |\{x \in [n] : \text{mdc}(x, n) = 1\}| \end{aligned}$$

designa-se por função de Euler. Por outras palavras, $\varphi(n)$ é igual ao número de primos relativos com n pertencentes a $[n]$.

Exemplo 8.4. Vamos calcular $\varphi(90)$.

¹ Leonhard Euler (1707–1783), nascido em Basileia (na Suiça), foi um dos maiores matemáticos de sempre.

Solução. De acordo com Definição 8.1, tendo em conta que $90 = 2 \cdot 3^2 \cdot 5$, considerando $M_{90}(2) = \{x \in [90] : 2|x\}$, $M_{90}(3) = \{x \in [90] : 3|x\}$ e $M_{90}(5) = \{x \in [90] : 5|x\}$ (ou seja, $M_{90}(d)$ denota o conjunto dos múltiplos de d em $[90]$), podemos concluir que

$$\varphi(90) = 90 - |M_{90}(2) \cup M_{90}(3) \cup M_{90}(5)|.$$

Por outro lado, aplicando o princípio de inclusão-exclusão,

$$\begin{aligned} |M_{90}(2) \cup M_{90}(3) \cup M_{90}(5)| &= |M_{90}(2)| + |M_{90}(3)| + |M_{90}(5)| \\ &\quad - |M_{90}(2) \cap M_{90}(3)| - |M_{90}(2) \cap M_{90}(5)| - |M_{90}(3) \cap M_{90}(5)| \\ &\quad + |M_{90}(2) \cap M_{90}(3) \cap M_{90}(5)| \\ &= 45 + 30 + 18 - 15 - 9 - 6 + 3 = 66. \end{aligned}$$

Logo, $\varphi(90) = 90 - 66 = 24$ (com efeito, os primos relativos com 90 pertencentes a $[90]$ são: 1, 7, 11, 13, 17, 19, 23, 29, 31, 27, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83 e 89). \square

Teorema 8.3. Para qualquer inteiro positivo n verifica-se a igualdade

$$\sum_{d|n} \varphi(d) = n. \quad (8.2)$$

Demonstração. Seja S o conjunto de pares de inteiros (c, d) tais que $d|n$, $1 \leq c \leq d$ e $\text{mdc}(c, d) = 1$. Nestas condições, conclui-se que $|S| = \sum_{d|n} \varphi(d)$. Resta provar que $|S| = n$ o que, por sua vez, é equivalente a provar que a função

$$\begin{array}{rccc} f: & S & \rightarrow & [n] \\ & (c, d) & \rightsquigarrow & \frac{cn}{d}. \end{array}$$

é uma bijecção (note-se que $d|n$ implica que $f(c, d)$ seja um número inteiro e $1 \leq c \leq d$ implica que $f(c, d) \in [n]$).

- *Prova da injectividade de f .* Suponha que $f(c, d) = f(c', d')$. Então $\frac{cn}{d} = \frac{c'n}{d'} \Leftrightarrow cd' = c'd$ e, consequentemente, $c|(c'd)$ e $c'|(cd')$. Porém,

$$\text{mdc}(c, d) = 1 \Rightarrow c|c' \text{ e } \text{mdc}(c', d') = 1 \Rightarrow c'|c.$$

Logo, podemos concluir que $c = c'$ e $d = d'$.

- *Prova da sobrejectividade de f .* Seja $x \in [n]$ e seja $k_x = \text{mdc}(x, n)$. Considere ainda $d_x = \frac{n}{k_x}$ e $c_x = \frac{x}{k_x}$. Uma vez que k_x é o máximo divisor comum entre x e n , vem que c_x e d_x são inteiros primos entre si. Segue-se que $f(c_x, d_x) = \frac{c_x n}{d_x} = x$, pelo que f é sobrejectiva. \square

Deste teorema decorre uma fórmula recursiva para a determinação da função de Euler. Com efeito, sabe-se que $\varphi(1) = 1$ e, da igualdade (8.2), obtém-se a fórmula recursiva

$$\varphi(n) = n - \sum_{d|n, d < n} \varphi(d).$$

Como exemplo de aplicação desta fórmula recursiva, vamos calcular $\varphi(12)$.

$$\begin{aligned} \varphi(12) &= 12 - \sum_{d|12, d < 12} \varphi(d) = 12 - \varphi(1) - \varphi(2) - \varphi(3) - \varphi(4) - \varphi(6) \\ &= 11 - \varphi(2) - \varphi(3) - \varphi(4) - \varphi(6). \end{aligned}$$

Logo, para calcular $\varphi(12)$, precisamos de $\varphi(2)$, $\varphi(3)$, $\varphi(4)$ e $\varphi(6)$. Porém,

$$\begin{aligned}\varphi(2) &= 2 - \sum_{d|2, d<2} \varphi(d) = 2 - \varphi(1) = 1, \\ \varphi(3) &= 3 - \sum_{d|3, d<3} \varphi(d) = 3 - \varphi(1) = 2, \\ \varphi(4) &= 4 - \sum_{d|4, d<4} \varphi(d) = 4 - \varphi(1) - \varphi(2) = 4 - 1 - 1 = 2, \\ \varphi(6) &= 6 - \sum_{d|6, d<6} \varphi(d) = 6 - \varphi(1) - \varphi(2) - \varphi(3) = 6 - 1 - 1 - 2 = 2.\end{aligned}$$

Como consequência,

$$\varphi(12) = 11 - \varphi(2) - \varphi(3) - \varphi(4) - \varphi(6) = 11 - 1 - 2 - 2 - 2 = 4.$$

O teorema a seguir estabelece uma fórmula de cálculo para $\varphi(n)$ em função dos primos que constam na factorização de n .

Teorema 8.4 (de Euler). *Se $n \geq 2$ é um inteiro cuja factorização em primos é $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, então*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Demonstração. Sendo $M_n(p_j) = \{x \in [n] : p_j|x\}$, para $j = 1, \dots, r$, podemos concluir que $\forall x \in [n]$ tal que $\text{mdc}(x, n) = 1$, $x \notin \bigcup_{j=1}^r M_n(p_j)$. Logo, pela fórmula de Daniel da Silva,

$$\begin{aligned}\varphi(n) &= n - \left| \bigcup_{j=1}^r M_n(p_j) \right| \\ &= n - \sum_{j=1}^r |M_n(p_j)| + \sum_{i < j} |M_n(p_i) \cap M_n(p_j)| \\ &\quad - \sum_{i < j < k} |M_n(p_i) \cap M_n(p_j) \cap M_n(p_k)| + \dots\end{aligned}$$

A intersecção $M_n(p_{j_1}) \cap M_n(p_{j_2}) \cap \dots \cap M_n(p_{j_q})$ tem como elementos os múltiplos de $P = p_{j_1} p_{j_2} \cdots p_{j_q}$ em $[n]$, que são, precisamente, os inteiros $P, 2P, \dots, \frac{n}{P}P$. Logo, a sua cardinalidade é

$$\frac{n}{P} = n \frac{1}{p_{j_1}} \frac{1}{p_{j_2}} \cdots \frac{1}{p_{j_q}}.$$

Segue-se então

$$\begin{aligned}\varphi(n) &= n - n \sum_{j=1}^r \frac{1}{p_j} + n \sum_{i < j} \frac{1}{p_i p_j} - n \sum_{i < j < k} \frac{1}{p_i p_j p_k} + \dots \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}\tag{8.3}$$

□

Como consequência imediata deste teorema, podemos concluir que se $n = y_1 \cdots y_k \in \mathbb{N}$, onde y_1, \dots, y_k são inteiros positivos primos entre si, então $\varphi(n) = \varphi(y_1) \cdots \varphi(y_k)$ (ver Exercício 8.12).

Aplicando o Teorema 8.4 à determinação dos primos relativos com 90, pertencentes a $[90]$, obtém-se, tal como anteriormente,

$$\varphi(90) = 90 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 90 \frac{1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5} = 24.$$

Observe-se que podemos reescrever (8.3) na forma

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}, \quad (8.4)$$

onde μ é precisamente a função de Möbius introduzida na secção 7.6, mas agora na sua versão clássica (caso particular do cpo $([n], |)$), para a qual se adopta a notação $\mu(d)$ em vez de $\mu(1, d)$. Assim, tendo em conta o Exemplo 7.36, podemos concluir a expressão

$$\mu(d) = \begin{cases} 1, & \text{se } d = 1, \\ (-1)^k, & \text{se } d \text{ é o produto de } k \text{ primos distintos,} \\ 0, & \text{se } d \text{ tem um factor primo repetido.} \end{cases}$$

Seguem-se alguns resultados obtidos no contexto particular da versão clássica da função de Möbius, mas que podem igualmente ser obtidos a partir dos resultados da secção 7.6.

Lema 8.5. *Dado um inteiro $n \geq 2$, verifica-se a igualdade*

$$\sum_{d|n} \mu(d) = 0.$$

Demonação. Supondo que n admite a factorização em primos $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, cada divisor tem a forma $d = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$ (com $0 \leq s_i \leq k_i$, para $i = 1, \dots, r$) e $\mu(d) = 0$, a menos que $s_i \in \{0, 1\} \forall i \in \{1, \dots, r\}$. Consequentemente, cada divisor d tal que $\mu(d) \neq 0$ corresponde ao subconjunto de elementos do conjunto $\{p_1, p_2, \dots, p_r\}$ cujo produto determina d . O número de tais subconjuntos de cardinalidade k é precisamente $\binom{r}{k}$ e, para os divisores d que lhes correspondem, obtém-se $\mu(d) = (-1)^k$. Nestas condições, vem

$$\sum_{d|n} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \dots + (-1)^r \binom{r}{r} = 0.$$

□

Com base neste resultado e sabendo que $\mu(1) = 1$, podemos calcular, recursivamente, a função de Möbius para qualquer inteiro positivo. Por exemplo, para calcular $\mu(12)$, uma vez que

$$\mu(12) = - \sum_{d|12, d<12} \mu(d) = -1 - \mu(2) - \mu(3) - \mu(4) - \mu(6),$$

basta conhecer $\mu(2)$, $\mu(3)$, $\mu(4)$ e $\mu(6)$. Porém,

$$\begin{aligned} \mu(2) &= - \sum_{d|2, d<2} \mu(d) = -\mu(1) = -1, \\ \mu(3) &= - \sum_{d|3, d<3} \mu(d) = -\mu(1) = -1, \\ \mu(4) &= - \sum_{d|4, d<4} \mu(d) = -\mu(1) - \mu(2) = -1 - (-1) = 0, \\ \mu(6) &= - \sum_{d|6, d<6} \mu(d) = -\mu(1) - \mu(2) - \mu(3) = -1 - (-1) - (-1) = 1. \end{aligned}$$

Como consequência,

$$\mu(12) = -\mu(1) - \mu(2) - \mu(3) - \mu(4) - \mu(6) = -1 - 0 - (-1) - (-1) - 1 = 0.$$

Segue-se uma das propriedades mais relevantes da versão clássica da função de Möbius que é conhecida por *fórmula da inversão de Möbius clássica*.

Teorema 8.6 (da inversão de Möbius clássica). *Considere-se uma função arbitrária $g : \mathbb{N} \mapsto \mathbb{N}$ e que a função f é obtida de g pela equação*

$$f(n) = \sum_{d|n} g(d). \quad (8.5)$$

Então a função g pode ser obtida a partir da função f pela equação

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right). \quad (8.6)$$

Demonstração. Tendo em conta a igualdade (8.5), vem

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{x|\frac{n}{d}} g(x) = \sum_{(x,d) \in X} \mu(d) g(x),$$

onde X denota o conjunto de todos os pares (x, d) tais que $d|n$ e $x|\frac{n}{d}$, o qual coincide com o conjunto de pares (x, d) tais que $x|n$ e $d|\frac{n}{x}$ (com efeito, $x|\frac{n}{d}$ significa que $\exists k \in \mathbb{N}$ tal que $\frac{n}{d} = kx \Leftrightarrow \frac{n}{x} = kd$ que, por sua vez, significa que $d|\frac{n}{x}$). Como consequência, rearranjando o somatório, obtém-se

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{x|n} g(x) \sum_{d|x} \mu(d).$$

Porém, de acordo com o Lema 8.5, sabe-se que $\sum_{d|\frac{n}{x}} \mu(d) = 0$, quando $\frac{n}{x} \geq 2$. Logo, resta apenas o termo que se obtém para $n = x$, donde decorre

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = g(n) \sum_{d|1} \mu(d) = g(n) \mu(1) = g(n).$$

□

Esta demonstração pode fazer-se recorrendo à versão mais geral da função de Möbius introduzida na Secção 7.6, considerando o cpo $([n], |)$ e tendo em conta que, de acordo com o Teorema 7.29, $g(n) = \sum_{d|n} f(d) \mu(d, n) \Leftrightarrow g(n) = \sum_{d|n} f(d) \mu(1, \frac{n}{d}) \Leftrightarrow g(n) = \sum_{d|n} f(\frac{n}{d}) \mu(1, d)$ e $\mu(1, d) = \mu(d)$. Como não podia deixar de ser, tendo em conta o Teorema 7.29, é claro que o recíproco do teorema da inversão de Möbius clássica é também verdadeiro, ou seja, se g é obtida de f pela equação $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$, então a f pode obter-se de g pela equação $f(n) = \sum_{d|n} g(d)$ (ver Exercício 8.13).

8.3. Relações de congruência

Dados dois inteiros x e y e um inteiro positivo m , diz-se que x é congruente com y módulo m e escreve-se $x \equiv y \pmod{m}$, se $m|(x - y)$. É fácil concluir que a relação de congruência módulo m é uma relação de equivalência, ou seja, é

- reflexiva (dado que $m|(x - x)$),
- simétrica (dado que se $m|(x - y)$ então $m|(y - x)$),

- transitiva (uma vez que se $m|(x - y) \Leftrightarrow \exists k_1 \in \mathbb{Z}$ tal que $x - y = k_1 m$ e $m|(y - z) \Leftrightarrow \exists k_2 \in \mathbb{Z}$ tal que $y - z = k_2 m$, então $x - z = x - y + y - z = (k_1 + k_2)m \Leftrightarrow m|(x - z)$).

Verifica-se também que se $x_1 \equiv x_2 \pmod{m}$ e $y_1 \equiv y_2 \pmod{m}$ (pelo que $x_1 - x_2 = mx$ e $y_1 - y_2 = my$, com x e y em \mathbb{Z}), então $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$ (uma vez que $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = mx + my = m(x + y)$) e $x_1 y_1 \equiv x_2 y_2 \pmod{m}$ (dado que $x_1 y_1 - x_2 y_2 = (x_1 - x_2)y_1 + x_2(y_1 - y_2) = m(xy_1 + x_2y)$).

O conjunto dos inteiros módulo m , que usualmente se denota por \mathbb{Z}_m , é o conjunto de todas as classes de equivalência módulo m pertencentes a \mathbb{Z} . No que se segue, vamos denotar as operações de adição e multiplicação em \mathbb{Z}_m , respectivamente, por \oplus e \odot . Por sua vez, dado um inteiro z , a correspondente classe de equivalência em \mathbb{Z}_m será denotada por $[z]$ (algumas vezes, porém, para simplificar a linguagem, denotaremos $[z]$, simplesmente, por z). Assim, considerando as classes de equivalência $[x]$ e $[y]$ de \mathbb{Z}_m , vem

$$[x] \oplus [y] = [x + y] \text{ e } [x] \odot [y] = [xy].$$

É fácil concluir que as operações de adição \oplus e multiplicação \odot em \mathbb{Z}_m satisfazem as seguinte propriedades: $\forall x, y, z \in \mathbb{Z}_m$

1. $x \oplus y \in \mathbb{Z}_m$ (\oplus é fechada em \mathbb{Z}_m);
2. $x \oplus y = y \oplus x$ (comutatividade);
3. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ (associatividade);
4. $\exists 0 \in \mathbb{Z}_m \ x \oplus 0 = x$ (existência de elemento nulo);
5. $\exists!(-z) \in \mathbb{Z}_m \ z \oplus (-z) = 0$ (existência de inverso);
6. $x \odot y \in \mathbb{Z}_m$ (\odot é fechada em \mathbb{Z}_m);
7. $x \odot y = y \odot x$ (comutatividade);
8. $x \odot (y \odot z) = (x \odot y) \odot z$ (associatividade);
9. $\exists 1 \in \mathbb{Z}_m \ 1 \odot x = x$ (existência de elemento unidade);
10. $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ (distributividade).

As propriedades 1-5 definem uma estrutura de grupo comutativo que se denota por (\mathbb{Z}_m, \oplus) . As propriedades 6-9 definem uma estrutura de monoide comutativo que se denota por (\mathbb{Z}_m, \odot) . Por sua vez, no seu conjunto, as propriedades 1-10 definem uma estrutura de *anel comutativo*, associativo e com elemento unidade, que se pode denotar por $(\mathbb{Z}_m, \oplus, \odot)$.

Exemplo 8.5. Vamos determinar as tabelas das operações \oplus e \odot do anel $(\mathbb{Z}_5, \oplus, \odot)$.

Solução. Ver Tabela 8.2. □

Definição 8.2 (Elemento invertível). Um elemento $z \in \mathbb{Z}_m$ diz-se invertível se existe $x \in \mathbb{Z}_m$ tal que $z \odot x = 1$. Nestas condições, x designa-se por inverso de z e denota-se por z^{-1} (uma vez que $z \odot x = x \odot z = 1$, conclui-se também que $z = x^{-1}$).

Definição 8.3 (Corpo). Seja $\mathcal{F} = (F, +, \cdot, 0, 1)$ um anel comutativo com operações binárias de adição "+" e multiplicação ".", com elemento nulo "0" e unidade "1" (satisfazendo as propriedades 1-10). Se $F^* = F \setminus \{0\}$ é um grupo abeliano relativamente à operação multiplicativa, então $(F, +, \cdot, 0, 1)$ diz-se um corpo. Se F é finito, então $(F, +, \cdot, 0, 1)$ diz-se um corpo finito.

\oplus	[0]	[1]	[2]	[3]	[4]	\odot	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[0]	[1]	[0]	[1]	[2]	[3]	[4]
[2]	[2]	[3]	[4]	[0]	[1]	[2]	[0]	[2]	[4]	[1]	[3]
[3]	[3]	[4]	[0]	[1]	[2]	[3]	[0]	[3]	[1]	[4]	[2]
[4]	[4]	[0]	[1]	[2]	[3]	[4]	[0]	[4]	[3]	[2]	[1]

Tabela 8.2: Tabelas das operações do anel $(\mathbb{Z}_5, \oplus, \odot)$

Um subconjunto S de um corpo $(F, +, \cdot, 0, 1)$ designa-se por *subcorpo* de F se $(S, +, \cdot, 0, 1)$, com as operações e os elementos 0 e 1 de F , forma um corpo. Neste caso diz-se que o corpo F é uma *extensão do corpo* S .

Exemplo 8.6. Vamos mostrar que se p é um número primo, então $(\mathbb{Z}_p, \oplus, \odot, 0, 1)$ é um corpo.

Solução. Com efeito, se p é um número primo, então \mathbb{Z}_p é um corpo relativamente às operações \oplus e \odot , ou seja, (\mathbb{Z}_p, \oplus) e $(\mathbb{Z}_p \setminus \{0\}, \odot)$ têm ambos estrutura de grupo comutativo e verifica-se a distributividade da operação \odot relativamente à operação \oplus . \square

Note-se que, em particular, de acordo de Tabela 8.2, $\mathbb{Z}_5^* = (\mathbb{Z}_5 \setminus \{[0]\}, \odot)$ é um grupo multiplicativo formado por todos os elementos invertíveis de \mathbb{Z}_5 .

Teorema 8.7. Um elemento $z \in \mathbb{Z}_m$ é invertível se e somente se $\text{mdc}(z, m) = 1$. Em particular, se p é um número primo, então todo o elemento de $\mathbb{Z}_p \setminus \{0\}$ é invertível.

Demonstração.

- (\Rightarrow) Suponha que $z \in \mathbb{Z}_m$ é invertível. Então $\exists x \in \mathbb{Z}_m$ tal que $z \odot x = 1$. Consequentemente, conclui-se que $\exists k$ tal que $zx - 1 = km \Leftrightarrow zx - km = 1$. Logo, qualquer divisor comum a z e m divide $zx - km$, pelo que também divide 1, o que implica que $\text{mdc}(z, m) = 1$.
- (\Leftarrow) Reciprocamente, suponha que $\text{mdc}(z, m) = 1$. Então existem inteiros x e y , tais que $zx + my = 1 \Leftrightarrow zx - 1 = m(-y)$, donde se conclui que $z \odot x = 1$. \square

Na sequência do Teorema 8.7, uma vez que o valor da função de Euler, $\varphi(m)$, é precisamente o número de números primos com m em $\{1, \dots, m\}$, podemos concluir que \mathbb{Z}_m tem $\varphi(m)$ elementos invertíveis.

Teorema 8.8. Seja I_m o conjunto dos elementos invertíveis de \mathbb{Z}_m . Se $y \in I_m$ então $y \odot I_m = \{y \odot x : x \in I_m\} = I_m$.

Demonstração.

1. Supondo que $z \in y \odot I_m$, donde $z = y \odot x$, com $y, x \in I_m$, então

$$z \odot (x^{-1} \odot y^{-1}) = (y \odot x) \odot (x^{-1} \odot y^{-1}) = y \odot (x \odot (x^{-1} \odot y^{-1})) = y \odot ((x \odot x^{-1}) \odot y^{-1}) = y \odot y^{-1} = 1.$$

Logo $z \in I_m$ e, consequentemente, $y \odot I_m \subseteq I_m$.

2. Supondo agora que $x \in I_m$, podemos escrever $x = (y \odot y^{-1}) \odot x = y \odot (y^{-1} \odot x) = y \odot z$, com $z \in y^{-1} \odot I_m$, pelo que, de acordo com a prova anterior, $z \in I_m$. Logo $x \in y \odot I_m$ e, consequentemente, $I_m \subseteq y \odot I_m$. \square

Teorema 8.9. Se y é invertível em \mathbb{Z}_m , então $y^{\varphi(m)} = 1$ em \mathbb{Z}_m .

Demonstração. Seja z o produto de todos os números de $I_m = \{x_1, \dots, x_k\}$, pelo que $z = x_1 \odot \cdots \odot x_k$ onde, de acordo com o Teorema 8.7, $k = \varphi(m)$. Uma vez que $y \odot I_m = I_m$, a sequência $y \odot x_1, \dots, y \odot x_k$ é, simplesmente, uma permutação dos elementos de I_m . Logo, $z = x_1 \odot \cdots \odot x_k = (y \odot x_1) \cdots (y \odot x_k) = y^k \odot z$. Porém, z é ele próprio invertível (com inverso $z^{-1} = x_k^{-1} \odot \cdots \odot x_1^{-1}$) donde, multiplicando a igualdade anterior por z^{-1} , vem $1 = y^k$. \square

Substituindo \mathbb{Z}_m por \mathbb{Z} , o teorema anterior corresponde ao teorema de Euler que a seguir se indica.

Teorema 8.10 (de Euler). *Se $\text{mdc}(y, m) = 1$ então $y^{\varphi(m)} \equiv 1 \pmod{m}$.*

Para o caso particular de $m = p$, onde p é um número primo, obtém-se o *pequeno teorema de Fermat*.

Teorema 8.11 (de Fermat). *Se p é primo e não divide y então $y^{p-1} \equiv 1 \pmod{p}$.*

Porém, tanto o teorema de Euler como o pequeno teorema de Fermat, são consequência directa do Teorema 8.9. Com efeito, se $\text{mdc}(y, m) = 1$ (p é primo e não divide y) então y é invertível em \mathbb{Z}_m (\mathbb{Z}_p) e, de acordo com o Teorema 8.9, $y^{\varphi(m)} = 1$ ($y^{p-1} = 1$) em \mathbb{Z}_m (\mathbb{Z}_p).

Em 1854, Daniel da Silva obteve a seguinte generalização do teorema de Euler [74]:

Teorema 8.12 (de Daniel da Silva). *Se $n \in \mathbb{N}$ é tal que $n = y_1 y_2 \cdots y_k$, onde y_1, y_2, \dots, y_k são primos entre si, então*

$$\sum_{j=1}^k y_j^{\frac{\varphi(n)}{\varphi(y_j)}} \equiv k - 1 \pmod{n}. \quad (8.7)$$

Demonstração. De acordo com o teorema de Euler, sabe-se que $y_j^{\varphi(y_i)} \equiv 1 \pmod{y_i}$, para $j \neq i$. Assim, podemos concluir que

$$y_j^{\varphi(y_1) \cdots \varphi(y_{j-1}) \varphi(y_{j+1}) \cdots \varphi(y_k)} = y_j^{\frac{\varphi(n)}{\varphi(y_j)}} \equiv 1 \pmod{y_i},$$

para $j \neq i$ e $y_i^{\frac{\varphi(n)}{\varphi(y_i)}} \equiv 0 \pmod{y_i}$. Adicionando estas congruências, para $j = 1, \dots, k$, vem

$$\sum_{j=1}^k y_j^{\frac{\varphi(n)}{\varphi(y_j)}} \equiv k - 1 \pmod{y_i} \Leftrightarrow y_i \left| \left(\sum_{j=1}^k y_j^{\frac{\varphi(n)}{\varphi(y_j)}} - (k - 1) \right) \right.,$$

para $i = 1, \dots, k$. Logo, tendo em conta que y_1, \dots, y_k são primos entre si,

$$\sum_{j=1}^k y_j^{\frac{\varphi(n)}{\varphi(y_j)}} - (k - 1) = x_1 y_1 = x_2 y_2 y_1 = \dots = x_k y_k \cdots y_1,$$

onde $x_1, \dots, x_k \in \mathbb{N}$ e, consequentemente,

$$n \left| \left(\sum_{j=1}^k y_j^{\frac{\varphi(n)}{\varphi(y_j)}} - (k - 1) \right) \right.. \quad \square$$

Note-se que o Teorema 8.12 implica o Teorema 8.10. Com efeito, sendo y e m dois números naturais relativamente primos, fazendo $n = ym$ (isto é, $k = 2$, $y_1 = y$ e $y_2 = m$) na congruência (8.7), vem

$$\begin{aligned} y^{\frac{\varphi(n)}{\varphi(y)}} + m^{\frac{\varphi(n)}{\varphi(m)}} &\equiv 2 - 1 \pmod{n} \\ &\Updownarrow \\ y^{\varphi(m)} + m^{\varphi(y)} &\equiv 1 \pmod{ym} \end{aligned}$$

Nestas condições, $(ym)|(y^{\varphi(m)} + m^{\varphi(y)} - 1) \Rightarrow m|(y^{\varphi(m)} - 1)$ (uma vez que $m|m^{\varphi(y)}$) e, consequentemente, $y^{\varphi(m)} \equiv 1 \pmod{m}$.

8.4. Equações e polinómios em corpos finitos

Podemos resolver equações e sistemas de equações em corpos finitos, recorrendo às regras usualmente utilizadas na resolução de equações e sistemas de equações em \mathbb{R} ou \mathbb{C} . Vamos considerar alguns exemplos, onde $x = y$ em \mathbb{Z}_p significa $x \equiv y \pmod{p}$ em \mathbb{Z} .

Exemplo 8.7. Vamos resolver a equação linear, a seguir indicada, em \mathbb{Z}_{53}

$$5 \odot x \oplus 7 = 0. \quad (8.8)$$

Solução. Uma vez que o corpo \mathbb{Z}_{53} é finito, podemos analisar cada um dos seus 53 elementos e determinar os que satisfazem a equação (8.8). Alternativamente, a resolução desta equação pode fazer-se, directamente, recorrendo às técnicas clássicas de resolução de equações. Vamos começar por reescrever a equação (8.8) na forma

$$5x + 7 \equiv 0 \pmod{53}$$

que, por sua vez, é equivalente a $5x \equiv -7 \pmod{53}$. Como consequência, dado que $-7 \equiv 46 \pmod{53}$, obtém-se

$$5x \equiv 46 \pmod{53}. \quad (8.9)$$

Tendo em conta que $5 \cdot 32 \equiv 1 \pmod{53}$, podemos concluir que $5^{-1} = 32$ em \mathbb{Z}_{53} . Logo, multiplicando ambos membros de (8.9) por 32, obtém-se $x \equiv 32 \cdot 46 \pmod{53}$, ou seja, $x = 41$ em \mathbb{Z}_{53} . \square

Exemplo 8.8. Vamos resolver o sistema de equações, a seguir indicado, em \mathbb{Z}_{11} .

$$\begin{cases} 2 \odot x \oplus 4 \odot y \oplus 9 = 0 \\ 4 \odot x \oplus 2 \odot y \oplus 1 = 0 \end{cases} \quad (8.10)$$

Solução. Uma vez que o corpo \mathbb{Z}_{11} é finito, um modo de resolver este sistema seria testar cada um dos $11^2 = 121$ pares de valores (x, y) e verificar qual ou quais os que satisfazem (8.10). Alternativamente, porém, podemos resolver, directamente, este sistema recorrendo às técnicas usuais. Vamos começar por reescrever o sistema (8.10) na forma

$$\begin{cases} 2x + 4y + 9 \equiv 0 \pmod{11} \\ 4x + 2y + 1 \equiv 0 \pmod{11} \end{cases} \quad (8.11)$$

Uma vez que $2 \cdot 6 \equiv 1 \pmod{11}$, vem que $2^{-1} = 6$ em \mathbb{Z}_{11} . Logo, multiplicando ambos membros da primeira relação de congruência do sistema (8.11) por 6, obtém-se

$$\begin{cases} x \equiv -4 \cdot 6y - 9 \cdot 6 \pmod{11} \\ 4x + 2y + 1 \equiv 0 \pmod{11} \end{cases}$$

Adicionalmente, dado que $-4 \cdot 6 \equiv 9 \pmod{11}$ e $-9 \cdot 6 \equiv 1 \pmod{11}$, este última sistema é equivalente ao sistema

$$\begin{cases} x \equiv 9y + 1 \pmod{11} \\ 4x + 2y + 1 \equiv 0 \pmod{11}. \end{cases}$$

Por sua vez, procedendo à substituição de x na segunda relação de congruência, vem

$$4(9y + 1) + 2y + 1 \equiv 0 \pmod{11},$$

ou seja,

$$5y + 5 \equiv 0 \pmod{11} \Leftrightarrow 5y \equiv 6 \pmod{11},$$

uma vez que $38 \equiv 5 \pmod{11}$ e $-5 \equiv 6 \pmod{11}$. Finalmente, dado que $5^{-1} = 9$ em \mathbb{Z}_{11} , obtém-se $y \equiv 9 \cdot 6 \pmod{11}$, ou seja, $y = 10$ em \mathbb{Z}_{11} e, consequentemente, $x \equiv 9 \cdot 10 + 1 \pmod{11}$, isto é, $x = 3$ em \mathbb{Z}_{11} . \square

Definição 8.4 (Polinómio sobre um anel $\mathbb{K}[x]$ e raiz de um polinómio). *Designa-se por polinómio de grau n e coeficientes $a_0, \dots, a_n \in \mathbb{K}$ (onde \mathbb{K} é um anel ou um corpo), toda a função $f : \mathbb{F} \rightarrow \mathbb{F}$, onde \mathbb{F} é uma estrutura algébrica que contém \mathbb{K} , definida pela expressão*

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n, \quad (8.12)$$

com $a_0 \neq 0$ (com exceção do polinómio nulo que é um polinómio de grau zero identicamente nulo), dizendo-se neste caso que $f \in \mathbb{K}[x]$ tem grau n e escreve-se $\text{grau } f = n$. Por sua vez, um elemento $r \in \mathbb{F}$ tal que $f(r) = 0$ designa-se por raiz do polinómio f .

No caso particular de um polinómio com coeficientes inteiros, racionais, reais ou complexos, diz-se que ele pertence a $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ ou $\mathbb{C}[x]$, respectivamente.

Deve observar-se que o conjunto dos polinómios $\mathbb{K}[x]$ (onde \mathbb{K} é um anel ou um corpo munido das operações usuais de adição e multiplicação de polinómios tem uma estrutura de anel comutativo, associativo e com elemento unidade. Adicionalmente, se $f, g \in \mathbb{K}[x]$ então

$$\begin{aligned} \text{grau}(f \cdot g) &= \text{grau } f + \text{grau } g, \\ \text{grau}(f + g) &\leq \max\{\text{grau } f, \text{grau } g\}. \end{aligned}$$

Teorema 8.13. *Se um polinómio de grau n com coeficientes inteiros (8.12) tem uma raiz racional na forma reduzida $\frac{p}{q}$ (ou seja, $p, q \in \mathbb{Z}$ e $\text{mdc}(p, q) = 1$), então $p|a_n$ e $q|a_0$.*

Demonstração. Com efeito, basta considerar a igualdade $0 = q^n f(\frac{p}{q})$, na forma

$$0 = a_0p^n + a_1p^{n-1}q + \dots + a_{n-1}pq^{n-1} + a_nq^n, \quad (8.13)$$

para se concluir que p divide as n primeiras parcelas do lado direito de (8.13) (e, consequentemente, também divide a última) e que q divide as n últimas parcelas de (8.13) (e, consequentemente, divide também a primeira). Porém, uma vez que $\text{mdc}(p, q) = 1$, $p|(a_nq^n) \Rightarrow p|a_n$ e $q|(a_0p^n) \Rightarrow q|a_0$. \square

Como consequência imediata deste teorema, se $f \in \mathbb{Z}[x]$ é um polinómio mónico (ou seja, $a_0 = 1$) e tem uma raiz racional, então essa raiz é inteira.

Segue-se um exemplo de aplicação desta propriedade de divisibilidade do numerador e do denominador de uma raiz racional na forma reduzida de um polinómio com coeficientes inteiros.

Exemplo 8.9. *Vamos determinar as raízes racionais do polinómio*

$$f(x) = 4x^5 - 4x^4 - 9x^3 + 11x^2 + x - 3.$$

Solução. Se $\frac{p}{q}$, com $p, q \in \mathbb{Z}$ e $\text{mdc}(p, q) = 1$, é uma raiz de f , aplicando o Teorema 8.13, podemos concluir que $p \in \{\pm 1, \pm 3\}$ e $q \in \{\pm 1, \pm 2, \pm 4\}$. Logo,

$$\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm 3, \pm \frac{3}{2} \text{ e } \pm \frac{3}{4}$$

são os únicos números racionais candidatos a raízes do polinómio f . Por verificação exaustiva, com facilidade se conclui que apenas $-\frac{3}{2}$, $-\frac{1}{2}$ e 1 são raízes racionais de f (na verdade, são as únicas raízes distintas de f). \square

Definição 8.5 (Corpo de decomposição de um polinómio). *Designa-se por corpo de decomposição de um polinómio $f \in \mathbb{K}[x]$, uma extensão \mathbb{L} de \mathbb{K} tal que*

- (1) $f(x)$ se decompõe em \mathbb{L} num produto de polinómios de grau 1 (i.e., factores lineares)
- (2) e \mathbb{L} é gerado sobre \mathbb{K} pelas raízes do polinómio f .

O corpo de decomposição de um polinómio f também se designa por *extensão de separação* de f .

Exemplo 8.10. Vamos determinar os corpos de decomposição dos seguintes polinómios:

1. $f(x) = x^2 - 2 \in \mathbb{Q}[x]$,

2. $g(x) = x^2 + 1 \in \mathbb{R}[x]$.

Solução.

1. Uma vez que as raízes do polinómio $f(x)$ são $\pm\sqrt{2}$, então o corpo de decomposição de f é o corpo $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
2. O polinómio $g(x)$ tem raízes $\pm i$, onde $i^2 = -1$. Como consequência, o corpo de decomposição de $g(x)$ é o corpo \mathbb{C} dos números complexos. \square

Dado que $(\mathbb{K}[x], +, \cdot)$ é um anel com elemento unidade que tem todos as propriedades de \mathbb{Z} , podemos concluir que dados dois polinómios $f, g \in \mathbb{K}[x]$, com $g \neq 0$, existem polinómios q e r , tais que $f(x) = g(x)q(x) + r(x)$, para cada $x \in \mathbb{K}$, com $\text{grau } r < \text{grau } g$. A determinação dos polinómios q e r designa-se usualmente por *divisão com resto* de f por g . Se $r = 0$, então diz-se que g divide f .

Sejam $f, g, r \in \mathbb{K}[x]$ e $f(x) = (x - \alpha)g(x) + r(x)$, com $\alpha \in \mathbb{K}$. Se $x = \alpha$, então $f(\alpha) = r(\alpha)$ e, consequentemente, podemos concluir que o polinómio mónico $x - \alpha$ divide $f(x)$ se e só se α é uma raiz de $f(x)$.

Existe um algoritmo simples para a divisão com resto de um polinómio arbitrário f , onde

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n,$$

por um polinómio linear $x - \alpha$, designado por *método de Horner*² que consiste no seguinte:

1. Seja $\sum_{i=0}^n a_i x^{n-i} = (x - \alpha)(b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-2}x + b_{n-1}) + r$.
2. Comparando os coeficientes associados às mesmas potências de x , obtém-se a sequência de igualdades:

$$\begin{aligned} a_0 &= b_0 & \Leftrightarrow b_0 &= a_0, \\ a_1 &= b_1 - \alpha b_0 & \Leftrightarrow b_1 &= a_1 + \alpha b_0, \\ a_2 &= b_2 - \alpha b_1 & \Leftrightarrow b_2 &= a_2 + \alpha b_1, \\ &\vdots && \vdots && \vdots \\ a_{n-1} &= b_{n-1} - \alpha b_{n-2} & \Leftrightarrow b_{n-1} &= a_{n-1} + \alpha b_{n-2}, \\ a_n &= r - \alpha b_{n-1} & \Leftrightarrow r &= a_n + \alpha b_{n-1}. \end{aligned}$$

Observe-se que $r = f(\alpha)$ e, como consequência, o esquema de Horner pode ser também utilizado para determinar o valor de um polinómio em α .

3. A partir destas fórmulas, podemos considerar a tabela a seguir indicada, onde os coeficientes da segunda linha são sucessivamente determinados da esquerda para a direita.

	a_0	a_1	a_2	\dots	a_{n-1}	a_n	
α	b_0	b_1	b_2	\dots	b_{n-1}	r	

(8.14)

Formalmente, o esquema de Horner pode representar-se pelo algoritmo que se segue.

²William George Horner (1786-1837) foi um mestre-escola inglês, cujo nome aparece ligado ao método que publicou em 1819. Porém, as bases deste método constam nos livros do matemático chinês Chu Shü-Kié que datam de 1299 e 1303.

Algoritmo 8.2: HORNER(A, n, α)

```

 $B[0] \leftarrow A[0]$ 
para  $i \leftarrow 1$  até  $n - 1$ 
  fazer  $B[i] \leftarrow A[i] + \alpha B[i - 1]$ 
 $r \leftarrow A[n] + \alpha B[n - 1]$ 
devolver  $(B, r)$ 
```

Exemplo 8.11. Por aplicação do esquema de Horner, vamos proceder à divisão com resto do polinómio $f(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$ por $x + 3$.

Solução. Procedendo à determinação da tabela (8.14), obtém-se

	1	2	3	4	5	6	7	
-3	1	-1	6	-14	47	-135	412	

Como consequência,

$$f(x) = (x^5 - x^4 + 6x^3 - 14x^2 + 47x - 135)(x + 3) + 412$$

e $f(-3) = 412$. □

Definição 8.6 (Polinómios redutíveis e irreduutíveis).

Um polinómio $f \in \mathbb{K}[x]$, com grau $f \geq 2$, diz-se redutível se existem dois polinómios $g, h \in \mathbb{K}[x]$, com graus superiores a 0, tais que $f(x) = g(x)h(x)$, para cada $x \in \mathbb{K}$. Caso contrário, o polinómio f diz-se irreduutível ou primo.

Se $f \in \mathbb{Z}_p[x]$ e grau $f \in \{2, 3\}$, então f é redutível se e só se $f(x)$ tem uma raiz em \mathbb{Z}_p .

Exemplo 8.12. Vamos demonstrar que o polinómio $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ é irreduutível (em \mathbb{Z}_2).

Solução. Dado que $f(0) = f(1) = 1 \neq 0$ em \mathbb{Z}_2 , então $f(x)$ é irreduutível em \mathbb{Z}_2 . □

Uma vez que $f(x) = x^2 + x + 1 = (x + 2)^2$ em $\mathbb{Z}_3[x]$, este polinómio é redutível em \mathbb{Z}_3 .

Definição 8.7 (Domínio de integridade e domínio euclidiano). Um anel comutativo, associativo e com elemento unidade $(A, \cdot, +)$ sem divisores de zero³ (ou seja, $ab = 0 \Rightarrow a = 0 \vee b = 0$) designa-se por domínio de integridade. Por sua vez, um domínio de integridade $(A, \cdot, +)$ é um domínio euclidiano se existe uma função $\theta : A \setminus \{0\} \rightarrow \mathbb{N}_0$ tal que $\forall a, b \in A \setminus \{0\}$

1. $\theta(a \cdot b) \geq \theta(a)$;
2. $\exists q, r \in A$, $a = bq + r$, com $r = 0$ ou $\theta(r) < \theta(b)$.

Os anéis \mathbb{Z} , \mathbb{Z}_p e $F[x]$, onde p é primo e F é um corpo, são exemplos de domínios de integridade. Porém, de entre estes, apenas \mathbb{Z} e $F[x]$ são domínios euclidianos. Em \mathbb{Z} a função θ é substituída pela função valor absoluto e em $F[x]$, $\theta(h) = \text{grau } h$, para cada $h \in F[x]$.

Como $F[x]$ é um domínio euclidiano, dados dois polinómios $f, g \in F[x]$, podemos considerar o divisor comum a f e g de maior grau. Vamos designar este divisor por *máximo divisor comum dos polinómios* f e g e denota-lo por $\text{mdc}(f, g)$. Por sua vez, vamos designar por *mínimo múltiplo comum* dos polinómios f e g e denotar por $\text{mmc}(f, g)$, o polinómio de menor grau que é divisível por f e por g . Diz-se que os polinómios f e g são *relativamente primos* ou *primos entre si* (ou *primos relativos*) quando $\text{mdc}(f, g) = 1$.

³Note-se que os anéis sem divisores de zero admitem o cancelamento (i.e., $ac = bc \wedge c \neq 0 \Rightarrow a = b$, uma vez que $ac = bc \Leftrightarrow (a - b)c = 0$).

Dado um polinómio $f \in F[x]$ tal que $f \neq 0$, define-se a relação de congruência módulo f , como sendo a relação binária \equiv tal que $g \equiv r \pmod{f}$ se e só se existe um polinómio $q \in F[x]$ tal que $g(x) - r(x) = q(x)f(x)$, para cada $x \in F$.

Exemplo 8.13. Vamos determinar as classes de congruência módulo $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Solução. Uma vez que na divisão com resto de um polinómio arbitrário $h \in \mathbb{Z}_2[x]$ por f , o resto $r(x)$ é um polinómio de grau inferior a 2, então $r(x)$ é igual a 0, 1, x ou $x + 1$. Logo,

$$\begin{aligned} [0] &= [x^2 + x + 1] = \{(x^2 + x + 1)h(x) : h(x) \in \mathbb{Z}_2[x]\}, \\ [1] &= \{(x^2 + x + 1)h(x) + 1 : h(x) \in \mathbb{Z}_2[x]\}, \\ [x] &= \{(x^2 + x + 1)h(x) + x : h(x) \in \mathbb{Z}_2[x]\}, \\ [x+1] &= \{(x^2 + x + 1)h(x) + x + 1 : h(x) \in \mathbb{Z}_2[x]\}. \end{aligned}$$

□

Sendo $f(x)$ um polinómio mónico em $F[x]$, com $\text{grau } f > 0$, um polinómio $g \in F[x]$ diz-se um *polinómio módulo f sobre F* se $\text{grau } g < \text{grau } f$. Adicionalmente, denota-se o conjunto de todos os polinómios com grau inferior a $\text{grau } f$ por $F[x]/f$ e, com argumentos análogos aos utilizados na prova das operações em \mathbb{Z} e \mathbb{Z}/m , verifica-se que $F[x]/f$ munido com as operações de adição e multiplicação de polinómios módulo f é um anel.

Exemplo 8.14. Dado o polinómio $f(x) = x^2 - 3 \in \mathbb{Z}_5[x]$, vamos verificar que f é irreductível em \mathbb{Z}_5 e determinar o número de elementos de $\mathbb{Z}_5[x]/(x^2 - 3)$.

Solução. Uma vez que

$$\begin{aligned} f([0]) &= [0] - [3] = [2], \\ f([1]) &= [1] - [3] = [3], \\ f([2]) &= [4] - [3] = [1], \\ f([3]) &= [4] - [3] = [1], \\ f([4]) &= [1] - [3] = [3], \end{aligned}$$

ou seja, $f([a]) \neq [0]$, para $[a] \in \mathbb{Z}_5$, então $f(x)$ é irreductível em \mathbb{Z}_5 . Logo,

$$\mathbb{Z}_5[x]/(x^2 - 3) = \{[a]x + [b] + (x^2 - 3)h(x) : [a], [b] \in \mathbb{Z}_5, h(x) \in \mathbb{Z}_5[x]\}.$$

Como consequência, existem 5 possibilidades para $[a]$ e 5 possibilidades para $[b]$, pelo que $\mathbb{Z}_5[x]/(x^2 - 3)$ tem $5^2 = 25$ elementos. □

8.5. Corpos de Galois

Até agora apenas consideramos corpos finitos de ordem p , onde p é um número primo. Porém, como veremos, existem corpos finitos cujo número de elementos não é primo.

Definição 8.8 (Característica de um corpo). Designa-se por característica de um corpo $(F, +, \cdot, 0, 1)$, o menor número natural n tal que

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ vezes}} = 0.$$

Quando um tal n não existe diz-se que o corpo tem característica 0.

Dever observar-se que todos corpos finitos têm característica positiva e, em particular, a característica de um corpo $(\mathbb{Z}_p, \oplus, \odot, 0, 1)$, com p primo, é igual p .

Exemplo 8.15. Sendo $(F, +, \cdot, 0, 1)$ um corpo finito com característica n , vamos provar que n é primo.

Solução. Se n não é primo, então existem os inteiros s e t , tais que $n = st$, $1 < s < n$ e $1 < t < n$. A propriedade de distributividade implica as igualdades

$$(s \cdot 1) \cdot (t \cdot 1) = (\underbrace{1 + \cdots + 1}_{s \text{ vezes}}) \cdot (\underbrace{1 + \cdots + 1}_{t \text{ vezes}}) = \underbrace{1 \cdot 1 + \cdots + 1 \cdot 1}_{st \text{ vezes}} = n \cdot 1 = 0.$$

Consequentemente, $s \cdot 1 = 0$ ou $t \cdot 1 = 0$, o que entra em contradição com a hipótese de n ser o menor natural tal que $n \cdot 1 = 0$. Logo, n é primo. \square

Dois corpos $\mathcal{F}_1 = (F_1, \oplus, \odot, 0, 1)$ e $\mathcal{F}_2 = (F_2, +, \cdot, 0, 1)$ dizem-se *isomorfos* se existe uma aplicação bijectiva, $\Phi : F_1 \rightarrow F_2$, que preserva as operações multiplicativa e aditiva (ou seja, para todos os $x, y \in F_1$, $\Phi(x \oplus y) = \Phi(x) + \Phi(y)$ e $\Phi(x \odot y) = \Phi(x) \cdot \Phi(y)$). Uma tal aplicação diz-se um *isomorfismo* entre \mathcal{F}_1 e \mathcal{F}_2 ou um automorfismo de \mathcal{F} , se $\mathcal{F} = \mathcal{F}_1 = \mathcal{F}_2$.

Definição 8.9 (Aplicação de Frobenius⁴). Dado um corpo $\mathcal{F} = (F, +, \cdot, 0, 1)$ de característica p , designa-se por aplicação de Frobenius a aplicação $\Phi : F \rightarrow F$ tal que $\Phi(x) = x^p$.

Exemplo 8.16. Sendo $\mathcal{F} = (F, +, \cdot, 0, 1)$ um corpo finito de característica p , vamos provar que a aplicação de Frobenius $\Phi : F \rightarrow F$ é um automorfismo. Adicionalmente, vamos provar que se $\mathcal{F} = \mathbb{Z}_p$ então Φ é o automorfismo identidade.

Solução. É claro que $\Phi(1) = 1$ e $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$. Por outro lado (escrevendo xy em vez de $x \cdot y$), tendo em conta as igualdades

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i = a^p + \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!} a^{p-i} b^i + b^p,$$

obtém-se $\Phi(a + b) = \Phi(a) + \Phi(b)$, uma vez que $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ é divisível por p , para $1 \leq i \leq p-1$. Para finalizarmos a prova de que Φ é um automorfismo, resta demonstrar que se trata de uma aplicação bijectiva, que é precisamente o que se segue.

Uma vez que $a \in \mathcal{F} \setminus \{0\}$ implica $\Phi(a) \neq 0$ (note-se que $1 = \Phi(1) = \Phi(a \cdot a^{-1}) = \Phi(a) \cdot \Phi(a^{-1})$), podemos concluir que se $a, b \in \mathcal{F}$ são tais que $a \neq b$, fazendo $c = a - b$,

$$\Phi(b) = \Phi(a + (b - a)) = \Phi(a + c) = \Phi(a) + \Phi(c) \neq \Phi(a),$$

onde Φ é injectiva e, consequentemente, sobrejectiva (dado que $|\text{Im}(\Phi)| = |F|$). Finalmente, tendo em conta o pequeno teorema de Fermat (Teorema 8.11), do qual decorre $x^p \equiv x \pmod{p}$, para $x = 0, 1, \dots, p-1$, obtém-se $\Phi(x) = x$. \square

Um *subcorpo* de um corpo $\mathcal{F} = (F, +, \cdot, 0, 1)$ é um subconjunto S de F que contém os elementos 0 e 1, tal que se $x, y \in S$, então $x + y, x - y, x \cdot y \in S$ e, adicionalmente,

$$z \in S \setminus \{0\} \Rightarrow z^{-1} \in S.$$

Tendo em conta o Exemplo 8.15, podemos concluir que todo o corpo \mathcal{F} de característica p primo, contém um subcorpo, chamado *subcorpo primitivo* (que é a intersecção de todos os subcorpos de \mathcal{F}), isomorfo a $(\mathbb{Z}_p, \oplus, \odot, 0, 1)$. Por este motivo, os subcorpos primitivos de \mathcal{F} denotam-se por \mathbb{Z}_p .

⁴Ferdinand Georg Frobenius (1849–1917), matemático alemão que trabalhou em teoria dos grupos, representação de grupos e teoria dos números.

O conjunto dos n -uplos $V = F^n$, onde $\mathcal{F} = (F, \oplus, \odot, 0, 1)$ é um corpo, é um *espaço vectorial*⁵ sobre o corpo \mathcal{F} , se quaisquer que sejam os n -uplos $(a_1, \dots, a_n), (b_1, \dots, b_n) \in V$ (que se designam por vectores) e qualquer que seja $\lambda \in F$ (que se designa por escalar)

$$\begin{aligned}(a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 \oplus b_1, \dots, a_n \oplus b_n), \\ \lambda \cdot (a_1, \dots, a_n) &= (\lambda \odot a_1, \dots, \lambda \odot a_n).\end{aligned}$$

As operações $+$ e \cdot designam-se por *adição de vectores* e *multiplicação de vectores por um escalar*. Em coerência com a definição destas operações, diz-se que o vector $x \in V$ é *combinação linear* dos vectores $x_1, \dots, x_k \in V$, se existem escalares $\lambda_1, \dots, \lambda_k \in F$ tais que

$$x = \lambda_1 x_1 + \dots + \lambda_k x_k.$$

Um conjunto de vectores $X = \{x_1, \dots, x_k\}$ diz-se *linearmente independente* se

$$\lambda_1 x_1 + \dots + \lambda_k x_k = \mathbf{0} \Rightarrow \lambda_1 = \dots = \lambda_k = 0,$$

com $\mathbf{0} = (0, \dots, 0) \in V$. Demonstra-se que n é o máximo número de vectores linearmente independentes em V e, consequentemente, diz-se que V tem *dimensão* n , designando-se por *base* de V todo o conjunto de n vectores linearmente independentes. Adicionalmente, prova-se que qualquer vector de V admite uma representação única como combinação linear dos vectores de uma base.

Tendo presente estes conceitos, dado um corpo finito $\mathcal{F} = (F, +, \cdot, 0, 1)$, com m elementos (isto é, de *ordem* m) e característica p , podemos considerar \mathcal{F} como um espaço vectorial sobre o subcorpo primitivo \mathbb{Z}_p . Admitindo que este espaço vectorial tem dimensão n , todos os seus vectores são combinação linear de uma base fixa de n elementos e, consequentemente, $m = p^n$, ou seja, \mathcal{F} é isomorfo a \mathbb{Z}_p^n . Assim, dado um corpo arbitrário de ordem m e característica p , existe $n \in \mathbb{N}$ tal que $m = p^n$ (onde podemos concluir que, por exemplo, não existe nenhum corpo de ordem 10, uma vez que 10 não é potência de um primo). Por outro lado, todos os corpos finitos de ordem p^n são isomorfos.

Exemplo 8.17. Vamos definir as tabelas das operações aditiva e multiplicativa de modo a obter um corpo \mathcal{F} com 4 elementos.

Solução. Denotando os elementos do corpo por 0, 1, a e b , as tabelas das operações aditiva e multiplicativa são as indicadas na Tabela 8.3. \square

+	0	1	a	b	.	0	1	a	b
0	0	1	a	b	0	0	0	0	0
1	1	0	b	a	1	0	1	a	b
a	a	b	0	1	a	0	a	b	1
b	b	a	1	0	b	0	b	1	a

Tabela 8.3: Tabelas das operações do corpo $\mathcal{F} \cong \mathbb{Z}_2^2$.

Exemplo 8.18. A Figura 8.2 representa um tabuleiro (com buracos) de um jogo que se inicia com todos os buracos preenchidos com pinos, com excepção do buraco central. O jogo prossegue fazendo saltar qualquer pino por cima de outro que lhe é adjacente (com movimentos horizontais ou verticais), abandonando o buraco que actualmente preenche para preencher outro que, no momento, esteja vazio e seja adjacente ao pino sobre o qual se dá o salto. Em cada jogada, o pino sobre o qual se salta é retirado do tabuleiro e deixa de fazer parte do jogo. O objectivo do jogo é remover todos os pinos do

⁵Embora a definição de espaço vectorial seja mais geral, para os objectivos deste texto, basta considerar este caso particular.

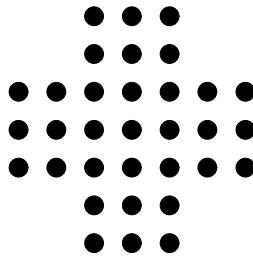


Figura 8.2: Tabuleiro do jogo solitário descrito neste exemplo.

tabuleiro, com exceção de um que, tradicionalmente, ocupa a posição central. Vamos provar que a posição central é, efectivamente, uma das posições possíveis para o último pino e que, embora existam outras posições possíveis, elas não são arbitrárias.

Solução. Vamos considerar o corpo \mathcal{F} com 2^2 elementos, cujas tabelas aditiva e multiplicativa foram determinadas no Exemplo 8.17, em função dos elementos 0, 1, a e b . Considerem-se os buracos do tabuleiro como um subconjunto do reticulado \mathbb{Z}^2 com origem $(0,0)$ no buraco central e eixos horizontal e vertical usuais. Sendo X um conjunto de pares ordenados que representam as posições dos pinos, vamos definir

$$A(X) = \sum_{(x,y) \in X} a^{x+y} \quad B(X) = \sum_{(x,y) \in X} a^{x-y}.$$

Admitindo que numa jogada arbitrária se transforma X em Y , deslocando um dado pino passando por cima da posição (\bar{x}, \bar{y}) , obtém-se um dos seguintes casos:

$$Y = (X \setminus \{(\bar{x}, \bar{y}), (\bar{x}-1, \bar{y})\}) \cup \{(\bar{x}+1, \bar{y})\}, \quad (8.15)$$

$$Y = (X \setminus \{(\bar{x}, \bar{y}), (\bar{x}+1, \bar{y})\}) \cup \{(\bar{x}-1, \bar{y})\}, \quad (8.16)$$

$$Y = (X \setminus \{(\bar{x}, \bar{y}), (\bar{x}, \bar{y}-1)\}) \cup \{(\bar{x}, \bar{y}+1)\}, \quad (8.17)$$

$$Y = (X \setminus \{(\bar{x}, \bar{y}), (\bar{x}, \bar{y}+1)\}) \cup \{(\bar{x}, \bar{y}-1)\}. \quad (8.18)$$

Como consequência, obtém-se para A , respectivamente,

$$A(Y) = A(X) - a^{\bar{x}+\bar{y}} - a^{\bar{x}+\bar{y}-1} + a^{\bar{x}+\bar{y}+1},$$

$$A(Y) = A(X) - a^{\bar{x}+\bar{y}} - a^{\bar{x}+\bar{y}+1} + a^{\bar{x}+\bar{y}-1},$$

$$A(Y) = A(X) - a^{\bar{x}+\bar{y}} - a^{\bar{x}+\bar{y}-1} + a^{\bar{x}+\bar{y}+1},$$

$$A(Y) = A(X) - a^{\bar{x}+\bar{y}} - a^{\bar{x}+\bar{y}+1} + a^{\bar{x}+\bar{y}-1},$$

e, em qualquer dos casos, conclui-se que $A(Y) = A(X) + a^{\bar{x}+\bar{y}+1} + a^{\bar{x}+\bar{y}} + a^{\bar{x}+\bar{y}-1} = A(X)$ (uma vez que, de acordo com a Tabela 8.3, $a^2 + a + 1 = 0$). De igual modo se conclui que $B(Y) = B(X)$. Assim, os pares $(A(X), B(X))$ são invariantes ao longo das sucessivas jogadas. Uma vez que na posição inicial X , $A(X) = B(X) = 1$, a posição final (x, y) é tal que $a^{x+y} = a^{x-y} = 1$. Logo, $x + y$ e $x - y$ são múltiplos de 3 (uma vez que $a^k = 1 \Rightarrow k = 3n$, com $n \in \mathbb{N}$) e, consequentemente, as únicas posições (x, y) em que é possível terminar o jogo são: $(-3, 0), (0, -3), (0, 0), (0, 3)$ e $(3, 0)$. \square

Definição 8.10 (Corpo de Galois). *Um corpo finito com p^n elementos, onde p é primo e $n \in \mathbb{N}$, designa-se por corpo de Galois⁶ e denota-se por $GF(p^n)$.*

⁶Evariste Galois (1811-1832), matemático francês que desenvolveu um trabalho notável, apesar de ter morrido em duelo com apenas 21 anos de idade.

Observe-se que, de acordo com a análise anterior, o corpo de Galois $GF(p^n)$ é isomorfo ao espaço vectorial de dimensão n sobre \mathbb{Z}_p , ou seja,

$$GF(p^n) \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ vezes}} = \mathbb{Z}_p^n.$$

Assim, os elementos de $G(p^n)$ podem ser vistos como n -uplos que representam polinómios de $\mathbb{Z}_p[x]$ módulo um polinómio irredutível de grau n (pelo que têm grau inferior a n). Nestas condições, o n -uplo $(a_0, a_1, \dots, a_{n-2}, a_{n-1}) \in \mathbb{Z}_p^n$ representa o polinómio $f(x) = a_0x^{n-1} + a_1x^{n-2} + \dots + a_{n-2}x + a_{n-1} \in \mathbb{Z}_p[x]$ e, como consequência, o resultado da multiplicação de dois elementos de $G(p^n)$ obtém-se de acordo com as regras usuais da multiplicação de polinómios módulo um polinómio irredutível de grau n em $\mathbb{Z}_p[x]$. Adicionalmente, tendo em conta que todos os corpos finitos de ordem p^n são isomorfos, podemos concluir que, a menos de isomorfismos, é indiferente o polinómio irredutível de grau n que se escolhe. Note-se que, tal como na aritmética modulo p (onde p é um número primo), para a qual o conjunto dos inteiros formam um corpo finito \mathbb{Z}_p (ver Exemplo 8.6), também com a aritmética modulo um polinómio irredutível (primo) f de grau n , o conjunto $\mathbb{Z}_p[x]/f$ forma um corpo finito isomorfo a $GF(p^n)$ (conforme se prova no teorema a seguir).

Teorema 8.14. *Sendo $GF(p^n)$ um corpo de Galois, onde p é primo e $n \in \mathbb{N}$, o anel $\mathbb{Z}_p[x]/f$ é um corpo finito de ordem p^n se e só se f é irredutível de ordem n em $\mathbb{Z}_p[x]$.*

Demonstração. Seja $g \in \mathbb{Z}_p[x]/f$ e suponha que f é primo. Se $g \neq 0$, então grau $g <$ grau f . Logo, $\text{mdc}(f, g) = 1$ e existem $u, v \in \mathbb{Z}_p[x]$ tais que $uf + vg = 1$, em $\mathbb{Z}_p[x]$, ou seja, $vg \equiv 1 \pmod{f}$, donde v é o inverso de g em $\mathbb{Z}_p[x]/f$. Reciprocamente, suponha que $\mathbb{Z}_p[x]/f$ é um corpo. Se f é redutível, então existem $g, h \in \mathbb{Z}_p[x]$ tais que $\text{grau } g > 0$, $\text{grau } h > 0$ e $f = gh$ e, como consequência, $gh \equiv 0 \pmod{f}$, o que é equivalente a afirmar que $gh = 0$ no corpo $\mathbb{Z}_p[x]/f$, o que é impossível. Finalmente, sendo f irredutível, é claro que $|\mathbb{Z}_p[x]/f| = p^n$ se e só se f tem grau n . \square

Exemplo 8.19. *Tendo em conta que $x^2 + x + 1$ é irredutível em $\mathbb{Z}_2[x]$, vamos determinar as tabelas das operações do corpo*

$$\mathbb{Z}_2[x]/(x^2 + x + 1).$$

Solução. Ver a Tabela 8.4 (e compare com o Exemplo 8.17). \square

+	0	1	x	$x + 1$.	0	1	x	$x + 1$
0	0	1	x	$x + 1$	0	0	0	0	0
1	1	0	$x + 1$	x	1	0	1	x	$x + 1$
x	x	$x + 1$	0	1	x	0	x	$x + 1$	1
$x + 1$	$x + 1$	x	1	0	$x + 1$	0	$x + 1$	1	x

Tabela 8.4: Tabelas das operações do corpo $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

Exemplo 8.20. *Considerando $\mathbb{Z}_2[x]/f$, com $f(x) = x^2 + 1$, vamos demonstrar que $f(x)$ é redutível e, como consequência, $\mathbb{Z}_2[x]/f$ não é um corpo.*

Solução. Uma vez que $f(x) = x^2 + 1 = (x+1)^2$ em $\mathbb{Z}_2[x]$, o polinómio não é irredutível. A Tabela 8.5 apresenta a multiplicação em $\mathbb{Z}_2[x]/f$. Analisando esta tabela, vem que, por exemplo, o elemento $x+1$ não tem inverso. Logo, $\mathbb{Z}_2[x]/f$ não é um corpo. \square

Note-se, porém, que $\mathbb{Z}_3[x]/f = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$, com $f(x) = x^2 + 1$, tem $3^2 = 9$ elementos e é um corpo.

.	0	1	x	$x + 1$
0	0	0	0	0
1	0	1	x	$x + 1$
x	0	x	1	$x + 1$
$x + 1$	0	$x + 1$	$x + 1$	0

Tabela 8.5: Multiplicação em $\mathbb{Z}_2[x]/(x^2 + 1)$.

Definição 8.11 (Polinómio separável). Um polinómio irreductível f sobre o corpo \mathbb{F} diz-se separável sobre \mathbb{F} se não tem raízes múltiplas num corpo de decomposição.

Uma vez que o corpo de decomposição é único (a menos de isomorfismos), é indiferente qual o corpo de decomposição escolhido para testar esta propriedade.

Definição 8.12 (Derivada formal de um polinómio). Seja K um corpo e $f(x) = a_0x^n + \dots + a_{n-1}x + a_n \in K[x]$. A derivada formal de f que se denota por f' ou por Df é o polinómio

$$f'(x) = na_0x^{n-1} + \dots + 2a_{n-2}x + a_{n-1},$$

onde os coeficientes $n, \dots, 2$ são elementos de K (pelo que devem ser convenientemente adaptados e lidos como tal).

Sabe-se que um polinómio $f \neq 0$ tem raízes múltiplas no seu corpo de decomposição se e somente se f e f' têm um factor comum de grau não inferior a 1. Esta propriedade permanece válida para qualquer corpo.

Teorema 8.15. Seja p um número primo e $q = p^n$, com $n \in \mathbb{N}$. Um corpo F tem ordem q se e só se é um corpo de decomposição do polinómio $f(x) = x^{p^n} - x$ definido sobre um corpo isomorfo a \mathbb{Z}_p .

Demonstração. Suponha que $|F| = q$. Então o conjunto $F \setminus \{0\}$ forma um grupo multiplicativo de ordem $q - 1$. Logo, se $0 \neq x \in F$, então $x^{q-1} = 1$ e, consequentemente, $x^q - x = 0$. Assim, dado que $0^q - 0 = 0$, qualquer elemento de F é raiz de $x^{p^n} - x$, donde f se decompõe em F num produto de factores lineares. Uma vez que as raízes de f esgotam F , este corpo é um corpo de decomposição do polinómio f definido sobre \mathbb{Z}_p .

Reciprocamente, seja F um corpo de decomposição de f sobre \mathbb{Z}_p . Dado que $f'(x) = p^n x^{p^n-1} - 1 \equiv -1 \pmod{p}$, f e f' são relativamente primos e, consequentemente, f tem q raízes distintas. Resta provar que o conjunto destas raízes é um corpo que, nestas condições, coincide com o corpo de decomposição F , pelo que $|F| = q$. Assim, para $\alpha, \beta \in F$, esta prova consiste na demonstração do seguinte: (1) $-\alpha \in F$, (2) se $\alpha \neq 0$ então $\alpha^{-1} \in F$, (3) $\alpha + \beta \in F$, (4) $\alpha\beta \in F$.

(1) Uma vez que $\alpha \in F$, ou seja, $f(\alpha) = 0$, calculando $f(-\alpha)$, vem

$$f(-\alpha) = (-\alpha)^{p^n} - (-\alpha) = (-1)^{p^n} \alpha^{p^n} - (-\alpha) = (-1)(\alpha^{p^n} - \alpha) = 0,$$

donde $-\alpha \in F$.

(2) Se $\alpha \neq 0$ então

$$\begin{aligned} f(\alpha^{-1}) &= (\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} \\ &= (\alpha^{p^n+1})^{-1}(\alpha^{p^n+1})((\alpha^{p^n})^{-1} - \alpha^{-1}) \\ &= -(\alpha^{p^n+1})^{-1}(\alpha^{p^n} - \alpha) = 0. \end{aligned}$$

Logo, $\alpha^{-1} \in F$.

(3) Dado que $\alpha, \beta \in F$, então

$$\begin{aligned} f(\alpha + \beta) &= (\alpha + \beta)^{p^n} - (\alpha + \beta) \\ &= \alpha^{p^n} + \binom{p^n}{1} \alpha^{p^n-1} \beta + \binom{p^n}{2} \alpha^{p^n-2} \beta^2 + \cdots + \beta^{p^n} - \alpha - \beta \\ &= (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = 0, \end{aligned}$$

pelo que $\alpha + \beta \in F$.

(4) Finalmente, obtém-se

$$\begin{aligned} f(\alpha\beta) &= (\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha^{p^n}\beta + \alpha^{p^n}\beta - \alpha\beta \\ &= \alpha^{p^n}(\beta^{p^n} - \beta) + \beta(\alpha^{p^n} - \alpha) = 0, \end{aligned}$$

e, como consequência, $\alpha\beta \in F$. □

Uma vez que os corpos de decomposição existem e são únicos (a menos de isomorfismos), o teorema a seguir caracteriza completamente todos os corpos finitos.

Teorema 8.16. *Para cada p primo e $n \in \mathbb{N}$ existe um único corpo (a menos de isomorfismos) com p^n elementos (corpo de Galois $GF(p^n)$) que coincide com o corpo de decomposição do polinómio $x^{p^n} - x \in \mathbb{Z}_p[x]$.*

Demonstração. Esta prova decorre directamente do Teorema 8.15. □

Exemplo 8.21. Vamos determinar os elementos do corpo $F = GF(2^3)$.

Solução. Considerando o polinómio $f(x) = x^3 + x + 1$, conclui-se que $f(x)$ é irreductível em \mathbb{Z}_2 . Logo, o corpo de Galois $F = GF(2^3)$ é isomorfo $\mathbb{Z}_2[x]/(x^3 + x + 1)$. Sendo α uma raiz de $f(x)$, vem que 1, α , α^2 formam um base para $\mathbb{Z}_2[x]/(x^3 + x + 1)$ e, consequentemente,

$$\begin{aligned} F &\cong \{a + bx + cx^2 : a, b, c \in \mathbb{Z}_2, x^3 + x + 1 = 0\} \\ &= \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}. \end{aligned}$$

A Tabela 8.6 corresponde à tabela da operação multiplicativa de $\mathbb{Z}_2[x]/(x^3 + x + 1)$. □

.	1	x	$x + 1$	x^2	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$
1	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
x	x	x^2	$x^2 + x$	$x + 1$	$x^2 + x + 1$	1	$x^2 + 1$
$x + 1$	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	1	x^2	x
x^2	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x	1
$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	x	$x + 1$	x^2
$x^2 + 1$	$x^2 + 1$	1	x^2	x	$x + 1$	$x^2 + x + 1$	$x^2 + x$
$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + 1$	x	1	x^2	$x^2 + 1$	$x + 1$

Tabela 8.6: Operação multiplicativa de $\mathbb{Z}_2[x]/(x^3 + x + 1)$.

Observe-se que todas as raízes de um polinómio irreductível de grau n sobre \mathbb{Z}_p (com p primo) pertencem ao corpo de Galois $GF(p^n)$. Logo, $GF(p^n)$ contém as raízes de todos os polinómios irreductíveis sobre \mathbb{Z}_p , cujos graus são divisores de n . Consequentemente, podemos determinar a factorização do polinómio $f(x) = x^{p^n} - x$ em $\mathbb{Z}_p[x]$.

Exemplo 8.22. Vamos factorizar o polinómio $x^2 - x = x^4 - x$ em \mathbb{Z}_2 .

Solução. Uma vez que x , $x + 1$, $x^2 + x + 1$ são todos os polinómios irreducíveis sobre \mathbb{Z}_2 com grau não superior 2, então

$$x^2 - x = x^4 - x = x(x + 1)(x^2 + x + 1).$$

□

Definição 8.13 (Polinómio primitivo). Um polinómio $f \in \mathbb{Z}[x]$ diz-se primitivo se os seus coeficientes, considerados na sua totalidade, são relativamente primos, ou seja, se não têm um divisor comum maior do que 1.

Note-se que se os coeficiente de um polinómio $f \in \mathbb{Z}[x]$ admitem um divisor comum maior do que 1, então podemos dividir, sucessivamente, todos os coeficientes por ele até que ele desapareça. Logo, todo o polinómio com coeficientes inteiros é proporcional a um polinómio primitivo (determinado de forma única, a menos da multiplicação por ± 1).

Teorema 8.17 (de Gauss). Se um polinómio com coeficientes inteiros se factoriza num produto de dois polinómios com coeficientes racionais, então ele factoriza-se num produto de polinómios com coeficientes inteiros, proporcionais aos polinómios da primeira factorização.

Demonstração. Seja $f \in \mathbb{Z}[x]$ e suponha que $f(x) = g(x)h(x)$, com $g, h \in \mathbb{Q}[x]$. Então g e h são proporcionais, respectivamente, aos polinómios primitivos g_1 e h_1 . Nestas condições, $f(x) = \mu g_1(x)h_1(x)$, com $\mu \in \mathbb{Q}$ e sendo $\mu = \frac{r}{q}$, com $\text{mdc}(r, q) = 1$, $qf(x) = rg_1(x)h_1(x)$. Vamos supor que $q \neq \pm 1$ e seja p um divisor primo de q . Então $rg_1(x)h_1(x) \equiv 0 \pmod{p}$, com $r \neq 0$ em \mathbb{Z}_p (uma vez que r e q são relativamente primos) e também com $g_1 \neq 0$ e $h_1 \neq 0$ em $\mathbb{Z}_p[x]$ (uma vez que tanto g_1 como h_1 são polinómios primitivos e, consequentemente, os coeficientes de qualquer deles não podem ser todos divisíveis por p). Dado que $\mathbb{Z}_p[x]$ não tem divisores de zero, obtém-se uma contradição que resulta de se haver suposto $q \neq \pm 1$. □

Por outras palavras, o Teorema 8.17 afirma que se $f \in \mathbb{Z}[x]$ e $f(x) = g(x)h(x)$, com $g, h \in \mathbb{Q}[x]$, então $\exists \lambda \in \mathbb{Q} \setminus \{0\}$ tal que $\lambda g, \lambda^{-1}h \in \mathbb{Z}[x]$. Como consequência, imediatamente, obtém-se seguinte corolário:

Corolário 8.18. Se um polinómio $f \in \mathbb{Z}[x]$ se factoriza num produto de dois polinómios de $\mathbb{Q}[x]$, com grau positivo, então ele factoriza-se num produto de polinómios de $\mathbb{Z}[x]$.

É óbvio que um polinómio redutível em $\mathbb{Z}[x]$ é também redutível em $\mathbb{Q}[x]$. Logo, tendo em conta o Corolário 8.18, podemos concluir que um polinómio é irreducível em $\mathbb{Q}[x]$ se e somente se é irreducível em $\mathbb{Z}[x]$.

Note-se, porém, que o teste de irreducibilidade de um polinómio por verificação exaustiva de todos os possíveis factores é, em geral, computacionalmente inatingível. Segue-se um critério que pode facilitar a detecção de irreducibilidade.

Teorema 8.19 (critério de Eisenstein⁷). Seja $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ um polinómio de grau n e suponha que existe um número primo p tal que

$$p \nmid a_0, \tag{8.19}$$

$$p \mid a_i, \text{ para } i = 1, \dots, n, \tag{8.20}$$

$$p^2 \nmid a_n. \tag{8.21}$$

Então f é irreducível em $\mathbb{Q}[x]$.

⁷Ferdinand Gotthold Eisenstein (1823–1852) foi um matemático alemão que trabalhou em teoria dos números e análise.

Demonstração. Pelo Teorema 8.17, basta mostrar que f é irreduzível sobre \mathbb{Z} . Assim, suponha que $f = gh$, onde

$$g(x) = b_0x^r + \cdots + b_{r-1}x + b_r \quad h(x) = c_0x^s + \cdots + c_{s-1}x + c_s$$

são polinómios de $\mathbb{Z}[x]$ de grau inferior a n . Então $r \geq 1$, $s \geq 1$ e $r + s = n$. Agora, $b_r c_s = a_n$ e, consequentemente, por (8.20), $p \mid b_r$ ou $p \mid c_s$. Porém, tendo em conta (8.21), p não divide, simultaneamente, b_r e c_s . Logo, sem perda de generalidade, podemos assumir que $p \mid b_r$ e $p \nmid c_s$. Se todos os coeficientes b_j são divisíveis por p , então a_0 é divisível por p o que contradiz (8.19). Suponha que p divide os coeficientes $b_r, b_{r-1}, \dots, b_{r-(j-1)}$, para algum $j > 0$, mas $p \nmid b_{r-j}$. Então, dado que

$$a_{n-j} = b_{r-j}c_s + \cdots + b_r c_{s-j},$$

e p divide $a_{n-j}, b_r, \dots, b_{r-(j-1)}$, mas não b_{r-j} , podemos concluir que p divide c_s , o que constitui uma contradição. Logo, f é irreduzível. \square

Exemplo 8.23. Vamos provar que o polinómio

$$f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} \in \mathbb{Q}[x]$$

é irreduzível sobre \mathbb{Q} .

Solução. O polinómio f é irreduzível sobre \mathbb{Q} se e somente se o polinómio

$$9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$$

é irreduzível sobre \mathbb{Q} . Logo, aplicando o critério de Eisenstein, com $p = 3$, concluímos que f é irreduzível. \square

Existem ainda outras técnicas para testar a irreduzibilidade de polinómios de $\mathbb{Z}[x]$. Uma técnica muito simples, consiste em considerar um homomorfismo de $\mathbb{Z} \rightarrow \mathbb{Z}_p$ tal que para cada $z \in \mathbb{Z}$, a imagem é a classe de congruência de z módulo p . Este homomorfismo estende-se, de um modo natural, ao respectivo anel de polinómios, obtendo-se o homomorfismo $\phi_p : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$. Assim, se f é um polinómio redutível em $\mathbb{Z}[x]$, então $f = gh$, com $g, h \in \mathbb{Z}[x]$ e tanto g como h têm menor grau do que grau f . Desde que p não seja um divisor do coeficiente associado à maior potência de um dado polinómio, podemos concluir que ϕ_p preserva a factorização, ou seja, $\phi_p(gh) = \phi_p(g)\phi_p(h)$ e, consequentemente, f é redutível em $\mathbb{Z}_p[x]$. Nestas condições, se a imagem de um polinómio é irreduzível em \mathbb{Z}_p , então o polinómio original é também irreduzível em $\mathbb{Z}[x]$. O recíproco, porém, nem sempre é verdadeiro. Com efeito, considerando o polinómio $x^2 - 2 \in \mathbb{Z}[x]$, vemos que $\phi_2(x^2 - 2) = x^2 \in \mathbb{Z}_2[x]$. Logo, $\phi_2(x^2 - 2) = x^2$ é redutível em $\mathbb{Z}_2[x]$, mas o polinómio original não é redutível em $\mathbb{Z}[x]$. A grande vantagem de se fazer o estudo da irreduzibilidade de um polinómio de $\mathbb{Z}[x]$, a partir da sua imagem em $\mathbb{Z}_p[x]$, por ϕ_p , reside no facto de $\mathbb{Z}_p[x]$ ser finito e, consequentemente, existir "apenas" um número finito de possibilidades de teste da irreduzibilidade. O segredo do êxito da aplicação desta técnica está, naturalmente, na escolha do valor de p .

Exemplo 8.24. Vamos estudar a irreduzibilidade do polinómio

$$f(x) = x^4 + 15x^3 + 7 \in \mathbb{Q}[x].$$

Solução. Primeiramente, deve observar-se que, pelo lema de Gauss, verificar se o polinómio f é irreduzível em $\mathbb{Q}[x]$ é equivalente a verificar se f é irreduzível em $\mathbb{Z}[x]$.

A imagem do polinómio f em $\mathbb{Z}_5[x]$, por ϕ_5 , é $x^4 + 2$. Se este polinómio é redutível em $\mathbb{Z}_5[x]$, então ele tem um factor de grau 1, ou dois factores de grau 2. O primeiro caso implica a existência de $z \in \mathbb{Z}_5$

tal que $z^4 + 2 = 0$, o que é impossível, dado que $0 \notin \{f(0), f(1), f(2), f(3), f(4)\}$. O segundo caso implica a verificação da igualdade

$$x^4 + 2 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b+ac+d)x^2 + (ad+bc)x + bd.$$

Logo, obtém-se $a + c = 0$, $b + ac + d = 0$ e $bd = 2$, donde vem que $b + d = a^2$ e, consequentemente, $a \in \{0, 1, 2\}$ (dado que 0, 1 e 4 são os únicos quadrados de \mathbb{Z}_5). Assim, vem

1. $a = 0 \Rightarrow c = 0, b = -d$ e $d^2 + 2 = 0$, o que é impossível,
2. $a = 1 \Rightarrow c = 4, b + d = 1$ e $b(1 - b) = 2$, o que é impossível,
3. $a = 2 \Rightarrow c = 3, b + d = 4$ e $b(4 - b) = 2$, o que é impossível.

Concluímos assim que o polinómio $x^4 + 2$ é irreductível em \mathbb{Z}_5 , donde o polinómio original $f(x)$ é irreductível em $\mathbb{Z}[x]$ e, consequentemente, em $\mathbb{Q}[x]$. \square

8.6. Quadrados latinos e quadrados mágicos

Definição 8.14 (Quasigrupo). *Um grupóide (isto é, um conjunto não vazio com uma lei de composição interna) (S, \odot) diz-se um quasigrupo de ordem n se $|S| = n$ e $\forall a, b \in S$ existe um único elemento $x \in S$ tal que $x \odot a = b$ e um único elemento $y \in S$ tal que $a \odot y = b$.*

De acordo com esta definição, sendo (S, \odot) um quasigrupo, com $S = [n]$, na matriz A , com entradas a_{ij} tais que $\forall i, j \in [n]$ $a_{ij} = i \odot j$, verifica-se que cada elemento de S ocorre exactamente uma vez em cada uma das linhas e colunas. Com efeito, supondo que existe $i \in [n]$ ($j \in [n]$) e que existem $j_1, j_2 \in [n]$ ($i_1, i_2 \in [n]$) tais que $i \odot j_1 = i \odot j_2$ ($i_1 \odot j = i_2 \odot j$), pela definição de quasigrupo, $j_1 = j_2$ ($i_1 = i_2$). Assim, numa matriz cujas entradas correspondem ao resultado da operação dos índices num quasigrupo de ordem n , (S, \odot) , que se designa por *tabela da operação* \odot , não existem linhas nem colunas com elementos repetidos e, uma vez que cada linha e coluna tem n elementos, podemos também concluir que cada linha e coluna contém todos os elementos de S .

Definição 8.15 (Quadrado latino). *As matrizes quadradas de ordem n , cujas entradas pertencem a um conjunto com n elementos e onde cada elemento ocorre exactamente uma vez em cada linha e coluna, designam-se por quadrados latinos de ordem n .*

Na pagina 153 representa-se um quadrado latino de ordem 5, com símbolos no conjunto $\{\spadesuit, \heartsuit, \clubsuit, \diamondsuit, \heartsuit\}$ e a particularidade de também não ter elementos repetidos ao longo de qualquer das diagonais.

Teorema 8.20. *Para cada $m \geq 2$, o grupo (\mathbb{Z}_m, \oplus) é um quasigrupo.*

Demonstração. Suponha-se que dado $i \in \mathbb{Z}_m$, existem $j, j' \in \mathbb{Z}_m$ tais que $i \oplus j = i \oplus j'$. Então, adicionando $-i$ a ambos os lados desta igualdade, obtém-se $j = j'$. Pela simetria da operação \oplus , de igual modo se conclui a existência de unicidade à esquerda. \square

Corolário 8.21. *A tabela da operação \oplus do quasigrupo (\mathbb{Z}_m, \oplus) define um quadrado latino.*

Demonstração. A demonstração é consequência imediata do teorema anterior. \square

Conclui-se deste modo que para qualquer $n \in \mathbb{N}$ existe pelo menos um quadrado latino de ordem n , o qual pode ser obtido pela tabela da operação \oplus em \mathbb{Z}_n . Porém, a determinação do número total de quadrados latinos distintos de ordem n , $L(n)$, para um número natural n arbitrário, é bem mais complicada. Na Tabela 8.7 apresentam-se os valores de $L(n)$, para $n \leq 7$.

O teorema a seguir estabelece um minorante para $L(n)$.

n	1	2	3	4	5	6	7
$L(n)$	1	2	12	576	161.280	812.851.200	61.479.419.904.000

Tabela 8.7: Números de quadrados latinos de ordem $n \leq 7$.

Teorema 8.22. *O número total de quadrados latinos distintos de ordem n , $L(n)$, para $n \in \mathbb{N}$, verifica a seguinte desigualdade*

$$L(n) \geq n!(n-1)!(n-2)! \cdots 2!1!$$

Demonstração. Existem $n!$ possibilidades para a escolha da primeira linha de um quadrado latino. Uma vez escolhida a primeira linha, existem pelo menos $(n-1)!$ possibilidades de escolher a segunda linha, etc. Logo, aplicando o princípio da multiplicação generalizada vem que $n!(n-1)!(n-2)! \cdots 2!1!$ é um minorante para o número de quadrados latinos de ordem n . \square

Definição 8.16 (Quadrado latino normalizado). *Um quadrado latino designa-se por normalizado, se a primeira linha é da forma 1 2 3 ... n .*

Observe-se que todo o quadrado latino L , pode ser *normalizado* por troca adequada de símbolos e quando tal acontece denota-se por L^* . Sendo $L^*(n)$ o número de quadrados latinos normalizados de ordem n , conclui-se imediatamente que $L(n) = n!L^*(n)$.

Outra questão associada aos quadrados latinos, diz respeito à determinação de pares de *quadrados latinos ortogonais* que são quadrados latinos L' e L'' tais que, para quaisquer pares de símbolos (α, β) existe uma única entrada (i, j) tal que

$$L'_{ij} = \alpha \text{ e } L''_{ij} = \beta.$$

Por exemplo, as matrizes L' e L'' , a seguir indicadas, representam dois quadrados latinos ortogonais de ordem 3.

$$L' = \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix} \quad \text{e} \quad L'' = \begin{bmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{bmatrix}.$$

Historicamente, o primeiro problema sobre quadrados latinos ortogonais, conhecido por *Problema dos trinta e seis oficiais*, foi analisado por Euler, com a seguinte formulação:

Admita-se a existência de seis destacamentos, em cada um dos quais ficam seis oficiais com patentes distintas, de entre seis possíveis. Pretende-se fazer uma parada militar, envolvendo estes trinta e seis oficiais, de tal forma que eles apareçam seis em cada linha sem que existam dois oficiais com a mesma patente ou pertencentes ao mesmo destacamento numa mesma linha ou coluna.

É claro que o problema dos trinta e seis oficiais é equivalente ao problema da existência de dois quadrados latinos ortogonais de ordem seis. Euler conjecturou que este problema não teria solução, conjectura (verdadeira) que no entanto só foi provada, por análise exaustiva de todas as possibilidades, em 1900 por Tarry⁸. Tomando como verdadeira a sua conjectura e tendo em conta que não existem quadrados latinos ortogonais de ordem 2, Euler conjecturou ainda a não existência de quadrados latinos ortogonais de ordem n , para $n \equiv 2 \pmod{4}$. Esta conjectura, porém, é falsa. Com efeito, Bose⁹, Shrikhande¹⁰, e Parker¹¹ demonstraram (em 1960) a existência de quadrados latinos ortogonais de ordem n para todo o natural n , com exceção de $n = 2$ e $n = 6$.

⁸Tarry Gaston (1843–1913) foi um matemático amador francês que obteve alguns resultados sobre quadrados latinos, tendo demonstrado, nomeadamente, a conjectura de Euler da impossibilidade de solução do problema dos 36 oficiais.

⁹Raj Chandra Bose (1901–1987) matemático indiano que trabalhou em teoria dos designs e teoria dos códigos com correção de erros.

¹⁰Sharadchandra Shankar Shrikhande (nasceu em 1917), matemático indiano que desenvolveu trabalho sobre geometrias finitas, quadrados latinos e teoria dos grafos.

¹¹Ernest Tilden Parker (1926–1991) foi um matemático americano com vários trabalhos em combinatória, quadrados latinos e teoria dos designs.

Um modo imediato de verificar se dois quadrados latinos de ordem n são ou não ortogonais, consiste em determinar a matriz dos pares de símbolos que se obtêm, para as entradas de ambos, e verificar se esta matriz tem ou não todas as n^2 entradas distintas. Por exemplo, considerando o par de quadrados latinos

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix}$$

e construindo a matriz

$$C = \begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{bmatrix}, \quad (8.22)$$

uma vez que todos os pares ordenados representados nas entradas da matriz C são distintos, podemos concluir que os quadrados latinos A e B são ortogonais.

Teorema 8.23. *Seja p primo e considere-se o corpo finito $(\mathbb{Z}_p, \oplus, \odot)$. Se $q \in \mathbb{Z}_p \setminus \{0\}$, então a matriz L^q tal que*

$$\forall_{i,j \in \mathbb{Z}_p} L_{ij}^q = (q \odot i) \oplus j$$

define um quadrado latino. Adicionalmente, $\forall r, s \in \mathbb{Z}_p \setminus \{0\}$ tal que $r \neq s$ os quadrados latinos L^r e L^s são ortogonais.

Demonação. Supondo que $L_{i_1,j_1}^q = L_{i_2,j_2}^q$, vem que $(q \odot i_1) \oplus j_1 = (q \odot i_2) \oplus j_2$. Logo, uma vez que q é invertível em (\mathbb{Z}_p, \odot) e j é invertível em (\mathbb{Z}_p, \oplus) , segue-se que $i_1 = i_2$. Utilizando argumentos semelhantes, prova-se que se $L_{i_1,j_1}^q = L_{i_2,j_2}^q$ então $j_1 = j_2$.

Resta provar a ortogonalidade dos quadrados latinos L^r e L^s , para $r \neq s$. Assim, suponha que $\exists i_1, i_2, j_1, j_2 \in \mathbb{N}_p$ tais que $(i_1, j_1) \neq (i_2, j_2)$ e

$$L_{i_1,j_1}^r = L_{i_2,j_2}^r = \alpha \quad \text{e} \quad L_{i_1,j_1}^s = L_{i_2,j_2}^s = \beta.$$

Como consequência,

$$\begin{cases} (r \odot i_1) \oplus j_1 = \alpha \\ (r \odot i_2) \oplus j_2 = \alpha \end{cases} \Rightarrow r \odot (i_1 - i_2) = j_2 - j_1 \quad (8.23)$$

$$\begin{cases} (s \odot i_1) \oplus j_1 = \beta \\ (s \odot i_2) \oplus j_2 = \beta \end{cases} \Rightarrow s \odot (i_1 - i_2) = j_2 - j_1. \quad (8.24)$$

Se $i_1 = i_2$, então $j_1 = j_2$, o que contraria a hipótese de se ter $(i_1, j_1) \neq (i_2, j_2)$. Assim, podemos concluir que $i_1 \neq i_2$ e, consequentemente, que $i_1 - i_2$ tem inverso em (\mathbb{Z}_p, \odot) . Logo, resolvendo as equações (8.23) e (8.24) em ordem a r e s , respectivamente, vem

$$r = s = (i_1 - i_2)^{-1} \odot (j_2 - j_1).$$

Desta forma podemos concluir que se $r \neq s$, então os símbolos α e β apenas podem ocorrer numa única entrada, para ambos os quadrados latinos. \square

Teorema 8.24. *Se L' e L'' são quadrados latinos ortogonais, então os quadrados normalizados $(L')^*$ e $(L'')^*$ são também ortogonais.*

Demonstração. Seja $L' = (l'_{ij})_{i,j=1,\dots,n}$ e $L'' = (l''_{ij})_{i,j=1,\dots,n}$ e suponha que a normalização de L' é obtida à custa da permutação σ do conjunto de símbolos $\{1, \dots, n\}$, ou seja, $(L')^* = (\sigma(l'_{ij}))_{i,j=1,\dots,n}$. Analogamente, vamos admitir que a normalização de L'' é obtida à custa da permutação τ dos símbolos, ou seja, $(L'')^* = (\tau(l''_{ij}))_{i,j=1,\dots,n}$. Suponha ainda que existem i, j, k, l tais que

$$(\sigma(l'_{ij}), \tau(l''_{ij})) = (\sigma(l'_{kl}), \tau(l''_{kl})).$$

Então, uma vez que σ e τ são bijeções, vem que $l'_{ij} = l'_{kl}$ e $l''_{ij} = l''_{kl}$. Logo, tendo em conta a ortogonalidade de L' e L'' , conclui-se que $(i, j) = (k, l)$. \square

Com base no Teorema 8.23, conclui-se que, dado um primo p , podemos construir $p - 1$ quadrados latinos mutuamente ortogonais. Este número é maximal na sentido do teorema que se segue.

Teorema 8.25. *Se L_1, L_2, \dots, L_m são quadrados latinos mutuamente ortogonais de ordem n , então $m \leq n - 1$.*

Demonstração. Podemos assumir, pelo Teorema 8.24, que todos os m quadrados latinos estão na forma normalizada. Supondo que o conjunto de símbolos é $\{1, \dots, n\}$ e sendo $L_k = (l_{ij}^{(k)})_{i,j=1,\dots,n}$ vamos calcular, de dois modos distintos, a cardinalidade do conjunto

$$U = \{(i, j, k) : l_{ij}^{(k)} = 1\}.$$

Por um lado, a cardinalidade de U é igual ao número de uns em L_1, L_2, \dots, L_m , ou seja,

$$|U| = mn. \quad (8.25)$$

Por outro lado, todo o triplo da forma $(1, 1, k)$, para $1 \leq k \leq m$, pertence a U , e nenhum dos triplos da forma $(1, j, k)$ e $(i, 1, k)$, para $i, j \neq 1$, pertence a U . Finalmente, dados $i, j \neq 1$, não mais do que um triplo da forma (i, j, k) , pertence a U . Logo,

$$|U| \leq m + (n - 1)^2. \quad (8.26)$$

Combinando as fórmulas (8.25) e (8.26), vem que

$$mn \leq m + (n - 1)^2 \Leftrightarrow m \leq n - 1.$$

\square

Mais adiante, na Secção 9.4 mostraremos que para $n = p^q$, com p primo e $q \in \mathbb{N}$, existem $n - 1$ quadrados latinos mutuamente ortogonais.

Designa-se por *quadrado mágico*¹² toda a matriz quadrada de ordem n , em cujas entradas aparecem n^2 números inteiros sucessivos (usualmente $1, \dots, n^2$ ou $0, \dots, n^2 - 1$), de tal forma que a soma das entradas de cada linha ou coluna é constante.

Observe-se que adicionando uma constante a cada uma das entradas de um quadrado mágico de ordem n se obtém um novo quadrado mágico (com outros números). Logo, dado um quadrado mágico com números $0, \dots, n^2 - 1$, obtém-se um quadrado mágico com números $k, \dots, n^2 + k - 1$, para todo $k \in \mathbb{Z}$. Verifica-se, ainda, a existência de quadrados mágicos de qualquer ordem n , com exceção de $n = 2$.

A partir de dois quadrados latinos, podemos construir um quadrado mágico. Por exemplo, considerando os pares representados nas entradas da matriz (8.22) e substituindo cada par (x, y) pelo

¹²Os quadrados mágicos eram conhecidos dos chineses, por volta de 2200 a. C., dos árabes, cerca de 800 e dos europeus, aproximadamente em 1300 (existindo um quadrado mágico, num quadro de Albrecht Dürer com data de 1514).

número $\overline{xy} = 4x + y$ (ou seja, considerando cada par (x, y) como representando o número com dois dígitos xy na base 4, obtém-se o quadrado mágico:

0	5	10	15
7	2	13	8
9	12	3	6
14	11	4	1

, (8.27)

cuja soma em linha e coluna é $4(0+1+2+3)+(0+1+2+3)=30$. Neste caso, obteve-se um quadrado mágico com números entre 0 e 15, cuja soma em linha e em coluna é igual a 30. Mais geralmente, utilizando este procedimento, a partir de dois quadrados latinos ortogonais de ordem n podemos obter um quadrado mágico (também de ordem n) com números entre 0 e $(n+1)(n-1)$ e soma

$$(0+1+2+\cdots+(n-1))(n+1) = \frac{n(n-1)}{2}(n+1).$$

Os quadrados mágicos cuja soma ao longo das diagonais é igual à soma em linha (e, consequentemente, em coluna) designam-se por *quadrados mágicos perfeitos*. Tais quadrados mágicos podem ser obtidos a partir de pares de quadrados latinos ortogonais, nos quais não existem dois elementos iguais em qualquer das diagonais. Por exemplo, considerando os quadrados latinos ortogonais

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix},$$

obtém-se o seguinte quadrado mágico perfeito

0	5	10	15
11	14	1	4
13	8	7	2
6	3	12	9

.

Existem algoritmos para gerar quadrados mágicos perfeitos de ordem $n \neq 2$, os quais se podem dividir em três casos distintos:

1. n ímpar,
2. $n \equiv 0 \pmod{4}$,
3. $n \equiv 2 \pmod{4}$.

Por simplicidade de cálculo, vamos adoptar os números $0, 1, \dots, n-1$, para índices das n linhas e das n colunas.

1º caso. Para n ímpar, o método mais conhecido é o método de *de la Loubere*¹³. Com este método, distribuem-se sucessivamente os números $1, 2, \dots, n^2$, a partir da entrada central da linha 0, com deslocamentos consecutivos, da entrada (i, j) para a entrada $(i-1 \pmod n, j+1 \pmod n)$, desde que esta última entrada ainda não esteja ocupada. Caso contrário, o deslocamento é feito para a entrada $(i+1 \pmod n, j)$.

Como exemplo, vamos determinar um quadrado mágico de ordem 5. Começamos por colocar o número 1 na entrada central da linha 0 (entrada $(0, 2)$ de A_1), segue-se o número 2 na entrada $(-1 \pmod 5, 3 \pmod 5) = (4, 3)$ e os números 3, 4 e 5 nas entradas obtidas de modo idêntico (ver A_2).

¹³Antoine de la Loubere, um aristocrata francês que criou este método em 1687–1688.

Uma vez que a partir de $(1, 1)$ não podemos continuar (note-se que a entrada $(0, 2)$ já está ocupada), de acordo com o método de la Loubere, passamos para a entrada $(2, 1)$ onde se coloca o número 6 (ver A_3).

$A_1 =$	<table border="1"><tr><td></td><td>1</td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>		1																											$A_2 =$	<table border="1"><tr><td></td><td>1</td><td></td><td></td></tr><tr><td></td><td>5</td><td></td><td></td></tr><tr><td>4</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>3</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>2</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>		1				5			4							3								2					$A_3 =$	<table border="1"><tr><td></td><td>1</td><td></td><td></td></tr><tr><td></td><td>5</td><td></td><td></td></tr><tr><td>4</td><td>6</td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>3</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>2</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>		1				5			4	6						3								2				
	1																																																																																								
	1																																																																																								
	5																																																																																								
4																																																																																									
			3																																																																																						
			2																																																																																						
	1																																																																																								
	5																																																																																								
4	6																																																																																								
			3																																																																																						
			2																																																																																						

O procedimento anteriormente referido repete-se para a distribuição dos restantes números pelas restantes entradas, conforme se indica em A_4 , A_5 e A_6 .

$A_4 =$	<table border="1"><tr><td></td><td>1</td><td>8</td><td></td></tr><tr><td></td><td>5</td><td>7</td><td></td></tr><tr><td>4</td><td>6</td><td></td><td></td></tr><tr><td>10</td><td></td><td></td><td>3</td></tr><tr><td></td><td></td><td>2</td><td>9</td></tr></table>		1	8			5	7		4	6			10			3			2	9	$A_5 =$	<table border="1"><tr><td></td><td>1</td><td>8</td><td></td></tr><tr><td></td><td>5</td><td>7</td><td></td></tr><tr><td>4</td><td>6</td><td></td><td></td></tr><tr><td>10</td><td></td><td></td><td>3</td></tr><tr><td>11</td><td></td><td>2</td><td>9</td></tr></table>		1	8			5	7		4	6			10			3	11		2	9	$A_6 =$	<table border="1"><tr><td>17</td><td>24</td><td>1</td><td>8</td><td>15</td></tr><tr><td>23</td><td>5</td><td>7</td><td>14</td><td>16</td></tr><tr><td>4</td><td>6</td><td>13</td><td>20</td><td>22</td></tr><tr><td>10</td><td>12</td><td>19</td><td>21</td><td>3</td></tr><tr><td>11</td><td>18</td><td>25</td><td>2</td><td>9</td></tr></table>	17	24	1	8	15	23	5	7	14	16	4	6	13	20	22	10	12	19	21	3	11	18	25	2	9
	1	8																																																																				
	5	7																																																																				
4	6																																																																					
10			3																																																																			
		2	9																																																																			
	1	8																																																																				
	5	7																																																																				
4	6																																																																					
10			3																																																																			
11		2	9																																																																			
17	24	1	8	15																																																																		
23	5	7	14	16																																																																		
4	6	13	20	22																																																																		
10	12	19	21	3																																																																		
11	18	25	2	9																																																																		

Formalmente, este método pode representar-se pelo Algoritmo 8.3 que designamos por DELALOUBERE.

Algoritmo 8.3: DELALOUBERE(n)

```

 $QM \leftarrow 0$ 
 $x \leftarrow \lfloor n/2 \rfloor - 1; y \leftarrow 1$ 
para  $i \leftarrow 1$  até  $n^2$ 
  fazer  $\begin{cases} x' \leftarrow (x + 1) \bmod n; y' \leftarrow (y - 1) \bmod n \\ \text{se } QM[x', y'] <> 0 \\ \quad \text{então } x' \leftarrow x; y' \leftarrow (y + 1) \bmod n \\ QM[x', y'] \leftarrow i \end{cases}$ 
devolver ( $QM$ )

```

Aplicando este método, para $n = 7$ e $n = 9$, obtém-se os quadrados mágicos perfeitos que a seguir se indicam.

30	39	48	1	10	19	28
38	47	7	9	18	27	29
46	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

47	58	69	80	1	12	23	34	45
57	68	79	9	11	22	33	44	46
67	78	8	10	21	32	43	54	56
77	7	18	20	31	42	53	55	66
6	17	19	30	41	52	63	65	76
16	27	29	40	51	62	64	75	5
26	28	39	50	61	72	74	4	15
36	38	49	60	71	73	3	14	25
37	48	59	70	81	2	13	24	35

Para $n = 3$, o único quadrado mágico perfeito existente (a menos de rotações e reflexões) e que é conhecido desde a antiga China, designa-se por *Lo Shu*, e tem o aspecto

8	1	6
3	5	7
4	9	2

2º caso. Para $n \equiv 0 \pmod{4}$, pode adoptar-se o seguinte procedimento: inicialmente, distribuem-se os números $1, \dots, n^2$, segundo esta ordem, colocando-os, sucessivamente, nas entradas $(0, 0)$, $(0, 1)$, \dots ,

$(0, n - 1)$, $(1, 0)$, $(1, 1)$, ..., $(n - 1, n - 1)$, ou seja, preenchendo sucessivamente todas as linhas. Desta forma, na entrada (i, j) coloca-se o número $in + j + 1$. Seguidamente, os números x que estão nas entradas (i, j) , relativas à parte sombreada da Figura 8.3, são substituídos pelos números $n^2 + 1 - x$.

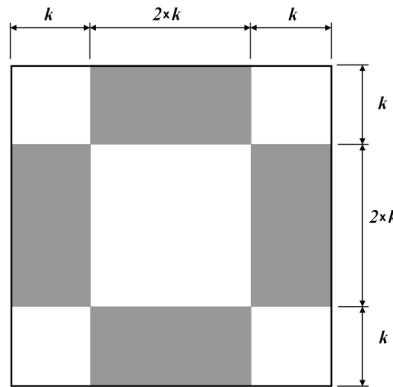


Figura 8.3: Determinação de quadrados mágicos perfeitos de ordem n , com $n \equiv 0 \pmod{4}$.

Por exemplo, para $n = 4$, as entradas correspondentes às entradas não sombreadas da Figura 8.3, são preenchidas conforme se apresenta em B_1 e as restantes entradas, juntamente com as primeiras, são apresentadas em B_2 .

$$B_1 = \begin{array}{|c|c|c|c|} \hline 1 & & & 4 \\ \hline & 6 & 7 & \\ \hline & 10 & 11 & \\ \hline 13 & & & 16 \\ \hline \end{array} \quad B_2 = \begin{array}{|c|c|c|c|} \hline 1 & 15 & 14 & 4 \\ \hline 12 & 6 & 7 & 9 \\ \hline 8 & 10 & 11 & 5 \\ \hline 13 & 3 & 2 & 16 \\ \hline \end{array}$$

Formalmente, este método pode representar-se pelo algoritmo Algoritmo 8.4 que é designado por QMÁGICO4.

Algoritmo 8.4: QMÁGICO4(n)

```

 $k \leftarrow n/4$ 
 $A \leftarrow \{x \in \mathbb{Z} : 0 \leq x \leq k - 1 \vee 3k \leq x \leq 4k - 1\}$ 
 $B \leftarrow \{x \in \mathbb{Z} : k \leq x \leq 3k - 1\}$ 
para  $i \leftarrow 0$  até  $n - 1$ 
  fazer para  $j \leftarrow 0$  até  $n - 1$ 
    fazer para  $x \leftarrow i * n + j + 1$ 
      se  $(i \in A \wedge j \in B) \vee (i \in B \wedge j \in A)$ 
        então  $x \leftarrow n^2 + 1 - x$ 
     $QM[i, j] \leftarrow x$ 
devolver ( $QM$ )
  
```

Aplicando este algoritmo, para $n = 8$, obtém-se o seguinte quadrado mágico perfeito:

1	2	62	61	60	59	7	8
9	10	54	53	52	51	15	16
48	47	19	20	21	22	42	41
40	39	27	28	29	30	34	33
32	31	35	36	37	38	26	25
24	23	43	44	45	46	18	17
49	50	14	13	12	11	55	56
57	58	6	5	4	3	63	64

3º caso. Para $n \equiv 2 \pmod{4}$, o número $\frac{n}{2}$ é ímpar e, utilizando o algoritmo de la Loubere, podemos determinar um quadrado mágico A de ordem $\frac{n}{2}$. Logo, colocando A em cada um dos quartos de um quadrado de ordem n , que denotamos por Q , obtém-se um quadrado com as mesmas somas ao longo das linhas, das colunas e das diagonais. Porém, os números do conjunto $\{1, \dots, \frac{n^2}{4}\}$ aparecem repetidos 4 vezes. Para resolver esta questão, vamos começar por introduzir uma matriz de ordem n que designamos por *matriz de factores* e denotamos por MF , cujas entradas são determinadas pelo Algoritmo 8.5 que se designa por QM6.

Algoritmo 8.5: QM6(i, j, n)

```

 $k \leftarrow n/2; t \leftarrow (k - 1)/2$ 
se  $i < t$  então  $r \leftarrow 3$ 
se  $i \geq t \wedge i < k$  então  $r \leftarrow 0$ 
se  $i \geq k \wedge i \leq n - t$  então  $r \leftarrow 2$ 
se  $i > n - t$  então  $r \leftarrow 1$ 
se  $j = t \wedge i = 0$  então  $r \leftarrow 0$ 
se  $j = t \wedge i = t$  então  $r \leftarrow 3$ 
se  $j \geq k$  então  $r \leftarrow 3 - r$ 
devolver ( $r$ )

```

Dado que $k = \frac{n}{2}$ e $t = \frac{k-1}{2}$, este algoritmo é equivalente ao seguinte procedimento:

- Na i -ésima linha, com $0 \leq i \leq k - 1$, colocam-se, primeiro t números 3, depois $k - t$ números 0, seguidamente $k - t + 1$ números 2 e, finalmente, $t - 1$ números 1, com excepção da t -ésima linha, a qual se inicia com um número 0, depois t números 3, seguem-se $k - t - 1$ números 0, depois $k - t + 1$ números 2 e, finalmente, $t - 1$ números 1.
- Na i -ésima linha, com $k \leq i \leq n - 1$, os números são colocados tal como na $(i - k)$ -ésima linha, mas substituindo as entradas x por $3 - x$, com $x \in \{0, 1, 2, 3\}$.

Como exemplo, para $n = 10$, obtém-se $k = 5$, $t = 2$ e matriz de factores

$$MF = \begin{pmatrix} 3 & 3 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 \\ 3 & 3 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 \\ 0 & 3 & 3 & 0 & 0 & 2 & 2 & 2 & 2 & 1 \\ 3 & 3 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 \\ 3 & 3 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 \\ 0 & 0 & 3 & 3 & 3 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 3 & 3 & 3 & 1 & 1 & 1 & 1 & 2 \\ 3 & 0 & 0 & 3 & 3 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 3 & 3 & 3 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 3 & 3 & 3 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}$$

Finalmente, tendo em conta o quadrado Q e a matriz de factores MF obtidos como anteriormente se referiu, estamos em condições de determinar um quadrado mágico QM , fazendo

$$QM_{ij} = Q_{ij} + \frac{n^2}{4} MF_{ij}, \quad \text{para } 0 \leq i, j \leq n - 1.$$

Mais formalmente, a determinação de quadrados mágicos perfeitos, para $n \equiv 2 \pmod{4}$, pode fazer-se com recurso ao Algoritmo 8.6 que designamos por QMÁGICO6.

Algoritmo 8.6: QMÁGICO6(n)

```

 $k \leftarrow n/2; m \leftarrow k^2$ 
 $A \leftarrow \text{DELA LOUBERE}(k)$ 
para  $i \leftarrow 1$  até  $k - 1$ 
  fazer para  $j \leftarrow 1$  até  $k - 1$ 
    
$$\begin{cases} QM[i, j] \leftarrow A[i, j] + m * \text{QM6}(i, j, n) \\ QM[i + k, j] \leftarrow A[i, j] + m * \text{QM6}(i + k, j, n) \\ QM[i, j + k] \leftarrow A[i, j] + m * \text{QM6}(i, j + k, n) \\ QM[i + k, j + k] \leftarrow A[i, j] + m * \text{QM6}(i + k, j + k, n) \end{cases}$$

devolver ( $QM$ )
  
```

Como exemplo, apresentam-se dois quadrados mágicos perfeitos obtidos por aplicação deste algoritmo, um com $n = 6$ e outro com $n = 10$.

35	1	6	26	19	24
3	32	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	5	34	12	14	16
4	36	29	13	18	11

92	99	1	8	15	67	74	51	58	40
98	80	7	14	16	73	55	57	64	41
4	81	88	20	22	54	56	63	70	47
85	87	19	21	3	60	62	69	71	28
86	93	25	2	9	61	68	75	52	34
17	24	76	83	90	42	49	26	33	65
23	5	82	89	91	48	30	32	39	66
79	6	13	95	97	29	31	38	45	72
10	12	94	96	78	35	37	44	46	53
11	18	100	77	84	36	43	50	27	59

Finalmente, segue-se o Algoritmo 8.7, para a determinação de quadrados mágicos perfeitos, de ordem arbitrária n , o qual designamos por QUADRADO MÁGICO.

Algoritmo 8.7: QUADRADO MÁGICO(n)

```

se  $n = 2$  então devolver (“não existe”)
se  $n \bmod 2 = 1$  então  $QM \leftarrow \text{DELA LOUBERE}(n)$ 
se  $n \bmod 4 = 0$  então  $QM \leftarrow \text{QMÁGICO4}(n)$ 
se  $n \bmod 4 = 2$  então  $QM \leftarrow \text{QMÁGICO6}(n)$ 
devolver ( $QM$ )
  
```

8.7. Exercícios

- 8.1. Supondo que um tanque com a capacidade de 20 litros tem duas torneiras para encher e outras duas para esvaziar, em ambos os casos com débitos de 9 e 15 litros por minuto, e que as torneiras podem ser comandadas à distância com intervalos de tempo (entre a abertura e o fecho) que são múltiplos do minuto, indique um procedimento para se armazenarem apenas 12 litros (note que se pode comandar apenas uma par de torneiras para encher e para esvaziar).
- 8.2. Determine $d = \text{mdc}(672, 448)$ e determine dois inteiros x e y tais que $672x + 448y = d$.
- 8.3. Mostre que, dados dois números naturais m e n , se existem dois inteiros x e y tais que $mx + ny = 1$, então $\text{mdc}(m, n) = 1$.
- 8.4. Sendo $d = \text{mdc}(m, n)$, prove que existem inteiros p e q que satisfazem a equação $pm + qn = c$ se e somente se $d | c$.

- 8.5. Supondo que p é um número primo e x_1, \dots, x_n são números inteiros, prove que se $p|(x_1 \cdots x_n)$, então $p|x_i$ para algum $i \in \{1, \dots, n\}$.
- 8.6. Prove o *teorema fundamental da aritmética*, onde se estabelece que para qualquer inteiro positivo $n \geq 2$, a menos da ordem dos factores, a respectiva factorização em primos é única.
- 8.7. Prove que existe uma infinidade de números primos.
- 8.8. Prove que $\forall k \in \mathbb{N}$ existem k números compostos consecutivos.
- 8.9. Prove que dados dois números naturais $n, m \in \mathbb{N}$, se n é o número de elementos de um conjunto S e m é o número de subconjuntos de S , A_1, A_2, \dots, A_m , tais que $\forall x, y \in S$, com $x \neq y$, existe $i \in \{1, \dots, m\}$ tal que $x \in A_i \wedge y \notin A_i$ ou $x \notin A_i \wedge y \in A_i$, então $n \leq 2^m$.
- 8.10. Calcule $\varphi(n)$, para cada n tal que $150 \leq n \leq 160$.
- 8.11. Calcule o número de números inteiros positivos, não superiores a 860, que não são relativamente primos com 860.
- 8.12. Prove que dados dois inteiros positivos m e n ,

$$\text{mdc}(m, n) = 1 \Leftrightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

- 8.13. Prove o recíproco do teorema da inversão de Möbius, ou seja, se f é obtida de g pela equação $f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d})$, então a g pode obter-se de f pela equação

$$g(n) = \sum_{d|n} f(d).$$

- 8.14. Dado um número natural $n \geq 2$, considerando a equação linear nas variáveis x_d , com $d \in D_n = \{d \in \mathbb{N}_n : d|n\}$,

$$\sum_{d|n} x_d = n, \tag{8.28}$$

prove que $x_d = \varphi(d) + z\mu(d)$, com d percorrendo D_n , constitui uma solução inteira da equação (8.28), qualquer que seja $z \in \mathbb{Z}$.

- 8.15. Determine uma solução inteira não negativa para o sistema de equações:

$$\begin{array}{rclclclclclcl} x_1 & + & x_2 & & + & x_4 & & & + & x_8 & = & 8 \\ x_1 & & & & & & & & + & x_7 & = & 7 \\ x_1 & + & x_2 & + & x_3 & & & + & x_6 & & = & 6 \\ x_1 & & & & & + & x_5 & & & & = & 5 \\ x_1 & + & x_2 & & + & x_4 & & & & & & = & 4 \end{array}$$

- 8.16. Prove que \mathbb{Z}_m com as operações \oplus e \odot tem estrutura de *anel*, ou seja, as operações \oplus e \odot verificam as propriedades:

- (a) $x \oplus y = y \oplus x$ e $x \odot y = y \odot x$.
- (b) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ e $x \odot (y \odot z) = (x \odot y) \odot z$.
- (c) $x \oplus 0 = x$ e $x \odot 1 = x$.

- (d) $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$.
(e) $\forall z \in \mathbb{Z}_m$ existe um único elemento $-z \in \mathbb{Z}_m$ tal que $z \oplus (-z) = 0$.
- 8.17. Prove que a lei do cancelamento, válida em \mathbb{Z} , em geral, não se verifica em \mathbb{Z}_m .
- 8.18. Determine os elementos invertíveis de \mathbb{Z}_8 e \mathbb{Z}_{13} .
- 8.19. Calcule os inversos de 3 em \mathbb{Z}_7 , de 5 em \mathbb{Z}_{11} e de 7 em \mathbb{Z}_{15} .
- 8.20. Prove que se p é um número primo então \mathbb{Z}_p , munido com as operações \oplus e \odot , é um corpo, i.e., (\mathbb{Z}_p, \oplus) e $(\mathbb{Z}_p \setminus \{0\}, \odot)$ têm ambos estrutura de grupo comutativo e verifica-se a distributividade da multiplicação relativamente à adição (ou seja, $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$).
- 8.21. Considerando o produto de todos os elementos não nulos de \mathbb{Z}_p , onde p é um número primo, mostre que $(p-1)! \equiv -1 \pmod{p}$.
- 8.22. Determine as raízes racionais dos polinómios:
(a) $f(x) = 3x^4 - 4x^3 - 14x^2 - 4x + 3$;
(b) $g(x) = 2x^4 + 3x^3 - 4x^2 - 3x + 2$.
- 8.23. Sendo p primo e f o polinómio ciclotómico

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$
prove que $f(x) = (x-1)^{p-1}$ em $\mathbb{Z}_p[x]$.
- 8.24. Prove que o polinómio ciclotómico f é irreduzível em \mathbb{Q}
- 8.25. Resolva as equações:
(a) $12x + 5 = 0$, em \mathbb{Z}_{13} ;
(b) $7x + 3 = 0$, em \mathbb{Z}_{47} ;
- 8.26. Resolva o sistema de equações

$$\begin{array}{rcl} 12x &+& 31y = 2, \\ 2x &+& 89y = 23. \end{array}$$
em \mathbb{Z}_{127} .
- 8.27. Para os pares de polinómios $f, g \in \mathbb{Q}[x]$, calcule o quociente e o resto da divisão de f por g .
(a) $f(x) = x^5 - x^2 + 3$ e $g(x) = x^4 + 5$.
(b) $f(x) = x^3 + 1$ e $g(x) = x^2$.
(c) $f(x) = 3x^3 - 13x^2 + x - 2$ e $g(x) = 2x + 1$.
- 8.28. Verifique a redutibilidade de cada um dos polinómios de $\mathbb{Q}[x]$ a seguir indicados.
(a) $x^4 + 1$;
(b) $x^7 + 11x^3 - 33x + 22$;
(c) $x^3 + x^2 + x + 1$.
- 8.29. Construa um quadrado latino de ordem 10.

- 8.30. Prove que, a menos de permutações de linhas ou colunas,
- existe um único quadrado latino de ordem 1,
 - existe um único quadrado latino de ordem 2,
 - existe um único quadrado latino de ordem 3,
 - e existem quatro quadrados latinos de ordem 4.
- 8.31. Calcule o número de quadrados latinos de ordem 4.
- 8.32. Determine um quadrado latino normalizado de ordem 7.
- 8.33. Construa um conjunto de 4 quadrados latinos de ordem 5, mutuamente ortogonais.
- 8.34. A partir do quadrado mágico (8.27), onde se utilizam números entre 0 e 15, construa um quadrado mágico onde se utilizam números entre 1 e 16.
- 8.35. Construa um quadrado mágicos de ordem 5, com números entre 0 e 24.
- 8.36. Considere 7 moedas colocadas em círculo em cima de uma mesa com a mesma face voltada para cima. Supondo que cada mudança das faces só é válida quando acontece para 5 moedas (ao mesmo tempo), responda:
- É possível colocar todas as moedas com a outra face voltada para cima com uma sequência de mudanças válidas?
 - No caso da resposta anterior ser afirmativa, como deve proceder e quantas mudanças válidas são suficientes?
 - Responda às questões anteriores, admitindo que cada mudança de face só é válida quando se verifica para 4 moedas (ao mesmo tempo).

9

Designs Combinatórios e Geometrias Finitas

Existem muitas configurações combinatórias de objectos com aplicações práticas, cujo estudo e manipulação requerem uma atenção muito particular e uma utilização adequada de conceitos e resultados decorrentes do crescente desenvolvimento da teoria dos *designs* e das geometrias finitas. Neste capítulo, estudam-se os *designs* combinatórios, os planos afins, os espaços projectivos e respectivas relações com quadrados latinos e matrizes de Hadamard.

9.1. Designs combinatórios

Suponha que uma empresa com actividades internacionais tem uma equipa de k técnicos (escolhidos ciclicamente de entre os elementos de um quadro de v técnicos) permanentemente no estrangeiro, em actividades de apoio aos seus produtos. A constituição destas equipas é alterada todas as semanas de tal modo que cada técnico seja destacado o mesmo número λ de vezes. Nestas condições, estamos interessados em formar subconjuntos do conjunto de v técnicos, as equipas, de tal forma que

- cada equipa tenha cardinalidade k ;
- cada técnico deva ser destacado para λ equipas.

Por exemplo, supondo que se dispõe do conjunto de técnicos

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

pelo que $v = 8$, que cada equipa é constituída por 4 técnicos, donde $k = 4$, e ainda que cada técnico é destacado 3 vezes, logo $\lambda = 3$, obtém-se as equipas

$$\{a, b, c, d\}, \{e, f, g, h\}, \{a, c, e, g\}, \{b, d, f, h\}, \{a, b, d, g\}, \{c, e, f, h\}. \quad (9.1)$$

No caso geral, dizemos que o par (X, \mathcal{B}) define um 1-*design* com parâmetros (v, k, λ) , se X é um conjunto de cardinalidade v , \mathcal{B} é uma família de subconjuntos de X cada um dos quais com cardinalidade k e cada elemento $x \in X$ pertence exactamente a λ elementos de \mathcal{B} (neste caso diz-se também que (X, \mathcal{B}) é um *design 1 – (v, k, λ)*). Usualmente, os subconjuntos de X pertencentes a \mathcal{B} designam-se por *blocos*. O exemplo anterior é um 1-*design* $(8, 4, 3)$ (ou seja, um *design 1 – (8, 4, 3)*), cujos blocos são os representados em (9.1).

Dado um terno de parâmetros arbitrários, nem sempre existe um 1-*design* que lhe corresponda. Por exemplo, não existe nenhum *design* com os parâmetros $1 – (12, 9, 5)$. Na tabela a seguir representa-se o 1-*design* com parâmetros $(8, 4, 3)$, onde cada linha está associada a um elemento do conjunto $X = \{x_1, \dots, x_8\}$, com $x_1 = a, \dots, x_8 = h$, e cada coluna corresponde a um bloco de $\mathcal{B} = \{B_1, \dots, B_6\}$.

A entrada ij é igual a 1 se $x_i \in B_j$ e igual a 0 no caso contrário. A matriz com estas entradas designa-se por *matriz de incidência do design*. Nestas condições, adicionando as entradas de uma linha x_i obtém-se o número de réplicas de x_i nos diferentes blocos, o qual, por definição, é igual λ . Por outro lado, adicionando as entradas da coluna B_j , obtém-se a cardinalidade k de cada bloco.

x_i	B_1 $\{a, b, c, d\}$	B_2 $\{e, f, g, h\}$	B_3 $\{a, c, e, g\}$	B_4 $\{b, d, f, h\}$	B_5 $\{a, b, d, g\}$	B_6 $\{c, e, f, h\}$	λ
a	1	0	1	0	1	0	3
b	1	0	0	1	1	0	3
c	1	0	1	0	0	1	3
d	1	0	0	1	1	0	3
e	0	1	1	0	0	1	3
f	0	1	0	1	0	1	3
g	0	1	1	0	1	0	3
h	0	1	0	1	0	1	3
k	4	4	4	4	4	4	

Tabela 9.1: Representação de um 1-design com parâmetros $(8, 4, 3)$.

O teorema a seguir estabelece uma condição necessária e suficiente para a existência de um 1-design.

Teorema 9.1. *Existe um design com parâmetros $1 - (v, k, \lambda)$ se e só se*

$$k|\lambda v - e| \leq \binom{v}{k}. \quad (9.2)$$

Demonstração. Suponha que existe um 1-design (X, \mathcal{B}) com parâmetros (v, k, λ) . Tendo em conta a Tabela 9.1, é claro que $\sum_{x \in X} \lambda = k|\mathcal{B}|$ e, consequentemente, obtém-se a igualdade $v\lambda = kb$, onde b é o número dos blocos (isto é, $b = |\mathcal{B}|$). Adicionalmente, dado que o número total de blocos (de cardinalidade k) não pode exceder $\binom{v}{k}$, conclui-se também que

$$b = \frac{\lambda v}{k} \leq \binom{v}{k}.$$

Reciprocamente, suponha que os números naturais v , k e λ satisfazem as condições (9.2). Seja \mathcal{B} uma família de $\frac{\lambda v}{k}$ subconjuntos distintos de cardinalidade k (que designamos, simplesmente, por k -subconjuntos), constituídos por elementos de um v -conjunto X (pelo que, a desigualdade $\frac{\lambda v}{k} \leq \binom{v}{k}$ é essencial). Então os números de réplicas dos elementos $x \in X$, $r(x)$, satisfazem a equação

$$\sum_{x \in X} r(x) = |\mathcal{B}|k = \lambda v \quad (9.3)$$

(uma vez que o somatório $\sum_{x \in X} r(x)$ e $|\mathcal{B}|k$ são, respectivamente, o número de uns na matriz de incidência obtido somando todas as linhas e todas as colunas). Se $\forall_{x \in X} r(x) = \lambda$ então (X, \mathcal{B}) é um design com parâmetros $1 - (v, k, \lambda)$. Caso contrário, existem $x_1, x_2 \in X$, tais que $r(x_1) > \lambda > r(x_2)$ ¹.

¹Com efeito, se admitirmos que tal não acontece, então $\forall_{x \in X} r(x) \geq \lambda$ (ou $\forall_{x \in X} r(x) \leq \lambda$) e como existe pelo menos um elemento $x_1 \in X$ tal que $r(x_1) > \lambda$ ($x_2 \in X$ tal que $r(x_2) < \lambda$) vem que $\sum_{x \in X} r(x) > \lambda v$ ($\sum_{x \in X} r(x) < \lambda v$), o que contradiz a igualdade (9.3).

Seja $c_{1\bar{2}}$ o número de blocos que contêm x_1 mas não contêm x_2 . Seja $c_{\bar{1}2}$ o número de blocos que contêm x_2 mas não contêm x_1 . Seja c_{12} o número de blocos que contêm x_1 e x_2 . Então, $c_{12} = r(x_1) - c_{1\bar{2}}$ e $c_{\bar{1}2} = r(x_2) - c_{12}$, e, consequentemente, $c_{1\bar{2}} - c_{\bar{1}2} = r(x_1) - r(x_2) > 0$.

Seja J_{12} o conjunto de índices tal que os blocos $B_j \in \mathcal{B}$, com $j \in J_{12}$, são os que contêm x_1 mas não x_2 e, para cada $j \in J_{12}$, seja $B_j^* = (B_j \setminus \{x_1\}) \cup \{x_2\}$. Nestas condições, os blocos B_j^* obtidos contêm x_2 e não contêm x_1 e, uma vez que $c_{12} > c_{\bar{1}2}$ existe pelo menos um B_j^* que não pertence à coleção original. Seja $B_{j^*}^*$ um tal bloco. Removendo B_j de \mathcal{B} e substituindo-o por $B_{j^*}^*$ obtém-se uma nova família \mathcal{B}^* de k -subconjuntos de X tal que os números de réplicas de x , $r^*(x)$, em \mathcal{B}^* , são os mesmos com exceção de x_1 e x_2 , para os quais se verifica

$$\begin{aligned} r^*(x_1) &= r(x_1) - 1, \\ r^*(x_2) &= r(x_2) + 1. \end{aligned}$$

Caso a família obtida, \mathcal{B}^* , seja um 1-design, o problema está resolvido. Caso contrário o procedimento repete-se.

Deste modo, de passo para passo, vamos convergindo para um 1-design, com a sucessiva aproximação de duas réplicas entre si. Consequentemente, ao fim de um número finito de passos todos os números de réplicas são iguais, obtendo-se um 1-design. \square

Exemplo 9.1. Tendo em conta que este teorema tem uma demonstração construtiva, vamos utilizar a técnica de construção de 1-designs, sugerida na demonstração, na construção de um design com os parâmetros $1-(10, 5, 3)$.

Solução. Note-se que este 1-design existe, uma vez que $5|10 \cdot 3$ e $\frac{10 \cdot 3}{5} \leq \binom{10}{5} = 252$. Vamos começar por apresentar uma família de $\frac{10 \cdot 3}{5} = 6$ subconjuntos de $X = \{1, 2, \dots, 10\}$ com cardinalidade 5, ou seja, $\mathcal{B} = \{B_1, B_2, B_3, B_4, B_5, B_6\}$, cuja matriz de incidências (x, B_j) se representa na Tabela 9.2.

x	B_1	B_2	B_3	B_4	B_5	B_6	$r(x)$
1	1	0	1	0	1	1	4
2	1	0	0	1	1	0	3
3	1	0	1	0	1	0	3
4	1	0	0	1	0	0	2
5	1	0	1	0	0	1	3
6	0	1	0	1	1	1	4
7	0	1	1	0	1	1	4
8	0	1	0	1	0	0	2
9	0	1	1	0	0	1	3
10	0	1	0	1	0	0	2

Tabela 9.2: Representação da família \mathcal{B} de subconjuntos $X = \{1, 2, \dots, 10\}$.

1^a iteração. Começamos por escolher $x_1, x_2 \in X$ tais que $r(x_1) > 3 > r(x_2)$. Para tal, basta fazer $x_1 = 1$ e $x_2 = 4$ (com os quais se obtém $4 = r(1) > r(4) = 2$). Considerem-se os subconjuntos B_j , com $j \in J_{14}$, que contêm 1 mas não contêm 4 (que são, precisamente, B_3, B_5 e B_6) e determinem-se os conjuntos $B_j^* = (B_j \setminus \{1\}) \cup \{4\}$, ou seja, $B_3^* = \{3, 4, 5, 7, 9\}$, $B_5^* = \{2, 3, 4, 6, 7\}$ e $B_6^* = \{4, 5, 6, 7, 9\}$. Fazendo $B_{j^*}^* = B_3^*$ e substituindo em \mathcal{B} , B_3 por B_3^* , obtém-se a Tabela 9.3.

2^a iteração. Escolher $x_1, x_2 \in X$ tais que $r(x_1) > 3 > r(x_2)$. Seja $x_1 = 6$ e $x_2 = 8$ (com os quais se obtém $4 = r(6) > r(8) = 2$). Considerem-se os subconjuntos B_j que contêm 6 mas não contêm 8

x	B_1	B_2	B_3	B_4	B_5	B_6	$r(x)$
1	1	0	0	0	1	1	3
2	1	0	0	1	1	0	3
3	1	0	1	0	1	0	3
4	1	0	1	1	0	0	3
5	1	0	1	0	0	1	3
6	0	1	0	1	1	1	4
7	0	1	1	0	1	1	4
8	0	1	0	1	0	0	2
9	0	1	1	0	0	1	3
10	0	1	0	1	0	0	2

Tabela 9.3: 1^a actualização da Tabela 9.2.

(que são B_5 e B_6) e determinem-se os conjuntos $B_j^* = (B_j \setminus \{6\}) \cup \{8\}$, ou seja, $B_5^* = \{1, 2, 3, 7, 8\}$ e $B_6^* = \{1, 5, 7, 8, 9\}$. Fazendo $B_{j^*}^* = B_5^*$ e substituindo em \mathcal{B} , B_5 por B_5^* obtém-se a Tabela 9.4.

x	B_1	B_2	B_3	B_4	B_5	B_6	$r(x)$
1	1	0	0	0	1	1	3
2	1	0	0	1	1	0	3
3	1	0	1	0	1	0	3
4	1	0	1	1	0	0	3
5	1	0	1	0	0	1	3
6	0	1	0	1	0	1	3
7	0	1	1	0	1	1	4
8	0	1	0	1	1	0	3
9	0	1	1	0	0	1	3
10	0	1	0	1	0	0	2

Tabela 9.4: 2^a actualização da Tabela 9.2.

3^a iteração. Escolher $x_1, x_2 \in X$ tais que $r(x_1) > 3 > r(x_2)$. Seja $x_1 = 7$ e $x_2 = 10$ (com os quais se obtém $4 = r(7) > r(10) = 2$). Considerem-se os subconjuntos B_j que contêm 7 mas não contêm 10 (que são, B_3 , B_5 e B_6) e determinem-se os conjuntos $B_j^* = (B_j \setminus \{7\}) \cup \{10\}$, ou seja, $B_3^* = \{3, 4, 5, 9, 10\}$, $B_5^* = \{1, 2, 3, 8, 10\}$ e $B_6^* = \{1, 5, 6, 9, 10\}$. Fazendo $B_{j^*}^* = B_5^*$ e substituindo em \mathcal{B} , B_5 por B_5^* obtém-se a Tabela 9.5.

x	B_1	B_2	B_3	B_4	B_5	B_6	$r(x)$
1	1	0	0	0	1	1	3
2	1	0	0	1	1	0	3
3	1	0	1	0	1	0	3
4	1	0	1	1	0	0	3
5	1	0	1	0	0	1	3
6	0	1	0	1	0	1	3
7	0	1	1	0	0	1	3
8	0	1	0	1	1	0	3
9	0	1	1	0	0	1	3
10	0	1	0	1	1	0	3

Tabela 9.5: 3^a actualização da Tabela 9.2.

Desta forma obtém-se os blocos

$$\mathcal{B} = \{\{1, 2, 3, 4, 5\}, \{6, 7, 8, 9, 10\}, \{3, 4, 5, 7, 9\}, \{2, 4, 6, 8, 10\}, \{1, 2, 3, 8, 10\}, \{1, 5, 6, 7, 9\}\}$$

que formam um *1-design* (X, \mathcal{B}) , com parâmetros $(10, 5, 3)$. \square

O conceito de *1-design* pode ser generalizado de acordo com a definição que se segue.

Definição 9.1 (*Design t – (v, k, λ)*). *Dados os inteiros positivos t, k, v e λ tais que t < k < v, o par (X, \mathcal{B}) diz-se um design t – (v, k, λ), ou t-design com parâmetros (v, k, λ) , se X é um conjunto de cardinalidade v e \mathcal{B} é uma coleção de k-subconjuntos de X, designados por blocos, onde quaisquer t elementos de X estão contidos em exactamente λ blocos.*

Neste contexto mais geral, é usual designar-se, simplesmente, por *design* (v, k, λ) , um *design* com parâmetros $2 – (v, k, \lambda)$.

Teorema 9.2. *Se (X, \mathcal{B}) é um design t – (v, k, λ), então o número de blocos b vem dado por*

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}. \quad (9.4)$$

Demonstração. Contando de dois modos distintos o número de todos os t-subconjuntos de X em todos os blocos, conclui-se que existem $\binom{v}{t}$ t-subconjuntos de X, cada um dos quais está contido em λ blocos e, por sua vez, existem b blocos cada um contendo $\binom{k}{t}$ t-subconjuntos. Logo,

$$b \binom{k}{t} = \lambda \binom{v}{t}$$

o que implica (9.4). \square

Teorema 9.3. *Seja (X, \mathcal{B}) um t-design com parâmetros (v, k, λ) . Dado $s \leq t$, seja S um s-subconjunto de X, $X' = X \setminus S$ e $\mathcal{B}' = \{A \setminus S : S \subseteq A, A \in \mathcal{B}\}$, ou seja, considere-se a família \mathcal{B}' constituída por todos os blocos que contêm S, depois de se remover S de cada um deles. Então (X', \mathcal{B}') é um $(t-s)$ -design com parâmetros $(v-s, k-s, \lambda)$.*

Demonstração. Existem $v-s$ pontos em X' e cada bloco de \mathcal{B}' contém $k-s$ elementos. Seja Y um subconjunto de $X \setminus S$ com cardinalidade $t-s$. Então $Y \cup S$ é um t-subconjunto de X, pelo que pertence a λ blocos de \mathcal{B} os quais, retirando S, passam a ser blocos de \mathcal{B}' que contêm Y. \square

Corolário 9.4. *Para $s \leq t$, qualquer t-design com parâmetros (v, k, λ) é também um design s – (v, k, λ_s) , onde*

$$\lambda_s = \lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

Demonstração. Seja (X, \mathcal{B}) um design t – (v, k, λ). Então, dado um s-subconjunto $S \subseteq X$, pelo Teorema 9.3, $(X \setminus S, \mathcal{B}')$ (com \mathcal{B}' definido como anteriormente) é um design $(t-s) – (v-s, k-s, \lambda)$, com λ_s blocos, cada um dos quais reunido com S é um bloco de \mathcal{B} . Assim, o s-subconjunto S está contido em λ_s blocos do t-design (v, k, λ) , (X, \mathcal{B}) , pelo que (X, \mathcal{B}) é também um design s – (v, k, λ_s) . \square

Corolário 9.5. *Se (X, \mathcal{B}) é um t-design com parâmetros (v, k, λ) , então cada $x \in X$ pertence a r blocos, onde*

$$r = \lambda \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}. \quad (9.5)$$

Demonstração. Seja (X, \mathcal{B}) um design t – (v, k, λ). Então, pela Corolário 9.4, para $s = 1$, (X, \mathcal{B}) é também um design 1 – (v, k, λ_1) e, por definição, cada $x \in X$ pertence a λ_1 blocos. \square

Segue-se uma condição necessária para a existência de *designs* $2 - (v, k, \lambda)$, conhecida por desigualdade de Fischer².

Teorema 9.6 (Desigualdade de Fischer). *Se (X, \mathcal{B}) é um 2-design (v, k, λ) , então $|\mathcal{B}| \geq v$.*

Demonstração. Para $t = 2$ a formula (9.5) implica

$$r = \lambda \frac{v-1}{k-1}. \quad (9.6)$$

Seja M a matriz de incidência do *design* $2 - (v, k, \lambda)$ a que corresponde o par (X, \mathcal{B}) , com $X = \{x_1, \dots, x_v\}$. Então MM^T é uma matriz quadrada de ordem v tal que

$$(MM^T)_{ij} = \sum_{k=1}^b (M)_{ik}(M^T)_{kj} = \sum_{k=1}^b (M)_{ik}(M)_{jk}$$

corresponde ao número de blocos que contêm x_i e x_j que, por sua vez, é igual ao número de réplicas de x_i , r , se $i = j$ e igual a λ se $i \neq j$. Calculando o determinante de MM^T , vem

$$\begin{aligned} \det(MM^T) &= \begin{vmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{vmatrix} \\ &= \begin{vmatrix} r + (v-1)\lambda & r + (v-1)\lambda & \dots & r + (v-1)\lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{vmatrix} \quad (9.7) \end{aligned}$$

$$\begin{aligned} &= (r + (v-1)\lambda) \begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & r-\lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & r-\lambda \end{vmatrix} \quad (9.8) \\ &= rk(r-\lambda)^{v-1}, \quad (9.9) \end{aligned}$$

tendo em conta que a igualdade (9.7) se obtém adicionando à primeira linha todas as outras, a igualdade (9.8) se obtém subtraindo λ vezes a primeira linha a todas as outras, depois de se pôr em evidência $(r + (v-1)\lambda)$ e, finalmente, que a igualdade (9.9) decorre de (9.6) e do cálculo do determinante da matriz triangular superior. Como consequência, a matriz MM^T é não singular, pelo que a sua característica é v . Assim, dado que a característica de MM^T é não superior à característica de M que, por sua vez, é não superior ao seu número b de colunas, conclui-se que $v \leq b$. \square

Deve observar-se que não é possível garantir a existência (ou não existência) de t -*designs* arbitrários. Apenas se conhecem alguns resultados para tipos particulares de *designs*, como é o caso dos 1-*designs*, anteriormente considerados.

Definição 9.2 (Design simétrico). *Designa-se por design simétrico um $2-(v, k, \lambda)$ design, (X, \mathcal{B}) , tal que $|\mathcal{B}| = b = v$.*

²Ernst Sigismund Fischer (1875–1954), matemático austríaco com trabalho de relevo em teoria da integração de Lebesgue.

Por outras palavras, um $2 - (v, k, \lambda)$ design, (X, \mathcal{B}) , é simétrico se o número de blocos é igual à cardinalidade de X . De modo equivalente, também se pode afirmar que (X, \mathcal{B}) é um $2 - (v, k, \lambda)$ design simétrico, se $k = r$, onde r denota o número de réplicas de cada elemento $x \in X$, ou seja, r é o número de blocos que contêm um elemento $x \in X$. Com efeito, tendo em conta o Teorema 9.2,

$$b = \lambda \frac{v(v-1)}{k(k-1)}. \quad (9.10)$$

Combinando (9.10) com (9.6), obtém-se a igualdade pretendida. Assim, também se diz que um 2 -design (X, \mathcal{B}) é simétrico quando a cardinalidade de cada bloco é igual ao número de blocos que contêm um elemento $x \in X$.

Um $design t - (v, k, \lambda)$, com $\lambda = 1$, designa-se por *sistema de Steiner* e denota-se por $S(t, v, k)$. Tanto quanto se sabe, ainda não se determinaram sistemas de Steiner com $t > 5$ e os únicos sistemas de Steiner já determinados, com $t = 5$ são: $S(5, 12, 6)$, $S(5, 24, 8)$, $S(5, 24, 6)$, $S(5, 48, 6)$, $S(5, 84, 6)$, $S(5, 28, 7)$ e $S(5, 72, 6)$. Por outro lado, os únicos sistemas de Steiner $S(4, v, k)$ conhecidos são os que decorrem dos sistemas de Steiner $S(5, v, k)$ já determinados.

Os casos particulares de sistemas de Steiner $S(2, v, 3)$, designam-se por sistemas de *triplos de Steiner* e denotam-se, usualmente, por $STS(v)$ (ou seja, $STS(v)$ é um $2 - (v, 3, 1)$). Por exemplo, os blocos $\{1, 2, 3\}$, $\{4, 5, 6\}$, $\{7, 8, 9\}$, $\{1, 4, 7\}$, $\{1, 6, 8\}$, $\{1, 5, 9\}$, $\{2, 5, 8\}$, $\{3, 6, 9\}$, $\{2, 4, 9\}$, $\{3, 5, 7\}$, $\{2, 6, 7\}$, $\{3, 4, 8\}$, constituem um sistema de triplos de Steiner $STS(9)$.

Vamos apresentar um algoritmo para a determinação de sistemas de triplos de Steiner, adoptando uma abordagem idêntica à seguida em [62]. Antes porém, convém introduzir o seguinte resultado.

Lema 9.7. Se (X, \mathcal{B}) é um $STS(n)$, então qualquer elemento $x \in X$ ocorre exactamente em $r = \frac{n-1}{2}$ blocos e o número de blocos é $|\mathcal{B}| = \frac{n(n-1)}{6}$.

Demonstração. Seja \mathcal{B}_x o conjunto dos blocos que contêm um elemento arbitrário $x \in X$. Então $X = \bigcup_{B \in \mathcal{B}_x} B$ e, dado que $\forall B', B'' \in \mathcal{B}_x \quad B' \cap B'' \neq \emptyset$, podemos concluir que $|\mathcal{B}_x| = \frac{n-1}{2}$, o que prova a primeira parte. Por sua vez, a prova de que o número de blocos é $\frac{n(n-1)}{6}$ decorre da igualdade $3|\mathcal{B}| = rn$. \square

Como consequência imediata deste lema, dado $n \in \mathbb{N}$, se $STS(n)$ existe então

$$n \equiv \begin{cases} 1 & (\text{mod } 6) \\ \text{ou} \\ 3 & (\text{mod } 6). \end{cases} \quad (9.11)$$

Na verdade provou-se, há mais de 100 anos, que existe um $STS(n)$ se e somente se a relação de congruência (9.11) se verifica. A prova da suficiência da condição (9.11) é construtiva, conduzindo-nos a um método para a determinação de pelo menos um $STS(n)$, qualquer que seja n admissível (i. e., que verifique (9.11)).

Designa-se por *sistema de triplos de Steiner parcial* um par (X, \mathcal{B}) , onde \mathcal{B} é uma família de blocos de X de cardinalidade 3, relativamente à qual, cada par de pontos de X está contido, no máximo, num único bloco. Sendo $|X| = n$, um tal sistema de triplos de Steiner parcial denota-se por $STSP(n)$, designando-se o seu número de blocos por *tamanho* do $STSP(n)$ (note-se que sendo $X = [n]$, com $n \geq 3$, e $\mathcal{B} = \{\{1, 2, 3\}\}$, o par (X, \mathcal{B}) corresponde a um $STSP(n)$ de tamanho 1). É fácil concluir que qualquer $STSP(n)$ tem, no máximo, $\frac{n(n-1)}{6}$ blocos e que atingindo este número é um $STS(n)$. Assim, podemos considerar o problema da determinação de um $STS(n)$ como um problema de optimização combinatória.

Seja $\mathcal{FB}(X)$ o conjunto de todas as famílias \mathcal{B} de blocos para as quais o par (X, \mathcal{B}) é um $STSP(n)$. Logo, qualquer $STS(n)$ fica determinado por uma família $\mathcal{B}^* \in \mathcal{FB}(X)$ de blocos tal que

$$|\mathcal{B}^*| = \max\{|\mathcal{B}| : \mathcal{B} \in \mathcal{FB}(X)\},$$

sabendo-se que $|\mathcal{B}^*| = \frac{n(n-1)}{6}$.

- Seja (X, \mathcal{B}) um $STSP(n)$ arbitrário. Um elemento $x \in X$ diz-se um *ponto vivo* se $r(x) < \frac{n-1}{2}$ (onde $r(x)$ denota o número de réplicas de x , i. e., o número de blocos de \mathcal{B} em que x ocorre). Um par de elementos de X distintos, (x, y) , diz-se um *par vivo* se não existe nenhum bloco $B \in \mathcal{B}$ tal que $\{x, y\} \subseteq B$.
- Se o $STSP(n)$ tem tamanho inferior a $\frac{n(n-1)}{6}$, então existe um ponto vivo. Adicionalmente, sendo x um ponto vivo, então existem, pelo menos, dois elementos $y, z \in X$ ($y \neq z$) tais que os pares (x, y) e (x, z) são ambos pares vivos (tal acontece porque $r(x) \leq \frac{(n-3)}{2}$ e, consequentemente, x ocorre nos diferentes blocos com, no máximo, $n - 3$ elementos distintos de x).

A pesquisa exaustiva dos pontos e pares de pontos vivos, pode provocar o que se designa por *explosão combinatória*. Em alternativa a uma pesquisa exaustiva dos pontos e pares de pontos vivos, vamos apresentar um algoritmo heurístico, o qual vamos designar por AHSTS e que tem como argumentos de entrada um par (X, \mathcal{B}) , definindo um $STSP(n)$. Com este algoritmo heurístico, a partir de escolhas aleatórias de pontos vivos x e de elementos $y, z \in X$ tais que (y, x) e (x, z) são pares vivos, sempre que possível, incrementa-se a cardinalidade do $STSP(n)$ corrente e, quando tal não é possível, um dos blocos é substituído por um bloco novo. Com esta estratégia, espera-se que a aleatoriedade das escolhas e, a substituição de alguns blocos por outros, proporcione uma aproximação ao sistema de triplos de Steiner pretendido.

Algoritmo 9.1: AHSTS(X, \mathcal{B})

```

enquanto  $|\mathcal{B}| < \frac{|X|(|X|-1)}{6}$ 
    escolher um ponto vivo  $x \in X$ 
    escolher  $y, z \in X$  tais que  $(y, x), (x, z)$  são pares vivos
    fazer {
        se  $(y, z)$  é par vivo
            então  $\mathcal{B} \leftarrow \mathcal{B} \cup \{\{x, y, z\}\}$ 
        senão
            sendo  $B \in \mathcal{B}$  tal que  $y, z \in B$ ,
             $\mathcal{B} \leftarrow (\mathcal{B} \setminus \{B\}) \cup \{\{x, y, z\}\}$ 
    devolver  $(\mathcal{B})$ 
}

```

9.2. Planos projectivos e afins

Já foi referido anteriormente que existem vários tipos de geometrias, as quais decorrem dos axiomas utilizados. Nesta secção vamos analisar, essencialmente, as propriedades combinatórias de dois casos particulares de geometrias finitas, as quais são introduzidas como estruturas de incidência.

Definição 9.3 (Estrutura de incidência). *Uma estrutura de incidência é um triplo da forma $S = (P, L, I)$, onde*

1. *P é um conjunto não vazio, cujos elementos se designam por pontos;*
2. *L é um conjunto não vazio, cujos elementos se designam por blocos (os quais, neste texto, correspondem a subconjuntos de P);*
3. *I é uma relação de P para L, ou seja, $I \subseteq P \times L$, que se designa por relação da incidência de blocos em pontos (ou relação de pertença de pontos a blocos).*

A estrutura dual de uma estrutura de incidência $S = (P, L, I)$ é a estrutura de incidência $\bar{S} = (P, L, \bar{I})$, onde $\bar{I} \subseteq L \times P$ é tal que $\bar{I} = \{(b, p) : (p, b) \in I\}$.

Exemplo 9.2. Seja (X, \mathcal{B}) um design $t - (v, k, \lambda)$. Vamos mostrar que (X, \mathcal{B}, \in) é uma estrutura de incidência com $|X|$ pontos e $|\mathcal{B}|$ blocos.

Solução. Sendo $P = X$ e $L = \mathcal{B}$ podemos ver que cada bloco é incidente com k elementos (pontos) distintos, e cada subconjunto de t pontos distintos é incidente com exactamente λ pontos. \square

Como exemplo de estrutura de incidência podemos apresentar a geometria.

Definição 9.4 (Geometria). Uma geometria é uma estrutura de incidência (P, L, \in) , onde P denota o conjunto de pontos, L o conjunto de rectas (ou seja, conjunto de subconjuntos de P) e \in a relação de incidência entre rectas e pontos, satisfazendo os seguintes axiomas:

- A_1 para cada par de pontos distintos $p_1, p_2 \in P$, existe uma única recta $l \in L$ que incide em ambos os pontos p_1 e p_2 (ou seja, tal que $p_1, p_2 \in l$);
- A_2 existem, pelo menos, quatro pontos tais que quaisquer três deles não estão incluídos numa recta;
- A_3 cada recta $l \in L$ contém pelo menos dois pontos (ou seja, $|l| \geq 2$).

Neste caso, escreve-se $G = (P, L)$ para indicar que a geometria G tem P como conjunto dos pontos e L como conjunto das rectas.

Numa linguagem menos formal, podemos dizer que uma geometria é uma estrutura de pontos e rectas tal que por dois pontos passa uma única recta e existe um conjunto de quatro pontos que não contém três pontos colineares³.

A geometria diz-se finita se o conjunto dos pontos (e consequentemente, o conjunto das rectas) é finito. Muitas vezes, as geometrias de dimensão⁴ dois designam-se por *planos*.

Para simplificar a linguagem, a relação de incidência definida por "a recta l é incidente no ponto p ", escreve-se simplesmente por $p \in l$ e diz-se "o ponto p pertence à recta l ". Também se diz que " p é o ponto de intersecção das rectas l_1 e l_2 ", para indicar que o ponto p é comum às rectas l_1 e l_2 (ou seja, $p \in l_1$ e $p \in l_2$).

Exemplo 9.3. Vamos verificar quais das estruturas de incidência (P, \mathcal{B}, \in) , a seguir indicadas, definem geometrias.

1. P é um conjunto finito, com $|P| \geq 4$, e \mathcal{B} é o conjunto de todos os subconjuntos de P de cardinalidade dois.
2. P é um conjunto finito, com $|P| \geq 4$, e \mathcal{B} é o conjunto de todos os subconjuntos de P de cardinalidade dois e três.
3. $P = \{a, b, c\}$ e \mathcal{B} é o conjunto de todos os subconjuntos de P de cardinalidade dois.
4. $P = \{a, b, c, d\}$ e $\mathcal{B} = \{\{a, b, c, d\}\}$.
5. P é o conjunto de todos os pontos de um espaço euclidiano e \mathcal{B} é o conjunto de todas as rectas desse espaço.

Solução.

1. Uma vez que cada dois pontos de P formam uma recta, os axiomas A_1 e A_3 verificam-se. Por outro lado, dado que $|P| \geq 4$ e não existem três pontos pertencentes a uma mesma recta, então o axioma A_2 também se verifica. Logo, (P, \mathcal{B}) é uma geometria (finita).

³ k pontos dizem-se colineares quando pertencem a uma mesma recta.

⁴Por enquanto, consideramos apenas o conceito intuitivo de dimensão.

2. Sejam $a, b, c \in P$ três pontos distintos. Então os pontos a e b pertencem (pelo menos) a duas rectas distintas: $\{a, b\}$ e $\{a, b, c\}$. Logo, (P, \mathcal{B}) não é uma geometria.
3. Embora o axioma A_1 se verifique, dado que não existem quatro pontos distintos, o axioma A_2 não se verifica. Logo, (P, \mathcal{B}) não é uma geometria.
4. O axioma A_1 verifica-se, mas o axioma A_2 não se verifica. Logo, (P, \mathcal{B}) não é uma geometria.
5. Como consequência dos postulados de Euclides, (P, \mathcal{B}) é uma geometria. \square

Uma vez que a definição de geometria é muito geral, precisamos de alguns axiomas adicionais para obter uma teoria mais forte. Por exemplo, na geometria euclidiana assumem-se os postulados de Euclides. Neste texto, vamos considerar dois tipos de geometria: os espaços afins e os espaços projectivos.

Definição 9.5 (Plano afim). *Um plano afim é uma geometria $\mathcal{A} = (P, L)$ que, adicionalmente, satisfaz o seguinte axioma:*

AF₃ Dado um ponto $p \in P$ e uma recta $l \in L$ tal que l não é incidente em p , existe uma única recta $l' \in L$ que é incidente em p e é disjunta de l . Neste caso diz-se que l e l' são rectas paralelas⁵.

Um plano afim é finito se P é finito.

Informalmente, um plano afim \mathcal{A} é uma geometria que satisfaz o quinto postulado de Euclides (axioma das paralelas). É claro que, por definição, os planos afins verificam todos os axiomas da geometria. Assim, nas demonstrações de resultados sobre planos afins, muitas vezes é necessário considerar, separadamente, os casos de rectas paralelas e de rectas não paralelas.

Definição 9.6 (Plano projectivo). *Um plano projectivo é uma geometria $\pi = (P, L)$ que, adicionalmente, satisfaz o seguinte axioma:*

AP₃ Para cada par de rectas $l_1, l_2 \in L$ distintas, existe um único ponto $p \in P$ no qual ambas as rectas l_1 e l_2 incidem.

Numa linguagem menos formal, o plano projectivo π é uma geometria onde quaisquer duas rectas distintas se intersectam num único ponto. É claro que, por definição, no plano projectivo todos os axiomas da geometria se verificam. Os planos projectivos são utilizados no estudo das perspectivas (representação bidimensional de objectos tridimensionais), considerando-se, neste caso, que duas rectas "paralelas" se intersectam num ponto do infinito.

Exemplo 9.4. Vamos mostrar que o plano do Fano,

definido por $P = \{1, 2, 3, 4, 5, 6, 7\}$ e $L = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}\}$ é um plano projectivo.

Solução. Na Figura 9.1 apresenta-se graficamente o plano de Fano. Observe-se que por cada dois pontos passa uma única recta, e cada duas rectas têm exactamente um ponto em comum. Finalmente, podemos observar que, por exemplo, o conjunto de quatro pontos $\{1, 4, 6, 7\}$ não contém três pontos colineares.

Por razões que mais adiante explicaremos, o plano de Fano é um plano projectivo com o mínimo número de pontos.

Estamos agora em condições de provar um teorema onde se estabelecem algumas conclusões, relativamente aos planos projectivos finitos.

⁵Duas rectas l e l' de um plano são paralelas se $l = l'$ ou l e l' são disjuntas.

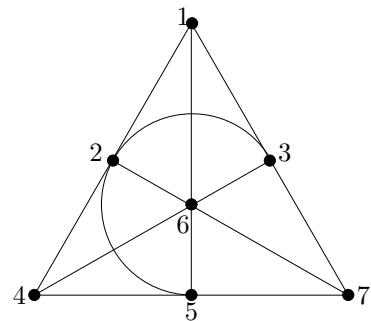


Figura 9.1: Plano de Fano.

\square

Teorema 9.8. Seja $\pi = (P, L)$ um plano projectivo finito. Se uma recta $l \in L$ contém $q + 1$ pontos, com $q \in \mathbb{N}$, então

- (1) cada recta tem $q + 1$ pontos, ou seja, cada recta passa por $q + 1$ pontos,
- (2) cada ponto pertence a $q + 1$ rectas,
- (3) existem, exactamente, $q^2 + q + 1$ rectas,
- (4) o plano tem, exactamente, $q^2 + q + 1$ pontos.

Demonstração.

- (1) Sejam $p_1, p_2, \dots, p_{q+1} \in l$ e considere-se uma outra recta $l' \in L$. Vamos mostrar que a recta l' contém, exactamente, $q + 1$ pontos.

Com efeito, existe $p \in P$ tal que $p \notin l \cap l'$ (caso contrário, todos os pontos pertencem l e l' , o que é impossível, tendo em conta que, de acordo com o axioma A_2 , existem três pontos não colineares). Por outro lado, o ponto p , juntamente com cada um dos pontos p_1, p_2, \dots, p_{q+1} , determina $q + 1$ rectas distintas $pp_1, pp_2, \dots, pp_{q+1}$ (ver Figura 9.2) e não existe nenhuma outra recta, l'' , distinta de $pp_1, pp_2, \dots, pp_{q+1}$ que contenha p (caso contrário, pelo axioma AP_3 , essa recta intersectaria l , ou seja, um dos $q + 1$ pontos de l pertenceria a l'' , o que é contraditório). Assim, p pertence a, exactamente, $q + 1$ rectas. Adicionalmente, de acordo com o axioma AP_3 , a recta l' intersecta as rectas $pp_1, pp_2, \dots, pp_{q+1}$ em $q + 1$ pontos distintos e não contém qualquer outro ponto x (caso contrário, de acordo com o axioma A_1 , existiria uma recta que passaria por x e por p).

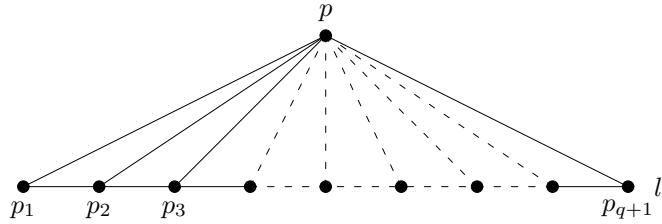


Figura 9.2: Ilustração da demonstração do Teorema 9.8

- (2) Seja p um ponto (isto é, $p \in P$). Vamos mostrar que existem, exactamente $q + 1$ rectas, incidentes em p .

Seja l uma recta que não contém p (note-se que uma tal recta existe, tendo em conta o axioma A_2). De acordo com (1), a recta l tem, exactamente, $q + 1$ pontos que, juntamente com p , determinam $q + 1$ rectas (ver Figura 9.2). Logo, são precisamente estas $q + 1$ rectas que incidem em p .

- (3) Seja l uma recta do plano projectivo π . Já sabemos, por (1), que l contém, exactamente, $q + 1$ pontos e, por (2), que cada ponto de l está contido em q rectas distintas de l . Logo, podemos concluir que π contém, exactamente, $q(q + 1) + 1 = q^2 + q + 1$ rectas.

- (4) Dado um ponto arbitrário $p \in P$, podemos concluir que ele é a intersecção de, exactamente, $q + 1$ rectas distintas que contêm todos os pontos do plano π . Uma vez que cada uma destas rectas tem, exactamente, q pontos distintos de p , então $|P| = q(q + 1) + 1 = q^2 + q + 1$. □

Definição 9.7 (Ordem de um plano projectivo). Diz-se que um plano projectivo finito $\pi = (P, L)$ tem ordem q , com $q \in \mathbb{N}$, se toda a recta $l \in L$ tem, exactamente, $q + 1$ pontos.

Por outras palavras, a ordem de um plano projectivo corresponde ao número de pontos de cada recta menos uma unidade. Como consequência, tendo em conta que o plano de Fano tem ordem 2 e que, se existisse um plano projectivo de ordem 1, então ele teria $1^2 + 1 + 1 = 3$ pontos (o que contraria o axioma A_2), podemos concluir que o plano de Fano é um plano projectivo de ordem mínima.

Exemplo 9.5. Vamos determinar um plano projectivo de ordem 3.

Solução. Considere-se um plano projectivo $\pi = (P, L)$, cuja ordem é $q = 3$. Assim, π contém $q^2 + q + 1 = 13$ pontos e 13 rectas. Sendo $P = \{1, 2, \dots, 13\}$, podemos concluir que

$$\begin{aligned} L = & \{\{1, 4, 7, 13\}, \{2, 5, 8, 13\}, \{3, 6, 9, 13\}, \{1, 5, 9, 12\}, \{2, 6, 7, 12\}, \\ & \{3, 4, 8, 12\}, \{1, 2, 3, 11\}, \{4, 5, 6, 11\}, \{7, 8, 9, 11\}, \{1, 6, 8, 10\}, \\ & \{2, 4, 9, 10\}, \{3, 5, 7, 10\}, \{10, 11, 12, 13\}\} \end{aligned}$$

verifica todos os axiomas de plano projectivo. Na Figura 9.3 faz-se a representação gráfica deste plano π . \square

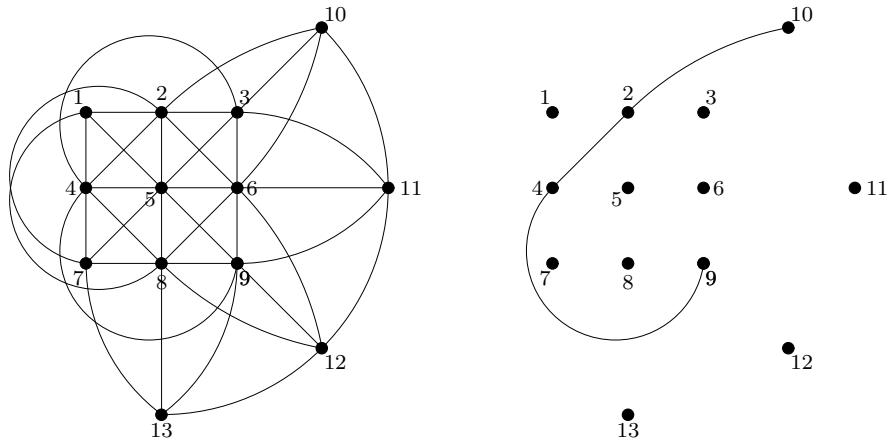


Figura 9.3: Representação gráfica do plano projectivo de ordem 3 e da recta $\{2, 4, 9, 10\}$ do Exemplo 9.5.

Teorema 9.9. Qualquer plano projectivo $\pi = (P, L)$ de ordem q é um design simétrico $2 - (q^2 + q + 1, q + 1, 1)$ e, consequentemente, é também uma sistema de Steiner.

Demonstração. Note-se que os pontos e rectas de π são, respectivamente, os pontos e blocos de um $2 - (q^2 + q + 1, q + 1, 1)$ design e quaisquer dois pontos pertencem a um único bloco. \square

Como um plano projectivo $\pi = (P, L)$ de ordem q é um $2 - (v, k, 1)$ design (P, L) , utilizando as fórmulas (9.6) e (9.10), vem

$$vr = bk \quad \text{e} \quad v - 1 = r(k - 1), \tag{9.12}$$

onde $v = |P| = q^2 + q + 1$, $b = |L| = q^2 + q + 1$, $k = r = q + 1$.

Exemplo 9.6. Vamos mostrar que qualquer design simétrico $2 - (v, k, 1)$, com $v \geq 4$, é um plano projectivo.

Solução. Dado um design simétrico $2 - (v, k, 1)$, (P, L) , por definição, o número de pontos é igual ao número de blocos, ou seja, $v = b$, e a cardinalidade de cada bloco é igual ao número de réplicas de cada

ponto, ou seja, $k = r$. Logo, a equação (9.6) implica a igualdade $v - 1 = k(k - 1)$. Consequentemente, fazendo $q = k - 1$, obtém-se

$$v = k(k - 1) + 1 = (q + 1)q + 1 = q^2 + q + 1,$$

ou seja, o *design* simétrico (P, L) é um *design* $2 - (q^2 + q + 1, q + 1, 1)$. Assim, basta mostrar que este *design* verifica os axiomas da geometria e o axioma AP_3 .

A_1 Por definição de um *2-design* cada dois pontos pertencem a um único bloco (recta).

A_2 Dado um bloco (recta) arbitrário X , uma vez que $q^2 + q + 1 - |X| = q^2 \geq 4$, podemos concluir que existem dois pontos $p_1, p_2 \in X$ e dois pontos $p_3, p_4 \notin X$. Logo, por definição de *2-design*, não existe um bloco que contenha quaisquer três pontos do conjunto $\{p_1, p_2, p_3, p_4\}$.

A_3 Por definição de um *2-design*, tendo em conta que as rectas são os respectivos blocos, verifica-se, imediatamente, que todas as rectas têm pelo menos dois pontos.

AP_3 É imediato que a intersecção de quaisquer dois blocos não contém mais do que um ponto. Por outro lado, se existissem dois blocos disjuntos, X_1 e X_2 , uma vez que cada par de pontos do produto cartesiano $X_1 \times X_2$ está contido num único bloco e que a pares de pontos distintos correspondem blocos distintos, então existiriam pelo menos $(q + 1)^2 + 2$ blocos, o que é superior a $q^2 + q + 1$. Logo, podemos concluir que a intersecção de quaisquer dois blocos distintos consiste, precisamente, num ponto. \square

Exemplo 9.7. Vamos verificar se as estruturas de incidência $\mathcal{A} = (P, L)$, a seguir indicadas, são planos afins.

(a) $P_1 = \{1, 2, 3, 4\}$ e $L_1 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$.

(b) $P_2 = \{1, 2, \dots, 9\}$ e $L_2 = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}, \{1, 5, 9\}, \{3, 4, 8\}, \{2, 6, 7\}\}$.

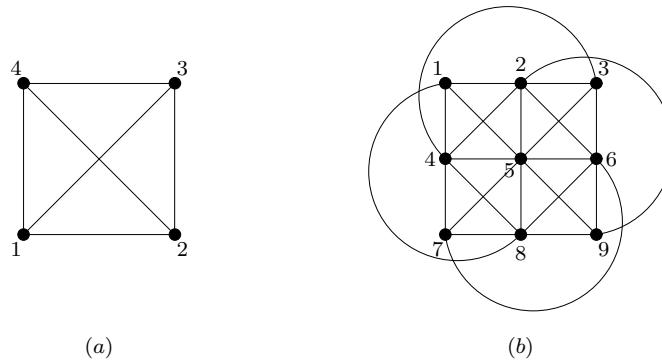


Figura 9.4: Planos afins definidos no Exemplo 9.7.

Solução.

- (a) Na Figura 9.4-(a) representa-se graficamente a estrutura de incidência (P_1, L_1) e facilmente se verifica que todos os axiomas da geometria são satisfeitos. Note-se que, por exemplo, as rectas $\{1, 4\}$ e $\{2, 3\}$ são paralelas. No caso da recta $\{2, 3\}$ e do ponto 1, a única recta que passa por 1 e é paralela a $\{2, 3\}$ é a recta $\{1, 4\}$.

- (b) Na Figura 9.4-(b) representa-se a estrutura de incidência (P_2, L_2) e, mais uma vez, com facilidade se verifica que todos os axiomas da geometria e o axioma AF_3 são satisfeitos. Note-se que, neste caso, existem conjuntos de três rectas paralelas, como são o caso, por exemplo, das rectas $\{3, 5, 7\}$, $\{1, 6, 8\}$ e $\{2, 4, 9\}$. \square

Teorema 9.10. Seja $\pi = (P, L)$ um plano afim finito. Se um ponto $p \in P$ pertence a exactamente $q + 1$ rectas, com $q \in \mathbb{N}$, então

- (1) cada ponto pertence a, exactamente, $q + 1$ rectas,
- (2) cada recta contém, exactamente, q pontos,
- (3) o plano tem, exactamente, q^2 pontos,
- (4) existem, exactamente, $q^2 + q$ rectas,
- (5) para cada recta l existem, exactamente, q rectas paralelas a l .

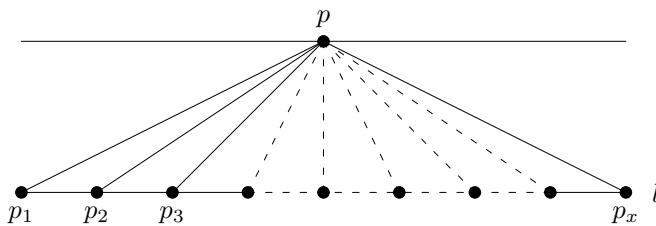


Figura 9.5: Ilustração da demonstração do Teorema 9.10

Demonstração.

- (1) Sejam $l \in L$ uma recta e $p \in P$ um ponto que não pertence à recta l . Dado que l contém x pontos, vem que p pertence a $x + 1$ rectas (ver Figura 9.5). Sendo $p', p'' \in P$ dois pontos arbitrários, como consequência do axioma A_2 , existe (pelo menos) uma recta $r \in L$ que não contém nem p' nem p'' . Logo, ambos os pontos pertencem a $|l| + 1$ rectas e, consequentemente, todos os pontos pertencem a, exactamente, $q + 1$ rectas.
- (2) Seja $l \in L$ uma recta. Como consequência do axioma A_2 , existe (pelo menos) um ponto p que não pertence a l . Logo, uma vez que p pertence a $q + 1$ rectas, l contém, exactamente, q pontos (ver Figura 9.5).
- (3) Seja v o número de pontos e b o número de rectas. Uma vez que cada recta contém q pontos e cada ponto pertence a $q + 1$ rectas, então o número de pontos é igual

$$v = \frac{bq}{q+1}. \quad (9.13)$$

Adicionalmente, contando o número de pares de pontos de duas maneiras distintas, vem que, por um lado existem $\binom{v}{2}$ pares de pontos e, uma vez que cada recta contém $\binom{q}{2}$ pares de pontos, podemos concluir que $\binom{v}{2} = b\binom{q}{2}$ e, consequentemente,

$$b = \frac{\binom{v}{2}}{\binom{q}{2}} = \frac{v(v-1)}{q(q-1)}. \quad (9.14)$$

Substituindo b , a partir de (9.13), na equação (9.14), obtém-se

$$\frac{v(q+1)}{q} = \frac{v(v-1)}{q(q-1)} \Leftrightarrow v = q^2.$$

(4) Substituindo $v = q^2$ na equação (9.14), obtém-se

$$b = \frac{q^2(q^2 - 1)}{q(q - 1)} = q(q + 1).$$

(5) Sejam l e l' duas rectas não paralelas. Por cada ponto de l' passa, exactamente, uma recta paralela a l (recordese que cada recta é, também, paralela a si própria). Por outro lado, pelo axioma AF_3 , não existe uma recta paralela a l e l' (caso contrario, admitindo que l'' é uma recta paralela a l e a l' , as rectas l e l' são ambas paralelas a l'' e passam pelo ponto de intersecção de l e l' , o que é contraditório). Logo, o número de rectas paralelas a l é igual ao número de pontos na recta l' , isto é, q . \square

Como consequência directa deste teorema, um plano afim de ordem q é também um *design 2- $(q^2, q, 1)$* .

Definição 9.8 (Ordem de um plano afim). *Seja $\mathcal{A} = (P, L)$ um plano afim finito. Se toda a recta $l \in L$ tem q pontos, então diz-se que o plano afim têm ordem q .*

Por outras palavras, a ordem de um plano afim finito é igual ao números de pontos de cada recta.

Teorema 9.11. *A partir de um plano projectivo finito, podemos construir um plano afim com a mesma ordem, eliminando uma das rectas (escolhida arbitrariamente) e todos os pontos que ela contém. Reciprocamente, dado um plano afim, podemos construir um plano projectivo com a mesma ordem, adicionando um ponto por cada classe de rectas paralelas, incluindo esse ponto em cada elemento da classe e adicionando a recta constituída por estes pontos.*

Demonstração. Seja $\pi = (P, L)$ um plano projectivo de ordem q e seja l uma recta de π (isto é, $l \in L$). Seja $\pi - l = (P', L')$ a estrutura de incidência que se obtém de π eliminando a recta l e todos os pontos contidos em l . Por exemplo, na Figura 9.6 ilustra-se esta operação, no caso do plano de Fano.

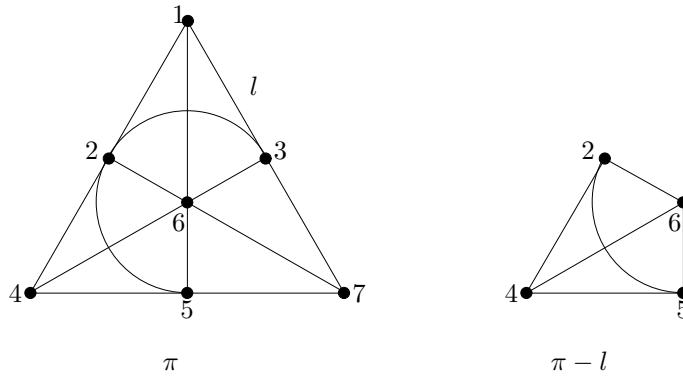


Figura 9.6: Construção de um plano afim a partir do plano de Fano.

Vamos mostrar que $\mathcal{A} = \pi - l$ é um plano afim de ordem q . Porém, uma vez que os axiomas da geometria são obviamente verificados, apenas vamos provar que \mathcal{A} verifica AF_3 .

Seja l' uma recta em \mathcal{A} e p um ponto que não pertence a l' . Primeiramente, vamos mostrar que existe uma única recta em \mathcal{A} que passa por p e é paralela a l' . Com efeito, seja p' o ponto comum às rectas l e l' no plano π (ou seja, $l \cap l' = \{p'\}$) e seja l'' a recta que em π passa por p e p' . Logo, $l'' - p'$ é uma recta em \mathcal{A} que passa por p e é paralela de l' . Por exemplo, utilizando a Figura 9.6, se $l' = \{4, 5, 7\}$ e $p = 2$, então $p' = 7$, $l'' = \{2, 6, 7\}$ e $l'' - p' = \{2, 6\}$ e é claro que, no plano $\pi - l$, as

rectas $l' = \{4, 5\}$ e $l'' - p' = \{2, 6\}$ são paralelas. Note-se que, eliminando l , ficamos com $q^2 + q$ rectas, cada uma das quais com q pontos.

Para provarmos a segunda parte, considere-se um plano afim \mathcal{A} de ordem q que, naturalmente, tem $q + 1$ classes de rectas paralelas, cada uma das quais tem q rectas, e, para cada classe i , com $1 \leq i \leq q+1$, adicione-se um novo ponto ω_i (chamado ponto no infinito), incluindo-o em cada uma das rectas da classe. Finalmente, seja $l_\infty = \{\omega_1, \omega_2, \dots, \omega_{q+1}\}$. Com esta construção, obtém-se $q^2 + q + 1$ pontos, cada um dos quais pertencente a $q + 1$ rectas, e $q^2 + q + 1$ rectas, cada uma das quais contém $q + 1$ pontos. Adicionalmente, quaisquer dois pontos pertencem a uma única recta. Logo, a estrutura obtida é um *design* $2-(q^2 + q + 1, q + 1, 1)$ e, consequentemente, tendo em conta o Exemplo 9.6, é um plano projectivo. \square

Uma consequência imediata desta teorema é que um plano projectivo de ordem q existe se e só se existe um plano afim com a mesma ordem. Por outro lado, tendo em conta a construção introduzida neste teorema, podemos considerar um plano projectivo como uma "extensão" de um plano afim.

Exemplo 9.8. Considerando um plano afim de ordem três (ver Exemplo 9.7-(b)) com 9 pontos e 12 rectas, vamos construir um plano projectivo de ordem três (com 13 pontos e 13 rectas).

Solução. A partir do plano afim representado na Figura 9.4-(b), podemos determinar as seguintes $q + 1 = 4$ classes de rectas paralelas:

$$C_1 : \{1, 6, 8\}, \{2, 4, 9\} \text{ e } \{3, 5, 7\};$$

$$C_2 : \{1, 2, 3\}, \{4, 5, 6\} \text{ e } \{7, 8, 9\};$$

$$C_3 : \{2, 6, 7\}, \{3, 4, 8\} \text{ e } \{1, 5, 9\};$$

$$C_4 : \{1, 4, 7\}, \{2, 5, 8\} \text{ e } \{3, 6, 9\}.$$

De acordo com a construção introduzida no Teorema 9.11, para a classe C_1 adicionamos o vértice $\omega_1 = 10$, para C_2 o vértice $\omega_2 = 11$, para C_3 o vértice $\omega_3 = 12$ e para C_4 o vértice $\omega_4 = 13$. Adicionalmente, acrescenta-se o vértice ω_i a cada recta da classe C_i , para $i = 1, 2, 3, 4$. Desta forma, obtém-se as 12 rectas:

$$\{1, 6, 8, 10\}, \{2, 4, 9, 10\} \text{ e } \{3, 5, 7, 10\};$$

$$\{1, 2, 3, 11\}, \{4, 5, 6, 11\} \text{ e } \{7, 8, 9, 11\};$$

$$\{2, 6, 7, 12\}, \{3, 4, 8, 12\} \text{ e } \{1, 5, 9, 12\};$$

$$\{1, 4, 7, 13\}, \{2, 5, 8, 13\} \text{ e } \{3, 6, 9, 13\}.$$

Finalmente, definindo a décima terceira recta pelo conjunto dos vértices acrescentados, obtém-se o plano projectivo de ordem três representado na Figura 9.3. \square

Teorema 9.12. Qualquer que seja $q = p^n$, onde p é primo e $n \in \mathbb{N}$, existe um plano afim de ordem q .

Demonstração. Dado um corpo de Galois $\mathcal{F} = GF(p^n)$, vamos definir a estrutura de incidência $\pi = (P, L)$, onde o conjunto de pontos é o conjunto

$$P = \mathcal{F} \times \mathcal{F} = \{(x, y) : x, y \in \{0, 1, \dots, q - 1\}\},$$

pelo que $|P| = q^2$, e onde cada recta de L é definida por

$$l(a, b, c) = \{(x, y) \in \mathcal{F}^2 : ax + by + c = 0\},$$

com $a, b, c \in \mathcal{F}$, tais que a e b não são ambos nulos (ou seja, $a \neq 0$ ou $b \neq 0$)⁶. Como consequência, o conjunto das rectas vem dado por

$$L = \{l(a, b, c) : a, b, c \in \mathcal{F}, (a \neq 0 \vee b \neq 0)\}.$$

Resta provar que π é um plano afim, ou seja, que π verifica os axiomas da geometria e o axioma AF_3 .

A_1 Dado dois pontos arbitrários distintos, $p_0 = (x_0, y_0)$ e $p_1 = (x_1, y_1)$, vamos provar que existe uma única recta que os contém. Com efeito, considerando a recta $l = l(y_1 - y_0, x_0 - x_1, y_0x_1 - y_1x_0)$, dado que

$$\begin{aligned}(y_1 - y_0)x_0 + (x_0 - x_1)y_0 + y_0x_1 - y_1x_0 &= 0, \\ (y_1 - y_0)x_1 + (x_0 - x_1)y_1 + y_0x_1 - y_1x_0 &= 0,\end{aligned}$$

podemos concluir que ambos os pontos pertencem à recta l , pelo que basta mostrar que l é a única recta que contém p_0 e p_1 . Suponha que existe uma outra recta $l' = l(a, b, c)$ que contém estes pontos, ou seja, tal que

$$ax_0 + by_0 + c = 0 \quad \text{e} \quad ax_1 + by_1 + c = 0,$$

onde $a(x_1 - x_0) + b(y_1 - y_0) = 0$. Uma vez que os pontos p_0 e p_1 são distintos, sem perda de generalidade, vamos assumir que $x_0 \neq x_1$. Como consequência, $b \neq 0$ e

$$\begin{aligned}a &= -b(y_1 - y_0)(x_1 - x_0)^{-1}, \\ c &= -by_0 + bx_0(y_1 - y_0)(x_1 - x_0)^{-1}.\end{aligned}$$

Logo, a recta l' contém as soluções da equação

$$-b(y_1 - y_0)(x_1 - x_0)^{-1}x + by - by_0 + bx_0(y_1 - y_0)(x_1 - x_0)^{-1} = 0,$$

a qual (multiplicando por $-b^{-1}(x_1 - x_0)$), é equivalente à equação que define a recta l .

A_2 É fácil verificar que os pontos $(0, 0)$, $(0, 1)$, $(1, 0)$ e $(1, 1)$ pertencem a P e são três a três não colineares. Por exemplo, suponha que os pontos $(0, 0)$, $(0, 1)$ e $(1, 0)$ são colineares, ou seja, que existem $a, b, c \in \mathcal{F}$, com $a \neq 0$ ou $b \neq 0$, tais que a recta $l(a, b, c)$ os contém. Então,

$$\begin{aligned}a \cdot 0 + b \cdot 0 + c &= 0 \Rightarrow c = 0, \\ a \cdot 0 + b \cdot 1 &= 0 \Rightarrow b = 0, \\ a \cdot 1 &= 0 \Rightarrow a = 0,\end{aligned}$$

o que constitui uma contradição.

A_3 Tendo em conta a definição de L , é claro que qualquer recta $l \in L$ contém pelo menos dois pontos.

AF_3 Seja $l = l(a, b, c)$ uma recta e $p_0 = (x_0, y_0)$ um ponto não contido em l . Considerando a recta $l' = l(a, b, -ax_0 - by_0)$, uma vez que $ax_0 + by_0 - ax_0 - by_0 = 0$, podemos concluir que o ponto p_0 pertence a l' . Assim, resta provar que as rectas l e l' são paralelas e que l' é a única recta distinta de l nestas condições. Supondo que existe um ponto (x_1, y_1) pertencente a $l \cap l'$, então, dado que $ax_1 + by_1 = -c$ e $ax_1 + by_1 = ax_0 + by_0$, $ax_0 + by_0 = -c$ e, consequentemente, (x_0, y_0) pertence a l , o que constitui uma contradição. Logo, l' é uma recta paralela a l que contém p_0 . Por sua vez, a prova da unicidade da recta l' é idêntica à prova da unicidade em A_1 . \square

⁶Deve observar-se que uma mesma recta pode ser definida por ternos de parâmetros distintos.

O problema da existência de um plano projectivo de ordem distinta de uma potência de um número primo é um problema em aberto. Os menores números conhecidos que não são potências de números primos são 6 e 10 e, para este números sabe-se (por verificação exaustiva realizada por computador) que não existem planos projectivos com tais ordens. Para números n não inferiores a 12 que não sejam potências de primos, o problema da eventual existência de planos projectivos (e, obviamente, planos afins) de ordem n é um problema em aberto.

Exemplo 9.9. Vamos construir um plano afim de ordem 3 a partir do corpo de Galois $\mathcal{F} = GF(3)$.

Solução. Uma vez que a ordem é $q = 3$, o plano afim tem $q^2 = 9$ pontos e $q^2 + q = 12$ rectas. Aplicando a técnica construtiva do Teorema 9.12, obtém-se o conjunto dos pontos

$$P = \{(x_0, x_1) : x_0, x_1 \in \{0, 1, 2\}\}$$

e as rectas definidas pelas soluções das equações (que aparecem agrupadas em classes de rectas paralelas):

1. $x_0 = 0, x_0 = 1$ e $x_0 = 2$;
2. $x_1 = 0, x_1 = 1$ e $x_1 = 2$;
3. $x_0 + x_1 = 0, x_0 + x_1 = 1$ e $x_0 + x_1 = 2$;
4. $x_0 + 2x_1 = 0, x_0 + 2x_1 = 1$ e $x_0 + 2x_1 = 2$.

O plano obtido é o representado na Figura 9.7. \square

Com uma metodologia semelhante à anteriormente adoptada, é possível definir analiticamente um plano projectivo de ordem $q = p^n$, com p primo e $n \in \mathbb{N}$, a partir de um corpo de Galois $\mathcal{F} = GF(q)$. Com efeito, seja

$$V^* = \{(x_0, x_1, x_2) : \mathcal{F}^3 : (x_0, x_1, x_2) \neq (0, 0, 0)\}$$

\sim a relação de equivalência definida em V^* tal que para $x = (x_0, x_1, x_2) \in V^*$ e $y = (y_0, y_1, y_2) \in V^*$

$$x \sim y \Leftrightarrow \exists_{\lambda \in \mathcal{F}^*} \forall_{i \in \{0, 1, 2\}} x_i = \lambda y_i.$$

Denotando a classe de equivalência que contém o elemento x por $[x]$, podemos definir o conjunto dos pontos do plano projectivo por

$$P = \{[x] : x \in V^*\}.$$

Nestas condições, a recta com parâmetros $a, b, c \in V^*$ corresponde ao conjunto

$$l_{a,b,c} = \{[x] : x = (x_0, x_1, x_2) \in V^* \text{ e } ax_0 + bx_1 + cx_2 = 0\}.$$

Como consequência, o conjunto das rectas vem dado por

$$L = \{l_{a,b,c} : (a, b, c) \in V^*\}.$$

Mais adiante, na Secção 9.4, introduziremos o conceito de espaço projectivo e provaremos que (P, L) não só é um plano projectivo de ordem q como também é um caso particular destes espaços mais gerais.

9.3. Quadrados latinos e planos afins e projectivos

Recorde-se que os quadrados latinos A_1, A_2, \dots, A_r de ordem n são *quadrados latinos mutuamente ortogonais* se para cada par $i, j \in [r]$, com $i \neq j$, os quadrados A_i e A_j são ortogonais. Pelo Teorema 8.23, dado um primo p , podemos construir $p - 1$ quadrados latinos mutuamente ortogonais. Mais geralmente, vamos provar o seguinte teorema.

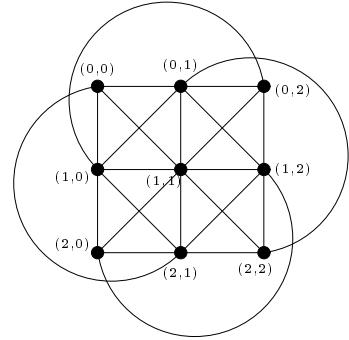


Figura 9.7: Plano afim de ordem três do Exemplo 9.9.

Teorema 9.13. Se $q = p^n$, com p primo e $n \in \mathbb{N}$, então existem $q - 1$ quadrados latinos mutuamente ortogonais de ordem q .

Demonstração. Seja $F = GF(q)$ um corpo de Galois tal que $F = \{0, a_1 = 1, a_2, \dots, a_{q-1}\}$, e sejam

$$L^{(k)} = \begin{bmatrix} 0 & 1 & \cdots & a_{q-1} \\ a_k & a_k + 1 & \cdots & a_k + a_{q-1} \\ a_k a_2 & a_k a_2 + 1 & \cdots & a_k a_2 + a_{q-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_k a_{q-1} & a_k a_{q-1} + 1 & \cdots & a_k a_{q-1} + a_{q-1} \end{bmatrix}, \quad \text{para } 1 \leq k \leq q - 1.$$

Uma vez que $(F, +)$ e (F^*, \cdot) são grupos finitos, facilmente se conclui que cada matriz $L^{(k)}$, para $1 \leq k \leq q - 1$, define um quadrado latino. Assim, resta mostrar a ortogonalidade dos quadrados latinos $L^{(r)}$ e $L^{(s)}$, para $r \neq s$.

Considere as entradas (i, j) de $L^{(r)}$ e $L^{(s)}$, ou seja, $L_{ij}^{(r)} = a_r a_{i-1} + a_{j-1}$ e $L_{ij}^{(s)} = a_s a_{i-1} + a_{j-1}$ e suponha que existe uma outra entrada (\bar{i}, \bar{j}) , para $L^{(r)}$ e $L^{(s)}$, respectivamente, tal que

$$(a_r a_{i-1} + a_{j-1}, a_s a_{i-1} + a_{j-1}) = (a_r a_{\bar{i}-1} + a_{\bar{j}-1}, a_s a_{\bar{i}-1} + a_{\bar{j}-1}),$$

com $1 \leq i, j, \bar{i}, \bar{j} \leq q$. Logo, $a_r(a_{i-1} - a_{\bar{i}-1}) = a_{\bar{j}-1} - a_{j-1}$ e $a_s(a_{i-1} - a_{\bar{i}-1}) = a_{\bar{j}-1} - a_{j-1}$. Porém, uma vez que $a_r \neq a_s$, então $a_{i-1} = a_{\bar{i}-1}$ e $a_{j-1} = a_{\bar{j}-1}$ e, consequentemente, que $i = \bar{i}$ e $j = \bar{j}$. \square

Exemplo 9.10. Considerando o corpo de Galois $GF(2^2) = \{0, 1, \alpha, \beta\}$ e utilizando a construção introduzida na demonstração do Teorema 9.13, vem

$$L^{(1)} = \begin{bmatrix} 0 & 1 & \alpha & \beta \\ 1 & 0 & \beta & \alpha \\ \alpha & \beta & 0 & 1 \\ \beta & \alpha & 1 & 0 \end{bmatrix}, \quad L^{(2)} = \begin{bmatrix} 0 & 1 & \alpha & \beta \\ \alpha & \beta & 0 & 1 \\ \beta & \alpha & 1 & 0 \\ 1 & 0 & \beta & \alpha \end{bmatrix} \quad \text{e} \quad L^{(3)} = \begin{bmatrix} 0 & 1 & \alpha & \beta \\ \beta & \alpha & 1 & 0 \\ 1 & 0 & \beta & \alpha \\ \alpha & \beta & 0 & 1 \end{bmatrix}.$$

Logo, pelo Teorema 9.13, os quadrados latinos $L^{(1)}$, $L^{(2)}$ e $L^{(3)}$ são quadrados latinos mutuamente ortogonais. \square

Estamos agora em condições de analisar algumas relações entre quadrados latinos mutuamente ortogonais de ordem p^n , com p primo e $n \in \mathbb{N}$, e planos afins da mesma ordem.

Exemplo 9.11. Vamos determinar um plano afim de ordem $q = 2^2$, a partir de $q - 1 = 3$ quadrados latinos mutuamente ortogonais de ordem $q = 4$.

Solução. Vamos começar por utilizar os quadrados latinos mutuamente ortogonais de ordem 4, determinados no Exemplo 9.10. Porém, para simplificar a notação, vamos substituir 0 por 1, 1 por 2, α por 3 e β por 4. Assim,

$$M^{(1)} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad M^{(2)} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix} \quad \text{e} \quad M^{(3)} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Considere-se a seguinte matriz $q \times q$ (com $q = 2^2$):

$$S = \begin{bmatrix} s_{11} & s_{12} & s_{13} & s_{14} \\ s_{21} & s_{22} & s_{23} & s_{24} \\ s_{31} & s_{32} & s_{33} & s_{34} \\ s_{41} & s_{42} & s_{43} & s_{44} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}$$

onde as entradas correspondem aos números de $[q^2]$ que se apresentam pela ordem natural em cada uma das linhas. Sendo $P = [16]$ o conjunto dos pontos do plano afim, a partir da matriz S e dos quadrados latinos mutuamente ortogonais $M^{(1)}$, $M^{(2)}$ e $M^{(3)}$, vamos determinar todas as $q^2 + q = 20$ rectas, agrupando-as em classes de rectas paralelas. Assim, considerando

- (1) os conjuntos definidos pelas linhas de S : $\{1, 2, 3, 4\}$, $\{5, 6, 7, 8\}$, $\{9, 10, 11, 12\}$ e $\{13, 14, 15, 16\}$;
- (2) os conjuntos definidos pelas colunas de S : $\{1, 5, 9, 13\}$, $\{2, 6, 10, 14\}$, $\{3, 7, 11, 15\}$ e $\{4, 8, 12, 16\}$;
- (3) os conjuntos definidos pelas entradas de S que correspondem às entradas com o mesmo valor (respectivamente, 1, 2, 3 e 4) em $M^{(1)}$:

$$\begin{aligned}\{S_{ij} : M_{ij}^{(1)} = 1\} &= \{1, 6, 11, 16\}, \\ \{S_{ij} : M_{ij}^{(1)} = 2\} &= \{2, 5, 12, 15\}, \\ \{S_{ij} : M_{ij}^{(1)} = 3\} &= \{3, 8, 9, 14\}, \\ \{S_{ij} : M_{ij}^{(1)} = 4\} &= \{4, 7, 10, 13\}.\end{aligned}$$

- (4) os conjuntos definidos pelas entradas de S que correspondem às entradas com o mesmo valor (respectivamente, 1, 2, 3 e 4) em $M^{(2)}$:

$$\begin{aligned}\{S_{ij} : M_{ij}^{(2)} = 1\} &= \{1, 8, 10, 15\}, \\ \{S_{ij} : M_{ij}^{(2)} = 2\} &= \{2, 7, 9, 16\}, \\ \{S_{ij} : M_{ij}^{(2)} = 3\} &= \{3, 6, 12, 13\}, \\ \{S_{ij} : M_{ij}^{(2)} = 4\} &= \{4, 5, 11, 14\}.\end{aligned}$$

- (5) e os conjuntos definidos pelas entradas de S que correspondem às entradas com o mesmo valor (respectivamente, 1, 2, 3 e 4) em $M^{(3)}$:

$$\begin{aligned}\{S_{ij} : M_{ij}^{(3)} = 1\} &= \{1, 7, 12, 14\}, \\ \{S_{ij} : M_{ij}^{(3)} = 2\} &= \{2, 8, 11, 13\}, \\ \{S_{ij} : M_{ij}^{(3)} = 3\} &= \{3, 5, 10, 16\}, \\ \{S_{ij} : M_{ij}^{(3)} = 4\} &= \{4, 6, 9, 15\}.\end{aligned}$$

obtém-se as 20 rectas, cada uma das quais tem cardinalidade 4, agrupadas em classes de rectas paralelas.

Agora, vamos mostrar que cada par de pontos $p_1, p_2 \in P$ pertence a uma única recta, ou seja, que o par (P, L) , onde L denota o conjunto das rectas, é um 2-design. Para tal, vamos considerar dois casos distintos: (a) o primeiro onde p_1 e p_2 pertencem a uma mesma linha ou coluna de S e (b) o segundo no caso contrário.

- (a) Verifica-se que cada uma das rectas das classes (3), (4) e (5) contém um elemento de cada linha e coluna de S . Logo, nenhuma recta destas classes contém dois pontos da mesma linha ou coluna. Porém, quaisquer dois pontos da mesma linha ou coluna estão contidos numa única recta das classes (1) ou (2).
- (b) Considere-se que os pontos $p_1, p_2 \in P$ não pertencem a uma mesma linha ou coluna de S . Uma vez que as rectas das classes (3), (4) e (5) são disjuntas, dentro de cada classe, podemos concluir

que p_1 e p_2 não pertencem, simultaneamente, a mais do que uma recta de uma mesma classe. Assim, vamos supor que os pontos p_1 e p_2 pertencem, simultaneamente, a duas rectas de classes distintas, por exemplo, a uma recta da classe definida por $M^{(k)}$ e a uma recta da classe definida por $M^{(l)}$, com $k \neq l$. Então, admitindo que $p_1 = S_{ij}$ e $p_2 = S_{i\bar{j}}$, vem que $M_{ij}^{(l)} = M_{i\bar{j}}^{(l)}$ e também que $M_{ij}^{(k)} = M_{i\bar{j}}^{(k)}$, o que é contraditório, tendo em conta a relação de ortogonalidade entre $M^{(k)}$ e $M^{(l)}$. Logo, cada dois pontos pertencentes a linhas e colunas distintas não ocorrem, simultaneamente, em mais do que uma recta.

Uma vez que cada recta contém $\binom{4}{2} = 6$ pares de pontos (por exemplo, a recta $\{1, 2, 3, 4\}$ contém $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}$ e $\{3, 4\}$), as 20 rectas contêm $20 \cdot 6 = 120$ pares. Consequentemente, dado que em P existem $\binom{16}{2} = 120$ pares de pontos distintos, cada dois pontos pertencem a uma única recta. \square

Mais geralmente, supondo que temos $q - 1$ quadrados latinos mutuamente ortogonais $M^{(1)}, M^{(2)}, \dots, M^{(q-1)}$ de ordem $q \in \mathbb{N}$, cujo conjunto de símbolos é $\{1, 2, \dots, q\}$ e definindo a matriz S , como sendo a matriz $q \times q$ tal que

$$S = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1q} \\ s_{21} & s_{22} & \cdots & s_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ s_{q1} & s_{q2} & \cdots & s_{qq} \end{bmatrix} = \begin{bmatrix} 1 & 2 & \cdots & q \\ q+1 & q+2 & \cdots & 2q \\ \vdots & \vdots & \ddots & \vdots \\ (q-1)q+1 & (q-1)q+2 & \cdots & q^2 \end{bmatrix},$$

podemos determinar um plano afim (P, L) , recorrendo ao procedimento utilizado no Exemplo 9.11. Assim, com este procedimento, vem que $P = \{1, \dots, q^2\}$ e as rectas são definidas (em classes de rectas paralelas) do seguinte modo:

- (1) Conjuntos formados pelas entradas de cada uma das q linhas da matriz S .
 - (2) Conjuntos formados pelas entradas de cada uma das q colunas da matriz S .
 - (3) Conjuntos de cardinalidade q formados pelas entradas da matriz S que correspondem às entradas da matriz $M^{(1)}$ com valor constante.
- ⋮
- (q+1) Conjuntos de cardinalidade q formados pelas entradas da matriz S que correspondem às entradas da matriz $M^{(q-1)}$ com valor constante.

Com este procedimento, obtém-se $(q+1)q = q^2 + q$ rectas, cada uma das quais com q pontos, tais que não existem dois pontos pertencentes a mais do que uma recta. Porém, uma vez que estas rectas, no seu conjunto, contêm

$$q(q+1)\binom{q}{2} = \frac{1}{2}q^2(q^2-1) = \binom{q^2}{2}$$

pares de pontos distintos, podemos concluir que quaisquer dois pontos de P pertencem a uma única recta. Deste modo, obtém-se $q(q+1)$ rectas que satisfazem as seguintes condições:

I cada recta contém q pontos,

II cada ponto pertence a $q+1$ rectas (note-se que cada ponto pertence, precisamente, a uma recta de cada uma das classes obtidas em (1), (2), ..., (q+1)),

III cada dois pontos pertencem, simultaneamente, a uma única recta,

IV cada duas rectas contêm, no máximo, um ponto comum (note-se que a existência de duas rectas l_1 e l_2 tais que $|l_1 \cap l_2| \geq 2$ contradiz o item 3).

Conclui-se ainda que as rectas podem ser agrupadas em $q + 1$ classes de q rectas paralelas. Adicionalmente, mostra-se que esta estrutura de incidência satisfaz o axioma AF_3 e, consequentemente, é uma geometria afim. Para tal, sendo $l = \{p_1, p_2, \dots, p_q\}$ uma recta arbitrária e p' um ponto não pertencente a l , vamos mostrar que existe uma única recta que contém p' e é paralela a l . Com efeito, qualquer que seja o ponto $p_i \in l$, com $i \in \{1, \dots, q\}$, existe uma única recta l_i que contém ambos os pontos p_i e p' . É claro que se $i \neq j$, então $l_i \neq l_j$ (caso contrário, $p_i, p_j \in l \cap l_i$, o que entra em contradição com a condição IV). Logo, existem apenas q rectas l_i tais que $p' \in \bigcap_{i=1}^q l_i$ e cada uma delas intersecta l . Porém, sabe-se que, de acordo com a condição II, p' pertence a exactamente $q + 1$ rectas. Consequentemente, existe uma única recta que passa por p' e é paralela a l .

Concluímos assim que esta estrutura de incidência, com q^2 pontos e $q^2 + q$ rectas, satisfaz os axiomas da geometria afim de ordem q o que também significa que se trata de um *design* $2 - (q^2, q, 1)$, o qual coincide com um sistema de triplos de Steiner $STS(q^2)$.

Teorema 9.14. *Existe um plano afim de ordem q se e só se existe um conjunto de $q - 1$ quadrados latinos mutuamente ortogonais de ordem q .*

Demonstração. Uma vez que anteriormente já se provou que se existe um conjunto de $q - 1$ quadrados latinos mutuamente ortogonais de ordem q , então existe um plano afim de ordem q , vamos provar apenas o recíproco, ou seja, que a existência de um plano afim de ordem q implica a existência de $q - 1$ quadrados latinos mutuamente ortogonais de ordem q .

Suponhamos que existe um plano afim de ordem q , o que é equivalente a afirmar que existe um *design* $2 - (q^2, q, 1)$. Assim, tendo em conta o Teorema 9.8, podemos concluir que existem $r = q + 1$ classes de rectas paralelas, cada uma das quais com q rectas. Escolhendo, arbitrariamente, duas destas classes, por exemplo, $L^1 = \{l_1^1, l_2^1, \dots, l_q^1\}$ e $L^2 = \{l_1^2, l_2^2, \dots, l_q^2\}$, a cada ponto p do plano afim, podemos associar o par de "coordenadas" (i, j) tal que p é o único ponto da intersecção das rectas l_i^1 e l_j^2 . Seja S uma matriz $q \times q$ onde cada entrada s_{ij} determina o ponto do plano com coordenadas (i, j) . A partir de cada uma das restantes $q - 1$ classes de rectas paralelas L^k , com $k \in \{3, \dots, q + 1\}$, vamos determinar a matriz M^k , de acordo com o seguinte procedimento:

- Escolher uma classe de rectas paralelas $L^k = \{l_1^k, l_2^k, \dots, l_q^k\}$, com $k \geq 3$;
- Determinar a matriz quadrada M^k de ordem q , cujas entradas m_{ij}^k vêm dadas por

$$m_{ij}^k = \alpha \Leftrightarrow s_{ij} \in l_\alpha^k.$$

Vamos mostrar que a matriz obtida é um quadrado latino e que as matrizes M^k , para $k = 3, \dots, q + 1$, são quadrados latinos mutuamente ortogonais.

- Suponha que $m_{ij}^k = m_{i,\bar{j}}^k = \alpha$, com $j \neq \bar{j}$. Então os pontos $s_{ij}, s_{i\bar{j}}$ pertencem à rectas l_i^1 e l_α^k , o que é contraditório com a condição III, logo nenhuma das linhas da matriz M^k tem entradas repetidas. De igual modo se prova que nenhuma das colunas da matriz M^k tem entradas repetidas. Logo M^k é um quadrado latino.
- Resta provar que quaisquer dois quadrados latinos M^u e M^v , com $u \neq v$, obtidos no item anterior, são ortogonais. Assim, suponha que existem entradas distintas (i, j) e (\bar{i}, \bar{j}) tais que $m_{ij}^u = m_{i\bar{j}}^u = \alpha$ e $m_{ij}^v = m_{i\bar{j}}^v = \beta$. Então s_{ij} e $s_{i\bar{j}}$ pertencem ambos a $l_\alpha^u \cap l_\beta^v$, o que, mais uma vez, entra em contradição com a condição III. \square

Vamos terminar esta secção com um resultado que é consequência directa dos Teoremas 9.11 e 9.14.

Teorema 9.15 (de Bose). *As seguintes afirmações são equivalentes.*

- (1) *Existe um conjunto de $q - 1$ quadrados latinos mutuamente ortogonais de ordem q .*
- (2) *Existe um plano afim de ordem q .*
- (3) *Existe um plano projectivo de ordem q .*

9.4. Espaços projectivos

Os planos projectivos que temos vindo a estudar são casos particulares de estruturas mais gerais que se designam por espaços projectivos. Tendo em vista a definição destes espaços, vamos considerar um corpo de Galois $\mathcal{F} = GF(q)$, com $q = p^n$ elementos, onde p é primo e $n \in \mathbb{N}$, e vamos considerar um espaço vectorial de dimensão $r + 1$

$$V = V(r, q) = \{(x_0, x_1, \dots, x_r) : \forall_{0 \leq i \leq r} x_i \in GF(q)\}.$$

Sendo $V^* = V \setminus \{\mathbf{0}\}$, onde $\mathbf{0} = (0, 0, \dots, 0)$, vamos definir em V^* a relação de equivalência \sim tal que, dados $x, y \in V^*$, com $x = (x_0, x_1, \dots, x_r)$ e $y = (y_0, y_1, \dots, y_r)$,

$$x \sim y \Leftrightarrow \exists_{\lambda \in \mathcal{F}^*} \forall_{i \in \{0, \dots, r\}} x_i = \lambda y_i.$$

Como usualmente, a classe de equivalência de x será representada por $[x]$.

Definição 9.9 (Espaço projectivo). *Designa-se por espaço projectivo de dimensão r associado a V e denota-se por $PG_r(V)$, o conjunto de classes de equivalência $\{[x] : x = (x_0, x_1, \dots, x_r) \in V^*\}$.*

Note-se que os pontos de $PG_r(V)$ são subespaços de V de dimensão um, as rectas projectivas são planos vectoriais, os planos projectivos são subespaços vectoriais de dimensão três e os hiperplanos de $PG_r(V)$ são subespaços de V de dimensão r . Por sua vez, um plano projectivo é um espaço projectivo de dimensão 2 que se denota por $PG_2(V)$.

Exemplo 9.12. *Sendo $\mathcal{F} = GF(p)$, com p primo, vamos construir o espaço projectivo $PG_2(V)$.*

Solução. Existem $p^3 - 1$ vectores $(x_0, x_1, x_2) \neq (0, 0, 0)$ em V^* . Uma vez que os vectores (x_0, x_1, x_2) e $(\lambda x_0, \lambda x_1, \lambda x_2)$ são equivalentes, para $\lambda = 1, 2, \dots, p - 1$, podemos concluir que cada classe de equivalência tem exactamente $p - 1$ elementos e, como consequência, o espaço projectivo $PG_2(V)$ tem $\frac{p^3 - 1}{p - 1} = p^2 + p + 1$ pontos.

No caso particular de $p = 2$, vem que $\mathcal{F} = \{0, 1\}$ e V é o espaço vectorial de dimensão três sobre \mathcal{F} , donde podemos concluir que $|V| = 2^3 = 8$ (ou seja, V é constituído por 8 vectores da forma (x_0, x_1, x_2) , com $x_i \in \{0, 1\}$, para $i = 0, 1, 2$). Na Figura 9.8-(a), representam-se todos os vectores de V e, a partir dela, podemos observar a existência dos seguintes 7 planos:

$$\begin{aligned} & \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 0)\}, \{(0, 0, 0), (1, 0, 0), (0, 0, 1), (1, 0, 1)\}, \\ & \{(0, 0, 0), (1, 0, 0), (0, 1, 1), (1, 1, 1)\}, \{(0, 0, 0), (0, 1, 0), (1, 1, 1), (1, 0, 1)\}, \\ & \{(0, 0, 0), (0, 1, 0), (0, 1, 1), (0, 0, 1)\}, \{(0, 0, 0), (0, 0, 1), (1, 1, 1), (1, 1, 0)\}, \\ & \{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}. \end{aligned}$$

Como cada recta em V tem exactamente dois pontos, vem que sete rectas passam pelo ponto $(0, 0, 0)$. Cada plano tem quatro pontos, logo o espaço projectivo $PG_2(V)$ tem sete pontos e sete rectas (plano de Fano) que é ilustrado na Figura 9.8-(b). \square

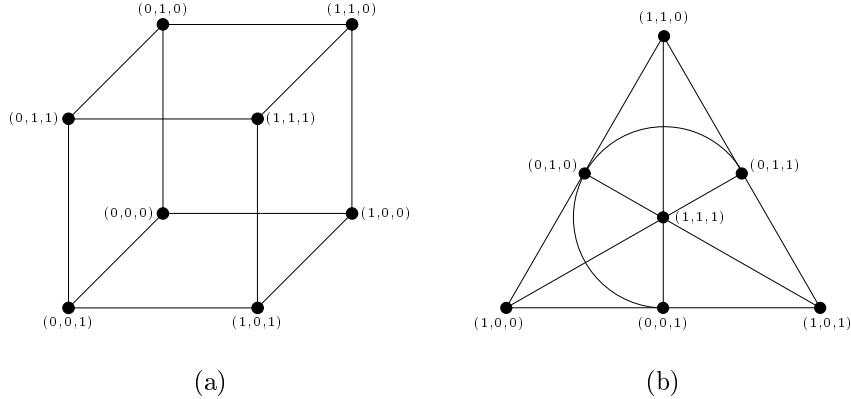


Figura 9.8: Construção do plano projectivo do Exemplo 9.12.

Teorema 9.16. Um espaço projectivo $PG_r(V)$, onde V é um espaço vectorial de dimensão $r+1$ sobre $\mathcal{F} = GF(q)$, satisfaz as seguintes propriedades:

- (1) O número de pontos de $PG_r(V)$ é igual $\frac{q^{r+1}-1}{q-1} = q^r + q^{r-1} + \cdots + q + 1$.
- (2) Cada par de pontos de $PG_r(V)$ pertence a uma única recta.
- (3) Cada recta contém precisamente $q+1$ pontos.

Demonstração.

- (1) Uma vez que cada um dos $q^{r+1}-1$ vectores não nulos em $V(r, q)$ admite $q-1$ múltiplos escalares, podemos concluir que o espaço projectivo $PG_r(V)$ tem $\frac{q^{r+1}-1}{q-1} = q^r + q^{r-1} + \cdots + q + 1$ pontos.
- (2) Sejam $[x]$ e $[y]$ dois pontos distintos de $PG_r(V)$. Então a recta que contém estes pontos é o conjunto $\{\lambda[x] + \mu[y] : \lambda, \mu \in \mathcal{F}, (\lambda, \mu) \neq (0, 0)\}$ que é único.
- (3) Dado que $|\{(\lambda, \mu) \in \mathcal{F}^2 : (\lambda, \mu) \neq (0, 0)\}| = q^2 - 1$ e cada vector de V admite $q - 1$ múltiplos escalares não nulos, podemos concluir que cada recta do espaço projectivo $PG_r(V)$ tem cardinalidade $\frac{q^2-1}{q-1} = q + 1$. □

Exemplo 9.13. Considerando $\mathcal{F} = GF(3)$ e $V = \mathcal{F}^3$, vamos determinar o espaço projectivo $PG_2(V)$.

Solução. O espaço projectivo $PG_2(V)$ fica completamente determinado, uma vez que sejam conhecidos o respectivo conjunto de pontos e o respectivo conjunto de rectas. Vamos começar por determinar os conjuntos candidatos, respectivamente, a conjunto de pontos e a conjunto de rectas e, posteriormente, vamos provar que estes conjuntos definem um plano projectivo.

- **Determinação do conjunto de pontos.** Uma vez que $\mathcal{F} = GF(3) = \{0, 1, 2\}$, então o espaço vectorial $V = \{(x_0, x_1, x_2) : x_i \in \mathbb{Z}_3, i = 0, 1, 2\}$ tem cardinalidade $|V| = 3^3 = 27$. Por outro lado, se $x \in V^* = V \setminus \{(0, 0, 0)\}$, então $[x] = \{x, 2x\}$. Como consequência, existem $(27-1)/2 = 13$

classes de equivalência, ou seja, existem 13 pontos que são, precisamente,

$$\begin{aligned} [(0, 0, 1)] &= \{(0, 0, 1), (0, 0, 2)\}, [(0, 1, 0)] = \{(0, 1, 0), (0, 2, 0)\}, \\ [(0, 1, 1)] &= \{(0, 1, 1), (0, 2, 2)\}, [(0, 1, 2)] = \{(0, 1, 2), (0, 2, 1)\}, \\ [(1, 0, 0)] &= \{(1, 0, 0), (2, 0, 0)\}, [(1, 0, 1)] = \{(1, 0, 1), (2, 0, 2)\}, \\ [(1, 0, 2)] &= \{(1, 0, 2), (2, 0, 1)\}, [(1, 1, 0)] = \{(1, 1, 0), (2, 2, 0)\}, \\ [(1, 1, 1)] &= \{(1, 1, 1), (2, 2, 2)\}, [(1, 1, 2)] = \{(1, 1, 2), (2, 2, 1)\}, \\ [(1, 2, 0)] &= \{(1, 2, 0), (2, 1, 0)\}, [(1, 2, 1)] = \{(1, 2, 1), (2, 1, 2)\}, \\ [(1, 2, 2)] &= \{(1, 2, 2), (2, 1, 1)\}, \end{aligned}$$

candidatos a pontos de $PG_2(V)$.

- **Determinação do conjunto de rectas.** Uma vez que V é um espaço vectorial de dimensão três sobre o corpo finito $GF(3)$ e o número 3 é primo, os conjuntos de pontos candidatos a rectas de $PG_2(V)$ definem-se do seguinte modo: sendo $a = (a_0, a_1, a_2) \in V^*$,

$$L_a = \{[x] : x = (x_0, x_1, x_2) \in V^* \text{ e } a_0x_0 + a_1x_1 + a_2x_2 = 0\}.$$

Note-se que $a_0x_0 + a_1x_1 + a_2x_2 = 0$ implica $\lambda a_0x_0 + \lambda a_1x_1 + \lambda a_2x_2 = 0$, para qualquer $\lambda \in \mathcal{F}^*$. Logo, $L_a = L_{\lambda a}$, para $\lambda \in \mathcal{F}^*$.

- **Verificação de que por quaisquer dois pontos passa uma única recta.** Dados dois pontos arbitrários distintos, $[x] = [(x_0, x_1, x_2)]$ e $[y] = [(y_0, y_1, y_2)]$, do conjunto anteriormente determinado, basta mostrar que existe uma única classe de ternos $a = (a_0, a_1, a_2) \in V^*$ tal que

$$\begin{cases} a_0x_0 + a_1x_1 + a_2x_2 = 0, \\ a_0y_0 + a_1y_1 + a_2y_2 = 0. \end{cases} \quad (9.15)$$

Uma vez que $[x] \neq \lambda[y]$, para todo o $\lambda \in \mathcal{F}^*$, então as equações da sistema (9.15) são independentes, relativamente às incógnitas a_0 , a_1 e a_2 . Logo, pelo menos um dos determinantes

$$\left| \begin{array}{cc} x_0 & x_1 \\ y_0 & y_1 \end{array} \right| \text{ ou } \left| \begin{array}{cc} x_1 & x_2 \\ y_1 & y_2 \end{array} \right| \text{ é não nulo. Supondo, sem perda de generalidade, que}$$

$$\left| \begin{array}{cc} x_0 & x_1 \\ y_0 & y_1 \end{array} \right| \neq 0,$$

e fixando (arbitrariamente) o valor de $a_2 \in \mathcal{F}^*$, obtém-se uma única solução para a_0 e a_1 . Admitindo que $a_0 = ka_2$ e $a_1 = k'a_2$, com $k, k' \in \mathcal{F}$, podemos concluir que $(ka_2, k'a_2, a_2) = a_2(k, k', 1)$ define o conjunto de soluções para o sistema (9.15). Assim, todas as soluções de (9.15) são equivalentes e, consequentemente, por cada par de pontos $[x]$ e $[y]$ passa uma única recta.

Tendo em conta a análise anterior, podemos concluir que as rectas de $PG_2(V)$ são os conjuntos de pontos:

1. $L_{(1,0,0)}$ que é determinado pelo conjunto das soluções da equação $x_0 = 0$, isto é, $L_{(1,0,0)} = \{[(0, 0, 1)], [(0, 1, 0)], [(0, 1, 1)], [(0, 1, 2)]\}$;
2. $L_{(1,1,0)}$ que é determinado pelo conjunto das soluções da equação $x_0 + x_1 = 0$, isto é, $L_{(1,1,0)} = \{[(0, 0, 1)], [(1, 2, 0)], [(1, 2, 1)], [(1, 2, 2)]\}$;
3. $L_{(1,2,0)}$ que é determinado pelo conjunto das soluções da equação $x_0 + 2x_2 = 0$, isto é, $L_{(1,2,0)} = \{[(0, 0, 1)], [(1, 1, 0)], [(1, 1, 1)], [(1, 1, 2)]\}$;

:

13. $L_{(1,2,2)}$ que é determinado pelo conjunto das soluções da equação $x_0 + 2x_1 + 2x_2 = 0$, isto é, $L_{(1,2,2)} = \{[(0, 1, 1)], [(1, 0, 1)], [(1, 1, 0)], [(1, 1, 2)]\}$. \square

O próximo teorema, que se apresenta sem prova, uma vez que ela decorre, directamente, do processo construtivo utilizado na resolução do Exemplo 9.13, generaliza este último resultado, .

Teorema 9.17. *Para cada corpo finito $\mathcal{F} = GF(p^n)$, com p primo e $n, r \in \mathbb{N}$, existe um espaço projectivo $PG_r(p^n)$ de ordem p^n e dimensão r .*

A partir de um corpo de Galois $\mathcal{F} = GF(p^n)$, com p primo e $n \in \mathbb{N}$, podemos construir um plano afim $AF = (P, L)$, sobre \mathcal{F} , determinando o conjunto de pontos, como sendo o conjunto $P = \mathcal{F}^2 = \{(x_0, x_1) : x_0, x_1 \in \mathcal{F}\}$ e definindo cada uma das rectas como sendo o conjunto

$$l(m, a, c) = \{(x_0, x_1) \in \mathcal{F}^2 : x_1 = mx_0 + b \text{ ou } x_0 = c\},$$

onde $m, b, c \in \mathcal{F}$.

Deve observar-se que enquanto no plano projectivo cada ponto tem três coordenadas, no plano afim cada ponto tem apenas duas coordenadas. Intuitivamente, os pontos do plano projectivo cuja terceira coordenada é nula são pontos no infinito. Note-se que o ponto (x_0, x_1) do plano afim corresponde ao ponto $(x_0, x_1, 1)$ no plano projectivo e ao ponto $(x_0, x_1, 0)$ no infinito. Por sua vez, a recta $a_0x_0 + a_1x_1 + a_2 = 0$ do plano afim corresponde à recta $a_0x_0 + a_1x_1 + a_2x_2 = 0$ do plano projectivo.

Exemplo 9.14. *Vamos construir um plano afim (e três quadrados latinos mutuamente ortogonais) a partir de corpo de Galois $GF(4)$.*

Solução. Sendo $\mathcal{F} = GF(2^2) = \{0, 1, \alpha, \beta\}$, conforme se concluiu anteriormente (ver Exemplo 9.10), sabe-se que o plano afim de ordem quatro tem $4^2 = 16$ pontos e $4^2 + 4 = 20$ rectas. Por simplicidade, vamos representar as rectas por intermédio das equações $x_1 = mx_0 + b$ ou $x_0 = c$, com $b, c, m \in \mathcal{F}$. Assim, podemos partir o conjunto das rectas nas seguintes cinco classes de rectas paralelas:

$$C_1 : x_0 = 0, x_0 = 1, x_0 = \alpha \text{ e } x_0 = \beta; \quad (\text{verticais})$$

$$C_2 : x_1 = 0, x_1 = 1, x_1 = \alpha \text{ e } x_1 = \beta; \quad (\text{horizontais})$$

$$C_3 : x_1 = x_0, x_1 = x_0 + 1, x_1 = x_0 + \alpha \text{ e } x_1 = x_0 + \beta; \quad (\text{declive 1})$$

$$C_4 : x_1 = \alpha x_0, x_1 = \alpha x_0 + 1, x_1 = \alpha x_0 + \alpha \text{ e } x_1 = \alpha x_0 + \beta; \quad (\text{declive } \alpha)$$

$$C_5 : x_1 = \beta x_0, x_1 = \beta x_0 + 1, x_1 = \beta x_0 + \alpha \text{ e } x_1 = \beta x_0 + \beta; \quad (\text{declive } \beta)$$

Agora, vamos determinar como se distribuem os 16 pontos do plano afim pelas rectas das diferentes classe de rectas paralelas (ver Teorema 9.11). Uma vez que para as classes C_1 (rectas verticais) e C_2 (rectas horizontais) esta distribuição é óbvia e, para cada uma das classes C_3, C_4 e C_5 a distribuição dos pontos pelas respeirivas rectas é idêntica, apenas vamos determinar, com detalhe, a distribuição dos pontos pelas diferentes rectas da classe C_3 . Assim, utilizando a notação que a seguir se indica para cada uma das equações:

$$\textcircled{1} : x_1 = x_0 + 0,$$

$$\textcircled{2} : x_1 = x_0 + 1,$$

$$\textcircled{3} : x_1 = x_0 + \alpha,$$

$$\textcircled{4} : x_1 = x_0 + \beta,$$

vem

$$\begin{pmatrix} \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} \\ (0,0) & (0,1) & (0,\alpha) & (0,\beta) \\ \textcircled{4} & \textcircled{1} & \textcircled{2} & \textcircled{3} \\ (1,0) & (1,1) & (1,\alpha) & (1,\beta) \\ \textcircled{3} & \textcircled{4} & \textcircled{1} & \textcircled{2} \\ (\alpha,0) & (\alpha,1) & (\alpha,\alpha) & (\alpha,\beta) \\ \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{1} \\ (\beta,0) & (\beta,1) & (\beta,\alpha) & (\beta,\beta) \end{pmatrix}$$

onde cada ponto (x_0, x_1) aparece associado ao número da única recta da classe C_3 a que pertence. Como resultado, obtém-se o quadrado latino cujo conjunto de símbolos coincide com os símbolos destas rectas.

$$\begin{pmatrix} \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} \\ \textcircled{4} & \textcircled{1} & \textcircled{2} & \textcircled{3} \\ \textcircled{3} & \textcircled{4} & \textcircled{1} & \textcircled{2} \\ \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{1} \end{pmatrix}.$$

Procedendo como anteriormente, para as classes C_4 e C_5 , obtém-se os seguintes quadrados latinos:

$$C_4 : \begin{pmatrix} \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} \\ \textcircled{3} & \textcircled{4} & \textcircled{1} & \textcircled{2} \\ \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{1} \\ \textcircled{4} & \textcircled{1} & \textcircled{2} & \textcircled{3} \end{pmatrix} \quad C_5 : \begin{pmatrix} \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} \\ \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{1} \\ \textcircled{4} & \textcircled{1} & \textcircled{2} & \textcircled{3} \\ \textcircled{3} & \textcircled{4} & \textcircled{1} & \textcircled{2} \end{pmatrix}.$$

Com este procedimento, obtivemos três quadrados latinos mutuamente ortogonais. \square

Uma vez que um plano projectivo de ordem q é um *design* simétrico, os pontos e as rectas têm propriedades análogas relativamente à relação de incidência, nomeadamente, cada recta contém $q+1$ pontos e cada ponto pertence a $q+1$ rectas. Logo, qualquer propriedade que envolva pontos, rectas e a relação de incidência, é também válida quando se trocam as palavras "pontos" por "rectas" e "rectas" por "pontos". Nesta condições, diz-se que a propriedade, assim obtida, é uma propriedade *dual*. Como consequência, para cada afirmação ou teorema sobre planos projectivos existe a, respectiva, afirmação ou teorema dual. Por exemplo, a afirmação "dois pontos distintos determinam uma única recta" tem como afirmação dual "duas rectas distintas determinam um único ponto".

A Figura 9.9 ilustra esta relação de dualidade entre pontos e rectas, no caso de um plano projectivo de ordem três, tendo em conta que os símbolos " \bullet " representam pontos, os símbolos " \circ " representam rectas e os segmentos definem a relação da incidência. Com efeito, trocando o símbolo " \bullet " com o símbolo " \circ " mais próximo obtém-se uma estrutura de incidência equivalente.

9.5. Matrizes de Hadamard

Uma matriz de Hadamard é uma matriz quadrada com entradas 1 e -1 introduzida por James Sylvester em 1867, com a designação de *anallagmatic pavement*, e que mais tarde (em 1893) veio a ser redescoberta por Jacques Hadamard.

Definição 9.10 (Matriz de Hadamard). *Uma matriz H quadrada de ordem n , com entradas 1 e -1, diz-se uma matriz de Hadamard se $HH^T = nI_n$, onde H^T é a transposta de H e I_n é a matriz identidade de ordem n .*

De modo equivalente, pode afirmar-se que uma matriz $H = (h_{ij})$, $n \times n$, com entradas 1 e -1, é uma matriz de Hadamard se as linhas (e colunas) de H são ortogonais, isto é, $\sum_{k=1}^n h_{ik}h_{jk} = 0$, para $i \neq j$.

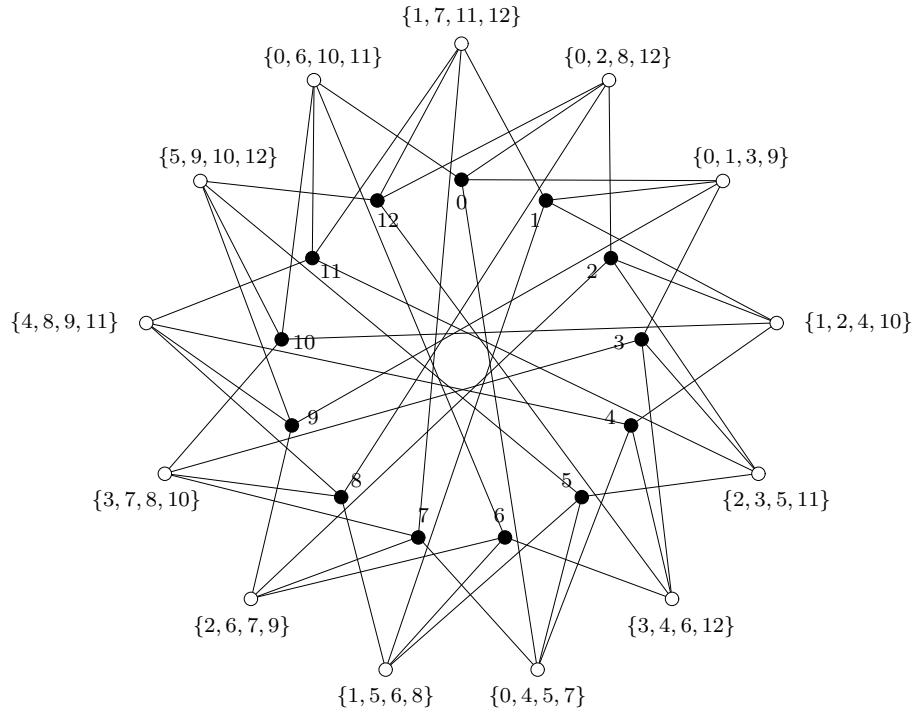


Figura 9.9: Dualidade entre pontos e rectas de um plano projectivo de ordem três.

Exemplo 9.15. Vamos mostrar que as matrizes a seguir indicadas são matrizes de Hadamard.

$$H_1 = \begin{pmatrix} 1 \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{e} \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Solução. Multiplicando cada uma destas matrizes pela respectiva transposta, obtém-se

$$H_1 H_1^T = \begin{pmatrix} 1 \end{pmatrix}, \quad H_2 H_2^T = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{e} \quad H_4 H_4^T = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Por outro lado, pode observar-se que as linhas (e colunas) destas matrizes são duas a duas ortogonais. \square

Muitas vezes, as matrizes de Hadamard de ordem n são representadas por tabuleiros $n \times n$ com casas brancas e pretas, de tal forma que as casas pretas correspondem a 1 e as casas brancas a -1. Como ilustração, a matriz H_4 do exemplo anterior pode representar-se na forma

$$H_4 = \begin{array}{|c|c|c|c|} \hline & \text{\textcolor{black}{\blacksquare}} & \text{\textcolor{white}{\square}} & \text{\textcolor{white}{\square}} \\ \hline \text{\textcolor{white}{\square}} & \text{\textcolor{black}{\blacksquare}} & \text{\textcolor{white}{\square}} & \text{\textcolor{white}{\square}} \\ \hline \text{\textcolor{white}{\square}} & \text{\textcolor{white}{\square}} & \text{\textcolor{black}{\blacksquare}} & \text{\textcolor{black}{\blacksquare}} \\ \hline \text{\textcolor{white}{\square}} & \text{\textcolor{white}{\square}} & \text{\textcolor{black}{\blacksquare}} & \text{\textcolor{black}{\blacksquare}} \\ \hline \end{array}$$

Note-se que dada uma matriz de Hadamard, trocando todos valores das entradas de uma linha (coluna) pelos seus simétricos, se obtém novamente uma matriz de Hadamard. Como consequência,

podemos considerar apenas as matrizes de Hadamard com uns ao longo da primeira linha e primeira coluna. Uma tal matriz designa-se por *matriz de Hadamard normalizada*. As matrizes H_1 , H_2 e H_4 do Exemplo 9.15 são normalizadas.

Teorema 9.18. *Se H é uma matriz de Hadamard de ordem n , então $n = 1$ ou $n = 2$ ou $n = 4k$, com $k \in \mathbb{N}$.*

Demonstração. Sem perda de generalidade, assuma-se que H é uma matriz de Hadamard normalizada. Com base no Exemplo 9.15, pode concluir-se a existência de matrizes de Hadamard de ordens um e dois.

Supondo $n \geq 3$, vamos considerar as três primeiras linhas de H . Sejam i, j, k e s o número de colunas de H nas quais as primeiros três entradas têm valores, respectivamente, $1, 1, 1$, $-1, 1, -1$, $1, -1, 1$ e $-1, -1, -1$. Da definição de matriz de Hadamard normalizada decorre o sistema de equações lineares

$$\begin{cases} i + j + k + s = n, & (\text{número das colunas}) \\ i + j - k - s = 0, & (\text{ortogonalidade entre a primeira e segunda linhas}) \\ i - j + k - s = 0, & (\text{ortogonalidade entre a primeira e terceira linhas}) \\ i - j - k + s = 0, & (\text{ortogonalidade entre a segunda e terceira linhas}) \end{cases}$$

cuja solução é $i = j = k = s = \frac{n}{4}$. □

A conjectura de Hadamard, ainda em aberto, diz que para todo $n = 4k$, com k natural, existe uma matriz de Hadamard de ordem n . A menor ordem n para qual não se sabe se existe uma matriz de Hadamard é $n = 668$.

Como consequência directa da demonstração do Teorema 9.18, obtém-se os corolários que se seguem.

Corolário 9.19. *Se H é uma matriz de Hadamard, normalizada, de ordem $n > 1$, então cada linha (coluna), com exceção da primeira, contém o mesmo número de entradas iguais a 1 e o mesmo número de entradas iguais a -1. Adicionalmente, cada par de linhas (colunas) tem o mesmo número de posições com entradas idênticas e o mesmo número de posições com entradas simétricas.*

Corolário 9.20. *Se H é uma matriz de Hadamard, normalizada, de ordem n , então o número de entradas iguais a 1 é $\frac{n(n+1)}{2}$ e o número de entradas iguais a -1 é $\frac{n(n-1)}{2}$.*

Exemplo 9.16. *Vamos mostrar que se H é uma matriz de Hadamard, de ordem n , então a matriz $\bar{H} = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ é uma matriz de Hadamard de ordem $2n$.*

Solução. Procedendo à multiplicação "por blocos" da matriz \bar{H} pela sua transposta, obtém-se

$$\begin{aligned} \bar{H}\bar{H}^T &= \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \begin{pmatrix} H^T & H^T \\ H^T & -H^T \end{pmatrix} = \begin{pmatrix} 2HH^T & 0 \\ 0 & 2HH^T \end{pmatrix} \\ &= \begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} = 2nI_{2n}. \end{aligned}$$
□

Note-se que, considerando as matrizes do Exemplo 9.15 e utilizando o procedimento do Exemplo 9.16, a matriz H_2 é obtida a partir de H_1 e a matriz H_4 a partir de H_2 . Repetindo este procedimento, podemos obter as matrizes de Hadamard de ordem 8, 16, ..., conforme a Figura 9.10 ilustra.

Apesar das múltiplas e interessantes propriedades algébricas das matrizes de Hadamard (por exemplo, são soluções do problema das matrizes de máximo determinante de entre as matrizes quadradas cujas entradas têm valor absoluto não superior a um) neste texto apenas vamos analisar algumas relações entre matrizes de Hadamard e *designs*.

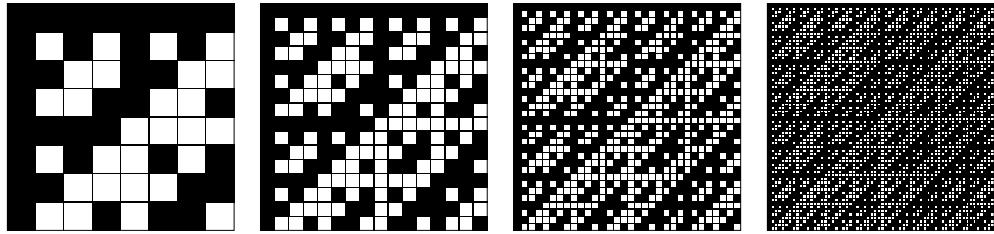


Figura 9.10: Matrizes de Hadamard obtidas pelo procedimento do Exemplo 9.16, para $n = 8, 16, 32$ e 64 .

Definição 9.11 (Design de Hadamard). *Designa-se por design de Hadamard de ordem n , todo o 2-design, com parâmetros $(4n - 1, 2n - 1, n - 1)$.*

Da definição decorre que o número de blocos de um $2 - (v, k, \lambda)$ design de Hadamard de ordem n é

$$b = \lambda \frac{v(v - 1)}{k(k - 1)} = (n - 1) \frac{(4n - 1)(4n - 2)}{(2n - 1)(2n - 2)} = 4n - 1 = v.$$

Logo, um *design* de Hadamard é um *design* simétrico.

Teorema 9.21 (de Hadamard). *Sendo $n > 1$, existe um design de Hadamard de ordem n se e só se existe uma matriz de Hadamard de ordem $4n$.*

Demonstração. Inicialmente vamos mostrar que se existe uma matriz de Hadamard normalizada H de ordem $4n$, com $n > 1$, então existe também um *design* de Hadamard de ordem n . Com efeito, a partir da matriz H podemos construir uma matriz quadrada A_H , de ordem $4n - 1$, retirando a primeira linha e a primeira coluna e substituindo todas as entradas -1 por 0 . Uma vez que cada linha de A_H tem, exactamente, $2n - 1$ entradas 1 e quaisquer duas colunas de A_H têm, exactamente, $n - 1$ uns nas mesmas posições, vem que a matriz A_H é uma matriz de incidência de um *design* $2 - (4n - 1, 2n - 1, n - 1)$.

Reciprocamente, podemos inverter este procedimento para obter uma matriz de Hadamard, a partir um design de Hadamard. Como efeito, suponhamos que existe um *design* $2 - (4n - 1, 2n - 1, n - 1)$, com $n > 1$, e seja A a respectiva matriz de incidência. Considerando a matriz H_A que se obtém de A substituindo os valores das entradas nulas por -1 e adicionando-lhe uma linha e uma coluna com entradas todas unitárias, conclui-se que H_A é uma matriz de Hadamard de ordem $4n$. \square

Exemplo 9.17. Dada a matriz de Hadamard 8×8

$$H = \begin{array}{|c|c|c|c|c|c|c|c|} \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline & & & & & & & \\ \hline \end{array}$$

vamos construir um *design* $2 - (7, 3, 1)$.

Solução. Recorrendo ao procedimento utilizado na demonstração do Teorema 9.21, obtém-se a matriz

$$A_H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

que é a matriz de incidência do *design* simétrico $2 - (7, 3, 1)$, com blocos $\{1, 4, 5\}, \{2, 4, 6\}, \{1, 2, 3\}, \{1, 6, 7\}, \{2, 5, 7\}, \{3, 5, 6\}, \{3, 4, 7\}$. \square

Exemplo 9.18. Dado o design 2 – (11, 5, 2) (X, \mathcal{B}) , com $X = \{1, 2, \dots, 11\}$ e $\mathcal{B} = \{\{1, 4, 8, 9, 10\}, \{2, 5, 9, 10, 11\}, \{1, 3, 6, 10, 11\}, \{1, 2, 4, 7, 11\}, \{1, 2, 3, 5, 8\}, \{2, 3, 4, 6, 9\}, \{3, 4, 5, 7, 10\}, \{4, 5, 6, 8, 11\}, \{1, 5, 6, 7, 9\}, \{2, 6, 7, 8, 10\}, \{3, 7, 8, 9, 11\}\}$, vamos determinar a matriz de Hadamard de ordem 12 que lhe corresponde.

Solução. Considerando a matriz de incidência do *design* (X, \mathcal{B}),

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

trocando os zeros por -1 e adicionando uma linha e uma coluna de uns, obtém-se a matriz de Hadamard

9.6. Exercícios

- 9.1. Para cada um dos ternos de parâmetros a seguir indicados, construa o respectivo 1-*design* (n, p, q) ou justifique porque é que um tal *design* não existe.

 - (a) $(n, p, q) = (6, 3, 1)$.
 - (b) $(n, p, q) = (5, 2, 1)$.
 - (c) $(n, p, q) = (7, 3, 3)$.
 - (d) $(n, p, q) = (9, 6, 4)$.

- 9.2. Qual o valor de λ para o *design* $1-(n, k, \lambda)$ cujos blocos são todos os k -subconjuntos de $\{1, 2, \dots, 7\}$.
- 9.3. Determine um *design* (X, \mathcal{B}) com parâmetros $2-(7, 3, 1)$.
- 9.4. Determine os parâmetros do *design* complementar do *design* $2-(7, 3, 1)$ (ou seja, do *design* que se obtém substituindo os blocos do *design* $2-(7, 3, 1)$ pelos seus complementares em $\{1, 2, \dots, 7\}$).
- 9.5. Prove que não existe um *design* com parâmetros:
- $2-(16, 6, 1)$;
 - $1-(16, 6, 3)$.
- 9.6. Prove que não existe $\lambda \in \mathbb{N}$ e um *design* (X, \mathcal{B}) que satisfaça os parâmetros $2-(6, 3, \lambda)$ e $1-(6, 3, \lambda)$.
- 9.7. Dado um sistema de triplos de Steiner $STS(n)$, prove que o seu número de blocos é $b = \frac{n(n-1)}{6}$.
- 9.8. Prove que apenas existem sistemas de triplos de Steiner $STS(n)$, para $n \in \{6j+1, 6j+3 : j \in \mathbb{N}\}$ (este resultado é conhecido por *teorema de existência de Kirkman*).
- 9.9. Considerando um conjunto de dois quadrados latinos ortogonais de ordem 3, construa um plano projectivo e um plano afim de ordem três.
- 9.10. Complete a tabela a seguir, onde se indicam os diferentes parâmetros de planos afins obtidos a partir de corpos de Galois:

corpo de Galois	número de pontos	número de rectas	cardinalidade de cada recta	número de rectas que passam por um ponto
		30		
	81			
			7	
$GF(2^4)$				32

- 9.11. Determine cada uma das seguintes rectas:
- a recta do plano afim $AF = (P, L)$, sobre \mathbb{Z}_7 , que é paralela a $x_2 = 4x_1 + 2$ e passa pelo ponto $(3, 6)$,
 - a recta do plano afim $AF = (P, L)$, sobre \mathbb{Z}_{11} , que é paralela a $2x_1 + 3x_2 + 4 = 0$ e passa pelo ponto $(10, 7)$.
- 9.12. Calcule (directamente) o número de pontos do plano projectivo $PG_2(\mathbb{Z}_p)$, onde p é primo.
- 9.13. Considerando o corpo \mathbb{Z}_5 , represente (graficamente) a recta $2x_1 + 3x_2 = 1$.
- 9.14. Considerando o corpo \mathbb{Z}_7 e sendo $B_a = \{a, a+1, a+3\}$, com $a \in \mathbb{Z}_7$, determine um 2-design com blocos B_a .
- 9.15. Qual é o número de quadrados latinos de ordem três (com entradas $\{1, 2, \dots, 9\}$)?
- 9.16. Mostre que não existe um sistema de triplos de Steiner $STS(n)$, com $n = 17$.
- 9.17. Utilizando o teorema de Bruck-Ryser que se segue, mostre que não existem 5 quadrados latinos mutuamente ortogonais de ordem 6.

Teorema (Bruck-Ryser). *Se $n \equiv 1 \pmod{4}$ ou $n \equiv 2 \pmod{4}$ e não existem $a, b \in \mathbb{N}$ tais que $n = a^2 + b^2$, então não existe um plano projectivo de ordem n .*

9.18. Seja (X, \mathcal{B}) um *design* $2 - (v, k, \lambda)$ e seja $\overline{\mathcal{B}} = \{X \setminus B : B \in \mathcal{B}\}$. Mostre que $(X, \overline{\mathcal{B}})$ é um *design* $2 - (v, v - k, b - 2k + \lambda)$ se $b - 2k + \lambda > 0$.

9.19. Sendo (X, \mathcal{B}) um *design* $2 - (7, 3, 1)$, determine o *design* $2 - (7, 4, 2)$.

9.20. Mostre que se H é uma matriz de Hadamard, então H^T é também uma matriz de Hadamard.

9.21. Mostre que se H é uma matriz de Hadamard de ordem n , então $|\det H| = n^{n/2}$.

9.22. Determine um *design* $2 - (15, 7, 3)$.

9.23. Construa um *design* $2 - (13, 9, 6)$.

9.24. Tendo em conta que dadas duas matrizes $A = (a_{ij})$ de dimensão $m \times n$ e $B = (b_{ij})$ de dimensão $p \times r$, por definição, o *produto de Kronecker* \otimes destas matrizes corresponde à matriz de dimensão $mp \times nr$

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix},$$

mostre que se H_m e H_n são matrizes de Hadamard de ordem, respectivamente, m e n , então a matriz $H_m \otimes H_n$ é uma matriz de Hadamard de ordem mn .

9.25. Mostre que se A_1 e A_2 são dois quadrados latinos ortogonais de ordem m e B_1 e B_2 são dois quadrados latinos ortogonais de ordem n , então $A_1 \otimes B_1$ e $A_2 \otimes B_2$ são dois quadrados latinos ortogonais de ordem mn .

9.26. Seja $A = H_2 = \boxed{}$. Determine os matrizes $B = A \otimes A$ e $C = A \otimes B$.

9.27. Considerando uma família de conjuntos (blocos) que são os complementares das rectas do plano de Fano, demonstre que uma tal família constitui um *design* e determine os seus parâmetros.

9.28. Determine um *design* com seguintes parâmetros (onde b denota o número de blocos e r o número de réplicas de cada elemento do conjunto de cardinalidade v):

- (a) $v = b = 7, k = r = 3, \lambda = 1$;
- (b) $v = b = 13, k = r = 4, \lambda = 1$;
- (c) $v = 9, b = 12, k = 3, r = 4, \lambda = 1$;
- (d) $v = 6, b = 10, k = 3, r = 5, \lambda = 2$.

9.29. Verifique se existe algum *design* $t - (v, k, \lambda)$ com seguintes parâmetros (onde tanto b como r se referem à notação utilizada no exercício anterior):

- (a) $v = 15, b = 21, k = 4, r = 7, \lambda = 2$;
- (b) $v = b = 23, k = r = 7, \lambda = 2$;
- (c) $v = b = 43, k = r = 7, \lambda = 2$;
- (d) $v = 36, b = 42, k = 6, r = 7, \lambda = 1$.

9.30. Verifique qual ou quais dos parâmetros, a seguir apresentados, satisfazem as condições necessárias de existência de um *design* simétrico $2 - (v, k, \lambda)$.

- (a) $v = 21, k = 5, \lambda = 1;$
- (b) $v = 15, k = 7, \lambda = 3;$
- (c) $v = 19, k = 9, \lambda = 4;$
- (d) $v = 29, k = 8, \lambda = 2.$

10

Álgebras de Boole

Este capítulo evidencia a grande semelhança existente entre a teoria dos conjuntos e o cálculo proposicional. Note-se que esta semelhança não é fruto do acaso, uma vez que a teoria das álgebras de Boole constitui uma generalização, quer do cálculo proposicional, quer da teoria dos conjuntos. Para além da introdução das álgebras de Boole, apresentam-se os circuitos lógicos, como aplicação do cálculo proposicional, estudam-se isomorfismos entre álgebras de Boole e o teorema da representação de Stone, e analisa-se a simplificação de funções booleanas com recurso aos mapas de Karnaugh.

10.1. Definições e resultados básicos

Vamos iniciar este estudo com dois exemplos de duas álgebras muito conhecidas, a *álgebra das partes de um conjunto fixo* e a *álgebra dos valores lógicos*.

Exemplo 10.1. Álgebra das partes de um conjunto.

Seja Ω um conjunto fixo e $\mathcal{P}(\Omega)$ o conjunto de todos os subconjuntos de Ω . Este conjunto, $\mathcal{P}(\Omega)$, é conhecido por conjunto das partes de Ω (ou por conjunto potência do conjunto Ω , denotando-se também por 2^Ω). No conjunto $\mathcal{P}(\Omega)$ podemos definir duas operações com dois argumentos: a união de conjuntos \cup e a intersecção de conjuntos \cap . Sabe-se que estas operações satisfazem as propriedades de comutatividade, associatividade, distributividade e de absorção, ou seja, $\forall A, B, C \in \mathcal{P}(\Omega)$ verifica-se a

- comutatividade da reunião e da intersecção:

$$A \cup B = B \cup A \quad \text{e} \quad A \cap B = B \cap A;$$

- associatividade da reunião e da intersecção:

$$A \cup (B \cup C) = (A \cup B) \cup C \quad \text{e} \quad A \cap (B \cap C) = (A \cap B) \cap C;$$

- distributividade da reunião relativamente à intersecção e da intersecção relativamente à reunião:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{e} \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$

- absorção:

$$A \cup (A \cap B) = A \quad \text{e} \quad A \cap (A \cup B) = A.$$

Considerando os dois elementos particulares de $\mathcal{P}(\Omega)$ que são o conjunto vazio que se denota por \emptyset e o próprio conjunto Ω , sabe-se que $\forall A \in \mathcal{P}(\Omega)$ se verifica a propriedade de

- *dominância:*

$$A \cap \emptyset = \emptyset \quad e \quad A \cup \Omega = \Omega.$$

Finalmente, podemos concluir que $\forall A \in \mathcal{P}(\Omega)$ existe um conjunto $A^c \in \mathcal{P}(\Omega)$ que verifica a propriedade de

- *complementaridade:*

$$A \cap A^c = \emptyset \quad e \quad A \cup A^c = \Omega,$$

onde se conclui que $A^c = \Omega \setminus A$.

É claro que a álgebra das partes de um conjunto tem mais propriedades do que as indicadas, apenas se escolheram estas, pela a sua estrita ligação à definição de uma estrutura mais geral.

Exemplo 10.2. Álgebra dos valores lógicos.

Vamos utilizar o símbolo 0 para denotar "falso" e o símbolo 1 para denotar "verdadeiro". Nesta álgebra temos (pelo menos) duas operações com dois argumentos: a disjunção \vee e a conjunção \wedge , e uma operação com um único argumento: a negação \neg .

Dadas as proposições p , q e r , podemos concluir as seguintes propriedades:

- (comutatividade da disjunção e da conjunção):

$$p \vee q = q \vee p \quad e \quad p \wedge q = q \wedge p;$$

- (associatividade da disjunção e da conjunção):

$$p \vee (q \vee r) = (p \vee q) \vee r \quad e \quad p \wedge (q \wedge r) = (p \wedge q) \wedge r;$$

- (absorção):

$$p \vee (p \wedge q) = p \quad e \quad p \wedge (p \vee q) = p;$$

- (distributividade):

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r) \quad e \quad p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r);$$

- (dominância):

$$p \wedge 0 = 0 \quad e \quad p \vee 1 = 1;$$

- (complementaridade):

$$p \vee \neg p = 1 \quad e \quad p \wedge \neg p = 0.$$

Note-se que, para além dos símbolos referidos, é comum utilizarem-se ainda os símbolos e designações:

"F", falso para 0;
"T", "V", verdadeiro para 1;
+, soma lógica, ou inclusivo para \vee ;
·, &, produto lógico para \wedge ;
\neg , \sim , \sim , negação para \neg .

□

A afinidade existente entre a estrutura da álgebra das partes de um conjunto e a estrutura da álgebra dos valores lógicos sugeriu a introdução de uma estrutura mais geral que foi, precisamente, a estrutura considerada por George Boole (1815–1864) no ano de 1854. Esta estrutura que agora designamos por álgebra de Boole foi introduzida no Capítulo 7 (Definição 7.14) como reticulado distributivo e complementado. Segue-se um estudo detalhado das propriedades das álgebras de Boole.

Definição 10.1 (Álgebra de Boole). Uma álgebra de Boole é um sistema $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$, onde B é um conjunto, \sqcup e \sqcap são operações binárias definidas em B (ou seja, $\sqcup, \sqcap : B \times B \rightarrow B$), $'$ é uma operação unária definida em B (ou seja, $' : B \rightarrow B$) e $\mathbf{0}$, $\mathbf{1}$ são dois elementos distintos de B . Adicionalmente, quaisquer que sejam $x, y, z \in B$, verificam-se as propriedades de

- comutatividade:

$$x \sqcup y = y \sqcup x, \quad (10.1)$$

$$x \sqcap y = y \sqcap x, \quad (10.2)$$

- associatividade:

$$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z, \quad (10.3)$$

$$x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z, \quad (10.4)$$

- distributividade de \sqcap relativamente a \sqcup e de \sqcup relativamente a \sqcap :

$$x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z), \quad (10.5)$$

$$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z), \quad (10.6)$$

- absorção:

$$x \sqcup (x \sqcap y) = x, \quad (10.7)$$

$$x \sqcap (x \sqcup y) = x, \quad (10.8)$$

- dominância:

$$x \sqcap \mathbf{0} = \mathbf{0}, \quad (10.9)$$

$$x \sqcup \mathbf{1} = \mathbf{1}, \quad (10.10)$$

- complementaridade: para cada $x \in B$ existe $x' \in B$ tal que

$$x \sqcap x' = \mathbf{0} \quad (10.11)$$

$$x \sqcup x' = \mathbf{1}. \quad (10.12)$$

Na álgebra de Boole \mathcal{B} , o conjunto B designa-se por base da álgebra, a operação \sqcap designa-se por produto, a operação \sqcup por adição e a operação unária $'$ por complementação.

Para simplificar o texto, na ausência de qualquer possibilidade de confusão, designaremos a álgebra de Boole, simplesmente, por álgebra de Boole B , em vez de álgebra de Boole $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$.

Com facilidade se verifica que a álgebra das partes de um conjunto e a álgebra dos valores lógicos são ambas álgebras de Boole.

1. Com efeito, no primeiro caso (álgebra das partes de um conjunto fixo Ω), definindo-se o sistema

$$\langle \mathcal{P}(\Omega), \cup, \cap, {}^c, \emptyset, \Omega \rangle,$$

tendo em conta as propriedades descritas no Exemplo 10.1, conclui-se, imediatamente, que as condições (10.1)–(10.12) se verificam.

2. No segundo caso (álgebra dos valores lógicos), considerando o sistema

$$\langle \{0, 1\}, \vee, \wedge, \neg, 0, 1 \rangle$$

e, tendo em conta as propriedades descritas no Exemplo 10.2, conclui-se, mais uma vez, que as condições (10.1)–(10.12) se verificam. Deve notar-se ainda que esta álgebra dos valores lógicos é a menor das álgebras de Boole (no sentido da cardinalidade da base) e, uma vez que, por definição, $\mathbf{0} \neq \mathbf{1}$, podemos também concluir que qualquer álgebra de Boole tem, pelo menos, dois elementos.

De agora em diante vamos denotar por \mathbb{B} o conjunto de componentes binárias, ou seja,

$$\mathbb{B} = \{0, 1\}.$$

Segue-se mais um exemplo de uma álgebra de Boole.

Exemplo 10.3. Seja \mathbb{B}^n o conjunto dos n -uplos de componentes binárias. Dados os n -uplos (a_1, \dots, a_n) , $(b_1, \dots, b_n) \in \mathbb{B}^n$, definindo as operações \sqcup , \sqcap e $'$ por

$$\begin{aligned}(a_1, \dots, a_n) \sqcup (b_1, \dots, b_n) &= (\max\{a_1, b_1\}, \dots, \max\{a_n, b_n\}), \\ (a_1, \dots, a_n) \sqcap (b_1, \dots, b_n) &= (\min\{a_1, b_1\}, \dots, \min\{a_n, b_n\}), \\ (a_1, \dots, a_n)' &= (1 - a_1, \dots, 1 - a_n),\end{aligned}$$

vamos provar que o sistema $\langle \mathbb{B}^n, \sqcup, \sqcap, ', (0, \dots, 0), (1, \dots, 1) \rangle$ é uma álgebra de Boole.

Solução. Com efeito, uma vez que as propriedades de comutatividade, associatividade, dominância e complementaridade são claramente satisfeitas, resta mostrar as propriedades de distributividade e absorção. Tendo em conta a semilitude das provas para ambas as propriedades de dominância e ambas as propriedades de absorção, apenas vamos fazer a prova de uma delas em cada um dos casos. Por outro lado, tendo em conta que as operações são realizadas componente a componente (segundo a mesma regra), basta fazer a prova para uma das componentes. Assim, para $i \in \{1, 2, \dots, n\}$, vamos considerar as componentes $a_i, b_i, c_i \in \mathbb{B}$ dos n -uplos a, b e c .

Distributividade: Vamos provar que $\forall a_i, b_i, c_i \in \mathbb{B}$

$$\max\{a_i, \min\{b_i, c_i\}\} = \min\{\max\{a_i, b_i\}, \max\{a_i, c_i\}\}. \quad (10.13)$$

Embora se possa provar esta igualdade recorrendo a métodos algébricos, vamos fazer esta prova utilizando um método mais representativo, no contexto das álgebras de Boole, o método da tabela dos valores binários. Denote-se por E e D , respectivamente, a parte direita e esquerda da igualdade (10.13), isto é,

$$\begin{aligned}E &= \max\{a_i, \min\{b_i, c_i\}\}, \\ D &= \min\{\max\{a_i, b_i\}, \max\{a_i, c_i\}\}.\end{aligned}$$

Tendo em conta que na Tabela 10.1 se representam todos os valores possíveis para E e D , podemos concluir que para quaisquer valores a_i, b_i e c_i se verifica a igualdade $E = D$.

a_i	b_i	c_i	$\alpha = \min\{b_i, c_i\}$	$E = \max\{a_i, \alpha\}$	$\beta = \max\{a_i, b_i\}$	$\gamma = \max\{a_i, c_i\}$	$D = \min\{\beta, \gamma\}$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Tabela 10.1: Valores binários para a fórmula (10.13).

Absorção: Vamos provar que $\forall a_i, b_i \in \mathbb{B}$

$$\max\{a_i, \min\{a_i, b_i\}\} = a_i. \quad (10.14)$$

Com efeito, a partir da tabela dos valores binários apresentada na Tabela 10.2, podemos verificar que a primeira e a última colunas são iguais. \square

a_i	b_i	$\min\{a_i, b_i\}$	$\max\{a_i, \min\{a_i, b_i\}\}$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

Tabela 10.2: Valores binários para a fórmula (10.14).

Definição 10.2 (Expressão dual). *Dada a álgebra de Boole $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ e sendo E uma expressão de \mathcal{B} , designa-se por expressão dual de E e denota-se por \bar{E} , a expressão que se obtém de E trocando \sqcup por \sqcap , \sqcap por \sqcup , $\mathbf{0}$ por $\mathbf{1}$ e $\mathbf{1}$ por $\mathbf{0}$.*

Teorema 10.1 (Princípio da dualidade). *Seja $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole e seja E uma expressão de \mathcal{B} . Se E decorre directamente dos axiomas da álgebra \mathcal{B} então também a expressão dual \bar{E} é consequência directa dos mesmos axiomas.*

Demonstração. Uma vez que os axiomas que definem as álgebras de Boole se podem agrupar em pares de axiomas duais um do outro, partindo da prova da expressão E e trocando todas as expressões intermédias por expressões duais, obtém-se uma demonstração para a expressão \bar{E} . \square

Teorema 10.2. *Se $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ é uma álgebra de Boole, então os elementos $\mathbf{0}$ e $\mathbf{1}$ são únicos e, para cada $a \in B$, o elemento a' é também único.*

Demonstração. Suponhamos que numa álgebra de Boole \mathcal{B} existem dois elementos $\mathbf{0}$, os quais vamos denotar por 0_a e 0_b . Nestas condições, pela propriedade de dominância (10.9), vem

$$0_a \sqcap 0_b = 0_b, \quad 0_b \sqcap 0_a = 0_a.$$

Porém, uma vez que \sqcap é uma operação comutativa, podemos concluir que $0_a = 0_b$ e, consequentemente, que $\mathbf{0}$ é único.

De modo semelhante se prova a unicidade do elemento $\mathbf{1}$. Com efeito, supondo que existem dois elementos $\mathbf{1}$, os quais vamos denotar por 1_a e 1_b , aplicando a propriedade de dominância (10.10), vem

$$1_a \sqcup 1_b = 1_b, \quad 1_b \sqcup 1_a = 1_a.$$

Porém, dado que a operação \sqcup também é comutativa, podemos concluir que $1_a = 1_b$ e, consequentemente, que $\mathbf{1}$ é único. Deve observar-se que a unicidade de $\mathbf{1}$ decorre directamente da princípio da dualidade aplicado à prova da unicidade do elemento $\mathbf{0}$.

Vamos mostrar agora que dado um elemento arbitrário da álgebra de Boole \mathcal{B} , o seu complementar é único. Assim, seja a um elemento arbitrário da álgebra de Boole \mathcal{B} e seja x um elemento complementar de a . Então

$$\begin{aligned}
x &= x \sqcap (x \sqcup x') && \text{(absorção)} \\
&= x \sqcap \mathbf{1} && \text{(complementaridade)} \\
&= x \sqcap (a \sqcup a') && \text{(complementaridade)} \\
&= (x \sqcap a) \sqcup (x \sqcap a') && \text{(distributividade)} \\
&= \mathbf{0} \sqcup (x \sqcap a') && \text{(complementaridade)} \\
&= (a \sqcap a') \sqcup (x \sqcap a') && \text{(complementaridade)} \\
&= (a \sqcup x) \sqcap a' && \text{(distributividade)} \\
&= \mathbf{1} \sqcap a' && \text{(complementaridade)} \\
&= (a \sqcup a') \sqcap a' && \text{(complementaridade)} \\
&= a' && \text{(absorção).}
\end{aligned}$$

Logo, $x = a'$ e, consequentemente, a' é único. \square

Seguem-se mais algumas propriedades das álgebras de Boole, das quais, tendo em conta o princípio da dualidade, vamos provar apenas uma para cada um dos respectivos pares duais.

Teorema 10.3. Se $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ é uma álgebra de Boole, então $\forall a \in B$ verificam-se as seguintes propriedades:

1. $\mathbf{0}' = \mathbf{1}$ e $\mathbf{1}' = \mathbf{0}$;
2. $(a')' = a$; (propriedade da dupla complementaridade)
3. $a \sqcap a = a$ e $a \sqcup a = a$; (propriedade da idempotência)
4. $a \sqcap \mathbf{1} = a$ e $a \sqcup \mathbf{0} = a$. (propriedade do elemento neutro)

Demonstração. Vamos fazer a prova apenas para uma propriedade de cada um dos pares de propriedades duais.

1. Tendo em conta os axiomas de dominância e comutatividade, $\mathbf{0} \sqcup \mathbf{1} = \mathbf{1}$ e $\mathbf{0} \sqcap \mathbf{1} = \mathbf{1} \sqcap \mathbf{0} = \mathbf{0}$. Logo, podemos concluir que o elemento complementar de $\mathbf{0}$ é o elemento $\mathbf{1}$, ou seja, $\mathbf{0}' = \mathbf{1}$.
2. Por aplicação dos axiomas de complementaridade e comutatividade, $a' \sqcup a = a \sqcup a' = \mathbf{1}$ e $a' \sqcap a = a \sqcap a' = \mathbf{0}$. Então o elemento complementar de a' é o elemento a , pelo que $(a')' = a$. Note-se que no cálculo proposicional esta propriedade é conhecida por propriedade da *dupla negação*.
3. Se $x = a \sqcup a$, então

$$\begin{aligned}
x \sqcup a' &= (a \sqcup a) \sqcup a' && \text{(definição de } x\text{)} \\
&= a \sqcup (a \sqcup a') && \text{(associatividade)} \\
&= a \sqcup \mathbf{1} && \text{(complementaridade)} \\
&= \mathbf{1} && \text{(dominância)}
\end{aligned}$$

e

$$\begin{aligned}
x \sqcap a' &= (a \sqcup a) \sqcap a' && \text{(definição de } x\text{)} \\
&= (a \sqcap a') \sqcup (a \sqcap a') && \text{(distributividade)} \\
&= \mathbf{0} \sqcup \mathbf{0} && \text{(complementaridade)} \\
&= \mathbf{0} \sqcup (\mathbf{0} \sqcap a) && \text{(complementaridade)} \\
&= \mathbf{0} && \text{(dominância).}
\end{aligned}$$

Logo, x é o elemento complementar de a' e, tendo em conta propriedade da dupla complementaridade, $a \sqcup a = a$.

4.

$$\begin{aligned}
 a \sqcap \mathbf{1} &= a \sqcap (a \sqcup a') && (\text{complementaridade}) \\
 &= (a \sqcap a) \sqcup (a \sqcap a') && (\text{distributividade}) \\
 &= (a \sqcap a) \sqcup \mathbf{0} && (\text{complementaridade}) \\
 &= a \sqcup \mathbf{0} && (\text{idempotência}) \\
 &= a \sqcup (a \sqcap \mathbf{0}) && (\text{complementaridade}) \\
 &= a && (\text{dominância}). \quad \square
 \end{aligned}$$

No próximo teorema introduzem-se dois dos resultados mais conhecidos das álgebras de Boole, demonstrados por Augustos De Morgan (1806-1871), conhecidos por *leis de De Morgan* e que foram já referidos no Capítulo 1.

Teorema 10.4 (Leis de De Morgan). *Seja $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole. Então $\forall a, b \in B$ verificam-se as igualdades*

$$(a \sqcup b)' = a' \sqcap b' \quad \text{e} \quad (a \sqcap b)' = a' \sqcup b'.$$

Demonstração. Mostrar que $(a \sqcup b)' = a' \sqcap b'$ é equivalente a mostrar que os elementos $a \sqcup b$ e $a' \sqcap b'$ são complementares um de outro. Para tal, basta mostrar que $(a \sqcup b) \sqcap (a' \sqcap b') = \mathbf{0}$ e $(a \sqcup b) \sqcup (a' \sqcap b') = \mathbf{1}$. Assim,

$$\begin{aligned}
 (a \sqcup b) \sqcap (a' \sqcap b') &= (a \sqcap a' \sqcap b') \sqcup (b \sqcap a' \sqcap b') && (\text{distributividade}) \\
 &= (a \sqcap a' \sqcap b') \sqcup (b \sqcap b' \sqcap a') && (\text{comutatividade}) \\
 &= ((a \sqcap a') \sqcap b') \sqcup ((b \sqcap b') \sqcap a') && (\text{associatividade}) \\
 &= (\mathbf{0} \sqcap b') \sqcup (\mathbf{0} \sqcap a') && (\text{complementaridade}) \\
 &= \mathbf{0} \sqcup \mathbf{0} && (\text{dominância}) \\
 &= \mathbf{0} && (\text{idempotência})
 \end{aligned}$$

e

$$\begin{aligned}
 (a \sqcup b) \sqcup (a' \sqcap b') &= (a \sqcup b \sqcup a') \sqcap (a \sqcup b \sqcup b') && (\text{distributividade}) \\
 &= (a \sqcup a' \sqcup b) \sqcap (a \sqcup b \sqcup b') && (\text{comutatividade}) \\
 &= ((a \sqcup a') \sqcup b) \sqcap (a \sqcup (b \sqcup b')) && (\text{associatividade}) \\
 &= (\mathbf{1} \sqcup b) \sqcap (a \sqcup \mathbf{1}) && (\text{complementaridade}) \\
 &= \mathbf{1} \sqcap \mathbf{1} && (\text{dominância}) \\
 &= \mathbf{1} && (\text{idempotência}). \quad \square
 \end{aligned}$$

10.2. Cálculo proposicional e circuitos lógicos

Uma das álgebras de Boole mais conhecidas é a álgebra $\langle \{0, 1\}, \vee, \wedge, \neg, 0, 1 \rangle$ dos valores lógicos (ver Exemplo 10.2). Trata-se também da menor das álgebras de Boole, no sentido da cardinalidade da base. Nesta álgebra, é usual a utilização de tabelas de verdade para a determinação dos valores lógicos de expressões em função dos valores lógicos das respectivas variáveis. Note-se que a Tabela 1.2 do capítulo 1 é a tabela de verdade das operações de negação (\neg), disjunção (\vee) e conjunção (\wedge).

Seguem-se mais algumas operações, de entre as 16 operações que se podem definir nesta álgebra.

\Rightarrow — Implicação.

\Leftrightarrow — Equivalência.

$\dot{\vee}$ — Disjunção exclusiva (ou exclusivo, xor).

$\bar{\wedge}$ — Incompatibilidade (e-não, negação conjunta, nand).

$\underline{\vee}$ — Rejeição (ou-não, nem-nem, nor).

Observe-se que as designações *xor*, *nand* e *nor*, são as usualmente utilizadas em circuitos lógicos.

Na Tabela 10.3 definem-se todas estas operações. Note-se que não existem símbolos universais para as operações *ou exclusivo*, *e-não* e *ou-não*. Por exemplo, para o *ou exclusivo* também se utiliza o símbolo \oplus , o qual, por sua vez, também é muito utilizado (nas álgebras de Boole e não só) para denotar a adição módulo 2 e para a soma simples de álgebras de Boole.

p	q	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \dot{\vee} q$	$p \underline{\vee} q$	$p \bar{\wedge} q$
0	0	1	1	0	1	1
0	1	1	0	1	0	1
1	0	0	0	1	0	1
1	1	1	1	0	0	0

Tabela 10.3: Tabela de verdade para a *implicação*, *equivalência*, *ou exclusivo*, *e-não* e *ou-não*.

Exemplo 10.4. Vamos determinar as "novas" operações introduzidas na álgebra dos valores lógicos (isto é, a *implicação*, *equivalência*, *ou exclusivo*, *e-não* e *ou-não*) em função das operações definidoras das álgebras de Boole.

Solução.

- $x \Rightarrow y$ é equivalente a $\neg x \vee y$.
- $x \Leftrightarrow y$ é equivalente a $(x \wedge y) \vee (\neg x \wedge \neg y)$.
- $x \dot{\vee} y$ é equivalente a $(x \wedge \neg y) \vee (\neg x \wedge y)$.
- $x \underline{\vee} y$ é equivalente a $\neg(x \vee y)$.
- $x \bar{\wedge} y$ é equivalente a $\neg(x \wedge y)$.

□

A tecnologia digital, particularmente a electrónica digital e os computadores digitais, baseia-se em circuitos lógicos que utilizam todas estas operações lógicas. Neste contexto, tais operadores designam-se, usualmente, por *portas lógicas*. Dependendo da tecnologia, existem diferentes conjuntos de portas lógicas disponíveis. Frequentemente, temos portas de *negação*, *conjunção*, *disjunção* e *ou exclusivo*. Estas portas são representadas na Figura 10.1. Note-se que, nestas portas, o pequeno círculo denota a negação e existem portas *e*, *e-não*, *ou* e *ou-não* com mais do que duas entradas.

Os circuitos lógicos dividem-se em dois tipos. Aqueles em que os estados à saída dependem apenas dos estados à entrada, os quais se designam por *circuitos combinatórios* e os circuitos lógicos cujos estados à saída dependem não só dos estados à entrada mas também dos estados anteriores, os quais se designam por *circuitos sequenciais* ou *circuitos com memória*. Neste texto, vamos analisar apenas os circuitos combinatórios.

Exemplo 10.5. Vamos determinar os circuitos lógicos para calcular a soma módulo dois (\oplus) de

- (a) duas variáveis binárias,
- (b) três variáveis binárias.

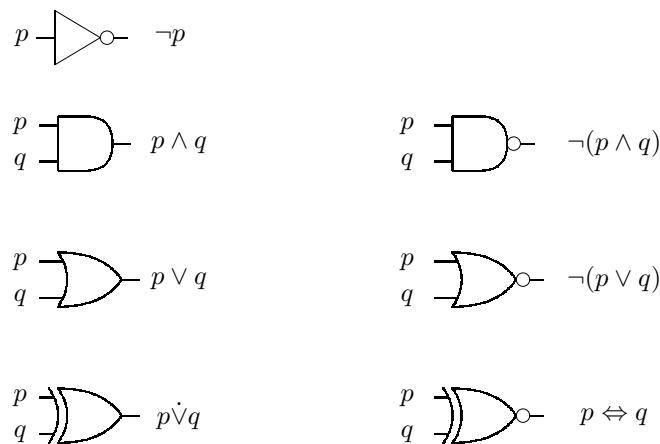


Figura 10.1: Portas lógicas.

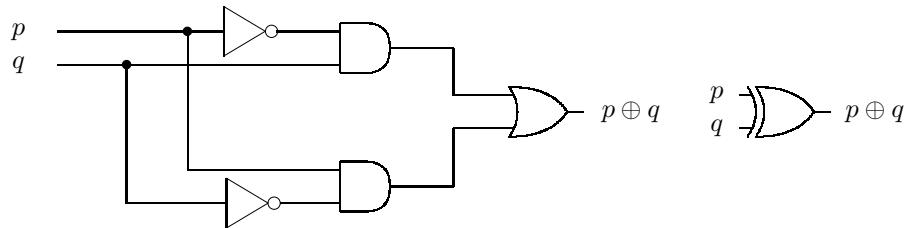
Solução. Note-se que a soma módulo dois é igual a 0 se e só se o número de uns é par.

Parte (a). Na Tabela 10.4 apresenta-se a tabela de valores da soma módulo 2 com duas realizações lógicas.

p	q	$p \oplus q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$	$p \dot{\vee} q$
0	0	0	0	0
0	1	1	1	1
1	0	1	1	1
1	1	0	0	0

Tabela 10.4: Tabela de valores da soma módulo 2 de duas variáveis binárias.

Assim, podemos apresentar (ver Figura 10.2) dois circuitos combinatórios distintos para esta soma. O primeiro só com portas *e*, *ou*, e de negação e o segundo com a utilização de uma única porta *ou exclusivo*.

Figura 10.2: Circuitos lógicos para o cálculo da expressão $p \oplus q$.

Parte (b). No caso de três variáveis binárias, na Tabela 10.5 apresentam-se duas fórmulas para calcular $p \oplus q \oplus r$. Note-se que a fórmula representada é mais simples do que a que se obtém utilizando apenas portas *ou* e *e*.

p	q	r	$p \oplus q \oplus r$	α	$\neg(p \vee q) \vee r$
0	0	0	0	0	0
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	0	0	0
1	0	0	1	1	1
1	0	1	0	0	0
1	1	0	0	0	0
1	1	1	1	1	1

Tabela 10.5: Tabela de valores da soma módulo dois de três variáveis binárias, onde $\alpha = (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r)$.

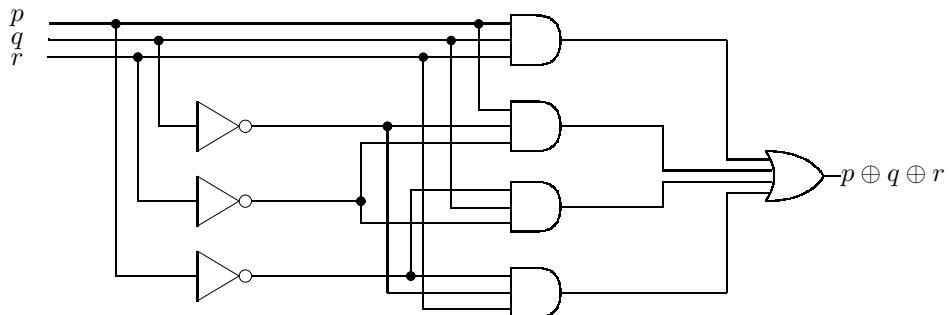


Figura 10.3: Circuito lógico para o cálculo de $p \oplus q \oplus r$.

A Figura 10.3 representa a realização deste circuito só com portas *não*, *ou* e *e* (note-se que são utilizadas portas com mais do que duas entradas). Por sua vez, na Figura 10.4, apresenta-se uma realização recorrendo unicamente a portas *ou exclusivo*.

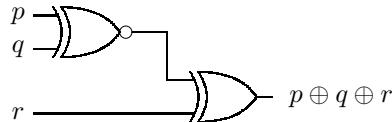


Figura 10.4: Circuito lógico para o cálculo de $p \oplus q \oplus r$, com utilização, unicamente, de portas *ou exclusivo* e *ou exclusivo-não*

Antes de prosseguirmos com mais exemplos, convém introduzir alguma informação sobre sistemas de numeração e sobre números binários.

Basicamente, podemos classificar os sistemas de numeração em *posicionais* e *não posicionais*. Como exemplo de sistema de numeração não posicional temos o sistema de numeração romano. Com efeito, neste sistema, o valor de um algarismo não depende da posição que o algarismo ocupa no número. Por exemplo, a sequência de algarismos III, onde a cada algarismo corresponde o valor 1, representa o número 3 que corresponde, precisamente à soma dos dígitos. Neste texto, porém, apenas vamos considerar sistemas de numeração posicionais.

Para cada sistema de numeração posicional existe um número especial b que se designa por *base do sistema* e um conjunto \mathcal{D} de dígitos. Neste texto, apenas vamos considerar sistemas de numeração com base inteira não inferior a dois. No entanto, existem também sistemas de base negativa e/ou não inteira. Os sistemas de numeração mais utilizados são o sistema *decimal*, cuja base é $b = 10$, o *binário*, cuja base é $b = 2$, o *hexadecimal*, cuja base é $b = 16$ e o *octal* que tem base $b = 8$.

Se b é uma base inteira não inferior a 2 então o respectivo conjunto de algarismos vem definido por

$$\mathcal{D} = \{0, 1, \dots, b - 1\}.$$

No caso do sistema decimal, obtém-se o conjunto de dígitos $\{0, 1, \dots, 9\}$, para o sistema binário obtém-se apenas dois dígitos $\{0, 1\}$, para o sistema octal o respectivo conjunto de dígitos é $\{0, 1, 2, 3, 4, 5, 6, 7\}$ e para o sistema hexadecimal obtém-se o conjunto de dezasseis dígitos $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$. Neste último caso, deve observar-se que se utilizam vários dígitos maiores do que nove. Assim, o dígito dez é denotado por A , o dígito onze por B , ..., e o dígito quinze por F .

Em geral, um número na base b é representado pela sequência de dígitos

$$(c_n c_{n-1} c_{n-2} \dots c_2 c_1 c_0, c_{-1} c_{-2} \dots c_{-m})_b$$

onde $c_i \in \mathcal{D}$ para $i = -m, \dots, n$. O índice i do dígito c_i designa-se por *posição* do dígito. Por simplicidade de escrita, na base mais frequentemente utilizada, a base 10, usualmente, não se escrevem nem os parêntesis nem o índice 10. Por exemplo, o número decimal $(1234, 56)_{10}$ escreve-se, simplesmente,

$$1234, 56$$

e, neste caso, conclui-se que $n = 3$, $m = 2$, que o dígito 1 está na posição 3, o dígito 2 ocupa a posição 2, o dígito 3 está na posição 1, o dígito 4 na posição 0, o dígito 5 ocupa a posição -1 , e o dígito 6 ocupa a posição -2 .

O valor (na base decimal) de um número numa base arbitrária b , vem dado por

$$(c_n c_{n-1} c_{n-2} \dots c_2 c_1 c_0, c_{-1} c_{-2} \dots c_{-m})_b = \sum_{k=-m}^n c_k b^k. \quad (10.15)$$

Como exemplo, vamos considerar o número binário

$$\begin{aligned} (1101, 01)_2 &= 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 + 0 \cdot 2^{-1} + 1 \cdot 2^{-2} \\ &= 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 + 0 \cdot \frac{1}{2} + 1 \cdot \frac{1}{4} \\ &= 8 + 4 + 0 + 1 + 0 + 0,25 \\ &= 13,25 \end{aligned}$$

e o número hexadecimal

$$\begin{aligned} (\text{F5A}, 2)_{16} &= 15 \cdot 16^2 + 5 \cdot 16^1 + 10 \cdot 16^0 + 2 \cdot 16^{-1} \\ &= 15 \cdot 256 + 5 \cdot 16 + 10 \cdot 1 + 2 \cdot \frac{1}{16} \\ &= 3840 + 80 + 10 + 0,125 \\ &= 3930,125. \end{aligned}$$

Em qualquer sistema posicional, a operação de adição realiza-se com a aplicação do mesmo algoritmo. Por exemplo, para se determinar a soma dos números binários $a = (1011, 110)_2$ e $b = (101, 101)_2$, procede-se do seguinte modo:

1. Somam-se os últimos dígitos de a e b e obtém-se $0 + 1 = (01)_2$, pelo que o último dígito de $a + b$ é 1 e o dígito de transporte é 0;
2. Somam-se os penúltimos dígitos de a e b com o dígito de transporte decorrente da soma anterior e obtém-se $0 + 1 + 0 = (01)_2$, pelo que o penúltimo dígito de $a + b$ é 1 e o dígito de transporte é 0;
3. Somam-se os antepenúltimos dígitos de a e b com o dígito de transporte decorrente da soma anterior e obtém-se $0 + 1 + 1 = (10)_2$, pelo que o antepenúltimo dígito de $a + b$ é 0 e o dígito de transporte é 1;

4. Somam-se os terceiros dígitos de a e b com o dígito de transporte decorrente da soma anterior e obtém-se $1 + 1 + 1 = (11)_2$, pelo que o terceiro dígito de $a + b$ é 1 e o dígito de transporte é 1;
 5. etc.

Como consequência, o algoritmo da soma completa-se do seguinte modo:

$$\begin{array}{r}
 1\ 1\ 1\ 1\ 1, \ 0\ 0 \quad \text{transporte} \\
 1\ 0\ 1\ 1, \ 1\ 1\ 0 \quad a \\
 + \ 1\ 0\ 1, \ 1\ 0\ 1 \quad b \\
 \hline
 1\ 0\ 0\ 0\ 1, \ 0\ 1\ 1 \quad a + b
 \end{array}$$

Note-se que os valores $a = (1011, 110)_2 = 11,75$, $b = (101, 101)_2 = 5,625$ e $a + b = (10001, 011)_2 = 17,375$ confirmam o resultado obtido.

Exemplo 10.6. Vamos determinar os circuitos lógicos para o cálculo da soma de

- (a) dois dígitos binários, (somador parcial; half adder; HA)
 (b) três dígitos binários. (somador completo; full adder; FA)

Solução. Uma vez que no sistema binário $0 = (00)_2$, $1 = (01)_2$, $2 = (10)_2$ e $3 = (11)_2$, conclui-se que para a representação binária do resultado da soma de dois ou três dígitos binários são necessários dois dígitos binários. Vamos denotar os dígitos binários que representam o resultado por T e s e os dígitos binários de entrada por a , b e t . No Exemplo 10.7, a seguir, dar-se-à uma explicação do significado desta notação. Por agora, basta saber que s é o bit da soma e que tanto t como T são dígitos binários de transporte (à entrada e saída, respectivamente).

Parte (a). Na Tabela 10.6 representam-se os valores da soma de dois dígitos binários.

A partir desta tabela, conclui-se imediatamente que $T = a \wedge b$ e $s = a \dot{\vee} b$.

a	b	$a + b$	T	s
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	2	1	0

Tabela 10.6: Tabela de valores da soma de dois dígitos binários.

A Figura 10.5 representa alguns dos circuitos lógicos que realizam o somador parcial, o último dos quais é apresentado na forma de *caixa preta*, i.e., com um símbolo cujos únicos detalhes são a entrada e a saída. Tendo em vista simplificar a explicitação de circuitos complexos, é frequente representarem-se alguns subcircuito lógicos mais simples (que fazem parte destes circuitos lógicos mais complexos) na forma de caixas pretas.

Parte (b). Na Tabela 10.7 representam-se os valores da soma de três dígitos binários a , b e t .

Sendo $s = a \oplus b \oplus t$, o dígito binário de transporte T vem dado por

$$T = (a \wedge b \wedge t) \vee (\neg a \wedge b \wedge t) \vee (a \wedge \neg b \wedge t) \vee (a \wedge b \wedge \neg t). \quad (10.16)$$

Simplificando a expressão (10.16), obtém-se

$$T = (a \wedge b) \vee (a \wedge t) \vee (b \wedge t).$$

A Figura 10.6 e a Figura 10.7 incluem diferentes realizações do somador completo.

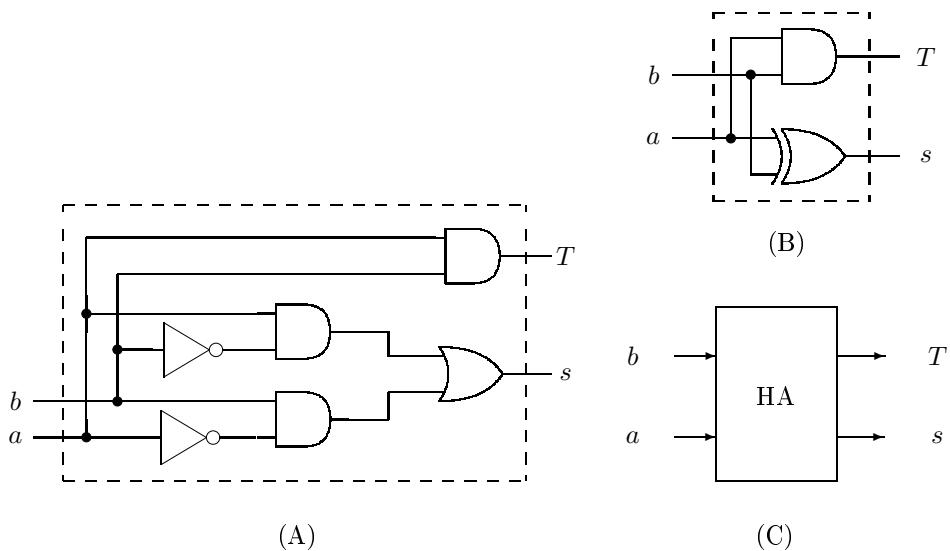


Figura 10.5: Circuitos lógicos que realizam o somador parcial (half adder; HA): (A) com portas de negação, e e ou, (B) com portas e e ou exclusivo e (C) com uma caixa preta.

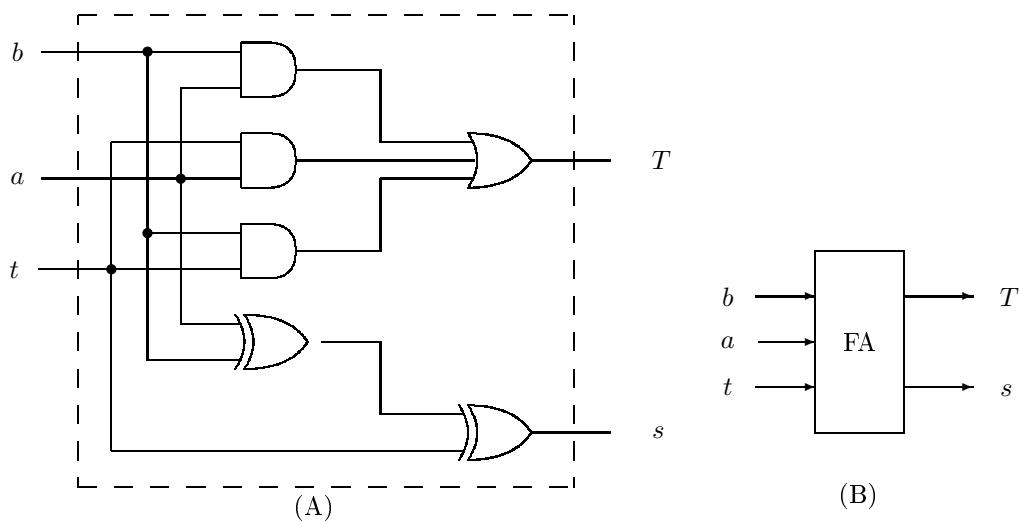


Figura 10.6: Somador completo (full adder, FA) com uma representação detalhada em (A) e uma representação como caixa preta em (B).

a	b	t	$a + b + t$	T	s
0	0	0	0	0	0
0	0	1	1	0	1
0	1	0	1	0	1
0	1	1	2	1	0
1	0	0	1	0	1
1	0	1	2	1	0
1	1	0	2	1	0
1	1	1	3	1	1

Tabela 10.7: Tabela de valores para o somador completo.

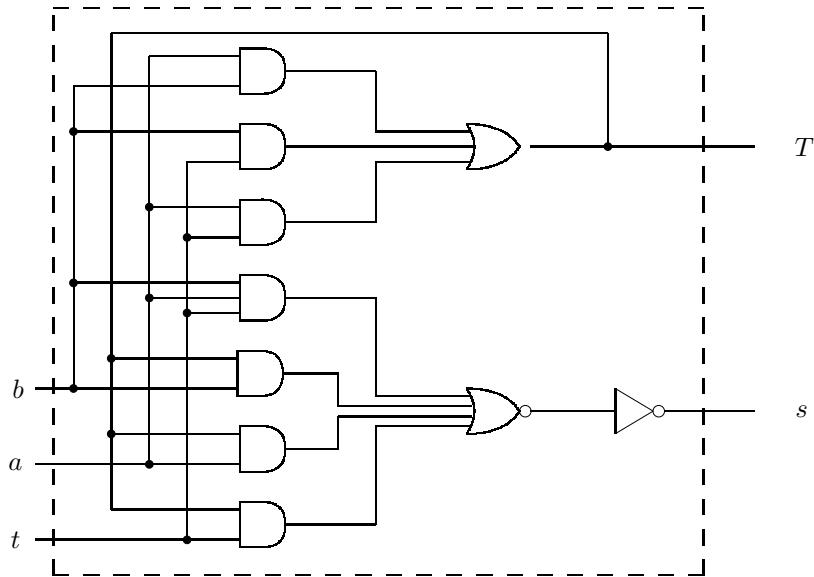


Figura 10.7: Somador completo (full adder, FA) que faz parte de alguns circuitos integrados, por exemplo SN7480 e SN7482.

Observe-se que, na prática, nem sempre se utilizam as realizações mais simples, mas sim aquelas que estão disponíveis no mercado e cuja produção, por sua vez, está condicionada por razões de natureza tecnológica.

A Figura 10.8 representa uma realização do somador completo com recurso a dois somadores parciais (e este facto está na origem da nomenclatura utilizada). \square

Exemplo 10.7. Vamos determinar os circuitos lógicos para o cálculo da soma de dois números binários.

Solução. Com o objectivo de calcular a soma de dois números a e b inteiros não negativos representados no sistema binário com n dígitos, considerem-se as representações binárias

$$\begin{aligned} a &= (a_{n-1}a_{n-2}\dots a_1a_0)_2 \\ b &= (b_{n-1}b_{n-2}\dots b_1b_0)_2. \end{aligned}$$

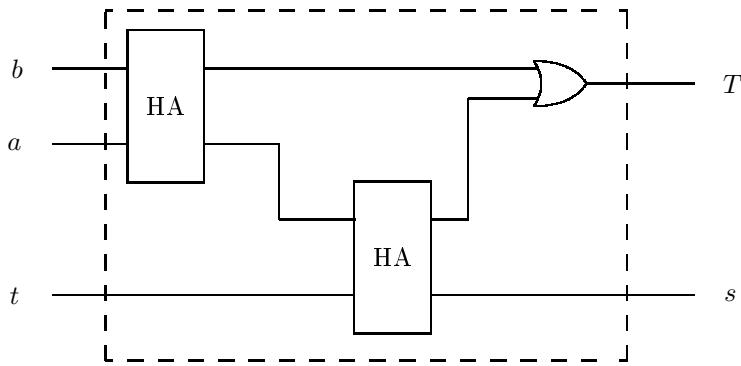


Figura 10.8: Somador completo (full adder) realizado com dois somadores parciais (half adders).

Para calcular o dígito binário s_i desta soma vamos adicionar módulo dois os dígitos binários a_i e b_i e ainda o dígito binário de transporte à entrada t (o qual resulta da adição anterior). Se a soma destes três dígitos é maior do que 1 então o dígito binário de transporte à saída T é igual a 1. Assim, para a adição dos dígitos relativos a uma dada posição podemos utilizar o somador completo do Exemplo 10.6. A Figura 10.9 representa o circuito combinatório para o cálculo da soma de dois números binários com 4 dígitos.

Uma vez que à soma de dois números (binários) com n dígitos pode corresponder um número com $n + 1$ dígitos, podemos concluir que o resultado tem a forma:

$$a + b = (Ts_{n-1}s_{n-2} \dots s_1s_0)_2.$$

Na prática, no resultado da soma de números com n dígitos binários utilizam-se apenas n dígitos binários, reservando-se o dígito de transporte T para a detecção de *overflow* na aritmética do computador.

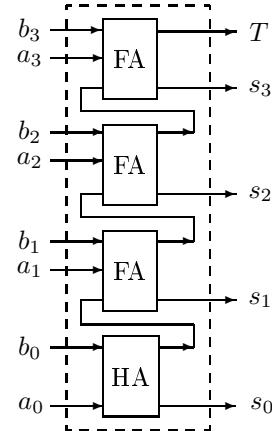


Figura 10.9: Circuito lógico para soma de números binários com 4 algarismos. \square

10.3. Átomos e isomorfismos

Seja $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole. Na base B vamos definir uma relação binária \sqsubseteq da seguinte forma:

Definição 10.3 (Relação \sqsubseteq). *Sendo $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole, então $\forall a, b \in B$*

$$a \sqsubseteq b \quad \text{se e só se} \quad a \sqcap b = a.$$

Teorema 10.5. *Se $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ é uma álgebra de Boole munida da relação \sqsubseteq da Definição 10.3, então \sqsubseteq é uma relação de ordem parcial definida na base B da álgebra.*

Demonastração. Note-se que uma relação de ordem parcial é uma relação reflexiva ($\forall a \in B \ a \sqsubseteq a$), anti-simétrica ($\forall a, b \in B$ se $a \sqsubseteq b$ e $b \sqsubseteq a$ então $a = b$) e transitiva ($\forall a, b, c \in B$ se $a \sqsubseteq b$ e $b \sqsubseteq c$ então $a \sqsubseteq c$). Com efeito, $\forall a, b, c \in B$

Reflexividade: Da propriedade de idempotência da álgebra de Boole, decorre $a \sqcap a = a$ e, consequentemente, da Definição 10.3, vem $a \sqsubseteq a$.

Anti-simetria: Se $a \sqsubseteq b$ e $b \sqsubseteq a$ então, pela Definição 10.3, $a \sqcap b = a$ e $b \sqcap a = b$, pela comutatividade de \sqcap , vem $a = b$.

Transitividade: Se $a \sqsubseteq b$ e $b \sqsubseteq c$ então, pela Definição 10.3, $a \sqcap b = a$ e $b \sqcap c = b$. Logo,

$$a \sqcap c = (a \sqcap b) \sqcap c = a \sqcap (b \sqcap c) = a \sqcap b = a,$$

e, consequentemente, $a \sqsubseteq c$. □

Exemplo 10.8. Vamos determinar a relação \sqsubseteq para as álgebras de Boole anteriormente consideradas nos Exemplos 10.1, 10.2 e 10.3.

Solução.

- No caso da **álgebra dos valores lógicos** $\langle \{0, 1\}, \vee, \wedge, \neg, 0, 1 \rangle$, uma vez que a base tem apenas dois elementos, basta analisar a respectiva relação entre eles. Assim, tendo em conta a igualdade $0 \wedge 1 = 0$, podemos concluir que $0 \sqsubseteq 1$ e dado que, no caso dos números inteiros, a relação \sqsubseteq é concordante com a relação \leq , nesta álgebra, vamos denotar a relação \sqsubseteq por \leq .
- No caso da **álgebra das partes de um conjunto** $\langle \mathcal{P}(\Omega), \cup, \cap, ^c, \emptyset, \Omega \rangle$, se $X, Y \in \mathcal{P}(A)$, então

$$X \sqsubseteq Y \Leftrightarrow X \cap Y = X \Leftrightarrow X \subseteq Y.$$

Logo, para a álgebra das partes de um conjunto, a relação \sqsubseteq é equivalente à relação de inclusão \subseteq (ou \subset).

- No caso da **álgebra de n -uplos binários** \mathbb{B}^n , sendo $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{B}^n$, obtém-se

$$\begin{aligned} (a_1, \dots, a_n) \sqsubseteq (b_1, \dots, b_n) &\Leftrightarrow (a_1, \dots, a_n) \sqcap (b_1, \dots, b_n) = (a_1, \dots, a_n) \\ &\Leftrightarrow (\min\{a_1, b_1\}, \dots, \min\{a_n, b_n\}) = (a_1, \dots, a_n) \\ &\Leftrightarrow (a_1 \leq b_1) \wedge \dots \wedge (a_n \leq b_n). \end{aligned}$$

Nesta álgebra, vamos denotar a relação \sqsubseteq por \preceq . □

Definição 10.4 (Relação \sqsubset). Dada uma álgebra de Boole, dizemos que o elemento a precede o elemento b (relativamente à relação \sqsubseteq) e escrevemos $a \sqsubset b$ quando $a \sqsubseteq b$ e $a \neq b$.

A relação \sqsubset será denotada por

- $<$ no caso da álgebra dos valores lógicos,
- \subsetneq no caso da álgebra das partes de um conjunto,
- \prec no caso da álgebra de n -uplos binários.

Definição 10.5 (Átomo de uma álgebra de Boole). Um elemento $a \neq \mathbf{0}$ da álgebra de Boole designa-se por **átomo** se o único elemento da álgebra que precede a é o elemento $\mathbf{0}$.

Exemplo 10.9. Vamos determinar os átomos das álgebras de Boole já consideradas.

Solução.

- **Álgebra dos valores lógicos** $\langle \{0, 1\}, \vee, \wedge, \neg, 0, 1 \rangle$. Neste caso, o único elemento distinto de 0 é o elemento 1, pelo que 1 é o único átomo.

- **Álgebra das partes de um conjunto** $\langle \mathcal{P}(\Omega), \cup, \cap, {}^c, \emptyset, \Omega \rangle$. Note-se que, por definição, os átomos desta álgebra são subconjuntos de Ω que não incluem subconjuntos não vazios. Consequentemente, os átomos da álgebra $\mathcal{P}(\Omega)$ são todos subconjuntos singulares de Ω , pelo que o seu número é igual $|\Omega|$.
- **Álgebra de n -uplos binários** \mathbb{B}^n . Por analogia com o caso anterior, os átomos desta álgebra são todos os n -uplos binários com uma única componente igual a 1 e todas as restantes $n - 1$ componentes iguais a zero. Logo, podemos concluir que esta álgebra tem n átomos. \square

Tendo em vista facilitar a demonstração do próximo teorema, vamos introduzir, previamente, os dois seguintes lemas auxiliares.

Lema 10.6. *Seja $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole e $a, b \in B$. Se $a \sqsubseteq b$, então*

1. $a \sqcup b = b$;
2. $\exists x \in B$ tal que $a \sqcup x = b$, $a \sqcap x = \mathbf{0}$ e $x \sqsubseteq b$.

Demonstração. Uma vez que a parte 1 corresponde ao dual da definição da relação \sqsubseteq , basta mostrar a parte 2. Assim, seja $x = a' \sqcap b$.

A propriedade $a \sqcup x = b$ decorre das igualdades:

$$\begin{aligned}
 a \sqcup x &= a \sqcup (a' \sqcap b) && (\text{definição de } x) \\
 &= (a \sqcup a') \sqcap (a \sqcup b) && (\text{distributividade}) \\
 &= \mathbf{1} \sqcap (a \sqcup b) && (\text{complementaridade}) \\
 &= a \sqcup b && (\text{identidade}) \\
 &= b && (\text{pela parte 1}).
 \end{aligned}$$

A propriedade $a \sqcap x = \mathbf{0}$ pode ser provada directamente, fazendo $a \sqcap x = a \sqcap a' \sqcap b = \mathbf{0} \sqcap b = \mathbf{0}$.

Finalmente, para mostrarmos que $x \sqsubseteq b$ observe-se que, por definição de \sqsubseteq , $x \sqsubseteq b$ é equivalente a $x \sqcap b = x$. Logo,

$$\begin{aligned}
 x \sqcap b &= (a' \sqcap b) \sqcap b && \text{definição de } x, \\
 &= a' \sqcap (b \sqcap b) && \text{associatividade,} \\
 &= a' \sqcap b && \text{idempotência,} \\
 &= x && \text{definição de } x.
 \end{aligned}$$

\square

Lema 10.7. *Seja $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole finita. Se $x \in B \setminus \{\mathbf{0}\}$, então existe um átomo α tal que $\alpha \sqsubseteq x$.*

Demonstração. Seja $x \in B \setminus \{\mathbf{0}\}$. Se x é um átomo, então $x \sqsubseteq x$ e o resultado verifica-se; caso contrário, por definição, existe $x_1 \neq \mathbf{0}$ tal que x_1 precede x . Se x_1 é um átomo, então $x_1 \sqsubseteq x$ e, mais uma vez, o resultado verifica-se; caso contrário, por definição, existe $x_2 \neq \mathbf{0}$ tal que x_2 precede x_1 e assim sucessivamente. É claro que todos os elementos x, x_1, x_2, \dots , são distintos. Logo, uma vez que a álgebra é finita, com este procedimento, necessariamente se obtém uma sequência finita, cujo último elemento é um átomo. \square

Teorema 10.8. *(da representação de uma álgebra de Boole finita) Dada uma álgebra de Boole finita $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$, se $b \in B \setminus \{\mathbf{0}\}$, então ou b é um átomo ou é soma (\sqcup) dos átomos que o precedem.*

Por outras palavras, se \mathcal{B} é uma álgebra de Boole finita e $A \subset B$ é o conjunto de todos os átomos de \mathcal{B} , então qualquer que seja $b \in B \setminus \{\mathbf{0}\}$ verifica-se a igualdade

$$b = \bigsqcup_{\substack{a \in A \\ a \sqsubseteq b}} a.$$

Adicionalmente, a representação de um elemento arbitrário $b \in B \setminus \{\mathbf{0}\}$ como soma de átomos da álgebra é única a menos da ordem dos termos na soma.

Atenção! Este teorema não é valido para álgebras de Boole infinitas (ou seja, para álgebras de Boole cujas bases tenham cardinalidade infinita). Compare esta afirmação com o Exercício 10.13.

Demonstração. Se b é um átomo, então o resultado verifica-se. Supondo que b não é um átomo, por aplicação do Lema 10.7, sabe-se que na álgebra de Boole \mathcal{B} , para qualquer elemento $x \neq \mathbf{0}$ existe um átomo tal que $a \sqsubseteq x$. Assim, sendo $X \subset A$ o conjunto (finito e não vazio) de todos os átomos de \mathcal{B} que precedem b e, sendo

$$c = \bigsqcup_{a \in X} a,$$

vamos mostrar que $c = b$. Com efeito, dado que

$$c \sqcap b = \left(\bigsqcup_{a \in X} a \right) \sqcap b = \bigsqcup_{a \in X} (a \sqcap b) = \bigsqcup_{a \in X} a = c,$$

conclui-se imediatamente que $c \sqsubseteq b$. Por outro lado, pelo Lema 10.6, existe $x \in B$ tal que

$$\begin{aligned} c \sqcup x &= b, \\ c \sqcap x &= \mathbf{0}, \\ x &\sqsubseteq b. \end{aligned} \tag{10.17}$$

Consequentemente, uma vez que $x = \mathbf{0}$ implica $c = b$, basta provar que $x = \mathbf{0}$. Vamos fazer esta prova por redução ao absurdo, supondo que $x \neq \mathbf{0}$. Então, aplicando Lema 10.7, existe um átomo a tal que $a \sqsubseteq x$. Porém, $a \sqsubseteq x \sqsubseteq b$ e, pela transitividade da relação \sqsubseteq , podemos concluir que $a \sqsubseteq b$. Adicionalmente, tendo em conta (1), conclui-se que a não pertence a X ,¹ o que contraria a definição de X , pelo que $x = \mathbf{0}$ e, consequentemente, $b = c$.

Para demonstrarmos a unicidade da representação, assumindo que existe um subconjunto de átomos Y tal que $b = \bigsqcup_{a \in Y} a$, vamos concluir a igualdade $X = Y$.

- Se $a_Y \in Y$, então $a_Y \sqcap b = a_Y \sqcap (\bigsqcup_{a \in Y} a) = \bigsqcup_{a \in Y} (a_Y \sqcap a) = a_Y$ e $a_Y \sqsubseteq b$. Logo, $a_Y \in X$ e, consequentemente, $Y \subseteq X$.
- Se $a_X \in X$, então

$$a_X = a_X \sqcap b = a_X \sqcap \left(\bigsqcup_{a \in Y} a \right) = \bigsqcup_{a \in Y} (a_X \sqcap a) \tag{10.18}$$

e, consequentemente, um dos termos $a_X \sqcap a$ da soma (10.18) é não nulo, o que implica que se tenha $a_X = a \in Y$, pelo que $X \subseteq Y$.

Logo, tendo conta as inclusões $X \subseteq Y$ e $Y \subseteq X$, podemos concluir a igualdade $X = Y$. \square

¹Caso contrário, $c \sqcap x = (a \sqcup a' \sqcup \dots) \sqcap x = (a \sqcap x) \sqcup (a' \sqcap x) \sqcup \dots \neq 0$, uma vez que $a \sqcap x = a$.

Definição 10.6 (Isomorfismo entre álgebras de Boole). *Dadas as álgebras de Boole $\mathcal{B}_1 = \langle B_1, \sqcup_1, \sqcap_1, \mathbf{1}_1, \mathbf{0}_1, \mathbf{1}_1' \rangle$ e $\mathcal{B}_2 = \langle B_2, \sqcup_2, \sqcap_2, \mathbf{1}_2, \mathbf{0}_2, \mathbf{1}_2' \rangle$ a bijecção φ entre estas álgebras ($\varphi : B_1 \rightarrow B_2$) diz-se um isomorfismo entre as álgebras de Boole \mathcal{B}_1 e \mathcal{B}_2 se $\forall x, y \in B_1$ se verificam as propriedades*

- $\varphi(x \sqcup_1 y) = \varphi(x) \sqcup_2 \varphi(y)$,
- $\varphi(x \sqcap_1 y) = \varphi(x) \sqcap_2 \varphi(y)$,
- $\varphi(x_1') = \varphi(x)_2'$.

Quando existe um isomorfismo entre duas álgebras de Boole dizemos que elas são isomórficas.

Exemplo 10.10. *Vamos mostrar que existe um isomorfismo entre a álgebra \mathbb{B}^n e a álgebra $\mathcal{P}([n])$ onde $[n] = \{1, \dots, n\}$.*

Solução. Dado um subconjunto arbitrário $A \subset [n]$, seja $\varphi(A)$ o n -uplo binário $b = (b_1, \dots, b_n)$ tal que $b_i = 1$ se e só se $i \in A$. Então a função $\varphi : \mathcal{P}([n]) \mapsto \mathbb{B}^n$ é uma bijecção. Com efeito, sejam A e B subconjuntos arbitrários de $[n]$. Se $\varphi(A \cup B) = (a_1, \dots, a_n)$ então $a_i = 1$ se e só se $i \in A \cup B$ o que é equivalente a $i \in A$ ou $i \in B$. Se $\varphi(A) \sqcup \varphi(B) = (b_1, \dots, b_n)$ então $b_i = 1$ se e só se $i \in A$ ou $i \in B$. Logo $\varphi(A \cup B) = \varphi(A) \sqcup \varphi(B)$. Se $\varphi(A \cap B) = (c_1, \dots, c_n)$ então $c_i = 1$ se e só se $i \in A \cap B$ o que é equivalente a $i \in A$ e $i \in B$. Se $\varphi(A) \sqcap \varphi(B) = (d_1, \dots, d_n)$ então $d_i = 1$ se e só se $i \in A$ e $i \in B$. Logo $\varphi(A \cap B) = \varphi(A) \sqcap \varphi(B)$. Finalmente, se $\varphi(A^c) = (e_1, \dots, e_n)$ então $e_i = 1$ se e só se $i \in A^c$, o que é equivalente a $i \notin A$. Se $\varphi(A^c) = (f_1, \dots, f_n)$ então $f_i = 1$ se e só se $i \notin A$. Logo, $\varphi(A^c) = \varphi(A)'$. \square

Marshall H. Stone (1903–1989) em 1930 demonstrou um teorema, hoje designado por teorema da representação de Stone, onde se estabelece que cada álgebra de Boole é isomorfa a uma álgebra de subconjuntos. O teorema a seguir, é uma particularização deste teorema para as álgebras finitas.

Teorema 10.9 (da representação de Stone). *Cada álgebra de Boole finita é isomorfa a uma álgebra das partes de um conjunto finito.*

Demonstração. Vamos dividir esta prova nos seguintes passos:

1. As definições de isomorfismo e de átomos implicam que para cada isomorfismo entre álgebras de Boole a imagem de qualquer átomo é um átomo.
2. As definições de isomorfismo e de átomos implicam que para cada isomorfismo entre álgebras de Boole a imagem recíproca de qualquer átomo é um átomo.
3. Os itens 1 e 2 implicam que álgebras de Boole isomórficas tenham o mesmo número de átomos.
4. Os itens 1 e 2, juntamente com o teorema da representação das álgebras de Boole finitas, implicam que duas álgebras de Boole finitas são isomórficas se e só se têm o mesmo número de átomos.
5. Tendo em conta o Exemplo 10.9, conclui-se que a álgebra de Boole $\mathcal{P}([n])$ tem n átomos.

Logo, qualquer álgebra de Boole finita com n átomos é isomorfa à álgebra de Boole $\mathcal{P}([n])$. \square

Exemplo 10.11. *Vamos mostrar que não existe uma álgebra de Boole com seis elementos.*

Solução. Tendo em conta o Teorema 10.9, convém notar que uma álgebra de Boole com n átomos tem, necessariamente, 2^n elementos e é isomorfa a uma álgebra de Boole $\mathcal{P}(A)$, onde A é um conjunto de cardinalidade n . Porém, não existe um número inteiro n tal que $2^n = 6$. Logo, podemos concluir que não existe uma álgebra de Boole com seis elementos. \square

10.4. Funções booleanas

Ao longo desta secção, por simplicidade de notação, vamos omitir o operador \wedge e, em lugar de \neg , vamos utilizar (tal como já aconteceu na álgebra de Boole) o símbolo $'$. Por exemplo, a expressão $\neg(x \vee y \wedge \neg z)$ será escrita na forma $(x \vee yz)'$. Trata-se de uma notação muito utilizada na teoria das funções booleanas.

Definição 10.7. *Uma função*

$$f : \mathbb{B}^n \longrightarrow \mathbb{B},$$

onde \mathbb{B} é um conjunto com dois elementos, designa-se por função de Boole ou função booleana n -ária (ou com n argumentos).

Exemplo 10.12. *Vamos calcular o número de funções booleanas com dois argumentos.*

Solução. Uma vez que as funções booleanas com dois argumentos são funções da forma $f : \mathbb{B}^2 \longrightarrow \mathbb{B}$, o seu domínio é \mathbb{B}^2 , com $|\mathbb{B}^2| = 4$, e o contradomínio é \mathbb{B} , com $|\mathbb{B}| = 2$. Assim, podemos representar estas funções por 4-uplos de componentes 0-1 e, consequentemente, o seu número é, precisamente, igual ao número destes 4-uplos, ou seja, $2^4 = 16$. Note-se que cada 4-uplo de componentes 0-1 pode representar um número binário de 4 dígitos de entre os números binários

$$\begin{aligned} (0000)_2 &= 0, & (0100)_2 &= 4, & (1000)_2 &= 8, & (1100)_2 &= 12, \\ (0001)_2 &= 1, & (0101)_2 &= 5, & (1001)_2 &= 9, & (1101)_2 &= 13, \\ (0010)_2 &= 2, & (0110)_2 &= 6, & (1010)_2 &= 10, & (1110)_2 &= 14, \\ (0011)_2 &= 3, & (0111)_2 &= 7, & (1011)_2 &= 11, & (1111)_2 &= 15. \end{aligned}$$

□

O conjunto das funções booleanas n -árias (ou com n argumentos), munido das operações \wedge , \vee e \neg , constitui uma álgebra de Boole que se designa por álgebra das funções booleanas n -árias (ou com n argumentos). Estas funções booleanas n -árias podem ser definidas pelas colunas da respectiva tabela de verdade. Como consequência, podemos concluir que a álgebra das funções booleanas n -árias é isomorfa à álgebra dos 2^n -uplos binários. Logo, existem 2^{2^n} funções booleanas n -árias (por exemplo, existem 4 funções binares 1-árias, 16 funções binares 2-árias, 256 funções binares 3-árias, 65.536 funções binares 4-árias e mais do que $4 \cdot 10^9$ funções binares 5-árias).

Exemplo 10.13. *Vamos determinar os átomos da álgebra de funções booleanas com dois argumentos.*

Solução. Uma vez que a álgebra das funções booleanas com dois argumentos tem 16 elementos (compare com o Exemplo 10.12), então podemos concluir que tem 4 átomos. Note-se que o Exemplo 10.9 implica que os átomos são funções com valor 1 para uma única conjunção de argumentos. Na Tabela 10.8 apresentam-se todos os átomos desta álgebra que não são mais do que as funções booleanas: $f_1(x, y) = xy$, $f_2(x, y) = xy'$, $f_3(x, y) = x'y$ e $f_4(x, y) = x'y'$.

□

x	y	xy	$x'y$	xy'	$x'y'$
0	0	0	0	0	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	0	0	0

Tabela 10.8: Átomos da álgebra das funções booleanas com dois argumentos.

Definição 10.8 (Minitermo e subminitermo). *Dada uma função booleana n -ária, designa-se por minitermo (subminitermo) toda a conjunção de n ($k \leq n$) literais, onde um literal é uma variável booleana ou a sua negação.*

Os minitermos de uma álgebra de funções booleanas são os seus átomos. Consequentemente, pelo teorema da representação, cada função booleana pode representar-se como disjunção (soma) dos seus minitermos. Esta representação designa-se por *forma normal* ou *forma normal disjuntiva*. Por aplicação do princípio da dualidade existe também a *forma normal conjuntiva* (que é a conjunção de disjunções de literais).

Assim, cada função booleana n -área pode ser definida por um 2^n -uplo de componentes binárias indexado por cada um dos seus minitermos (conjunções de n literais). Por exemplo, supondo que definimos as funções booleanas 3-áreas (nas variáveis x, y, z) por 2^3 -uplos cujas componentes são indexadas pelos minitermos xyz (1^a), xyz' (2^a), $xy'z$ (3^a), $xy'z'$ (4^a), $x'yz$ (5^a), $x'yz'$ (6^a), $x'y'z$ (7^a) e $x'y'z'$ (8^a), a função booleana $f(x, y, z) = xy \vee x'y'z$ vem definida pelo 8-uplo $(1, 1, 0, 0, 0, 0, 1, 0)$ (note-se que $xy \vee xy'z = xy(z \vee z') \vee xy'z = xyz \vee xyz' \vee x'y'z$). Nesta condições, se uma dada componente deste 8-uplo binário tem valor 1, isso significa que o correspondente minitermo está presente na forma normal disjuntiva de f e no caso contrário está ausente.

Exemplo 10.14. Vamos determinar a forma normal da expressão

$$(p \Rightarrow q) \dot{\vee} (p \vee q).$$

Solução. Considerando a Tabela 10.9 de valores da expressão anterior, conclui-se, imediatamente, que ela é equivalente a $pq' \vee p'q'$. \square

p	q	$(p \Rightarrow q) \dot{\vee} (p \vee q)$
0	0	1
0	1	0
1	0	1
1	1	0

Tabela 10.9: Tabela de verdade da expressão $(p \Rightarrow q) \dot{\vee} (p \vee q)$.

Por razões de ordem prática, é útil representar as funções booleanas com o menor número de operadores, onde cada operador é uma porta de um circuito lógico. A forma obtida em tais condições designa-se por *forma mínima* ou *forma disjuntiva mínima*. Conhece-se um algoritmo designado por *algoritmo de Quine-McCluskey* que transforma qualquer expressão lógica numa forma mínima. Porém, este algoritmo recorre a técnicas de optimização inteira que não são aqui abordadas. Em alternativa, na secção 10.5, apresenta-se um método muito popular para a determinação de formas mínimas de funções booleanas, com um máximo de 6 argumentos, que recorre a tabelas bidimensionais designadas por *Mapas de Karnaugh* (que foram introduzidos em 1950 por Maurice Karnaugh).

Muitas aplicações utilizam uma família particular de funções booleanas conhecida por família de *funções booleanas monótonas*.

Definição 10.9 (Função booleana monótona). *Uma função booleana n -ária, $f : \mathbb{B}^n \mapsto \mathbb{B}$, diz-se monótona quando, dados $x, y \in \mathbb{B}^n$,*

$$\text{se } x \preceq y \text{ então } f(x) \leq f(y).$$

Exemplo 10.15. Vamos determinar qual (ou quais) das seguintes funções booleanas é (são) monótona(s):

1. $f_1(p, q) = p \wedge q$,
2. $f_2(p, q) = p \vee q$,
3. $f_3(p, q) = p \dot{\vee} q$.

Solução. Na Tabela 10.10 apresentam-se os valores das funções f_1 , f_2 e f_3 . Uma vez, que $(0, 0) \prec (0, 1)$, $(0, 0) \prec (1, 0)$, $(0, 0) \prec (1, 1)$, $(0, 1) \prec (1, 1)$ e $(1, 0) \prec (1, 1)$, conclui-se que f_1 e f_2 são funções booleanas monótonas, mas f_3 não é monótona. \square

p	q	$f_1(p, q)$	$f_2(p, q)$	$f_3(p, q)$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Tabela 10.10: Tabela de valores das funções f_1 , f_2 e f_3 do Exemplo 10.15.

Tendo em vista à caracterização das funções booleanas monótonas, vamos introduzir o conceito de *forma disjuntiva reduzida*.

Definição 10.10 (Forma disjuntiva reduzida). *Designa-se por forma disjuntiva reduzida toda a expressão booleana definida por disjunções de conjunções de variáveis booleanas não negadas e, eventualmente, com constantes lógicas.*

Teorema 10.10. *Uma função booleana $f : \mathbb{B}^n \mapsto \mathbb{B}$ é monótona se e só se a podemos representar na forma disjuntiva reduzida.*

Demonstração. Seja $f : \mathbb{B}^n \mapsto \mathbb{B}$ uma função booleana monótona. Se f é constante nula, $f \equiv 0$, então o resultado verifica-se. Suponha que f não é a constante nula ($f \not\equiv 0$). Seja $\mathcal{X}_1 \subseteq \mathbb{B}^n$ o subconjunto de todas as conjunções de variáveis booleanas não negadas x tais que $f(x) = 1$ e, por abuso de linguagem, para $x \in \mathcal{X}_1$, dado um n -uplo arbitrário $y \in \mathbb{B}^n$, denotamos por $x(y)$ o valor lógico de y para x (ou seja, o valor lógico que se obtém para x , atribuindo às variáveis os valores determinados por y). Nestas condições, podemos concluir que para todo $x \in \mathcal{X}_1$,

$$\text{se } \exists y, z \in \mathbb{B}^n \text{ tais que } z \prec x \prec y \text{ então } x(z) = 0 \wedge x(y) = 1. \quad (10.19)$$

Vamos denotar por g a disjunção das conjunções de \mathcal{X}_1 e provar que $f \equiv g$.

Seja $y \in \mathbb{B}^n$.

- Se $\exists x \in \mathcal{X}_1$ tal que $x \preceq y$, então (pela monotonicidade de f) $f(y) = 1$. Por outro lado, tendo em conta (10.19), $x(y)=1$ e, consequentemente, $g(y) = 1$.
- Se $\nexists x \in \mathcal{X}_1$ tal que $x \preceq y$, podemos concluir, imediatamente que $\bigvee_{x \in \mathcal{X}_1} y \prec x$ e (de acordo com (10.19)) $x(y) = 0$. Logo, $g(y) = 0$ e, como consequência, $f(y) = 0$ (dado que $f(y) = 1$ implica a existência de $z \in \mathcal{X}_1$ tal que $z \preceq y$, o que contraria a afirmação anterior).

Reciprocamente, assuma-se que existe uma função f que não sendo monótona se pode definir na forma disjuntiva reduzida. Tal significa que existem n -uplos binários $z, y \in \mathbb{B}^n$ tais que $z \prec y$, $f(y) = 0$ e $f(z) = 1$. Porém, $f(z) = 1$ implica a existência, na forma disjuntiva reduzida que define f , de uma conjunção com o valor 1 para z . Adicionalmente, esta conjunção tem o valor 1 para todos os n -uplos binários $w \in \mathbb{B}^n$ tais que $z \prec w$ e, em particular, para o vector y (o que constitui uma contradição, uma vez que $f(y) = 0$). \square

Definição 10.11 (Vector reduzido mínimo). *Designa-se por vector reduzido mínimo de uma função booleana monótona $f : \mathbb{B}^n \mapsto \mathbb{B}$, todo o vector $\hat{x} \in \mathbb{B}^n$ tal que $f(\hat{x}) = 1$ e $f(\hat{y}) = 0$ para todos os n -uplos $\hat{y} \in \mathbb{B}^n$ tais que $\hat{y} \prec \hat{x}$,*

Definição 10.12 (Forma disjuntiva reduzida mínima). *Uma função booleana monótona diz-se expressa na forma disjuntiva reduzida mínima se a sua expressão na forma disjuntiva (disjunção de conjunções) tem o menor número possível de conjunções.*

Segue-se um teorema com especial importância em alguns dos capítulos subsequentes.

Teorema 10.11. *A cada conjunção da fórmula disjuntiva reduzida mínima de uma função booleana monótona f ($f : \mathbb{B}^n \mapsto \mathbb{B}$) corresponde um vector reduzido mínimo para f e reciprocamente. Com esta correspondência, as componentes unitárias dos vectores reduzidos mínimos determinam as variáveis presentes nas respectivas conjunções.*

Demonstração. Seja f uma função booleana monótona expressa na forma disjuntiva reduzida mínima. Nesta expressão, nenhuma conjunção é uma parte de outra conjunção (caso contrário, a expressão poderia reduzir-se o que, por definição, é impossível). Observe-se ainda que, de acordo com a definição, os vectores reduzidos mínimos não são \prec -comparáveis entre si. Por outro lado, a correspondência referida no teorema determina diferentes conjunções para diferentes vectores e diferentes vectores para diferentes conjunções. Assim, basta provar que qualquer vector que corresponda a uma conjunção da fórmula disjuntiva reduzida mínima de f é um vector reduzido mínimo para f e qualquer vector reduzido mínimo para f corresponde a uma conjunção da fórmula disjuntiva reduzida mínima de f .

- Seja \hat{x} o vector que corresponde a uma conjunção x da fórmula reduzida mínima de f . Então, se avaliarmos \hat{x} pela fórmula x (note-se que para esta avaliação consideramos x como uma função $x : \mathbb{B}^n \mapsto \mathbb{B}$ e \hat{x} como elemento de \mathbb{B}^n), é claro que $x(\hat{x}) = 1$ e, para qualquer outra conjunção y da fórmula reduzida mínima de f , $y(\hat{x}) = 0$. Adicionalmente, $f(\hat{x}) = 1$, para qualquer \hat{z} tal que $\hat{z} \prec \hat{x}$, $x(\hat{z}) = 0$ e, naturalmente, $f(\hat{z}) = 0$. Como consequência, tendo em conta a definição de vector reduzido mínimo, concluímos que \hat{x} é um vector reduzido mínimo.
- Seja \hat{x} um vector reduzido mínimo para f . Por definição, $f(\hat{x}) = 1$ e, consequentemente, existe uma conjunção y na forma reduzida mínima de f tal que $y(\hat{x}) = 1$. É claro que as variáveis da conjunção y correspondem a (pelo menos parte das) componentes unitárias de \hat{x} e é necessário provar que esta correspondência envolve todas estas componentes unitárias. Porém, caso o número de variáveis na conjunção y que correspondem a componentes unitárias de \hat{x} seja inferior ao número destas componentes, podemos concluir que $\hat{y} \prec \hat{x}$ e tal implica que \hat{x} não seja vector mínimo, obtendo-se uma contradição. Logo, as componentes unitárias de \hat{x} definem uma conjunção x da forma disjuntiva reduzida mínima de f . \square

O problema da determinação do número de funções booleanas n -árias monótonas é um problema que continua em aberto, sendo conhecido por *problema de Dedekind*.

10.5. Mapas de Karnaugh

Deve recordar-se que toda a função booleana com n variáveis se pode representar como disjunção (soma) dos minitermos, os quais correspondem a conjunções (produtos) de todas as n variáveis ou suas negações. Por exemplo, a função $f(x_1, x_2) = x_1 \vee x_2$, pode representar-se na forma:

$$f(x_1, x_2) = x_1 x_2 \vee x'_1 x_2 \vee x_1 x'_2. \quad (10.20)$$

A cada minitermo podemos associar a sequência de n dígitos binários $b_1 \dots b_n$ tal que o dígito b_i é igual 1, se a variável x_i aparece directamente na respectiva conjunção, e é igual 0, se a variável x_i aparece negada, ou seja, em vez de x_i aparece x'_i (por exemplo, para o minitermo $x_1 x'_2 x'_3 x_4 x_5$ obtém-se a sequência de dígitos binários 10011). Interpretando cada uma destas sequências de dígitos binários como número binário, designamo-la por *índice* do correspondente minitermo e denotamos um

minitermo com índice k por m_k . Assim, voltando ao exemplo da função booleana definida em (10.20), podemos concluir que ao minitermo x'_1x_2 corresponde a sequência binária 01 (ou seja, o índice 1), ao minitermo $x_1x'_2$ a sequência binária 10 (ou seja, o índice 2) e ao minitermo x_1x_2 a sequência binária 11 (ou seja, o índice 3). Como consequência, podemos escrever a função f na forma:

$$f(x_1, x_2) = m_1 \vee m_2 \vee m_3.$$

Dada uma função booleana $f(x_1, \dots, x_k)$, para simplificar a escrita, denota-se a soma dos minitermos $m_{i_1} \vee \dots \vee m_{i_k}$ por $\sum m(i_1, \dots, i_k)$. Logo, a função definida em (10.20), toma o aspecto:

$$f(x_1, x_2) = \sum m(1, 2, 3).$$

Antes de formalizarmos o processo de simplificação da representação de uma função booleana, considere-se o exemplo a seguir.

Exemplo 10.16. Vamos simplificar a representação da função booleana $g = \sum m(1, 3, 6, 7)$.

Solução. A partir da representação dada, conclui-se que

$$g(x_1, x_2, x_3) = x_1x_2x_3 \vee x_1x_2x'_3 \vee x'_1x_2x_3 \vee x'_1x'_2x_3.$$

Logo, no processo de simplificação, obtém-se a sequência de passos:

$$g(x_1, x_2, x_3) = x_1x_2x_3 \vee x_1x_2x'_3 \vee x'_1x_2x_3 \vee x'_1x'_2x_3 = x_1x_2(x_3 \vee x'_3) \vee x'_1x_3(x_2 \vee x'_2) = x_1x_2 \vee x'_1x_3.$$

Note-se que a função g consiste na disjunção de 4 minitermos onde existem dois pares que diferem exactamente num dígito binário. \square

Tendo em vista adoptar um procedimento eficiente para a simplificação da representação de funções booleanas, torna-se útil a utilização de uma tabela onde os minitermos que diferem exactamente num dígito fiquem situados em células vizinhas. Uma tal tabela pode obter-se com base no código de Gray e é conhecida por *mapa de Karnaugh*.

Definição 10.13 (Mapa de Karnaugh). *Dada uma função booleana, $f : \mathbb{B}^n \rightarrow \mathbb{B}$ (com $n \in \{2, 3, 4, 5, 6\}$), considere uma tabela T_n , com 2^n células, contendo todos os minitermos possíveis para as funções booleanas n -áreas, de tal forma que a cada célula corresponda um minitermo que difere de qualquer minitermo vizinho (numa célula adjacente) num único dígito binário. Então, designa-se por mapa Karnaugh da função f , a tabela de zeros e uns K_f que se obtém da tabela T_n , atribuindo-se o valor 1 às células correspondentes a minitermos da função booleana f (representada na forma normal disjuntiva) e o valor 0 às restantes.*

Como consequência desta definição, podemos concluir que existe uma bijecção entre as funções booleanas e os mapas de Karnaugh.

Nos casos mais simples das funções booleanas com duas variáveis ($f : \mathbb{B}^2 \rightarrow \mathbb{B}$), os mapas de Karnaugh correspondem a tabelas 2×2 . Na Figura 10.10 apresentam-se duas tabelas T_2 (ver Definição 10.13), com diferentes representações dos minitermos das funções com duas variáveis e o mapa de Karnaugh K_f que se obtém para o caso particular da função booleana $f(x_1, x_2) = x_1 \vee x_2$.

Figura 10.10: Tabelas T_2 e mapa de Karnaugh para $f(x_1, x_2) = x_1 \vee x_2$.

Por simplicidade, no que se segue, em geral, construiremos os mapas de Karnaugh, ignorando os índices dos minitermos que, na Figura 10.10, aparecem no canto inferior esquerdo das células.

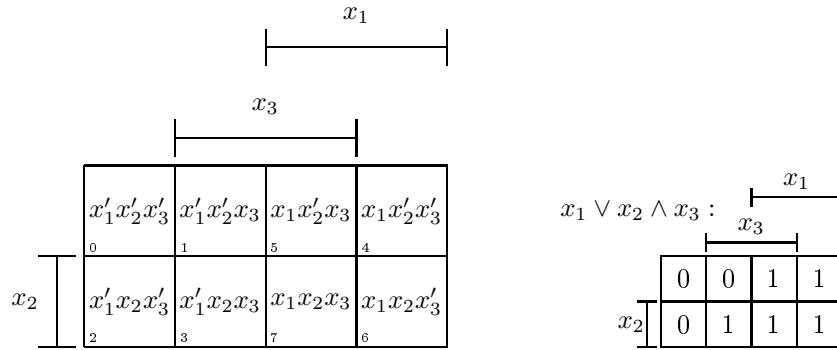


Figura 10.11: Tabela T_3 e mapa de Karnaugh para uma função booleana com três variáveis.

No caso das funções booleanas de três variáveis, o mapa de Karnaugh é formado por $2^3 = 8$ células (ver Figura 10.11). Neste caso, uma vez que os minitermos m_0 e m_4 são vizinhos e o mesmo acontece aos minitermos m_2 e m_6 , a parte esquerda e direita da fronteira do mapa devem ser "coladas" uma à outra. Como consequência, podemos imaginar este mapa construído na superfície de um torus, de um modo semelhante ao representado na Figura 10.12.

No caso das funções booleanas com quatro variáveis ($n = 4$), o mapa de Karnaugh tem $2^4 = 16$ células e dimensão 4×4 (ver Figura 10.13). Tal como no caso anterior, as fronteiras esquerda e direita são coladas uma à outra e o mesmo acontece às fronteiras superior e inferior do mapa, obtendo-se um torus semelhante ao representado na Figura 10.12.

De modo idêntico ao anteriormente descrito, poderíamos representar os mapas de Karnaugh para funções booleanas com cinco e seis variáveis. Porém, por razões de espaço (e porque o processo de construção não tem nada de novo), não consideramos estas representações neste texto. Note-se que a cada conjunção de variáveis ou suas negações corresponde, no mapa de Karnaugh, um conjunto de células que preenchem uma área rectangular do torus (ver Figura 10.14).

No caso geral, a determinação das células de um mapa de Karnaugh pode fazer-se, associando as linhas e colunas a variáveis booleanas e suas negações, tal como se indica na Figura 10.14. Note-se, que em cada um dos mapas desta figura, a primeira e segunda linhas estão associadas a x'_1 , a segunda e terceira linhas estão associadas a x_2 , a primeira e quarta linhas estão associadas a x'_2 e a terceira e quarta linhas estão associadas a x_1 . Por sua vez, as colunas estão associadas às variáveis de modo

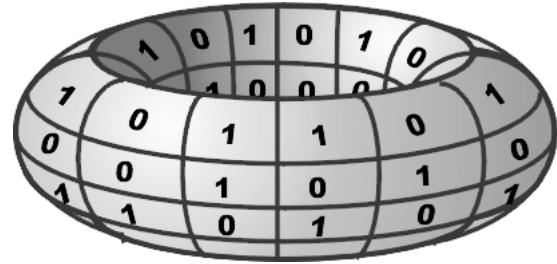


Figura 10.12: Mapa de Karnaugh representado no torus.

A figura mostra a Tabela T_4 para as funções booleanas com quatro variáveis (x_1, x_2, x_3, x_4). A Tabela T_4 é uma matriz de 4x4 com os seguintes minitermos:

m_0	m_8	m_{12}	m_4
m_2	m_{10}	m_{14}	m_6
m_3	m_{11}	m_{15}	m_7
m_1	m_9	m_{13}	m_5

Figura 10.13: Tabela T_4 para as funções booleanas com quatro variáveis.

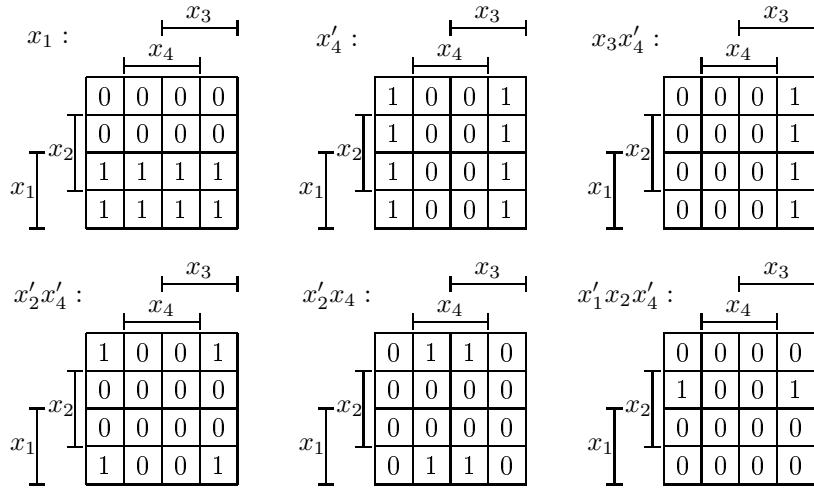


Figura 10.14: Exemplos de áreas rectangulares (que se podem obter no torus) para alguns mapas de Karnaugh.

semelhante.

Observe-se ainda que os comprimentos dos lados dos rectângulos (que se obtêm no torus) são potências de 2. Por outro lado, se o mapa de Karnaugh de uma função n -área é o relativo a um subminitermo definido pela conjunção de k variáveis ou suas negações (que se designam usualmente por literais), então existem exactamente 2^{n-k} células com valor 1.

Simplificação de uma função booleana:

1. Representar o mapa de Karnaugh que corresponde à função booleana.
2. Identificar subconjuntos de células com uns (e apenas com uns) que definem rectângulos cujos comprimentos dos lados são potências de 2, tais que:
 - (a) cada célula com valor 1 pertence a pelo menos um rectângulo,
 - (b) cada rectângulo tem a maior área possível,
 - (c) e o número de rectângulos é o menor possível.
3. Para cada rectângulo, determinar o subminitermo que lhe corresponde (tendo em conta que o subminitermo correspondente a um rectângulo é o definido pela conjunção de variáveis ou respectivas negações associadas às linhas e/ou colunas que exclusivamente o determinam) e fazer a disjunção dos subminitermos obtidos².

Exemplo 10.17. Vamos simplificar a representação da função $f : \mathbb{B}^4 \rightarrow \mathbb{B}$, com variáveis x, y, z e w , definida pelo mapa de Karnaugh representado na Figura 10.15.

²Ter em atenção que com esta operação de simplificação x_i aparece no subminitermo se e só se x'_i não está associado ao rectângulo (no sentido em que a linha ou coluna que lhe corresponde não intersecta o rectângulo). Analogamente, x'_i aparece no subminitermo se e só se x_i não está associado ao rectângulo.

Solução. Com base no mapa de Karnaugh representado, podemos observar que

$$\begin{aligned}
 f(x, y, z, w) &= x'y'z'w' \vee x'y'zw' \vee x'yz'w \vee x'yzw \vee \\
 &\quad xyz'w \vee xyzw \vee xy'z'w' \vee xy'zw' \\
 &= m_0 + m_2 + m_5 + m_7 + \\
 &= m_{13} + m_{15} + m_8 + m_{10} \\
 &= \sum m(0, 2, 5, 7, 8, 10, 13, 15).
 \end{aligned}$$

Observe-se que os uns podem ser agrupados, como se indica na Figura 10.16, de modo que as respectivas células definam duas áreas rectangulares nas condições do procedimento de simplificação anteriormente introduzido. Logo, podemos concluir que $f(x, y, z, w) = yw \vee y'w'$. \square

Em muitos casos particulares, sabe-se que algumas das configurações (minitermos) são impossíveis e, em tais casos, os valores das variáveis são *indiferentes* para o resultado da função booleana. Na linguagem dos circuitos digitais, estas configurações de entrada são conhecidas por *condições indiferentes*. Como consequência, tendo em vista a simplificação de funções booleanas com condições indiferentes, o procedimento a seguir deve consistir primeiro na simplificação da função com recurso ao mapa de Karnaugh e posteriormente na atribuição do valor mais conveniente ao minitermo relativo à condição indiferente. Com este objectivo, as células das condições indiferentes terão o "valor" \times e, na definição da função pelos minitermos, os índices correspondentes a condições indiferentes são colocado entre os parêntesis [e] (por exemplo, $f(x_1, x_2, x_3) = \sum m(0, 2, [3, 5])$). Note-se que adiando a decisão sobre os valores a atribuir às condições indiferente para depois da simplificação, em geral, conseguiremos uma maior simplificação da função booleana. Por outro lado, a construção dos rectângulos pode ser feita considerando todas as células com valor 1 e algumas com valor \times (mas nunca com valor 0), o que aumenta o número de possibilidades de obtenção dos subminitermos. A seguir, exemplifica-se a utilização de condições indiferentes.

Exemplo 10.18. O mostrador de sete segmentos (*seven-segment display*) (ver Figura 10.17) é utilizado para visualização de dígitos decimais. O circuito lógico para o descodificador tem como entrada a representação binária ($b_3b_2b_1b_0$) de um dígito decimal e como saída os estados (ligado/desligado) de todos os segmentos (por exemplo, o segmento a está ligado se e somente se $a = 1$). Vamos simplificar as funções booleanas (uma por cada segmento) para uma realização deste descodificador.

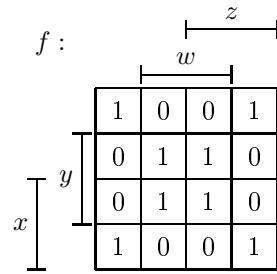


Figura 10.15: Definição da função f do Exemplo 10.17.

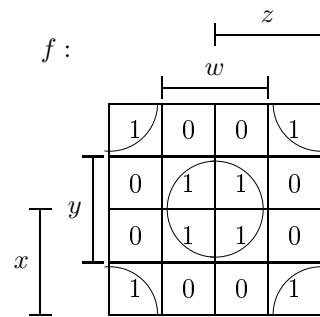


Figura 10.16: Simplificação da função booleana do Exemplo 10.17, concluindo-se que $f(x, y, z, w) = yw \vee y'w'$.

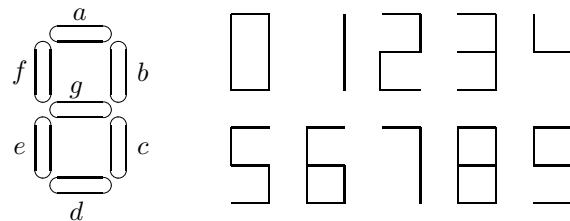
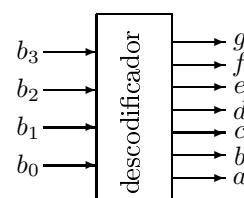


Figura 10.17: Mostrador de sete segmentos.



Solução. Tendo em consideração a Figura 10.17, com facilidade se obtém a Tabela 10.11. Note-se que as entradas relativas a índices pertencentes ao conjunto $\{10, \dots, 15\}$ são condições indiferentes (que nunca ocorrem). Em certas aplicações estas condições indiferentes são utilizadas para a visualização dos símbolos "-", "E", "r" e "o", com auxílio dos quais se representam os números negativos, os números em notação científica e a palavra "Error".

dígito	$b_3b_2b_1b_0$	a	b	c	d	e	f	g
0	0000	1	1	1	1	1	1	0
1	0001	0	1	1	0	0	0	0
2	0010	1	1	0	1	1	0	1
3	0011	1	1	1	1	0	0	1
4	0100	0	1	1	0	0	1	1
5	0101	1	0	1	1	0	1	1
6	0110	1	0	1	1	1	1	1
7	0111	1	1	1	0	0	0	0
8	1000	1	1	1	1	1	1	1
9	1001	1	1	1	1	0	1	1
	1010	x	x	x	x	x	x	x
	1011	x	x	x	x	x	x	x
	1100	x	x	x	x	x	x	x
	1101	x	x	x	x	x	x	x
	1110	x	x	x	x	x	x	x
	1111	x	x	x	x	x	x	x

Tabela 10.11: Tabela de verdade para o mostrador de sete segmentos.

A partir da tabela observa-se que

$$\begin{aligned} a &= \sum m(0, 2, 3, 5, 6, 7, 8, 9, [10, 11, 12, 13, 14, 15]), \\ b &= \sum m(0, 1, 2, 3, 4, 7, 8, 9, [10, 11, 12, 13, 14, 15]), \\ &\vdots \end{aligned}$$

Os mapas de Karnaugh para as funções a, \dots, g , que determinam as saídas do descodificador, bem como o processo de simplificação, aparecem representados na Figura 10.18.

Seguem-se as representações simplificadas das funções booleanas a, \dots, g .

$$\begin{aligned} a &= b_1 \vee b_3 \vee b'_0 b'_2 \vee b_0 b_2, \\ b &= b'_2 \vee b_3 \vee b'_0 b'_2 \vee b_0 b_2, \\ c &= b_0 \vee b'_1 \vee b_2, \\ d &= b_3 \vee b'_0 b_1 \vee b'_0 b'_2 \vee b_1 b'_2 \vee b_0 b'_1 b_2, \\ e &= b'_0 b_1 \vee b'_0 b'_2, \\ f &= b_3 \vee b'_0 b'_1 \vee b'_0 b_2 \vee b'_1 b_2 b'_3, \\ g &= b_3 \vee b'_0 b_2 \vee b_1 b'_2 \vee b'_1 b_2. \end{aligned}$$

□

Do ponto de vista da engenharia, para além da simplificação das funções booleanas, torna-se conveniente impor algumas restrições que favoreçam a estabilidade dos circuitos, no sentido em que pequenas perturbações (atrasos) no sinal de entrada não alterem as soluções obtidas. No entanto,

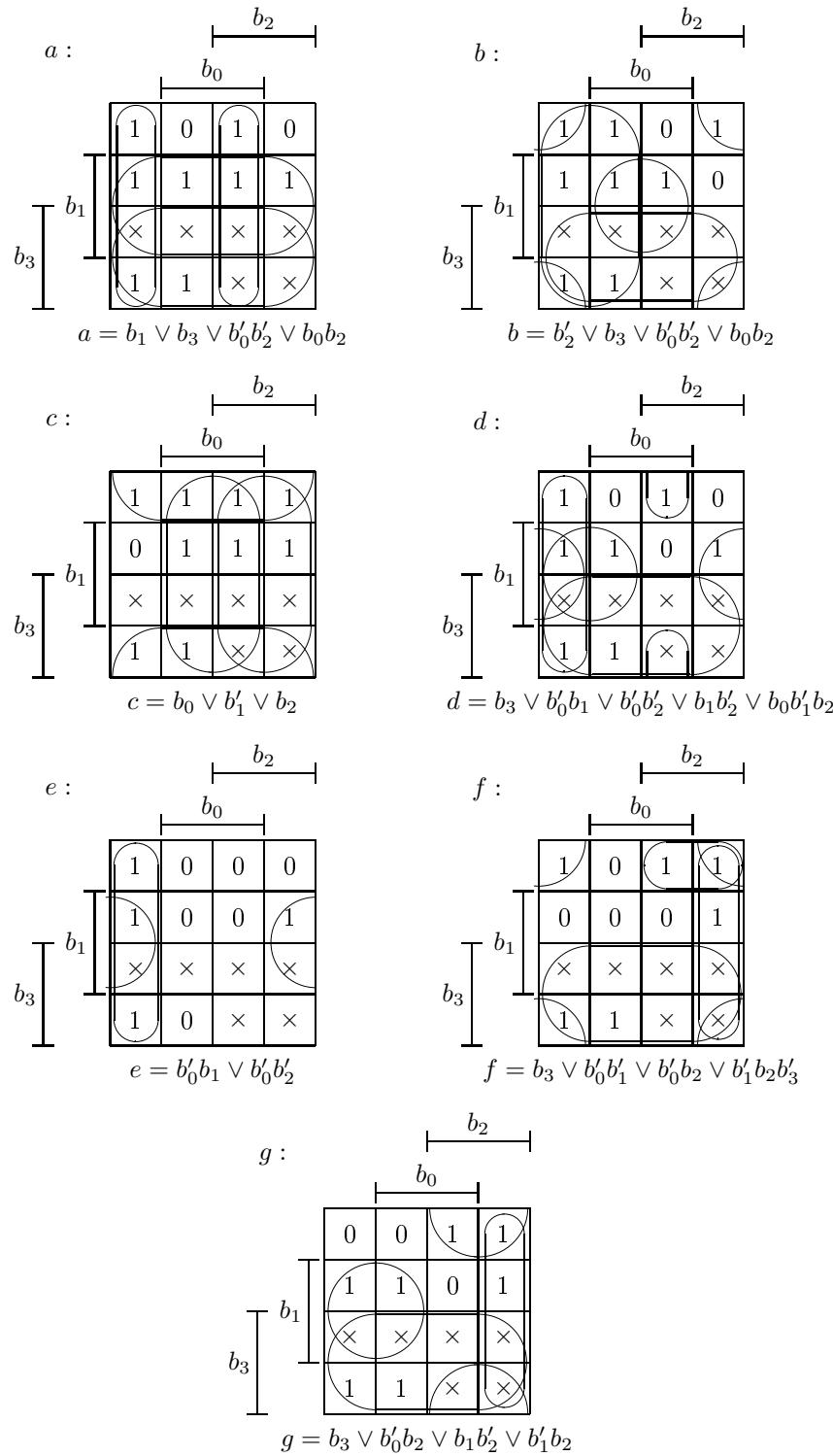


Figura 10.18: Simplificação das funções booleanas a, \dots, g , que realizam o mostrador de sete segmentos.

este tipo de questões está fora do âmbito deste texto. No nosso caso, apenas analisamos o problema conhecido em engenharia como problema de *risco*³. Na linguagem dos mapas de Karnaugh, quando duas células vizinhas têm valor 1 e não pertencem a um mesmo rectângulo, diz-se que ocorre o fenómeno de risco. Em tais situações, determina-se um circuito instável. Por exemplo, no mapa de Karnaugh da função g do mostrador de sete segmentos, as células que correspondem aos minitermos $b'_0 b_1 b'_2 b'_3$ e $b'_0 b_1 b_2 b'_3$ são vizinhas e, na forma simplificada, não existe um rectângulo que as inclua. Neste caso, convém considerar um rectângulo suplementar (com a maior área possível) com as duas células em causa, ou seja, o subminitermo $b'_0 b_1$ (ver Figura 10.19). Como consequência, obtém-se a representação menos simplificada mas sem risco para a função g :

$$g = b_3 \vee b'_0 b_2 \vee b_1 b'_2 \vee b'_1 b_2 \vee b'_0 b_1.$$

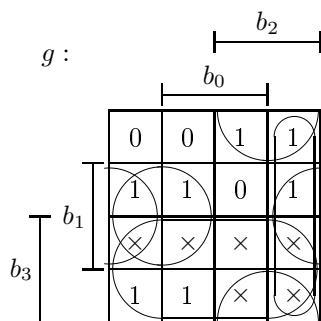


Figura 10.19: Exemplo de eliminação do fenómeno de risco para o mostrador de sete segmentos.

Atenção! Os mapas de Karnaugh podem também ser utilizados para a simplificação de funções na forma conjuntiva. Porém, nesses casos, as áreas rectangulares devem ser construídas à custa das células com valor 0.

10.6. Exercícios

- 10.1. Seja $n \in \mathbb{N}$ o produto de números primos distintos e seja D_n o conjunto de todos os divisores positivos de n . Denotando por \sqcup o menor múltiplo comum entre dois números e por \sqcap o máximo divisor comum entre dois números, mostre que D_n munido destas operações e da operação de complementação definida por $a' = \frac{n}{a}$ é uma álgebra de Boole.
- 10.2. Mostre que não existe uma álgebra de Boole com três elementos.
- 10.3. Mostre que dados três elementos arbitrários a, b e c de uma álgebra de Boole se verifica
 - (a) $a \sqsubseteq b$ se e somente se $b' \sqsubseteq a'$,
 - (b) se $a \sqsubseteq c$ e $b \sqsubseteq c$ então $(a \sqcup b) \sqsubseteq c$,
 - (c) para $a \neq \mathbf{0}$ se $a \sqsubseteq b$ então $a \not\sqsubseteq b'$.
- 10.4. Determine um isomorfismo entre a álgebra dos valores lógicos e a álgebra $\mathcal{P}(A)$ para um conjunto adequado A .
- 10.5. Defina os átomos e a relação \sqsubseteq , para a álgebra de Boole do Exercício 10.1.
- 10.6. Mostre que se $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$ é uma álgebra de Boole, então, para quaisquer elementos $a, b, c \in B$ tais que $a \sqsubseteq b$,

³Na língua inglesa este problema designa-se por "hazard problem".

$$a \sqcup b \sqcap c = (a \sqcup b) \sqcap c.$$

10.7. Mostre que se a, b e c são elementos arbitrários de uma álgebra de Boole, então

$$(a \sqcup b) \sqcap (a \sqcup b') = a \quad \text{e} \quad (a \sqcap b) \sqcup (a \sqcap b') = a.$$

10.8. Mostre que se a, b e c são elementos arbitrários de uma álgebra de Boole, então

$$(a \sqcup b) \sqcap (a' \sqcup c) = (a \sqcap c) \sqcup (a' \sqcap b) \quad \text{e} \quad (a \sqcap b) \sqcup (a' \sqcap c) = (a \sqcap c) \sqcup (a' \sqcap b).$$

10.9. Mostre que se a e b são elementos arbitrários de uma álgebra de Boole, então

$$a \sqcup b = b \quad \text{se e só se} \quad a \sqcap b = a.$$

10.10. Mostre que se a e b são elementos arbitrários de uma álgebra de Boole, então

$$(a \sqcap b) \sqsubseteq a \sqsubseteq (a \sqcup b)$$

e, como consequência, $\mathbf{0} \sqsubseteq a \sqsubseteq \mathbf{1}$.

10.11. Mostre que numa álgebra de Boole $a \neq 0$ é um átomo se e só se

$$a = b \sqcup c \quad \text{implica} \quad b = a \quad \text{ou} \quad c = a.$$

10.12. Mostre que se a, b e c são elementos arbitrários de uma álgebra de Boole, então

$$a \sqsubseteq b \quad \Rightarrow \quad (a \sqcap c) \sqsubseteq (b \sqcap c),$$

$$a \sqsubseteq b \quad \Rightarrow \quad (a \sqcup c) \sqsubseteq (b \sqcup c).$$

10.13. Seja B o conjunto da todas as uniões finitas de intervalos da forma $[a, b]$, onde $0 \leq a \leq b \leq 1$ e, para $x \in B$, seja $x' = [0, 1] \setminus x$.

- (a) Mostre que $\langle B, \cup, \cap, ', \emptyset, [0, 1] \rangle$ é uma álgebra de Boole infinita.
- (b) Mostre que esta álgebra não tem átomos.

10.14. Considere o circuito lógico representado na Figura 10.20.

- (a) Determine a função booleana que lhe corresponde.
- (b) Simplifique este circuito.

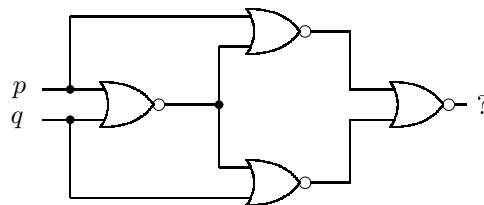


Figura 10.20: Um circuito lógico.

10.15. Represente os circuitos lógicos equivalentes às portas *não*, *ou* e *e*,

- (a) utilizando apenas portas *nand*,
 (b) utilizando apenas portas *nor*.
- 10.16. Converta os números a seguir indicados em números decimais.
- (a) $(101010, 10101)_2$,
 - (b) $(7654, 321)_8$,
 - (c) $(A3B5, FF)_{16}$,
 - (d) $(0, 11011)_2$,
 - (e) $(210, 012)_3$.
- 10.17. Calcule as operações de adição a seguir indicadas.
- (a) $(111, 101)_2 + (1001, 11)_2$,
 - (b) $(375, 24)_8 + (1234, 01)_8$,
 - (c) $(A01, 2)_{16} + (FFF, FF)_{16}$.
- 10.18. Dada uma álgebra de Boole, $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$, mostre que se verifica a seguinte lei de cancelamento:
- $$\text{se } (x \sqcup a = x \sqcup b \text{ e } x' \sqcup a = x' \sqcup b) \text{ então } a = b.$$
- 10.19. Dada uma álgebra de Boole, $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$, mostre que são verdadeiras as seguintes proposições:
- (a) se $x \in B$ e $x \sqsubseteq \mathbf{0}$, então $x = \mathbf{0}$,
 - (b) se $y \in B$ e $\mathbf{1} \sqsubseteq y$, então $y = \mathbf{1}$,
 - (c) se $x, y \in B$, $x \sqsubseteq y$ e $x \sqsubseteq y'$, então $x = \mathbf{0}$.
- 10.20. Sejam $f, g : \mathbb{B}^5 \rightarrow \mathbb{B}$ duas funções booleanas definidas por
- $$f = \sum m(1, 2, 4, 7, x) \quad \text{e} \quad g = \sum m(0, 1, 2, 3, 16, 25, y, z).$$
- Sabendo que $f \leq g$, determine x, y e z .
- 10.21. Sejam $f, g : \mathbb{B}^4 \rightarrow \mathbb{B}$ duas funções booleanas definidas por
- $$f = \sum m(2, 4, 6, 8) \quad \text{e} \quad g = \sum m(1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 13, 15).$$
- Determine uma função booleana h tal que $f = gh$.
- 10.22. Dada um álgebra de Boole, $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1} \rangle$, mostre que se verifica:
- $$\forall_{x,y,z \in B} (x \sqcup y) \sqsubseteq z \text{ se e só se } x \sqsubseteq z \text{ e } y \sqsubseteq z.$$
- 10.23. Com recurso aos mapas de Karnaugh, minimize as funções booleanas que a seguir se indicam.
- (a) $f = \sum m(0, 1, 2, 9, 11, 12, 13, 27, 28, 29)$.
 - (b) $f = \sum m(4, 5, 10, 11, 15, 18, 20, 24, 26, 30, 31, [9, 12, 14, 16, 19, 21, 25])$.
 - (c) $f = (a' \vee b' \vee c \vee d)(a \vee b' \vee c' \vee d) \vee (a \vee b \vee c \vee d)(a' \vee b)(a \vee d')$.
- 10.24. Determine um circuito lógico com três entradas cuja saída tem como resultado 1 se e só se

- (a) todas as três entradas são iguais,
 (b) o número de entradas iguais a 1 é superior ao número de entradas iguais a 0,
 (c) existem entradas com valores diferentes,
 (d) o número de entradas unitárias é ímpar (este circuito lógico é conhecido por *gerador do dígito (bit) de paridade*).
- 10.25. Determine um circuito lógico, conhecido por desmultiplexer, que é um circuito com um dígito binário de entrada d e vários outros dígitos D , determinando estes últimos um endereço de saída (posição de uma das saídas), com o qual se copia o dígito d para a saída (posição) definida pelo endereço D e todas as restantes saídas são colocadas a 0. Considere o caso particular em que D é constituído por dois dígitos e que existem quatro saídas com endereços 0, 1, 2 e 3.
- 10.26. Determine os seguintes circuitos lógicos:
- (a) circuito com duas entradas a e b e três saídas tal que a primeira saída é igual 1 se e só se $a < b$, a segunda saída é igual 1 se e só se $a > b$ e a terceira saída é igual 1 se e só se $a = b$;
 (b) circuito que compara dois números com quatro dígitos binários cada um (utilizando o circuito determinado em (a) como uma caixa preta).
- 10.27. Determine um circuito lógico cujo resultado é 1 se e só se o número de entrada, definido por quatro dígitos binários, é divisível por
- (a) 3;
 (b) 5.
- 10.28. Mostre a equivalências dos seguintes pares de proposições lógicas:
- (a) $(p \wedge q) \Rightarrow r$ e $p \Rightarrow (q \Rightarrow r)$;
 (b) $(p \wedge q) \vee r$ e $(p \vee q) \wedge (p \vee r)$;
 (c) $(p \vee q) \wedge r$ e $(p \wedge q) \vee (p \wedge r)$.
- 10.29. Verifique qual das proposições, a seguir indicadas, são tautologias.
- (a) $(p \vee q) \wedge (p' \wedge q')$.
 (b) $(p \Rightarrow q) \vee (q \Rightarrow p)$.
 (c) $(p \Rightarrow q) \wedge (p \Rightarrow q')$.
 (d) $((p \wedge q) \vee (q \wedge r)) \Rightarrow (p \wedge r)'$.
 (e) $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \vee q)$.
- 10.30. Considere os números representados no sistema negabinário⁴ que correspondem a números da forma $\sum_i d_i(-2)^i$, onde os dígitos $d_i \in \mathbb{B}$. Por exemplo, $(11, 01)_{-2} = (-2)^1 + (-2)^0 + (-2)^{-2} = -2 + 1 + \frac{1}{4} = 0,75$. Note-se que, com este sistema, os números positivos e negativos são representados sem recurso aos sinais + e -.

⁴Trata-se de um sistema de numeração de base negativa, introduzido por Vittorio Grunwald em 1885. O sistema negabinário foi utilizado nos computadores experimentais polacos SKRZAT e BINEG no início da década de 1950.

- (a) Mostre que o sistema negabinário permite a representação de todos os números inteiros.
- (b) Mostre que, num sistema negabinário, a representação de um inteiro negativo utiliza um número par de dígitos e a representação de um inteiro positivo utiliza um número ímpar de dígitos.
- (c) Determine um algoritmo para a adição de números inteiros no sistema negabinário.
- (d) Determine um algoritmo de troca de sinal de um número inteiro no sistema negabinário.

11

Grupos Finitos e Enumeração de Pólya

Neste capítulo apresenta-se uma breve introdução à teoria dos grupos finitos e descrevem-se algumas técnicas de enumeração muito poderosas mas de mais difícil utilização do que as abordadas no Capítulo 3.

11.1. Introdução aos grupos finitos

A teoria dos grupos constitui um ramo muito especializado da álgebra abstracta e é uma área com inúmeros resultados. Nesta secção, apresentamos apenas algumas definições e alguns resultados com aplicação em problemas combinatórios. Para um estudo mais aprofundado sobre teoria dos grupos ver, por exemplo, [36], [43], [46] ou [71].

Definição 11.1 (Grupo). *Um grupo \mathcal{G} é um par ordenado (G, \otimes) que consiste num conjunto G onde está definida a lei de composição interna (operação) \otimes que satisfaz as seguintes propriedades:*

1. $\forall_{x,y,z \in G} x \otimes (y \otimes z) = (x \otimes y) \otimes z$ (associatividade)
2. $\exists_{e \in G} \forall_{x \in G} x \otimes e = e \otimes x = x$ (existência de elemento neutro)
3. $\forall_{x \in G} \exists_{x^{-1} \in G} x \otimes x^{-1} = x^{-1} \otimes x = e$ (todos os elementos têm inverso)

O grupo $\mathcal{G} = (G, \otimes)$ diz-se um *grupo finito* se G é um conjunto finito e, neste caso, sendo $|G| = n$, diz-se que o grupo \mathcal{G} tem *ordem* n . Neste texto vamos considerar apenas grupos finitos, pelo que os designamos, simplesmente, por grupos.

Por abuso de linguagem, muitas vezes, identificamos o grupo \mathcal{G} pelo conjunto G dos respectivos elementos e, por economia, escreve-se xy em vez de $x \otimes y$, x^2 em vez de $x \otimes x$, x^{-2} em vez de $x^{-1} \otimes x^{-1}$, etc. Algumas vezes, também se denota o elemento neutro de G , e , por x^0 , onde x é um elemento arbitrário de G . Seguem-se alguns exemplos de grupos finitos.

Exemplo 11.1. Vamos mostrar que $\mathbb{Z}_n = (\{0, 1, \dots, n-1\}, \oplus_n)$, onde por \oplus_n denota a soma módulo n , é um grupo de ordem n .

Solução. É claro que \oplus_n é uma lei de composição interna em \mathbb{Z}_n .

1. *Associatividade.* Para mostrar que $\forall_{x,y,z \in \mathbb{Z}_n} x \oplus_n (y \oplus_n z) = (x \oplus_n y) \oplus_n z$, basta observar que ambos os lados desta equação são iguais a $(x + y + z) \bmod n$.

2. *Existência do elemento neutro.* Uma vez que $\forall_{x \in \mathbb{Z}_n} 0 \oplus_n x = x \oplus_n 0 = x$, o número 0 é o elemento neutro de \mathbb{Z}_n .
3. *Existência de inverso (aditivo)* para todo o elemento de \mathbb{Z}_n . Para $x \in \mathbb{Z}_n$, seja

$$x^* = \begin{cases} n - x, & \text{se } x \neq 0; \\ 0, & \text{se } x = 0. \end{cases}$$

Nestas condições, é imediato que $x \oplus_n x^* = x^* \oplus_n x = 0$, o que implica que x^* seja o inverso (aditivo) de x . \square

Um grupo G diz-se *abeliano* se $xy = yx$ quaisquer que sejam $x, y \in G$. Caso contrário, G diz-se *não-abeliano* (note-se que o grupo aditivo \mathbb{Z}_n do Exemplo 11.1 é um grupo abeliano).

Exemplo 11.2. Vamos mostrar que o conjunto S_n de todos as permutações de elementos do conjunto $[n] = \{1, 2, \dots, n\}$ com a operação de composição é um grupo não-abeliano.

Solução. Uma vez que cada permutação é uma bijecção e a composição de bijeções é uma bijecção então esta operação é uma lei de composição interna em S_n . Por sua vez, a associatividade da composição de permutações é consequência imediata da associatividade da composição de bijeções. Note-se que a permutação identidade $\pi_{id} \in S_n$ é o elemento neutro de S_n . Se $\pi \in S_n$ e $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$, então $\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix} \in S_n$ é a permutação inversa de π . Finalmente, o Exemplo 4.19 demonstra que, em geral, S_n é não-abeliano. \square

É imediato concluir que S_n , conhecido por grupo simétrico, tem ordem $n!$.

Definição 11.2 (Homomorfismo, isomorfismo e automorfismo). Dados dois grupos $\mathcal{G}_1 = (G_1, \otimes_1)$ e $\mathcal{G}_2 = (G_2, \otimes_2)$, designa-se por homomorfismo entre \mathcal{G}_1 e \mathcal{G}_2 toda a função $f : G_1 \rightarrow G_2$ que preserva em \mathcal{G}_2 a estrutura de \mathcal{G}_1 , ou seja,

$$\forall_{x, y \in G_1} f(x \otimes_1 y) = f(x) \otimes_2 f(y).$$

No caso do homomorfismo ser uma bijecção, dizemos que se trata de um isomorfismo e que \mathcal{G}_1 e \mathcal{G}_2 são isomorfos, denotando-se esta propriedade por $\mathcal{G}_1 \cong \mathcal{G}_2$. Por sua vez, um isomorfismo de um grupo \mathcal{G} em si próprio designa-se por automorfismo.

Definição 11.3 (Subgrupo). Dado um grupo $\mathcal{G} = (G, \otimes)$, diz-se que o grupo $\mathcal{H} = (H, \otimes)$ é um subgrupo de \mathcal{G} e denota-se por $\mathcal{H} \leq \mathcal{G}$ se $H \subseteq G$. Na verdade, a operação definida em \mathcal{H} é a operação definida em \mathcal{G} , mas restringida aos elementos de H , porém, por simplicidade de notação utilizamos o mesmo símbolo.

Para mostrar que um subconjunto não vazio H de um grupo (G, \otimes) determina um subgrupo, basta mostrar que $\forall_{x, y \in H} x \otimes y^{-1} \in H$. No caso de G ser finito, basta provar que a operação \otimes restringida aos elementos de H é uma lei de composição interna.

O teorema a seguir evidencia a importância do grupo simétrico.

Teorema 11.1 (de Cayley). Todo o grupo de ordem $n \in \mathbb{N}$ é isomorfo a um subgrupo do grupo simétrico S_n .

Demonstração. Seja G um grupo de ordem n e, para cada $x \in G$, defina-se f_x como sendo uma aplicação entre G e G tal que $f_x(y) = xy$. Logo, pode concluir-se que f_x é injetiva, uma vez que

$$f_x(y) = f_x(z) \Leftrightarrow xy = xz \Leftrightarrow y = z$$

(bastando, para o efeito, multiplicar ambos os membros à esquerda por x^{-1}). Dado que f_x é uma aplicação injectiva de G em si próprio, podemos concluir que f_x é uma bijecção e, consequentemente, que f_x é uma permutação dos n elementos de G . Assim, resta provar que o conjunto de todas estas permutações (isto é, o conjunto $F = \{f_x : x \in G\}$) munido da operação de composição de aplicações, \otimes , é um grupo isomorfo a G . Para se obter esta prova, basta considerar o isomorfismo $\Psi : G \rightarrow F$ tal que $\Psi(x) = f_x$, para o qual $\Psi(xy) = f_{xy}$, com $f_{xy}(z) = (xy)z = x(yz) = f_x(yz) = f_x(f_y(z))$, pelo que $f_{xy} = f_x \otimes f_y$, ou seja, $\Psi(xy) = \Psi(x) \otimes \Psi(y)$. Adicionalmente,

$$\Psi(x) = \Psi(y) \Leftrightarrow f_x = f_y \Leftrightarrow \forall z \in G \quad xz = yz \Leftrightarrow x = y$$

(tendo em conta que $xz = yz \Leftrightarrow xzz^{-1} = yzz^{-1} \Leftrightarrow xe = ye \Leftrightarrow x = y$), donde Ψ é injectiva e, como também é sobrejectiva (por construção), conclui-se que se trata de um isomorfismo entre G e F . Uma vez que F munido da operação \otimes é um grupo e existe o isomorfismo entre (F, \otimes) e um subgrupo de S_n , conclui-se o pretendido. \square

Exemplo 11.3. Vamos mostrar que o grupo $\mathbb{Z}_5 = (\{0, 1, 2, 3, 4\}, \oplus_5)$ é isomorfo a um subgrupo de S_5 .

Solução. De acordo com a demonstração do Teorema 11.1, para o grupo \mathbb{Z}_5 obtém-se o conjunto de bijecções $F = \{f_0, f_1, f_2, f_3, f_4\}$, onde

$f_0 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$, $f_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}$, $f_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$, $f_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix}$ e $f_4 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix}$, o qual (substituindo 0 por 5) constitui um subgrupo de S_5 (note-se que f_0 constitui o elemento neutro, f_4 o inverso de f_1 , f_2 o inverso de f_3 e reciprocamente). \square

Dado um grupo finito G , para cada $x \in G$, prova-se que o conjunto $\langle x \rangle = \{x^k : k \in \mathbb{N}\}$ é um subgrupo de G que se designa por *subgrupo de G gerado por x* .

Definição 11.4 (Grupo cíclico). Diz-se que um grupo G é cíclico se existe $x \in G$ tal que $\langle x \rangle = G$.

No Exercício 11.3 apresentam-se algumas propriedades dos grupos cíclicos.

Definição 11.5 (Classe lateral). Sendo H um subgrupo de G e $x \in G$, designa-se por classe lateral (à direita) de H em G determinada pelo elemento x e denota-se por Hx , o conjunto $\{hx : h \in H\}$. Por sua vez, designa-se por classe lateral (à esquerda) de H em G o conjunto $xH = \{xh : h \in H\}$.

Note-se, porém, que dado um subgrupo H de um grupo arbitrário G , apesar de nem sempre se verificar a igualdade $Hx = xH$, no que diz respeito à cardinalidade (de acordo com o Exemplo 11.4) essa igualdade verifica-se, ou seja, $\forall_{x \in G} |Hx| = |xH| = |H|$.

Exemplo 11.4. Vamos mostrar que se G e H são dois grupos tais que $H \leq G$, então verificam-se as seguintes propriedades:

$$1. \quad \forall_{x,y \in G} xH \cap yH \neq \emptyset \Rightarrow xH = yH,$$

$$2. \quad \bigcup_{x \in G} xH = G,$$

$$3. \quad \forall_{x,y \in G} xH = yH \Leftrightarrow x^{-1}y \in H,$$

$$4. \quad \forall_{x \in G} |xH| = |H|.$$

Solução.

1. Suponhamos que $xH \cap yH \neq \emptyset$, então existe $z \in G$ tal que $z \in xH \cap yH$. Como consequência, $\exists_{p,q \in H} xp = z \wedge yq = z$, pelo que $x = yqp^{-1}$. Logo,

$$a \in xH \Rightarrow \exists_{b \in H} xb = a \Rightarrow \exists_{b \in H} yqp^{-1}b = a \Rightarrow \exists_{c=qp^{-1}b \in H} yc = a \Rightarrow a \in yH.$$

Por simetria, trocando x e y , vem que $a \in yH \Rightarrow a \in xH$.

2. Tendo em conta que $\forall_{x \in G} x \in xH \wedge xH \subseteq G$, conclui-se a igualdade pretendida.

3. Dados $x, y \in G$,

$$xH = yH \Leftrightarrow y \in xH \Leftrightarrow \exists_{a \in H} xa = y \Leftrightarrow x^{-1}y = x^{-1}xa = a \in H.$$

4. Considerando a função $\varphi : H \rightarrow xH$ tal que $\varphi(h) = xh$, basta mostrar que φ é uma bijecção. Com efeito, uma vez que

$$\varphi(a) = \varphi(b) \Rightarrow xa = xb \Rightarrow a = b,$$

a função φ é injectiva e como também é sobrejectiva (por construção), conclui-se que φ é bijectiva.

□

É claro que se podem concluir as mesmas propriedades para as classes laterais à direita.

Definição 11.6 (Subgrupo normal). *Um subgrupo H de G diz-se normal e denota-se por $H \triangleleft G$ se $\forall_{x \in G} xH = Hx$ (de modo equivalente, diz-se que H é subgrupo normal de G se e só se $\forall_{x \in G} xHx^{-1} = H$).*

Como consequência das propriedades 1 e 2 do Exemplo 11.4, se G e H são tais que $H \leq G$, então a família das classes laterais distintas à esquerda (à direita) de H constitui uma partição de G . Uma vez que, de acordo com as propriedades 2 e 4 do Exemplo 11.4, o número de classes laterais à esquerda é igual ao número de classes laterais à direita, podemos introduzir a seguinte definição.

Definição 11.7 (Índice). *Seja G um grupo e $H \leq G$. Designa-se por índice de H em G e denota-se por $[G : H]$, o número de classes laterais à esquerda (ou à direita) de H em G distintas.*

Teorema 11.2 (de Lagrange). *Se G é um grupo finito e H é um seu subgrupo, então $|G| = |H|[G : H]$ e, em particular, $|H|$ é um divisor de $|G|$.*

Demonstração. Uma vez que H é um subgrupo de um grupo finito G , conclui-se que o conjunto G/H das classes laterais à direita de H em G é finito e, se $G/H = \{Hx_1, \dots, Hx_{[G:H]}\}$, então G é a união disjunta de $Hx_1, \dots, Hx_{[G:H]}$, pelo que $|G| = |Hx_1| + \dots + |Hx_{[G:H]}| = |H|[G : H]$ (uma vez que, de acordo com o ponto 4 do Exemplo 11.4, $|Hx_i| = |H|$ para $i \in \{1, \dots, [G : H]\}$). □

Como consequência imediata de Teorema de Lagrange, o índice de H em G é determinado pela expressão

$$[G : H] = \frac{|G|}{|H|}. \quad (11.1)$$

Definição 11.8 (Grupo quociente). *Se G é um grupo finito e H é um seu subgrupo normal, isto é, $H \triangleleft G$, então $(G/H, \otimes)$, onde $G/H = \{Hx : x \in G\}$ e $Hx \otimes Hy = H(xy)$, designa-se por grupo quociente de G por H .*

É fácil verificar que a Definição 11.8 corresponde à definição de grupo. Por outro lado, deve observar-se que se $H \not\triangleleft G$, então a operação \otimes pode não fazer sentido.

Definição 11.9 (G -conjunto). *Dado um grupo G e um conjunto arbitrário X , diz-se que G opera sobre X (ou que X é um G -conjunto) quando se define uma função $\theta : G \times X \rightarrow X$ que satisfaz as seguintes propriedades:*

$$(a) \quad \forall_{x \in X} \theta(e, x) = x \text{ (onde } e \text{ é o elemento neutro de } G\text{)},$$

$$(b) \quad \forall_{g,h \in G} \theta(g, \theta(h, x)) = \theta(gh, x).$$

Por economia de escrita, em geral, escreve-se gx em vez de $\theta(g, x)$, pelo que em (a) pode escrever-se $ex = x$ e em (b) $g(hx) = (gh)x$. Convém, no entanto, reter que enquanto g e h são elementos do grupo G , x é um elemento de X .

Definição 11.10 (Órbita). *Sendo X um G -conjunto de um grupo G (pelo que G opera sobre X por intermédio de uma certa função $\theta : G \times X \rightarrow X$) e $x \in X$, designa-se por órbita (ou trajectória) de x e denota-se por $\text{Orb}(x)$ (ou $\text{Orb}_G(x)$), o conjunto $\{\theta(g, x) : g \in G\}$ (em notação mais aligeirada pode escrever-se, simplesmente, $\text{Orb}(x) = \{gx : g \in G\}$).*

Habitualmente, se $y \in \text{Orb}(x)$, pelo que $\exists_{g \in G} y = gx$, diz-se que g desloca x para y .

Definição 11.11 (Estabilizador). *Sendo X um G -conjunto de um grupo G e $x \in X$, designa-se por estabilizador do elemento x e denota-se por $\text{Stb}(x)$ (ou $\text{Stb}_G(x)$) o conjunto $\{g \in G : \theta(g, x) = x\}$ (isto é, $\text{Stb}(x) = \{g \in G : gx = x\}$). Este conjunto também se designa por conjunto de estacionaridade.*

Verifica-se (ver Teorema 11.3 (iii)) que o estabilizador de um elemento x , $\text{Stb}(x)$, constitui um subgrupo de G .

Exemplo 11.5. Vamos determinar os estabilizadores de um grupo finito G que operam sobre ele próprio por intermédio da função $\theta : G \times G \rightarrow G$ tal que $\theta(g, h) = ghg^{-1}$.

Solução. Neste caso, o G -conjunto é o próprio conjunto G e a operação θ designa-se por operação de conjugação. Para cada $x \in G$, a órbita de x é definida pelo conjunto $\text{Orb}(x) = \{gxg^{-1} : g \in G\}$ e, neste caso, o estabilizador de x é

$$\text{Stb}(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}.$$

Um tal conjunto, designa-se por conjunto centralizador de G em relação a x . □

Com facilidade, ainda se verifica que a operação de conjugação define uma relação de equivalência em G (a prova destas afirmação é proposta no Exercício 11.4).

Teorema 11.3. Sendo G um grupo finito e X um G -conjunto, verificam-se as seguintes propriedades:

$$(i) \quad \bigcup_{x \in X} \text{Orb}(x) = X,$$

$$(ii) \quad \forall_{x,y \in X} \text{Orb}(x) \cap \text{Orb}(y) \neq \emptyset \Rightarrow \text{Orb}(x) = \text{Orb}(y),$$

$$(iii) \quad \forall_{x \in X} \text{Stb}(x) \leq G,$$

$$(iv) \quad \forall_{x \in X} [G : \text{Stb}(x)] = |\text{Orb}(x)| \text{ ou, de modo equivalente, } |G| = |\text{Stb}(x)| \cdot |\text{Orb}(x)|.$$

Demonstração.

(i) Pela propriedade (a) da Definição 11.9, $\forall_{x \in X} x = ex \in \text{Orb}(x)$, donde vem que $X = \bigcup_{x \in X} \text{Orb}(x)$.

- (ii) Suponha que $\text{Orb}(x) \cap \text{Orb}(y) \neq \emptyset$. Então $\exists g, h \in G$ tais que $gx = hy$. Se $z \in \text{Orb}(x)$, então $\exists f \in G$ tal que $fx = z$ e, uma vez que $x = g^{-1}hy$,

$$z = fx = fg^{-1}hy \in \text{Orb}(y).$$

Logo, $\text{Orb}(y) \supseteq \text{Orb}(x)$. Por simetria (trocando x e y) obtém-se a inclusão recíproca $\text{Orb}(x) \supseteq \text{Orb}(y)$ e, como consequência, $\text{Orb}(x) = \text{Orb}(y)$.

- (iii) Seja $x \in X$. É claro que $e \in \text{Stb}(x)$ (uma vez que $ex = x$) e, consequentemente, não só $\text{Stb}(x) \neq \emptyset$ como $\text{Stb}(x)$ tem elemento neutro. Assim, basta mostrar que

$$\forall_{a,b \in \text{Stb}(x)} ab^{-1} \in \text{Stb}(x).$$

Porém, por definição, $ax = x$ e $bx = x \Rightarrow b^{-1}bx = b^{-1}x \Rightarrow b^{-1}x = x$. Logo, $ab^{-1}x = ax = x$ e, consequentemente, $ab^{-1} \in \text{Stb}(x)$.

- (iv) Considere o conjunto das classes laterais (à esquerda) de $\text{Stb}(x)$ em G , e a função

$$\eta_x : \{g \text{Stb}(x) : g \in G\} \rightarrow \text{Orb}(x), \text{ tal que } \eta_x(g \text{Stb}(x)) = gx.$$

Uma vez que, por construção, η_x é uma aplicação sobrejectiva, vamos provar apenas que também é injectiva. Suponha que existem duas classes laterais $h \text{Stb}(x)$ e $f \text{Stb}(x)$ tais que

$$\eta_x(h \text{Stb}(x)) = \eta_x(f \text{Stb}(x)) \text{ ou, de modo equivalente, } hx = fx.$$

Então $f^{-1}hx = x$, pelo que $f^{-1}h \in \text{Stb}(x)$ e, consequentemente, $h = f(f^{-1}h) \in f \text{Stb}(x)$. Dado que $h \in h \text{Stb}(x)$, vem

$$h \in h \text{Stb}(x) \cap f \text{Stb}(x).$$

Logo, tendo em conta que as classes laterais constituem uma partição de G , $h \text{Stb}(x) = f \text{Stb}(x)$, o que completa a prova da injectividade de η_x . Finalmente, da bijectividade de η_x decorre $[G : \text{Stb}(x)] = |\{g \text{Stb}(x) : g \in G\}| = |\text{Orb}(x)|$. \square

Como consequência imediata do Teorema 11.3 (i) e (ii), podemos concluir que o conjunto das órbitas distintas de X constitui uma partição de X . Por outro lado, tendo em conta a equação orbital (iv), $[G : \text{Stb}(x)] = |\text{Orb}(x)|$, a fórmula para o índice $[G : \text{Stb}(x)] = \frac{|G|}{|\text{Stb}(x)|}$ implica a igualdade $|G| = |\text{Stb}(x)| \cdot |\text{Orb}(x)|$. Assim, concluímos que a grupos de estacionaridade de cardinalidade elevada correspondem órbitas de pequena cardinalidade e reciprocamente.

11.2. Lema de Burnside

Introduzidos os instrumentos e resultados (da teoria dos grupos) necessários, estamos agora em condições de abordar um tema, tipicamente combinatório, relacionado com a enumeração (ou contagem) de diferentes (ou não equivalentes) configurações de objectos, para o que se torna imprescindível o desenvolvimento de técnicas adequadas para a respectiva distinção. Uma destas técnicas consiste em interpretar as classes de configurações equivalentes como órbitas de uma certa operação de um grupo sobre o conjunto das diferentes configurações a analisar. Assim, depois de se definirem os critérios segundo os quais duas configurações se distinguem, escolhendo (de um modo conveniente) um grupo que opere adequadamente sobre o conjunto de todas as configurações, o número de configurações não equivalentes corresponderá ao número de órbitas distintas. O teorema a seguir, conhecido por lema de Burnside¹ fornece um método para a contagem destas órbitas.

¹ William Burnside publicou este resultado em 1900, depois de Augustin-Louis Cauchy em 1845 e Georg Frobenius em 1887 o terem feito. Por esta razão, o lema de Burnside é conhecida também como lema de Cauchy-Frobenius, lema de Pólya-Burnside e lema que não é de Burnside.

Definição 11.12 (Função de peso). *Dado um grupo G e um G -conjunto X , designa-se por função peso toda a função $w : X \rightarrow \mathbb{Z}$ que é constante em cada órbita $\text{Orb}(x)$, para $x \in X$. Por abuso de linguagem, também se escreve $w(\text{Orb}(x)) = w(x)$.*

Teorema 11.4 (Lema de Burnside). *Seja G um grupo finito que opera sobre um G -conjunto finito X e, para cada $g \in G$, seja $F(g) = \{x \in X : x = gx\}$ e $\lambda(g) = |F(g)|$. Se G tem k órbitas distintas O_1, O_2, \dots, O_k que determinam X , então*

$$\sum_{i=1}^k w(O_i) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in F(g)} w(x),$$

ou, no caso particular em que $\forall_{x \in X} w(x) = 1$,

$$k = \frac{1}{|G|} \sum_{g \in G} \lambda(g).$$

Demonstração. Pelo Teorema 11.3 (iv), se x e y pertencem à mesma órbita, então os estabilizadores de x e y têm a mesma cardinalidade. Logo, para $x \in O_i$, fazendo $|\text{Stb}(x)| = s(O_i)$, de acordo com o Teorema 11.3 (iv), $|O_i|s(O_i) = |G|$. Consequentemente,

$$\begin{aligned} \sum_{g \in G} \sum_{x \in F(g)} w(x) &= \sum_{x \in X} \sum_{g \in \text{Stb}(x)} w(x) = \sum_{x \in X} w(x) \sum_{g \in \text{Stb}(x)} 1 \\ &= \sum_{x \in X} w(x)|\text{Stb}(x)| = \sum_{i=1}^k s(O_i) \sum_{x \in O_i} w(x) \\ &= \sum_{i=1}^k s(O_i)|O_i|w(O_i) = |G| \sum_{i=1}^k w(O_i). \end{aligned} \quad \square$$

O lema de Burnside estabelece que o número de órbitas é igual ao número médio de pontos fixos determinados pelos conjuntos $F(g)$, cuja união $\bigcup_{g \in G} F(g)$ se designa, habitualmente, por *conjunto de pontos fixos* da operação de G sobre X (ou conjunto de pontos fixos do G -conjunto X).

Nos exemplos a seguir, vamos utilizar o lema de Burnside na resolução de problemas de enumeração combinatória.

Exemplo 11.6. *Vamos calcular em quantas factorizações distintas como produtos de três números naturais se consegue decompor o número 1000 (considerando que duas factorizações são distintas se não se podem obter uma da outra por permutação dos respectivos factores).*

Solução. Dado que $1000 = 2^35^3$, qualquer factorização de 1000 no produto de três números naturais é da forma $(2^{\alpha_1}5^{\beta_1})(2^{\alpha_2}5^{\beta_2})(2^{\alpha_3}5^{\beta_3})$, onde o 6-uplo $(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3)$ é tal que $\alpha_i, \beta_i \in \{0, 1, 2, 3\}$ para $i \in \{1, 2, 3\}$ e $\alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3 = 3$. Se M é o conjunto de tais 6-uplos, então $M = M_\alpha \times M_\beta$, onde $M_\alpha = \{(\alpha_1, \alpha_2, \alpha_3) \in \{0, 1, 2, 3\}^3 : \alpha_1 + \alpha_2 + \alpha_3 = 3\}$ e $M_\beta = \{(\beta_1, \beta_2, \beta_3) \in \{0, 1, 2, 3\}^3 : \beta_1 + \beta_2 + \beta_3 = 3\}$. Logo, $|M| = |M_\alpha||M_\beta| = |M_\alpha|^2$, uma vez que $|M_\alpha| = |M_\beta|$ e, consequentemente, dado que $M_\alpha = \{(1, 1, 1), (2, 1, 0), (2, 0, 1), (1, 2, 0), (0, 2, 1), (1, 0, 2), (3, 0, 0), (0, 3, 0), (0, 0, 3)\}$, conclui-se que $|M| = 10^2$.

Tendo em conta que as diferentes factorizações são invariantes relativamente à ordem dos factores $(2^{\alpha_i}5^{\beta_i})$, vamos considerar a operação do grupo gerado pelos ciclos relativos às permutações do conjunto $\{1, 2, 3\}$, S_3 , sobre M , definida do seguinte modo:

$$\forall_{\pi \in S_3} \pi \otimes (\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3) = (\alpha_{\pi(1)}, \alpha_{\pi(2)}, \alpha_{\pi(3)}, \beta_{\pi(1)}, \beta_{\pi(2)}, \beta_{\pi(3)}).$$

Nestas condições, duas factorizações são consideradas equivalentes se podem ser obtidas, uma da outra, por permutações dos ternos de pares (α_1, β_1) , (α_2, β_2) e (α_3, β_3) . Consequentemente, esta equivalência verifica-se se e só se os 6-uplos definidos pelas factorizações pertencem à mesma órbita, pelo que o resultado pretendido é, precisamente, o número de órbitas de M .

Para se aplicar o lema de Burnside, temos de calcular o número de pontos fixos, ou seja, temos de determinar $\lambda(g)$, para cada $g \in G$. Assim,

1. sendo $\sigma_1 = \pi_{id}$, o elemento identidade de G , obtém-se $\lambda(\sigma_1) = 100$;
2. sendo $\sigma_2 \in G$ uma transposição, obtém-se $\lambda(\sigma_2) = 4$ (por exemplo, se $\sigma_2 = [1\ 2]$, então mantêm-se fixos $(1, 1, 1, 1, 1, 1)$, $(0, 0, 3, 1, 1, 1)$, $(1, 1, 1, 0, 0, 3)$ e $(0, 0, 3, 0, 0, 3)$);
3. sendo σ_3 um ciclo de comprimento 3, obtém-se $\lambda(\sigma_3) = 1$ (uma vez que, neste caso, apenas o ponto $(1, 1, 1, 1, 1, 1)$ fica fixo).

Consequentemente, denotando por $|\sigma_i|$ o número de elementos de G do tipo σ_i , para $i \in \{1, 2, 3\}$, de acordo com o lema de Burnside, o número de órbitas vem dado por

$$\frac{1}{|G|} \sum_{g \in G} \lambda(g) = \frac{1}{3!} (100|\sigma_1| + 4|\sigma_2| + 1|\sigma_3|).$$

Tendo em conta que $|\sigma_1| = 1$, $|\sigma_2| = 3$ ($[1\ 2]$, $[2\ 3]$, $[1\ 3]$) e $|\sigma_3| = 2$ ($[1\ 2\ 3]$ e $[1\ 3\ 2]$), o número de órbitas (e de factorizações) fica

$$\frac{1}{|G|} \sum_{g \in G} \lambda(g) = \frac{1}{6} (100 \cdot 1 + 4 \cdot 3 + 1 \cdot 2) = 19.$$

Com efeito, as factorizações distintas possíveis são: $1 \cdot 1 \cdot 1000$, $1 \cdot 2 \cdot 500$, $1 \cdot 4 \cdot 250$, $1 \cdot 5 \cdot 200$, $1 \cdot 8 \cdot 125$, $1 \cdot 10 \cdot 100$, $1 \cdot 20 \cdot 50$, $1 \cdot 25 \cdot 40$, $2 \cdot 2 \cdot 250$, $2 \cdot 4 \cdot 125$, $2 \cdot 5 \cdot 100$, $2 \cdot 10 \cdot 50$, $2 \cdot 20 \cdot 25$, $4 \cdot 5 \cdot 50$, $4 \cdot 10 \cdot 25$, $5 \cdot 5 \cdot 40$, $5 \cdot 8 \cdot 25$, $5 \cdot 10 \cdot 20$ e $10 \cdot 10 \cdot 10$. \square

Embora a aplicação do lema de Burnside se torne suficiente na resolução de vários problemas relacionados com contagens de configurações não equivalentes, o facto de obrigar à determinação do número de pontos fixos de um G -conjunto, torna-o impraticável em muitas situações.

Uma técnica muito usual em contagens (ou enumerações) consiste em identificar os objectos a enumerar como funções entre conjuntos apropriadamente escolhidos. Assim, sendo A e B os conjuntos considerados, os quais vamos supor finitos e não vazios, o conjunto das funções $f : A \rightarrow B$, B^A , como é sabido, tem cardinalidade $|B|^{|A|}$. Algumas destas funções, porém, embora correspondam a diferentes elementos do conjunto B^A , são consideradas equivalentes quando, por exemplo, as suas imagens em B correspondem a configurações equivalentes. Por razões relacionadas com as aplicações, os elementos do conjunto B designam-se por *cores* e as funções $f : A \rightarrow B$ designam-se por *colorações*.

Por outro lado, se algumas configurações de elementos do conjunto A são equivalentes, então existe um grupo de permutações de elementos do conjunto A , G^* , para o qual cada permutação de G^* transforma configurações equivalentes umas nas outras. Por sua vez, o grupo G^* gera um grupo G de permutações de elementos de B^A que produz as órbitas do conjunto $X = B^A$, cada uma das quais determina uma configuração distinta (não equivalente). O cálculo do número destas órbitas pode ser efectuado recorrendo ao lema de Burnside.

Muitas vezes é difícil calcular $\lambda(g)$ para todos os elementos do grupo G . Porém, esta dificuldade pode ser ultrapassada, tendo em conta que uma função $f \in X = B^A$ é um ponto fixo se e só se a permutação g^* é fixa em cada um dos seus $c(g^*)$ ciclos. Logo, $\lambda(g) = |B|^{c(g^*)}$ e, neste caso, o lema de Burnside pode escrever-se na forma:

$$k = \frac{1}{|G^*|} \sum_{g^* \in G^*} |B|^{c(g^*)}. \quad (11.2)$$

Exemplo 11.7. Vamos calcular o número de colares de cinco contas distintos que podemos construir, colorindo as respectivas contas com

1. duas cores,
2. três cores.

Solução. Uma vez que um colar é um ciclo de comprimento cinco, para além da permutação identidade $(1\ 2\ 3\ 4\ 5) = [1][2][3][4][5]$, existem quatro rotações de uma, duas, três e quatro contas, ou seja, $(2\ 3\ 4\ 5\ 1) = [2\ 3\ 4\ 5\ 1]$, $(3\ 4\ 5\ 1\ 2) = [1\ 3\ 5\ 2\ 4]$, $(4\ 5\ 1\ 2\ 3) = [1\ 4\ 2\ 5\ 3]$, $(5\ 1\ 2\ 3\ 4) = [1\ 5\ 4\ 3\ 2]$ e, como consequência, existe uma permutação com cinco ciclos e quatro permutações com um ciclo. Adicionalmente, considerando o colar representado num plano e rodando-o no espaço tridimensional, em torno de um eixo, também representado no plano (levantando uma conta de um lado da recta e baixando outra conta do lado oposto), podemos obter (consoante a escolha do eixo) 5 reflexões, cada uma das quais relativa a uma recta que passe por uma conta e pela aresta oposta, cada uma das quais determina uma permutação: $(1\ 5\ 4\ 3\ 2) = [1][2\ 5][3\ 4]$, $(3\ 2\ 1\ 5\ 4) = [2][1\ 3][4\ 5]$, etc. Uma vez que cada uma destas permutações tem três ciclos, de acordo com a fórmula (11.2), obtém-se

1. $\frac{1}{5}(1 \cdot 2^5 + 4 \cdot 2^1) = 8$ colares distintos, considerando unicamente as rotações planares, ou $\frac{1}{10}(1 \cdot 2^5 + 4 \cdot 2^1 + 5 \cdot 2^3) = 8$ colares distintos, quando se consideram as rotações planares e todas as possíveis reflexões.
2. $\frac{1}{5}(1 \cdot 3^5 + 4 \cdot 3^1) = 51$ colares distintos, considerando unicamente as rotações planares, ou $\frac{1}{10}(1 \cdot 3^5 + 4 \cdot 3^1 + 5 \cdot 3^3) = 39$ colares distintos, quando se consideram as rotações planares e todas as possíveis reflexões.

Deve observar-se que no caso de duas cores, considerar todas as possíveis reflexões, conjuntamente com as rotações no plano, não diminui o número de colares distintos que se podem obter. \square

Exemplo 11.8. Vamos calcular o número de colorações distintas das casas de um tabuleiro de dimensão 2×2 , utilizando duas cores (branco e preto).

Solução. Vamos atribuir um número a cada casa do tabuleiro, tal como se indica:

1	2
4	3

. Neste caso, existe a permutação identidade $(1\ 2\ 3\ 4) = [1][2][3][4]$ e três permutações correspondentes a rotações de 90° $-(2\ 3\ 4\ 1) = [2\ 3\ 4\ 1]$, de 180° $-(3\ 4\ 1\ 2) = [1\ 3][2\ 4]$ e de 270° $-(4\ 1\ 2\ 3) = [4\ 3\ 2\ 1]$. Como consequência, existe uma permutação com quatro ciclos, uma permutação com dois ciclos e duas permutações com um ciclo. Logo, de acordo com a fórmula (11.2), existem $\frac{1}{4}(1 \cdot 2^4 + 1 \cdot 2^2 + 2 \cdot 2^1) = 6$ colorações distintas para o tabuleiro 2×2 .

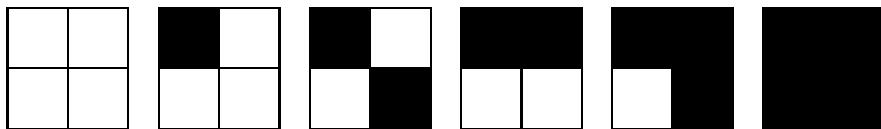


Figura 11.1: Diferentes colorações das casas de um tabuleiro de dimensão 2×2 , com recurso às cores branco e preto.

Na verdade, tal como se apresenta na Figura 11.1, existem apenas seis colorações distintas, com duas cores, para as casas de um tabuleiro 2×2 . \square

É claro que se pode concluir que existem $\frac{1}{4}(k^4 + k^2 + 2k)$ colorações distintas das casas de um tabuleiro de dimensão 2×2 , utilizando k cores. No Exercício 11.7 propõe-se a generalização deste resultado para um tabuleiro de dimensão $n \times n$.

Exemplo 11.9. Vamos calcular o número de colorações das faces de um cubo, utilizando k cores.

Solução. Vamos determinar todos as simetrias de um cubo (permutações das faces) e respectivos números de ciclos. Assim, podemos detectar a existência de:

- uma permutação identidade, com 6 ciclos de comprimento 1;
- quatro rotações de 120° e quatro rotações de 240° , em torno das rectas que passam pelos 4 pares de vértices opostas – cada uma delas com dois ciclos de comprimento 3;
- seis rotações de 180° , em torno das rectas que passam pelos centros dos seis pares de arestas opostas – cada uma delas com três ciclos de comprimento 2;
- nove rotações, em torno das rectas que passam pelos centros dos três pares de faces opostas, das quais
 - três de 90° e três de 270° – cada uma delas com um ciclo de comprimento 4 e dois ciclos de comprimento 1,
 - e três de 180° – cada uma delas com dois ciclos de comprimento 2 e dois ciclos de comprimento 1.

Conjuntamente, conclui-se que existe uma permutação com seis ciclos, três permutações com quatro ciclos, doze permutações com três ciclos e oito permutações com dois ciclos. Logo, de acordo com a fórmula (11.2) existem

$$c_k = \frac{1}{24}(k^6 + 3k^4 + 12k^3 + 8k^2)$$

colorações das faces de um cubo, utilizando k cores (ver Tabela 11.1). □

k	1	2	3	4	5	6
c_k	1	10	57	240	800	2.226

Tabela 11.1: Número c_k de colorações das faces de um cubo, utilizando k cores, para $k = 1, \dots, 6$.

11.3. Teorema de Pólya

Antes de prosseguirmos com alguns resultados da teoria da enumeração de Pólya, convém introduzir o conceito de estrutura cíclica de uma permutação. Assim, dada uma permutação $\pi \in S_n$, representada por um produto de ciclos disjuntos (que é único a menos da ordem dos factores), designa-se por *estrutura cíclica* de π o n -uplo $c(\pi) = (c_1(\pi), c_2(\pi), \dots, c_n(\pi))$, onde $c_i(\pi)$ é igual ao número de ciclos de comprimento i na sua representação cíclica. Note-se que $1c_1(\pi) + 2c_2(\pi) + \dots + nc_n(\pi) = n$.

Por exemplo, a permutação $\pi \in S_8$, dada por $\pi = (3\ 5\ 6\ 8\ 4\ 1\ 7\ 2)$, tem a representação cíclica $\pi = [7][1\ 3\ 6][2\ 5\ 4\ 8]$, à qual corresponde a estrutura cíclica $c(\pi) = (1, 0, 1, 1, 0, 0, 0, 0)$.

Dado um grupo G , identificado como sendo o grupo de permutações sobre o conjunto X (tal que $|X| = m$), a cada permutação $g \in G$ sobre X está associada uma estrutura cíclica $c(g) = (c_1(g), \dots, c_m(g))$ que, por sua vez, dá origem ao que se designa por *índice cíclico* de g que a seguir se define.

Definição 11.13 (Índice cíclico de uma permutação). *Dada uma permutação g de elementos de um conjunto de cardinalidade m , designa-se por índice cíclico de g o monómio²*

$$z(g; x_1, \dots, x_m) = x_1^{c_1(g)} x_2^{c_2(g)} \cdots x_m^{c_m(g)} = \prod_{i=1}^m x_i^{c_i(g)},$$

onde os símbolos x_i , para $i = 1, \dots, m$, denotam variáveis.

O conceito de índice cíclico é extensível a um grupo G de permutações, denotando-se esta extensão por $Z(G; x_1, \dots, x_m)$ (ou, simplesmente, $Z(x_1, \dots, x_m)$, quando é claro que se trata do grupo G).

Definição 11.14 (Índice cíclico de um grupo). *Dado um grupo G de permutações de elementos de um conjunto de cardinalidade m , designa-se por índice cíclico de G o polinómio*

$$Z(G; x_1, \dots, x_m) = \frac{1}{|G|} \sum_{g \in G} z(g; x_1, \dots, x_m) = \frac{1}{|G|} \sum_{g \in G} x_1^{c_1(g)} x_2^{c_2(g)} \cdots x_m^{c_m(g)}.$$

Deve observar-se, por um lado, que no polinómio $Z(G; x_1, \dots, x_m)$ fica registada, simbolicamente, toda a informação relativa aos comprimentos dos ciclos disjuntos em que se decompõem as várias permutações de G ($G \leq S_m$) e, por outro, que a sua determinação depende unicamente de G .

Tendo presente, novamente, o grupo finito G da secção 11.2 que opera sobre o conjunto de colorações dos elementos de A por intermédio das cores definidas pelos elementos de B (funções de B^A), vamos definir o conceito de *polinómio padrão de g* . Antes porém, convém introduzir o conceito de *tipo de coloração*. Assim, diz-se que um dado conjuntos de colorações são do tipo (k_1, \dots, k_n) quando cada uma delas atribui a cor 1 a k_1 objectos, a cor 2 a k_2 objectos, etc.

Definição 11.15 (Polinómio padrão de uma permutação). *Supondo que se pretendem colorir os m objectos de um conjunto A com as n cores de um conjunto B , considerando um grupo G de permutações de elementos de A que actua sobre os elementos de B^A (colorações), para cada $g \in G$, sendo $a_{k_1, \dots, k_n}(g)$ o número de colorações do tipo (k_1, \dots, k_n) que ficam invariantes em relação a g (isto é, que são g -equivalentes), designa-se por polinómio padrão de g e denota-se por $p_g(x_1, \dots, x_n)$, o polinómio nas variáveis x_1, \dots, x_n :*

$$p_g(x_1, \dots, x_n) = \sum_{k_1 + \dots + k_n = m} a_{k_1, \dots, k_n}(g) x_1^{k_1} \cdots x_n^{k_n}.$$

Da definição de polinómio padrão de g decorre que o número de colorações g -invariantes de elementos de A , utilizando as cores de B , vem dado por

$$p_g(1, \dots, 1) = \sum_{k_1 + \dots + k_n = m} a_{k_1, \dots, k_n}(g),$$

onde $|A| = m$ e $|B| = n$.

Uma vez definido o polinómio padrão de um elemento de G , podemos estender este conceito ao próprio G .

Definição 11.16 (Polinómio padrão de um grupo). *Dado um grupo de permutações G , designa-se por polinómio padrão de G e denota-se por $P_G(x_1, \dots, x_n)$, o polinómio nas variáveis x_1, \dots, x_n :*

$$P_G(x_1, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} p_g(x_1, \dots, x_n).$$

²George Pólya escolheu a letra z por ser a inicial da palavra de origem alemã *zyclenzeiger* (que se traduz por indicador de ciclo).

Deve observar-se que o polinómio padrão de $g \in G$, determina, simbolicamente, o número de colorações g -invariantes de cada um dos tipos. Por exemplo, no termo $a_{k_1, \dots, k_n}(g)x_1^{k_1} \cdots x_n^{k_n}$ o coeficiente $a_{k_1, \dots, k_n}(g)$ dá o número de colorações g -invariantes cujo tipo é definido por $x_1^{k_1} \cdots x_n^{k_n}$, ou seja, cujo tipo é (k_1, \dots, k_n) . O interesse desta representação simbólica, em detrimento de uma eventual listagem dos diferentes valores obtidos para as diferentes colorações, reside no facto de $p_g(x_1, \dots, x_n)$ poder ser deduzido directamente a partir da estrutura cíclica de g . Com efeito, conforme o teorema de Pólya³ estabelece (mais adiante), o polinómio P_G (que está definido em função da operação de G sobre o conjunto de colorações) pode exprimir-se em função do índice cíclico $Z(G; x_1, \dots, x_m)$, o qual depende unicamente de G , quando G é considerado como um subgrupo de S_n .

Teorema 11.5 (de Pólya). *Dado um grupo finito G que opera sobre o conjunto de funções B^A (onde $|A| = m$ e $|B| = n$), para cada $g \in G$, com estrutura cíclica $c(g) = (c_1(g), \dots, c_m(g))$, verifica-se*

$$a) \quad P_g(x_1, \dots, x_n) = z(g; \sum_{j=1}^n x_j, \sum_{j=1}^n x_j^2, \dots, \sum_{j=1}^n x_j^m) = \prod_{i=1}^m \left(\sum_{j=1}^n x_j^i \right)^{c_i(g)},$$

b) $z(g; n, \dots, n)$ corresponde ao número de colorações g -invariantes.

Demonstração.

a) Seja $g \in G$ tal que $g = \sigma_1\sigma_2\dots\sigma_r$, onde $\sigma_1, \sigma_2, \dots, \sigma_r$ são ciclos disjuntos de comprimento $|\sigma_1|, |\sigma_2|, \dots, |\sigma_r|$, respectivamente. Interpretando as funções de B^A como colorações de elementos de A pelas cores de B , para que os elementos de A sejam g -invariantes, torna-se necessário que os $|\sigma_1|$ elementos afectados por σ_1 tenham a mesma cor, de entre as n possíveis. Consequentemente, para os $|\sigma_1|$ elementos afectados por σ_1 , obtém-se o polinómio padrão (preliminar)

$$a_{|\sigma_1|, 0, \dots, 0} x_1^{|\sigma_1|} + a_{0, |\sigma_1|, \dots, 0} x_2^{|\sigma_1|} + \cdots + a_{0, 0, \dots, |\sigma_1|} x_n^{|\sigma_1|} = x_1^{|\sigma_1|} + x_2^{|\sigma_1|} + \cdots + x_n^{|\sigma_1|}.$$

De modo análogo, para os $|\sigma_2|$ elementos afectados por σ_2 , obtém-se

$$a_{|\sigma_2|, 0, \dots, 0} x_1^{|\sigma_2|} + a_{0, |\sigma_2|, \dots, 0} x_2^{|\sigma_2|} + \cdots + a_{0, 0, \dots, |\sigma_2|} x_n^{|\sigma_2|} = x_1^{|\sigma_2|} + x_2^{|\sigma_2|} + \cdots + x_n^{|\sigma_2|}.$$

Porém, uma vez que cada cor atribuída aos elementos de σ_1 é compatível com qualquer das cores atribuídas aos elementos de σ_2 , a totalidade das colorações g -invariantes de $|\sigma_1| + |\sigma_2|$ elementos de A vem (simbolicamente) determinada pela adição de todos os possíveis produtos de $x_i^{|\sigma_1|}$ por $x_j^{|\sigma_2|}$, com $i, j \in \{1, \dots, n\}$, a qual corresponde ao produto

$$(x_1^{|\sigma_1|} + x_2^{|\sigma_1|} + \cdots + x_n^{|\sigma_1|})(x_1^{|\sigma_2|} + x_2^{|\sigma_2|} + \cdots + x_n^{|\sigma_2|}).$$

Da repetição deste argumento para os restantes ciclos da decomposição $g = \sigma_1\sigma_2\dots\sigma_r$, decorre o polinómio padrão da permutação g

$$\prod_{k=1}^r (x_1^{|\sigma_k|} + x_2^{|\sigma_k|} + \cdots + x_n^{|\sigma_k|}).$$

Tendo em atenção que o número de ciclos de comprimento $|\sigma_k|$ da decomposição de g é $c_{|\sigma_k|}(g)$, com $1 \leq k \leq r$, e que $\forall k \in \{1, \dots, m\}$, finalmente, vem

$$P_g(x_1, x_2, \dots, x_n) = \prod_{k=1}^r (x_1^{|\sigma_k|} + \cdots + x_n^{|\sigma_k|}) = \prod_{i=1}^m (x_1^i + \cdots + x_n^i)^{c_i(g)}.$$

³George Pólya (1887–1985), de nacionalidade húngara, publicou esta teorema em 1937 num artigo com o título *Kombinatorische Anzahlbestimmung für Gruppen, Graphen und chemische Verbindungen*, Acta Math. 68, 145–254.

- b) Uma vez que g apresenta a estrutura cíclica $c(g) = (c_1(g), c_2(g), \dots, c_m(g))$, as funções (colorações) que ficam fixas quando operadas com g , são as funções constantes para todos os elementos de cada ciclo de g . Dado que existem $c_1(g) + \dots + c_m(g)$ ciclos, a cada um dos quais é associado um dos n elemento de B , o número de funções invariantes por g é $n^{c_1(g)+\dots+c_m(g)} = z(g; n, \dots, n)$.

□

Como consequência imediata deste teorema, obtém-se o corolário a seguir.

Corolário 11.6. *Supondo que m objectos (elementos de um conjunto A) são coloridos com n cores (elementos de um conjunto B), qualquer que seja o subgrupo G de S_m ($G \leq S_m$), o número de colorações (funções de $f : A \rightarrow B$) G -não equivalentes do tipo (k_1, \dots, k_n) (onde $k_j = |f^{-1}(x_j)|$ para $j = 1, \dots, n$) é o coeficiente de $x_1^{k_1} \cdots x_n^{k_n}$ no índice cíclico de G , o qual é determinado pelo polinómio*

$$P_G(x_1, \dots, x_n) = Z(G; \sum_{j=1}^n x_j, \sum_{j=1}^n x_j^2, \dots, \sum_{j=1}^n x_j^m).$$

Adicionalmente, o número total de colorações G -não equivalentes vem dado por $P_G(1, 1, \dots, 1) = Z(G; n, n, \dots, n)$.

No que se segue, vamos demonstrar e aplicar um resultado equivalente ao Teorema 11.5, recorrendo ao conceito de função peso, utilizada no contexto das colorações (configurações) de objectos. Assim, sendo $w : B \rightarrow \mathbb{R}$ uma função peso definida num conjunto de cores B , designa-se por *peso de uma configuração* f (isto é, de uma função $f : A \rightarrow B$)

$$W(f) = \prod_{a \in A} w(f(a)).$$

É claro que se duas funções pertencem a uma mesma órbita, então os pesos das respectivas configurações são iguais. Tal como anteriormente, por abuso de linguagem, consideramos o peso de uma órbita O_i como sendo o peso de um dos seu elementos, ou seja,

$$\forall_{f \in O_i} W(O_i) = W(f).$$

Teorema 11.7 (de Burnside-Pólya). *Seja G um grupo finito que opera sobre um G -conjunto finito X de funções $f : A \rightarrow B$ (com $|A| = m$ e $|B| = n$). Se G tem k órbitas distintas O_1, O_2, \dots, O_k , então*

$$\sum_{i=1}^k W(O_i) = Z(G; \sum_{b \in B} w(b), \sum_{b \in B} w^2(b), \dots, \sum_{b \in B} w^m(b)).$$

No caso particular em que $\forall_{b \in B} w(b) = 1$, obtém-se $k = Z(G; n, \dots, n)$.

Demonstração. Com recurso ao lema de Burnside,

$$\sum_{i=1}^k W(O_i) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in F(g)} W(x),$$

onde $F(g) = \{x \in B^A : x \text{ é constante nos ciclos de } g\} = \{x \in B^A : \forall_{a \in \sigma_i} x(a) = b_i, b_i \in B, i = 1, \dots, s_g\}$ e $\sigma_1, \dots, \sigma_{s_g}$, são ciclos de g . Então

$$\sum_{x \in F(g)} W(x) = \sum_{b_1, \dots, b_{s_g} \in B} \prod_{i=1}^{s_g} w(b_i)^{|\sigma_i|} = \prod_{j=1}^m \left(\sum_{b \in B} w^j(b) \right)^{c_j(g)}$$

e, como consequência,

$$\sum_{i=1}^k W(O_i) = \frac{1}{|G|} \sum_{g \in G} \prod_{j=1}^m \left(\sum_{b \in B} w^j(b) \right)^{c_j(g)} = Z(G; \sum_{b \in B} w(b), \dots, \sum_{b \in B} w^n(b)).$$

□

Usualmente utilizam-se os pesos 1 e x , se existem duas cores, 1, x e y se existem três cores, etc. Por exemplo, se no índice cíclico do grupo das permutações de elementos de A que actua em B^A se verifica a igualdade $x_i = 1 + x^i + y^i$, então podemos interpretar este índice cíclico como uma função geradora do número de configurações (onde, por exemplo, o coeficiente de $x^s y^t$ é o número de configurações, onde existem s elementos coloridos com a segunda cor, t elementos coloridos com a terceira cor e $|A| - s - t$ elementos coloridos com a primeira cor).

Exemplo 11.10. Vamos determinar os índices cílicos dos grupos referidos nos Exemplos 11.7, 11.8 e 11.9.

Solução.

11.7. Uma vez que se consideram apenas rotações, podemos concluir que existem 5 permutações: uma permutação identidade com cinco ciclos de comprimento 1 que corresponde ao termo do índice cíclico relativo a x_1^5 e quatro permutações com um ciclo de comprimento cinco, cada uma das quais corresponde ao termo do índice cíclico relativo a x_5^1 . Logo, o índice cíclico vem dado por

$$Z(G; x_1, x_2, x_3, x_4, x_5) = \frac{1}{5}(x_1^5 + 4x_5).$$

É claro que $Z(G; 2, 2, 2, 2, 2) = 8$ é o número de colorações com duas cores e $Z(G; 3, 3, 3, 3, 3) = 51$ é o número de colorações com três cores. Assim, para o caso de duas cores, fazendo $x_i = 1 + x^i$, obtém-se

$$f_2(x) = \frac{1}{5}((1+x)^5 + 4(1+x^5)) = 1 + x + 2x^2 + 2x^3 + x^4 + x^5,$$

onde f_2 denota a função geradora do número de colorações, utilizando duas cores (por exemplo, branco e preto). Como exemplo, note-se que o termo $2x^3$ da função geradora $f_2(x)$ significa que existem duas configurações com exactamente três contas pretas (e as restantes brancas). Analogamente, para o caso de três cores, fazendo $x_i = 1 + x^i + y^i$, obtém-se

$$\begin{aligned} f_3(x, y) &= \frac{1}{5}((1+x+y)^5 + 4(1+x^5+y^5)) \\ &= 1 + x + y + 2x^2 + 4xy + 2y^2 + 2x^3 + 6x^2y + 6xy^2 + 2y^3 + x^4 + \\ &\quad 4x^3y + 6x^2y^2 + 4xy^3 + y^4 + x^5 + x^4y + 2x^3y^2 + 2x^2y^3 + xy^4 + y^5, \end{aligned}$$

onde f_3 é a função geradora do número de colorações do colar de 5 contas, utilizando três cores (por exemplo, branco, preto e vermelho). Como exemplo, note-se que o termo $6x^2y$ da função geradora $f_3(x, y)$, significa que existem seis configurações com duas contas pretas, uma conta vermelha e as restantes $5 - 2 - 1 = 2$ brancas.

11.8. Existem quatro permutações do tabuleiro de dimensão 2×2 : uma permutação identidade, com quatro ciclos de comprimento 1, à qual corresponde o termo do índice cíclico relativo a x_1^4 , uma permutação com dois ciclos de comprimento dois, à qual corresponde o termo do índice cíclico relativo a x_2^2 e duas permutações com um ciclo de comprimento quatro, às quais correspondem os dois termos do índice cíclico relativos a x_4 . Logo, o índice cíclico é

$$Z(G; x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4).$$

Tal como anteriormente, fazendo $x_i = 1 + x^i$, obtém-se a função geradora do número de colorações do tabuleiro de dimensão 2×2 , utilizando duas cores,

$$f_2(x) = \frac{1}{4} ((1+x)^4 + (1+x^2)^2 + 2(1+x^4)) = 1 + x + 2x^2 + x^3 + x^4.$$

Finalmente, fazendo $x_i = 1 + x^i + y^i$, obtém-se a função geradora para o número de colorações do tabuleiro de dimensão 2×2 , utilizando três cores,

$$f_3(x, y) = \frac{1}{4} ((1+x+y)^4 + (1+x^2+y^2)^2 + 2(1+x^4+y^4)).$$

- 11.9. Neste caso, tendo presente a descrição efectuada no Exemplo 11.9 das diferentes permutações das faces do cubo que se podem obter por simetria, o índice cíclico vem dado por

$$Z(G; x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}(x_1^6 + 8x_3^2 + 6x_2^3 + 6x_1^2x_4 + 3x_1^2x_2^2). \quad (11.3)$$

Como consequência, fazendo $x_i = 1 + x^i$, a função geradora para o número de colorações das faces de um cubo, utilizando duas cores, vem dada por

$$f_2(x) = 1 + x + 2x^2 + 2x^3 + 2x^4 + x^5 + x^6.$$

□

11.4. Grupo diedral

Designa-se por *grupo diedral* e denota-se por D_n , o grupo de simetrias de um polígono regular com n vértices. Por exemplo, o grupo D_3 formado pelas simetrias de um triângulo equilátero tem 6 elementos: as 3 rotações de ângulos 0 (ou 2π), $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ em torno do centro e as três reflexões em torno dos eixos de simetria (ver Figura 11.3).

$$D_3 = \{\pi_{id} = (1\ 2\ 3), (3\ 1\ 2), (2\ 3\ 1), (1\ 3\ 2), (3\ 2\ 1), (2\ 1\ 3)\}. \quad (11.4)$$

O grupo de simetrias D_n de um polígono regular com n vértices (e, consequentemente, n lados) tem $2n$ elementos; n rotações e n reflexões. Sendo P_n um polígono regular com n vértices $V = \{v_1, \dots, v_n\}$, podemos considerar P_n como o transformado nele próprio pelos elementos do subgrupo cíclico C_n , gerado pelas rotações ρ^k em torno do centro, no sentido anti-horário, de um ângulo de $\frac{2k\pi}{n}$, para $k = 0, 1, \dots, n-1$. Como consequência, sendo σ uma reflexão em torno de um eixo de simetria, ou seja, a reflexão em torno de um dos n eixos que passam pelo centro do polígono e por um dos vértices (eixos de simetria de P_n), podemos explicitar os elementos de D_n da seguinte forma:

$$D_n = \{\pi_{id}, \rho^1, \dots, \rho^{n-1}, \sigma, \sigma \circ \rho, \dots, \sigma \circ \rho^{n-1}\} = \langle \rho, \sigma \rangle.$$

Com base na observação dos elementos que constituem D_n , podemos deduzir as seguintes propriedades básicas:

1. $\sigma^2 = \pi_{id} = \rho^n$.
2. O grupo cíclico $C_n = \{\pi_{id}, \rho, \dots, \rho^{n-1}\}$ é um subgrupo (normal) de D_n com índice 2.
3. Os elementos $\sigma, \sigma \circ \rho, \dots, \sigma \circ \rho^{n-1}$ são todos distintos, uma vez que

$$\sigma \circ \rho^i = \sigma \circ \rho^j \Leftrightarrow \rho^i = \rho^j \Leftrightarrow i = j (\mod n).$$

4. $\sigma \circ \rho^k$ não é uma rotação de C_n , uma vez que para $p, q \in \{1, \dots, n\}$

$$\sigma \circ \rho^p = \rho^q \Leftrightarrow \sigma = \rho^{q-p},$$

o que é impossível.

5. $\rho \circ \sigma = \sigma \circ \rho^{-1}$, dado que, de acordo com o item 4, $\sigma \circ \rho$ não é uma rotação. Logo, trata-se uma reflexão σ' (dado que D_n tem apenas rotações e reflexões). Tendo em conta 1, $\pi_{id} = \sigma' \circ \sigma' = (\rho \circ \sigma)^2$, ou seja, $(\rho \circ \sigma) \circ (\rho \circ \sigma) = \pi_{id} \Leftrightarrow \rho \circ \sigma = \sigma \circ \rho^{-1}$.

Observe-se que para o grupo diedral D_n as simetrias $\pi_{id}, \rho, \rho^2, \dots, \rho^{n-1}$ são rotações e as simetrias $\sigma, \sigma \circ \rho, \sigma \circ \rho^2, \dots, \sigma \circ \rho^{n-1}$ são reflexões. As rotações do grupo diedral D_n formam um subgrupo que é isomorfo ao grupo cíclico C_n .

Exemplo 11.11. Vamos mostrar que, no grupo diedral D_n ,

1. a composição de duas rotações ou de duas reflexões é uma rotação,
2. a composição de uma rotação com uma reflexão é uma reflexão.

Solução.

1. Sendo ϕ e ψ duas rotações, vem $\phi = \rho^k$ e $\psi = \rho^l$, com $k, l \in \{0, \dots, n-1\}$. Como consequência, $\phi \circ \psi = \rho^k \circ \rho^l = \rho^{k+l}$ é uma rotação.
Analogamente, sendo ϕ e ψ duas reflexões, vem $\phi = \sigma \circ \rho^k$ e $\psi = \sigma \circ \rho^l$, com $k, l \in \{0, \dots, n-1\}$. Como consequência,

$$\phi \circ \psi = \sigma \circ \rho^k \circ \sigma \circ \rho^l = \sigma \circ \sigma \circ \rho^{-k} \circ \rho^l = \sigma^2 \circ \rho^{l-k} = \rho^{l-k}$$

é uma rotação.

2. Sendo ϕ uma rotação e ψ ma reflexão, vem $\phi = \rho^k$ e $\psi = \sigma \circ \rho^l$, com $k, l \in \{0, \dots, n-1\}$. Como consequência,

$$\phi \circ \psi = \rho^k \circ \sigma \circ \rho^l = \sigma \circ \rho^{-k} \circ \rho^l = \sigma \circ \rho^{l-k}$$

é uma reflexão. □

Atenção! Uma vez que $\rho \circ \sigma \neq \sigma \circ \rho$, o grupo diedral é não-abeliano, para $n > 2$.

Exemplo 11.12. Vamos determinar o grupo diedral D_4 do quadrado e o índice cíclico dele.

Solução. Sendo ρ a rotação em torno de O de ângulo $\pi/2$ e σ a reflexão em torno do eixo horizontal, vem

$$\begin{aligned} \pi_{id} &= (1\ 2\ 3\ 4), & \rho &= [2\ 3\ 4\ 1], & \rho^2 &= [1\ 3][2\ 4], & \rho^3 &= [1\ 4\ 3\ 2], \\ \sigma &= [2\ 4], & \sigma \circ \rho &= [1\ 4][2\ 3], & \sigma \circ \rho^2 &= [1\ 3] & \text{e} & \sigma \circ \rho^3 = [1\ 2][3\ 4], \end{aligned}$$

conforme se ilustra na Figura 11.2 e, a partir desta decomposição cíclica, obtém-se

$$Z(D_4; x_1, x_2, x_3, x_4) = \frac{1}{8}(x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2x_2).$$

Exemplo 11.13. Vamos determinar o índice cíclico do grupo diedral D_3 .

Solução. Tenho em conta (11.4) temos $c(1\ 2\ 3) = (3, 0, 0)$, $c(3\ 1\ 2) = (0, 0, 1)$, $c(2\ 3\ 1) = (0, 0, 1)$, $c(1\ 3\ 2) = (1, 1, 0)$, $c(3\ 2\ 1) = (1, 1, 0)$, $c(2\ 1\ 3) = (1, 1, 0)$. Logo

$$Z(D_3; x_1, x_2, x_3) = \frac{1}{6}(x_1^3 + 2x_3 + 3x_1x_2).$$

□

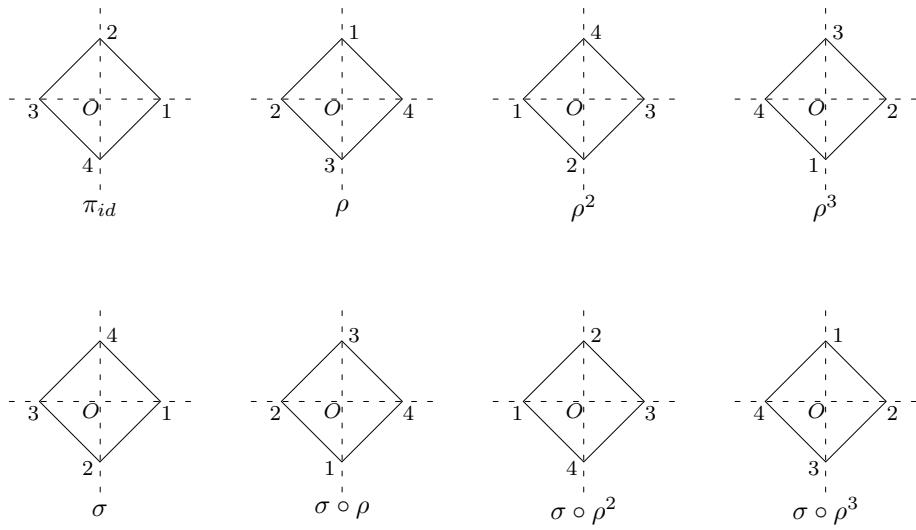


Figura 11.2: Grupo diedral de simetrias do quadrado.

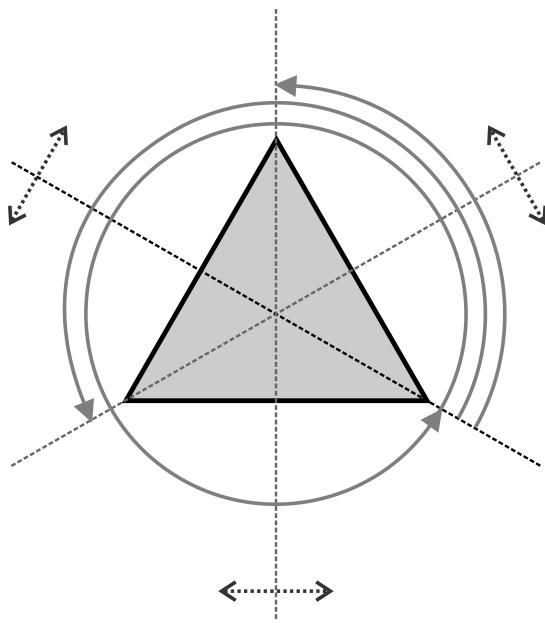


Figura 11.3: Grupo diedral de simetrias do triângulo equilátero.

11.5. Exercícios.

- 11.1. Sendo A_n o conjunto de todas as permutações pares de elementos do conjunto $\{1, \dots, n\}$, prove que A_n munido do produto de transposições é um grupo.
- 11.2. Prove que A_n é um subgrupo de S_n de índice 2 e que, consequentemente, é um subgrupo normal de S_n .
- 11.3. Dado um grupo arbitrário G de ordem n , onde e denota o elemento neutro, e dado $x \in G$, prove que
- $\langle x \rangle$ é um grupo;
 - $k = |\langle x \rangle|$ é o menor inteiro positivo tal que $x^k = e$;
 - $x^n = e$.
- 11.4. Dado um grupo G , prove que a relação de conjugação em G , R , definida por $(f, h) \in R$ se e só se $\exists g \in G$ tal que $f = g^{-1}hg$, é uma relação de equivalência.
- 11.5. Supondo que G é um grupo finito, que \leq define uma relação linear em G e que X é um G -conjunto, prove que a relação \preceq , definida em $G \times X$ por $(g_1, x_1) \preceq (g_2, x_2) \Leftrightarrow (g_1x_1 = g_2x_2 \wedge g_1 \leq g_2)$, é uma relação de ordem parcial.
- 11.6. Determine o número de colares distintos de n contas que podemos construir, colorindo as respectivas contas com apenas k cores, admitindo que dois colares são distintos se um deles não se pode obter do outro por simples rotação (ver Exemplo 11.7).
- 11.7. Determine o número de colorações distintas das casas de um tabuleiro de dimensão $n \times n$, utilizando k cores. Resolva este mesmo problema admitindo que o tabuleiro é transparente, pelo que a mesma coloração pode ser vista de ambas as faces.
- 11.8. Supondo que se pretende colorir os 6 vértices de um octaedro regular (ver Figura 11.4) utilizando três cores distintas (por exemplo, verde, azul e vermelho), quantas colorações distintas são possíveis e (em particular) quantas, de entre estas, têm 3 vértices verdes, 1 azul e 2 vermelhos?

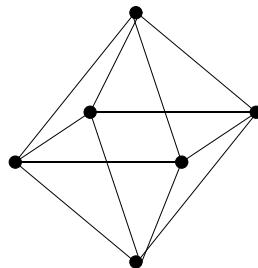


Figura 11.4: Representação do octaedro.

- 11.9. Determine o grupo diedral de simetrias do pentágono regular, D_5 , e o respectivo índice cíclico.
- 11.10. Determine o grupo diedral de simetrias do hexágono regular, D_6 , e o respectivo índice cíclico.
- 11.11. Mostre que o índice cíclico do grupo cíclico C_n vem dado por

$$Z(C_n; x_1, \dots, x_n) = \frac{1}{n} \sum_{k|n} \varphi(k) x_k^{n/k},$$

onde φ denota a função de Euler.

11.12. Mostre que o índice cíclico do grupo diedral D_n vem dado por

$$Z(D_n; x_1, \dots, x_n) = \frac{1}{2} Z(C_n; x_1, \dots, x_n) + \begin{cases} \frac{1}{2} x_1 x_2^{(n-1)/2}, & \text{se } n \text{ é ímpar;} \\ \frac{1}{4} (x_2^{n/2} + x_1^2 x_2^{(n-2)/2}), & \text{se } n \text{ é par.} \end{cases}$$

11.13. Seja D_n um grupo diedral, com $n > 2$. Mostre que

- (a) D_n é não-abeliano,
- (b) $\rho \circ \sigma = \sigma \circ \rho^{-1}$, onde ρ é uma rotação e σ é uma reflexão.

11.14. Sendo D_4 o grupo diedral e $H = \{\text{id}, \sigma\} \subseteq D_4$, determine as classes laterais à direita e à esquerda de H .

11.15. Sendo (G, \cdot) e (G', \cdot') dois grupos com elementos unidade e e e' , respectivamente, e $\phi : G \rightarrow G'$ um homomorfismo, mostre que

- (a) $\phi(e) = e'$;
- (b) $\phi(g^{-1}) = (\phi(g))^{-1}$, para cada $g \in G$;
- (c) o núcleo de ϕ , N_ϕ , definido por $N_\phi = \{g \in G : \phi(g) = e'\}$, é um subgrupo normal de G ;
- (d) $\phi(G)$ é um subgrupo de G' .

11.16. Seja $f = [1 2][3 4 5 6] \in S_7$ e $G = \langle f \rangle$.

- (a) Determine G .
- (b) Determine $\text{Stb}(x)$, para cada $x \in \{1, 2, \dots, 7\}$.

11.17. Determine o número de colares que se podem obter, com 4 contas azuis e 3 contas vermelhas.

11.18. Sendo $G = \{\text{id}, [1 2], [3 4], [1 2][3 4]\} \subseteq S_4$, determine o índice cíclico do grupo G .

11.19. Mostre que para qualquer permutação $f \in S_n$, f e a sua inversa f^{-1} têm a mesma estrutura cíclica (tipo).

11.20. Utilizando o lema de Burnside, calcule o número de colorações de vértices de um hexágono regular utilizando 3 cores.

11.21. Determine todos os elementos do grupo D_5 como permutações cíclicas.

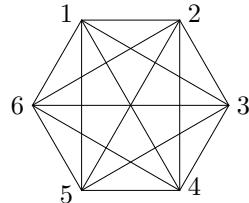
11.22. Sabendo que dado um grupo G que opera sobre o conjunto X , G é transitivo se para quaisquer dois elementos $x, y \in X$ existe $g \in G$ tal que $g \cdot x = y$, demonstre as seguintes proposições verdadeiras:

- (a) o grupo simétrico S_n é transitivo;
- (b) se G é um subgrupo de permutações ($G \subseteq S_n$) e G é transitivo, então existe $g \in G$ sem pontos fixos.
- (c) o subgrupo $H = \{\text{id}, [1 2][3 4], [1 3][2 4], [1 4][2 3]\} \subseteq S_4$ é transitivo.
- (d) o subgrupo $H' = \{\text{id}, [1 2][3 4], [1 3][2 4], [1 4][2 3]\} \subseteq S_5$ não é transitivo.

11.23. Demonstre, utilizando o lema de Burnside, que para qualquer subgrupo $G \subseteq S_n$

$$\frac{1}{|G|} \sum_{g \in G} \lambda(g) \geq 1.$$

- 11.24. Dada a permutação $\pi = (2, 3, \dots, n, 1) \in S_n$, determine π^k , com $k \in \mathbb{N}$.
- 11.25. Determine o índice cíclico de G , onde
- G é o grupo de permutações das arestas do tetraedro regular, obtidas por rotações;
 - G é o grupo de permutações de faces do tetraedro regular, obtidas por rotações,
 - G é um grupo isomorfo a S_3 ($G \cong S_3$);
 - G é um grupo isomorfo a $A_4 \triangleleft S_4$ ($G \cong A_4 \triangleleft S_4$);
 - G é o grupo de permutações de vértices de um octaedro regular.
- 11.26. Determine a função geradora do número de colorações dos vértices de um cubo utilizando duas cores.
- 11.27. Considere a classe das moléculas orgânicas da forma
-
- onde C denota um átomo de carbono e cada X denota um dos seguintes componentes: SH_3 (metil), C_2H_5 (étil), H (hidrogénio), Cl (cloro). A estrutura geométrica de cada uma destas moléculas é formada por um vértice central (que supomos localizado no interior de um tetraedro), ocupado pelo átomo de carbono, ligado aos vértices do tetraedro que são ocupados pelos componentes X .
- Determine o número de moléculas que se podem obter com esta estrutura.
 - Determine o número de moléculas, com esta estrutura, que não contêm nenhum átomo de cloro.
- 11.28. Prove que o grupo $(\mathbb{Z}, +)$, opera sobre o conjunto \mathbb{R} (recta), com as seguintes translações:
- $\mathbb{Z} \times \mathbb{R} \rightarrow \mathbb{R}$, $(n, x) \rightarrow n + x$;
 - $\mathbb{Z} \times \mathbb{R} \rightarrow \mathbb{R}$, $(n, x) \rightarrow (-1)^n x$.
- 11.29. Considere um hexágono regular, com vértices $V = \{1, 2, 3, 4, 5, 6\}$, e acrescente segmentos de recta unindo todos os pares de vértices entre si (os quais designaremos, simplesmente, por segmentos), conforme figura a seguir representa.



Denotando a figura obtida por K_6 , responda às seguintes questões:

- determine o índice cíclico de D_6 (isto é, o grupo de simetrias do hexágono);

- (b) encontre as órbitas da acção (operação) de D_6 sobre o conjunto E de todos os segmentos de K_6 que unem pares de pontos;
- (c) determine o estabilizador do segmento que une os vértices 1 e 2;
- (d) para cada $g \in D_6$, determine o conjunto de pontos fixos de g , $F(g)$.
- 11.30. Considere o grupo multiplicativo $C_2 = (\{-1, 1\}, \cdot)$ e \mathcal{B}_n o conjunto de todas as funções binárias n -áreas. Considerando que o grupo $C_2^n = (\{-1, 1\}^n, \odot)$, onde $(x_1, \dots, x_n) \odot (y_1, \dots, y_n) = (x_1 \cdot y_1, \dots, x_n \cdot y_n)$, opera sobre o conjunto \mathcal{B}_n , conforme a seguir se indica,

$$\forall_{\alpha=(\alpha_1, \alpha_2, \dots, \alpha_n) \in C_2^n} \quad \forall_{f \in \mathcal{B}_n} \quad \alpha f(x_1, \dots, x_n) = f(x_1^{\alpha_1}, \dots, x_n^{\alpha_n}),$$

com $x_i^1 = x_i$ e $x_i^{-1} = (-1) \cdot x_i$, responda às seguintes questões:

- (a) Mostre que no conjunto $\{f \in \mathcal{B}_n : |f^{-1}(1)| = k\}$, o número de órbitas é igual

$$\frac{1}{2^n} \binom{2^n}{k}, \quad \text{se } k \equiv 1 \pmod{2}$$

e

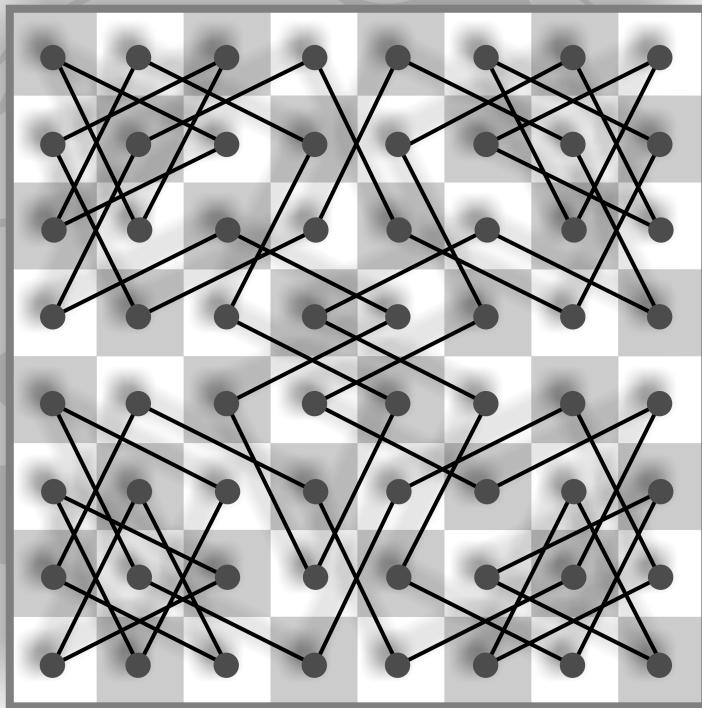
$$\frac{1}{2^n} \left(\binom{2^n}{k} + (2^n - 1) \binom{2^{n-1}}{k/2} \right), \quad \text{se } k \equiv 0 \pmod{2}.$$

- (b) Mostre que no conjunto \mathcal{B}_n , o número de órbitas é igual

$$\frac{1}{2^n} \left(2^{2^n} + (2^n - 1) 2^{2^{n-1}} \right).$$

Parte IV

Teoria dos Grafos e Algoritmos



12

Conceitos e Resultados Fundamentais

Muitos problemas do mundo real podem descrever-se (definir-se) na linguagem dos "grafos" – ou seja, por intermédio de uma figura que consiste num conjunto de pontos e um conjunto de linhas que ligam alguns pares de pontos. Mais geralmente, uma relação binária \mathcal{R} definida sobre um conjunto V (ver Secção 1.6) pode representar-se, graficamente, por um conjunto de pontos que corresponde ao conjunto V e por um conjunto de arcos (ou linhas não orientadas, no caso da relação \mathcal{R} ser simétrica) que ligam pares de pontos $x, y \in V$ tais que $x\mathcal{R}y$. Este modo de representação regista e torna evidente muitas propriedades que, por vezes, não são fáceis de detectar e/ou explicitar de outro modo. Por exemplo, considerando um conjunto de cidades no qual se define a relação binária: *a cidade A está relacionada com a cidade B se existe uma ligação directa entre elas.* No caso do número de cidades ser elevado, responder a uma simples questão, como seja,

| Utilizando, unicamente, as ligações definidas por esta relação, será que é possível viajar entre quaisquer duas cidades?

pode ser bastante difícil, utilizando apenas a linguagem das relações. Porém, olhando para o mapa de ligações entre cidades que decorre da representação gráfica desta relação, com facilidade se obtém a resposta pretendida. Este exemplo ilustra o tipo de dificuldades que podemos ultrapassar, recorrendo à linguagem dos grafos, podendo as questões tornarem-se substancialmente mais complicadas e de resolução praticamente impossível sem utilização de ferramentas apropriadas fornecidas pela teoria dos grafos. Este capítulo inicia o estudo da teoria dos grafos, abordando alguns conceitos e resultados fundamentais.

12.1. Grafos orientados e não orientados

Nesta secção introduzem-se as definições e notações básicas da teoria dos grafos e, uma vez que na literatura a terminologia e a notação utilizadas não são únicas, vamos apresentar as que consideramos mais frequentes.

Definição 12.1 (Grafo e grafo orientado). *Designa-se por grafo (não orientado) um terno $G = (V(G), E(G), \psi_G)$, onde $V = V(G)$ é um conjunto não vazio, $E = E(G)$ é um conjunto disjunto de V e ψ_G é uma função tal que, para cada $e \in E$, $\psi_G(e)$ denota um par não ordenado de elementos (não necessariamente distintos) de V . Neste caso, V designa-se por conjunto dos vértices, E por conjunto das arestas e ψ_G por função de incidência.*

No caso da função de incidência determinar, para cada $e \in E$, um par ordenado de elementos de V , o terno $\vec{G} = (V(\vec{G}), E(\vec{G}), \psi_{\vec{G}})$ designa-se por grafo orientado (ou digrafo) e o conjunto E designa-se por conjunto dos arcos.

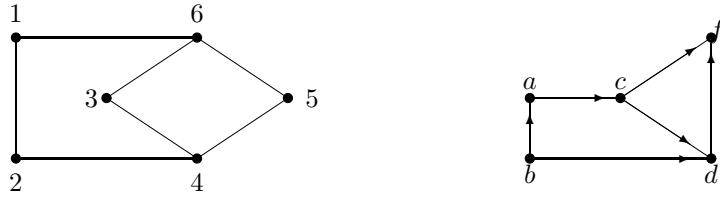


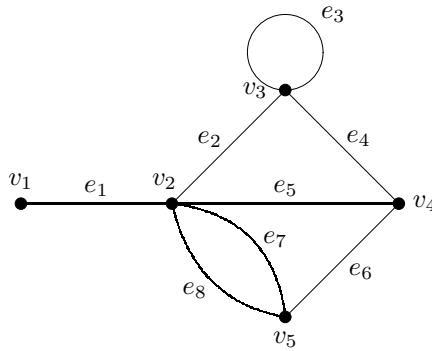
Figura 12.1: Exemplos de grafo e digrafo.

Dado um grafo (digrafo) G , por simplicidade de escrita, denotaremos as arestas (arcos) $e \in E(G)$ pelas respectivas imagens $\psi_G(e) = uv$, onde uv denota um par não ordenado (ordenado) de vértices. Neste caso, diz-se que u e v são os vértices *extremos* da aresta (do arco). Adicionalmente, se G é orientado, o vértice u designa-se por *cauda* e o vértice v por *cabeça* do arco e .

A partir de agora, sempre que se tornar irrelevante distinguir se um grafo é orientado ou não, adoptaremos a terminologia e a notação associada aos grafos não orientados, o mesmo se aplicando às respectivas propriedades.

Em geral, diz-se que uma aresta é *incidente* nos seus vértices extremos, os quais, por esse motivo, se dizem *adjacentes*. Também se diz que duas arestas incidentes num mesmo vértice são arestas *adjacentes*. O conjunto de todos os vértices adjacentes a um vértice $v \in V(G)$ designa-se por *vizinhança* de v e denota-se por $N_G(v)$ ou $N(v)$ quando não há dúvida relativamente ao grafo.

Uma aresta e com ambos os extremos no mesmo vértice, ou seja, tal que $\psi_G(e) = vv$, diz-se um *lacete*. Por sua vez, duas arestas com os mesmos vértices extremos designam-se por arestas *paralelas* (ver Figura 12.2).

Figura 12.2: Grafo $G = (V, E, \psi)$, tal que $V = \{v_1, v_2, v_3, v_4, v_5\}$, $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$ e $\psi(e_1) = v_1v_2$, $\psi(e_2) = v_2v_3$, etc. Note-se que os vértices v_1 e v_2 são extremos da aresta e_1 , a aresta e_3 é um lacete e as arestas e_7 e e_8 são paralelas.

É importante distinguir um grafo da figura que o representa. Com efeito, um grafo é um objecto abstrato – um terno, caracterizado pela Definição 12.1, que pode ser representado por várias figuras. Porém, embora um mesmo grafo possa admitir várias representações gráficas, cada representação gráfica determina um único grafo.

Definição 12.2 (Grafo simples). *Um grafo (digrafo) diz-se simples se não contém arestas (arcos) paralelas(os) nem lacetes.*

A Figura 12.3 representa um exemplo de grafo simples. Note-se que num grafo simples uma aresta é completamente determinada pelos seus vértices extremos e, neste caso, um grafo G simples pode definir-se, unicamente, pelo par de conjuntos $(V(G), E(G))$, onde cada elemento de $E(G)$ se denota

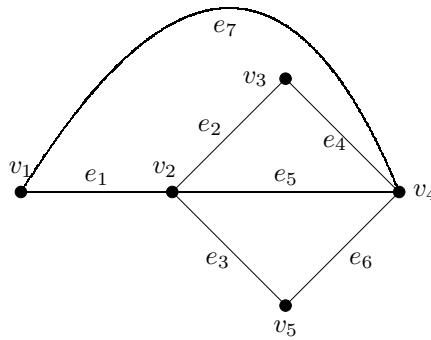


Figura 12.3: Grafo simples G , onde $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$ e $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$, com $e_1 = v_1v_2$, $e_2 = v_2v_3$, $e_3 = v_2v_5$, $e_4 = v_3v_4$, $e_5 = v_2v_4$, $e_6 = v_4v_5$ e $e_7 = v_1v_4$.

pelo correspondente par não orientado de vértices uv . Por outro lado, no caso de um grafo (digráfico) com lacetes e/ou arestas paralelas, para acentuar esse facto, é comum designá-lo por *multigrafo* (*multidigráfico*).

Um grafo simples com um único vértice designa-se por *grafo trivial*. Um grafo G diz-se um *grafo finito* se ambos os conjuntos $V(G)$ e $E(G)$ são finitos, ou seja, $|V(G)| < \infty$ e $|E(G)| < \infty$. Ao longo deste texto, designamos os grafos finitos, simplesmente, por grafos e os que não são finitos por *grafos infinitos*.

O número de vértices de um grafo G , ou seja, $|V(G)|$, designa-se por *ordem* de G e denota-se por $\nu(G)$ ou ν , no caso de não haver dúvidas em relação ao grafo a que se refere. Por outro lado, o número de arestas $|E(G)|$ designa-se por *dimensão* do grafo G e denota-se por $\varepsilon(G)$ ou, simplesmente, por ε .

Definição 12.3 (Igualdade de grafos). *Dois grafos G e H dizem-se iguais, escrevendo-se $G = H$, se*

$$V(G) = V(H), \quad E(G) = E(H) \quad \text{e} \quad \psi_G = \psi_H.$$

É claro que dois grafos iguais admitem uma mesma representação gráfica.

Definição 12.4 (Grau de um vértice). *Dado um grafo G e um vértice $v \in V(G)$, designa-se por *grau* (ou *valência*) de v e denota-se por $d_G(v)$ ou, simplesmente, por $d(v)$, o número de arestas incidentes no vértice v (onde os lacetes, caso existam, contam duas vezes). O maior grau dos vértices de G denota-se por $\Delta(G)$ e o menor grau por $\delta(G)$, ou seja,*

$$\Delta(G) = \max_{v \in V(G)} d_G(v) \quad \text{e} \quad \delta(G) = \min_{v \in V(G)} d_G(v).$$

Exemplo 12.1. Vamos determinar os graus dos vértices do grafo representado na Figura 12.3, bem como $\delta(G)$ e $\Delta(G)$.

Solução. Por observação da Figura 12.3, facilmente se conclui que $d_G(v_1) = 2$, $d_G(v_2) = 4$, $d_G(v_3) = 2$, $d_G(v_4) = 4$ e $d_G(v_5) = 2$.

Logo, $\delta(G) = 2$ e $\Delta(G) = 4$. □

No caso de um digrafo, \vec{G} , podemos separar o grau de um vértice $v \in V(\vec{G})$ em semigrau de entrada

$$d_{\vec{G}}^-(v) = |\{xv \in E(\vec{G})\}|$$

e semigrau de saída

$$d_{\vec{G}}^+(v) = |\{(vx \in E(\vec{G})\}|,$$

pelo que $d_{\vec{G}}^-(v) = d_{\vec{G}}^-(v) + d_{\vec{G}}^+(v)$. Como exemplo, o vértice c do digrafo representado na Figura 12.1 é tal que $d^-(c) = 1$, $d^+(c) = 2$ e $d(c) = 3$.

Definição 12.5 (Grafo complementar). *Dado um grafo G simples, designa-se por grafo complementar de G e denota-se por G^c , um grafo simples cujo conjunto de vértices é $V(G)$ e no qual dois vértices são adjacentes se e só se não são adjacentes em G .*

Na Figura 12.4 representa-se um grafo G e o seu complementar G^c .

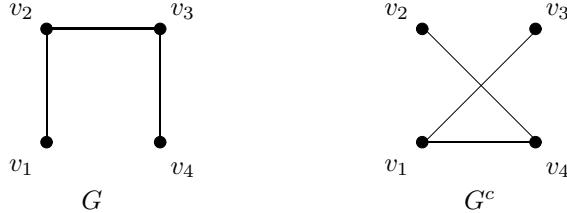


Figura 12.4: Par de grafos complementares G e G^c .

É muitas vezes, útil representar um grafo por intermédio de uma matriz, como seja, a *matriz de incidência* ou a *matriz de adjacência*.

Definição 12.6 (Matriz de incidência). *Dado um grafo G , tal que $V(G) = \{v_1, v_2, \dots, v_\nu\}$ e $E(G) = \{e_1, e_2, \dots, e_\varepsilon\}$, designa-se por matriz de incidência aresta vértice de G ou, simplesmente, matriz de incidência de G , a matriz $M_G = (m_{ij})$, $1 \leq i \leq \nu$, $1 \leq j \leq \varepsilon$, tal que*

$$m_{ij} = \begin{cases} 0, & \text{se } e_j = v_p v_q, \text{ com } i \notin \{p, q\}; \\ 1, & \text{se } e_j = v_i v_k, \text{ com } k \neq i; \\ 2, & \text{se } e_j = v_i v_i. \end{cases}$$

No caso de grafos orientados sem lacetes \vec{G} , as entradas da matriz de incidência $M_{\vec{G}} = (m_{ij})$ são definidas por

$$m_{ij} = \begin{cases} 0, & \text{se } e_j = v_p v_q, \text{ com } i \notin \{p, q\}; \\ -1, & \text{se } e_j = v_k v_i, \text{ para algum vértice } v_k; \\ 1, & \text{se } e_j = v_i v_k, \text{ para algum vértice } v_k. \end{cases}$$

Definição 12.7 (Matriz de adjacência). *Dado um grafo G , tal que $V(G) = \{v_1, v_2, \dots, v_\nu\}$, designa-se por matriz de adjacência dos vértices de G ou, simplesmente, matriz de adjacência de G e denota-se por $A_G = (a_{ij})$, a matriz de dimensão $\nu \times \nu$, tal que a_{ij} é igual ao número de arestas entre os vértices v_i e v_j . No caso de grafos orientados, a_{ij} é igual ao número de arcos com cauda em v_i e cabeça em v_j .*

Exemplo 12.2. Vamos determinar as matrizes de incidência e de adjacência do grafo representado na Figura 12.3.

Solução. Uma vez que o grafo G representado na Figura 12.3, tem ordem $\nu = 5$, dimensão $\varepsilon = 7$, $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$ e $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$, com $e_1 = v_1 v_2$, $e_2 = v_2 v_3$, $e_3 = v_2 v_5$, $e_4 = v_3 v_4$, $e_5 = v_2 v_4$, $e_6 = v_4 v_5$ e $e_7 = v_1 v_4$, a matriz de incidência vem dada por

$$M_G = \begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} & = & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{matrix}$$

e a matriz de adjacência toma a forma

$$A_G = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 \\ v_1 & 0 & 1 & 0 & 1 & 0 \\ v_2 & 1 & 0 & 1 & 1 & 1 \\ v_3 & 0 & 1 & 0 & 1 & 0 \\ v_4 & 1 & 1 & 1 & 0 & 1 \\ v_5 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

□

Deve observar-se que no caso dos grafos não orientados a respectiva matriz de adjacência é simétrica.

A demonstração do teorema que se segue constitui um exemplo de aplicação da matriz de incidência na obtenção de resultados relacionados com a estrutura de um grafo.

Teorema 12.1. *Dado um grafo G , verifica-se que a soma dos graus dos vértices é igual ao dobro do número de arestas, ou seja,*

$$\sum_{v \in V(G)} d_G(v) = 2|E(G)|.$$

Demonstração. Vamos fazer esta prova apenas para grafos não orientados, sendo imediata a respetiva generalização para grafos arbitrários (orientados ou não).

Seja $V(G) = \{v_1, v_2, \dots, v_\nu\}$ e $E(G) = \{e_1, e_2, \dots, e_\varepsilon\}$ e seja $M_G = (m_{ij})$ a correspondente matriz de incidência. Logo, a soma das entradas da linha correspondente ao vértice v é igual $d_G(v)$ e, como consequência, $\sum_{v \in V} d_G(v)$ é igual à soma de todas as entradas da matriz M_G . Por outro lado, uma vez que a soma das entradas de cada coluna de M_G é igual a 2, podemos concluir que a soma de todas as entradas de M_G é igual a $2|E(G)|$. □

Como consequência imediata deste teorema, podemos concluir que num grafo arbitrário G o número de vértices de grau ímpar é par.

No caso de grafos orientados é também imediato concluir que

$$\sum_{v \in V(G)} d_G^+(v) = \sum_{v \in V(G)} d_G^-(v) = |E(G)|.$$

12.2. Representações de grafos em computador

A possibilidade de utilização de computadores na resolução de problemas de teoria dos grafos influenciou, decisivamente, o alcance e diversidade das áreas de aplicação desta teoria. Na grande maioria dos problemas do mundo real, cujos modelos são grafos, a dimensão atinge proporções tão elevadas que os torna impossíveis de resolver sem recurso a meios computacionais. Com efeito, o desenvolvimento tecnológico foi em grande parte o responsável pelo interesse crescente que a teoria dos grafos tem sido alvo, tendo permitido a resolução de problemas que há algum tempo atrás seriam impossíveis de resolver.

Uma das questões essenciais para uma abordagem algorítmica eficiente dos problemas de aplicação da teoria dos grafos, é a da escolha das estruturas de dados a utilizar na *representação de um grafo em computador*. Actualmente, utilizam-se vários tipos de representações de grafos em computador, cada um dos quais tem vantagens e desvantagens, dependendo da estrutura do grafo, do problema a resolver, da linguagem de programação, etc. Segue-se uma descrição das principais representações de grafos.

Matriz de adjacência. A representação de um grafo G pela sua matriz de adjacência A_G (ver Definição 12.7) é talvez a mais popular. Uma vez que a matriz de adjacência tem dimensão $\nu \times \nu$, este tipo de representação necessita de $\Theta(\nu^2)$ células de memória, ou seja, tem complexidade espacial $\Theta(\nu^2)$ (ver notação assimptótica no Apêndice A). Embora, por vezes, seja possível reduzir um pouco a memória necessária para armazenar a matriz de adjacência de um grafo (como, por exemplo, no caso de um grafo não orientado cuja matriz é simétrica e, consequentemente, para o qual basta armazenar uma das entradas a_{ij} ou a_{ji}), o seu registo em computador exige sempre $\Theta(\nu^2)$ células de memória.

Matriz de incidência. A utilização da matriz de incidência M_G (ver Definição 12.6) de um grafo G é outro modo, muito utilizado, de armazenamento de grafos em computador. Este tipo de representação exige $\Theta(\nu\varepsilon)$ células de memória, o que pode ser maior ou menor do que ν^2 . Muitas vezes, porém, o número de arestas é maior do que o número de vértices, pelo que, nestes casos, a matriz de incidência requer mais células de memória do que a matriz de adjacência.

Lista de arestas. Um outro modo de representação de um grafo consiste na utilização de uma lista das respectivas arestas, por exemplo, o grafo da Figura 12.3 pode ser representado pela lista de pares não ordenados (ordenados, no caso de grafos orientados):

$$[v_1v_2, v_1v_4, v_2v_3, v_2v_4, v_2v_5, v_3v_4, v_4v_5].$$

Note-se que com esta representação perde-se a informação sobre a eventual existência de vértices isolados, ou seja, vértices de grau zero. Esta representação utiliza $\Theta(\varepsilon)$ células de memória e, nestas condições, se o número de arestas $\varepsilon = o(\nu^2)$, então a lista das arestas utiliza menos memória do que a matriz de adjacência. Porém, embora este tipo de representação utilize, em geral, menos memória, na maior parte dos casos, os algoritmos que recorrem a estas listas apresentam maior complexidade computacional.

Dois vectores. Uma representação de grafos que consiste numa modificação da representação por lista de arestas é a representação com recurso a dois vectores (duas sequências):

$$F = (f_1, f_2, \dots, f_\varepsilon) \quad \text{e} \quad H = (h_1, h_2, \dots, h_\varepsilon),$$

tais que a aresta e_i , para $i = 1, \dots, \varepsilon$, tem como vértices extremos f_i e h_i (ou, no caso de grafos orientados, o arco e_i tem cauda f_i e cabeça h_i). Por exemplo, para o grafo da Figura 12.3, os dois vectores que o representa têm a forma:

$$F = (v_1, v_2, v_2, v_3, v_2, v_4, v_1), \quad H = (v_2, v_3, v_5, v_4, v_4, v_5, v_4).$$

Esta representação utiliza $\Theta(\varepsilon)$ células de memória e tem as mesmas vantagens e desvantagens das lista de arestas.

Listas de sucessores (listas de adjacência). A representação de um grafo por uma lista de listas de sucessores, consiste na utilização de ν listas (ou vectores) tais que para cada vértice v a lista que lhe corresponde contém todos os vértices que lhe são adjacentes (ou todos os vértices que são a cabeça de um arco com cauda em v , se o grafo é orientado), com eventual repetição no caso de multigrafos. Por exemplo, para o grafo da Figura 12.3 obtém-se a seguinte lista de sucessores:

$$\begin{aligned} v_1 &: v_2, v_4 \\ v_2 &: v_1, v_3, v_4, v_5 \\ v_3 &: v_2, v_4 \\ v_4 &: v_1, v_2, v_3, v_5 \\ v_5 &: v_2, v_4 \end{aligned}$$

Esta representação utiliza $\Theta(\nu + \varepsilon)$ células de memória e, para vários algoritmos, trata-se de uma representação muito eficiente.

Existem ainda outras representações de grafos, por exemplo, com recurso à estrutura dos objectos (das linguagens de programação), pela função de incidência, etc. Todas estas representações são, matematicamente, equivalentes – uma vez que representam um mesmo grafo. Porém, a complexidade computacional dos algoritmos depende muito da representação e estrutura de dados utilizada.

12.3. Isomorfismos, grafos etiquetados e não etiquetados

É claro que dois grafos iguais admitem uma mesma representação gráfica. Porém, existem grafos distintos que admitem representações idênticas se excluirmos a etiquetação dos vértices ou arestas. Tais grafos designam-se por grafos isomorfos. Mais formalmente, temos a seguinte definição.

Definição 12.8 (Grafos isomorfos). *Dois grafos $G = (V(G), E(G), \psi_G)$ e $H = (V(H), E(H), \psi_H)$ dizem-se isomorfos, denotando-se esta relação de isomorfismo por $G \cong H$, se existem duas bijecções $\varphi : V(G) \rightarrow V(H)$ e $\theta : E(G) \rightarrow E(H)$ tais que*

$$\psi_G(e) = uv \quad \text{se e só se} \quad \psi_H(\theta(e)) = \varphi(u)\varphi(v).$$

Por outras palavras, dois grafos dizem-se isomorfos se existe uma bijecção entre os respectivos conjuntos de vértices e uma bijecção entre os respectivos conjuntos de arestas que preservam as relações de adjacência e de incidência. É fácil verificar que a relação de isomorfismo entre grafos é uma relação de equivalência. As classes quociente desta relação de isomorfismo designam-se por *grafos não etiquetados*. Uma vez que todos os grafos isomorfos admitem uma mesma representação gráfica, a menos das etiquetas dos vértices ou arestas, podemos concluir que esta representação, sem qualquer etiqueta, determina o grafo não etiquetado que define a correspondente classe.

No caso de grafos simples, nos quais as arestas ficam determinadas pelos respectivos extremos, a relação de isomorfismo reduz-se à existência de uma bijecção entre os respectivos conjuntos de vértices que preserva a adjacência. Mais formalmente, temos a seguinte definição.

Definição 12.9 (Isomorfismo entre grafos simples). *Designa-se por isomorfismo entre dois grafos simples G e H , uma bijecção $\varphi : V(G) \rightarrow V(H)$ tal que*

$$uv \in E(G) \quad \text{se e só se} \quad \varphi(u)\varphi(v) \in E(H).$$

De acordo com as Definições 12.8 e 12.9, no caso dos grafos simples, podemos concluir que dois grafos são isomorfos quando existe um isomorfismo entre eles.

Como exemplo, podemos concluir que os grafos G e G^c , representados na Figura 12.4, são isomorfos, uma vez que a bijecção $\varphi : V(G) \rightarrow V(G^c)$ definida por $\varphi(v_1) = v_2$, $\varphi(v_2) = v_4$, $\varphi(v_3) = v_1$ e $\varphi(v_4) = v_3$ é um isomorfismo entre G e G^c . Os grafos isomorfos aos respectivos complementares designam-se por *grafos autocomplementares*.

Exemplo 12.3. *Vamos demonstrar que os dois grafos representados na Figura 12.5 são isomorfos.*

Solução. Pretendemos encontrar uma bijecção

$$\varphi : \{u, v, w, x, y, z\} \rightarrow \{l, m, n, p, q, r\}$$

que preserve a relação de adjacência entre vértices. Assim, como todos os vértices têm um mesmo grau, escolhemos arbitrariamente, $\varphi(u) = l$. Consequentemente, dado que u é adjacente aos vértices

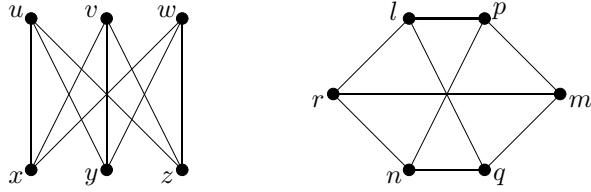


Figura 12.5: Exemplo de dois grafos isomorfos.

x , y e z , para φ ser um isomorfismo é necessário que l seja adjacente a $\varphi(x)$, $\varphi(y)$ e $\varphi(z)$. Seguidamente, escolhendo $\varphi(x) = p$, $\varphi(y) = q$ e $\varphi(z) = r$, apenas falta definir uma correspondência entre os subconjuntos de vértices que ainda não foram utilizados, ou seja, $\{v, w\} \rightarrow \{m, n\}$. Logo, tendo em conta que o vértice v é adjacente aos vértices x , y e z , cujas imagens por φ são, respectivamente, p , q e r , vem que $\varphi(v) = m$ e $\varphi(w) = n$. Finalmente, por verificação exaustiva, com facilidade se conclui que φ é um isomorfismo. \square

Exemplo 12.4. Vamos demonstrar que os isomorfismos entre grafos preservam os graus dos vértices.

Solução. Uma vez que (como consequência directa da definição de isomorfismo) um isomorfismo preserva os lacetes e as arestas paralelas, basta fazer a prova para o caso de grafos simples.

Sejam G e H dois grafos simples isomorfos ($G \cong H$) e seja φ um isomorfismo entre G e H . Então, $\varphi : V(G) \rightarrow V(H)$ é uma bijecção que preserva a relação de adjacência. Sendo $v \in V(G)$, tal que $d_G(v) = k$ e $N_G(v) = \{w_1, \dots, w_k\}$, podemos concluir que os vértices $\varphi(w_1), \varphi(w_2), \dots, \varphi(w_k)$ são todos distintos e adjacentes ao vértice $\varphi(v)$ em H . Por outro lado, tendo em conta a definição de isomorfismo, não existem outros vértices de H adjacentes a $\varphi(v)$. Logo, $d_H(\varphi(v)) = k$. \square

Definição 12.10 (Automorfismo). Designa-se por automorfismo de um grafo G , toda a bijecção $\varphi : V(G) \rightarrow V(G)$ que preserva o número de arestas entre pares de vértices.

No caso de um grafo simples G , podemos afirmar que um automorfismo é um isomorfismo entre G e G . No caso de um multigrafo H , para um dado automorfismo, podem existir mais do que um isomorfismo entre H e H . Deve observar-se ainda que qualquer grafo admite pelo menos um automorfismo que é a função identidade.

12.4. Conceitos métricos

Os conceitos métricos usuais podem estender-se aos grafos, de forma natural, com a introdução dos conceitos de *passeio*, *trajecto* e *caminho*.

Definição 12.11 (Passeio, trajecto e caminho). Dado um grafo G , designa-se por passeio em G toda a sequência não vazia

$$P = v_0e_1v_1e_2\dots e_kv_k,$$

tal que $v_0, v_1, \dots, v_k \in V(G)$, $e_1, e_2, \dots, e_k \in E(G)$ e os vértices v_{i-1} e v_i são vértices extremos da aresta e_i , para $i = 1, \dots, k$. O vértice v_0 designa-se por vértice inicial, o vértice v_k designa-se por vértice final e os vértices v_1, \dots, v_{k-1} designam-se por vértices intermédios do passeio P . Neste caso, também se diz que P é um passeio entre os vértices v_0 e v_k ou um (v_0, v_k) -passeio. Se em P todas as arestas são distintas então o passeio P designa-se por trajecto e se, adicionalmente, todos os vértices são distintos o passeio P designa-se por caminho.

Nos grafos simples todas as arestas são determinadas pelos seus extremos e, como consequência, um passeio é determinado pela sequência dos sucessivos vértices (ou seja, $P = v_0v_1\dots v_k$).

Um trajecto com pelo menos uma aresta e tal que $v_0 = v_k$, designa-se por *trajecto fechado* ou por *círculo*. Por sua vez, um *caminho fechado*, isto é, um passeio com pelo menos uma aresta e sem repetição de arestas nem vértices (com excepção dos vértices inicial e final), designa-se por *ciclo*.

Definição 12.12 (Comprimento e distância). *Dado um passeio P de um grafo G designa-se por comprimento de P e denota-se por $\text{comp}(P)$, o número de arestas (com eventual repetição) que o constitui. No caso dos caminhos, o comprimento coincide exactamente com o respectivo número de arestas.*

Dados dois vértices $x, y \in V(G)$, denotando por $\mathcal{P}_{x,y}$ o conjunto de todos os (x, y) -caminhos de G , designa-se por distância entre vértices de G a função $\text{dist}_G : V(G) \times V(G) \rightarrow \{0, \dots, \nu(G) - 1, \infty\}$ tal que

$$\text{dist}_G(x, y) = \begin{cases} \min_{P \in \mathcal{P}_{x,y}} \text{comp}(P) & \text{se } \mathcal{P}_{x,y} \neq \emptyset, \\ \infty & \text{se } \mathcal{P}_{x,y} = \emptyset. \end{cases} \quad (12.1)$$

Como consequência imediata desta definição, podemos concluir que uma aresta é um caminho de comprimento 1 e um vértice um caminho de comprimento 0. Por outro lado, um triângulo é um ciclo de comprimento 3.

Exemplo 12.5. Considerando o grafo G representado na Figura 12.6, vamos determinar todas as distâncias entre os seus vértices.

Solução. Observe-se que, por definição, $\text{dist}(a, a) = 0$, $\text{dist}(a, b) = 2$ uma vez que o caminho akb têm comprimento 2, $\text{dist}(a, c) = 2$ uma vez que o caminho ack têm comprimento 2, etc. Na Tabela 12.1 representam-se todas as distâncias entre vértices de G . \square

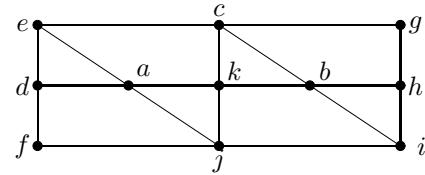


Figura 12.6: Grafo G do Exemplo 12.5.

Tabela 12.1: Distâncias entre vértices do grafo representado na Figura 12.6.

Teorema 12.2. Seja G um grafo simples. Se $\delta(G) \geq 2$, então G contém um caminho P e um ciclo C tais que $\text{comp}(P) \geq \delta(G)$ e $\text{comp}(C) \geq \delta(G) + 1$.

Demonstração. Seja $P = v_0, \dots, v_k$ um caminho de maior comprimento em G . Então todos os vizinhos de v_k estão em P (caso contrário, P poderia ser estendido para um vizinho e não teria comprimento máximo). Logo,

$$\text{comp}(P) = k \geq d_G(v_k) \geq \delta(G).$$

Por outro lado, se v_i é o vértice de menor índice em P tal que $v_i v_k \in E(G)$, então $v_i, v_{i+1}, \dots, v_k, v_i$ é um ciclo de comprimento pelo menos $\delta(G) + 1$ (dado que $\{v_i, v_{i+1}, \dots, v_k\}$ contém todos os vértices adjacentes a v_k , cujo número é não inferior a $\delta(G)$).

A Figura 12.7 ilustra a demonstração deste teorema. \square

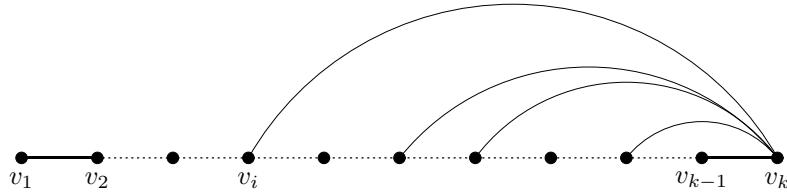


Figura 12.7: Ilustração da demonstração do Teorema 12.2.

Definição 12.13 (Cintura de um grafo). *Dado um grafo G , designa-se por cintura de G e denota-se por $g(G)$ o comprimento do circuito de menor comprimento em G , caso tal circuito exista. Caso contrário, diz-se que o grafo tem cintura infinita e escreve-se $g(G) = \infty$.*

Teorema 12.3 (Mantel). *Dado um grafo simples G , se $\varepsilon(G) > \frac{1}{4}\nu(G)^2$, então $g(G) = 3$ (ou seja, G contém um triângulo).*

Demonstração. Suponha que $\varepsilon(G) = \varepsilon$, $\nu(G) = \nu$ e ainda que $g(G) > 3$. Nestas condições, dados dois vértices adjacentes arbitrários, $x, y \in V(G)$, os conjuntos dos respectivos vizinhos têm intersecção vazia, ou seja,

$$\forall_{xy \in E(G)} N_G(x) \cap N_G(y) = \emptyset.$$

Consequentemente, qualquer que seja a aresta $xy \in E(G)$, $d_G(x) + d_G(y) \leq \nu$, donde se obtém

$$\sum_{ij \in E(G)} (d_G(i) + d_G(j)) = \sum_{v \in V(G)} d_G(v)^2 \leq \varepsilon\nu. \quad (12.2)$$

Por outro lado, de acordo com a desigualdade de Chebyshev (ver Exemplo 2.12).

$$\sum_{v \in V(G)} d_G(v)^2 \geq \frac{1}{\nu} \left(\sum_{v \in V(G)} d_G(v) \right)^2 = \frac{4\varepsilon^2}{\nu}. \quad (12.3)$$

Tendo em conta (12.2) e (12.3), vem

$$\frac{4\varepsilon^2}{\nu} \leq \sum_{v \in V(G)} d_G(v)^2 \leq \varepsilon\nu$$

e, consequentemente, $\varepsilon \leq \frac{1}{4}\nu^2$. \square

No Capítulo 14 analisam-se mais alguns resultados sobre conceitos métricos em grafos.

12.5. Grafos e subgrafos particulares

Seguem-se algumas definições de grafos especiais com utilização frequente, nomeadamente neste texto.

Definição 12.14 (Grafo completo e grafo nulo). *Seja G um grafo simples de ordem $n > 0$. Diz-se que G é um grafo completo e denota-se por K_n quando todos os pares de vértices são adjacentes. Por sua vez, diz-se que G é um grafo nulo quando não tem arestas, ou seja, $E(G) = \emptyset$.*

Note-se que (a menos de isomorfismos) existe um único grafo completo de ordem n , K_n . Por outro lado, todo o grafo nulo é o complementar de um grafo completo. Como consequência, podemos denotar o grafo nulo de ordem n por K_n^c . Apenas no caso do grafo trivial se verifica a igualdade $K_1 = K_1^c$. Na Figura 12.8 representam-se os grafos completos K_1, \dots, K_5 .

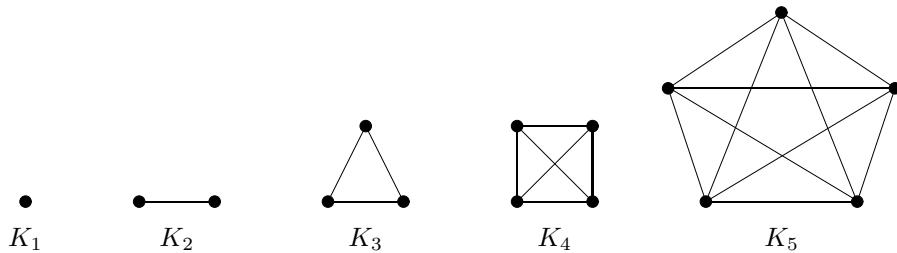


Figura 12.8: Grafos completos K_1, \dots, K_5 .

Definição 12.15 (Grafo regular). *Um grafo diz-se k -regular se todos os seus vértices têm grau k e diz-se regular se é k -regular para algum k .*

Os grafos 3-regulares também se designam por *grafos cúbicos*. São exemplos de grafos regulares, o grafo completo K_n (que é $(n - 1)$ -regular) e o grafo nulo K_n^c (que é 0-regular).

Definição 12.16 (Subgrafo). *Dados dois grafos G e H , diz-se que H é um subgrafo de G e denota-se $H \subseteq G$, se $V(H) \subseteq V(G)$, $E(H) \subseteq E(G)$ e ψ_H é a restrição de ψ_G ao conjunto $E(H)$. Se $H \subseteq G$ e $H \neq G$, então H designa-se por subgrafo próprio de G e denota-se $H \subset G$.*

Se H é um subgrafo de G , também se diz que G é um *supergrafo* de H .

Definição 12.17 (Subgrafo abrangente). *Diz-se que um grafo H é um subgrafo abrangente (ou de suporte) do grafo G se $H \subseteq G$ e $V(H) = V(G)$.*

Dado um grafo G , eliminando todos os lacetes e substituindo cada conjunto de arestas paralelas por uma única aresta, obtém-se o subgrafo abrangente de G que se designa por *subgrafo de suporte das arestas de G* . Nestas condições, podemos concluir que os grafos simples coincidem com o seu subgrafo de suporte das arestas.

Definição 12.18 (Subgrafo induzido). *Dado um grafo G e $\emptyset \neq \widehat{V} \subseteq V(G)$, designa-se por subgrafo de G induzido por \widehat{V} e denota-se por $G[\widehat{V}]$, o subgrafo cujo conjunto de vértices é \widehat{V} e o conjunto de arestas coincide com as arestas de G com extremos em \widehat{V} .*

Por simplicidade de escrita, o subgrafo induzido $G[V - \widehat{V}]$ que corresponde ao grafo obtido após a eliminação dos vértices do subconjunto \widehat{V} e, consequentemente, de todas as arestas incidentes em \widehat{V} , denota-se também por $G - \widehat{V}$. Adicionalmente, quando $\widehat{V} = \{v\}$, em vez de $G - \{v\}$ escreve-se, simplesmente, $G - v$.

Na Figura 12.9 representam-se alguns exemplos de subgrafos. Nesta figura verifica-se que G_1 é um subgrafo abrangente de G e $G_2 = G - v_5 = G[\{v_1, v_2, v_3, v_4\}]$ é o subgrafo induzido pelo subconjunto de vértices $\{v_1, v_2, v_3, v_4\}$.

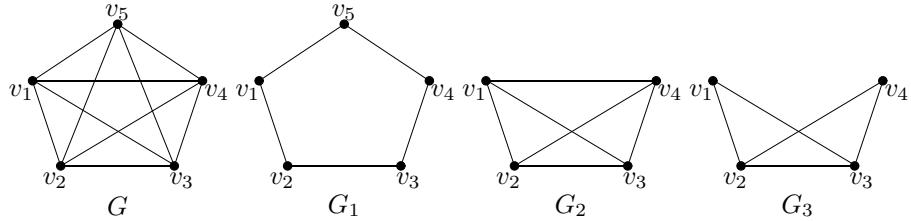


Figura 12.9: Exemplo de um grafo G com alguns dos seus subgrafos.

Definição 12.19 (Subgrafo induzido pelas arestas). *Dado um grafo G e $\emptyset \neq \hat{E} \subseteq E$, designa-se por subgrafo de G induzido pelo subconjunto de arestas \hat{E} e denota-se por $G[\hat{E}]$, o subgrafo cuja conjunto de arestas é \hat{E} e o conjunto de vértices é constituído pelos vértices extremos das arestas de \hat{E} .*

O subgrafo abrangente cujo conjunto de arestas é $E - \hat{E}$ denota-se por $G - \hat{E}$ e, no caso de $\hat{E} = \{e\}$, simplesmente, por $G - e$. Observe-se que, em geral, os grafos $G[E - \hat{E}]$ e $G - \hat{E}$ são distintos. Por outro lado, dado um grafo $G = (V, E)$, podemos concluir que $G = G[V]$, mas nem sempre se verifica a igualdade $G = G[E]$. Com efeito, $G = G[E]$ se e só se G não tem vértices isolados.

Definição 12.20 (Grafo bipartido). *Um grafo G diz-se bipartido se existe uma partição do seu conjunto de vértices em X e Y tal que não existem arestas entre qualquer par de vértices de X nem entre qualquer par de vértices de Y (ou seja, cada aresta de G tem um extremo em X e outro em Y). Esta partição (X, Y) do conjunto dos vértices de G designa-se por bipartição dos vértices e, neste caso, o grafo G denota-se pelo terno (X, Y, E) , onde $E = E(G)$.*

Um grafo bipartido $G = (X, Y, E)$, tal que $\forall_{x \in X} \forall_{y \in Y} xy \in E(G)$, designa-se por *grafo bipartido completo*. Se $|X| = m$ e $|Y| = n$, então existe um único (a menos de um isomorfismo) grafo bipartido completo com esta bipartição, o qual se denota por $K_{m,n}$.

Analogamente se define *grafo k-partido* e *grafo k-partido completo*.

Embora a conexidade seja estudada com detalhe no Capítulo 13, antes de introduzirmos uma condição necessária e suficiente para um grafo ser bipartido, convém antecipar este conceito referindo, informalmente, que um grafo *conexo* é um grafo onde existe um caminho entre quaisquer dois vértices. Por sua vez, um subgrafo induzido maximal (no sentido da inclusão de vértices) conexo designa-se por *componente conexa*.

Teorema 12.4. *Um grafo G é bipartido se e só se não tem circuitos de comprimento ímpar.*

Demonstração. Se G é um grafo bipartido, com bipartição de vértices (X, Y) , então é claro que todos os circuitos têm comprimento par. Com efeito, uma vez que tanto em X como em Y não existem vértices adjacentes, partindo-se, por exemplo, de um vértice em X , de cada vez que se passa para Y , para se obter um circuito, tem de se voltar a X na aresta seguinte, consequentemente, qualquer circuito tem comprimento par. Para provarmos o recíproco, uma vez que um grafo é bipartido se e só se cada uma das suas componentes conexas é um subgrafo bipartido, podemos supor, sem perda de generalidade, que G é conexo. Adicionalmente, suponha que G não tem circuitos de comprimento ímpar, considere-se um vértice arbitrário $z \in V(G)$ e seja $X = \{x \in V(G) : d_G(z, x) \text{ é ímpar}\}$. Nestas condições, não existem arestas que liguem vértices de X (caso contrário existiriam circuitos de comprimento ímpar). Por outro lado, como todos os vértices de $V(G) \setminus X$ estão a uma distância par de z (em particular z está à distância 0 dele próprio), não existem vértices adjacentes em $V(G) \setminus X$ (uma vez que, por razões idênticas às anteriores, em tais condições, existiriam circuitos de comprimento ímpar). Logo, fazendo $Y = V(G) \setminus X$, obtém-se a bipartição dos vértices (X, Y, E) . \square

12.6. Exemplos de enumeração de grafos simples

Seguem-se alguns casos particulares de enumeração de grafos simples com certas propriedades.

Exemplo 12.6. Considerando o conjunto de grafos simples \mathcal{G} tais que $\forall_{G \in \mathcal{G}} V(G) = \{1, \dots, \nu\}$, vamos

- (a) provar a validade da desigualdade $\varepsilon(G) \leq \binom{\nu}{2}$;
- (b) calcular o número de grafos G com ε arestas;
- (c) calcular a cardinalidade de \mathcal{G} .

Solução.

- (a) Cada grafo simples com ν vértices é um subgrafo de um grafo completo K_ν e, como consequência, $E(G) \subseteq E(K_\nu)$. Por outro lado, o número de arestas do grafo K_ν é igual ao número de subconjuntos de vértices de cardinalidade 2, isto é, $\binom{\nu}{2}$. Logo,

$$\varepsilon(G) = |E(G)| \leq |E(K_\nu)| = \binom{\nu}{2}.$$

- (b) Cada um dos grafos simples com ν vértices e ε arestas, pode ser considerado como um subgrafo abrangente de K_ν e, consequentemente, unicamente determinado por um subconjunto de $E(K_\nu)$ de cardinalidade ε . Dado que, tal como se concluiu em (a), $|E(K_\nu)| = \binom{\nu}{2}$, podemos concluir que o número de grafos simples com ν vértices e ε arestas é igual a

$$\binom{\binom{\nu}{2}}{\varepsilon}.$$

- (c) Tal como em (b), podemos considerar que cada grafo simples com ν vértices corresponde a um subgrafo abrangente de K_ν . Logo, o número de grafos simples com ν vértices é igual ao número de subconjuntos de $E(K_\nu)$, isto é,

$$2^{\binom{\nu}{2}}.$$

Podemos chegar a esta mesma conclusão, recorrendo ao resultado obtido no item (b) e adicionando as cardinalidades dos conjuntos de grafos com ε arestas, para $\varepsilon = 0, 1, \dots, \binom{\nu}{2}$, ou seja,

$$\sum_{\varepsilon=0}^{\binom{\nu}{2}} \binom{\binom{\nu}{2}}{\varepsilon} = 2^{\binom{\nu}{2}}.$$

□

Exemplo 12.7. Vamos representar graficamente todos os grafos simples não isomorfos, com 5 vértices e 5 arestas.

Solução. A Figura 12.10 apresenta a solução obtida por análise exaustiva de todas as possibilidades.

□

Exemplo 12.8. Vamos calcular o número de vértices e o número de arestas do grafo bipartido completo $K_{n,m}$.

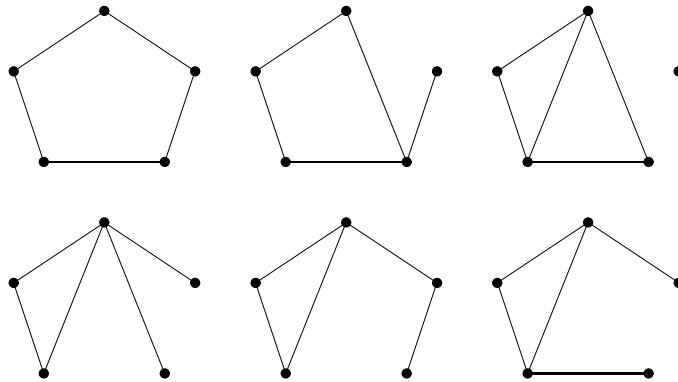


Figura 12.10: Representação de todos os grafos simples, não isomorfos, de ordem e dimensão 5.

Solução. No grafo $K_{n,m}$, existem n e m vértices, respectivamente, em cada subconjunto da bipartição. Logo, vem que

$$\nu(K_{n,m}) = n + m.$$

Uma vez que entre cada par de vértices (x, y) , tais que $x \in X$ e $y \in Y$, existe uma única aresta, podemos concluir que o número de arestas de $K_{n,m}$ é igual ao número destes pares (que corresponde à cardinalidade do produto cartesiano $X \times Y$), isto é,

$$\varepsilon(K_{n,m}) = nm.$$

□

Definição 12.21 (k -cubo). Designa-se por k -cubo e denota-se por Q_k , um grafo cujos vértices são etiquetados por k -uplos binários e onde dois vértices são adjacentes se e só se as etiquetas que lhes correspondem diferem num único dígito.

Na Figura 12.11 representam-se os k -cubos, com $k = 0, 1, 2, 3$.

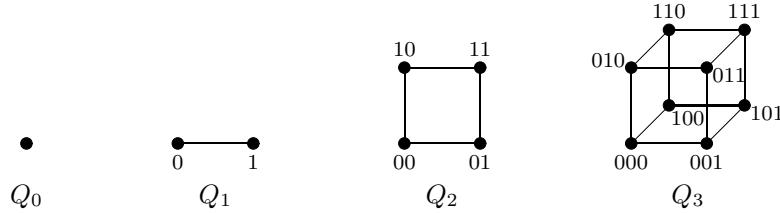


Figura 12.11: Representação dos k -cubos, com $k = 0, \dots, 3$.

Exemplo 12.9. Vamos demonstrar que os k -cubos, com $k \geq 1$, são grafos bipartidos.

Solução. Denotando por X o conjunto dos vértices do k -cubo, Q_k , com etiquetas cujo número de uns é par e por Y o conjunto dos vértices etiquetados com um número ímpar de uns, vem que X e Y constituem uma partição do conjunto dos vértices de Q_k . Como consequência, verifica-se que as etiquetas de dois vértices de X (e também de Y) diferem num número par de uns, isto é, ou têm o mesmo número de uns ou diferem em pelo menos dois uns. Em qualquer dos casos, dois vértices pertencentes ao mesmo conjunto não podem ter apenas um dígito distinto. Logo, por definição de k -cubo, quaisquer dois vértices em X (e em Y) são não adjacentes, pelo que Q_k é um grafo bipartido, com a bipartição (X, Y) . □

Exemplo 12.10. Vamos demonstrar que o k -cubo é um grafo k -regular e vamos determinar a sua ordem e dimensão.

Solução. Uma vez que num k -cubo dois vértices são adjacentes se as correspondentes etiquetas diferem num único dígito binário, se $v \in V(Q_k)$, então existem k sequências binárias que diferem da etiqueta de v num único bit. Tal significa que existem exactamente k vértices adjacentes a v e, como consequência, $d(v) = k$. Logo, o k -cubo é k -regular.

Dado que existem 2^k sequências binárias de comprimento k , por um lado,

$$\nu(Q_k) = 2^k$$

e, por outro lado, tendo em conta que (de acordo com o Teorema 12.1) $k\nu(Q_k) = 2\varepsilon(Q_k)$, vem

$$\varepsilon(Q_k) = k2^{k-1}.$$

□

12.7. Sequências de graus de vértices

Os graus dos vértices de um grafo fornecem informação que pode ser muito útil na resolução de problemas modelados por grafos, conforme o exemplo a seguir ilustra.

Exemplo 12.11. Assumindo que a relação de conhecimento é simétrica (ou seja, assumindo que uma pessoa conhece outra se essa outra pessoa também a conhece), vamos mostrar que num conjunto de quaisquer seis pessoas existem três pessoas que ou se conhecem todasumas às outras ou não se conhecem mutuamente.

Solução. Este problema pode ser formulado, na linguagem dos grafos, conforme se indica:

| Dado um grafo simples G , com 6 vértices, podemos afirmar que G contém um triângulo (grafo completo K_3) ou o seu complementar G^c contém um triângulo.

Com efeito, seja G um grafo simples de ordem 6 e considere-se o vértice $v \in V(G)$. Nestas condições, sabe-se que

$$d_G(v) + d_{G^c}(v) = 5.$$

Como consequência, um dos graus de v (em G ou em G^c) é não inferior a 3. Sem perda de generalidade, suponha que

$$d_G(v) \geq 3.$$

Tal significa que existem pelo menos três vértices $v_1, v_2, v_3 \in V(G)$ adjacentes a v em G . Se existe uma aresta entre qualquer par de vértices de $\{v_1, v_2, v_3\}$, então existe um triângulo em G . Caso contrário, existe o triângulo formado pelos vértices v_1, v_2, v_3 no grafo G^c .

□

Nem toda a sequência de inteiros não negativos corresponde a uma sequência de graus de um grafo. Com efeito, arbitrada uma sequência de inteiros não negativos, nem sempre existe um grafo cujos vértices admitam, precisamente, essa sequência de graus.

Definição 12.22 (Sequência gráfica). Designa-se por sequência gráfica (ou sequência dos graus dos vértices de um grafo), toda a sequência de inteiros não negativos para a qual existe um grafo simples cujos vértices admitem essa sequência como sequência dos seus graus.

Exemplo 12.12. Dada a sequência não crescente de inteiros não negativos $d = (d_1, d_2, \dots, d_n)$, seja

$$d' = (d_2 - 1, d_3 - 1, \dots, d_{d_1+1} - 1, d_{d_1+2}, \dots, d_n).$$

(a) Vamos demonstrar que d é uma sequência gráfica se e só se d' é uma sequência gráfica.

- (b) Com recurso a (a), vamos descrever um algoritmo que admita como dados de entrada uma sequência d de inteiros não negativos e (caso exista) produza um grafo simples G cuja sequência dos graus dos vértices é d .
- (c) Com recurso a (a) e (b), vamos determinar um grafo simples que admite como sequência dos graus dos vértices a sequência $(6, 5, 5, 4, 4, 3, 2, 2, 1)$.

Solução.

- (a) Suponha que d é uma sequência gráfica. Logo, existe um grafo simples G que admite d como sequência dos graus dos vértices. Sejam $V(G) = \{v_1, v_2, \dots, v_n\}$ e $d_G(v_i) = d_i$, para $i = 1, \dots, n$. Se o vértice v_1 é adjacente aos vértices v_2, \dots, v_{d_1+1} , então o grafo $G - v_1$ admite d' como sequência dos graus dos vértices, pelo que d' é uma sequência gráfica. Caso contrário, existe um vértice v_i , com $2 \leq i \leq d_1 + 1$, tal que v_1 não é adjacente a v_i e, consequentemente, uma vez que $d_G(v_1) = d_1$, existe v_j adjacente a v_1 , com $j > d_1 + 1$. Logo, dado que d é não crescente e $i < j$, podemos concluir que

$$d_G(v_i) = d_i \geq d_j = d_G(v_j).$$

Assim, existem duas possibilidades:

$d_i = d_j$: Neste caso, trocando os índices dos vértices v_i e v_j entre si, a sequência dos graus mantém-se, mas v_1 passa a ser adjacente a v_i .

$d_i > d_j$: Neste caso, existe um vértice v_k adjacente a v_i e não adjacente a v_j . Seja G^* o grafo obtido a partir do grafo G , fazendo as seguintes transformações: eliminam-se as arestas v_1v_j e v_iv_k e adicionam-se as arestas v_1v_i e v_kv_j (as quais não alteram os graus dos vértices). Desta forma, a sequência de graus mantém-se e os vértices v_1 e v_i passam a ser adjacentes em G^* .

Este procedimento pode ser repetido até que se obtenha um grafo em que v_1 é adjacente aos vértices v_2, \dots, v_{d_1+1} e, como consequência, prova-se que d' é uma sequência gráfica.

Reciprocamente, suponha que d' é uma sequência gráfica, pelo que existe um grafo simples G' que admite d' como sequência dos graus dos vértices. Adicionando a G' um novo vértice com d_1 arestas incidentes que o ligam aos d_1 vértices de G' , cujos graus correspondem aos primeiros termos da sequência d' , obtém-se um grafo G que admite d como sequência dos graus dos seus vértices.

- (b) Com recurso à técnica utilizada em (a), partir da sequência d vamos determinar d' , depois $(d')'$ etc., reordenando as sequências que se vão obtendo, transformando-as sempre em sequências não crescentes. Este procedimento termina quando nos defrontamos com uma sequência d^* numa das seguintes situações:

1. A sequência d^* é uma sequência binária (contendo apenas zeros e uns). Neste caso, a sequência é gráfica se e só se o número de uns é par.
2. Não podemos aplicar a técnica utilizada em (a) à sequência d^* (como por exemplo, nos casos $d^* = (5, 4, 0, 0, 0, 0, 0)$ ou $d^* = (5, 4, 3)$). Neste caso, podemos concluir que d não é uma sequência gráfica.

No caso 1, supondo que o número de uns é par, estamos em condições de construir um grafo que admite d como sequência de graus dos seus vértices, para tal vamos adoptar o seguinte procedimento: primeiramente construímos o grafo simples associado a d^* (que é constituído por vértices e arestas isoladas) e, a partir dele, com recurso ao inverso da técnica adoptada em (a), obtém-se sucessivamente novos grafos até se chegar ao grafo associado a d . Mais formalmente, o Algoritmo 12.1 TESTEDESEQUÊNCIAGRÁFICA, cujo pseudo código se apresenta a seguir, verifica se uma sequência d de inteiros não negativos é (ou não) uma sequência gráfica.

Algoritmo 12.1: TESTEDESEQUÊNCIAGRÁFICA(d, n)

```

repetir
  Ordenar( $d[1 \dots n]$ )
  se  $d[1] = 0$  então devolver ( verdadeiro )
   $NúmeroDeTermosPositivos \leftarrow n$ 
  enquanto  $d[NúmeroDeTermosPositivos] > 0$ 
    fazer  $NúmeroDeTermosPositivos \leftarrow NúmeroDeTermosPositivos - 1$ 
    se  $d[1] = 1$  então devolver ( $NúmeroDeTermosPositivos \bmod 2 = 0$ )
    se  $NúmeroDeTermosPositivos < d[1] + 1$  então devolver ( falso )
    para  $i \leftarrow 2$  até  $d[1] + 1$ 
      fazer  $d[i] \leftarrow d[i] - 1$ 
     $n \leftarrow n - 1$ 
    para  $i \leftarrow 1$  até  $n$ 
      fazer  $d[i] \leftarrow d[i + 1]$ 
    Ordenar( $d[1 \dots NúmeroDeTermosPositivos]$ )
  até falso

```

- (c) Vamos começar por verificar se a sequência $d = (6, 5, 5, 4, 4, 3, 2, 2, 1)$ é uma sequência gráfica, ou seja, se existe um grafo G , com $V(G) = \{v_1, v_2, \dots, v_9\}$, tal que $d_G(v_1) = 6$, $d_G(v_2) = 5$, $d_G(v_3) = 5$, $d_G(v_4) = 4$, $d_G(v_5) = 4$, $d_G(v_6) = 3$, $d_G(v_7) = 2$, $d_G(v_8) = 2$ e $d_G(v_9) = 1$. De acordo o procedimento proposto em (b), obtém-se os seguintes passos:

1. Determina-se a sequência que decorre da eliminação do primeiro termo de d e da subtração de uma unidade aos d_1 primeiros termos, ou seja,

$$(4, 4, 3, 3, 2, 1, 2, 1);$$

2. Determina-se d' , ordenando os termos da sequência obtida em 1, pelo que

$$d' = (4, 4, 3, 3, 2, 2, 1, 1).$$

Note-se que neste caso, os graus da sequência d' correspondem à sequência de vértices $(v_2, v_3, v_4, v_5, v_6, v_8, v_7, v_9)$.

3. Determina-se d'' por aplicação a d' dos passos 1 e 2, pelo que

$$d'' = (3, 2, 2, 2, 1, 1, 1).$$

Neste caso, os graus da sequência d'' correspondem à sequência de vértices $(v_3, v_4, v_5, v_8, v_6, v_7, v_9)$.

4. Determina-se d''' a partir de d'' segundo procedimento análogo aos anteriores, pelo que

$$d''' = (1, 1, 1, 1, 1, 1).$$

Neste caso, d''' é uma sequência binária que corresponde à sequência de vértices $(v_4, v_5, v_8, v_6, v_7, v_9)$.

Fazendo agora o percurso inverso, começando por determinar G''' a partir de d''' , G'' a partir de G''' e d'' , G' a partir de G'' e d' , etc, obtém-se:

- a) G''' é tal que $V(G''') = \{v_4, v_5, v_8, v_6, v_7, v_9\}$ e $E(G''') = \{v_4v_5, v_8v_6, v_7v_9\}$ (ver Figura 12.12-(a));
- b) G'' é tal que $V(G'') = V(G''') \cup \{v_3\}$ e $E(G'') = E(G''') \cup \{v_3v_4, v_3v_5, v_3v_8\}$ (ver Figura 12.12-(b));
- c) G' é tal que $V(G') = V(G'') \cup \{v_2\}$ e $E(G') = E(G'') \cup \{v_2v_3, v_2v_4, v_2v_5, v_2v_6\}$ (ver Figura 12.12-(c));
- d) G é tal que $V(G) = V(G') \cup \{v_1\}$ e $E(G) = E(G') \cup \{v_1v_2, v_1v_3, v_1v_4, v_1v_5, v_1v_6, v_1v_7\}$ (ver Figura 12.12-(d)). \square

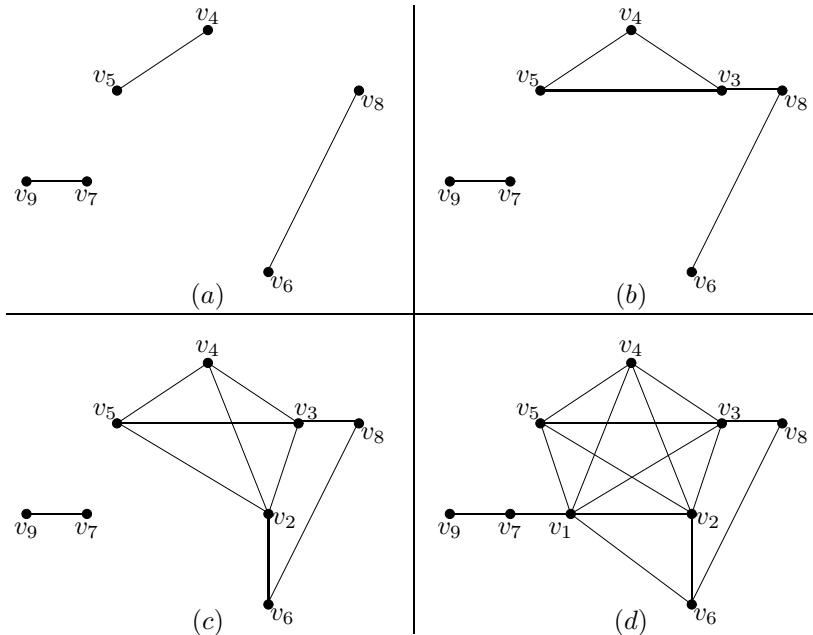


Figura 12.12: Construção de um grafo que admite a sequência de graus $(6, 5, 5, 4, 4, 3, 2, 2, 1)$ (ver Exemplo 12.12).

Exemplo 12.13. Vamos demonstrar que se a sequência $d_1 \geq d_2 \geq \dots \geq d_n$ é uma sequência gráfica então

$$(1) \sum_{i=1}^n d_i \text{ é par;}$$

$$(2) \sum_{i=1}^k d_i \leq k(k-1) + \sum_{j=k+1}^n \min(k, d_j), \quad \text{para } 1 \leq k \leq n.$$

(Erdős e Gallai demonstraram um resultado mais geral onde estas condições não só são necessárias como também são suficientes.)

Solução. A prova de (1) é imediata, tendo em conta que a soma dos graus dos vértices de qualquer grafo é par (ver Teorema 12.1). Tendo em vista demonstrar (2), seja $d = (d_1, d_2, \dots, d_n)$ uma sequência gráfica não crescente, k um inteiro tal que $1 \leq k \leq n$, v_i o vértice associado ao termo d_i e $V_{(k)} = \{v_1, v_2, \dots, v_k\}$. Antes de prosseguirmos, convém observar que $\sum_{i=1}^k d_i$ é igual ao número de arestas

incidentes num vértice de $V_{(k)}$, contando duas vezes as arestas com ambos os extremos em $V_{(k)}$. Partindo o conjunto de todas as arestas incidentes em pelo menos um vértice de $V_{(k)}$ nos subconjuntos:

E_1 – conjunto das arestas com exactamente um dos suas extremos em $V_{(k)}$,

E_2 – conjunto das arestas com ambos os extremos em $V_{(k)}$,

vem

$$\sum_{i=1}^k d_i = |E_1| + 2|E_2|,$$

onde $|E_2|$ é não superior ao número de arestas do grafo completo com k vértices, isto é,

$$|E_2| \leq \binom{k}{2} = \frac{k(k-1)}{2}.$$

Por outro lado, cada aresta do conjunto E_1 tem um extremo em $V_{(k)}$ e outro em $V \setminus V_{(k)}$. Assim, se $v_j \in V \setminus V_{(k)}$ (isto é, $k+1 \leq j \leq n$), então o número de arestas de E_1 incidentes em v_j é não superior nem $d(v_j) = d_j$, nem a $|V_{(k)}|$. Como consequência,

$$|E_1| \leq \sum_{j=k+1}^n \min(k, d_j)$$

e, finalmente,

$$\sum_{i=1}^k d_i = |E_1| + 2|E_2| \leq \sum_{j=k+1}^n \min(k, d_j) + k(k-1).$$

□

12.8. Algoritmos de pesquisa em grafos

Existem dois métodos, muito utilizados e que se descrevem a seguir, de pesquisar um grafo, percorrendo todos os seus vértices e arestas, passando sucessivamente de um vértice para o seu adjacente (sempre que possível).

- i. A *pesquisa em profundidade* ou *depth-first search* (na terminologia inglesa) ou ainda DFS (que corresponde às respectivas iniciais) que foi introduzida por Hopcroft e Tarjan, consiste em escolher um vértice inicial (centro de busca) v e, a partir dele, procurar um novo centro de busca w que lhe é adjacente e ainda não foi centro de busca. Caso não exista um vértice com estas propriedades, recua-se para o centro de busca imediatamente anterior (caso exista), repetindo-se o mesmo processo, ou escolhe-se um qualquer outro vértice que não foi centro de busca. Este procedimento termina quando não existem vértices que não foram centros de busca.
- ii. A *pesquisa em largura* ou *breadth-first search* (na terminologia inglesa) ou ainda BFS (que corresponde às respectivas iniciais), consiste em analisar todas as arestas incidentes num vértice inicial v , designado por centro de busca e, a partir dele, escolher, sucessivamente, um novo centro de busca w ainda não utilizado como tal, se possível adjacente a um dos centros de busca anteriores. Este procedimento é repetido até se esgotarem todos os vértices que não foram centros de busca.

Como exemplo de aplicação destes métodos de pesquisa, vamos utilizar cada um deles na enumeração dos vértices de um grafo G (com indicação da ordem de cada um na contagem realizada) e na partição de $E(G)$ no subconjunto de arestas percorridas e subconjunto das restantes, os quais designamos, respectivamente, por *Árvore* e *Restantes* (no Capítulo 15, mais adiante, estudaremos o conceito de árvore abrangente que motiva a designação adoptada para o primeiro conjunto).

Com o algoritmo de pesquisa em profundidade, na primeira visita ao vértice v , marca-se v com o número $Número[v]$, onde $Número[v] = i$ significa que o vértice v foi o i -ésimo vértice visitado. Segue-se uma descrição mais detalhada da aplicação do método DFS.

Algoritmo de pesquisa em profundidade – DFS.

Dados de entrada: Grafo G não orientado definido pela sua lista de arestas e centro de busca inicial $x \in V(G)$.

Resultados da saída: Tabela *Ordena* que descreve a ordem seguda a qual cada vértice de G foi visitado e partição de $E(G)$ nos subconjuntos *Árvore* e *Restantes*.

1. Fazer $v \leftarrow x$, $i \leftarrow 0$, $\text{Árvore} \leftarrow \emptyset$, $\text{Restantes} \leftarrow \emptyset$;
 2. Fazer $i \leftarrow i + 1$, $\text{Ordena}[v] \leftarrow i$;
 3. Procurar uma aresta, ainda não percorrida, incidente em v ;
 - (a) Se uma tal aresta não existe, então passar para 5;
 - (b) Se uma tal aresta vw existe, então escolher vw ;
 4. Visitar o vértice w . Se w é visitado pela primeira vez,
 - (a) então juntar a aresta vw ao conjunto *Árvore*, fazer $v \leftarrow w$ e passar para 2;
 - (b) senão juntar a aresta vw ao conjunto *Restantes* e passar para 3;
 5. Verificar se existe uma aresta uv no conjunto *Árvore*, com $\text{Ordena}[u] < \text{Ordena}[v]$.
 Se uma tal aresta existe,
 - (a) então fazer $v \leftarrow u$ e passar para 3.
 - (b) senão PARAR.
-

Uma vez que este tipo de descrição de algoritmos se torna, por vezes, um pouco ambígua, vamos descrever o algoritmo DFS na sua versão recursiva, utilizando pseudocódigo (linguagem já anteriormente utilizada).

Algoritmo 12.2: DFS(G, x)

```

global Ordena, Árvore, Restantes
 $v \leftarrow x$ 
Ordena[ $v$ ]  $\leftarrow$  Visitados  $\leftarrow 1$ 
para todo  $w \in N_G(v)$ 
  fazer se Ordena[ $w$ ] = 0
    então  $\begin{cases} \text{Visitados} \leftarrow \text{Visitados} + 1 \\ \text{Ordena}[w] \leftarrow \text{Visitados} \\ \text{Árvore} \leftarrow \text{Árvore} \cup \{vw\} \\ \text{DFS}(G, w) \end{cases}$ 
    senão se Ordena[ $w$ ] < Ordena[ $v$ ]
      então Restantes  $\leftarrow$  Restantes  $\cup \{vw\}$ 
  devolver (Ordena, Árvore, Restantes)

```

Deve observar-se que, antes da execução propriamente dita do Algoritmo 12.2 DFS, é necessário iniciar (ou seja, concretizar) as variáveis, por exemplo, da seguinte forma:

```

para todo  $v \in V(G)$ 
  fazer Ordena[ $v$ ]  $\leftarrow 0$ 
  Árvore  $\leftarrow$  Restantes  $\leftarrow \emptyset$ 

```

Existem muitas aplicações deste algoritmo, algumas das quais vão ser apresentadas nos capítulos subsequentes. Um exemplo simples de aplicação do algoritmo DFS é o Algoritmo 12.3 ORDENAR-VÉRTICES que ordena todos os vértices de um grafo G .

Algoritmo 12.3: ORDENARVÉRTICES(G)

```

para todo  $v \in V$ 
  fazer  $Ordena[v] \leftarrow 0$ ;
   $\text{Árvore} \leftarrow \text{Restantes} \leftarrow \emptyset$ 
  para todo  $v \in V$ 
    fazer se  $Ordena[v] = 0$  então  $\text{DFS}(G, v)$ 
```

O Algoritmo 12.4 DFS1 é uma versão não recursiva do Algoritmo 12.2 DFS. Neste algoritmo, utiliza-se uma tabela *Pilha* que contém os vértices que se devem voltar a visitar. Por sua vez, $NPilha$ é o número de vértices da *Pilha*, I_v é a tabela de vértices adjacentes a v e NI_v é o número de vértices adjacentes a v . As implementações reais deste algoritmo, por questões de eficiência, recorrem à estrutura de dados *pilha* que, para tornar a exposição mais simples, é aqui simulada por uma *tabela*.

Algoritmo 12.4: DFS1(G, x)

```

global  $Ordena, \text{Árvore}, \text{Restantes}$ 
 $Ordena[x] \leftarrow \text{Visitados} \leftarrow 1$ 
 $NPilha \leftarrow 1; Pilha[NPilha] \leftarrow x$ 
enquanto  $NPilha > 0$ 
  fazer
    { senão
      {  $v \leftarrow Pilha[NPilha]$ 
        se  $NI_v = 0$ 
          então  $NPilha \leftarrow NPilha - 1$ 
            {  $w \leftarrow I_v[1]$ 
               $NI_v \leftarrow NI_v - 1$ 
              para  $i \leftarrow 1$  até  $NI_v$ 
                fazer  $I_v[i] \leftarrow I_v[i - 1]$ 
              se  $Ordena[w] = 0$ 
                então
                  {  $Visitados \leftarrow Visitados + 1$ 
                     $Ordena[w] \leftarrow Visitados$ 
                     $\text{Árvore} \leftarrow \text{Árvore} \cup \{vw\}$ 
                     $NPilha \leftarrow NPilha + 1$ 
                     $Pilha[NPilha] \leftarrow w$ 
                  senão  $Restantes \leftarrow Restantes \cup \{vw\}$ 
                }
      devolver ( $Ordena, \text{Árvore}, \text{Restantes}$ )
```

A complexidade computacional destes três algoritmos é da ordem de $O(\nu + \varepsilon)$, quando o grafo é representado por uma lista de arestas.

Tal como anteriormente, vamos determinar a ordem segunda qual cada um dos vértices de um grafo é visitado, bem como uma partição das arestas no subconjunto das arestas percorridas (*Árvore*) e restantes, mas desta vez utilizando a pesquisa em largura.

Algoritmo de pesquisa em largura - BFS

Dados de entrada: Grafo G não orientado definido pela sua lista de arestas e centro de busca inicial $x \in V(G)$.

Resultados da saída: Tabela *Ordena* que descreve a ordem segunda a qual cada vértice de G foi visitado e partição de $E(G)$ nos subconjuntos *Árvore* e *Restantes*.

1. Fazer $Ordena[x] \leftarrow 1$, $\text{Árvore} \leftarrow \emptyset$, $\text{Restantes} \leftarrow \emptyset$ e inserir x na $Fila$;
 2. Se $Fila$ é vazia, então PARAR;
 3. Retirar v da $Fila$;
 4. Para cada $w \in N_G(v)$ fazer:
 - (a) Se $Ordena[w] = 0$, então fazer $Ordena[w]$ igual ao número de vértices até agora visitados, inserir w na $Fila$ e juntar a aresta vw ao subconjunto Árvore ;
 - (b) Se $Ordena[w] \neq 0$, então se $vw \notin \text{Árvore}$ juntar vw ao subconjunto Restantes .
 5. Passar para 2.

O Algoritmo 12.5 BFS descreve, formalmente, todos estes passos em pseudocódigo onde, para simplificar, se simula a estrutura de dados *fila* por intermédio de uma *tabela*.

Nos algoritmos de pesquisa (DSF, DSF1 e BSF) apresentados, percorrem-se todos os vértices e todas as arestas do grafo, o que, em geral, não acontece nas aplicações reais, para muitas das quais basta analisar os vértices. Quando tal acontece, podemos omitir todas as passos relacionados com os conjuntos *Árvore* e *Restantes*. Nos capítulos que se seguem apresentaremos vários exemplos de aplicação destas diferentes estratégias de pesquisa em grafos.

Algoritmo 12.5: BFS(G, x)

```

global Ordena, Árvore, Restantes
Ordena[ $x$ ]  $\leftarrow$  Visitados  $\leftarrow$  1
NFila  $\leftarrow$  1; Fila[NFila]  $\leftarrow$   $x$ 
enquanto NFila  $>$  0
    fazer  $v \leftarrow$  Fila[1]; NFila  $\leftarrow$  NFila - 1
        para  $i \leftarrow 1$  até NFila
            fazer Fila[i]  $\leftarrow$  Fila[i + 1]
        para  $i \leftarrow 1$  até NIv
            fazer  $w \leftarrow I_v[i]$ 
            se Ordena[w] = 0
                então  $\begin{cases} \text{Visitados} \leftarrow \text{Visitados} + 1 \\ \text{Ordena}[w] \leftarrow \text{Visitados} \\ \text{Árvore} \leftarrow \text{Árvore} \cup \{vw\} \\ \text{NFila} \leftarrow \text{NFila} + 1 \\ \text{Fila}[NFila] \leftarrow w \end{cases}$ 
            senão  $\text{Restantes} \leftarrow \text{Restantes} \cup \{vw\}$ 
    devolver (Ordena, Árvore, Restantes)

```

12.9. Exercícios

- 12.1. Represente graficamente exemplos de grafos G_1 , G_2 , G_3 e G_4 , cada um dos quais com 5 vértices e 8 arestas, tais que G_1 é um grafo simples, G_2 não é simples e não contém lacetes, G_3 não é simples e não contém arestas paralelas, G_4 não é simples, contém lacetes e arestas paralelas.
 - 12.2. Demonstre que em qualquer grafo o número de vértices de grau ímpar é par.
 - 12.3. Caso exista, determine o número de arestas e represente graficamente um exemplo de cada um dos seguintes grafos:

- (a) Grafo cúbico (3-regular) com $\nu(G) = 9$;
 (b) Grafo com $\nu(G) = 10$, tal que dois vértices têm grau 4 e os restantes grau 3.

12.4. Qual o número de arestas de um grafo simples G , sabendo que $\nu(G) = 56$ e $\varepsilon(G^c) = 80$?

12.5. Demonstre que se um grafo G é k -regular, então $\varepsilon(G) = \frac{1}{2}k\nu(G)$.

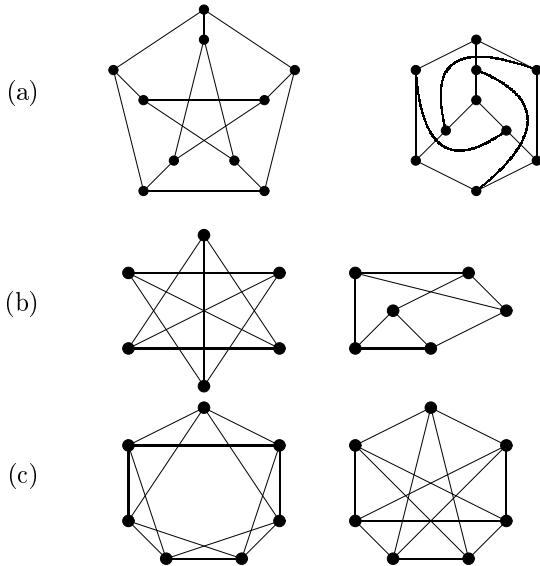
12.6. Demonstre que se um grafo bipartido G com pelo menos uma aresta, com bipartição dos vértices (X, Y) , é regular, então $|X| = |Y|$.

12.7. Sendo G um grafo simples, demonstre que se $\varepsilon(G) > \binom{\nu-1}{2}$, então G não tem vértices isolados.

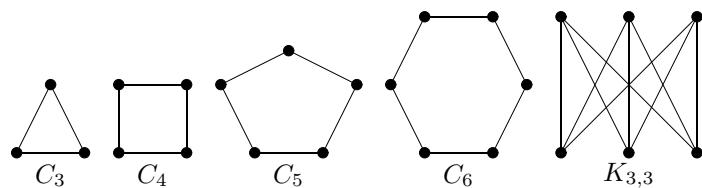
12.8. Sendo $M_G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 0 & 1 \end{pmatrix}$, represente graficamente G .

12.9. Demonstre que em qualquer grafo simples G não trivial existem dois vértices com o mesmo grau.

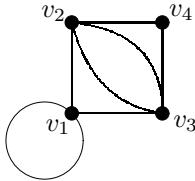
12.10. Verifique qual ou quais dos pares de grafos a seguir representados são isomorfos.



12.11. Denotando por C_3, C_4, C_5 e C_6 os ciclos de comprimento $3, \dots, 6$, respectivamente, indique os que são subgrafos de $K_{3,3}$ (ver figura a seguir).

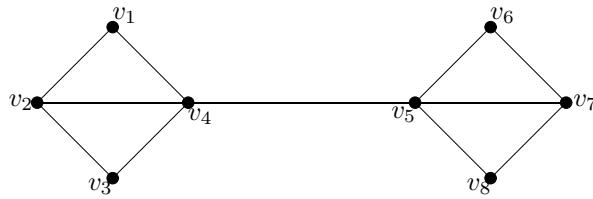


12.12. No grafo representado na figura a seguir, procure:



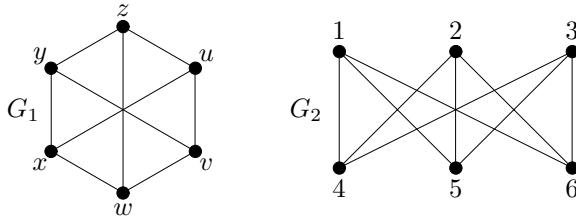
- (a) um passeio entre v_1 e v_4 , com comprimento 7;
 (b) todos os caminhos de comprimento 1, 2, 3 e 4;
 (c) um caminho de maior comprimento.

12.13. Considerando o grafo a seguir representado, determine todos os (v_1, v_8) -caminhos.



12.14. Considere os grafos representados na figura a seguir.

- (a) Mostre que G_1 e G_2 são isomorfos.
 (b) Quantos isomorfismos distintos existem entre G_1 e G_2 ?



- 12.15. (a) Quantos caminhos de comprimento 5 existem no grafo $K_{3,7}$?
 (b) Quantos caminhos de comprimento 4 existem no mesmo grafo?
 (c) Dados $m, n, p \in \mathbb{N}$, com $2m < n$ e $1 \leq p \leq 2m$, quantos caminhos de comprimento p existem em $K_{m,n}$?

12.16. Desenhe todos os grafos simples, com conjunto de vértices V , tais que

- (a) $V = \{1\}$,
 (b) $V = \{1, 2\}$,
 (c) $V = \{1, 2, 3\}$,
 (d) $V = \{1, 2, 3, 4\}$.

12.17. Seja G um grafo simples cujos vértices correspondem às permutações do conjunto $[n]$ (onde $n \in \mathbb{N}$ é fixo). Neste grafo, dois vértices são adjacentes se e só se as correspondentes permutações se podem transformar uma na outra com recurso a uma única transposição.

- (a) Determine a ordem e dimensão de G .
 (b) Verifique se G é regular.
 (c) Verifique se G é bipartido.

- 12.18. *Problema do lobo, da ovelha e da couve.* Um lobo, uma ovelha e uma couve estão na mesma margem de um rio, juntamente com um barqueiro que os pretende transferir para a outra margem. Porém, como o barco (além do barqueiro) só pode transportar um de cada vez, sabendo que o lobo gosta de comer ovelhas e que as ovelhas gostam de comer couves, o transporte tem de ser feito de modo que na mesma margem não fiquem a ovelha e o lobo ou a ovelha e a couve, em ambos os casos, sem a presença do barqueiro. O problema consiste em propor ao barqueiro um plano eficiente para transportar o lobo, a ovelha e a couve sãos e salvos para a outra margem. Com este objectivo, desenhe um grafo cujos vértices correspondem a situações admissíveis (por exemplo, a ovelha numa margem e o lobo e a couve na outra) e no qual dois vértices são adjacentes se e só se as respectivas situações se podem transformar uma na outra com uma viagem entre margens. De que modo pode utilizar este grafo para resolver o problema?
- 12.19. Seja G um grafo simples cujos vértices correspondem aos quadrados de um tabuleiro de xadrez de dimensão $n \times n$ (onde $n \geq 3$ é um número natural fixo). Neste grafo, dois vértices são adjacentes se e só se é possível executar um movimento de cavalo entre os correspondentes quadrados.
- Desenhe o grafo G , para $n = 3, 4, 5$.
 - Verifique se G é regular, para $n = 3, 4, 5$.
 - Verifique se G é bipartido, para $n = 3, 4, 5$.
 - Verifique se é possível percorrer todos os quadrados do tabuleiro (passando uma única vez por cada um) com movimentos de cavalo, para $n = 3, 4, 5$.
- 12.20. Seja G um grafo simples cujos vértices correspondem aos subconjuntos de $[n]$ (onde $n > 1$ é um número natural) de cardinalidade 2. Neste grafo, dois vértices são adjacentes se e só se os correspondentes subconjuntos têm intersecção vazia.
- Determine a ordem de G .
 - Verifique que G é regular e determine a sua dimensão.
 - Verifique se G é bipartido.
 - Desenhe o grafo G , para $n = 5$ (note que este grafo é conhecido por grafo de Petersen).
- 12.21. Considere um grafo simples cujos vértices correspondem aos subconjuntos de $[n]$ de cardinalidade k (onde $k, n \in \mathbb{N}$ são fixos), relativamente ao qual dois vértices são adjacentes se e só se os correspondentes subconjuntos têm intersecção vazia. Os grafos deste tipo designam-se por grafos de Kneser e denotam-se por KG_{nk} .
- Determine a ordem, dimensão e graus dos vértices de KG_{nk} .
 - Verifique se KG_{nk} é regular.
 - Verifique se KG_{nk} é bipartido.
 - Desenhe os grafos $KG_{n,n}$, $KG_{n,n-1}$, $KG_{n,1}$ e $KG_{5,k}$, para $k = 1, 2, 3, 4, 5$.
- 12.22. Seja G um grafo simples cujos vértices correspondem às palavras da língua portuguesa e no qual dois vértices são adjacentes se e só se as correspondentes palavras diferem em exactamente uma letra (como é o caso, por exemplo, das palavras "bolo" e "bola"). Determine um subgrafo induzido de G isomorfo ao grafo
- completo K_3 ;
 - completo K_4 ;
 - determinado por um ciclo de comprimento superior a três.

- 12.23. Demonstre, utilizando o princípio de gaiola dos pombos, que qualquer grafo não trivial simples contém dois vértices com o mesmo grau.
- 12.24. Desenhe todos os grafos simples, não-isomorfos, com conjunto de vértices V , tais que
- $V = \{1\}$,
 - $V = \{1, 2\}$,
 - $V = \{1, 2, 3\}$,
 - $V = \{1, 2, 3, 4\}$.
- 12.25. Determine o número de grafos com conjunto dos vértices $V = [\nu]$, com $\nu \in \mathbb{N}$, que têm ε arestas, com $\varepsilon \in \mathbb{N}_0$, nos casos em que
- não existem arestas paralelas (sendo permitidos lacetes);
 - não existem lacetes (sendo permitidas arestas paralelas).
- 12.26. Seja G um grafo simples de ordem ν , com grau médio $\bar{d} > 0$.
- Mostre que existem dois vértices $x, y \in V(G)$ tais que $xy \in E(G)$ e $\frac{1}{2}(d(x) + d(y)) \geq \bar{d}$.
 - Existem dois vértices não adjacentes x e y com a propriedade indicada na alínea anterior?
 - Existe uma aresta xy tal que $\frac{1}{2}(d(x) + d(y)) \leq \bar{d}$?
 - Existem dois vértices não adjacentes x e y tais que $\frac{1}{2}(d(x) + d(y)) \leq \bar{d}$?
- 12.27. Seja G um grafo de ordem ν e $\varepsilon(G) = \varepsilon$ que não contém um subgrafo isomorfo $K_{2,m}$.
- Prove a desigualdade $\sum_{x \in V} \binom{d(x)}{2} \leq (m-1)\binom{\nu}{2}$.
 - A partir da desigualdade obtida na alínea anterior, deduza a desigualdade $\varepsilon \leq \frac{\sqrt{m-1}}{2}\nu^{3/2} + \frac{\nu}{4}$.
 - Dado um conjunto de n pontos do plano, prove que o número de pares de pontos a uma distância unitária é não superior a $\frac{n^{3/2}}{\sqrt{2}} + \frac{n}{4}$.
 - Seja A um conjunto de pontos no plano e $f(A)$ o número de pares de pontos de A a uma distância unitária. Definindo-se a função $g(n) = \max\{f(A) : |A| = n\}$, a desigualdade obtida em (c) determina um majorante para $g(n)$. Sugira um limite inferior para $g(n)$?
- 12.28. Dezoito estações de telefones celulares são colocadas numa área citadina com raio de 6 Km. Sabendo que estas estações podem transmitir entre si quando a distância não é superior a 6 Km, prove que, independentemente da sua localização na cidade, pelo menos duas estações poderão transmitir para pelo menos cinco outras estações.
- 12.29. Mostre que existe um número finito de grafos simples regulares com a seguinte propriedade: cada par de vértices adjacentes têm exactamente um vizinho comum e cada par de vértices não-adjacentes têm exactamente dois vizinhos comuns. Adicionalmente, determine os graus possíveis para estes grafos e respectivas e ordens.
- 12.30. Sendo G um grafo simples de ordem $\nu = \nu(G)$ cujo menor grau é $\delta = \delta(G)$ e o maior grau é $\Delta = \Delta(G)$, determine $\delta(G^c)$ e $\Delta(G^c)$, em função de ν , δ e Δ .
- 12.31. Demonstre que qualquer grafo com arestas múltiplos mas sem lacetes admite um subgrafo bipartido com pelo menos $\frac{\varepsilon(G)}{2}$ arestas.

12.32. Seja G um grafo de ordem ν e com 56 arestas. Determine o valor de ν , sabendo que $\varepsilon(G^c) = 80$.

12.33. Mostre que para qualquer grafo simples G se verificam as seguintes desigualdades:

$$\delta(G) \leq 2 \frac{\varepsilon(G)}{\nu(G)} \leq \Delta(G)$$

12.34. Verifique qual ou quais das sequências a seguir indicadas é uma sequência gráfica e, nos casos afirmativos, determine um grafo que admite a respectiva sequência como sequência de graus dos vértices:

- (a) $(7, 7, 5, 5, 3, 3, 1, 1)$;
- (b) $(7, 5, 5, 5, 3, 3, 2, 1, 1, 0)$;
- (c) $(4, 4, 4, 4, 4, 4, 4, 4)$;
- (d) $(5, 2, 1, 1)$.

12.35. Considere a sequência $(1, 1, 2, 3, 3, 5)$ e verifique a veracidade de cada uma das seguintes afirmações:

- (a) Trata-se da sequência dos graus dos vértices de um grafo simples G .
- (b) Trata-se da sequência dos graus dos vértices de um grafo (no qual, naturalmente, podem existir lacetes e arestas paralelas).
- (c) Trata-se da sequência dos graus dos vértices de um grafo sem lacetes (mas, eventualmente, com arestas paralelas).
- (d) Trata-se da sequência dos graus dos vértices de um grafo sem arestas paralelas (mas, eventualmente, com lacetes).

13

Conexidade

Um dos primeiros problemas que usualmente se colocam quando investigamos um grafo é o de saber se é conexo ou não e, quando não é conexo, quais são as componentes conexas que o constituem. Além do seu interesse intrínseco, a conexidade é parte importante de muitos outros problemas mais complexos. Por exemplo, verificar se um grafo é ou não representável no plano sem que existam arestas que se cruzem, é equivalente a verificar se cada uma das suas componentes conexas admite uma tal representação.

Embora, muitas vezes, por simples observação, se possa concluir se um grafo é ou não conexo, quando o grafo é definido, por exemplo, por uma lista de arestas ou pela matriz de adjacência, tal conclusão pode não ser evidente. Com base nas diferentes representações de grafos em computador, são necessários algoritmos eficientes que determinem se um grafo é conexo ou não.

13.1. Grafos Conexos

Segue-se a definição formal de grafo conexo.

Definição 13.1 (Grafo conexo). *Um grafo diz-se conexo se entre cada par de vértices existe um caminho que os une. Caso contrário o grafo diz-se desconexo (ou não conexo).*

Observe-se que um grafo com um único vértice v é conexo, uma vez que, neste caso, podemos considerar que existe um caminho de comprimento nulo entre v e v (isto é, existe um caminho- (v, v) sem arestas).

Definição 13.2 (Vértices conexos, componente conexa). *Dado um grafo G , dois vértices $u, v \in V(G)$ dizem-se conexos se existe em G um caminho- (u, v) . A relação de conexidade entre vértices é uma relação de equivalência sobre o conjunto dos vértices $V(G)$. Supondo que $V(G)$ se parte nas classes de equivalência V_1, V_2, \dots, V_k , designa-se por componente conexa (ou, simplesmente, componente) de G cada um dos subgrafos induzidos $G[V_1], G[V_2], \dots, G[V_k]$.*

Com base nesta definição, podemos concluir que dois vértices são conexos se e só se pertencem a uma mesma componente.

Ao longo deste texto, vamos denotar o número das componentes conexas de um grafo G por $cc(G)$ (ou, simplesmente, cc quando não existem dúvidas relativamente ao grafo). Note-se que se $cc(G) = 1$, então o grafo G é conexo e no caso contrário ($cc(G) > 1$) G não é conexo. De um modo equivalente, podemos definir componente conexa como sendo um subgrafo maximal conexo.

Exemplo 13.1. *Vamos demonstrar que um grafo não trivial G é conexo se e só se qualquer que seja a partição de $V(G)$ em dois subconjuntos não vazios V_1 e V_2 , existe uma aresta com um extremo em V_1 e outro em V_2 .*

Solução. Suponha que o grafo não trivial G é conexo e sejam V_1 e V_2 subconjuntos de uma bipartição de $V(G)$, tal que $V_1 \neq \emptyset \neq V_2$. Logo, existem dois vértices $u, v \in V(G)$, tais que $u \in V_1$ e $v \in V_2$ e, dado que G é conexo, existe um caminho- (u, v) , o qual podemos escrever na forma:

$$v_0e_1v_1e_2v_2e_3 \cdots e_{k-1}v_{k-1}e_kv_k, \quad \text{com } u = v_0 \text{ e } v = v_k.$$

Tendo em conta que $v_0 \in V_1$ e $v_k \in V_2$, podemos concluir que existe j , com $0 \leq j \leq k-1$, tal que $v_j \in V_1$ e $v_{j+1} \in V_2$. Como consequência, a aresta $e_{j+1} = v_jv_{j+1}$ tem um extremo em V_1 e outro em V_2 .

Reciprocamente, suponha que G é um grafo não trivial, onde para qualquer bipartição de $V(G)$ em subconjuntos não vazios V_1 e V_2 se verifica existir uma aresta com um extremo em V_1 e outro em V_2 . Sendo $u, v \in V(G)$ dois vértices arbitrários e fazendo $v_0 = u$, $V_1 = \{v_0\}$ e $V_2 = V \setminus \{v_0\}$, obtém-se a bipartição de $V(G)$, V_1 e V_2 e, tendo em conta a hipótese, existe $v_0v_1 \in E(G)$, com $v_1 \in V_2$. Se $v_1 = v$, então existe um caminho- (u, v) . Caso contrário, fazemos $V_1 = \{v_0, v_1\}$, $V_2 = V \setminus \{v_0, v_1\}$ e concluímos, novamente, existir uma aresta $v_1v_2 \in E(G)$ ou $v_0v_2 \in E(G)$ com $v_2 \in V_2$, pelo que existe um caminho- (v_0, v_2) . Se $v_2 = v$, então existe um caminho- (u, v) , caso contrário, este procedimento repete-se. Tendo em conta que o grafo G é finito, ao fim de um número finito de passos, k , obtém-se $v_k = v$, pelo que existe um caminho- (u, v) . \square

Exemplo 13.2. Vamos demonstrar que se G é um grafo simples, com $\nu = \nu(G)$ e $\varepsilon = \varepsilon(G)$, tal que $\varepsilon > \binom{\nu-1}{2}$, então G é conexo. Adicionalmente, sendo $\nu > 1$, vamos determinar um grafo simples não conexo tal que $\varepsilon = \binom{\nu-1}{2}$.

Solução. Vamos fazer esta prova por contraposição, admitindo que G é um grafo simples não conexo. Então, de acordo com o Exemplo 13.1, existe uma bipartição do conjunto dos vértices $V(G)$, nos subconjuntos não vazios V_1 e V_2 , tal que não existe nenhuma aresta com um extremo em V_1 e outro em V_2 . É claro que G é um subgrafo da união dos grafos completos no conjuntos dos vértices V_1 e V_2 . Se $|V_1| = k$, então vem que

$$\varepsilon(G) \leq \varepsilon(K_k \cup K_{\nu-k}) = \binom{k}{2} + \binom{\nu-k}{2} = k^2 - k\nu + \frac{1}{2}\nu^2 - \frac{1}{2}\nu.$$

É fácil verificar que o polinómio quadrático $f(k) = k^2 - k\nu + \frac{1}{2}\nu^2 - \frac{1}{2}\nu$ na variável k , com $1 \leq k \leq \nu-1$, atinge o seu máximo para $k = 1$ e $k = \nu-1$, com $f(\nu-1) = f(1) = 1 - \nu + \frac{1}{2}\nu^2 - \frac{1}{2}\nu = \binom{\nu-1}{2}$. Como consequência,

$$\varepsilon(G) \leq \binom{\nu-1}{2},$$

o que completa a prova.

Um exemplo de grafo simples desconexo, com $\nu > 1$ vértices e $\varepsilon = \binom{\nu-1}{2}$ arestas é a união de um grafo trivial (K_1) com um grafo completo $K_{\nu-1}$. \square

Teorema 13.1. Seja G um grafo simples de ordem ν . Se G tem $cc = cc(G)$ componentes conexas, então verificam-se as desigualdades

$$\nu - cc \leq \varepsilon \leq \binom{\nu - cc + 1}{2},$$

onde $\varepsilon = \varepsilon(G)$ denota o número de arestas.

Demonstração. Vamos provar a desigualdade $\nu - cc \leq \varepsilon$, por indução sobre o número das arestas ε , tendo em conta que para $\varepsilon = 0$, esta desigualdade se verifica (note-se que, neste caso, $cc = \nu$). Suponha $\varepsilon > 0$ e que a desigualdade $\nu - cc \leq \varepsilon(G')$ se verifica para todos os grafos G' com menos do

que ε arestas. Sendo G um grafo com $\varepsilon = \varepsilon(G)$ arestas e $e \in E(G)$, é claro que o grafo $G - e$ é tal que $\text{cc}(G - e) \in \{\text{cc}(G), \text{cc}(G) + 1\}$. Logo, $\text{cc}(G) \geq \text{cc}(G - e) - 1$ e, como consequência,

$$\nu - \text{cc}(G) \leq \nu - \text{cc}(G - e) + 1 \leq \varepsilon(G - e) + 1 = \varepsilon(G), \quad (13.1)$$

ou seja, $\nu - \text{cc} \leq \varepsilon$.

Segue-se a demonstração da desigualdade $\varepsilon \leq \binom{\nu - \text{cc} + 1}{2}$. Dado um grafo simples G com ν vértices e cc componentes conexas, seja G^* o grafo obtido a partir de G por adição de arestas de tal forma que cada componente de G^* é um subgrafo completo (é claro que $\varepsilon(G) \leq \varepsilon(G^*)$).

Sejam $G^*[V_1]$ e $G^*[V_2]$ duas componentes de G com n_1 e n_2 vértices, respectivamente. Por definição de G^* , $G^*[V_1] \cong K_{n_1}$ e $G^*[V_2] \cong K_{n_2}$ e, sem perda de generalidade, podemos assumir que $n_1 \geq n_2 > 1$. Passando um vértice de V_2 para V_1 , eliminando todas as arestas que o ligavam a vértices de V_2 e acrescentando as arestas necessárias para o ligar aos restantes vértices de V_1 , obtém-se um novo grafo G^* com o mesmo número de vértices e componentes, mas com maior número de arestas. Assim, a diferença entre o número de arestas depois e o número de arestas antes da passagem do vértice de V_2 para V_1 vem dada por

$$\begin{aligned} \binom{n_1 + 1}{2} + \binom{n_2 - 1}{2} - \left(\binom{n_1}{2} + \binom{n_2}{2} \right) \\ = \frac{1}{2} (n_1(n_1 + 1) - n_1(n_1 - 1) + (n_2 - 1)(n_2 - 2) - n_2(n_2 - 1)) \\ = \frac{1}{2} (2n_1 - 2n_2 + 2) = n_1 - n_2 + 1 > 0. \end{aligned}$$

Logo, podemos concluir que cada vez que procedemos a este tipo de modificação aumentamos o número de arestas e, consequentemente, atingimos o máximo valor quando reduzimos, desta forma, todas as componentes menos uma a subgrafos triviais, ou seja, com G^* constituído por uma componente isomorfa a $K_{\nu - \text{cc} + 1}$ e $\text{cc} - 1$ componentes triviais (designadas, usualmente, por *vértices isolados*). Nestas condições, obtém-se

$$\varepsilon(G) \leq \varepsilon(G^*) \leq \binom{\nu - \text{cc} + 1}{2}. \quad \square$$

Observe-se que o resultado demonstrado no Exemplo 13.2 decorre directamente deste teorema.

Exemplo 13.3. *Dado um grafo simples G , vamos demonstrar que se G é um grafo desconexo, então G^c é conexo. Adicionalmente, vamos provar que a implicação recíproca não é verdadeira.*

Solução.

- Suponha que o grafo simples G não é conexo, ou seja, G tem pelo menos duas componentes conexas e sejam u e v dois vértices arbitrários de G . Vamos demonstrar que existe um caminho- $-(u, v)$ em G^c . Com efeito, se u e v pertencem às duas componentes distintas de G , então $uv \in E(G^c)$. Caso contrário, se u e v pertencem a uma mesma componente de G , então existe um vértice w , pertencente a outra componente de G e $uw, vw \in E(G^c)$. Logo, uvw é um caminho- $-(u, v)$ em G^c .
- Considerando o ciclo com 5 vértices, C_5 , $C_5^c \cong C_5$ (i.e. C_5 é autocomplementar). Logo, a implicação recíproca é falsa. \square

Exemplo 13.4. *Vamos demonstrar que se G é um grafo simples conexo não trivial, onde todos os vértices têm grau par, então*

$$\forall_{v \in V(G)} \text{cc}(G - v) \leq \frac{1}{2} d_G(v).$$

Solução. Seja v um vértice do grafo simples G .

- Se $G - v$ é conexo, então, uma vez que $d_G(v) \geq 2$, vem

$$\text{cc}(G - v) = 1 \leq \frac{1}{2}d_G(v).$$

- Se $G - v$ não é conexo, então podemos concluir que cada componente em G está ligada a v por, pelo menos, duas arestas (caso contrário, existiria uma componente ligada a v por uma única aresta e , como consequência, em $G - v$ existiria um único vértice de grau ímpar numa componente de $G - v$, o que constitui uma contradição, tendo em conta o Teorema 12.1). Logo, o número de componentes de $G - v$ é não superior a $\frac{1}{2}d_G(v)$. \square

Definição 13.3 (Ponte). *Uma aresta e de um grafo G diz-se uma ponte ou uma aresta de corte se $\text{cc}(G - e) > \text{cc}(G)$. Por outras palavras, a aresta e é uma ponte de G se a eliminação de e aumenta o número de componentes de G .*

Na Figura 13.6 apresenta-se um grafo com uma ponte (assinalada por e).

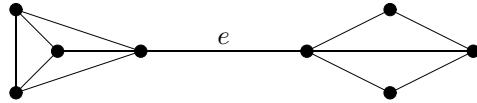


Figura 13.1: Exemplo de grafo com uma única ponte (a aresta e).

Teorema 13.2. *Se G é um grafo e $uv \in E(G)$, então as seguintes afirmações são equivalentes:*

- a aresta uv é uma ponte de G ,
- $\text{cc}(G - uv) = \text{cc}(G) + 1$,
- os vértices u e v não são conexos em $G - uv$,
- a aresta uv não está contida em nenhum circuito de G .

Demonstração.

(a) \Rightarrow (b) Como consequência directa da definição de ponte (Definição 13.3), vem que $\text{cc}(G - uv) \geq \text{cc}(G) + 1$. Seja $G[V_1]$ a componente em G que contém a aresta uv e seja $x \in V_1$. Como $G[V_1]$ é conexo, então existe um caminho- (x, u) em $G[V_1]$ (e em G). Se uv está contido neste caminho, então no grafo $G - uv$ existe caminho- (x, v) . Caso contrário, no grafo $G - uv$ existe um caminho- (x, u) . Logo, no grafo $G - uv$, para cada $x \in V_1$, os vértices x e u são conexos ou os vértices x e v são conexos, mas não ambos, uma vez que $\text{cc}(G - uv) > \text{cc}(G)$. Como consequência, o subgrafo de $G[V_1]$ em $G - uv$ parte-se em duas componentes, donde vem que $\text{cc}(G - uv) = \text{cc}(G) + 1$.

(b) \Rightarrow (c) Tal como anteriormente, considerando $G[V_1]$ como sendo a componente em G que contém uv , podemos concluir que, para cada $x \in V_1$, o vértice x é conexo com vértice u ou v em $G - uv$, mas não com ambos, uma vez que $\text{cc}(G - uv) = \text{cc}(G) + 1$. Logo, u e v pertencem a componentes distintas de $G - uv$, pelo que não são conexos.

(c) \Rightarrow (d) (Por contraposição) Suponha que uv pertence a um circuito C do grafo G . Então $C - uv$ é um caminho- (u, v) em $G - uv$ e, consequentemente, os vértices u e v são conexos em $G - uv$.

(d) \Rightarrow (a) (Por contraposição) Suponha que uv não é uma ponte de G . Então $cc(G - uv) = cc(G)$ e, consequentemente, os vértices u e v são conexos em $G - uv$. Porém, tal implica a existência de um caminho- (u, v) P em $G - uv$, donde vem que $P + uv$ é um circuito em G que contém a aresta uv . \square

Podemos definir vértice de corte de modo análogo.

Definição 13.4 (Vértice de corte). *Um vértice v de um grafo G diz-se um vértice de corte se existe uma bipartição do conjunto das arestas $E(G)$ nos subconjuntos não vazios E_1 e E_2 , tal que v é o único vértice comum aos subgrafos $G[E_1]$ e $G[E_2]$.*

Observe-se que se G é um grafo não trivial sem lacetes, então v é um vértice de corte se e só se $cc(G - v) > cc(G)$ (uma vez que os grafos $G[E_1] - v$ e $G[E_2] - v$ não estão ligados).

Exemplo 13.5. Sendo k um número natural, vamos construir um grafo conexo G , com um vértice de corte v , tal que $cc(G - v) = k$.

Solução. Observe que uma estrela $K_{1,k}$ (ou seja, um grafo com um vértice de grau k e k vértices de grau 1 – ver Figura 13.2) é um grafo conexo. Porém, eliminando o vértice central v , resulta um grafo que contém k vértices isolados, isto é, $cc(K_{1,k} - v) = k$.

É claro que a estrela não é a única construção possível para este tipo de grafos. Por exemplo, se na estrela substituirmos os vértices v_1, \dots, v_k pelos grafos conexos G_1, \dots, G_k , respectivamente, com G_1, \dots, G_k , denotando grafos disjuntos, eliminando o vértice central v obtém-se um grafo cujas componentes são G_1, \dots, G_k . \square

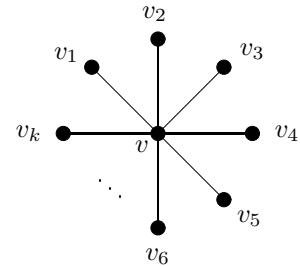


Figura 13.2: Estrela $K_{1,k}$.

13.2. Determinação de componentes conexas

Convém relembrar que os algoritmos de pesquisa em grafos (anteriormente estudados) – a pesquisa em profundidade (DFS) e a pesquisa em largura (BFS) – proporcionam uma visita a todos os vértices (e arestas) de um grafo, a partir de um vértice arbitrário v . É claro que condicionando os nossos movimentos apenas aos vértices adjacentes, só podemos atingir vértices pertencentes à componente que contém v e, desta forma, estes algoritmos podem ser utilizados para a determinação das componentes conexas de um grafo. Neste caso, podemos simplificar os algoritmos de pesquisa, uma vez que não precisamos da partição do conjunto de arestas.

Segue-se o Algoritmo 13.1 COMPONENTEDFS que é uma versão modificada do Algoritmo 12.2 DFS para a determinação da componente conexa de um grafo G que contém o vértice $v \in V(G)$. Analogamente, podem ainda obter-se versões modificadas de outros algoritmos de pesquisa (BFS, DFS1) com vista à determinação de componentes conexas.

No algoritmo que se segue, assume-se inicialmente $Componente = \emptyset$.

Algoritmo 13.1: COMPONENTEDFS(G, v)

```

global Componente
Componente  $\leftarrow$  Componente  $\cup \{v\}$ 
para todo  $w \in N_G(v)$ 
  fazer se  $w \notin$  Componente então COMPONENTEDFS( $G, w$ )

```

O Algoritmo 13.2 NCC, utiliza o algoritmo COMPONENTEDFS para a determinação do número de componentes de um grafo G .

Observe-se que a complexidade computacional do Algoritmo 13.2 é idêntica à do algoritmo DFS, isto é, $O(\nu + \varepsilon)$.

Algoritmo 13.2: NCC(G)

```

 $cc \leftarrow 0$ 
 $Componente \leftarrow \emptyset$ 
para todo  $v \in V(G)$ 
  fazer se  $v \notin Componente$ 
  então  $\begin{cases} \text{COMPONENTEDFS}(G, v) \\ cc \leftarrow cc + 1 \end{cases}$ 
devolver ( $cc$ )

```

Exemplo 13.6. Utilizando o algoritmo COMPONENTEDFS, vamos determinar a componente que contém o vértice a do grafo representado pela lista de sucessores:

a :	b, e
b :	a, c, d, e, f
c :	b, d
d :	b, c
e :	a, b, f, g
f :	b, e, g
g :	e, f

Solução. Assumimos que os vértices são considerados por ordem alfabética. Na Tabela 13.1 apresentam-se todos os passos necessários para a determinação da componente que contém o vértice a . \square

Dado um grafo G , representado pela sua matriz de adjacência A_G , um modo de testar se G é ou não conexo, consiste em analisar todas as permutações de linhas e colunas de A_G e verificar se alguma produz uma matriz diagonal por blocos. Se o número máximo de blocos é maior do que um, então o grafo não é conexo e o número de blocos corresponde ao número de componentes conexas. Porém, existem $\nu(G)!$ permutações de linhas e colunas de A_G , o que torna este método não efectivo para valores elevados de $\nu(G)$. Um método mais eficiente, consiste em determinar a matriz soma das potências, entre 1 e $\nu(G) - 1$, de A_G , ou seja, a matriz $Y = A + A^2 + \dots + A^{\nu-1}$ e verificar se Y tem entradas nulas. Com efeito, como veremos mais adiante (no Capítulo 14), a entrada y_{ij} é não nula se e só se os vértices v_i e v_j são conexos.

Mesmo assim, este método necessita de um grande número de operações aritméticas, o que o torna pouco competitivo em relação ao *método de fusão* que vamos passar a descrever.

13.3. Algoritmo de fusão de vértices

Dados dois vértices v_i e v_j de um grafo G , designa-se por *fusão dos vértices* v_i e v_j a operação de substituição destes vértices por um único vértice z , cujos vizinhos passam a ser os vizinhos de v_i e os vizinhos de v_j . Nestas condições, obtém-se um novo grafo, \widehat{G} , com as seguintes propriedades:

1. $V(\widehat{G}) = V(G) \setminus \{v_i, v_j\} \cup \{z\}$, com $z \notin V(G)$.

<i>v</i>	<i>w</i>	<i>Componente</i>	observações
		\emptyset	inicialização das variáveis
<i>a</i>	<i>b</i>	{ <i>a</i> }	
<i>b</i>	<i>a</i>	{ <i>a</i> , <i>b</i> }	não se volta a visitar <i>a</i>
<i>b</i>	<i>c</i>		
<i>c</i>	<i>b</i>	{ <i>a</i> , <i>b</i> , <i>c</i> }	não se volta a visitar <i>b</i>
<i>c</i>	<i>d</i>		
<i>d</i>	<i>b</i>	{ <i>a</i> , <i>b</i> , <i>c</i> , <i>d</i> }	não se volta a visitar <i>b</i>
<i>d</i>	<i>c</i>		voltamos ao vértice <i>c</i> , donde se chegou a <i>d</i>
<i>c</i>			voltamos ao vértice <i>b</i> , donde se chegou a <i>c</i>
<i>b</i>	<i>d</i>		não se volta a visitar <i>d</i>
<i>b</i>	<i>e</i>		
<i>e</i>	<i>a</i>	{ <i>a</i> , <i>b</i> , <i>c</i> , <i>d</i> , <i>e</i> }	não se volta a visitar <i>a</i>
<i>e</i>	<i>b</i>		não se volta a visitar <i>b</i>
<i>e</i>	<i>f</i>		
<i>f</i>	<i>b</i>	{ <i>a</i> , <i>b</i> , <i>c</i> , <i>d</i> , <i>e</i> , <i>f</i> }	não se volta a visitar <i>b</i>
<i>f</i>	<i>e</i>		não se volta a visitar <i>e</i>
<i>f</i>	<i>g</i>		
<i>g</i>	<i>e</i>	{ <i>a</i> , <i>b</i> , <i>c</i> , <i>d</i> , <i>e</i> , <i>f</i> , <i>g</i> }	podemos parar, com todos os vértices já visitados
<i>g</i>	<i>f</i>		
<i>f</i>			
<i>e</i>	<i>g</i>		
<i>b</i>	<i>f</i>		
<i>a</i>	<i>e</i>		

Tabela 13.1: Descrição dos passos decorrentes da aplicação do Algoritmo 13.1, COMPONENTEDFS, na resolução do Exemplo 13.6.

2. Para cada par de vértices v_p e v_q , com $\{p, q\} \cap \{i, j\} = \emptyset$, verifica-se que

$$v_p v_q \in E(\widehat{G}) \Leftrightarrow v_p v_q \in E(G),$$

ou seja, as arestas não incidentes em qualquer dos vértices v_i ou v_j permanecem inalteráveis.

3. Qualquer que seja o vértice $v \in V(G)$ tal que $v_i \neq v \neq v_j$, verifica-se que

$$vz \in E(\widehat{G}) \Leftrightarrow \{vv_i, vv_j\} \cap E(G) \neq \emptyset,$$

ou seja, o vértice $v \in V(G)$ é adjacente ao novo vértice z em \widehat{G} , se e só se v é adjacente a v_i ou a v_j em G . Adicionalmente, o número de arestas paralelas entre v e z é igual à soma do número de arestas paralelas entre v e v_i e entre v e v_j .

4. Por cada um dos lacetes $v_i v_i$ e $v_j v_j$, existentes em G , produz-se em \widehat{G} um novo lacete incidente no vértice z .
5. Por simplicidade, com vista à verificação da conexidade do grafo G , o grafo \widehat{G} pode ainda ser modificado, com a substituição das arestas paralelas por uma única aresta e a eliminação de todos os lacetes, de modo a transformar \widehat{G} num grafo simples.

A operação de fusão de dois vértices v_i e v_j é fácil de implementar para qualquer das representações usuais de grafos em computador. Por exemplo, se o grafo é representado pela sua lista de sucessores, para se fundirem os vértices v_i e v_j , basta eliminar as listas que lhes correspondem e adicionar uma

nova lista (que corresponde ao novo vértice z) que é, precisamente, a união das listas eliminadas. Adicionalmente, nas listas que correspondem aos restantes vértices, substitui-se v_i e v_j por z .

No caso de grafos simples representados pela matriz de adjacência, a operação de fusão de dois vértices v_i e v_j corresponde à operação lógica \vee (disjunção), aplicada aos pares de entradas (em posições idênticas) nas i -ésima e j -ésima linha e coluna, registrando-se o resultado obtido na i -ésima linha e coluna ou na j -ésima linha e coluna e eliminando-se a outra (linha e coluna). Deve observar-se que embora este procedimento elimine (automaticamente) as arestas paralelas, eventualmente produzidas, ele pode originar o aparecimento de lacetes, sem contudo dar origem a lacetes paralelos.

Por questões de eficiência e simplicidade, o algoritmo que se segue, Algoritmo 13.3 FUNDEVÉRTICES, funde o primeiro vértice (que corresponde à primeira linha e coluna da matriz de adjacência) com um vértice i arbitrário ($i \neq 1$) que é dado como parâmetro de entrada. Os restantes parâmetros de entrada deste algoritmo são A que denota a matriz de adjacência e ν que denota o número de vértices. Uma vez executada a operação de fusão do vértice v_1 com o vértice v_i , o novo vértice z é colocado na primeira posição (em substituição de v_1) e o vértice v_i é eliminado, substituindo-se a i -ésima linha e coluna pela última linha e coluna. Deste modo, a complexidade computacional desta operação é de apenas $O(\nu)$.

Algoritmo 13.3: FUNDEVÉRTICES(A, ν, i)

```

para  $k \leftarrow 1$  até  $\nu$ 
    fazer
         $\begin{cases} A[1, k] \leftarrow A[1, k] \vee A[i, k] \\ A[k, 1] \leftarrow A[k, 1] \vee A[k, i] \\ A[i, k] \leftarrow A[\nu, k] \\ A[k, i] \leftarrow A[k, \nu] \end{cases}$ 
     $\nu \leftarrow \nu - 1$ 
devolver  $(A, \nu)$ 
```

Com base no Algoritmo 13.3, estamos em condições de apresentar um algoritmo de fusão de todos os vértices de uma componente conexa de um grafo G que contém um vértice fixo $v \in V(G)$. Vamos começar por uma descrição informal deste algoritmo.

1. Fundir v com um dos vértices que lhe são adjacentes;
2. Repetir o procedimento de fusão, do passo anterior, substituindo v pelo novo vértice obtido até que o novo vértice seja um vértice sem vértices adjacentes distintos dele próprio.

Desta forma, reduzimos a componente conexa de G , que contém o vértice inicial $v \in V(G)$, a um único vértice. Depois das operações de fusão executadas, caso se obtenha um grafo de ordem 1, G é conexo, caso contrário, podemos repetir este procedimento para as restantes componentes. O Algoritmo 13.4 FUNDECOMPONENTE descreve, formalmente, o procedimento de fusão da componente de um grafo G , de ordem ν e matriz de adjacência A , que contém um vértice particular v . Note-se que a tabela $perm$ é utilizada para recuperação das etiquetas iniciais dos vértices. Mais precisamente, $perm[i]$ é a etiqueta do vértice que ocupa a i -ésima linha e coluna da matriz A depois de modificada pelo algoritmo. Inicialmente, esta tabela contém as etiquetas correspondentes à matriz A , sem qualquer modificação.

Dado que o algoritmo FUNDECOMPONENTE tem o ciclo **repetir** que é executado no máximo ν vezes e, dentro dele, os passos executados têm uma complexidade $O(\nu)$, podemos concluir que a complexidade deste algoritmo, na sua globalidade, é $O(\nu^2)$. Segue-se um exemplo de aplicação.

Algoritmo 13.4: FUNDECOMPONENTE(A, ν, v)

```

global perm
para  $k \leftarrow 1$  até  $\nu$  fazer  $\begin{cases} A[1, k] \leftrightarrow A[v, k] \\ A[k, 1] \leftrightarrow A[k, v] \end{cases}$ 
perm[ $v$ ]  $\leftarrow$  perm[1];  $Z \leftarrow \{v\}$ 
repetir
   $i \leftarrow 2$ 
  enquanto ( $i < \nu$ )  $\wedge$  ( $A[1, i] = 0$ ) fazer  $i \leftarrow i + 1$ 
  se  $A[1, i] = 0$ 
    então devolver ( $A, \nu, Z$ )
  senão  $\begin{cases} Z \leftarrow Z \cup \{\text{perm}[i]\} \\ \text{FUNDEVÉRTICES}(A, \nu, i) \\ \text{perm}[i] \leftarrow \text{perm}[\nu + 1] \end{cases}$ 
até falso

```

Exemplo 13.7. Utilizando o algoritmo FUNDECOMPONENTE, vamos determinar a componente conexa que contém o vértice v_8 do grafo definido pela seguinte matriz de adjacência¹:

$$A = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 & v_9 & v_{10} \\ v_1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ v_2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ v_3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ v_4 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ v_5 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ v_6 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ v_7 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ v_8 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ v_9 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ v_{10} & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Solução. No passo inicial trocam-se (entre si) as posições dos vértices v_8 e v_1 , na matriz de adjacência, e inicializam-se as restantes variáveis (Figura 13.3-(A)):

$$A = \begin{array}{ccccccccccl} & \text{perm} & z & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_1 & v_9 & v_{10} \\ & & \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} & & & & & & & & \\ & z & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & v_2 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ & v_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ & v_4 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ & v_5 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ & v_6 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & v_7 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ & v_1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ & v_9 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ & v_{10} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array} \quad \text{e} \quad Z = \{v_8\}.$$

Uma vez que o vértice z é adjacente a v_2 , fundimos z e v_2 , executando o algoritmo FUNDEVÉRTICES($A, \nu, 2$). Como resultado obtém-se:

¹Na descrição da aplicação dos diferentes passos do algoritmo, vamos denotar por z o vértice que resulta da fusão dos vértices em Z

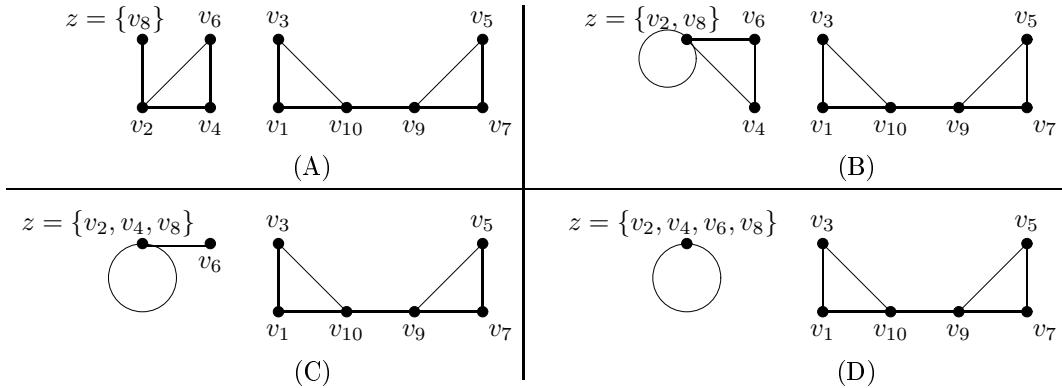


Figura 13.3: Subgrafos obtidos, consecutivamente, pela aplicação dos passos do algoritmo de fusão de uma componente conexa (ver Exemplo 13.7).

$$\begin{array}{ll}
 \begin{matrix} perm & z \ v_{10} \ v_3 \ v_4 \ v_5 \ v_6 \ v_7 \ v_1 \ v_9 \end{matrix} \\
 \begin{matrix} z \\ v_{10} \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \\ v_1 \\ v_9 \end{matrix} & \left(\begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{matrix} \right) \quad \text{e} \quad Z = \{v_2, v_8\}, \\
 A = &
 \end{array}$$

onde A é à matriz de adjacência do grafo representado na Figura 13.3-(B). Agora, o primeiro vértice adjacente a z é v_4 . Fundindo estes vértices, executando o algoritmo FUNDEVÉRTICES($A, \nu, 4$), obtém-se:

$$\begin{array}{ll}
 \begin{matrix} perm & z \ v_{10} \ v_3 \ v_9 \ v_5 \ v_6 \ v_7 \ v_1 \end{matrix} \\
 \begin{matrix} z \\ v_{10} \\ v_3 \\ v_9 \\ v_5 \\ v_6 \\ v_7 \\ v_1 \end{matrix} & \left(\begin{matrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{matrix} \right) \quad \text{e} \quad Z = \{v_2, v_4, v_8\}, \\
 A = &
 \end{array}$$

onde A é à matriz de adjacência do grafo representado na Figura 13.3-(C). Continuando com este procedimento, a fusão dos vértices z e v_6 produz:

$$\begin{array}{ccccccccc}
 & perm & z & v_{10} & v_3 & v_9 & v_5 & v_1 & v_7 \\
 \\
 A = & \begin{matrix} z \\ v_{10} \\ v_3 \\ v_9 \\ v_5 \\ v_1 \\ v_7 \end{matrix} & \left(\begin{array}{ccccccc}
 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 1 & 0 & 0
 \end{array} \right) & e & Z = \{v_2, v_4, v_6, v_8\}.
 \end{array}$$

Uma vez que o vértice z é agora um vértice isolado (ver Figura 13.3-(D)), podemos concluir que a componente a que pertence v_8 é induzida pelo conjunto de vértices $Z = \{v_2, v_4, v_6, v_8\}$. \square

Caso seja necessário determinar apenas o número de todas as componentes de um grafo, é claro que o algoritmo se pode simplificar, uma vez que, nesse caso, a informação sobre a ordem inicial dos vértices é irrelevante. Assim, em tais condições, o algoritmo reduz-se ao procedimento de fundir, sucessivamente, dois vértices adjacentes até que cada componente se reduza a um único vértice.

Procedimento para a determinação do número de componentes. Dado um grafo G , representado pela sua matriz de adjacência, o algoritmo de determinação do número de componentes conexas, $cc(G)$, divide-se nos seguintes passos:

1. Procurar um elemento não nulo a_{ij} , fora da diagonal principal (ou seja, com $i \neq j$). Se tal elemento não existe, então passar para 3.
2. Fundir os vértices associados às colunas (ou linhas) i e j e voltar a 1.
3. Determinar o número de linhas (ou colunas) da matriz A_G que é igual ao número de componentes $cc(G)$ do grafo inicial.

Com este procedimento podemos utilizar o Algoritmo 13.3 FUNDEVÉRTICES ou o Algoritmo 13.4 FUNDECOMPONENTE.

Exemplo 13.8. Dado um grafo G , representado pela matriz de adjacência

$$A_G = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

vamos determinar o seu número de componentes $cc(G)$.

Solução. É claro que o número de vértices $\nu(G)$ é igual ao número de linhas (colunas) da matriz A_G , ou seja, $\nu(G) = 4$. Uma vez que o Algoritmo 13.3 FUNDEVÉRTICES, funde os vértices associados, respectivamente, à primeira e a uma outra linha (coluna) i da matriz A_G , vamos escolher i de tal modo que $a_{1,i} \neq 0$. Neste caso, escolhemos $a_{1,2}$ e fundimos os vértices associados, respectivamente, à primeira e segunda linha (coluna), executando $\text{FUNDEVÉRTICES}(A, 4, 2)$. Nestas condições, como resultado, obtém-se o subgrafo G_1 , cuja matriz de adjacência é

$$A_{G_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Recorde-se que o algoritmo FUNDEVÉRTICES coloca a última linha de A_G na segunda linha de A_{G_1} (para $i = 2$, considerando apenas as entradas não eliminadas). Com o resultado obtido, verifica-se que o vértice de G_1 associado à primeira linha de A_{G_1} é um vértice isolado. Uma vez que a matriz A_{G_1} tem elementos não nulos fora da diagonal principal, é necessário trocar a ordem dos vértices. Assim, passando a segunda linha (coluna) para primeira, a terceira para segunda e a primeira para última, obtém-se a matriz de adjacência

$$A_{G_2} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Uma vez que entrada $a_{1,3} = 1$, fundimos a primeira e terceira linha (coluna), executando FUNDEVÉRTICES($A, 3, 3$), pelo que se obtém

$$A_{G_3} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Na matriz A_{G_3} , todos os elementos não nulos estão na diagonal principal. Logo, uma vez que o número de linhas (colunas) desta matriz é 2, vem que o número de componentes conexas de G é $cc(G) = 2$. \square

Definição 13.5 (Conexidade e aresta-conexidade). *Um grafo G diz-se k -vértice conexo (ou simplesmente k -conexo) se não existe $X \subset V(G)$ tal que $|X| < k$ e $G - X$ é desconexo. Adicionalmente, designa-se por conexidade de G e denota-se por $\kappa(G)$ o maior k tal que G é k -conexo. Por convenção, considera-se $\kappa(K_\nu) = \nu - 1$. Por sua vez, um grafo H diz-se k -aresta-conexo se não existe $Y \subset E(H)$ tal que $|Y| < k$ e $H - Y$ é desconexo. Adicionalmente, designa-se por aresta-conexidade de H e denota-se por $\kappa'(H)$ o maior k tal que H é k -aresta-conexo. Por convenção, considera-se $\kappa'(K_1) = 0$.*

Como consequência desta definição, um grafo é 1-conexo (1-aresta-conexo) se e somente se é conexo. Por outro lado, dado um grafo arbitrário G , podemos concluir o seguinte:

1. $\kappa(G) = 0$ ($\kappa'(G) = 0$) se e só se G não é conexo ou $G = K_1$. Por outro lado, $\kappa(G) = \nu(G) - 1$ se e só se G é um grafo completo.
2. Se G é conexo, $\nu = \nu(G)$ e $G \neq K_\nu$, então $1 \leq \kappa(G) \leq \nu - 2$.
3. $\kappa(G) \leq \kappa'(G) \leq \delta(G)$.

As provas de 1 e 2 são imediatas. Por sua vez, a prova das desigualdades 3 obtém-se tendo em conta o seguinte:

- a) (desigualdade da esquerda) escolhendo $\kappa'(G)$ arestas que desconexam G , se eliminarmos um vértice extremo de cada uma destas arestas, então elas são automaticamente eliminadas e, consequentemente, o grafo fica desconexo;
- b) (desigualdade da direita) escolhendo um vértice v de G de menor grau, $\delta(G)$, se eliminarmos as arestas incidentes em v , então o vértice v fica isolado e, consequentemente, o grafo fica desconexo.

Teorema 13.3. *Se G é um grafo 2-conexo, então qualquer que seja o par de vértices existe um ciclo que os contém.*

Demonstração. Seja G um grafo 2-conexo e suponha que existem dois vértices $u, v \in V(G)$ que não estão contidos em qualquer ciclo. Seja w um vértice que juntamente com u pertence a um dado ciclo C e está tão próximo quanto possível de v (note-se que um tal ciclo C com $w \neq u$ existe, caso contrário, uma das arestas incidentes em u seria uma ponte, o que contraria a 2-conexidade de G). Seja P este caminho entre u e v e que passa por w . Tendo em conta a 2-conexidade de G existe um caminho alternativo P' entre u e v que não passa por w e este caminho contém um vértice u' que é o vértice de $V(C) \cap V(P')$ mais próximo de v . Então, a parte de P' , entre u' e v intersecta pelo menos um vértice da parte do caminho P entre w e v . Sendo w' o primeiro destes vértices, existe um ciclo que envolve os vértices u, u', w e w' , o que contraria a escolha de w . \square

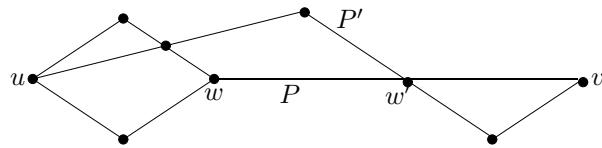


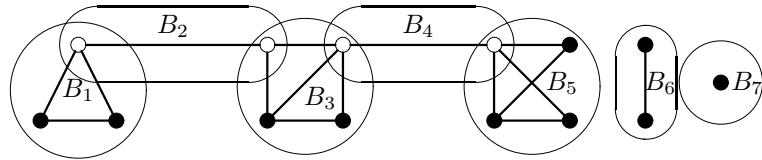
Figura 13.4: Figura que ilustra a demonstração do Teorema 13.3.

Seguem-se os conceitos de bloco e bloco extremo de um grafo que são conceitos relacionados com a k -conexidade.

Definição 13.6 (Bloco e bloco extremo). *Dado um grafo G designa-se por bloco todo o subgrafo maximal sem vértices de corte. Por sua vez, designa-se por bloco extremo de G todo o bloco que contém exactamente um vértice de corte em G .*

Como consequência desta definição, podemos concluir que um bloco de um grafo G ou é um subgrafo 2-conexo maximal ou uma ponte ou um vértice isolado. Tendo em conta a propriedade de maximalidade, dois blocos diferentes de um mesmo grafo conexo, G , ou são disjuntos ou se sobrepõem num único vértice que, em tais condições, é um vértice de corte de G . Consequentemente, pode concluir-se que cada aresta pertence a um único bloco e que um grafo é união dos seus blocos, podendo interpretar-se que os blocos são as componentes 2-conexas que constituem o grafo.

Na Figura 13.5, apresenta-se um grafo simples, G , com todos os seus blocos B_1, \dots, B_7 . Nesta figura, os vértices de corte de G são apresentados com uma cor clara para se distinguirem dos restantes vértices que aparecem a negro. Assim, é fácil ver que apenas B_1 e B_5 são blocos extremos.

Figura 13.5: Grafo G no qual se destacam os respectivos blocos B_1, \dots, B_7 .

Dado um grafo G , algumas vezes é útil considerar um grafo que se designa por *grafo dos blocos* de G , cujos vértices correspondem aos blocos de G e no qual dois vértices são adjacentes se e só se os correspondentes blocos têm um vértice comum². Na Figura 13.6, representa-se o grafo dos blocos do grafo G representado na Figura 13.5, devendo observar-se que aos blocos extremos de G correspondem vértices de grau um no grafo dos blocos.

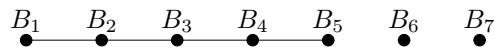


Figura 13.6: Grafo dos blocos do grafo representado na Figura 13.5.

13.4. Grafos orientados fortemente conexos

No caso dos digrafos a sua conexão, enquanto grafos não orientados, designa-se por *conexão fraca*. Por sua vez, a conexão que tem em conta os sentidos dos arcos designa-se por *conexão forte*.

²Note-se que se G é conexo, então o seu grafo dos blocos é uma árvore (ver Capítulo 15).

Definição 13.7 (Vértice atingível). *Dado um grafo orientado \vec{G} . Um vértice $w \in V(\vec{G})$ diz-se atingível a partir de um vértice $v \in V(\vec{G})$ se existe um caminho- (v, w) orientado no digrafo \vec{G} . Adicionalmente, diz-se que os vértices v e w são mutuamente atingíveis, se v é atingível a partir de w e w é atingível a partir de v .*

Definição 13.8 (Matriz de atingibilidade). *Dado um grafo orientado \vec{G} com conjunto de vértices $V(\vec{G}) = \{v_1, \dots, v_\nu\}$, designa-se por matriz de atingibilidade do digrafo \vec{G} , a matriz quadrada binária $D_{\vec{G}} = (d_{ij})$ de ordem ν tal que $d_{ij} = 1$ se o vértice v_j é atingível a partir do vértice v_i .*

Definição 13.9 (Componente fortemente conexa). *Designa-se por componente fortemente conexa de um digrafo \vec{G} todo o subgrafo maximal induzido $\vec{G}[\hat{V}]$ orientado, onde quaisquer dois vértices de \hat{V} são mutuamente atingíveis em $G[\hat{V}]$. Em particular, se quaisquer dois vértices do digrafo \vec{G} são mutuamente atingíveis, então \vec{G} diz-se fortemente conexo.*

Designa-se por conexidade ou vértice-conexidade (arco-conexidade) de um digrafo fortemente conexo \vec{G} e denota-se por $\kappa_v(\vec{G})$ ($\kappa_a(\vec{G})$) o menor número de vértices (arcos) cuja remoção produz um digrafo que não é fortemente conexo. Dado um grafo G , substituindo cada aresta por dois arcos com sentidos opostos e denotando o digrafo obtido por \overleftrightarrow{G} , podemos concluir que $\kappa_v(\overleftrightarrow{G}) = \kappa_v(G)$ ($\kappa_a(\overleftrightarrow{G}) = \kappa_e(G)$).

Teorema 13.4. *Um subconjunto maximal de vértices de um digrafo induz uma componente fortemente conexa se e só se os seus vértices definem linhas idênticas na matriz de atingibilidade.*

Demonstração. Por definição, os elementos diagonais da matriz de atingibilidade $D_{\vec{G}}$ são iguais a um. Dadas duas linhas idênticas em $D_{\vec{G}}$, por exemplo, as linhas i e j , podemos concluir que

$$d_{ij} = d_{jj} = 1 = d_{ii} = d_{ji}.$$

Isto significa que os vértices v_i e v_j são mutuamente atingíveis e, como consequência, pertencem a uma mesma componente fortemente conexa. Logo, os vértices que têm associadas linhas iguais induzem uma componente fortemente conexa. Reciprocamente, dado uma componente fortemente conexa constituída pelo conjunto de vértices $\{v_{i_1}, v_{i_2}, \dots, v_{i_k}\}$, então as linhas i_1, i_2, \dots, i_k contêm uns nas posições i_1, i_2, \dots, i_k , uma vez que $d_{i_r i_r} = d_{ii_r}$, para $i \in \{i_1, i_2, \dots, i_k\}$ e para $r = 1, \dots, k$. Adicionalmente, se existe $j \notin \{i_1, i_2, \dots, i_k\}$ tal que $d_{i_r j} = 1$ para algum $r \in \{1, \dots, k\}$, tal significa que v_j é atingível a partir de v_{i_r} e, consequentemente, pela transitividade da relação de atingibilidade, também é atingível a partir de qualquer dos restantes vértices do conjunto $\{v_{i_1}, v_{i_2}, \dots, v_{i_k}\}$, pelo que podemos concluir que as linhas associadas a este conjunto de vértices são idênticas. \square

Aparentemente, o Teorema 13.4 resolve o problema de verificar se um digrafo é ou não fortemente conexo, bem como o problema da determinação de uma componente fortemente conexa. Infelizmente, a determinação da matriz de atingibilidade é computacionalmente complexa (para dimensões elevadas, obriga a um grande número de operações).

No que se segue, dado um digrafo arbitrário \vec{G} , vamos considerar $A_{\vec{G}}$ como sendo a matriz de adjacência do respectivo grafo de suporte dos arcos o qual, para o estudo da conexidade, é suficiente.

Tendo em conta que, dado um digrafo \vec{G} , a entrada (i, j) da potência de ordem k da matriz de adjacência, $(A_{\vec{G}})^k$, é igual ao número de passeios orientados existentes entre o vértice v_i e o vértice v_j e ainda que a existência de um passeio implica a existência de um caminho, a determinação da matriz de atingibilidade pode ser feita a partir destas potências, definindo-se uma matriz binária $P_{\vec{G}} = A_{\vec{G}}$, na qual a entrada (i, j) da sua k -ésima potência, $(P_{\vec{G}})^k$, é igual a 1 se e só se existe um caminho- (v_i, v_j) orientado de comprimento k , logo as operações em $(P_{\vec{G}})^k$ são operações de uma álgebra de Boole. Desta forma, podemos determinar a matriz de atingibilidade recorrendo ao seguinte procedimento:

1. Fazer $B = P_{\vec{G}} + I$, onde I é a matriz identidade de dimensão $\nu \times \nu$.
2. Determinar B^k (sobre uma álgebra de Boole), para $k = 1, 2, \dots$, até se ter $B^k = B^{k-1}$.

É fácil mostrar que a potência B^k devolvida no passo 2 é tal que $B^k = D_{\vec{G}}$. Infelizmente, porém, por vezes é necessário calcular todas as potências até $k = \nu - 1$, o que torna este método computacionalmente muito dispendioso.

Alternativamente, a matriz de atingibilidade de um digrafo \vec{G} , pode ser determinada utilizando o procedimento a seguir indicado que recorre, novamente, à matriz $P_{\vec{G}}$ para a determinação, linha a linha, de $D_{\vec{G}}$. Por simplicidade de notação, vamos assumir que os vértices são etiquetados pelos números $1, \dots, \nu$. Assim, a determinação da i -ésima linha de $D_{\vec{G}}$ faz-se executando os seguintes passos:

1. Marcar o vértice v_i .
2. Escolher um vértice já marcado v_k e marcar todos os vértices v_j , tais que $p_{k,j} = 1$, para a matriz $P_{\vec{G}}$. Se não se pode marcar nenhum vértice, ainda não marcado, passar para 3. Caso contrário repetir 2.
3. Inserir uns nas entradas da i -ésima linha da matriz $D_{\vec{G}}$ que correspondem a vértices marcados.

Deve observar-se que este procedimento não é mais do que o algoritmo de pesquisa em largura (BFS) e pode ser utilizado para a determinação de componentes fortemente conexas de digrafos, como parte integrante de algoritmos de pesquisa (como são o caso dos algoritmos de Kosaraju, de Tarjan e de Gabow). Na proxima secção, vamos apresentar um outro algoritmo para determinação de componentes fortemente conexas, conhecido por algoritmo de Leifman.

13.5. Algoritmo de Leifman

A determinação de componentes fortemente conexas utilizando a matriz de atingibilidade, do ponto de vista prático, não é muito útil para grafos de grandes dimensões. Um dos algoritmos mais eficientes foi introduzido por Leifman em 1966, para a determinação de todas as componentes fortemente conexas de um digrafo. A elevada eficiéncia deste algoritmo tem motivado a sua utilização noutros problemas relacionados com redes e digrafos. Antes de passarmos à sua descrição, convém lembrar que, dado um digrafo \vec{G} e um vértice $v \in V(\vec{G})$, o grau de v divide-se nos semigraus de saída $d^+(v) = |\{e \in E : \psi_{\vec{G}}(e) = (v, x)\}|$ e de entrada $d^-(v) = |\{e \in E : \psi_{\vec{G}}(e) = (x, v)\}|$. Neste algoritmo, os vértices vão ser marcados com pares de marcas que se denotam do seguinte modo:

- $l(v)$ — marca esquerda do vértice v ,
- $r(v)$ — marca direita do vértice v .

Por outro lado, \mathcal{C} denotará um conjunto vazio à entrada do algoritmo e, à saída, um conjunto onde cada elemento é um subconjunto de vértices que induz uma componente fortemente conexa.

Algoritmo de Leifman (para a determinação das componentes fortemente conexas de um digrafo \vec{G}).

1. Procurar em \vec{G} os vértices $v \in V(\vec{G})$ tais que $d^+(v) = 0$ ou $d^-(v) = 0$. Acrescentar a \mathcal{C} os conjuntos singulares formados pelos vértices nestas condições, eliminando-os do digrafo \vec{G} . Este procedimento deve ser repetido até não existirem novas componentes triviais, obtendo-se, como resultado, o subdigrafo \vec{G}^o .
2. Escolher um vértice $v_o \in V(\vec{G}^o)$, onde \vec{G}^o é o subdigrafo que resulta dos pontos 1 ou 4, com marcas $(l(v), r(v))$, de acordo com seguinte procedimento:

- (a) Inicialmente, todos os vértices $v \in V(\vec{G})$ têm marcas $(0, 0)$. Todos os sucessores v (vértices atingíveis percorrendo, pelo menos, um arco) de v_o são marcados com $l(v) = 1$, depois todos os sucessores de vértices com $l(v) = 1$ são marcados com $l(v) = 1$, etc. Este procedimento termina quando não existem mais vértices para marcar com a marca esquerda igual a 1. Como consequência, todos os sucessores de v_o , em \vec{G}^o , têm marca esquerda igual a 1.
- (b) Tal como anteriormente, marca-se $r(v) = 1$ em todos os vértices v a partir dos quais se atinge v_o (percorrendo, pelo menos, um arco) em \vec{G}^o , com a diferença de, neste caso, se procurarem antecessores em vez de sucessores.

Depois da aplicação deste procedimento, o conjunto de vértices $V(\vec{G}^o)$ parte-se em quatro subconjuntos (alguns dos quais poderão ser vazios)

$$V(\vec{G}^o) = V_{00} \cup V_{01} \cup V_{10} \cup V_{11},$$

tais que cada vértice v pertence ao subconjunto $V_{l(v)r(v)}$.

3. Para a determinação de novas componentes fortemente conexas, existem duas possibilidades:
- (a) Se $V_{11} \neq \emptyset$, então V_{11} induz uma nova componente fortemente conexa – que deve ser adicionada a \mathcal{C} . Se os conjuntos V_{00} , V_{01} e V_{10} são todos vazios, então passar para 4. Caso contrário, memorizar todos os conjuntos não vazios de entre V_{00} , V_{01} e V_{10} para utilização nos próximos passos (dado que as componentes fortemente conexas ainda não determinadas vão ser induzidas por subconjuntos de vértices contidos num destes subconjuntos) e passar ao passo 4.
- (b) Se $V_{11} = \emptyset$, então $v_o \in V_{00}$ e v_o forma uma componente trivial $\{v_o\}$ que se junta a \mathcal{C} , modificando-se V_{00} para $V_{00} \leftarrow V_{00} \setminus \{v_o\}$. Todos os conjuntos não vazios de entre V_{00} , V_{01} e V_{10} devem ser memorizados para utilização nos próximos passos e passar para o passo 4.
4. Caso existam alguns conjuntos memorizados no passo 3 ainda não utilizados, escolher um deles como novo conjunto V^o , determinar o novo subgrafo $\vec{G}^o = (V^o, E^o)$ e passar para o passo 2. Caso contrário, PARAR (o conjunto \mathcal{C} contém todos as componentes fortemente conexas do digrafo \vec{G}).

Este algoritmo é formalmente apresentado a seguir, em pseudocódigo, com a designação de Algoritmo 13.5: LEIFMAN. Como entrada, recebe um digrafo \vec{G} e como resultado devolve o conjunto \mathcal{C} , cujos elementos são os subconjuntos de vértices que induzem todas as componentes fortemente conexas. O conjunto de vértices x tais que $vx \in E(\vec{G})$ ($xv \in E(\vec{G})$) denota-se por $N_{\vec{G}}^+(v)$ ($N_{\vec{G}}^-(v)$). Por outro lado, embora, por simplicidade de apresentação, se tenha utilizado uma tabela em substituição de uma pilha, na prática, porém, é conveniente que se recorra à estrutura de dados pilha.

O Teorema 13.5, a seguir, onde \vec{G}_{lp} denota o subdigrafo induzido pelo conjunto de vértices V_{lp} determinado no passo 2, ou seja,

$$\vec{G}_{lr} = \vec{G}[V_{lr}],$$

justifica a validade deste algoritmo.

Teorema 13.5. *Se $V_{11} \neq \emptyset$, então o subdigrafo \vec{G}_{11} é uma componente fortemente conexa e $v_o \in V_{11}$. Caso contrário ($V_{11} = \emptyset$), o subconjunto $\{v_o\}$ é uma componente fortemente conexa e $v_o \in V_{00}$. Adicionalmente, cada componente fortemente conexa pertence a um subdigrafo $\vec{G}_{lr} = \vec{G}[V_{lr}]$, com $l, r \in \{0, 1\}$.*

Algoritmo 13.5: LEIFMAN(\vec{G})

```

 $\mathcal{C} \leftarrow \emptyset; Pilha[1] \leftarrow V(\vec{G}); NPilha \leftarrow 1$ 
repetir
   $V_o \leftarrow Pilha[NPilha]; NPilha \leftarrow NPilha - 1$ 
  repetir
     $encontrado \leftarrow 0$ 
    para todo  $v \in V_o$ 
      fazer se  $d^+(v) = 0 \vee d^-(v) = 0$ 
      então  $\begin{cases} encontrado \leftarrow v; \mathcal{C} \leftarrow \mathcal{C} \cup \{\{v\}\}; V_o \leftarrow V_o \setminus \{v\}; G \leftarrow G - v \\ interromper \end{cases}$ 
    até  $encontrado = 0$ 
    se  $V_o \neq \emptyset$ 
      para todo  $v \in V_o$ 
        fazer  $l(v) \leftarrow r(v) \leftarrow 0$ 
        escolher  $v_o \in V_o$ 
         $S[1] \leftarrow v_o; NS \leftarrow 1$ 
        repetir
           $v \leftarrow s[NS]; NS \leftarrow NS - 1$ 
          para todo  $w \in N_{\vec{G}}^+(v)$ 
            fazer se  $l(w) = 0$ 
            então  $l(w) \leftarrow 1; NS \leftarrow NS + 1; S[NS] \leftarrow w$ 
          até  $NS = 0$ 
           $S[1] \leftarrow v_o; NS \leftarrow 1$ 
          repetir
             $v \leftarrow s[NS]; NS \leftarrow NS - 1$ 
            para todo  $w \in N_{\vec{G}}^-(v)$ 
              fazer se  $r(w) = 0$ 
              então  $r(w) \leftarrow 1; NS \leftarrow NS + 1; S[NS] \leftarrow w$ 
            até  $NS = 0$ 
         $V_{00} \leftarrow V_{01} \leftarrow V_{10} \leftarrow V_{11} \leftarrow \emptyset$ 
        para todo  $v \in V_o$ 
          fazer  $V_{l(v),r(v)} \leftarrow V_{l(v),r(v)} \cup \{v\}$ 
        se  $V_{11} \neq \emptyset$  então  $\mathcal{C} \leftarrow \mathcal{C} \cup \{V_{11}\}; G \leftarrow G - V_{11}$ 
        para todo  $V_{ij}$ 
          fazer se  $(i,j) \neq (0,0) \wedge V_{ij} \neq \emptyset$ 
          então  $NPilha \leftarrow NPilha + 1; Pilha[NPilha] \leftarrow V_{ij}$ 
      até  $NPilha = 1$ 
      devolver ( $\mathcal{C}$ )
    
```

Demonstração. Se $V_{11} \neq \emptyset$, então existe um vértice $v \in V_{11}$ e, por definição, V_{11} contém os vértices v_o e v que são mutuamente atingíveis. Isto implica que existam caminhos (v_o, v) e (v, v_o) orientados, os quais, conjuntamente, formam um caminho- (v_o, v_o) orientado. Logo, $v_o \in V_{11}$ e todos os pares de vértices de V_{11} são mutuamente atingíveis (via v_o). Como consequência, V_{11} é uma componente fortemente conexa.

Se $V_{11} = \emptyset$, então não existem vértices mutuamente atingíveis relativamente a v_o . Tal significa que não existe qualquer outro vértice distinto de v_o pertencente à mesma componente fortemente conexa de v_o . Logo, v_o forma uma componente trivial.

Seja $U \subseteq V^o$ o conjunto dos vértices de uma componente fortemente conexa do digrafo \vec{G}^o e seja $u \in U$ um vértice desta componente. Se os vértices u e v_o são mutuamente atingíveis, pela primeira parte da prova vem que $U = V_{11}$ induz uma componente fortemente conexa. Logo, assumindo-se que u e v_o não são mutuamente atingíveis, existem três possibilidades:

1. Existe um caminho- (v_o, u) orientado, mas não existe um caminho- (u, v_o) orientado. Neste caso, u é marcado com $l(u) = 1$ e $r(u) = 0$ e, como consequência, todos os vértices $v \in U$ por definição de componente fortemente conexa e pela transitividade da relação de atingibilidade são marcados com $l(v) = 1$ e $r(v) = 0$. Logo, $U \subseteq V_{10}$.
2. Não existe um caminho- (v_o, u) orientado, mas existe um caminho- (u, v_o) orientado. Neste caso, u é marcado com $l(u) = 0$ e $r(u) = 1$. Como consequência, todos os vértices $v \in U$ por definição de componente fortemente conexa e pela transitividade da relação de atingibilidade são marcados com $l(v) = 0$ e $r(v) = 1$. Logo, $U \subseteq V_{01}$.
3. Não existe um caminho- (v_o, u) orientado nem um caminho- (u, v_o) orientado. Neste caso, todos os vértices $v \in U$ são marcados com $l(v) = 0$ e $r(v) = 0$. Logo, $U \subseteq V_{00}$. \square

Exemplo 13.9. Vamos determinar todas as componentes fortemente conexas do digrafo definido pela matriz binária de adjacência:

$$P_{\vec{G}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

com recurso ao algoritmo de Leifman.

Solução. Por aplicação do passo 1 do algoritmo, verifica-se que apenas o vértice v_3 não tem sucessores. Logo, $\{v_3\}$ é uma componente fortemente conexa e, após a aplicação do passo 1, vem

$$V^o = \{v_1, v_2, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11}, v_{12}\}, \quad \mathcal{C} = \{\{v_3\}\}.$$

Escolhendo para v_o um vértice arbitrário de V^o , por exemplo v_4 , aplicando o passo 2 do algoritmo, obtém-se a seguinte partição de V :

$$\begin{aligned} V_{00} &= V_{01} = \emptyset, \\ V_{10} &= \{v_1, v_2, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11}\}, \\ V_{11} &= \{v_4, v_{12}\}. \end{aligned}$$

O conjunto V_{11} induz uma nova componente e, uma vez que existe apenas um conjunto para analisar, $V^o = V_{10}$. Logo, obtém-se

$$V^o = \{v_1, v_2, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11}\}, \quad \mathcal{C} = \{\{v_3\}, \{v_4, v_{12}\}\}.$$

Escolhendo agora para v_o , por exemplo $v_6 \in V^o$, por aplicação do passo 2 do algoritmo obtém-se a partição de V^o :

$$\begin{aligned}V_{00} &= V_{10} = \emptyset, \\V_{01} &= \{v_1, v_2, v_5, v_7, v_8, v_9, v_{11}\}, \\V_{11} &= \{v_6, v_{10}\}.\end{aligned}$$

Como consequência, o conjunto V_{11} induz uma nova componente e, como existe apenas um conjunto para analisar, $V^o = V_{01}$. Logo,

$$V^o = \{v_1, v_2, v_5, v_7, v_8, v_9, v_{11}\}, \quad \mathcal{C} = \{\{v_3\}, \{v_4, v_{12}\}, \{v_6, v_{10}\}\}.$$

Escolhendo para v_o , por exemplo $v_5 \in V^o$, por aplicação do passo 2 do algoritmo obtém-se a partição de V^o :

$$\begin{aligned}V_{00} &= V_{01} = \emptyset, \\V_{10} &= \{v_1, v_7, v_9, v_{11}\}, \\V_{11} &= \{v_2, v_5, v_8\}.\end{aligned}$$

Consequentemente, o conjunto V_{11} induz uma nova componente e, como existe apenas um conjunto para analisar, $V^o = V_{01}$. Logo,

$$V^o = \{v_1, v_7, v_9, v_{11}\}, \quad \mathcal{C} = \{\{v_3\}, \{v_4, v_{12}\}, \{v_6, v_{10}\}, \{v_2, v_5, v_8\}\}.$$

Escolhendo para v_o , por exemplo $v_1 \in V^o$, por aplicação de passo 2 de algoritmo obtém-se a partição de V^o :

$$\begin{aligned}V_{00} &= V_{01} = V_{10} = \emptyset, \\V_{11} &= \{v_1, v_7, v_9, v_{11}\}.\end{aligned}$$

Logo, o conjunto V_{11} induz uma nova componente fortemente conexa e, como não existe qualquer outro conjunto para analisar, podemos concluir que

$$\mathcal{C} = \{\{v_3\}, \{v_4, v_{12}\}, \{v_6, v_{10}\}, \{v_2, v_5, v_8\}, \{v_1, v_7, v_9, v_{11}\}\}$$

contém todos os subconjuntos de vértices que induzem componentes fortemente conexas. Observe-se (ver Figura 13.7) que as componentes fortemente conexas determinadas pelo algoritmo de Leifman constituem uma decomposição da estrutura do digrafo e todas contêm um ciclo orientado. \square

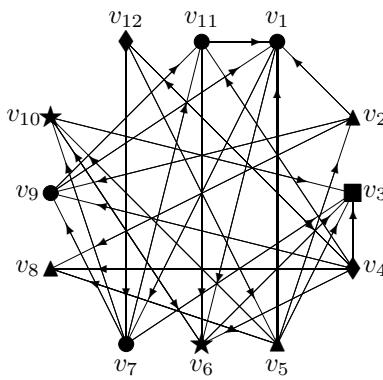


Figura 13.7: Componentes fortemente conexas de um digrafo (ver Exemplo 13.9), onde vértices de componentes distintas são representados por símbolos distintos.

13.6. Exercícios

- 13.1. Determine, utilizando algoritmo de Leifman, a componente fortemente conexa que contém o vértice v_6 do digrafo definido pela matriz de adjacência:

$$A_{\vec{G}} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

- 13.2. Mostre que se um grafo tem exatamente dois vértices de grau ímpar então existe um caminho entre deles.
- 13.3. Desenhe um grafo com cinco vértices que não contenha nenhum vértice de corte.
- 13.4. Mostre que um grafo G é conexo se e só se existe um passeio em G que contém todos os vértices.
- 13.5. Seja G um grafo tal que $\delta(G) = 1$ e seja $v \in V(G)$ um vértice de grau um. Mostre que G é conexo se e só se $G - v$ é conexo.
- 13.6. Mostre que se G é um grafo conexo e $e \in E(G)$ é uma aresta de G que está contida num ciclo de G , então $G - e$ é também conexo.
- 13.7. Sendo G um grafo conexo com pelo menos dois vértices, prove que existe um vértice v de G tal que o grafo $G - v$ é conexo. Adicionalmente, prove que se na afirmação anterior substituímos a palavra "vértice" por "aresta", a proposição continua verdadeira.
- 13.8. Mostre que um grafo simples é um ciclo se e só se é 2-regular, conexo e tem ordem não inferior a 2.
- 13.9. Seja G um grafo cujos vértices correspondem aos subconjuntos de um conjunto finito X e tal que dois vértices são adjacentes se e só se os correspondentes subconjuntos são equipotentes e não são disjuntos. Determine as componentes conexas de G e desenhe este grafo, para o caso particular de $X = \{1, 2, 3, 4\}$.
- 13.10. Seja G_k um grafo cujos vértices correspondem a sequências binárias de comprimento k e dois vértices são adjacentes se e só se as correspondentes sequências binárias têm distância de Hamming 2. Determine as componentes conexas de G_k e desenhe os grafos G_k , para $k = 1, 2, 3, 4$.
- 13.11. Mostre que cada grafo conexo com ordem ν contém pelo menos $\nu - 1$ arestas.
- 13.12. Sendo G um grafo simples não trivial, qual (ou quais) das seguintes afirmações é (são) verdadeira(s):
- (a) Se G é um grafo conexo, então cada subgrafo induzido é também conexo.
 - (b) Se G é um grafo conexo, então contém um subgrafo próprio não trivial que também é conexo.

- (c) Para cada $\nu \geq 2$, existe um grafo conexo G de ordem ν tal que cada um dos seus subgrafos induzidos é conexo.

13.13. Considerando um grafo G , prove a equivalência das seguintes proposições:

- (a) o grafo G é 2-aresta-conexo;
- (b) as arestas de G podem ser orientadas de modo que o digrafo obtido \vec{G} seja fortemente conexo.

13.14. Seja G um grafo 3-regular, então mostre que a vértice-conectividade é igual à aresta-conectividade.

13.15. Tendo em conta que um conjunto separador de um grafo G é um subconjunto de vértices $U \subset V(G)$ tal que $cc(G - U) > cc(G)$, prove que se G não tem um conjunto separador, então é um grafo completo.

13.16. Dado um grafo 2-conexo, G , e três vértices arbitrários distintos $u, v, w \in V(G)$, prove as seguinte afirmações:

- (a) Existe um caminho entre u e w que não contém v .
- (b) Existe um caminho entre u e w que contém v .

13.17. Determine todas as componentes conexas do grafo definido no Exercício 13.1, com recurso a um dos algoritmos de pesquisa em grafos.

13.18. Determine a componente conexa que contém o vértice v_1 (que corresponde à primeira linha e coluna) do grafo definido pela matriz de adjacência:

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

13.19. Demonstre que se G é um grafo simples, tal que $\delta(G) > \lfloor \frac{1}{2}\nu(G) \rfloor - 1$, então G é conexo.

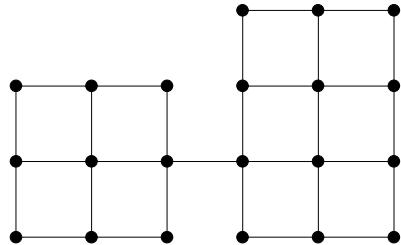
13.20. Demonstre que se G é um grafo conexo, tal que cada vértice de G tem grau par, então $cc(G - v) \leq \frac{1}{2}d_G(v)$.

13.21. Com recurso à pesquisa em profundidade, determine uma orientação das arestas do grafo de Petersen de tal forma que o digrafo obtido seja fortemente conexo.

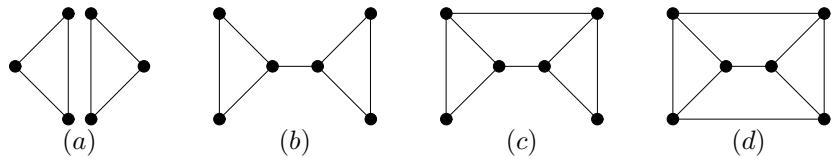
13.22. Represente um grafo G , 4-vértice-conexo e 5-aresta-conexo tal que $\delta(G) = 6$.

13.23. Determine a vértice-conexidade e a aresta-conexidade do grafo de Petersen.

- 13.24. Considerando o grafo representado na figura a seguir, mostre que não existe qualquer orientação das suas arestas que produza um digrafo fortemente conexo e determine uma aresta a acrescentar a este grafo, com a qual é possível obter uma orientação que produza um digrafo fortemente conexo.



- 13.25. Verifique qual (quais) dos seguintes grafos admite(m) uma orientação das arestas de tal forma que o digrafo obtido seja fortemente conexo.



14

Caminhos

Se a cada aresta (arco) de um grafo (digrafo) associarmos um número, ou seja, um *custo* ou *peso*, então o grafo (digrafo) designa-se por grafo (digrafo) com custos ou pesos nas arestas (nos arcos). Neste caso, o custo de um caminho é igual a soma dos custos das suas arestas (dos seus arcos). Observe-se que um grafo (digrafo) sem custos pode ser interpretado como um grafo (digrafo) com todos os custos iguais a 1. Como consequência, todos os algoritmos desenvolvidos para grafos (digrafos) com custos nas arestas (nos arcos) podem ser utilizados também para grafos (digrafos) sem custos. Em grafos (digrafos) com custos nas arestas (nos arcos), muitas vezes designamos os caminhos de custo mínimo por caminhos mais curtos.

Os problemas de determinação de caminhos mais curtos em grafos são muito comuns em aplicações práticas, por exemplo, em redes de transporte. Existem vários tipos de problemas de caminho mais curto, dos quais, neste capítulo, vamos analisar os mais frequentes.

14.1. Relações entre diâmetro, cintura e número de vértices

Vimos anteriormente que os conceitos métricos em grafos decorrem do conceito de caminho mais curto entre dois vértices ao qual está associada a noção de distância. Estamos agora em condições de introduzir outras noções, também associadas ao conceito de distância entre vértices, como são o caso das noções de *diâmetro*, *raio* e *centro* de um grafo. Alguns destes conceitos podem relacionar-se directamente entre si, com a regularidade do grafo ou com o seu número de vértices. Vamos analisar, detalhadamente, algumas destas relações.

Definição 14.1 (Excentricidade de um vértice). *Seja G um grafo e v um vértice, então a maior distância entre v e todos os outros vértices de G designa-se por excentricidade de v e denota-se por $e_G(v)$ ou $e(v)$. Mais formalmente,*

$$e(v) = \max_{u \in V(G)} \text{dist}_G(u, v).$$

Definição 14.2 (Diâmetro, raio, vértice central e centro de um grafo). *Dado um grafo G , a maior excentricidade dos seus vértices designa-se por diâmetro e denota-se por $\text{diam}(G)$. Por sua vez, a menor excentricidade dos vértices de G designa-se por raio e denota-se por $r(G)$, ou seja,*

$$\text{diam}(G) = \max_{u \in V(G)} e(u) \quad e \quad r(G) = \min_{v \in V(G)} e(v).$$

Cada vértice $v \in V(G)$ tal que $e(v) = r(G)$, designa-se por vértice central de G e o conjunto de todos os vértices centrais designa-se por centro de G .

Por outras palavras, o diâmetro de um grafo é igual à máxima distância entre os seus pares de vértices e um vértice é central se a sua distância ao vértice mais distante é mínima.

Exemplo 14.1. Vamos demonstrar que, dado um grafo arbitrário G , se verificam as desigualdades:

$$r(G) \leq \text{diam}(G) \leq 2r(G). \quad (14.1)$$

Solução. Das definições de diâmetro e de raio decorre, directamente, a desigualdade

$$r(G) \leq \text{diam}(G).$$

Uma vez que, para qualquer vértice $w \in V(G)$, $\text{dist}(u, v) \leq \text{dist}(u, w) + \text{dist}(w, v)$, sendo x um vértice central,

$$\begin{aligned} \text{diam}(G) &= \max\{\text{dist}_G(u, v) : u, v \in V(G)\} \\ &\leq \max\{\text{dist}_G(u, x) + \text{dist}_G(x, v) : u, v \in V(G)\} \\ &\leq \max\{\text{dist}_G(u, x) : u \in V(G)\} + \max\{\text{dist}_G(x, v) : v \in V(G)\} \\ &= 2r(G). \end{aligned}$$

Note-se que existem grafos G tais que $\text{diam}(G) = r(G)$ e grafos H para os quais $\text{diam}(H) = 2r(H)$, pelo que o majorante e o minorante das desigualdades (14.1) são atingidos. \square

Exemplo 14.2. Vamos determinar o diâmetro, o raio e a cintura dos seguintes grafos de ordem $\nu \geq 3$:

1. Grafo completo, K_ν .
2. Caminho com ν vértices (de comprimento $\nu - 1$), P_ν .
3. Ciclo de comprimento ν , C_ν .

Solução.

1. Pela definição de grafo completo, é claro que

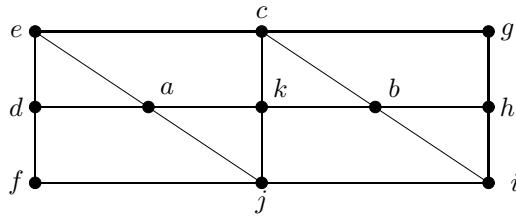
$$\forall_{u, v \in V(K_\nu)} \text{dist}_{K_\nu}(u, v) = 1.$$

Logo, $\text{diam}(K_\nu) = 1$ e $r(K_\nu) = 1$. Adicionalmente, tendo em conta que, para $\nu \geq 3$, K_ν contém um triângulo, $g(K_\nu) = 3$.

2. Os vértices mais afastados em P_ν são os vértices extremos que estão à distância $\nu - 1$, pelo que $\text{diam}(P_\nu) = \nu - 1$. Se ν é par, então os vértices centrais são os dois vértices adjacentes mais afastados dos vértices extremos, pelo que, neste caso, $r(P_\nu) = \frac{\nu}{2}$. Se ν é ímpar, existe um único vértice central que é o mais afastado dos vértices extremos, donde, neste caso, $r(P_\nu) = \frac{\nu-1}{2}$. Em ambos casos, $r(P_\nu) = \lfloor \frac{\nu}{2} \rfloor$. Finalmente, uma vez que P_ν não tem ciclos, podemos concluir que $g(P_\nu) = \infty$. \square
3. Neste caso todos os vértices têm a mesma excentricidade. Logo, se ν é par, então $\text{diam}(C_\nu) = r(C_\nu) = \frac{\nu}{2}$; caso contrário, $\text{diam}(C_\nu) = r(C_\nu) = \frac{\nu-1}{2}$. Em ambos casos, $\text{diam}(C_\nu) = r(C_\nu) = \lfloor \frac{\nu}{2} \rfloor$. Uma vez que C_ν tem um único ciclo de comprimento ν , podemos concluir que $g(C_\nu) = \nu$. \square

Exemplo 14.3. Considerando o grafo G representado na Figura 14.1 vamos determinar

1. a excentricidade do vértice f ;

Figura 14.1: Grafo G tal que $\text{diam}(G) = 4$.

2. todos os vértices de excentricidade máxima;

3. o centro de G .

Solução. Observe-se que G é o grafo definido no Exemplo 12.5.

1. Utilizando os valores da Tabela 12.1, vem que a excentricidade do vértice f é igual ao máximo valor na linha correspondente ao vértice f . Logo $e(f) = 4$.
2. De modo semelhante, utilizando os valores da Tabela 12.1 vem que $e(k) = 2$, $e(a) = e(b) = e(c) = e(e) = e(i) = e(j) = 3$ e $e(d) = e(f) = e(g) = e(h) = 4$. Logo, os vértices d , f , g e h têm excentricidade máxima.
3. Tenho em conta o item 2, apenas o vértice k tem excentricidade mínima. Logo, o centro deste grafo é constituído, unicamente, pelo vértice k . \square

Teorema 14.1. Se o grafo G contém um ciclo, então $g(G) \leq 2 \text{diam}(G) + 1$.

Demonstração. Seja C um ciclo de menor comprimento em G e suponha que $g(G) > 2 \text{diam}(G) + 1$, ou seja,

$$g(G) = \text{comp}(C) \geq 2 \text{diam}(G) + 2.$$

Então existem $x, y \in V(C)$ tais que $\text{dist}_C(x, y) = \text{diam}(G) + 1$. Uma vez que em G existe um caminho P , entre x e y cujo comprimento é não superior ao diâmetro, podemos concluir que P não é um subgrafo de C . Logo, em $P \cup C$ (e, consequentemente, em G) existe um ciclo C' tal que

$$\text{comp}(C') \leq \text{dist}_C(x, y) + \text{comp}(P) < 2 \text{dist}_C(x, y) \leq \text{comp}(C),$$

o que contraria a hipótese. \square

Teorema 14.2. Se G é um grafo conexo simples tal que $g(G) = 2 \text{diam}(G) + 1$, então G é regular.

Demonstração. Primeiramente vamos provar que (1) quaisquer dois vértices à distância $\text{diam}(G)$ têm o mesmo grau. Depois, com base neste facto, vamos provar que (2) todos os vértices de um ciclo C de comprimento $g(G)$ têm o mesmo grau e, posteriormente, que (3) todos os vértices não pertencentes a $V(C)$ têm o mesmo grau dos vértices em C .

- (1) Sejam $x, y \in V(G)$ tais que $\text{dist}_G(x, y) = \text{diam}(G) = d$ e seja P um caminho de comprimento d entre x e y . Seja $z \in N_G(y) \setminus V(P)$. Então $d = \text{dist}_G(x, y) \leq \text{dist}_G(x, z) + 1 \Leftrightarrow d - 1 \leq \text{dist}_G(x, z)$ e, consequentemente, $\text{dist}_G(x, z) = d$ (uma vez que $\text{dist}_G(x, z) = d - 1$ implica a existência de um ciclo em G de comprimento não superior a $2d$). Logo, qualquer que seja $z \in N_G(y) \setminus V(P)$ existe um único caminho entre x e z de comprimento d (caso contrário, ter-se-ia $g(G) \leq 2d$). Cada caminho deste tipo utiliza diferentes vizinhos de x e, consequentemente, x tem pelo menos tantos vizinhos quantos os vizinhos de y . Analogamente se conclui que y tem pelo menos tantos vizinhos quantos os vizinhos de x . Logo, podemos concluir que quaisquer dois vértices x e y à distância d têm exactamente o mesmo número de vizinhos.

- (2) Sendo C um ciclo de comprimento $2d + 1$, a partir de um vértice arbitrário $v \in V(C)$, determinando os dois vértices distintos de C à distância d de v , concluímos que ambos têm o grau de v . Assim, todos os vértices de C têm o mesmo grau.
- (3) Considerando um vértice arbitrário v fora de C , bem como o caminho de comprimento $i \leq d$ entre v e $u \in V(C)$, podemos concluir que existe em C um vértice w à distância $d - i$ de u e, consequentemente, à distância $\text{dist}_G(v, w) \leq d - i + i = d$. Porém, se $\text{dist}_G(v, w) < d$, então existe um ciclo de comprimento inferior a $2d$ o que é contraditório. Logo, v está à distância d de w e, consequentemente, tem o mesmo número de vizinhos de w .

Assim, fica provado que todos os vértices têm o mesmo grau. \square

Teorema 14.3. *Dado um grafo simples e conexo G e $k = \left\lfloor \frac{g(G)-1}{2} \right\rfloor$, verifica-se a desigualdade*

$$|V(G)| \geq 1 + \delta(G) \sum_{i=0}^{k-1} (\delta(G) - 1)^i. \quad (14.2)$$

Demonstração. Primeiramente, dado $x \in V(G)$, vamos provar, por indução sobre i , com $1 \leq i \leq k - 1$, que o número de vértices à distância i de x é, pelo menos, $\delta(G)(\delta(G) - 1)^{i-1}$, isto é,

$$|\{v \in V(G) : d_G(x, v) = i\}| \geq \delta(G)(\delta(G) - 1)^{i-1}.$$

O resultado é trivialmente verdadeiro para $i = 1$.

Suponha que o resultado é verdadeiro para $i = j$, com $1 \leq j < k - 1$. Se $v \in V(G)$ é tal que $\text{dist}_G(x, v) = j$ então (a) existe um único vizinho y de v à distância $j - 1$ de x e (b) nenhum vizinho à distância j , conforme a seguir se prova.

- (a) Suponha que existem dois vértices vizinhos de v à distância $j - 1$. Então existem dois caminhos distintos P' e P'' , entre x e cada um destes vizinhos, tais que $\text{comp}(P') = \text{comp}(P'') = j - 1 < k - 1$, cuja união com as arestas que os ligam a v contém um ciclo C tal que

$$\begin{aligned} \text{comp}(C) &\leq \text{comp}(P') + \text{comp}(P'') + 2 \\ &= 2j < 2k = 2 \left\lfloor \frac{g(G)-1}{2} \right\rfloor \leq g(G) - 1, \end{aligned}$$

o que é contraditório.

- (b) Suponha que existe um vértice z adjacente a v , à distância j de x . Então, tal como anteriormente, existem dois caminhos distintos, P' e P'' , entre x e v e entre x e z , respectivamente, cuja união com a aresta vz contém um ciclo C tal que

$$\begin{aligned} \text{comp}(C) &\leq \text{comp}(P') + \text{comp}(P'') + 1 \\ &= 2j + 1 < 2k = 2 \left\lfloor \frac{g(G)-1}{2} \right\rfloor \leq g(G) - 1, \end{aligned}$$

o que, mais uma vez, é contraditório.

Logo, para cada vértice v à distância j de x , existem pelo menos $\delta(G) - 1$ vértices adjacentes a v à distância $j + 1$ de x e um único vértice adjacente a v à distância $j - 1$ de x .

Analogamente se conclui que, para cada vértice y à distância $j + 1$ de x , existe um único vértice adjacente a y à distância j de x (dado que por hipótese $2(j+1) \leq 2k < g(G)$).

Uma vez que, por hipótese de indução, existem pelo menos $\delta(G)(\delta(G) - 1)^{j-1}$ vértices à distância j de x , conclui-se que existem, pelo menos,

$$\delta(G)(\delta(G) - 1)^{j-1}(\delta(G) - 1) = \delta(G)(\delta(G) - 1)^j$$

vértices à distância $j+1$. Consequentemente, tendo em conta que $\bigcup_{i=0}^k V_i \subseteq V(G)$, onde $V_i = \{v \in V(G) : \text{dist}_G(x, v) = i\}$, para $i = 0, \dots, k$, vem que

$$|V(G)| \geq |V_0| + |V_1| + |V_2| + \dots + |V_k| \geq 1 + \delta(G) \sum_{j=0}^{k-1} (\delta(G) - 1)^j.$$

□

Deste teorema decorre imediatamente que se $k = \left\lfloor \frac{\delta(G)-1}{2} \right\rfloor$ e $\delta(G) > 2$, então

$$|V(G)| \geq 1 + \delta(G) \frac{(\delta(G) - 1)^k - 1}{\delta(G) - 2}. \quad (14.3)$$

Teorema 14.4. Se G é um grafo simples, conexo, com $r = r(G) > 0$, então

$$|V(G)| \leq 1 + \Delta(G) \sum_{i=0}^{r-1} (\Delta(G) - 1)^i.$$

Demonstração. Seja $v \in V(G)$ um vértice central em G e seja

$$V_i = \{x \in V(G) : \text{dist}_G(v, x) = i\},$$

para $i = 0, \dots, r$. Então $V(G) = \bigcup_{i=0}^r V_i$ e $V_p \cap V_q = \emptyset$ para $p \neq q$, pelo que $|V(G)| = \sum_{i=0}^r |V_i|$. Por outro lado, sabe-se que

$$\begin{aligned} |V_0| &= 1, \\ |V_1| &\leq \Delta, \\ |V_2| &\leq \Delta|V_1| - |V_1| = |V_1|(\Delta - 1) \leq \Delta(\Delta - 1), \\ |V_3| &\leq \Delta|V_2| - |V_2| = |V_2|(\Delta - 1) \leq \Delta(\Delta - 1)^2, \\ &\vdots && \vdots \\ |V_r| &\leq \Delta|V_{r-1}| - |V_{r-1}| = |V_{r-1}|(\Delta - 1) \leq \Delta(\Delta - 1)^{r-1}, \end{aligned}$$

onde vem

$$|V(G)| = \sum_{i=0}^{r-1} |V_i| \leq 1 + \Delta \sum_{i=0}^{r-1} (\Delta - 1)^i.$$

□

Como consequência imediata deste teorema, sendo $\text{diam}(G) = d$ e tendo em conta (14.1), conclui-se a desigualdade

$$|V(G)| \leq 1 + \Delta \sum_{i=0}^{d-1} (\Delta - 1)^i, \quad (14.4)$$

a qual, para $\Delta(G) > 2$, pode tomar a forma:

$$|V(G)| \leq 1 + \Delta \frac{(\Delta - 1)^d - 1}{\Delta - 2}.$$

Tendo em conta as desigualdades (14.3) e (14.1), se $\text{diam}(G) \leq d$, $k = \left\lfloor \frac{g(G)-1}{2} \right\rfloor$ e $\delta(G) > 2$, então

$$1 + \delta \frac{(\delta - 1)^k - 1}{\delta - 2} \leq |V(G)| \leq 1 + \Delta \frac{(\Delta - 1)^d - 1}{\Delta - 2}. \quad (14.5)$$

Como exemplo de aplicação, considerando o grafo cúbico G representado na Figura 14.2, onde $g(G) = 5$ (pelo que $k = \left\lfloor \frac{g(G)-1}{2} \right\rfloor = 2$) e $\text{diam}(G) = 3$, vem

$$10 = 1 + 3 \frac{(3-1)^2 - 1}{3-2} \leq |V(G)| \leq 1 + 3 \frac{(3-1)^3 - 1}{3-2} = 22.$$

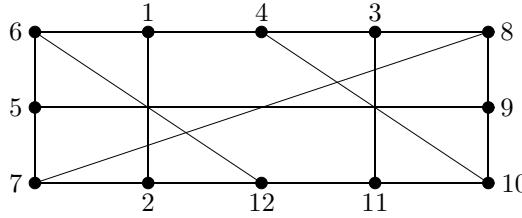


Figura 14.2: Grafo cúbico G tal que $g(G) = 5$ e $\text{diam}(G) = 3$.

Teorema 14.5. *Sendo G um grafo simples, conexo, de ordem $\nu > 2$, com diâmetro $d \in \mathbb{N}$, a desigualdade (14.4) verifica-se na forma de igualdade se e só se G é regular e $g(G) = 2d + 1$.*

Demonstração. Seja G um grafo conexo tal que $\text{diam}(G) = d$.

Se G não é Δ -regular então, tendo em conta a demonstração do Teorema 14.4, é fácil concluir que a desigualdade (14.4) não se verifica na forma de igualdade (deve observar-se que a escolha do diâmetro em vez do raio, permite que o vértice v do conjunto singular inicial V_0 seja tal que $d_G(v) < \Delta(G)$). Por outro lado, uma vez que G tem ordem $\nu > 2$, se G é Δ -regular então contém um ciclo, donde, pelo Teorema 14.1, $g(G) \neq 2d + 1 \Rightarrow g(G) < 2d + 1$. Assim, suponha-se que G é Δ -regular, $g(G) \neq 2d + 1$ e que, mesmo assim, a desigualdade (14.4) se verifica na forma de igualdade. Nestas condições, tendo em conta o processo construtivo do Teorema 14.4, podemos concluir que $|V_i| = (\Delta - 1)|V_{i-1}|$, para $i = 1, \dots, d$. Porém, uma vez que existe em G um ciclo C cujo comprimento é não superior a $2d$, começando com o conjunto singular V_0 formado por um vértice v pertencente ao ciclo C , existe um conjunto V_k , com $1 \leq k \leq d$, que ou tem dois vértices adjacentes (conforme a Figura 14.3-(A) exemplifica) ou tem um vértice $z \in V_k$ que é um vizinho comum a dois vértices distintos $x, y \in V_{k-1}$ (conforme Figura 14.3-(B) exemplifica). Como consequência, ou $|V_{k+1}| < (\Delta - 1)|V_k|$ ou $|V_k| < (\Delta - 1)|V_{k-1}|$ o que, em qualquer caso, constitui uma contradição.

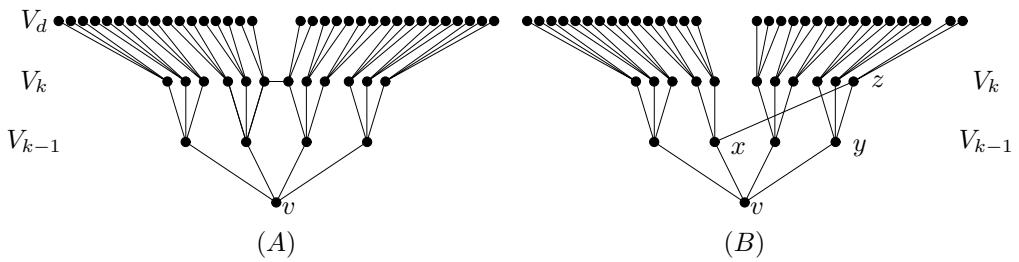


Figura 14.3: Processo construtivo utilizado na demonstração do Teorema 14.4

Reciprocamente, suponha agora que G é Δ -regular e $g(G) = 2d + 1$. Nestas condições, fazendo $k = \left\lfloor \frac{g(G)-1}{2} \right\rfloor$, obtém-se $k = d$ e, dado que $\delta(G) = \Delta(G) = \Delta$, combinando (14.4) com (14.2), vem

$$1 + \Delta \sum_{i=0}^{d-1} (\Delta - 1)^i \leq |V(G)| \leq 1 + \Delta \sum_{i=0}^{d-1} (\Delta - 1)^i,$$

ou seja,

$$|V(G)| = 1 + \Delta \sum_{i=0}^{d-1} (\Delta - 1)^i. \quad (14.6) \quad \square$$

Os grafos simples, conexos, não triviais, para os quais a desigualdade (14.4) se verifica na forma de igualdade, designam-se por *grafos de Moore*. Como consequência imediata do Teorema 14.5, os grafos de Moore de ordem superior a 2 são grafos simples, conexos, regulares, com cintura $2d + 1$, onde d denota o diâmetro. Por outro lado, de acordo com os Teoremas 14.2 e 14.5, todo o grafo simples, conexo, com cintura $2d + 1$, onde d denota o diâmetro, é um grafo de Moore. Na Figura 14.4 representa-se um exemplo de grafo de Moore. Note-se que todos os grafos simples, completos, de ordem superior a um, são grafos de Moore e, com exceção destes, para além do grafo de Petersen¹, representado na Figura 14.4, apenas se conhecem mais dois, sendo um deles o grafo 2-regular de ordem 5 e o outro o grafo 7-regular de ordem 50, conhecido por grafo de Hoffman-Singleton. Suspeita-se da existência de apenas mais um grafo de Moore que, a existir, é 57-regular e tem ordem 3.250. Com exceção dos grafos completos K_n , cujo diâmetro é 1, todos estes grafos G têm diâmetro $d = 2$ donde, tendo em conta (14.6), $|V(G)| = \Delta^2 + 1$.

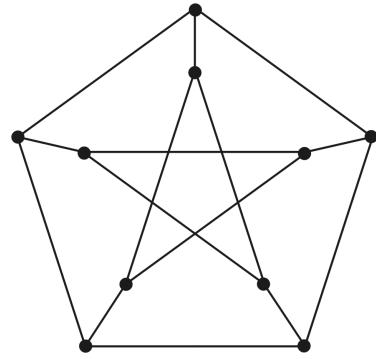


Figura 14.4: Exemplo de um grafo de Moore (conhecido por grafo de Petersen).

14.2. Pesquisa em largura em grafos sem custos nas arestas

A determinação do comprimento de um caminho mais curto entre dois vértices fixos s e t , num grafo sem custos nas arestas (ou, equivalentemente, com custos idênticos em todas as arestas) pode obter-se com recurso ao algoritmo de pesquisa em largura (BFS), conforme a seguir se indica.

Descrição do algoritmo.

1. Marcar o vértice s com 0 e iniciar i com 0 ($i \leftarrow 0$).
 2. Todos os vértices vizinhos dos vértices marcados com i (ou sucessores, no caso orientado), ainda sem qualquer marca, são marcados com $i + 1$.
 3. $i \leftarrow i + 1$ e se existem vértices marcados com i passar ao passo 2.
-

¹O grafo de Petersen é um caso particular, $K(5, 2)$, dos grafos de Kneser, $K(p, q)$, definidos para $p \geq 2q$, cujos vértices denotam q -subconjuntos de um conjunto de cardinalidade p , nos quais, dois vértices são adjacentes se e só se os correspondentes subconjuntos são disjuntos. Deve observar-se ainda que o grafo de Petersen corresponde ao complementar de $L(K_5)$.

Mais precisamente, este procedimento é apresentado com recurso ao pseudocódigo Algoritmo 14.1 DISTBFS. Neste algoritmo, a tabela d contém todas as distâncias já determinadas (isto é, $d[i] = \text{dist}(s, v_i)$). Dentro do ciclo **repetir**, P é o conjunto dos vértices a uma distância de s igual a $k - 1$ e N é o conjunto dos vértices até ao momento analisados que estão a uma distância de s igual a k . O algoritmo termina quando se determina a distância entre s e t (ou seja, quando $w = t$) ou quando se determinam todas as distâncias entre s e os vértices da componente que contém s mas não contém t (neste caso, $N = \emptyset$).

Algoritmo 14.1: DISTBFS(G, s, t)

```

para todo  $v \in V(G)$  fazer  $d[v] \leftarrow \infty$ 
 $d[s] \leftarrow 0$ ;  $N \leftarrow \{s\}$ ;  $k \leftarrow 0$ 
repetir
     $P \leftarrow N$ ;  $N \leftarrow \emptyset$ ;  $k \leftarrow k + 1$ 
    para todo  $v \in P$  fazer para todo  $w \in N_G(v)$ 
        fazer se  $d[w] = \infty$  então  $\begin{cases} d[w] \leftarrow k; N \leftarrow N \cup \{w\} \\ \text{se } w = t \text{ então interromper} \end{cases}$ 
    até  $N = \emptyset$ 
    devolver  $(d[t])$ 
```

Já sabemos que a complexidade computacional deste algoritmo é igual a $\mathcal{O}(\nu + \varepsilon)$.

Atenção! Note-se que a simples modificação deste algoritmo, provocada pela eliminação da instrução condicional

se $w = t$ então interromper

implica a determinação de todas as distâncias entre s e os restantes vértices. Uma tal modificação pode ser utilizada, por exemplo, para se determinar a excentricidade de um vértice s .

Exemplo 14.4. Considerando o grafo G , definido pela matriz de adjacência

$$A_G = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 & v_9 \\ v_1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ v_2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ v_3 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ v_4 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ v_5 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ v_6 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ v_7 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ v_8 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ v_9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

vamos determinar $\text{dist}(v_1, v_9)$, com recurso ao algoritmo DISTBFS.

k	$d[v_1]$	$d[v_2]$	$d[v_3]$	$d[v_4]$	$d[v_5]$	$d[v_6]$	$d[v_7]$	$d[v_8]$	$d[v_9]$
0	0	∞							
1	0	1	∞						
2	0	1	2	∞	∞	2	∞	∞	∞
3	0	1	2	3	3	2	∞	∞	∞
4	0	1	2	3	3	2	4	4	∞
5	0	1	2	3	3	2	4	4	5

Tabela 14.1: Determinação de $\text{dist}_G(v_1, v_9)$, por aplicação ao grafo G representado na Figura 14.5, do algoritmo DISTBFS.

Solução. Na Tabela 14.1 apresentam-se os valores que se vão obtendo ao longo da execução do algoritmo DIST-BFS. Note-se que os valores obtidos (em cada iteração k) para os vértices do conjunto P aparecem a negrito e que, a partir desta tabela, se obtém

$$\text{dist}(v_1, v_9) = 5.$$

O grafo deste exemplo está representado na Figura 14.5.

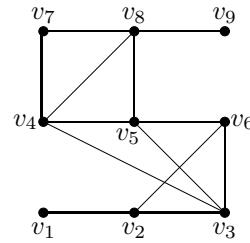


Figura 14.5: Grafo G definido pela matriz de adjacência A_G do Exemplo 14.4. \square

14.3. Custos não negativos – algoritmo de Dijkstra

Recorde-se que para grafos com custos ou pesos nas arestas, o custo de um caminho é igual à soma dos custos ou pesos das suas arestas e o mesmo se passa no caso de grafos orientados com custos (ou pesos) nos arcos. Em certas aplicações, porém, os custos referem-se a distâncias entre vértices, pelo que, algumas vezes, designa-se o custo de um caminho como sendo o seu comprimento. Assim, neste contexto, o caminho de custo mínimo ou o caminho mais curto não é necessariamente o que tem menor número de arestas no caso dos grafos, ou arcos no caso dos digrafos.

Por exemplo, no grafo representado na Figura 14.6, existem três caminhos entre os vértices v_1 e v_2 , cujos custos são os apresentados na Tabela 14.2. Conforme se pode verificar, de entre estes caminhos, o caminho de custo mínimo é o que tem maior número de arestas.

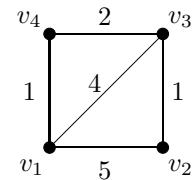


Figura 14.6: Grafo com custos nas arestas.

caminho	número de arestas	soma de pesos
v_1v_2	1	5
$v_1v_3v_2$	2	5
$v_1v_4v_3v_2$	3	4

Tabela 14.2: Comprimentos dos caminhos entre os vértices v_1 e v_2 do grafo da Figura 14.6.

Um grafo simples com custos nas arestas representa-se pelo terno $G = (V, E, W)$, onde $W = (w_{ij})$ denota a matriz de custos. Nesta matriz, a entrada w_{ij} corresponde ao custo da aresta ij , se uma tal aresta existe, ou $w_{ij} = \infty$ se $ij \notin E(G)$. Adicionalmente, assume-se que $w_{ii} = 0$ para cada i . Deste modo, podemos lidar com o grafo como se tratasse de um grafo completo, no qual as arestas com custo infinito correspondem a arestas ausentes no grafo original. Por exemplo, o grafo representado na Figura 14.6 tem como matriz de custos a matriz:

$$W = \begin{pmatrix} 0 & 5 & 4 & 1 \\ 5 & 0 & 1 & \infty \\ 4 & 1 & 0 & 2 \\ 1 & \infty & 2 & 0 \end{pmatrix}.$$

Quando todos os custos das arestas são não negativos, o algoritmo que frequentemente mais se utiliza na determinação de um caminho de custo mínimo entre dois vértices s e t é o *algoritmo de Dijkstra*². A ideia básica deste algoritmo consiste em agrupar num conjunto, sucessivamente mais

²Edsger W. Dijkstra (1930–2002) foi um informático holandês.

alargado, os vértices à menor distância de s até se incluir nesse conjunto o vértice t , marcando-se temporariamente os vértices que no passo corrente se consideram mais próximos de s e mudando-se a marca temporária de um vértice v para marca permanente quando se obtém o caminho mais curto entre s e v . Na descrição formal deste algoritmo vamos utilizar a seguinte notação:

- $\text{Marca}[v]$ – comprimento do caminho mais curto entre s e v de entre os caminhos já determinados;
 - $\text{Antecessor}[v]$ – antecessor do vértice v no caminho mais curto entre s e v de entre os já determinados;
 - Temporários – conjunto dos vértices com marca temporária;
 - z – vértice com menor marca temporária corrente, a qual vai passar a marca permanente.
-

Descrição do algoritmo de Dijkstra.

1. Inicialização das variáveis. Marcar inicialmente o vértice s com a marca permanente 0 (uma vez que $\text{dist}(s, s) = 0$) e marcar todos os restantes vértices com a marca temporária ∞ , ou seja, $\text{Marca}[s] \leftarrow 0$, $\text{Marca}[v] \leftarrow \infty$, para $v \neq s$, $\text{Temporários} \leftarrow V(G) \setminus \{s\}$ e $z \leftarrow s$.
2. Para cada vértice v que não tenha marca permanente determinar uma nova marca, conforme se indica:

$$\text{Marca}[v] = \begin{cases} \text{Marca}[z] + w_{zv}, & \text{se } \text{Marca}[v] > \text{Marca}[z] + w_{zv}, \\ \text{Marca}[v], & \text{se } \text{Marca}[v] \leq \text{Marca}[z] + w_{zv}. \end{cases}$$

Observe-se que a desigualdade $\text{Marca}[v] > \text{Marca}[z] + w_{zv}$, significa que o caminho mais curto entre s e v , de entre os caminhos já determinados, passa pelo vértice z , ou seja, é o definido pelo caminho- (s, z) mais curto, ao qual se junta a aresta (ou arco) zv . Neste caso, o antecessor de v é z , ou seja, $\text{Antecessor}[v] \leftarrow z$.

3. Determinar um novo vértice z de marca mínima, de entre todos os vértices com marca temporária. Mudar a marca de z para marca permanente, ou seja, $\text{Temporários} \leftarrow \text{Temporários} \setminus \{z\}$.
4. Se $z \neq t$, então voltar ao passo 2.
5. FIM — o comprimento de um caminho mais curto entre s e t ($\text{dist}(s, t)$) é igual a $\text{Marca}[t]$ e este caminho é o definido pela sequência de vértices

$$(s, \dots, \text{Antecessor}[\text{Antecessor}[t]], \text{Antecessor}[t], t).$$

Segue-se um teorema que estabelece convergência do algoritmo de Dijkstra num número finito de passos em grafos com pesos não negativos nas arestas.

Teorema 14.6. *Dado um grafo simples, conexo G , dois vértices $s, t \in V(G)$ e uma matriz de custos W , o algoritmo de Dijkstra determina, num número finito de passos, o caminho mais curto (ou custo mínimo) entre s e t .*

Demonstração. Denotando por T^k o subconjunto de vértices com marca temporária na k -ésima execução do passo 2 do algoritmo, com $T^1 = V(G) \setminus \{s\}$, e tendo em conta que no passo 3 se verifica o decréscimo $|T^{k+1}| \leftarrow |T^k| - 1$, é claro que o algoritmo termina num número finito de passos. Logo, resta provar que $\text{Marca}[t]$ corresponde à distância entre s e t (note-se ainda que a função $\text{Antecessor}[z]$ determina um ou o respectivo caminho mais curto entre s e t). Vamos provar,

por indução sobre o número k de vértices incluídos no subconjunto com marcas permanentes, que $\forall z \in V(G) \setminus T^k \quad d_G(s, z) = \text{Marca}[z]$.

Durante a execução do passo 2, o conjunto de vértices $V(G)$ está partido em dois subconjuntos, o subconjunto com marcas temporárias T^k e o subconjunto com marcas permanentes $V(G) \setminus T^k$. Vamos supor que $\forall z \in V(G) \setminus T^k \quad \text{Marca}[z] = d_G(s, z)$ e ainda que para todo o vértice $y \in T^k$, $\text{Marca}[y]$ é o comprimento de um caminho mais curto entre s e y de entre os caminhos onde s e os vértices intermédios têm marca permanente (ou seja, pertencem ao subconjunto $V(G) \setminus T^k$). É imediato que estas propriedades se verificam para $k = 1$. Então, para $k < \nu(G)$, sendo $z \in T^k$ tal que $\text{Marca}[z] = \min\{M[y] : y \in T^k\}$, qualquer caminho entre s e z que não contenha apenas vértices com marca permanente é da forma $P = s, x_1, \dots, x_p, y_1, \dots, y_q, z$, onde $\{s, x_1, \dots, x_p\} \subseteq V(G) \setminus T^k$ e $\{y_1, \dots, y_q, z\} \subseteq T^k$. Logo, o comprimento do caminho P é $\text{comp}(P) = \text{Marca}[y_1] + \sum_{e \in E(P')} W(e)$, onde $P' = y_1, \dots, y_q, z$ e, sendo $e = ij$, $W(e) = w_{ij}$. Dado que $\text{Marca}[z] \leq \text{Marca}[y_1]$ e $\sum_{e \in E(P')} W(e) \geq 0$, podemos concluir que $\text{Marca}[z] \leq \text{Marca}[y_1] + \text{comp}(P') = \text{comp}(P)$, ou seja, $\text{Marca}[z] = d_G(s, z)$. Por outro lado, tendo em conta a actualização de $\text{Marca}[y]$ efectuada pelo algoritmo, vamos considerar as duas situações mutuamente exclusivas:

1. Se $zy \notin E(G)$, então temos dois subcasos:

- 1.1 $\text{Marca}[y] = \infty$ e neste caso não existe qualquer caminho entre s e y cujos vértices intermédios pertencem unicamente a $V(G) \setminus T^k \cup \{z\}$, permanecendo $\text{Marca}[y]$ com o mesmo valor,
- 1.2 ou $\text{Marca}[y] < \infty$ e neste caso, embora exista pelo menos um caminho entre s e y cujos vértices intermédios pertencem a $V(G) \setminus T^k \cup \{z\}$, todos eles utilizam unicamente vértices de $V(G) \setminus T^k$, pelo que a inclusão de z nos vértices com marca permanente não veio alterar a minimalidade de $\text{Marca}[y]$ em relação ao comprimento dos caminhos cujos vértices intermédios estão em $V(G) \setminus T^k \cup \{z\}$.

2. Se $zy \in E(G)$, então temos novamente dois subcasos:

- 2.1 $\text{Marca}[y] \leq \text{Marca}[z] + w_{zy}$, o que significa que o comprimento do caminho de menor comprimento de entre os caminhos entre s e y cujos vértices intermédios estão em $V(G) \setminus T^k$ é não superior ao comprimento de qualquer caminho entre s e y cujos vértices intermédios estão em $V(G) \setminus T^k \cup \{z\}$ (uma vez que a possibilidade de passar por z não traz qualquer redução),
- 2.2 $\text{Marca}[y] > \text{Marca}[z] + w_{zy}$, o que significa que existe um caminho entre s e y cujos vértices intermédios estão unicamente em $V(G) \setminus T^k \cup \{z\}$ e cujo comprimento, $\text{Marca}[z] + w_{zy}$, é o menor possível de entre os caminhos cujos vértices intermédios estão em $V(G) \setminus T^k \cup \{z\}$.

□

Mais formalmente, segue-se o pseudocódigo, Algoritmo 14.2 DIJKSTRA, que descreve este algoritmo. **Atenção!** Mudando o passo 4 (da descrição informal) deste algoritmo para:

"4. Se $\text{Temporários} \neq \emptyset$, então voltar ao passo 2."

ou, de modo equivalente, mudando no pseudocódigo, Algoritmo 14.2, até $x = t$ para

até $\text{Temporários} = \emptyset$

a nova versão do algoritmo de Dijkstra determina os caminhos mais curtos entre s e todos os restantes vértices do grafo.

Algoritmo 14.2: DIJKSTRA($G = (V, E, W), s, t$)

```

para todo  $v \in V$  fazer  $Marca[v] \leftarrow \infty$ ;  $Antecessor[v] \leftarrow 0$ 
 $Marca[s] \leftarrow 0$ ;  $Temporários \leftarrow V \setminus \{s\}$ ;  $z \leftarrow s$ 
repetir
     $M \leftarrow \infty$ 
    para todo  $u \in Temporários$ 
        fazer  $\begin{cases} \text{se } Marca[u] > Marca[z] + W[z, u] \text{ então } \begin{cases} Marca[u] \leftarrow Marca[z] + W[z, u] \\ Antecessor[u] \leftarrow z \end{cases} \\ \text{se } Marca[u] \leq M \text{ então } x \leftarrow u; M \leftarrow Marca[u] \end{cases}$ 
         $Temporários \leftarrow Temporários \setminus \{x\}$ ;  $z \leftarrow x$ 
    até  $x = t$ 
devolver ( $Marca[t]$ )

```

Exemplo 14.5. Utilizando o algoritmo de Dijkstra, vamos determinar um caminho mais curto (e a respectiva distância) entre os vértices v_5 e v_8 do grafo definido pela matriz de distâncias:

$$W = \begin{pmatrix} 0 & 12 & \infty & \infty & 12 & \infty & \infty & \infty \\ 12 & 0 & 13 & \infty & 12 & 14 & 15 & \infty \\ \infty & 13 & 0 & 13 & \infty & \infty & 11 & 15 \\ \infty & \infty & 13 & 0 & \infty & \infty & \infty & 11 \\ 12 & 12 & \infty & \infty & 0 & 15 & \infty & \infty \\ \infty & 14 & \infty & \infty & 15 & 0 & 13 & \infty \\ \infty & 15 & 11 & \infty & \infty & 13 & 0 & 12 \\ \infty & \infty & 15 & 11 & \infty & \infty & 12 & 0 \end{pmatrix}.$$

Solução. A Tabela 14.3 apresenta os valores obtidos durante a aplicação do algoritmo de Dijkstra em cada um dos respectivos passos. Note-se que nesta tabela, para cada vértice v , em cada passo determinamos um par

$$(Marca[v], Antecessor[v]),$$

onde $Marca[v]$ corresponde à distância corrente ao vértice inicial que aparece a negrito quando passa a permanente. Analisando a tabela, conclui-se que $dist(v_5, v_8) = 39$ e que o caminho- (v_5, v_8) mais curto (possivelmente não único) é o determinado pela sequência de vértices $v_5v_2v_7v_8$. \square

v_5	v_1	v_2	v_3	v_4	v_6	v_7	v_8
(0, -)	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$
(12, v₅)	$(12, v_5)$	$(\infty, -)$	$(\infty, -)$	$(15, v_5)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$
(12, v₅)	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$	$(15, v_5)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$
		$(25, v_2)$	$(\infty, -)$	(15, v₅)	$(27, v_2)$	$(\infty, -)$	
		(25, v₂)	$(\infty, -)$		$(27, v_2)$	$(\infty, -)$	
			$(38, v_3)$		(27, v₂)	$(40, v_3)$	
			(38, v₃)			$(39, v_7)$	
						(39, v₇)	

Tabela 14.3: Determinação de um caminho mais curto entre os vértices v_5 e v_8 , por aplicação do algoritmo de Dijkstra.

Observe-se que o ciclo exterior **repetir** do algoritmo de Dijkstra é executado não mais do que $\nu - 1$ vezes (uma vez que, em cada execução, um dos vértices com marca temporária passa a ter marca permanente e, consequentemente, no pior caso, o vértice t é o último vértice a obter uma

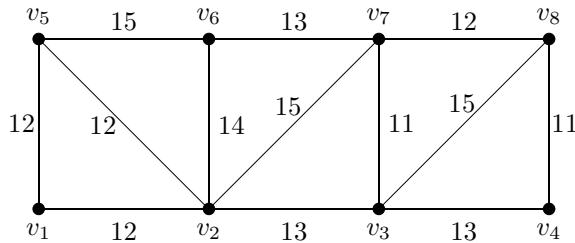


Figura 14.7: Grafo do Exemplo 14.5.

marca permanente). Dado que cada execução do conjunto dos passos que constituem o ciclo exterior corresponde a $\mathcal{O}(\nu)$ operações, podemos concluir que a complexidade computacional do algoritmo de Dijkstra, em ambas as versões – para a determinação de $\text{dist}(s, t)$ e para a determinação das distâncias entre s e os restantes vértices – é igual a $\mathcal{O}(\nu^2)$.

Exemplo 14.6. Com recurso ao algoritmo de Dijkstra, vamos determinar um caminho mais curto (e a respectiva distância) entre Aveiro e Vila Real, utilizando o mapa de Portugal representado na Figura 14.8.

Solução. A Tabela 14.4 apresenta parte da execução do algoritmo de Dijkstra para este caso. Observe que, após quatro iterações, a distância entre Aveiro e Vila Real é constante. Logo, esta distância (184 km) é a que corresponde ao caminho mais curto entre Aveiro e Vila Real, ou seja, ao comprimento do caminho: Aveiro – Porto – Vila Real. \square

C	FF	P	V	L	VR	G	B	VC
(58, A)	(64, A)	(68, A)	(95, A)	(∞ , -)				
(58, A)	(64, A)	(68, A)	(95, A)	(125, C)	(∞ , -)			
(58, A)	(64, A)	(68, A)	(95, A)	(118, FF)	(∞ , -)			
(58, A)	(64, A)	(68, A)	(95, A)	(118, FF)	(184, P)	(117, P)	(121, P)	(139, P)
...
(58, A)	(64, A)	(68, A)	(95, A)	(118, FF)	(184, P)	(117, P)	(121, P)	(139, P)

Tabela 14.4: Determinação de um caminho mais curto entre Aveiro e Vila Real (ver Exemplo 14.6), onde A=Aveiro, C=Coimbra, FF=Figueira da Foz, V=Viseu, L=Leria, VR=Vila Real, G=Guimarães, B=Braga, VC=Viana do Castelo.

Exemplo 14.7. Vamos determinar excentricidade de Lisboa, utilizando o mapa de Portugal representado na Figura 14.8.

Solução. Por aplicação do algoritmo de Dijkstra modificado, obtém-se as distâncias entre Lisboa e todas as outras cidades de Portugal. Na Tabela 14.3 representa-se parte da execução do algoritmo de Dijkstra, para este caso. Deve observar-se que a excentricidade de Lisboa é a maior das distâncias que a separa das restantes cidades, ou seja, é a distância entre Lisboa e Bragança. Logo, $e(\text{Lisboa}) = \text{dist}(\text{Lisboa}, \text{Bragança}) = 548$ km. \square

Exemplo 14.8. Vamos determinar o diâmetro, o raio e a cidade central de Portugal, a partir do grafo representado na Figura 14.8.

Solução. Com um procedimento semelhante ao utilizado no Exemplo 14.7, vamos determinar as excentricidades de todas as cidades representadas na Figura 14.8:

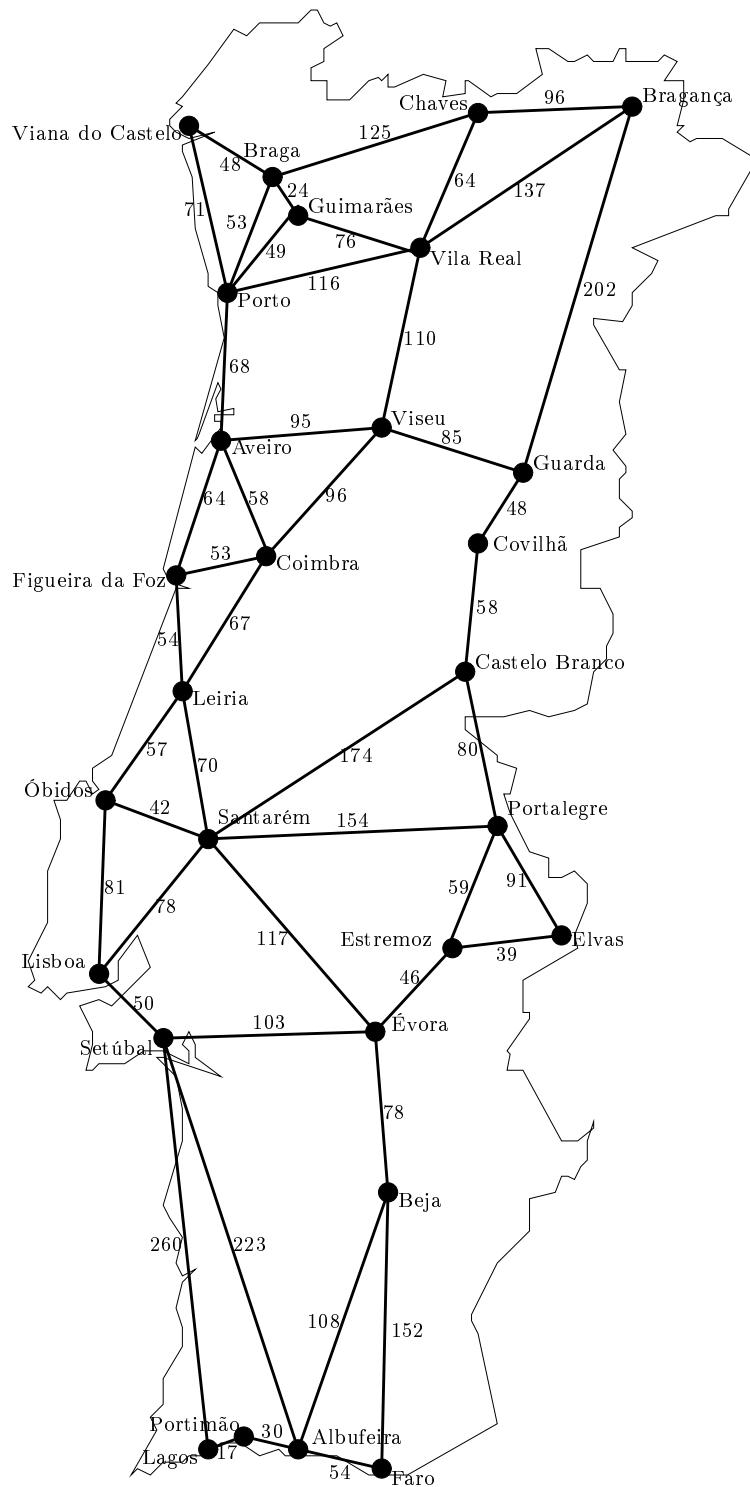


Figura 14.8: Mapa de Portugal com indicação das ligações entre as principais cidades e respectivas distâncias.

Ó	Sa	Se	É	A	La	Le	CB	Po
(81, L)	(78, L)	(50, L)	(∞ , -)					
(81, L)	(78 , L)	(50 , L)	(153, Se)	(273, Se)	(310, Se)	(∞ , -)	(∞ , -)	(∞ , -)
(81 , L)	(78 , L)	(50 , L)	(153, Se)	(273, Se)	(310, Se)	(148, Sa)	(252, Sa)	(232, Sa)
...
(81, L)	(78 , L)	(50 , L)	(153 , Se)	(273 , Se)	(310 , Se)	(148 , Sa)	(252 , Sa)	(232 , Sa)

Tabela 14.5: Determinação da excentricidade de Lisboa (ver Exemplo 14.7), onde L=Lisboa, Sa=Santarém, Ó=Óbidos, Se=Setúbal, É=Évora, A=Albufeira, La=Lagos, Le=Leiria, CB=Castelo Branco e Po=Portalegre.

$$\begin{aligned}
 e(\text{Albufeira}) &= \text{dist}(\text{Albufeira}, \text{Chaves}) = 710 \text{ km}, \\
 e(\text{Aveiro}) &= \text{dist}(\text{Aveiro}, \text{Lagos}) = 538 \text{ km}, \\
 e(\text{Beja}) &= \text{dist}(\text{Beja}, \text{Chaves}) = 602 \text{ km}, \\
 e(\text{Braga}) &= \text{dist}(\text{Braga}, \text{Lagos}) = 659 \text{ km}, \\
 e(\text{Bragança}) &= \text{dist}(\text{Bragança}, \text{Lagos}) = 726 \text{ km}, \\
 &\dots \quad \dots \quad \dots \\
 e(\text{Viseu}) &= \text{dist}(\text{Viseu}, \text{Lagos}) = 583 \text{ km}.
 \end{aligned}$$

Considerando o diâmetro de Portugal como a maior das excentricidades das cidades representadas no mapa, vem

$$\text{diam}(\text{Portugal}) = e(\text{Chaves}) = e(\text{Lagos}) = \text{dist}(\text{Chaves}, \text{Lagos}) = 757 \text{ km}.$$

Por sua vez, considerando o raio de Portugal como a menor das excentricidades das cidades representadas no mapa, vem

$$r(\text{Portugal}) = e(\text{Leiria}) = \text{dist}(\text{Leiria}, \text{Lagos}) = 420 \text{ km}.$$

Como consequência, podemos concluir que Leiria é a cidade central de Portugal. \square

Observe-se que, nos Exemplos 14.6–14.8, os resultados obtidos dependem do mapa considerado. Com efeito, utilizando outro conjunto de cidades ou outro conjunto de ligações, os resultados podem ser diferentes.

A determinação de um ciclo de comprimento mínimo de um grafo simples G (ou seja, um ciclo cujo comprimento é igual a $g(G)$), pode fazer-se com recurso à determinação, para cada aresta $uv \in E(G)$, de um caminho mais curto entre os vértices u e v no grafo $G - uv$. Uma vez obtido um tal caminho, juntando-lhe a aresta uv fica determinado um ciclo de comprimento mínimo de entre todos os ciclos que contêm a aresta uv , C_{uv} . Logo, um ciclo de comprimento mínimo é um ciclo C tal que

$$\text{comp}(C) = \min\{\text{comp}(C_{uv}) : uv \in E(G)\}.$$

14.4. Custos arbitrários – algoritmo de Bellman-Ford

Quando alguns dos custos das arestas (arcos) são negativos, o algoritmo de Dijkstra não funciona correctamente. Com efeito, no procedimento de marcação de vértices, assume-se que o comprimento de um caminho nunca é inferior ao comprimento de um subcaminho com menos arestas, o que pode ocorrer no caso de se considerarem arestas com custos negativos. Para resolver este problema, Bellman³ propôs as seguintes alterações ao algoritmo de Dijkstra:

³Richard Bellman, informático americano nascido em 1920.

1. consideram-se como vértices com marcas temporárias, apenas aqueles cujas marcas foram alteradas na iteração anterior;
2. termina-se a execução do algoritmo quando não existem vértices com marcas temporárias.

Infelizmente porém, com estas alterações e no caso de grafos com custos negativos, o algoritmo pode entrar em ciclo (ou seja, pode não atingir as condições de paragem). Com efeito, se num grafo existe um ciclo cuja soma dos custos das suas arestas é negativa, repetindo este ciclo, pode reduzir-se o comprimento de um caminho tanto quanto se queira. Para este tipo de grafos, diz-se que o problema da determinação de um caminho mais curto está *mal definido*. Esta dificuldade resolve-se detectando os grafos para os quais o problema está mal definido. No entanto, verificar se existe um ciclo de comprimento negativo é mais complicado do que determinar um caminho mais curto (quando tal é possível). Um modo eficiente de contornar estas dificuldades, consiste em não deixar o algoritmo executar mais do que $\nu - 1$ iteração, concluindo-se, nos casos em que tal ocorre, que para o grafo em causa o problema está mal definido. Note-se que na k -ésima iteração, o algoritmo determina um caminho mais curto de entre os caminhos com não mais do que k arestas. Segue-se o pseudocódigo deste procedimento que se designa por Algoritmo 14.3 BELLMAN-FORD, onde k denota a iteração corrente e onde *Marca* e *MarcaAnterior* denotam as tabelas das marcas actuais e das marcas da iteração anterior, respectivamente.

Algoritmo 14.3: BELLMAN-FORD($G = (V, E, W)$, s)

```

para todo  $v \in V$ 
  fazer MarcaAnterior[ $v$ ]  $\leftarrow \infty$ ; Antecessor[ $v$ ]  $\leftarrow 0$ 
MarcaAnterior[ $s$ ]  $\leftarrow 0$ ; Temporários  $\leftarrow \{s\}$ ;  $k \leftarrow 0$ ;
repetir
   $k \leftarrow k + 1$ ; Marca  $\leftarrow$  MarcaAnterior
  para todo  $u \in$  Temporários
    fazer para todo  $v \in N_G(u)$ 
      fazer se Marca[ $v$ ]  $>$  MarcaAnterior[ $u$ ] +  $W[u, v]$ 
      então  $\begin{cases} \text{i} Marca[v] \leftarrow MarcaAnterior[u] + W[u, v] \\ \text{i} Antecessor[v] \leftarrow u \end{cases}$ 
    Temporários  $\leftarrow \{v \in V : Marca[v] \neq MarcaAnterior[v]\}$ 
    MarcaAnterior  $\leftarrow$  Marca
  até Temporários  $= \emptyset \vee k = \nu - 1$ 
  se Temporários  $\neq \emptyset$ 
    então output (“O grafo contém um ciclo de comprimento negativo”)
  devolver (Marca)

```

Uma vez que o ciclo **repetir** não se executa mais do que $\nu - 1$ vezes (cada execução correspondendo a uma iteração) e cada iteração necessita de $\mathcal{O}(\nu^2)$ operações, podemos concluir que a complexidade computacional do algoritmo de Bellman-Ford é $\mathcal{O}(\nu^3)$.

Exemplo 14.9. Vamos determinar os caminhos orientados mais curtos entre o vértice v_1 e os restantes vértices do digrafo definido pela seguinte matriz de custos:

$$W = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\ v_1 & 0 & 1 & \infty & \infty & 2 & \infty & \infty & \infty \\ v_2 & 1 & 0 & 4 & \infty & \infty & 1 & \infty & \infty \\ v_3 & \infty & 4 & 0 & 4 & 3 & \infty & 3 & \infty \\ v_4 & \infty & \infty & 4 & 0 & \infty & 3 & 4 & 7 \\ v_5 & 2 & 2 & \infty & \infty & 0 & 3 & \infty & \infty \\ v_6 & \infty & \infty & -2 & 3 & \infty & 0 & 5 & \infty \\ v_7 & \infty & \infty & \infty & 4 & \infty & 5 & 0 & 6 \\ v_8 & \infty & \infty & \infty & 7 & \infty & \infty & 6 & 0 \end{pmatrix}.$$

Solução. Uma vez que a matriz de custos contém alguns elementos negativos, é aconselhável utilizar o algoritmo de Bellman-Ford, em vez do algoritmo de Dijkstra.

A Tabela 14.6 apresenta os valores obtidos durante a execução sucessiva de todos os passos do algoritmo de Bellman-Ford e, em cada vértice (coluna), as entradas referem-se aos pares (marca actual, antecessor) e os pares com marcas temporárias são assinalados a negrito.

v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8
(0, -)	(∞ , -)						
(0, -)	(1, v_1)	(∞ , -)	(∞ , -)	(2, v_1)	(∞ , -)	(∞ , -)	(∞ , -)
(0, -)	(1, v_1)	(5, v_2)	(∞ , -)	(2, v_1)	(2, v_2)	(∞ , -)	(∞ , -)
(0, -)	(1, v_1)	(0, v_6)	(9, v_3)	(2, v_1)	(2, v_2)	(7, v_6)	(∞ , -)
(0, -)	(1, v_1)	(0, v_6)	(4, v_3)	(1, v_3)	(2, v_2)	(3, v_3)	(11, v_4)
(0, -)	(1, v_1)	(0, v_6)	(4, v_3)	(1, v_3)	(2, v_2)	(3, v_3)	(9, v_7)
(0, -)	(1, v_1)	(0, v_6)	(4, v_3)	(1, v_3)	(2, v_2)	(3, v_3)	(9, v_7)

Tabela 14.6: Determinação dos caminhos orientados mais curtos entre o vértice v_1 e os restantes vértices do digrafo representado na Figura 14.9, por aplicação do algoritmo de Bellman-Ford.

Observe-se que na Tabela 14.6, as duas últimas linhas são idênticas. Isto significa que a determinação dos caminhos orientados mais curtos entre o vértice v_1 e os restantes vértices está completa. Por exemplo, um dos (v_1, v_8) -caminhos orientados mais curtos é o determinado pela sequência de vértices $v_1 v_2 v_6 v_3 v_7 v_8$ e tem comprimento 9. Observe-se ainda que o comprimento do caminho orientado mais curto entre v_1 e v_3 , ou seja, do caminho orientado $v_1 v_2 v_6 v_3$ é igual a 0. \square

O digrafo do Exemplo 14.9 é representado na Figura 14.9, onde, por simplicidade, as arestas não orientadas denotam pares de arcos paralelos com sentidos opostos.

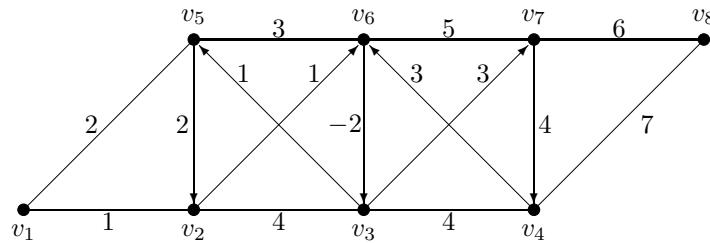


Figura 14.9: Digrafo do Exemplo 14.9.

14.5. Algoritmo de Floyd

A determinação dos caminhos mais curtos entre os $\binom{\nu}{2}$ pares de vértices de um grafo G (digrafo \vec{G}), pode fazer-se executando o algoritmo de Dijkstra ou de Bellman-Ford, consoante o caso, ν vezes, ou seja, determinando os caminhos mais curtos entre cada vértice e os restantes. No caso de custos não negativos nas arestas (nos arcos), a complexidade computacional resultante é $O(\nu^3)$. Por sua vez, no caso de grafos (digrafos) com arestas (arcos) de custos negativos, a complexidade resultante da aplicação do algoritmo de Bellman-Ford, para todos os vértices, é igual a $O(\nu^4)$. Para o caso geral, em que os grafos (digrafos) podem ter ou não arestas (arcos) de custos negativos, vamos introduzir um algoritmo que tem complexidade $O(\nu^3)$ e que se designa por algoritmo de Floyd⁴.

Descrição do algoritmo de Floyd. Na k -ésima iteração, conhecidos os caminhos mais curtos entre cada par de vértices, com vértices interiores pertencentes ao conjunto $\{1, \dots, k-1\}$, o passo básico consiste na determinação dos caminhos mais curtos entre os diferentes pares de vértices, com vértices interiores pertencentes ao conjunto $\{1, \dots, k\}$. Com este fim, a partir da matriz de custos $W^0 = W$, que representa os comprimentos dos caminhos sem vértices interiores, construímos uma sequência de matrizes

$$W^{(1)}, W^{(2)}, \dots, W^{(n)},$$

onde o elemento $w_{ij}^{(k)}$ da matriz $W^{(k)}$ é igual ao comprimento do caminho mais curto entre os vértices v_i e v_j , com vértices interiores no conjunto $\{1, 2, \dots, k\}$. Como consequência, os elementos da matriz $W^{(k)}$, podem determinar-se a partir da matriz $W^{(k-1)}$, aplicando a seguinte fórmula:

$$\begin{aligned} w_{ij}^{(0)} &= w_{ij}, \\ w_{ij}^{(k)} &= \min \left\{ w_{ij}^{(k-1)}, w_{ik}^{(k-1)} + w_{kj}^{(k-1)} \right\}, \quad \text{para } k = 1, 2, \dots, n. \end{aligned}$$

Logo, na primeira iteração, para a obtenção do caminho- (v_i, v_j) , junta-se o vértice v_1 como vértice interior se $w_{ij} > w_{i1} + w_{1j}$. Na segunda iteração pode (eventualmente) juntar-se o vértice v_2 como vértice interior, etc.

Observe-se que este algoritmo determina apenas os comprimentos dos caminhos mais curtos, mas não determina estes caminhos. Para os determinarmos, é necessário introduzir uma matriz $P = (p_{ij})$ de dimensão $\nu \times \nu$ (designada por *matriz dos antecessores*). O elemento p_{ij} denota o antecessor directo do vértice v_j no caminho mais curto entre v_i e v_j . A determinação desta matriz P pode fazer-se executando o seguinte procedimento:

1. Iniciar a matriz P , com as entradas

$$p_{ij} = \begin{cases} i, & \text{se } w_{ij} < \infty, \\ 0, & \text{se } w_{ij} = \infty. \end{cases}$$

Os valores diagonais podem permanecer nulos ao longo do procedimento.

2. Na k -ésima iteração, se o vértice v_k é inserido no conjunto dos vértices interiores do caminho- (v_i, v_j) mais curto (ou seja, se $w_{ij} > w_{ik} + w_{kj}$), então $p_{ij} \leftarrow p_{kj}$.

Mais formalmente, este procedimento é apresentado em pseudocódigo, com a designação de Algoritmo 14.4 FLOYD.

Exemplo 14.10. Utilizando o algoritmo de Floyd, vamos determinar os caminhos mais curtos entre os diferentes pares de vértices do grafo representado na Figura 14.10.

⁴Robert W. Floyd (1936–2001), foi um informático americano.

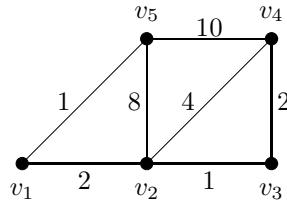


Figura 14.10: Grafo do Exemplo 14.10.

Algoritmo 14.4: FLOYD($G = (V, E, W)$)

```

 $MA \leftarrow W$ 
para todo  $v \in V$ 
  fazer para todo  $w \in V$ 
    fazer se  $v = w \vee W[v, w] = \infty$ 
      então  $P_{\text{Anterior}}[v, w] \leftarrow 0$ 
      senão  $P_{\text{Anterior}}[v, w] \leftarrow v$ 
    para  $k = 1$  até  $|V|$ 
      fazer {
        Marca  $\leftarrow MA$ ;  $P \leftarrow P_{\text{Anterior}}$ 
        para todo  $v \in V$ 
          fazer para todo  $w \in V$ 
            fazer {
              se  $MA[v, w] > MA[v, k] + MA[k, w]$ 
                então {
                  Marca $[v, w] \leftarrow MA[v, k] + MA[k, w]$ 
                   $P[v, w] \leftarrow P_{\text{Anterior}}[k, w]$ 
                }
              para todo  $v \in V$ 
                fazer {
                  se  $Marca[v, v] < 0$ 
                    então {
                      output ("O problema está mal definido")
                      stop
                    }
                }
            }
        devolver  $(Marca, P)$ 

```

Solução. Começamos por iniciar as matrizes $W^{(0)}$ e P , obtendo-se:

$$W^{(0)} = \begin{pmatrix} 0 & 2 & \infty & \infty & 1 \\ 2 & 0 & 1 & 4 & 8 \\ \infty & 1 & 0 & 2 & \infty \\ \infty & 4 & 2 & 0 & 10 \\ 1 & 8 & \infty & 10 & 0 \end{pmatrix} \quad \text{e} \quad P^{(0)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 2 & 2 & 2 \\ 0 & 3 & 0 & 3 & 0 \\ 0 & 4 & 4 & 0 & 4 \\ 5 & 5 & 0 & 5 & 0 \end{pmatrix}.$$

Seguidamente, determina-se a matriz $W^{(1)}$ que corresponde à matriz $W^{(0)}$, apenas, com as entradas $w_{2,5}$ (dado que $w_{2,5}^{(0)} > w_{2,1}^{(0)} + w_{1,5}^{(0)}$) e $w_{5,2}$ actualizadas. Logo, determina-se a matriz $P^{(1)}$ que corresponde à matriz $P^{(0)}$ com as seguintes actualizações: $p_{25} \leftarrow p_{15}$ e $p_{52} \leftarrow p_{12}$. Como consequência, obtém-se

$$W^{(1)} = \begin{pmatrix} 0 & 2 & \infty & \infty & 1 \\ 2 & 0 & 1 & 4 & 3 \\ \infty & 1 & 0 & 2 & \infty \\ \infty & 4 & 2 & 0 & 10 \\ 1 & 3 & \infty & 10 & 0 \end{pmatrix} \quad \text{e} \quad P^{(1)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 2 & 2 & 1 \\ 0 & 3 & 0 & 3 & 0 \\ 0 & 4 & 4 & 0 & 4 \\ 5 & 1 & 0 & 5 & 0 \end{pmatrix}.$$

Analogamente, determina-se a matriz $W^{(2)}$ que corresponde à matriz $W^{(1)}$, com as entradas $w_{1,3}$, $w_{1,4}$, $w_{3,1}$, $w_{3,5}$, $w_{4,1}$, $w_{5,3}$ e $w_{5,4}$ actualizadas. Logo, determina-se a matriz $P^{(2)}$ que corresponde à

matriz $P^{(1)}$ com as respectivas actualizações. Como consequência, vem

$$W^{(2)} = \begin{pmatrix} 0 & 2 & 3 & 6 & 1 \\ 2 & 0 & 1 & 4 & 3 \\ 3 & 1 & 0 & 2 & 4 \\ 6 & 4 & 2 & 0 & 7 \\ 1 & 3 & 4 & 7 & 0 \end{pmatrix} \quad \text{e} \quad P^{(2)} = \begin{pmatrix} 0 & 1 & 2 & 2 & 1 \\ 2 & 0 & 2 & 2 & 1 \\ 2 & 3 & 0 & 3 & 1 \\ 2 & 4 & 4 & 0 & 1 \\ 5 & 1 & 2 & 2 & 0 \end{pmatrix}.$$

Tal como anteriormente, determina-se $W^{(3)}$ e $P^{(3)}$, obtendo-se:

$$W^{(3)} = \begin{pmatrix} 0 & 2 & 3 & 5 & 1 \\ 2 & 0 & 1 & 3 & 3 \\ 3 & 1 & 0 & 2 & 4 \\ 5 & 3 & 2 & 0 & 6 \\ 1 & 3 & 4 & 6 & 0 \end{pmatrix} \quad \text{e} \quad P^{(3)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 1 \\ 2 & 0 & 2 & 3 & 1 \\ 2 & 3 & 0 & 3 & 1 \\ 2 & 3 & 4 & 0 & 1 \\ 5 & 1 & 2 & 3 & 0 \end{pmatrix}.$$

Continuando, vem que $W^{(3)} = W^{(4)} = W^{(5)}$ e, como consequência, $P^{(3)} = P^{(4)} = P^{(5)}$, pelo que as matrizes W e P ficam determinadas.

A matriz W regista os comprimentos e a matriz P regista os dados que definem os caminhos mais curtos (não necessariamente únicos) entre todos os pares de vértices. Por exemplo, o caminho mais curto entre os vértices v_4 e v_5 tem comprimento $w_{45} = 6$ e um destes caminhos fica definido pela sequência de vértices registados nas entradas da matriz P , $p_{43}p_{42}p_{41}p_{45}v_5$, ou seja, este caminho tem forma $v_4v_3v_2v_1v_5$. Deve observar-se que este caminho se obtém (pelos antecessores) do vértice final até ao vértice inicial. \square

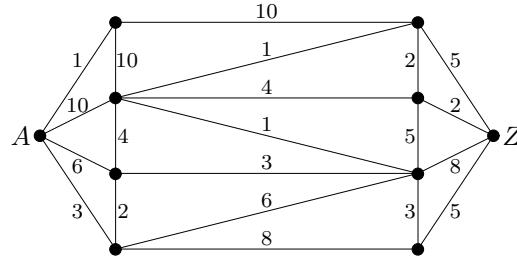
A escolha entre os algoritmos de Dijkstra, de Bellman-Ford e de Floyd, depende do problema que queremos resolver. O algoritmo de Dijkstra é muito eficiente, mas apenas se pode utilizar em grafos (digrafos) com custos não negativos nas arestas (nos arcos) ou em grafos (digrafos) sem custos nas arestas (nos arcos), o que é equivalente a que todas as arestas (arcos) tenham custo unitário. O algoritmo de Floyd é utilizado para a determinação de caminhos mais curtos entre todos os pares de vértices de um grafo (digrafo) com alguns custos negativos nas arestas (nos arcos). No caso de custos negativos, a execução ν vezes do algoritmo de Dijkstra é mais eficiente. Finalmente, o algoritmo de Bellman-Ford é utilizado para a determinação de caminhos mais curtos a partir de um vértice fixo num grafo (digrafo) com alguns custos negativos.

14.6. Exercícios

- 14.1. Demonstre que a função dist_G constitui uma métrica no conjunto dos vértices de um grafo simples conexo, G , com custos positivos nas arestas.
- 14.2. Dado um grafo simples conexo com ν vértices, qual é o mínimo e o máximo número de vértices centrais.
- 14.3. Dado um grafo simples conexo com ν vértices, qual é o mínimo e o máximo número de vértices periféricos (ou seja, com excentricidade máxima).
- 14.4. Determine os caminhos mais curtos entre cada par de vértices do digrafo definido pela seguinte matriz de custos nas arestas:

$$W = \begin{pmatrix} 0 & 2 & \infty & 1 & \infty & \infty \\ \infty & 0 & 1 & 8 & \infty & \infty \\ -2 & \infty & 0 & \infty & \infty & 2 \\ \infty & \infty & \infty & 0 & 10 & \infty \\ \infty & 4 & \infty & \infty & 0 & 2 \\ \infty & 6 & 1 & \infty & 3 & 0 \end{pmatrix}$$

- 14.5. Determine a distância e um caminho mais curto entre Lisboa e Faro, a partir do grafo representado no mapa de Portugal, na Figura 14.8.
- 14.6. Determine a excentricidade do Porto, a partir do grafo representado no mapa de Portugal, na Figura 14.8.
- 14.7. Determine o diâmetro e o raio do digrafo representado na Figura 14.7.
- 14.8. Utilizando algoritmo de Floyd determine distâncias entre todos os pares dos vértices do grafo representado na Figura 14.6 (ver página 387).
- 14.9. Mostre que qualquer grafo simples com pelo menos uma aresta tem pelo menos dois vértices que não são vértices de corte.
- 14.10. Mostre que se G é um grafo simples tal que $\forall uv \in E(G) N_G(u) \cup N_G(v) = V(G)$, então contém pelo menos $\frac{\varepsilon(4\varepsilon - \nu^2)}{3\nu}$ triângulos (C_3).
- 14.11. Dado um grafo simples conexo, G , prove que se G não contém P_4 nem C_4 como subgrafos induzidos, então existe um vértice de grau $\nu(G) - 1$.
- 14.12. Considerando um grafo G , sem arestas paralelas (mas que pode ter lacetes), prove as seguintes afirmações:
- Se $n \in \mathbb{N}$, G é conexo e $\varepsilon(G) = \nu(G) + n$, então G contém pelo menos $n + 1$ ciclos.
 - G contém pelo menos $cc(G) + \varepsilon(G) - \nu(G)$ ciclos.
 - Mostre que o minorante obtido em (a) é o melhor possível para grafos simples.
- 14.13. Caso exista, represente um grafo que satisfaça as condições que a seguir se indicam.
- Uma árvore com 6 vértices e 6 arestas.
 - Um grafo desconexo com 10 vértices e 8 arestas.
 - Um grafo desconexo com 12 vértices, 11 arestas e sem nenhum ciclo.
 - Uma árvore com 6 vértices em que a soma dos graus dos vértices é igual a 12.
 - Um grafo conexo com 6 arestas, 4 vértices e exactamente 2 ciclos.
 - Um grafo com 6 vértices, 6 arestas e sem ciclos.
- 14.14. Sendo G um grafo simples, com $\nu(G) = 2n - 1$ e $\varepsilon(G) = n^2$, prove que G contém pelo menos $n - 1$ triângulos.
- 14.15. Demonstre que se um grafo G de ordem ν não tem triângulos, então $\varepsilon(G) \leq \left\lfloor \frac{\nu^2}{4} \right\rfloor$.
- 14.16. Dado um grafo G , com pelo menos 4 vértices, demonstre que G é 2-conexo se e só se qualquer que seja o par de conjuntos disjuntos de vértices de cardinalidades superior a 2, $X, Y \subset V(G)$, existem dois caminhos completamente disjuntos com vértices iniciais em X e finais em Y e com vértices internos não pertencentes nem a X nem a Y .
- 14.17. Sendo $f(n)$ o número mínimo de arestas dos grafos conexos de ordem n , nos quais cada arestas pertence a um triângulo, prove que para $n \geq 3$ $f(n) = \left\lceil \frac{3(n-1)}{2} \right\rceil$.
- 14.18. Considere o grafo representado na figura a seguir e determine todos os caminhos mais curtos entre A e Z .



14.19. Seja G um grafo simples de ordem ν e sejam $u, v \in V(G)$ dois vértices adjacentes. Prove as seguintes afirmações:

- (a) O número de triângulos que contêm u e v é igual a $|N_G(u) \cap N_G(v)|$.
- (b) Prove a desigualdade $|N_G(u) \cap N_G(v)| \geq d_G(v) + d_G(u) - \nu$.

14.20. Seja \mathcal{G}_n o conjunto de todos um grafos simples G tais que $V(G) = [n] = \{1, 2, \dots, n\}$.

- (a) Prove que existe uma bijecção entre o subconjunto de grafos de ordem n , $\{G \in \mathcal{G}_n : d_G(x)$ é par $\forall x \in V(G)\}$ e \mathcal{G}_{n-1} .
- (b) Prove que $|\{G \in \mathcal{G}_n : d_G(x)$ é par $\forall x \in V(G)\}| = 2^{\binom{n-1}{2}}$.

14.21. Sendo G um grafo não nulo, prove que existe um subgrafo H de G tal que $\delta(H) > \frac{\varepsilon(H)}{\nu(H)} > \frac{\varepsilon(G)}{\nu(G)}$.

15

Árvores

As árvores, enquanto subgrafos abrangentes conexos minimais (no sentido do número de arestas), podem considerar-se como esqueletos. Assim, podemos concluir que os grafos que não são árvores têm vários esqueletos. O facto da resolução de muitos problemas associados a grafos se fazer com recurso a uma ou várias das suas árvores abrangentes, tornam as árvores especialmente importantes no contexto da teoria dos grafos. Os primeiros estudos sobre árvores foram realizados por Cayley¹ em 1857, pelo que o reconhecimento da sua importância vem, praticamente, desde as origens da teoria dos grafos.

15.1. Árvores e florestas

Como o próprio nome indica, informalmente, as florestas são conjuntos de árvores, que, naturalmente, têm sido também muito estudados em teoria dos grafos. Seguem-se as definições de árvore e floresta (de entre muitas que se conhecem).

Definição 15.1 (Floresta e árvore). *Um grafo simples G diz-se uma floresta se G não contém circuitos. Por sua vez, uma floresta conexa designa-se por árvore, ou seja, uma árvore é uma componente conexa de uma floresta.*

Na Figura 15.1 apresenta-se um exemplo de uma floresta com três árvores.

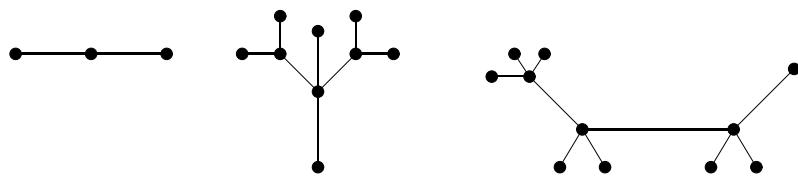


Figura 15.1: Floresta com três árvores.

Teorema 15.1. *Se G é um grafo simples com ν vértices, então as seguintes afirmações são equivalentes.*

- (a) G é uma árvore,
- (b) G não contém ciclos e tem $\nu - 1$ arestas,

¹Arthur Cayley (1821–1895), matemático inglês que publicou mais de 900 artigos, com resultados em várias áreas da matemática.

- (c) G é conexo e tem $\nu - 1$ arestas,
- (d) G é conexo e cada aresta é uma ponte,
- (e) quaisquer dois vértices de G estão ligados por um único caminho,
- (f) G não contém ciclos, mas acrescentando uma aresta obtém-se um ciclo.

Demonstração.

(a) \Rightarrow (b) Vamos fazer a prova por indução sobre o número de vértices ν . É claro que se $\nu = 1$, então a única árvore com 1 vértice é o grafo trivial com $0 = \nu - 1$ arestas, pelo que a implicação se verifica. Suponha que a implicação é verdadeira para todas as árvores com menos de $\nu \geq 2$ vértices. Uma vez que, por definição, G não contém ciclos, a remoção de qualquer aresta, subdivide o grafo em duas componentes G_1 e G_2 , cada uma das quais é uma árvore (ver Figura 15.2-(A)). Supondo que G_1 tem ν_1 vértices e que G_2 tem ν_2 vértices, com $\nu_1 + \nu_2 = \nu$, por hipótese de indução, $\varepsilon(G_1) = \nu_1 - 1$ e $\varepsilon(G_2) = \nu_2 - 1$. Logo, o número total de arestas de G é igual a

$$\varepsilon(G) = \varepsilon(G_1) + \varepsilon(G_2) + 1 = \nu_1 - 1 + \nu_2 - 1 + 1 = \nu - 1.$$

- (b) \Rightarrow (c) Suponha que G não é conexo. Então, cada componente de G é um grafo conexo sem circuitos, pelo que, por hipótese, o número de vértices de cada componente excede em uma unidade o número de arestas. Logo, o número total de vértices de G , excede o número total de arestas de G em pelo menos duas unidades, contradizendo a hipótese de G ter $\nu - 1$ arestas.
- (c) \Rightarrow (d) Como G é conexo, com $\nu - 1$ arestas, a remoção de uma qualquer aresta produz um grafo com ν vértices e $\nu - 2$ arestas e, consequentemente, pelo Teorema 13.1, esse grafo não é conexo (uma vez que um grafo conexo de ordem ν tem, pelo menos, $\nu - 1$ arestas).
- (d) \Rightarrow (e) Dados dois vértices arbitrários u e v , por definição de grafo conexo, existe um caminho- (u, v) . Uma vez que, por hipótese, qualquer aresta desse caminho é uma ponte, podemos concluir que esse caminho é único.
- (e) \Rightarrow (f) Supondo que G contém um ciclo, então quaisquer dois vértices desse ciclo estão ligados por, pelo menos, dois caminhos e, consequentemente, existem vértices de G que estão ligados por mais do que um caminho. Logo, se entre quaisquer dois vértices de G existe um único caminho, então G não contém ciclos. Porém, acrescentando uma aresta entre dois vértices u e v , como, por hipótese, já existe um caminho- (u, v) , criamos um ciclo (ver Figura 15.2-(C)).
- (f) \Rightarrow (a) Note-se que basta provar que se G satisfaz a hipótese, então é conexo. Suponha que G satisfaz a hipótese, mas não é conexo. Se acrescentarmos uma aresta a G , ligando dois vértices pertencentes a componentes distintas, não se cria qualquer ciclo, o que constitui uma contradição. \square

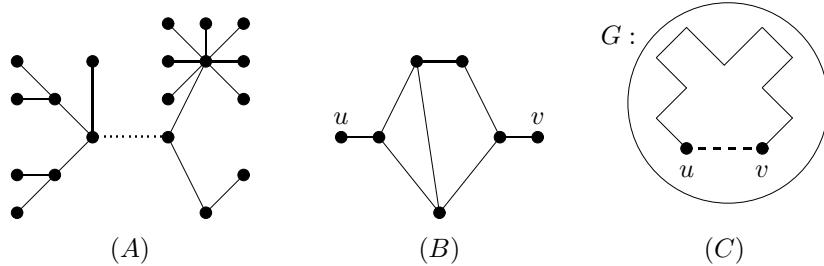


Figura 15.2: Ilustrações para a demonstração do Teorema 15.1.

Teorema 15.2. *Cada árvore não trivial contém pelo menos dois vértices de grau um (que se designam por folhas).*

Demonstração. Seja G uma árvore não trivial com ν vértices. Como uma árvore é conexa, então $\forall_{v \in V(G)} d(v) \geq 1$. Recorrendo ao Teorema 12.1 sobre o número de arestas e o Teorema 15.1, podemos concluir que

$$\sum_{v \in V} d(v) = 2\nu - 2.$$

Como consequência, pelo menos dois vértices têm grau um (caso contrário, $\sum_{v \in V} d(v) \geq 2\nu - 1$). \square

Segue-se uma condição necessária e suficiente para um grafo ser uma floresta.

Teorema 15.3. *Um grafo G é uma floresta se e só se*

$$\varepsilon(G) - \nu(G) + \text{cc}(G) = 0.$$

Demonstração.

(\Rightarrow) A prova da condição necessária vai ser feita por indução sobre o número de arestas de G , tendo em conta que o resultado se verifica trivialmente para $\varepsilon(G) = 0$.

Suponha que o resultado se verifica para todas as florestas com menos do que $\varepsilon(G)$ arestas e $\varepsilon(G) > 0$. Seja G' um subgrafo de G obtido por eliminação de uma aresta arbitrária. Logo, G' é uma floresta com $\varepsilon(G) - 1$ arestas, $\nu(G)$ vértices e $\text{cc}(G) + 1$ componentes. Por hipótese de indução, aplicada a G' ,

$$\begin{aligned} 0 &= \varepsilon(G') - \nu(G') + \text{cc}(G') = \varepsilon(G) - 1 - \nu(G) + \text{cc}(G) + 1 \\ &= \varepsilon(G) - \nu(G) + \text{cc}(G). \end{aligned}$$

(\Leftarrow) Para provar a condição suficiente suponha que G tem p componentes, G_1, \dots, G_p , pelo que $\varepsilon(G) - \nu(G) + p = \sum_{j=1}^p (\varepsilon(G_j) - \nu(G_j) + 1)$. Então

$$\varepsilon(G) - \nu(G) + p = 0 \Leftrightarrow \sum_{j=1}^p (\varepsilon(G_j) - \nu(G_j) + 1) = 0$$

e, uma vez que $\forall_{j \in [p]} \varepsilon(G_j) - \nu(G_j) + 1 \geq 0$,

$$\forall_{j \in [p]} \varepsilon(G_j) - \nu(G_j) + 1 = 0.$$

Consequentemente, de acordo com o Teorema 15.1, todos os grafos G_j , com $j \in \{1, \dots, p\}$, são árvores. \square

Deste teorema decorre que todo o grafo G tal que $\varepsilon(G) \geq \nu(G)$ contém pelo menos um circuito.

15.2. Número de árvores abrangentes

Definição 15.2 (Árvore abrangente). *Dado um grafo conexo G , designa-se por árvore abrangente (ou de suporte) de G , todo o subgrafo abrangente de G que é uma árvore, ou seja, todo o subgrafo que é uma árvore e contém todos os vértices de G .*

Teorema 15.4. *Todo o grafo conexo admite uma árvore abrangente.*

Demonstração. Seja G um grafo conexo e seja T um subgrafo abrangente conexo minimal de G , ou seja, tal que $\text{cc}(T) = 1$ e $\text{cc}(T - e) > 1$, para cada $e \in T$. Então, cada aresta de T é uma ponte e, tendo em conta o Teorema 15.1, T é uma árvore. \square

Teorema 15.5. *Seja G um grafo conexo, então $e \in E(G)$ é uma ponte se e só se a aresta e pertence a todas as árvores abrangentes de G .*

Demonstração. Seja e uma ponte de G , com extremos u e v , e suponha que existe um árvore abrangente T de G tal que $e \notin E(T)$. Por definição de árvore abrangente, em T existe um caminho $-(u, v)$, o que entra em contradição com o facto da aresta $e = uv$ ser uma ponte. Reciprocamente, se a aresta $e = uv$ pertence a todas as árvores abrangentes, tal significa que a aresta e é o único caminho entre u e v e, consequentemente, trata-se de uma aresta de corte. \square

Segue-se a definição da operação de contracção de arestas que, a par da operação de eliminação de arestas já introduzida na secção 12.5 (na sequência da Definição 12.19), será utilizada ao longo deste texto em vários capítulos.

Definição 15.3 (Contracção de arestas). *Dado um grafo G , diz-se que uma aresta e de G é contraída se os seus vértices extremos são fundidos, todas as arestas paralelas e lacetes (eventualmente) produzidos são eliminados. Esta operação designa-se por operação de contracção de arestas de G e, para uma aresta particular $e \in E(G)$, denota-se por G/e .*

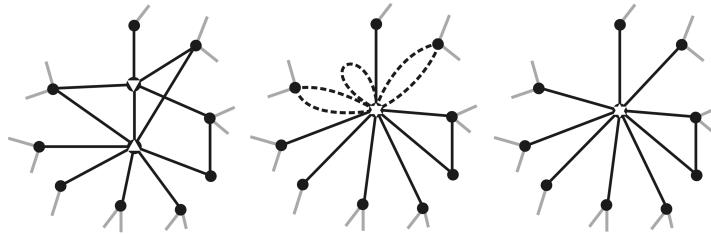


Figura 15.3: Exemplo que ilustra a operação de contracção de uma aresta.

Uma variante da operação de contracção de arestas é a operação de *fusão de extremos de uma aresta* (ou fusão de vértices extremos de uma aresta) que, em concordância com a definição de fusão de vértices da Secção 13.3 (página 362), difere da contracção de uma aresta no facto de, com excepção da aresta contraída, todas as restantes arestas se mantêm no grafo (incluindo arestas paralelas e lacetes eventualmente produzidos).² Como consequência, dado um grafo G , após a fusão dos extremos de uma aresta $e \in E(G)$, a qual vamos denotar por $G//e$, o número de arestas decresce uma unidade, ou seja,

$$|E(G//e)| = |E(G)| - 1.$$

Verifica-se que a operação de fusão de extremos de arestas comuta com a operação de eliminação de arestas, ou seja, dadas duas arestas distintas $e, f \in E(G)$, verifica-se que

$$(G//e) - f = (G - f)//e.$$

Denotando por $\tau(G)$ o número de árvores abrangentes do grafo G , segue-se uma fórmula recursiva para a determinação do número de árvores abrangentes.

² Alguns autores utilizam a designação de contracção de uma aresta, precisamente para a operação que aqui designamos por fusão de extremos de uma aresta.

Teorema 15.6. *Dado um grafo G , se $e \in E(G)$ não é um lacete em G , então*

$$\tau(G) = \tau(G - e) + \tau(G//e). \quad (15.1)$$

Demonastração. Sem perda de generalidade, vamos assumir que G é um grafo conexo (uma vez que para grafos não conexos ambos os lados da igualdade (15.1) são iguais a zero). Tendo em conta que toda a árvore abrangente de um grafo G que não contém a aresta e é uma árvore abrangente para o grafo $G - e$ e reciprocamente, podemos concluir que $\tau(G - e)$ é igual ao número das árvores abrangentes de G que não contêm a aresta e . Por outro lado, a cada árvore abrangente T do grafo G que contém a aresta e corresponde uma árvore abrangente $T//e$ do grafo $G//e$ (devendo observar-se que esta correspondência é biunívoca). Como consequência, $\tau(G//e)$ é igual ao número de árvores abrangentes de G que contém a aresta e . Logo, $\tau(G) = \tau(G - e) + \tau(G//e)$. \square

Exemplo 15.1. *Seja G um grafo conexo e seja $e \in E(G)$ uma ponte de G . Denotando por G_1 e G_2 as duas componentes do grafo $G - e$, vamos determinar o número de árvores abrangentes do grafo G , em função de $\tau(G_1)$ e $\tau(G_2)$.*

Solução. Uma vez que o grafo $G - e$ não é conexo,

$$\tau(G - e) = 0.$$

Por outro lado, cada árvore abrangente de $G//e$ é constituída por uma árvore abrangente de G_1 e uma árvore abrangente de G_2 . Consequentemente, aplicando princípio da multiplicação, vem

$$\tau(G//e) = \tau(G_1)\tau(G_2).$$

Logo, tendo em conta o Teorema 15.6, obtém-se

$$\tau(G) = \tau(G - e) + \tau(G//e) = \tau(G_1)\tau(G_2). \quad \square$$

Para simplificar o processo de determinação do número de árvores abrangentes de um grafo, vamos considerar alguns casos especiais:

- se G não é conexo, então $\tau(G) = 0$;
- se G é uma árvore, então $\tau(G) = 1$;
- se G é um ciclo, com k arestas, então $\tau(G) = k$ (uma vez que a eliminação de uma aresta do ciclo produz uma árvore abrangente);
- se G é um grafo, constituído por dois vértices ligados por k arestas, então $\tau(G) = k$ (uma vez que cada aresta constitui uma árvore abrangente).

Vamos utilizar estas propriedades para determinar o número de árvores abrangentes no exemplo a seguir.

Exemplo 15.2. *Utilizando fórmula de recorrência (15.1) vamos determinar o número das árvores abrangentes do grafo completo K_4 .*

Solução. Tendo em conta o Teorema 15.6, obtém-se a sequência de igualdades:

$$\begin{aligned} \tau\left(\begin{array}{c} \text{square} \\ | \\ e \end{array}\right) &= \tau\left(\begin{array}{c} \text{square} \\ | \\ \end{array}\right) + \tau\left(\begin{array}{c} \text{triangle} \\ | \\ \end{array}\right) \\ \tau\left(\begin{array}{c} e \\ \text{triangle} \end{array}\right) &= \tau\left(\begin{array}{c} \text{triangle} \\ | \\ \end{array}\right) + \tau\left(\begin{array}{c} \text{triangle} \\ | \\ \end{array}\right) = \tau\left(\begin{array}{c} \text{triangle} \\ | \\ \end{array}\right) + 4, \end{aligned}$$

$$\begin{aligned}\tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) &= \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) + \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) = \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) + 2, \\ \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) &= \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) + \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) = 0 + 2 = 2,\end{aligned}$$

onde, se conclui que

$$\tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) = 2 + 2 = 4 \quad \text{e} \quad \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) = 4 + 4 = 8.$$

Assim, resta determinar o número das árvores abrangentes de um "quadrado com uma diagonal":

$$\tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) = \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) + \tau\left(\begin{array}{c} \text{graph} \\ e \end{array}\right) = 4 + 4 = 8,$$

Finalmente, vem $\tau(K_4) = 8 + 8 = 16$.

Conforme veremos mais adiante, a determinação de $\tau(K_4)$ pode fazer-se mais facilmente, recorrendo ao teorema de Cayley (Teorema 15.7). \square

15.3. Geração de todas as árvores abrangentes

O problema de gerar todos as árvores abrangentes de um grafo conexo é um problema computacionalmente complexo, uma vez que o número de árvores abrangentes pode ser muito grande (ver teorema de Cayley (Teorema 15.7)). Teoricamente, podemos gerar todos os subconjuntos de arestas de cardinalidade $\nu - 1$ e verificar quais os que representam árvores. Observe-se que, após a escolha de $k \geq 3$ arestas, podemos verificar se formam um ciclo e, no caso afirmativo, concluir que qualquer superconjunto que as contenha não é uma árvore.

Com o objectivo de gerar todas as árvores abrangentes, vamos ordenar todas as arestas, formando uma lista de arestas $(e_1, e_2, \dots, e_\varepsilon)$. Cada subconjunto destas arestas, será representado por uma sublistas (de acordo com a ordem inicialmente estabelecida). A geração de todas as árvores abrangentes será realizada recorrendo ao *backtracking*, a partir da lista vazia.

Exemplo 15.3. Vamos gerar todas as árvores abrangentes do grafo representado na Figura 15.4.

Solução. De acordo do Exemplo 15.2, o grafo ("quadrado com diagonal") tem oito árvores abrangentes distintas. Para as gerar, vamos definir (por exemplo) a seguinte lista ordenada de arestas:

$$(a, b, c, d, e).$$

Observe-se que cada árvore abrangente tem exactamente três arestas que são definidas pelas correspondentes sublistas que serão obtidas, por *backtracking*, a partir da lista vazia. Para simplificar a descrição, durante o procedimento de *backtracking*, vamos riscar as sublistas que contêm um ciclo e colocar um bordo nas que definem árvores abrangentes (as restantes sublistas definem florestas abrangentes).

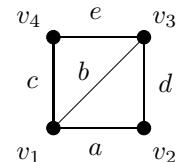


Figura 15.4: Grafo do Exemplo 15.3.

1. $((), (a), (a, b), \boxed{(a, b, c)})$ (primeira árvore abrangente).
2. Eliminando a última aresta c da última lista obtida e continuando o procedimento: $\boxed{(a, b, d)}$ (contém um ciclo). Eliminando d e continuando: $\boxed{(a, b, e)}$ (segunda árvore abrangente).

3. Eliminando a última aresta e da última lista obtida, conclui-se que não se pode continuar (completando a sublista (a, b)). Eliminando a aresta b da última lista obtida e continuando: (a, c) , $\boxed{(a, c, d)}$ (terceira árvore abrangente).
4. Eliminando a última aresta d da última lista obtida e continuando: $\boxed{(a, c, e)}$ (quarta árvore abrangente).
5. Eliminando a última aresta e e, posteriormente, a aresta c da última lista obtida e continuando: (a, d) , $\boxed{(a, d, e)}$ (quinta árvore abrangente).
6. Eliminando a última aresta e e, posteriormente, a aresta d da última lista obtida e continuando: (a, e) . Conclui-se a impossibilidade de prosseguir, com esta lista, pelo que, eliminando a aresta e e, posteriormente, a aresta a e continuando: (b) , (b, c) , $\boxed{(b, c, d)}$ (sexta árvore abrangente).
7. Eliminando a última aresta d da última lista obtida e continuando: $\cancel{(b, c, e)}$ (contém um ciclo). Eliminamos a aresta e e, posteriormente, a aresta c e continuando: (b, d) , $\boxed{(b, d, e)}$ (sétima árvore abrangente).
8. Eliminando a última aresta e e, posteriormente, a aresta d da última lista obtida e continuando: (b, e) . Eliminando a última aresta e e, posteriormente, a aresta b da última lista obtida e continuando: (c) , (c, d) , $\boxed{(c, d, e)}$ (oitava árvore abrangente).
9. Eliminando a última aresta e e, posteriormente, a aresta d da última lista obtida e continuando: (c, e) . Eliminando a última aresta e e, posteriormente, a aresta c da última lista obtida e continuando: (d) , (d, e) , (e) . Como consequência, não existem mais árvores abrangentes.

A Figura 15.5. representa todas as oito árvores abrangentes, segunda a ordem determinada pelo algoritmo (note-se que as 24 florestas abrangente do grafo da Figura 15.4 também foram geradas). \square

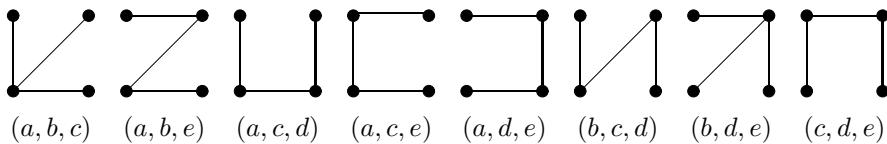


Figura 15.5: Todas as árvores abrangentes do grafo da Figura 15.4, apresentadas segundo a ordem lexicográfica das respectivas listas (ver Exemplo 15.3).

O maior problema deste algoritmo é o modo como se verifica quando uma nova aresta produz um ciclo. No exemplo anterior, essa verificação foi feita por inspeção do grafo. Para se implementar um bom algoritmo, é necessário encontrar critérios eficientes para se concluir, automaticamente, se uma dada aresta deve ou não ser acrescentada à lista. Um modo de o conseguir, consiste em introduzir uma estrutura de dados mais rica do que uma lista (por exemplo a floresta de árvores com raízes) e algoritmos que funcionem, eficientemente, com esta estrutura. Assim, para cada árvore da floresta abrangente, vamos destacar um vértice que designamos por *raiz* (*da árvore*) e para cada vértice v do grafo, vamos associar dois atributos: $Raiz[v]$ (que designa a raiz de árvore que contém v) e $Antecessor[v]$ (que é o antecessor do vértice v no único caminho existente entre $Raiz[v]$ e v). Observa-se que a raiz de uma árvore é o único vértice dessa árvore que não tem antecessor. No algoritmo, a implementar, por convenção, denota-se o antecessor de uma raiz pelo valor 0 (que, naturalmente, nunca é utilizado). Tal como para o algoritmo apresentado no Exemplo 15.3 são necessárias duas operações

sobre esta estrutura (floresta com raízes nas árvores): as operações de inserção e de eliminação de uma aresta.

Vamos começar por descrever os algoritmos que realizam estas operações.

Inserção de uma aresta numa floresta (juntando duas árvores). É possível inserir uma aresta $e = (u, v)$ numa floresta se e só se os seus extremos pertencem a árvores distintas, ou seja, se e só se $Raiz[u] \neq Raiz[v]$ (assumindo-se, sem perda de generalidade, que $Raiz[u] \leq Raiz[v]$). Denotando por T_u a árvore a que pertence vértice u e por T_v a árvore a que pertence o vértice v , podemos dividir o algoritmo em duas partes:

1. Modificar os atributos dos vértices da árvore T_v , de tal forma que a raiz de T_v passe a ser o vértice v , por aplicação do Algoritmo 15.1 RAIZNOVA:

Algoritmo 15.1: RAIZNOVA(v)

```

external  $G, Antecessor, Raiz$ 
 $RaizVelha \leftarrow Raiz[v]$ 
se  $RaizVelha = v$  então abandonar
 $v_1 \leftarrow 0; v_2 \leftarrow v$ 
repetir
     $p \leftarrow v_1; v_1 \leftarrow v_2; v_2 \leftarrow Antecessor[v_1]; Antecessor[v_1] \leftarrow p$ 
    até  $v_1 = RaizVelha$ 
para todo  $w \in V(G)$  fazer se  $Raiz[w] = RaizVelha$  então  $Raiz[w] \leftarrow v$ 

```

2. Modificar o antecessor do vértice v que passa a ser u e as raízes de todos os vértices de T_v que passam a ser $Raiz[u]$.
-

O Algoritmo 15.2 INSEREARESTA, formaliza a realização de ambas as partes deste algoritmo.

Algoritmo 15.2: INSEREARESTA($e = uv$)

```

external  $G, Antecessor, Raiz$ 
 $v_1 \leftarrow Raiz[u]; v_2 \leftarrow Raiz[v]$ 
se  $v_2 < v_1$ 
    então  $v_1 \leftrightarrow v_2; u \leftrightarrow v$ 
 $RaizNova(v)$ 
 $Antecessor[v] \leftarrow u$ 
para todo  $w \in V(G)$  fazer se  $Raiz[w] = v_2$  então  $Raiz[w] \leftarrow v_1$ 

```

Observe-se que o Algoritmo 15.2 INSEREARESTA não verifica a admissibilidade da aresta inserida. Esta verificação será feita no no programa principal (GERAÁRVORES).

Eliminação de uma aresta de uma floresta (partição de uma árvore). Observe-se que se $e = uv$ é uma aresta de uma árvore, então o antecessor de u é v ou antecessor de v é u . Sem perda de generalidade, vamos assumir que antecessor de v é u . Neste caso, após a eliminação da aresta e , podemos concluir que a subárvore que contém u permanece inalterada. Porém, em todos os vértices da subárvore que contém v , a marca relativa à raiz deve ser modificada para v , utilizando o algoritmo

de pesquisa em largura (ou em profundidade). Este procedimento pode ser realizado por aplicação do Algoritmo 15.3 ELIMINAARESTA.

Algoritmo 15.3: ELIMINAARESTA($e = uv$)

```

external  $G$ , Antecessor, Raiz
se Antecessor[ $u$ ] =  $v$  então  $u \leftrightarrow v$ 
Antecessor[ $v$ ]  $\leftarrow 0$ 
para todo  $w \in$  subárvore que contém  $v$  fazer Raiz[ $w$ ]  $\leftarrow v$ 
```

Geração de todas as árvores abrangentes de um grafo. Segue-se a descrição de um algoritmo que gera todas as árvores abrangentes de um grafo conexo arbitrário G .

1. Ordenar todas as arestas do grafo G , por intermédio de uma lista cuja parte inicial contém todas as arestas incidentes num vértice v^* (arbitrário):

$$e_1, e_2, \dots, e_{d(v^*)}, e_{d(v^*)+1}, \dots, e_\varepsilon. \quad (15.2)$$

Para cada vértice $v \in V(G)$, definir:

$$\text{Raiz}[v] \leftarrow v; \quad \text{Antecessor}[v] \leftarrow 0.$$

Iniciar as variáveis:

$k \leftarrow 1$ (onde k é o índice da aresta a considerar),
 $fim \leftarrow d(v^*) + 1$ (em alternativa, fazendo $fim \leftarrow \varepsilon$, o algoritmo vai gerar todas as florestas abrangentes).

2. Se $k = \varepsilon + 1$, então passar para o passo 5. Caso contrário, considerar a aresta $e_k = u_k v_k$ e proceder da seguinte forma:
 - (a) Se $\text{Raiz}[u_k] = \text{Raiz}[v_k]$ (o que significa que os extremos u_k e v_k pertencem a uma mesma árvore e a eventual inserção de e_k produziria um ciclo), então fazer $k \leftarrow k + 1$ e repetir o passo 2;
 - (b) Se $\text{Raiz}[u_k] \neq \text{Raiz}[v_k]$, então passar para o passo 3 (onde se insere a aresta e_k);
3. Ligar duas árvores da floresta corrente por intermédio da aresta $e_k = u_k v_k$ (executando INSERIRARESTA(e_k)) e fazer $k \leftarrow k + 1$;
4. Se o número de arestas inseridas é igual a $\nu - 1$, então devolver a árvore abrangente produzida e passar ao passo 5. Caso contrário, passar ao passo 2;
5. Sendo $e_l = u_l v_l$ a última aresta inserida, eliminar e_l (executando ELIMINAARESTA(e_l)) e fazer $k \leftarrow l + 1$. Se a lista de arestas a inserir é vazia e $k = fim$, então parar (neste caso, todas as árvores abrangentes foram geradas). Caso contrário, passar para o passo 2.

Mais formalmente, segue-se o pseudocódigo do Algoritmo 15.4 GERAÁRVORES que descreve este procedimento, assumindo-se que o grafo G é definido pela respectiva lista de arestas, de acordo com (15.2), e que $e_k = u_k v_k$. Neste algoritmo, a tabela Árvore denota a lista de arestas inseridas e a variável i denota o número de arestas inseridas.

Algoritmo 15.4: GERAÁRVORES(G, fim)

```

external RAIZNOVA(), INSEREARESTA(), ELIMINAARESTA()
para todo  $v \in V(G)$ 
  fazer Raiz[ $v$ ] =  $v$ ; Antecessor[ $v$ ] ← 0
   $k \leftarrow 1$ ;  $i \leftarrow 0$ 
  repetir
    se Raiz[ $u_k$ ] ≠ Raiz[ $v_k$ ]
      então  $\begin{cases} \text{INSEREARESTA}(e_k) \\ i \leftarrow i + 1 \\ \text{Árvore}[i] \leftarrow e_k \end{cases}$ 
    se  $i = \nu(G) - 1$  então output ( $\text{Árvore}$ )
    se  $i = \nu(G) - 1 \vee k = \varepsilon(G)$ 
      então  $\begin{cases} \text{ELIMINAARESTA}(\text{Árvore}[i]) \\ k \leftarrow \text{Árvore}[i] + 1 \\ i \leftarrow i - 1 \end{cases}$ 
    senão  $k \leftarrow k + 1$ 
  até  $\text{Árvore}[1] = e_{fim}$ 

```

Exemplo 15.4. Vamos determinar todas as árvores abrangentes do grafo G definido pela matriz de incidência:

$$M_G = \begin{pmatrix} & a & b & c & d & e & f & g \\ v_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ v_2 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ v_3 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ v_4 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ v_5 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Solução. Durante a aplicação do Algoritmo 15.4 GERAÁRVORES, vamos recorrer à notação utilizada no Exemplo 15.3, relativamente à qual, para maior simplicidade de escrita, vamos eliminar as vírgulas e parêntesis nas listas. Adicionalmente, assume-se que as arestas são consideradas por ordem alfabética e que $fim = 3$ (uma vez $d(v_1) = 2$).

Seguem-se as listas sucessivamente geradas pelo algoritmo:

–, a , ab , abe , abd , \boxed{abde} , \boxed{abdf} , \boxed{abdg} , \boxed{abef} , \boxed{abeg} , \boxed{abfg} , abg , ac , acd , \boxed{acde} , \boxed{acef} , \boxed{acdg} , ace , \boxed{acef} , \boxed{aceg} , acf , \boxed{acfg} , acg , ad , ade , \boxed{adef} , \boxed{adeg} , adf , \boxed{adfg} , adg , aef , \boxed{aefg} , aeg , af , afg , ag ,

b , bc , bcd , \boxed{bcde} , \boxed{bdef} , \boxed{bcdg} , bce , \boxed{bcef} , \boxed{bceg} , bcf , \boxed{bcfg} , bcg , bd , bde , \boxed{bdef} , \boxed{bdg} , bdf , \boxed{bdg} ,

bdg , be , bef , \boxed{befg} , beg , bf , bf , bg , bg ,

c .

Dado que $fim = 3$, não é necessário gerar mais florestas. Observe-se que se um subgrafo não contém a aresta a nem a b , então o vértice v_1 aparece isolado e, como consequência, o subgrafo obtido não é um árvore abrangente. Logo, podemos concluir que as 21 árvores abrangentes geradas são todas as árvores abrangentes do grafo. \square

Na Figura ?? faz-se uma representação do grafo G do Exemplo 15.4.

15.4. Código de Prüfer

Arthur Cayley deduziu (em 1889) uma fórmula que determina o número de árvores abrangentes de um grafo completo com n vértices, ou seja, $\tau(K_n)$. Para demonstrar este resultado, vamos recorrer a um método baseado num código de representação de árvores, desenvolvido em 1918, conhecido por *código de Prüfer*³. Denotando por $\mathcal{T}(G)$ o conjunto das árvores abrangentes de um grafo G , a demonstração deste resultado, vai basear-se no estabelecimento de uma bijecção entre o conjunto de todas as árvores abrangentes do grafo completo de ordem $n \geq 2$, $\mathcal{T}(K_n)$, e o conjunto de sequências da forma $(t_1, t_2, \dots, t_{n-2})$, tais que $1 \leq t_i \leq n$, ou seja, o produto cartesiano $[n]^{n-2}$. É, precisamente, esta bijecção, caracterizada pelos $(n-2)$ -uplos $(t_1, t_2, \dots, t_{n-2})$ que se designa por *código de Prüfer*.

Teorema 15.7 (Teorema de Cayley). *O número de árvores abrangentes do grafo completo de ordem $n \in \mathbb{N}$ é dado por*

$$\tau(K_n) = n^{n-2}.$$

Demonstração. É claro que para $n \in \{1, 2\}$ o resultado se verifica. Seja $n > 2$, $V(K_n) = [n]$ e seja T uma árvore abrangente de K_n , a qual vamos representar pelo $(n-2)$ -uplo (t_1, \dots, t_{n-2}) , determinado tal como a seguir se indica. Dado que $V = V(K_n)$ é um conjunto totalmente ordenado pela relação \leq , podemos eliminar sucessivamente, para $i = 1, \dots, n-2$, o menor vértice de grau 1, s_i , da árvore $T - \{s_1, \dots, s_{i-1}\}$, cujo único vizinho é t_i .

Por exemplo, para a árvore representada na Figura 15.7, obtém-se o código de Prüfer é $(4, 3, 5, 3, 4, 5)$.

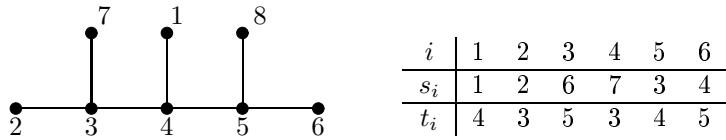


Figura 15.7: Construção de código de Prüfer para a árvore representada.

Mais formalmente, o Algoritmo 15.5 PRÜFER descreve a determinação código de Prüfer.

Algoritmo 15.5: PRÜFER(T)

```

 $R \leftarrow T$ ;  $n \leftarrow \nu(T)$ 
para  $i \leftarrow 1$  até  $n-2$ 
  fazer
     $\begin{cases} s \leftarrow \min\{x \in V(R) : d_R(x) = 1\} \\ t[i] \leftarrow N_R(s) \\ R \leftarrow R - s \end{cases}$ 
devolver  $(t)$ 

```

É claro que este algoritmo define a função

$$\text{PRÜFER} : \mathcal{T}(K_n) \longrightarrow [n]^{n-2}. \quad (15.3)$$

Assim, para completar a prova, basta mostrar que esta função é uma bijecção.

Sobrejectividade. Basta mostrar que para cada sequência $(t_1, t_2, \dots, t_{n-2}) \in [n]^{n-2}$ existe uma árvore que admite este código. Tendo em conta que cada vértice v da árvore T aparece $d_T(v) - 1$ vezes no código $(t_1, t_2, \dots, t_{n-2})$, podemos concluir que as folhas (vértices de grau um) não aparecem neste código e podemos descrever o procedimento de descodificação do seguinte modo:

³Ernst Heinz Prüfer (1896–1934), matemático alemão que trabalhou em grupos abelianos, números algébricos, teoria dos nós e geometria projectiva.

1. Sendo s_1 o menor vértice de V que não aparece em (t_1, \dots, t_{n-2}) , os vértices s_1 e t_1 devem ser ligados por uma aresta.
 2. Sendo s_2 o menor vértice de $V \setminus \{s_1\}$ que não aparece em (t_2, \dots, t_{n-2}) , os vértices s_2 e t_2 devem ser ligados por uma aresta.
- ⋮
- $n - 2$. Sendo s_{n-2} o menor vértice de $V \setminus \{s_1, \dots, s_{n-3}\}$ que não aparece em (t_{n-2}) , os vértices s_{n-2} e t_{n-2} devem ser ligados por uma aresta.
 - $n - 1$. A última aresta (a que não é eliminada pelo algoritmo) é obtida, a partir do conhecimento dos graus dos vértices que se obtêm directamente do código, ligando os vértices do grafo corrente cujos graus diferem em uma unidade do seu valor em T .

Note-se que este procedimento de descodificação permite concluir que a cada código definido por um $(n-2)$ -uplo, (t_1, \dots, t_{n-2}) , corresponde uma única árvore (ou seja, a relação de descodificação é uma função).

Mais formalmente, designando o algoritmo de descodificação (ou reconstrução) de uma árvore, a partir do respectivo código de Prüfer, por Algoritmo 15.6 INVPRÜFER, podemos descrevê-lo, em pseudocódigo, tal como adiante se indica.

Algoritmo 15.6: INVPRÜFER($t[1..n - 2], n$)

```

 $R \leftarrow \{1, 2, \dots, n\}; T \leftarrow \emptyset$ 
para  $i \leftarrow 1$  até  $n - 2$ 
  fazer {
    para  $s \leftarrow 1$  até  $n$ 
      fazer se  $s \in R \wedge s \notin t[i..n - 2]$  então interromper
     $T \leftarrow T \cup \{\text{aresta entre } s \text{ e } t[i]\}; R \leftarrow R \setminus \{s\}$ 
  }
   $T \leftarrow T \cup \{\text{aresta entre } \min(R) \text{ e } \max(R)\}$ 
devolver ( $T$ )
  
```

Injectividade. Suponha que existem duas árvores distintas $T_1, T_2 \in \mathcal{T}(K_n)$ com o mesmo código de PRÜFER. Tendo em conta que o código ordena as arestas, e_1, \dots, e_{n-2} , segundo a ordem pela qual vão sendo eliminadas pelo algoritmo, podemos concluir que as arestas e_1, \dots, e_{n-2} pertencem a ambas as árvores. Logo, T_1 e T_2 distinguem-se apenas em duas arestas, cada uma das quais não é eliminada pelo algoritmo. Porém, tal não é possível, uma vez que (conforme se provou anteriormente) cada código determina uma só árvore.

Como consequência, a função PRÜFER (15.3) é uma bijecção e, por aplicação do princípio da bijecção, o número de árvores abrangentes do grafo completo com n vértices, $\tau(K_n)$, é igual ao número de $(n - 2)$ -uplos com elementos num conjunto de cardinalidade n , ou seja, $\tau(K_n) = n^{n-2}$. \square

Exemplo 15.5. Vamos determinar

- (a) o código de Prüfer para a árvore T apresentada na Figura 15.8,
- (b) a árvore cujo código de Prüfer é $(5, 3, 1, 7, 1, 7)$.

Solução.

- (a) De acorde com o algoritmo PRÜFER, determina-se sucessivamente:

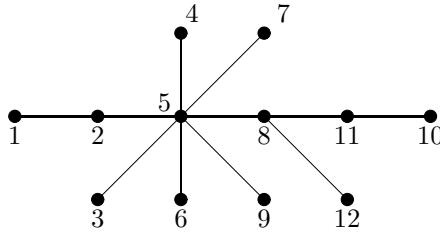


Figura 15.8: Árvore do Exemplo 15.5-(a).

i	1	2	3	4	5	6	7	8	9	10
s_i	1	2	3	4	6	7	9	5	10	11
t_i	2	5	5	5	5	5	5	8	11	8

Logo, o código de Prüfer da árvore T é $(2, 5, 5, 5, 5, 5, 5, 8, 11, 8)$.

(b) Por aplicação do algoritmo INVPRÜFER ao código $(5, 3, 1, 7, 1, 7)$, obtém-se

i	s_i	t_i	$R = V \setminus \{s_1, \dots, s_i\}$
1	2	5	$\{1, 3, 4, 5, 6, 7, 8\}$
2	4	3	$\{1, 3, 5, 6, 7, 8\}$
3	3	1	$\{1, 5, 6, 7, 8\}$
4	5	7	$\{1, 6, 7, 8\}$
5	6	1	$\{1, 7, 8\}$
6	1	7	$\{7, 8\}$

Na Figura 15.9, apresenta-se a árvore que corresponde a esta descodificação. \square

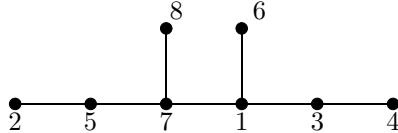


Figura 15.9: Árvore obtida por descodificação do código do Exemplo 15.5-(b).

15.5. Árvores abrangentes de custo mínimo

No caso de grafos com custos nas arestas, o *custo de um subgrafo* corresponde ao custo determinado pela soma dos custos das suas arestas. Em muitas aplicações, é frequente a determinação de árvores abrangentes de custo mínimo. Os algoritmos mais populares para a determinação de árvores abrangentes de custo mínimo, são o algoritmo de Kruskal (que é um algoritmo guloso, *greedy* na terminologia inglesa) e o algoritmo de Prim (que escolhe o vizinho mais próximo).

15.5.1 Algoritmo de Kruskal

O passo básico do algoritmo de Kruskal, aplicado a um grafo G com custos nas arestas, consiste na escolha sucessiva de uma aresta com custo mínimo e na sua posterior eliminação, obtendo-se uma versão modificada do grafo original. Uma vez determinado um subconjunto de arestas $S \subset E(G)$ com

menor custo e que não formam um ciclo no grafo original, determina-se uma aresta e de custo mínimo em $E(G) \setminus S$ tal que $S \cup \{e\}$ continua a não formar um ciclo no grafo original (note-se que a aresta de custo mínimo que é analisada é eliminada do grafo modificado, independentemente de ser ou não escolhida para S). Este procedimento é repetido até se obterem $\nu(G) - 1$ arestas ou até não existirem mais arestas no grafo modificado (neste último caso, conclui-se que o grafo original não é conexo). Para se testar se uma dada aresta forma ou não um ciclo com as arestas já em S , podemos recorrer aos atributos *Raiz* e *Antecessor*, já utilizados anteriormente (ver Secção 15.3), conjuntamente com o Algoritmo 15.2 INSEREARESTA. Segue-se a descrição formal, em pseudocódigo, do Algoritmo 15.7 KRUSKAL, onde $w(e)$ denota o custo da aresta e .

O teorema que se segue, mostra que o algoritmo de Kruskal determina uma árvore abrangente de custo mínimo de um grafo conexo com custos nas arestas.

Teorema 15.8. *Se G é um grafo conexo, então o algoritmo de Kruskal determina uma árvore abrangente de custo mínimo.*

Demonstração. É claro que o algoritmo de Kruskal determina uma árvore abrangente (no caso de grafos conexos). Vamos mostrar, por redução ao absurdo, que esta árvore tem custo mínimo.

Primeiramente, deve observar-se que após Ordenar($E(G)$) (que ordena as arestas segundo os respectivos custos), vem $w(e_1) \leq w(e_2) \leq \dots \leq w(e_\varepsilon)$. Suponha que a árvore \tilde{T} , determinada pelo algoritmo de Kruskal, não é optima (ou seja, não tem custo mínimo).

Algoritmo 15.7: KRUSKAL(G, w)

```

external INSEREARESTA()
para todo  $v \in V(G)$ 
  fazer Raiz[ $v$ ] =  $v$ ; Antecessor[ $v$ ] ← 0
  Ordena( $E(G)$ )
  Árvore ← ∅;  $E \leftarrow E(G)$ ;  $k \leftarrow 1$ 
  repetir
     $u, v \leftarrow$  extremos de aresta  $e_k$ 
    se Raiz[ $u$ ] ≠ Raiz[ $v$ ]
      então INSEREARESTA( $e_k$ ); Árvore ← Árvore ∪ { $e_k$ }
       $E \leftarrow E \setminus \{e_k\}$ ;  $k \leftarrow k + 1$ 
    até |Árvore| = | $V$ | - 1 ∨ | $E$ | = 0
    se |Árvore| ≠ | $V$ | - 1 então output ("O grafo  $G$  não é conexo.")
    devolver (Árvore)
  
```

Considere-se uma árvore abrangente óptima T tal que T e \tilde{T} têm as mesmas arestas com índices não superiores a $k - 1$ e que k é o maior índice nestas condições. Então, e_k é a próxima aresta a inserir no conjunto de arestas que vão formar \tilde{T} e é tal que $e_k \notin E(T)$. Logo, $E(T) \cup \{e_k\}$ contém um ciclo C que, necessariamente, contém uma aresta e que não pertence a $E(\tilde{T})$ e é tal que $w(e) \geq w(e_k)$. Logo, substituindo $E(T)$ por $(E(T) \setminus \{e\}) \cup \{e_k\}$ obtém-se uma árvore abrangente T' de custo não superior ao custo de T .

1. Se $w(e) > w(e_k)$, então T' tem custo inferior ao de T o que é absurdo, uma vez que, por hipótese, T é uma árvore óptima.
2. Se $w(e) = w(e_k)$, então T' tem custo igual ao de T o que é absurdo, uma vez que T' tem pelo menos as k primeiras arestas coincidentes com as de \tilde{T} (o que contraria a definição de T).

Como consequência, podemos concluir que \tilde{T} é uma árvore abrangente óptima. □

Para determinar a complexidade computacional do algoritmo de Kruskal, vamos dividir este algoritmo em duas partes. A primeira diz respeito à ordenação das arestas e pode fazer-se em $\mathcal{O}(\varepsilon \log \varepsilon)$ operações. A segunda produz uma árvore abrangente óptima, com escolhas sucessivas de arestas de custo mínimo de um subconjunto, sucessivamente modificado, de $E(G)$, para a qual são necessárias $\mathcal{O}(\varepsilon \log \nu)$ operações. Uma vez que $\varepsilon = \mathcal{O}(\nu^2)$, podemos concluir que o algoritmo de Kruskal tem uma complexidade computacional de $\mathcal{O}(\varepsilon \log \nu)$.

Exemplo 15.6. Vamos determinar um árvore abrangente de custo mínimo do grafo G com custos nas arestas, definido pela matriz de custos:

$$W_G = \begin{pmatrix} 0 & 1 & \infty & 10 & 8 & 3 \\ 1 & 0 & 13 & 10 & 6 & 4 \\ \infty & 13 & 0 & 15 & \infty & 4 \\ 10 & 10 & 15 & 0 & 9 & \infty \\ 8 & 6 & \infty & 9 & 0 & 7 \\ 3 & 4 & 4 & \infty & 7 & 0 \end{pmatrix},$$

utilizando o algoritmo de Kruskal.

Solução. O primeiro passo do algoritmo consiste na ordenação das arestas de G . Vamos assumir que, como resultado desta ordenação, se obtém: $e_1 = v_1v_2$, $e_2 = v_1v_6$, $e_3 = v_2v_6$, $e_4 = v_3v_6$, $e_5 = v_2v_5$, $e_6 = v_5v_6$, $e_7 = v_1v_5$, $e_8 = v_4v_5$, $e_9 = v_1v_4$, $e_{10} = v_2v_4$, $e_{11} = v_2v_3$ e $e_{12} = v_3v_4$.

Segue-se uma tabela, onde se pretende descrever cada um dos passos resultantes da aplicação do algoritmo.

k	e_k	$w(e_k)$	Insere e_k ?	Árvore
1	v_1v_2	1	sim	$\{v_1v_2\}$
2	v_1v_6	3	sim	$\{v_1v_2, v_1v_6\}$
3	v_2v_6	4	não	
4	v_3v_6	4	sim	$\{v_1v_2, v_1v_6, v_3v_6\}$
5	v_2v_5	6	sim	$\{v_1v_2, v_1v_6, v_3v_6, v_2v_5\}$
6	v_5v_6	7	não	
7	v_1v_5	8	não	
8	v_4v_5	9	sim	$\{v_1v_2, v_1v_6, v_3v_6, v_2v_5, v_4v_5\}$

Note-se que o algoritmo termina, após a inserção da quinta aresta. Na Figura 15.10, representa-se o grafo G e a árvore abrangente de custo mínimo obtida. \square

15.5.2 Algoritmo de Prim

O algoritmo de Prim, também conhecido por *algoritmo do vizinho mais próximo*, aplicado a um grafo G , começa com um vértice arbitrário $a \in V(G)$, a partir do qual se escolhe a aresta de custo mínimo ab , de entre as que lhe são incidentes, com a qual se forma o conjunto corrente de arestas candidatas a incluir na árvore abrangente de custo mínimo. Sendo T o conjunto corrente dos vértices extremos das arestas candidatas a incluir na árvore abrangente de custo mínimo, determina-se a aresta de custo mínimo, de entre as pertencentes ao conjunto de arestas com um único extremo em T , $\partial(T)$, adicionando a T o vértice extremo não pertencente a T da aresta escolhida. Nestas condições, é claro que a aresta escolhida não forma qualquer ciclo. Este procedimento é repetido, até se ter $\partial(T) = \emptyset$ (o que acontece quando $T = V(G)$, no caso de G ser conexo). A determinação do vizinho mais próximo de um vértice v_i pode fazer-se, com recurso a uma estrutura de dados (α_i, β_i) , onde $\alpha_i \in T$ é um vértice mais próximo de v_i , de entre os vértices em T , e β_i é a distância entre o vértice v_i e T , ou seja, o custo da aresta $v_i\alpha_i$. Segue-se a descrição formal, em pseudocódigo, do Algoritmo 15.8 PRIM.

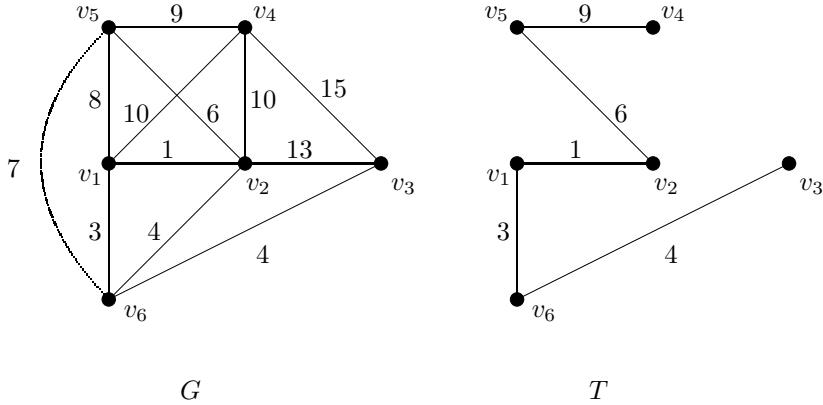


Figura 15.10: Grafo G do Exemplo 15.6 e árvore abrangente de custo mínimo T (obtida pelo algoritmo de Kruskal).

Algoritmo 15.8: PRIM(G, W, v_0)

```

para todo  $v \in V(G)$ 
  fazer  $\begin{cases} \beta[v] \leftarrow W[v, v_0] \\ \text{se } vv_0 \in E(G) \text{ então } \alpha[v] \leftarrow v_0 \end{cases}$ 
 $T \leftarrow \{v_0\}$ ; Árvore  $\leftarrow \emptyset$ ;  $k \leftarrow 1$ 
repetir
   $w_{min} \leftarrow \infty$ 
  para todo  $v \in V(G) \setminus T$ 
    fazer se  $\beta[v] < w_{min}$  então  $w_{min} \leftarrow \beta[v]$ ;  $v_{min} \leftarrow v$ 
    se  $w_{min} = \infty$  então output ("O grafo  $G$  não é conexo.")
     $T \leftarrow T \cup \{v_{min}\}$ 
    Árvore  $\leftarrow$  Árvore  $\cup$  {aresta entre  $v_{min}$  e  $\alpha[v_{min}]$ }
  para todo  $v \in (V(G) \setminus T) \cap N_G(v_{min})$ 
    fazer se  $W[v, v_{min}] < \beta[v]$  então  $\beta[v] \leftarrow W[v, v_{min}]$ ;  $\alpha[v] \leftarrow v_{min}$ 
até  $T = V(G)$ 
devolver (Árvore)
  
```

Para determinar a complexidade computacional de algoritmo de Prim observe-se que o ciclo **repetir** é executado no máximo $\nu - 1$ vezes e de cada vez são necessárias $\mathcal{O}(\nu)$ operações. Logo, a complexidade computacional deste algoritmo é de $\mathcal{O}(\nu^2)$. Pode referir-se, ainda, que recorrendo a estruturas de dados mais elaboradas, se consegue melhorar este algoritmo de modo a obter-se uma complexidade computacional de $\mathcal{O}(\varepsilon \log \nu)$.

Exemplo 15.7. Vamos determinar uma árvore abrangente de custo mínimo, para o grafo do Exemplo 15.6, por aplicação do algoritmo de Prim.

Solução. Seja v_3 , por exemplo, o vértice inicial, pelo que $T = \{v_3\}$ e $\text{Árvore} = \emptyset$. Depois de iniciadas as diferentes variáveis, na tabela a seguir, apresentam-se os diferentes atributos associados aos vértices de $V \setminus T$.

i	1	2	4	5	6
α_i	v_3	v_3		v_3	
β_i	∞	13	15	∞	4

Seguem-se as tabelas de valores (dos atributos) obtidos ao longo das cinco iterações necessárias para a determinação da árvore abrangente de custo mínimo, por aplicação do algoritmo de Prim.

- O menor valor de β_i é $\beta_6 = 4$. Logo, inserimos o vértice v_6 em T e a aresta v_3v_6 na árvore. Como consequência, $T = \{v_3, v_6\}$, $\text{Árvore} = \{v_3v_6\}$ e, actualizando os atributos, obtém-se:

i	1	2	4	5
α_i	v_6	v_6	v_3	v_6
β_i	3	4	15	7

- Neste caso, o menor valor de β_i é $\beta_1 = 3$. Logo, $T = \{v_1, v_3, v_6\}$, $\text{Árvore} = \{v_3v_6, v_1v_6\}$ e, actualizando os atributos, obtém-se:

i	2	4	5
α_i	v_1	v_1	v_6
β_i	1	10	7

- O menor valor de β_i é $\beta_2 = 1$. Logo, $T = \{v_1, v_2, v_3, v_6\}$, $\text{Árvore} = \{v_3v_6, v_1v_6, v_1v_2\}$ e, actualizando os atributos, obtém-se:

i	4	5
α_i	v_1	v_2
β_i	10	6

- O menor valor de β_i é $\beta_2 = 6$. Logo, $T = \{v_1, v_2, v_3, v_5, v_6\}$, $\text{Árvore} = \{v_3v_6, v_1v_6, v_1v_2, v_2v_5\}$ e

i	4
α_i	v_5
β_i	9

- Tendo em conta a última tabela obtida, conclui-se que o vértice v_2 é o vértice da árvore mais próximo de v_4 . Logo, obtém-se a árvore abrangente de custo mínimo: $T = V(G)$ e $\text{Árvore} = \{v_3v_6, v_1v_6, v_1v_2, v_2v_5, v_4v_5\}$.

Note-se que, embora as arestas tenham sido inseridas por uma ordem distinta, a árvore abrangente de custo mínimo obtida pelo algoritmo de Prim é a mesma que foi obtida pelo algoritmo de Kruskal. No caso geral, porém, quando existem várias árvores abrangentes óptimas, nem sempre os algoritmos de Kruskal e de Prim produzem a mesma árvore abrangente de custo mínimo. \square

Em geral, é difícil dizer qual é o melhor algoritmo, de entre os algoritmos de Kruskal e de Prim, uma vez que a sua complexidade computacional é semelhante. Na prática, porém, verifica-se que o algoritmo de Prim é mais rápido para grafos de ordem pequena e dimensão elevada e o algoritmo de Kruskal comporta-se melhor para grafos de ordem elevada e com poucas arestas.

Exemplo 15.8. Utilizando o algoritmo de Prim, vamos determinar uma árvore abrangente de comprimento mínimo no mapa de Portugal representado na Figura 14.8.

Solução. Escolhemos como o vértice inicial a cidade de Lisboa. Logo, $T = \{\text{Lisboa}\}$.

Determinamos a primeira aresta da árvore, considerando todas as arestas entre T e T^c , isto é,

- Lisboa-Óbidos (81 km),
- Lisboa-Santarém (78 km),
- Lisboa-Setúbal (50 km).

Como a aresta mais curta é a última, então Lisboa-Setúbal é a primeira aresta da árvore e fazemos $T = \{\text{Lisboa, Setúbal}\}$.

Determinamos a segunda aresta da árvore, considerando todas as arestas entre T e T^c , isto é,

- Lisboa-Óbidos (81 km),
- Lisboa-Santarém (78 km),
- Setúbal-Évora (103 km),
- Setúbal-Lagos (260 km),
- Setúbal-Albufeira (223 km).

Como a aresta mais curta é Lisboa-Santarém, então inclui-se esta aresta na árvore e fazemos $T = \{\text{Lisboa, Setúbal, Santarém}\}$.

Determinamos a terceira aresta da árvore, considerando todas as arestas entre T e T^c , isto é,

- Lisboa-Óbidos (81 km),
- Setúbal-Évora (103 km),
- Setúbal-Lagos (260 km),
- Setúbal-Albufeira (223 km)
- Santarém-Leiria (70 km),
- Santarém-Castelo Branco (174 km),
- Santarém-Óbidos (42 km),
- Santarém-Portalegre (154 km),
- Santarém-Évora (117 km).

Como a aresta mais curta é Santarém-Óbidos, então inclui-se esta aresta na árvore e fazemos $T = \{\text{Lisboa, Setúbal, Santarém, Óbidos}\}$.

Depois de 27 iterações, obtém-se a árvore abrangente de comprimento mínimo que contém todas as 28 cidades do mapa. Esta árvore está representada na Figura 15.11 e têm um comprimento total 1.614 km.

□

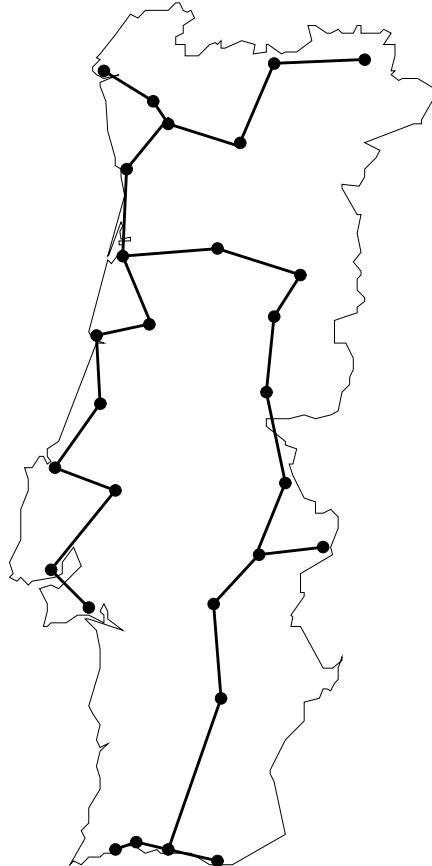


Figura 15.11: Árvore abrangente de comprimento mínimo do mapa de Portugal.

15.6. Exercícios

- 15.1. Represente graficamente todas as árvores de ordem três com raiz e indique o número destas árvores duas a duas não isomórficas.
- 15.2. Represente graficamente todas as árvores com raiz de ordem quatro e indique o número destas árvores duas a duas não isomórficas.
- 15.3. Represente graficamente todas as árvores com raiz de ordem cinco e indique o número destas árvores duas a duas não isomórficas.
- 15.4. Sendo T uma árvore, responda às seguintes questões:
 - (a) Prove que $\sum_{v \in V(T)} (2 - d_T(v)) = 2$.
 - (b) Prove que se T tem um vértice de grau $m \geq 2$, então tem pelo menos m vértices de grau 1.
 - (c) Dê um exemplo de uma árvore com um vértice de grau m e apenas m folhas.

- 15.5. Mostre que qualquer árvore tem exactamente um ou dois vértices centrais.
- 15.6. Dados dois inteiros positivos n e p tais que $3 \leq p \leq n$, seja $T(n, p - 1)$ o grafo de Turan, ou seja, grafo $(p - 1)$ -partido completo de ordem n tal que o número de vértices em cada duas partições ou é igual ou difere em apenas uma unidade. Prove que este grafo é único.
- 15.7. Demonstre que se um grafo G de ordem ν tem no máximo $\nu - 2$ arestas, então é desconexo.
- 15.8. Demonstre que se um grafo G de ordem ν tem pelo menos ν arestas, contém um ciclo.
- 15.9. Dados dois grafos G_1 e G_2 definidos sobre o mesmo conjunto de vértices $V = V(G_1) = V(G_2)$, definimos $G_1 \oplus G_2 = G$ tal que $V(G) = V$ e $E(G) = E(G_1) \cup E(G_2)$. Sendo T_1, T_2, \dots, T_k , uma colecção de k árvores tal que $V(T_1) = V(T_2) = \dots = V(T_k)$, considerando o grafo $H = T_1 \oplus T_1 \oplus \dots \oplus T_k$, responda às seguintes questões:
- Verifique se os grafo H é k -aresta conexo.
 - Prove ou refute a seguinte afirmação: se $|V(H)| \geq k + 1$, então H é k -conexo.
 - Prove que $\exists v \in V(H)$ tal que $d_H(v) \leq 2k - 1$.
- 15.10. Seja T uma árvore de ordem $p + q$, com p vértices de grau um.
- Mostre que a soma dos graus dos vértices de grau superior a um é igual $p + 2(q - 1)$.
 - Mostre que se em T existem dois vértices de grau três, então também existem quatro vértices de grau um.
- 15.11. Dado um número natural $n \in \mathbb{N}$, sabendo que o grafo representativo da molécula de álcool $C_nH_{2n+1}OH$ tem como vértices C , H e O , com valências 4, 1 e 2, respectivamente, mostre que este grafo é uma árvore.
- 15.12. Determine o número de moléculas que correspondem à fórmula C_5H_{12} (tendo em conta que cada molécula é definida por uma árvore com 5 vértices C de grau 4 e 12 vértices H de grau 1).
- Represente os grafos que definem cada uma destas moléculas.
 - Determine o número de árvores de ordem 5 não isomorfos.
 - Tendo conta o resultado obtido na alínea anterior, estabeleça a sua relação com os subgrafos induzidos pelos vértices C (átomos de carbono) nas árvores que definem as moléculas referidas em (a).
- 15.13. Dado um grafo G , prove que se todos os vértices têm, pelo menos, grau 2, então G contém um ciclo.
- 15.14. Mostre que toda a árvore não trivial tem dois vértices de grau um.
- 15.15. Demonstre que se G é um grafo bipartido k -regular, então contém um 1-factor.
- 15.16. Sendo T uma árvore de ordem ν e G um grafo simples tal que $\delta(G) \geq \nu - 1$, mostre que G contém um subgrafo isomorfo a T .
- 15.17. Seja $k \in \mathbb{N}$ e seja T uma árvore de ordem $k + 1$. Mostre que se G é um grafo simples tal que $\delta(G) \geq k$, então G contém um subgrafo isomorfo de T .
- 15.18. Sejam T_1, T_2, \dots, T_k sub-árvores da árvore T de tal modo que quaisquer duas sub-árvores, T_i e T_j , têm um vértice em comum. Prove que todas as árvores têm um vértice em comum.

15.19. Mostre que o número de árvores abrangentes de um grafo completo K_n que não contém uma aresta fixa e , é igual $(n-2)n^{n-3}$.

15.20. Qual o número médio de árvores abrangentes entre todos os grafos simples com n vértices?

15.21. Considere o grafo G do exercício 19.33. Seja a_n o número de árvores abrangentes de G e b_n o número de árvores abrangentes que contêm a aresta x_1y_1 .

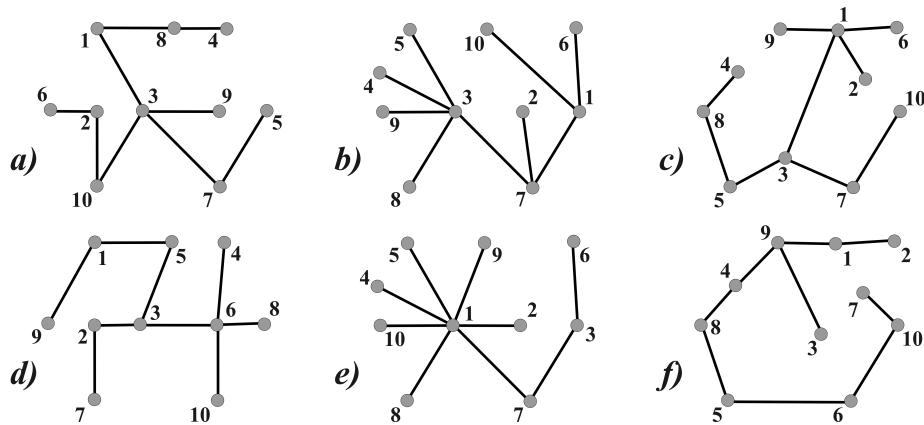
(a) Prove que $a_n = a_{n-1} + b_n$.

(b) Escreva uma expressão para b_n em função de a_{n-1} e b_{n-1} .

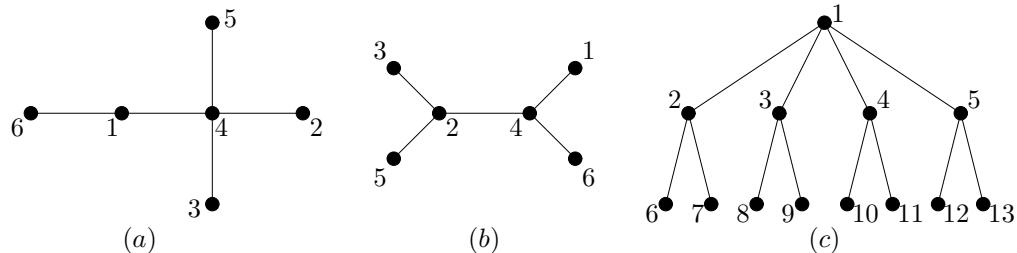
(c) Utilize os resultados obtidos em (a) e (b) para resolver a equação de recorrência de a_n .

15.22. Mostre que o número de árvores T tais que $V(T) = \{v_1, v_2, \dots, v_n\}$ e $d_T(v_1) = k$ é igual $\binom{n-2}{k-1}(n-1)^{n-k-1}$.

15.23. Determine os códigos de Prüfer das árvores representadas na figura que se segue.



15.24. Determine os códigos de Prüfer que correspondem às árvores que se representam na figura:



15.25. Determine as árvores etiquetadas definidas pelos seguintes códigos de Prüfer:

(a) $(1, 2, 3, 4, 5)$;

(b) $(3, 3, 3, 3, 3)$;

(c) $(2, 8, 6, 3, 1, 2)$.

15.26. Represente graficamente as árvores determinadas pelos seguintes códigos de Prüfer:

(a) $(7, 2, 3, 3, 3, 4)$,

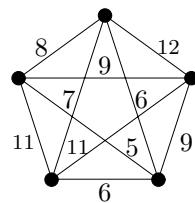
(b) $(1, 2, 3, 4, 5, 6)$,

- (c) $(8, 8, 8, 8, 8, 8)$,
 (d) $(1, 2, 1, 2, 1, 2)$,
 (e) $(2, 1, 2, 1, 2, 1)$.

15.27. Dados os números naturais d_1, d_2, \dots, d_n tais que $\sum_{i=1}^n d_i = 2n - 2$, determine o número de árvores com vértices $1, 2, \dots, n$ tais que $d(1) = d_1, d(2) = d_2, \dots, d(n) = d_n$.

15.28. Dada a sequência de graus dos vértices $\mathbf{d} = (d_1, d_2, \dots, d_n)$, mostre que existem exactamente $\frac{(n-2)!}{\prod_{i=1}^n (d_i-1)!}$ árvores etiquetadas, de ordem n com esta sequência de graus.

15.29. Determine uma árvore abrangente de custo mínimo do grafo representado na figura a seguir, utilizando o algoritmo de Prim.



15.30. Tendo presente a noção de distância entre dois vértices x e y , $d(x, y)$ (ver Definição 12.12) designa-se por *árvore binária* uma árvore T com um vértice especial, $r \in V(T)$, de grau 2 que se designa por raiz e onde os restantes vértices $v \in V(T) \setminus \{r\}$ têm grau não superior a 3, um único vizinho à distância $d(v, r) - 1$ de r e no máximo dois vizinhos à distância $d(v, r) + 1$ de r . Considerando esta definição de árvore binária, prove que o número de árvores binárias não isomórfas de ordem n vem dado por $C_n = \frac{1}{n+1} \binom{2n}{n}$, onde C_n denota o número de Catalan.

16

Fluxos em Redes

Este capítulo é dedicado a uma das aplicações mais frequentes dos grafos orientados com pesos nos arcos, os modelos de circulação de *fluxo* de uma certa substância, de objectos, de comunicações, etc, de uma origem a um destino, através de diferentes canais ligados entre si, muitas vezes, com limitações de capacidade. Por exemplo, o fluxo de veículos através de um sistema de estradas, petróleo através de condutas, mensagens através de redes de comunicação, pessoas através de alfândegas num grande aeroporto, etc. De um modo geral, além da limitação das quantidades que podem fluir por cada arco, existe um custo de transporte. Neste contexto, os grafos orientados aparecem quase sempre com capacidades e, algumas vezes, com custos associados aos arcos e designam-se por *redes* ou *redes de transporte*.

Definição 16.1 (Rede). *Um digrafo conexo sem lacetes \vec{R} diz-se uma rede (ou rede de transporte), se se verificam as seguintes condições:*

- (a) *Existe pelo menos um vértice $s \in V(\vec{R})$ que injecta fluxo na rede (vértice fonte).*
- (b) *Existe pelo menos um vértice $t \in V(\vec{R})$ que consome fluxo da rede (vértice sorvedouro).*
- (c) *Existe uma função de capacidade $c : E(\vec{R}) \mapsto \mathbb{R}_+ \cup \{\infty\}$ (onde \mathbb{R}_+ denota o conjunto dos números reais não negativos).*
- (d) *Existe uma função de custo $w : E(\vec{R}) \mapsto \mathbb{R} \cup \{\infty\}$.*

Nas aplicações onde as capacidades dos arcos não são relevantes, podemos considerar a função c como sendo uma função constante, tal que $c(e) = \infty \forall e \in E(\vec{R})$ (ou, simplesmente, ignora-la) e nas aplicações onde os custos dos arcos não são relevantes, podemos considerar a função w como sendo uma função constante, tal que $w(e) = 0 \forall e \in E(\vec{R})$ (ou, simplesmente, ignora-la).

Por exemplo, o digrafo representado na Figura 16.1 é uma rede, onde s é a origem, t é o destino e os pesos associados aos arcos correspondem às respectivas capacidades (neste caso, o custo dos arcos é irrelevante). Dado que $c(sa) + c(sb) = 5 + 7 = 12$ a quantidade total de bens a transportar de s para t , não pode exceder 12. Por outro lado, uma vez que $c(ct) + c(dt) = 5 + 6 = 11$, podemos concluir que, afinal, esta quantidade é não superior a 11.

16.1. Fluxo máximo em redes

Nos problemas de fluxo máximo em redes, como o próprio nome indica, o objectivo é a determinação da maior quantidade de fluxo que é possível transportar entre um vértice s e um vértice t da rede, respeitando os limites impostos pelas capacidades dos arcos. Como consequência, no caso dos problemas de fluxo máximo em redes, as redes que modelam estes problemas têm as seguintes particularidades:

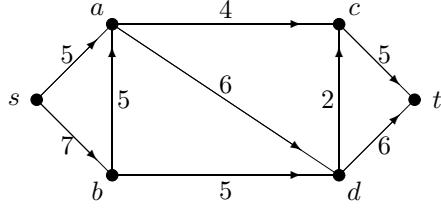


Figura 16.1: Exemplo de uma rede com capacidades nos arcos.

1. Existe apenas um vértice fonte $s \in V(\vec{R})$ cujo semigrau de entrada é nulo, ou seja, $d^-(s) = 0$, que se designa por origem da rede.
2. Existe apenas um vértice sorvedouro $t \in V(\vec{R})$ cujo semigrau de saída é nulo, ou seja, $d^+(t) = 0$, que se designa por destino da rede.

Segue-se a definição dos conceitos de fluxo e valor do fluxo.

Definição 16.2 (Fluxo, valor do fluxo). *Dada uma rede de transporte \vec{R} , designa-se por fluxo em \vec{R} a função $f : E(\vec{R}) \mapsto \mathbb{R}_+$ que verifica as seguintes condições:*

$$(a) \quad \forall_{e \in E(\vec{R})} f(e) \leq c(e),$$

$$(b) \quad \forall_{v \in V(\vec{R}) \setminus \{s, t\}} \sum_{w \in V(\vec{R})} f(wv) = \sum_{w \in V(\vec{R})} f(vw), \text{ onde } f(xy) = 0 \text{ se } xy \notin E(\vec{R}).$$

Por sua vez $\text{val}(f) = \sum_{w \in V(\vec{R})} f(sw)$, denota o valor do fluxo f .

A condição (a) impõe que o fluxo em qualquer arco não exceda a respectiva capacidade e a condição (b) impõe o designado *princípio de conservação do fluxo*, ou seja, em cada vértice $v \notin \{s, t\}$ a quantidade de fluxo que chega a v é igual à quantidade de fluxo que sai de v .

Na Figura 16.2 representa-se a rede da Figura 16.1, com um par $(c(e), h(e))$ associado a cada um dos arcos e , onde c denota uma função de capacidade e h uma função real (com valores não negativos) definida no conjunto dos arcos. Porém, verifica-se que a função h é um fluxo apenas em (A), uma vez que em (B) o princípio de conservação do fluxo não se verifica. Por exemplo, para o vértice b , vem $\sum_{w \in V} h(wb) = 5$ e $\sum_{w \in V} h(bw) = 4$.

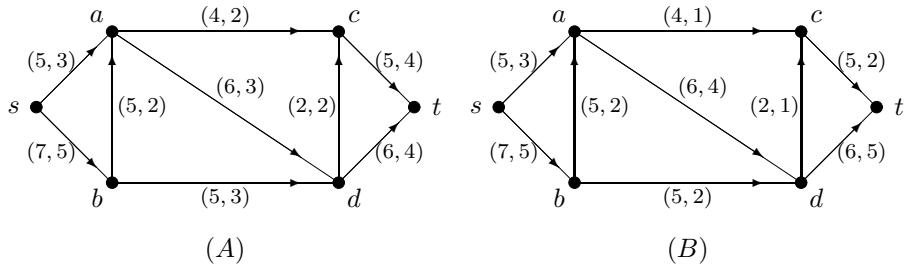


Figura 16.2: Exemplos de funções definidas nos arcos da rede da Figura 16.1.

Na Figura 16.2-(A), verifica-se ainda que o valor do fluxo na rede é

$$\text{val}(h) = h(sa) + h(sb) = 3 + 5 = 8.$$

Tendo em conta a Figura 16.2-(A), será que existe um outro fluxo f tal que $\text{val}(f) > \text{val}(h) = 8$? Note-se que, geralmente, neste tipo de problemas, o nosso objectivo é determinar um fluxo de valor máximo que, usualmente, se designa por *fluxo máximo*. Com este fim, antes de mais, convém observar que para o fluxo representado na Figura 16.2-(A), $\sum_{w \in V} f(sw) = \sum_{w \in V} f(wt) = 8$, ou seja, o fluxo total que sai da origem é igual ao fluxo total que entra no destino. Será que acontece sempre assim? A resposta é afirmativa, uma vez que pelo princípio da conservação do fluxo, para um vértice arbitrário v (distinto de s e t), a quantidade de fluxo que entra em v é igual à quantidade de fluxo que sai de v . Logo, a soma dos fluxos nos arcos de saída da fonte é igual à soma dos fluxos nos arcos de entrada no destino, o que não é mais do que $\text{val}(f)$. Observe-se, ainda, que na Figura 16.2-(A), para o arco dc , temos $h(dc) = c(dc) = 2$. Neste caso, diz-se que o arco está *saturado*. Quando, para um dado fluxo f , uma função de capacidade c e um arco e se verifica que $f(e) < c(e)$, diz-se que e é um arco *não saturado*.

16.1.1 Teorema de Ford e Fulkerson

Antes de prosseguirmos, convém introduzir os conceitos de corte e corte- uv .

Definição 16.3 (Corte e corte- uv). *Dado um grafo (digrafo) G designa-se por corte todo o subconjunto de arestas (arcos) $C \subset E(G)$ tal que $cc(G - C) > cc(G)$ e $\forall C' \subset C \quad cc(G - C') = cc(G)$. Dados dois vértices $u, v \in V(G)$ e um corte C , se u e v são conexos em G mas não são conexos em $G - C$, então o corte C designa-se por uv -corte.*

No caso das redes \vec{R} com origem s e destino t , dada a particular relevância dos cortes- st , vamos designá-los, simplesmente, por cortes. Assim, um corte C na rede \vec{R} é um conjunto de arcos que desconexa s e t . Por exemplo, na Figura 16.3, cada uma das linhas tracejadas indica um corte para a rede representada.

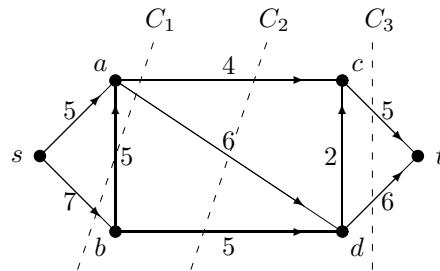


Figura 16.3: Exemplos de cortes de uma rede.

O corte C_1 consiste nos arcos sb, ba, ac e ad (ou seja, $C_1 = \{sb, ab, ac, ad\}$). O corte C_2 consiste em bd, ad, ac e $C_3 = \{ct, dt\}$. Note-se que qualquer corte determina uma partição do conjunto dos vértices da rede em dois subconjuntos não vazios P e P^c .

Neste capítulo, dada uma rede \vec{R} com origem s e destino t e um corte C , vamos denotar o subconjunto da respectiva partição de $V(\vec{R})$ que contém s por P_s e o subconjunto que contém t por P_t . Por sua vez, o corte C também se denota por $\partial(P_s, P_t)$ ou simplesmente por $\partial(P_s)$. O conjunto dos arcos com cauda em P_s e cabeça em P_t denota-se por $\partial^+(P_s)$ e o conjunto dos arcos com cabeça em P_s e cauda em P_t denota-se por $\partial^-(P_s)$. Assim, $\partial(P_s) = \partial^+(P_s) \cup \partial^-(P_s)$. Por exemplo, considerando o corte C_1 da rede da Figura 16.3, podemos concluir que $P_s = \{s, a\}$, $P_t = \{b, c, d, t\}$, $\partial^+(P_s) = \{sb, ac, ad\}$ e $\partial^-(P_s) = \{ba\}$.

A capacidade do corte $C = \partial(P_s)$ denota-se por $c(P_s, P_t)$ e define-se pela igualdade:

$$c(P_s, P_t) = \sum_{e \in \partial^+(P_s)} c(e).$$

Exemplo 16.1. Vamos determinar as capacidades dos cortes definidos na Figura 16.3.

Solução.

1. Para o corte C_1 , vem $P_s = \{s, a\}$ e

$$c(P_s, P_t) = c(sb) + c(ad) + c(ac) = 7 + 6 + 4 = 17.$$

2. Para o corte C_2 , vem $P_s = \{s, a, b\}$ e

$$c(P_s, P_t) = c(ac) + c(ad) + c(bd) = 4 + 6 + 5 = 15.$$

3. Para o corte C_3 , vem $P_s = \{s, a, b, c, d\}$ e

$$c(P_s, P_t) = c(ct) + c(dt) = 5 + 6 = 11.$$

□

Teorema 16.1. Seja f um fluxo na rede \vec{R} e $\partial(P_s)$ um st-corte. Então

$$\text{val}(f) = \sum_{e \in \partial^+(P_s)} f(e) - \sum_{e \in \partial^-(P_s)} f(e).$$

Demonstração. A demonstração baseia-se no facto de que qualquer fluxo da origem até ao destino tem de passar pelos arcos que ligam vértices dos conjuntos P_s e P_t . Assim, uma vez que $\sum_{e \in \partial^-(\{s\})} f(e) = 0$, podemos concluir as igualdades

$$\text{val}(f) = \sum_{e \in \partial^+(\{s\})} f(e) = \sum_{e \in \partial^+(\{s\})} f(e) - \sum_{e \in \partial^-(\{s\})} f(e).$$

Por outro lado, $\forall x \in P_s \setminus \{s\}$, $\sum_{e \in \partial^+(\{x\})} f(e) - \sum_{e \in \partial^-(\{x\})} f(e) = 0$. Logo,

$$\begin{aligned} \text{val}(f) &= \sum_{v \in P_s} \left(\sum_{e \in \partial^+(\{v\})} f(e) - \sum_{e \in \partial^-(\{v\})} f(e) \right) \\ &= \sum_{\substack{v \in P_s \\ x \in V}} f(vx) - \sum_{\substack{v \in P_s \\ x \in V}} f(xv) \\ &= \sum_{\substack{v \in P_s \\ x \in P_s}} f(vx) + \sum_{\substack{v \in P_s \\ x \in P_t}} f(vx) - \sum_{\substack{v \in P_s \\ x \in P_s}} f(xv) - \sum_{\substack{v \in P_s \\ x \in P_t}} f(xv) \\ &= \sum_{\substack{v \in P_s \\ x \in P_t}} f(vx) - \sum_{\substack{v \in P_s \\ x \in P_t}} f(xv) \\ &= \sum_{e \in \partial^+(P_s)} f(e) - \sum_{e \in \partial^-(P_s)} f(e). \end{aligned}$$

□

Como consequência imediata deste teorema, obtém-se o seguinte corolário:

Corolário 16.2. Sendo f um fluxo para a rede \vec{R} e $\partial(P_s)$ é um st -corte, então $\text{val}(f) \leq c(P_s, P_t)$.

Demonstração. Tendo em conta o Teorema 16.1, obtém-se

$$\text{val}(f) = \sum_{e \in \partial^+(P_s)} f(e) - \sum_{e \in \partial^-(P_s)} f(e) \leq c(P_s, P_t) - \sum_{e \in \partial^-(P_s)} f(e).$$

Logo, uma vez que $\sum_{e \in \partial^-(P_s)} f(e) \geq 0$, vem $\text{val}(f) \leq c(P_s, P_t)$. \square

Este corolário mostra que, dada uma rede arbitrária \vec{R} , o valor de qualquer fluxo é não superior à capacidade de qualquer corte e isto significa que o valor do fluxo máximo não pode exceder a capacidade do corte de menor capacidade, usualmente designado por *corte mínimo*.

Considerando uma rede \vec{R} e um seu fluxo f , o arco $e \in E(\vec{R})$, com extremos nos vértices u e v , diz-se útil relativamente ao fluxo f de u para v , se se verifica uma das seguintes condições:

$$e = uv \quad \text{e} \quad f(e) < c(e)$$

ou

$$e = vu \quad \text{e} \quad f(e) > 0.$$

No primeiro caso, o arco útil e diz-se *concordante* e no segundo diz-se *contrário*.

Definição 16.4 (Caminho de aumento). Dada uma rede \vec{R} e um seu fluxo f , designa-se por caminho de aumento para f , todo o caminho

$$v_0e_1v_1e_2v_2, \dots, v_{k-1}e_kv_k,$$

tal que $v_0 = s$ e, para $i = 1, 2, \dots, k$, o arco e_i é um arco útil, relativamente ao fluxo f , de v_{i-1} para v_i . Adicionalmente, se $v_k = t$, então o caminho de aumento diz-se completo.

Vamos mostrar que a existência de um caminho de aumento completo para o fluxo f implica que esse fluxo não seja máximo. Com efeito, seja $v_0e_1v_1e_2v_2, \dots, v_{k-1}e_kv_k$, um caminho de aumento completo, relativamente ao fluxo f , e seja

$$\delta = \min\{\delta(e_i) : 1 \leq i \leq k\},$$

onde

$$\delta(e_i) = \begin{cases} c(e_i) - f(e_i), & \text{se } e_i \text{ é concordante;} \\ f(e_i), & \text{se } e_i \text{ é contrário.} \end{cases}$$

É claro que $\delta > 0$. Logo, alterando o fluxo f nos arcos deste caminho de aumento completo, de modo a obter o fluxo f' tal que

$$f'(e_i) = \begin{cases} f(e_i) + \delta, & \text{se } e_i \text{ é concordante;} \\ f(e_i) - \delta, & \text{se } e_i \text{ é contrário,} \end{cases}$$

o valor do fluxo f' é superior ao valor do fluxo f .

Teorema 16.3. Sendo \vec{R} uma rede e f um fluxo, as seguintes afirmações são equivalentes.

- (a) O fluxo f é máximo.
- (b) Não existe nenhum caminho de aumento completo para f .
- (c) Existe um corte- st $\partial(P_s)$ tal que $\text{val}(f) = c(P_s, P_t)$.

Demonstração.

(a) \Rightarrow (b) Anteriormente demonstrou-se que a existência de um caminho de aumento completo implica que o fluxo não seja máximo e essa demonstração serve também para esta implicação.

(b) \Rightarrow (c) Suponha que f é um fluxo e não existe nenhum caminho de aumento completo relativamente a ele. Seja P_s o conjunto de vértices que são extremos de caminhos de aumento e $P_t = V(\vec{R}) \setminus P_s$. É claro, que $s \in P_s$ (uma vez que, por definição, o caminho s , sem arcos, é um caminho de aumento) e $t \in P_t$. Se $e \in \partial^+(P_s)$ ($e' \in \partial^-(P_s)$), por definição de P_s , $f(e) = c(e)$ ($f(e') = 0$). Logo,

$$\sum_{e \in \partial^+(P_s)} f(e) = c(P_s, P_t), \quad \sum_{e \in \partial^-(P_s)} f(e) = 0$$

e, consequentemente, tendo em conta o Teorema 16.1,

$$\text{val}(f) = c(P_s, P_t).$$

(c) \Rightarrow (a) Esta implicação é consequência directa de Corolário 16.2. \square

Segue-se um resultado clássico obtido (independentemente) por Ford e Fulkerson, publicado em 1955, conhecido por *teorema de Ford-Fulkerson* ou *teorema do fluxo máximo - corte mínimo* e que é consequência directa do teorema anterior.

Teorema 16.4 (Ford-Fulkerson). *Dada uma rede arbitrária, o valor de um fluxo máximo é igual à capacidade de um corte mínimo.*

A demonstração original de Ford e Fulkerson é construtiva e vai ser utilizada, mais adiante, para descrever um algoritmo de determinação de um fluxo máximo.

Exemplo 16.2. Vamos mostrar que o fluxo apresentado na Figura 16.4 é máximo.

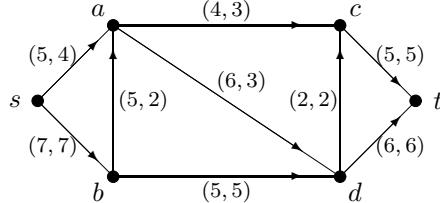


Figura 16.4: Exemplo de fluxo máximo.

Solução. Por definição, $\text{val}(f) = f(s, a) + f(s, b) = 4 + 7 = 11$. Por outro lado, a capacidade do corte C_3 representado na Figura 16.3 é $c(C_3) = 11$ (ver Exemplo 16.1). Logo, o fluxo f é máximo. \square

16.1.2 Algoritmo para o fluxo máximo

Segue-se o algoritmo de Ford-Fulkerson, para a determinação do fluxo máximo, o qual é baseado num *procedimento de visita e marcação de vértices*. Diz-se que um vértice é *visitado* quando a, a partir dele, se testa a possibilidade de marcação dos seus vizinhos. Por sua vez, o vértice v é marcado com $(p(v)^+, \Delta v)$ ($(p(v)^-, \Delta v)$), onde $p(v)$ denota o vértice candidato a enviar (retirar) o acréscimo (decréscimo) de fluxo Δv que o vértice v é capaz de receber (deixar de enviar) através do arco $p(v)v$ ($vp(v)$). Porém, o vértice s é marcado com $(-, \infty)$ para significar que s pode receber qualquer quantidade do fluxo do exterior. Uma vez que o objectivo do procedimento de marcação de vértices é a obtenção de um caminho de aumento completo, este procedimento também se designa por *procedimento de determinação de um caminho de aumento completo*.

Algoritmo de fluxo máximo

Dados de entrada: Rede \vec{R} e função de capacidade $c : E(\vec{R}) \mapsto \mathbb{R}_+$.

Resultados de saída: Fluxo máximo f .

Passo 1: Definir um fluxo inicial f em \vec{R} (por exemplo, fazendo $f(e) = 0$, para cada $e \in E(\vec{R})$).

Passo 2: Marcar a origem s , com $(-, \infty)$.

Passo 3: Se t está marcado, então passar ao passo 5 (existe um caminho de aumento completo). Se não existem vértices marcados por visitar, então PARAR (f é um fluxo máximo).

Passo 4: Escolher um vértice x marcado e não visitado e fazer:

- Para cada y ainda não marcado, tal que $xy \in E(\vec{R})$ e $f(xy) < c(xy)$, marcar y com $(x^+, \Delta y = \min\{\Delta x, c(xy) - f(xy)\})$ (note-se que y passa a estar marcado, mas ainda não foi visitado, e esta marca indica que o fluxo corrente de s para y pode ser aumentado Δy).
- Para cada y ainda não marcado, tal que $yx \in E(\vec{R})$ e $f(yx) > 0$, marcar y com $(x^-, \Delta y = \min\{\Delta x, f(yx)\})$ (note-se que y passa a estar marcado, mas ainda não foi visitado, e esta marca indica que o fluxo corrente de s para y pode ser aumentado Δy).
- Passar para o passo 3.

Passo 5: Modificar o fluxo f para f' , com $\text{val}(f') = \text{val}(f) + \Delta t$, de acordo com o seguinte procedimento:

- $z \leftarrow t$
- Se $z = s$, remover todas as marcas e passar ao passo 2.
- Se a marca de z é $(y^+, \Delta y)$, fazer $f'(yz) = f(yz) + \Delta t$.
- Se a marca de z é $(y^-, \Delta y)$, fazer $f'(zy) = f(zy) - \Delta t$.
- $z \leftarrow y$ e voltar ao item (b).

Observe-se que, neste algoritmo, quando um vértice pode ser marcado a partir de dois ou mais vértices distintos, a escolha do vértice x que determina a marcação é completamente arbitrária. Mais formalmente, este procedimento é descrito com recurso ao pseudocódigo Algoritmo 16.1 FORD-FULKERSON.

Segue-se um exemplo de aplicação deste algoritmo.

Exemplo 16.3. Vamos determinar um fluxo máximo para a rede da Figura 16.5.

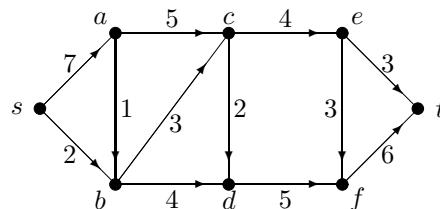


Figura 16.5: Rede com capacidades nos arcos.

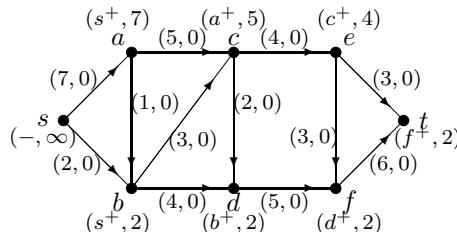
Algoritmo 16.1: FORD-FULKERSON(\vec{R}, c, s, t)

```

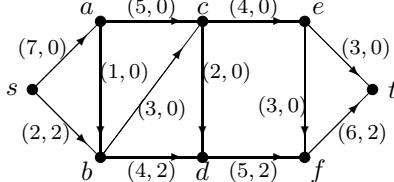
para todo  $e \in E(\vec{R})$  fazer  $f[e] \leftarrow 0$ 
    Marca[s]  $\leftarrow (-, \infty)$ ;  $W[1] \leftarrow s$ 
repetir
    Marcados  $\leftarrow 1$ ; Visitados  $\leftarrow 0$ ; NãoMarcados  $\leftarrow V(\vec{R}) \setminus \{s\}$ 
    repetir
        Visitados  $\leftarrow$  Visitados + 1;  $x \leftarrow W[Visitados]$ 
        para todo  $y \in \{y \in \text{NãoMarcados} : xy \in E(\vec{R}), f[xy] < c[xy]\}$ 
            fazer  $\begin{cases} \text{Marca}[y] \leftarrow (x^+, \min\{\Delta x, c[xy] - f(xy)\}) \\ \text{Marcados} \leftarrow \text{Marcados} + 1; W[\text{Marcados}] \leftarrow y \\ \text{NãoMarcados} \leftarrow \text{NãoMarcados} \setminus \{y\} \end{cases}$ 
        para todo  $y \in \{y \in \text{NãoMarcados} : yx \in E(\vec{R}), f[yx] > 0\}$ 
            fazer  $\begin{cases} \text{Marca}[y] \leftarrow (x^-, \min\{\Delta x, f(yx)\}) \\ \text{Marcados} \leftarrow \text{Marcados} + 1; W[\text{Marcados}] \leftarrow y \\ \text{NãoMarcados} \leftarrow \text{NãoMarcados} \setminus \{y\} \end{cases}$ 
        até  $t \notin \text{NãoMarcados} \vee \text{Marcados} = \text{Visitados}$ 
        se  $t \notin \text{NãoMarcados}$ 
            então  $\begin{cases} z \leftarrow t \\ \text{enquanto } z \neq s \\ \quad \text{fazer } \begin{cases} \text{se } \text{Marca}[z] = (y^+, \Delta y) \\ \quad \text{então } f[yz] \leftarrow f[yz] + \Delta t \\ \text{se } \text{Marca}[z] = (y^-, \Delta y) \\ \quad \text{então } f[zy] \leftarrow f[zy] - \Delta t \\ z \leftarrow y \end{cases} \end{cases}$ 
        até  $t \in \text{NãoMarcados}$ 
devolver  $(f)$ 

```

Solução. Aplicando o algoritmo de fluxo máximo a esta rede, a primeira iteração do procedimento de marcação tem como resultado as marcas representadas em (1.a) (ver figura a seguir), a partir das quais se obtém o fluxo representado em (1.b).

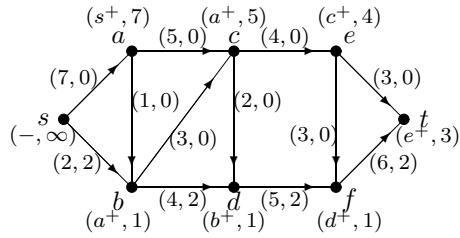


(1.a)

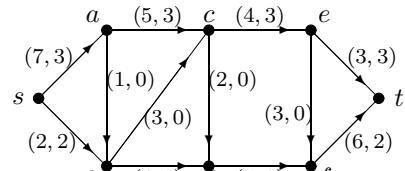


(1.b)

Observe-se que, com a aplicação do procedimento de marcação, o vértice c pode ser marcado com $(a^+, 5)$ ou $(b^+, 2)$ e o vértice t com $(f^+, 2)$ ou $(e^+, 3)$, tendo a escolha sido feita arbitrariamente. A segunda iteração do procedimento de marcação tem como resultado as marcas apresentadas em (2.a), na figura a seguir, a partir das quais se obtém o fluxo representado em (2.b).

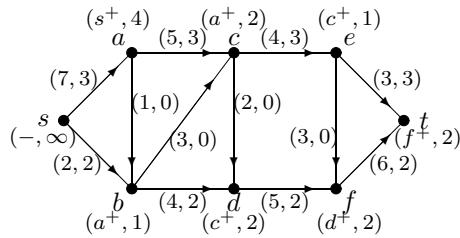


(2.a)

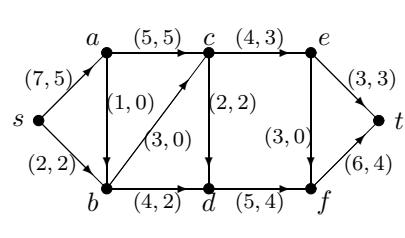


(2.b)

Note-se que nesta iteração do procedimento de marcação, a escolha das marcas de alguns vértices é arbitrária. Por exemplo, o vértice d pode ser marcado com $(b^+, 1)$ ou $(c^+, 2)$, etc. A terceira iteração do procedimento de marcação tem como resultado as marcas apresentadas em (3.a), na figura a seguir, a partir das quais se obtém o fluxo representado em (3.b).

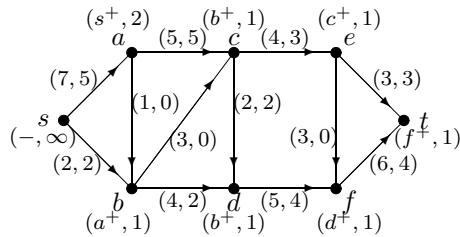


(3.a)

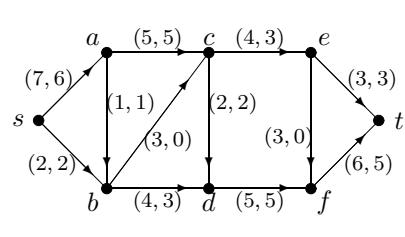


(3.b)

A quarta iteração do procedimento de marcação tem como resultado as marcas representadas em (4.a), na figura a seguir, a partir das quais se obtém o fluxo representado em (4.b).

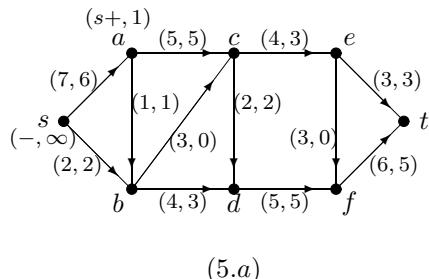


(4.a)

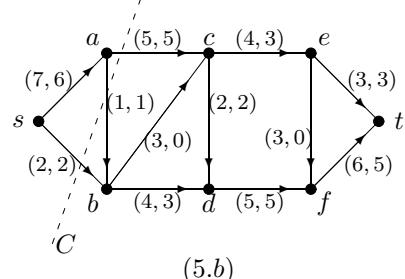


(4.b)

Nesta fase, não é possível obter qualquer caminho de aumento, uma vez que as marcações efectuadas pelo procedimento não atingem o vértice t , conforme se ilustra em (5.a), na figura a seguir.



(5.a)



(5.b)

Assim, podemos concluir que o fluxo corrente é máximo. Com efeito, conforme se pode observar em (5.b), podemos determinar o corte $C = (P_s, P_t)$, onde P_s é o conjunto dos vértices terminais de todos os caminhos de aumento, ou seja, P_s é o conjunto de todos os vértices marcados na última iteração. Como consequência, C é um corte mínimo cuja capacidade é igual ao valor do fluxo corrente, ou seja, $c(P_s, P_t) = \text{val}(f) = 8$. \square

Admitindo que, após as sucessivas iterações do procedimento de marcação do algoritmo de Ford-Fulkerson, o algoritmo termina (o que equivale à não existência de qualquer caminho de aumento completo), tendo em conta o Teorema 16.3, podemos concluir que o fluxo corrente é máximo. Assim, para se mostrar que o algoritmo de Ford-Fulkerson determina um fluxo máximo num número finito de passos, basta mostrar que o procedimento de marcação termina ao fim de um número finito de passos. Com efeito, supondo por simplicidade que as capacidades dos arcos são números inteiros, uma vez que durante a aplicação do procedimento de marcação Δt toma valores inteiros positivos e, em cada iteração o novo valor do fluxo passa a ser o antigo adicionado de Δt , as capacidades dos arcos obrigam a que ao fim de um número finito de iterações este procedimento termine.

Verifica-se ainda que a complexidade computacional deste algoritmo é da ordem de $\mathcal{O}(\nu^2\varepsilon)$.

Exemplo 16.4. Dado um digrafo conexo \vec{G} , vamos mostrar que o número de caminhos orientados disjuntos (nos arcos) entre dois vértices arbitrários de \vec{G} pode ser determinado por aplicação do algoritmo de Ford-Fulkerson.

Solução. É claro que se as capacidades dos arcos de uma rede são números inteiros, então o fluxo máximo obtido por aplicação do algoritmo de Ford-Fulkerson é também um fluxo de inteiros. Logo, associando a cada arco da rede \vec{G} a capacidade 1, quaisquer que sejam os vértices $s, t \in V(\vec{G})$, o valor do fluxo máximo obtido com o algoritmo de Ford-Fulkerson é igual ao número de caminhos orientados disjuntos (nos arcos) de s para t . Com efeito, nesta rede, qualquer fluxo de inteiros apresenta um dos valores 0 ou 1 em cada arco e, consequentemente, qualquer arco com valor 1 pertence a um único caminho orientado de s para t . Assim, se o valor do fluxo máximo obtido de s para t é m , significa que existem m caminhos orientados disjuntos (nos arcos) de s para t . \square

16.2. Fluxo de custo mínimo

Um outro problema muito comum em redes, é o problema da determinação do *fluxo de custo mínimo*, onde se consideram custos unitários de transporte de fluxo em cada arco. No caso particular do transporte de uma única unidade de fluxo, da origem s para o destino t , com o menor custo global possível, este problema reduz-se ao problema do caminho mais curto, num digrafo com custos nos arcos, o qual foi já considerado no Capítulo 14. Sendo esse o caso, podemos aplicar directamente o algoritmo de Dijkstra ou o algoritmo de Bellman-Ford.

No caso geral, porém, os problemas de fluxo de custo mínimo correspondem ao problema de optimização

$$\min \sum_{e \in E(\vec{R})} w(e)f(e) \quad (16.1)$$

$$\text{sujeito a } \sum_{e \in \partial^+(\{v\})} f(e) - \sum_{e \in \partial^-(\{v\})} f(e) = b_v, \quad \forall v \in V(\vec{R}), \quad (16.2)$$

$$l_e \leq f(e) \leq c(e), \quad \forall e \in E(\vec{R}), \quad (16.3)$$

onde l_e denota um minorante para o fluxo $f(e)$ no arco e e $c(e)$ a respectiva capacidade do arco (majorante para o fluxo que o atravessa). Deve observar-se que neste problema os custos $w(e)$ por unidade de fluxo transportado, em cada arco e , podem ser negativos. Note-se ainda que, neste tipo de problemas, o princípio de conservação do fluxo, válido para todos os vértices distintos da origem e do destino nos problemas de fluxo máximo, é aqui traduzido pelas equações (16.2) válidas para todos os vértices. Estas equações significam que, para cada vértice v , o fluxo que sai de v é igual ao fluxo produzido em v mais o fluxo que chega a v (se $b_v \geq 0$) ou que o fluxo que chega a v é igual ou fluxo que sai de v mais o fluxo consumido em v (se $b_v \leq 0$). Como consequência, o modelo

apresentado refere-se a uma *rede equilibrada*, ou seja, a uma rede onde a soma dos fluxos consumidos é igual à soma dos fluxos produzidos (pelo que $\sum_{v \in V(\vec{R})} b_v = 0$). Quando tal não acontece, é possível transformar o problema, com a introdução de um vértice artificial consumidor (produtor), caso haja produção (consumo) em excesso, ligando a esse vértice todos os vértices produtores (consumidores) com arcos de custo nulo. Nestes casos, as quantidades de fluxo que percorrem os arcos incidentes no vértice consumidor (produtor) artificial, correspondem às quantidades que ficam retidas (em falta) nos vértices produtores (consumidores). Assim, nos problemas de fluxo de custo mínimo, cada vértice v , ou consome fluxo da rede (se $b_v < 0$), ou injecta fluxo na rede (se $b_v > 0$), ou é apenas um vértice de passagem de fluxo (se $b_v = 0$), pelo que, nestes problemas, não faz sentido falar nem em vértice origem, nem em vértice destino.

Nos problemas de fluxo de custo mínimo, o objectivo é obter a circulação de fluxo com menor custo, satisfazendo todos os consumos e produções de fluxo existentes na rede. Dada uma rede \vec{R} tal que $|E(\vec{R})| = m$ e $|V(\vec{R})| = n$, denotando por $B_{\vec{R}} \in \mathbb{R}^{n \times m}$ a respectiva matriz de incidência arco vértice, por $w \in \mathbb{R}^m$ o vector de custos nos arcos (pelo que $w_e = w(e)$, para $e \in E(\vec{R})$), por $b \in \mathbb{R}^n$ o vector de fluxos produzidos (se $b_v > 0$) ou consumidos (se $b_v < 0$) nos vértices, por $l, c \in \mathbb{R}^m$ os vectores, respectivamente de minorantes para o fluxo e de capacidades dos arcos (pelo que $l_e \leq f(e)$ e $c_e = c(e)$, para $e \in E(\vec{R})$), e por $x \in \mathbb{R}^m$ o vector de variáveis tal que $x_e = f(e)$, para $e \in E(\vec{R})$, o problema de determinação do fluxo de custo mínimo (16.1)-(16.3) pode formular-se do seguinte modo:

$$\begin{aligned} & \min w^T x \\ \text{s. a } & B_{\vec{R}} x = b, \\ & l \leq x \leq c. \end{aligned}$$

16.2.1 Soluções básicas admissíveis

A resolução do problema de determinação do fluxo de custo mínimo (16.1)-(16.3) vai fazer-se com recurso à determinação sucessiva de soluções básicas admissíveis adjacentes, enquanto essa determinação for vantajosa. No caso das redes, uma *solução básica* ou *base* é uma árvore abrangente T que se diz *admissível* quando as quantidades de fluxo nos arcos, são admissíveis, ou seja, quando as quantidades de fluxo $f(e)$ associadas a cada um dos arcos $e \in E(T)$ são tais que $l_e \leq f(e) \leq c(e)$ e permitem alimentar todos os vértices consumidores e escoar todos os vértices produtores, pelo que $f(e) = 0$ se $e \in E(\vec{R}) \setminus E(T)$. Por sua vez, ainda no caso particular das redes, duas soluções básicas admissíveis dizem-se *adjacentes*, se uma se obtém da outra, eliminando um arco e acrescentando outro. Por exemplo, considerando a rede \vec{R} representada na Figura 16.6 (onde os minorantes para o fluxo nos arcos são todos iguais a zero e as capacidades são ilimitadas), as árvores abrangentes T e T' são soluções básicas admissíveis adjacentes (note-se que $E(T') = (E(T) \setminus \{45\}) \cup \{31\}$). O custo associado a uma solução básica admissível T , vem dado por $w(T) = \sum_{e \in E(T)} w(e)f(e)$. No caso do exemplo apresentado na Figura 16.6, o custo de T é $w(T) = 2 \cdot 6 + 0 \cdot 1 + 5 \cdot 1 + 1 \cdot 2 = 19$ e o de T' é $w(T') = 16$.

Por agora, vamos ignorar as dificuldades levantadas pelo (eventual) desconhecimento de uma solução básica admissível inicial e pela (eventual) existência de minorantes e capacidades dos arcos relativamente ao fluxo que os atravessa, ou seja, por enquanto, vamos admitir que conhecemos uma solução básica admissível inicial e que em qualquer arco e pode circular um fluxo arbitrário não negativo $f(e) \geq 0$. Por razões que mais adiante se esclarecerão, tal como a Figura 16.6 ilustra, é conveniente escolher um vértice para raiz e considerar a existência de um arco sem cabeça mas com cauda incidente precisamente nessa raiz.

Sendo T a árvore abrangente que define a solução básica admissível corrente para a rede \vec{R} , a determinação de uma solução básica admissível adjacente a T faz-se acrescentando um dado arco e retirando outro. Porém, esta troca só é interessante se for vantajosa, ou seja, se a solução básica admissível adjacente tiver custo inferior ao da base corrente. Assim, suponha que se acrescenta o arco

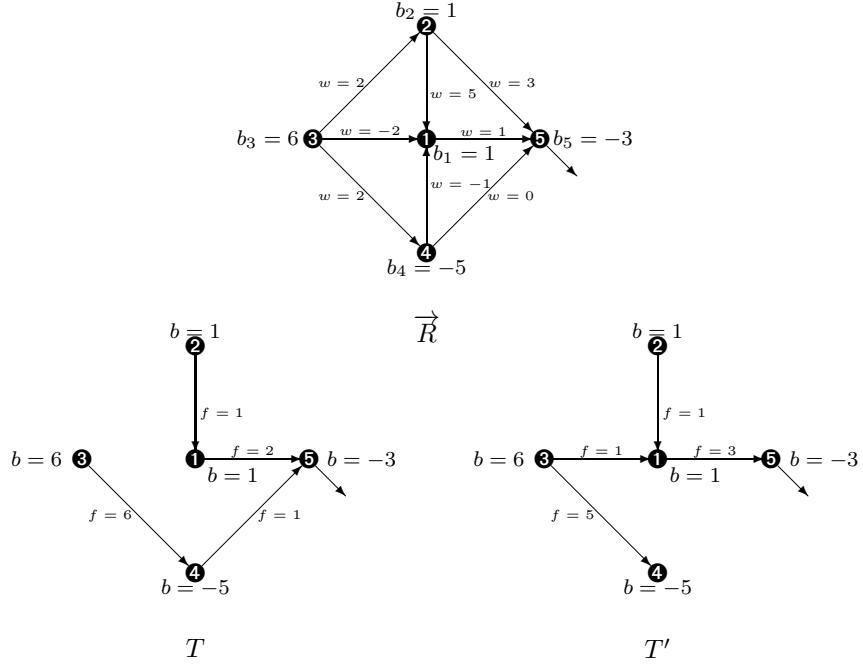


Figura 16.6: Rede com custos e duas soluções básicas admissíveis adjacentes T e T' .

uv à árvore T , obtendo-se o subgrafo abrangente $T + uv$ e, naturalmente, um ciclo C . Se o arco uv fizer parte da base adjacente T' a determinar, então podemos admitir que em T' o fluxo que atravessa uv passa a ser $\Delta > 0$ e, pela conservação de fluxo na rede, é necessário que ao longo do ciclo C , nos arcos concordantes com uv , haja um acréscimo de fluxo Δ (pelo que os vamos marcar com $+\Delta$) e nos arcos contrários haja um decréscimo de fluxo Δ (pelo que os vamos marcar com $-\Delta$), tal como a Figura 16.7 exemplifica.

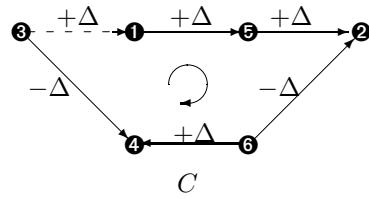


Figura 16.7: Exemplificação do ciclo obtido quando se acrescenta o arco 31 a uma árvore.

Uma vez que o fluxo em cada um dos arcos não pertencentes ao ciclo C se mantém inalterado, denotando por $m(e)$ a marca no arco $e \in E(C)$, podemos concluir que

$$w(T + uv) = w(T) + w(C)\Delta, \quad (16.4)$$

onde $w(C) = \sum_{ij \in E(C): m(ij)=+\Delta} w(ij) - \sum_{ij \in E(C): m(ij)=-\Delta} w(ij)$. Assim, dizemos que o arco uv é *candidato a entrar para a base* se $w(T + uv) < w(T)$ ou, o que é equivalente, se $w(C)\Delta < 0$, ou ainda,

no caso de se verificar a desigualdade

$$\sum_{ij \in E(C): m(ij)=+\Delta} w(ij) - \sum_{ij \in E(C): m(ij)=-\Delta} w(ij) < 0. \quad (16.5)$$

Considerando o sistema de equações

$$y_i - y_j = w(ij), \quad \forall ij \in E(T), \quad (16.6)$$

onde as variáveis y_v , para $v \in V(\vec{R})$, se designam por *variáveis duais*, determinando uma solução e substituindo em (16.5) cada um dos custos $w(ij)$, com $ij \in E(C) \setminus \{uv\}$, por $y_i - y_j$, obtém-se

$$w(uv) + \sum_{ij \in E(C) \setminus \{uv\}: m(ij)=+\Delta} (y_i - y_j) - \sum_{ij \in E(C): m(ij)=-\Delta} (y_i - y_j) < 0.$$

⇓

$$y_u - y_v - w(uv) > 0. \quad (16.7)$$

Assim, podemos concluir que um arco uv é candidato a entrar para a base se e só se a desigualdade (16.7) se verifica. Por exemplo, no caso do ciclo da Figura 16.6,

$$w(31) + (y_1 - y_5) + (y_5 - y_2) - (y_6 - y_2) + (y_6 - y_4) - (y_3 - y_4) = w(31) + y_1 - y_3$$

$$\text{e } w(31) + y_1 - y_3 < 0 \Leftrightarrow y_3 - y_1 - w(31) > 0.$$

Como consequência desta análise, a escolha do arco candidato a entrar para a base pode ser feita (de entre os candidatos) utilizando o critério de Dantzig¹ que consiste em determinar, de entre os arcos de \vec{R} não pertencentes à base corrente T , o arco uv tal que

$$y_u - y_v - w(uv) = \max\{y_i - y_j - w(ij) : ij \in E(\vec{R}) \setminus E(T)\}.$$

Se $y_u - y_v - w(uv) > 0$, então o arco uv é candidato a entrar para a base.

Verifica-se, facilmente, que o sistema (16.6) é indeterminado. Porém, escolhendo um dos vértices da rede (por exemplo, o vértice k) para raiz, no qual se supõe incidente um arco cuja cabeça não é incidente em nenhum vértice da rede (no caso da rede da Figura 16.6, o vértice 5 foi o escolhido para raiz), obtém-se a equação adicional $y_k = \text{const}$, a qual determina uma solução para cada valor de const . Por simplicidade de cálculo, usualmente, faz-se $y_k = 0$ e, a partir desta equação, conjuntamente com as equações (16.6), obtém-se a solução dual associada a T . Por exemplo, a solução dual y associada à base T da Figura 16.6 é a determinada pelo sistema de equações

$$\begin{aligned} y_5 &= 0 \\ y_2 - y_1 &= 5 \\ y_1 - y_5 &= 1 \\ y_4 - y_5 &= 0 \\ y_3 - y_4 &= 2 \end{aligned}$$

ou seja, $y = (1, 6, 2, 0, 0)$. Nesta condições,

$$\max\{y_3 - y_2 - w(32), y_3 - y_1 - w(31), y_4 - y_1 - w(41), y_2 - y_5 - w(25)\} = 3$$

¹George Dantzig (1914–2005), matemático americano que desenvolveu um método de optimização linear, conhecido por método simplex, que, ainda hoje, é o mais popular dos métodos para a resolução deste tipo de problemas.

e, uma vez que $y_3 - y_1 - w(31) = 3$, o arco 31 é candidato a entrar para a base.

Admitindo que o arco uv é candidato a entrar para a base, a escolha do arco ij a sair da base (sendo substituído pelo arco uv) faz-se, a partir do ciclo C produzido quando se acrescenta uv a T , tendo em conta que de acordo com (16.4), quanto maior é Δ maior é o decréscimo obtido para $w(T + uv)$. Porém, uma vez que nos arcos $ij \in E(C)$ marcados com $m(ij) = -\Delta$ vai haver um decréscimo de fluxo Δ que não pode produzir fluxos negativos, o máximo valor admissível para Δ é

$$f(xy) = \min\{f(ij) : ij \in E(C) \wedge m(ij) = -\Delta\}, \quad (16.8)$$

e, neste caso, $xy \in E(C)$ é o arco escolhido para sair da base. Note-se que se $\{f(ij) : ij \in E(C) \wedge m(ij) = -\Delta\} = \emptyset$, então o problema não tem óptimo finito. Com efeito, nestas condições, por um lado Δ pode tomar um valor tão grande quanto se queira (sem que as condições de conservação do fluxo sejam violadas) e, por outro lado, de acordo com (16.4) e (16.5),

$$\lim_{\Delta \rightarrow +\infty} w(T+xy) = -\infty.$$

Tendo em conta (16.8), a nova base T' é tal que $E(T') = (E(T) \setminus \{xy\}) \cup \{uv\}$ e a actualização do fluxo na rede vem dada por

$$f(ij) \leftarrow \begin{cases} f(ij), & \text{se } ij \in E(\vec{R}) \setminus E(C); \\ f(ij) + f(xy), & \text{se } ij \in E(C) \text{ e } m(ij) = +\Delta; \\ f(ij) - f(xy), & \text{se } ij \in E(C) \text{ e } m(ij) = -\Delta. \end{cases}$$

No caso do exemplo da Figura 16.6, uma vez que o arco 31 é candidato a entrar para a base, considerando o ciclo C formado pelos arcos 31, 15, 45 e 34, obtém-se as marcas assinaladas na Figura 16.7.

Como consequência, fazendo $\Delta = \min\{f(45), f(34)\} = f(45) = 1$, conclui-se que a nova base T' (ver Figura 16.6) se obtém eliminando o arco 45 e acrescentando o arco 31. Adicionalmente, o fluxo da base T' é o que aparece associado aos respectivos arcos na Figura 16.6.

A determinação de uma solução básica admissível inicial pode fazer-se com recurso ao que se designa por *método das duas fases*. Com este método, na primeira fase, resolve-se um problema auxiliar com uma rede que se obtém da original, acrescentando um vértice artificial a , com $b_a = 0$, ligando este vértice com arcos ai a todos os vértices i tais que $b_i < 0$ e ligando todos os vértices j tais que $b_j > 0$ ao vértice a , com arcos ja . Adicionalmente, atribuem-se custos unitários a todos os arcos introduzidos e custos nulos aos restantes. Se o custo do fluxo óptimo obtido é positivo, então podemos concluir que a rede original não tem qualquer árvore abrangente admissível (note-se que caso exista uma árvore abrangente com fluxo admissível, então esse mesmo fluxo estendido à rede transformada, com quantidades de fluídos para esta rede e teria custo zero). Caso o custo

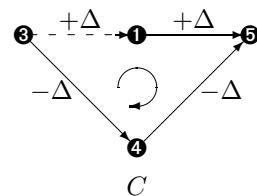


Figura 16.8: Ciclo C obtido acrescentando o arco 31 à árvore T da Figura 16.6.

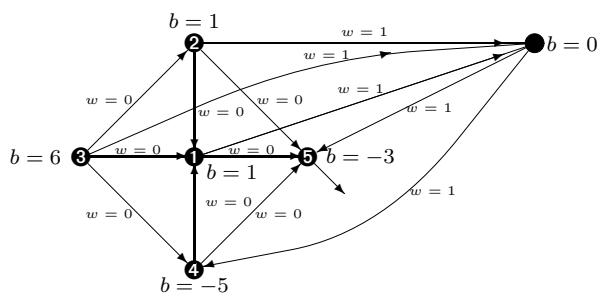


Figura 16.9: Rede, com um vértice artificial, utilizada para a determinação de uma solução básica admissível, aplicando o método das duas fases.

original e iniciamos a segunda fase resolvendo o problema com a solução básica admissível encontrada no final da primeira fase. A Figura 16.8 exemplifica a determinação de uma rede transformada com a introdução de um vértice artificial, para o caso da rede da Figura 16.6.

16.2.2 Método simplex para redes

O método simplex parte de uma solução básica admissível inicial e, a partir dela, determina, sucessivamente, uma solução básica admissível adjacente com melhor custo (enquanto tal for possível). Com efeito, tal como se prova a seguir, verifica-se que a melhor das soluções básicas admissíveis é uma solução óptima para este problema.

Teorema 16.5. *Se o problema da determinação do fluxo de custo mínimo (16.1)-(16.3) tem óptimo finito, então existe uma solução básica admissível que é óptima.*

Demonstração. Sem perda de generalidade, vamos admitir que no problema (16.1)-(16.3) os minorantes para o fluxo nos arcos são todos iguais a zero e as capacidades são ilimitadas. Seja G' um subgrafo abrangente para \vec{R} com o menor número possível de arcos tal que o fluxo nos seus arcos é admissível para a rede \vec{R} e tem custo mínimo. Nestas condições, é claro que se G' tem um ciclo C , então todos os arcos em C têm fluxo positivo. Caso contrário, se existisse um ciclo com um arco e tal que $f(e) = 0$, poderíamos eliminar esse arco, o que contraria a minimalidade do número de arcos de G' . Suponha-se que G' tem um ciclo C (pelo que todos os arcos em C têm fluxo positivo) e escolha-se um arco $e \in E(C)$ tal que, marcando os arcos $ij \in E(C)$ concordantes com e com $m(ij) = -\Delta$ (incluindo o próprio e) e com $+\Delta$ os restantes arcos deste ciclo,

$$\sum_{ij \in E(C): m(ij) = -\Delta} w(ij) \geq \sum_{ij \in E(C): m(ij) = +\Delta} w(ij). \quad (16.9)$$

Nestas condições, sendo $f(xy) = \min\{f(ij) : ij \in E(C) \wedge m(ij) = -\Delta\}$ e fazendo decrescer a quantidade de fluxo $\Delta = f(xy)$ nos arcos marcados com $-\Delta$ e crescer Δ nos arcos marcados com $+\Delta$, dado que

$$\begin{aligned} w(G' - xy) &= w(G' - C) + w(C - xy) \\ w(G') &= w(G' - C) + w(C), \end{aligned}$$

obtém-se $w(G' - xy) - w(G') = w(C - xy) - w(C)$, onde

$$w(C - xy) = w(C) + \Delta \left(\sum_{ij \in E(C): m(ij) = +\Delta} w(ij) - \sum_{ij \in E(C): m(ij) = -\Delta} w(ij) \right).$$

Logo, tendo em conta a desigualdade (16.9), conclui-se que $w(G' - xy) \leq w(G')$, o que é absurdo. \square

Para provarmos a validade do método simplex, resta provar que não havendo uma solução básica admissível adjacente à base corrente melhor do que ela, a solução básica admissível corrente é óptima. Esta prova, porém, embora seja muito fácil de obter no contexto da optimização linear, sai fora do âmbito deste texto.

Segue-se a descrição algorítmica do método simplex para redes (admitindo, por agora, que os minorantes para o fluxo nos arcos são todos iguais a zero e os arcos têm capacidades ilimitadas).

Algoritmo simplex para redes (primeira versão)

Dados de entrada: Rede \vec{R} , função $w : E(\vec{R}) \mapsto \mathbb{R}$ e base admissível T_0 .

Resultados de saída: Fluxo f de custo mínimo.

1. Determinar o fluxo f para a solução básica admissível inicial T_0 e fazer $k \leftarrow 0$.

2. Determinar uma solução dual y associada a T_k .

3. Determinar $uv \in E(\vec{R}) \setminus E(T_k)$ tal que

$$y_u - y_v - w(uv) = \max\{y_i - y_j - w(ij) : ij \in E(\vec{R}) \setminus E(T_k)\}.$$

4. Se $y_u - y_v - w(uv) \leq 0$ então PARAR (o fluxo corrente é óptimo).

5. Determinar o ciclo C em $T_k + uv$ e marcar com $+\Delta$ todos os arcos deste ciclo concordantes com o sentido uv e com $-\Delta$ os restantes.

6. Se $\{ij \in E(C) : ij \text{ está marcado com } -\Delta\} = \emptyset$ então PARAR (o problema não tem óptimo finito).

7. Determinar $xy \in E(C)$ tal que

$$f(xy) = \min\{f(ij) : ij \in E(C) \text{ e a marca de } ij \text{ é } -\Delta\}.$$

8. Para cada $ij \in E(\vec{R})$ fazer

$$f(ij) \leftarrow \begin{cases} f(ij), & \text{se } ij \in E(\vec{R}) \setminus E(C); \\ f(ij) + f(xy), & \text{se } ij \in E(C) \wedge m(ij) = +\Delta; \\ f(ij) - f(xy), & \text{se } ij \in E(C) \wedge m(ij) = -\Delta. \end{cases}$$

9. $T_{k+1} \leftarrow (T_k - xy) + uv$, $k \leftarrow k + 1$ e voltar ao passo 2.
-

Exemplo 16.5. Vamos determinar um fluxo de custo mínimo na rede representada na Figura 16.10-(A), onde os minorantes para a circulação de fluxo são todos iguais a zero e as capacidades nos arcos são ilimitadas, utilizando como solução básica admissível inicial a árvore representada na Figura 16.10-(B).

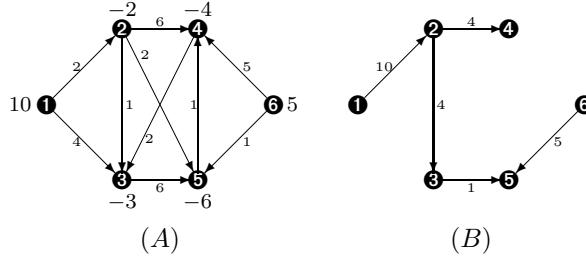


Figura 16.10: Rede com uma das suas árvores abrangentes, onde em (A) se associa a cada vértice a quantidades de fluxo produzido ou consumido (consoante o caso) e a cada arco o custo unitário de circulação de fluxo e em (B) se associa a cada arco a quantidade de fluxo que circula nele.

Solução. Considerando para solução básica admissível inicial a árvore abrangente T da Figura 16.10-(B), com as quantidades de fluxo nos arcos que estão representadas, conclui-se que o custo total deste fluxo inicial é 59. Antes de iniciarmos o processo iterativo, escolhemos o vértice 2 para raiz da rede.

Iteração 1. Começamos por determinar a solução dual associada a T , resolvendo o sistema de equações lineares:

$$\begin{cases} y_2 = 0 \\ y_1 - y_2 = 2 \\ y_2 - y_4 = 6 \\ y_2 - y_3 = 1 \\ y_3 - y_5 = 6 \\ y_6 - y_5 = 1 \end{cases} \Rightarrow y = (2, 0, -1, -6, -7, -6).$$

Calculando $y_i - y_j - w(ij)$, para cada arco $ij \in E(\vec{R}) \setminus E(T)$, obtém-se os valores $y_1 - y_3 - w(13) = -1$, $y_2 - y_5 - w(25) = 5$, $y_4 - y_3 - w(43) = -7$, $y_5 - y_4 - w(54) = -2$, $y_6 - y_4 - w(64) = -5$. Uma vez que o maior valor encontrado é 5, junta-se o arco 25 à solução básica corrente, obtendo-se o ciclo representado na Figura 16.11-(A).

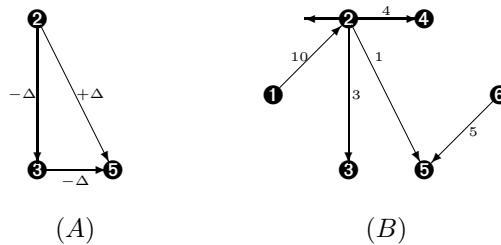


Figura 16.11: Primeira iteração do método simplex para redes.

Verifica-se que a menor quantidade de fluxo corrente nos arcos com marca $-\Delta$ é a que circula no arco 35, cujo valor é 1. Logo, o arco 35 sai da base e obtém-se o fluxo representado na Figura 16.11-(B), cujo custo total é 54.

Iteração 2. Considerando o sistema de equações associado à nova solução básica e resolvendo-o, vem

$$\begin{cases} y_2 = 0 \\ y_1 - y_2 = 2 \\ y_2 - y_4 = 6 \\ y_2 - y_3 = 1 \\ y_2 - y_5 = 2 \\ y_6 - y_5 = 1 \end{cases} \Rightarrow y = (2, 0, -1, -6, -2, -1).$$

Calculando $y_i - y_j - w(ij)$, para cada arco $ij \in E(\vec{R}) \setminus E(T)$, obtém-se os valores $y_1 - y_3 - w(13) = -1$, $y_3 - y_5 - w(35) = -5$, $y_4 - y_3 - w(43) = -7$, $y_5 - y_4 - w(54) = 3$, $y_6 - y_4 - w(64) = 0$. Uma vez que o maior valor encontrado é 3, junta-se o arco 54 à solução básica corrente, obtendo-se o ciclo representado na Figura 16.12-(A).

Dado que a marca $-\Delta$ aparece associada apenas ao arco 24, o arco 24 sai da base e obtém-se o fluxo representado na Figura 16.12-(B), cujo custo total é 42.

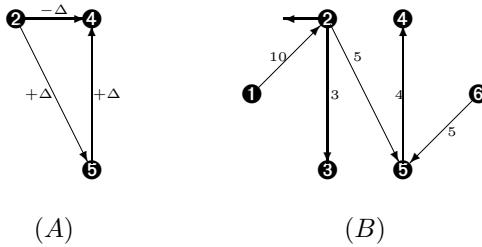


Figura 16.12: Segunda iteração do método simplex para redes.

Iteração 3. Considerando o sistema de equações associado à nova solução básica e resolvendo-o, vem

$$\begin{cases} y_2 = 0 \\ y_1 - y_2 = 2 \\ y_5 - y_4 = 1 \\ y_2 - y_3 = 1 \\ y_2 - y_5 = 2 \\ y_6 - y_5 = 1 \end{cases} \Rightarrow y = (2, 0, -1, -3, -2, -1).$$

Calculando $y_i - y_j - w(ij)$, para cada arco $ij \in E(\vec{R}) \setminus E(T)$, obtém-se os valores $y_1 - y_3 - w(13) = -1$, $y_3 - y_5 - w(35) = -5$, $y_4 - y_3 - w(43) = -4$, $y_2 - y_4 - w(24) = -3$, $y_6 - y_4 - w(64) = -4$. Uma vez que todos estes valores são negativos, podemos concluir que o fluxo representado na Figura 16.12-(B) é um fluxo de custo mínimo, cujo valor é 42. \square

Na ausência de soluções básicas admissíveis degeneradas (ou seja, na ausência de soluções básicas que têm pelo menos um arco básico e tal que $f(e) = 0$), o método simplex para redes converge num número finito de passos. Porém, caso haja degenerescência, o método pode entrar em ciclo. Uma tal entrada em ciclo significa que existe uma sequência de iterações ao longo das quais o custo das soluções encontradas se mantém constante e as sucessivas trocas de arcos conduzem à repetição de árvores abrangentes. Existem técnicas muito eficientes para evitar esta entrada em ciclo, as quais consistem em escolher unicamente bases que se designam por *bases fortemente admissíveis*. Identificando-se um vértice da rede como sendo a raiz r , uma árvore T diz-se fortemente admissível se qualquer dos seus arcos ij com fluxo nulo aponta na direcção oposta à da raiz, ou seja, o único caminho existente em T entre o vértice j e a raiz r inclui o vértice i . De acordo com esta definição, qualquer árvore abrangente cujos arcos têm todos fluxo positivo é uma bases fortemente admissível. O procedimento de determinação de uma base admissível inicial (anteriormente descrito) conduz-nos à obtenção de uma base fortemente admissível. Por outro lado, a escolha adequada do arco candidato a sair da base garante que se a base corrente é fortemente admissível então a nova base também é. Uma escolha adequada consiste no seguinte: se existe apenas um arco candidato a sair da base, então está escolhido por natureza. Caso contrário, dentro do ciclo C criado quando se acrescentou o arco candidato a entrar para a base, define-se o vértice de referência v como sendo o vértice mais próximo da raiz r (ou seja, com menos arcos entre ele e a raiz num caminho que os ligue). Percorremos o ciclo C , a partir do vértice de referência v , na direcção concordante com o arco que entra para a base. Assim, caso o arco ij seja um dos candidatos a sair da base, durante este percurso encontramos primeiro o vértice i e só depois o vértice j . O arco escolhida para abandonar a base é o que é encontrado em primeiro lugar. Prova-se (embora a prova saia fora do âmbito deste texto) que se o método simplex se inicia com uma base fortemente admissível e, em cada iteração, a escolha do arco a sair da base é feita de acordo com a regra anteriormente referida, então em todas as iterações a base corrente é fortemente admissível.

Prova-se ainda que a presença sistemática de bases fortemente admissíveis garante a convergência do método simplex num número finito de passos.

A versão do método simplex anteriormente apresentada, pode facilmente estender-se, com pequenas adaptações, aos problemas de fluxo de custo mínimo em redes com majorantes (capacidades) e minorantes para as quantidades de fluxo nos arcos, tendo em conta que nestes casos, sendo T a base admissível corrente, se $e \in E(\vec{R}) \setminus E(T)$ então $f(e) \in \{c(e), l_e\}$. Para este tipo de problemas, a determinação das variáveis duais não sofre qualquer alteração (uma vez que não são influenciadas pela presença de minorantes ou majorantes). No que diz respeito à escolha do arco candidato a entrar para a base, porém, podem existir candidatos (com fluxos iguais aos respectivos majorantes) cujo fluxo pode decrescer. Assim, é candidato a entrar para a base todo o arco $ij \in E(\vec{R}) \setminus E(T)$ tal que

$$y_i - y_j - w(ij) \begin{cases} < 0, & \text{e } f(ij) = c(ij); \\ > 0, & \text{e } f(ij) = l_{ij}. \end{cases}$$

Em geral, escolhe-se para candidato a entrar para a base o arco uv tal que

$$|y_u - y_v - w(uv)| = \max\{y_u - y_v - w(uv) : f(uv) = l_{uv}\} \cup \{-(y_u - y_v - w(uv)) : f(uv) = c(uv)\},$$

desde que $y_u - y_v - w(uv) \neq 0$. Caso não exista um arco em tais condições, podemos concluir que a base corrente é óptima. No que diz respeito à seleção do arco a sair da base, sendo C o ciclo produzido quando se acrescenta uv a T , se $f(uv) = c(uv)$ marcam-se com $-\Delta$ todos os arcos do ciclo concordantes com uv e com $+\Delta$ os restantes. Por sua vez, se $f(uv) = l_{uv}$ marcam-se com $+\Delta$ todos os arcos de C concordantes com uv e com $-\Delta$ os restantes. Posteriormente, escolhe-se para arco candidato a sair da base o arco xy tal que

$$\begin{aligned} \delta &= \min\{c(ij) - f(ij) : m(ij) = +\Delta\} \cup \{f(ij) - l_{ij} : m(ij) = -\Delta\} \\ &= \begin{cases} c(xy) - f(xy) \\ \text{ou} \\ f(xy) - l_{xy}. \end{cases} \end{aligned}$$

Se $\delta < +\infty$ então o fluxo é actualizado, fazendo

$$f(ij) \leftarrow \begin{cases} f(ij), & \text{se } ij \in E(\vec{R}) \setminus E(C); \\ f(ij) + \delta, & \text{se } ij \in E(C) \wedge m(ij) = +\Delta; \\ f(ij) - \delta, & \text{se } ij \in E(C) \wedge m(ij) = -\Delta. \end{cases}$$

Caso contrário, o problema não tem óptimo finito.

Admitindo que δ é finito, podem ocorrer ainda as seguintes situações:

- Se $\delta = c(uv) - l_{uv}$, então uv não entra para a base e, consequentemente, a base T permanece a mesma, embora com fluxos eventualmente distintos nos respectivos arcos.
- Caso contrário, obtém-se uma nova base $T' = (T + uv) - xy$.

Em qualquer dos casos, o algoritmo prossegue com a escolha de um novo arco candidato a entrar para a base e todos os restantes passos do algoritmo simplex para redes se mantêm. Segue-se a descrição algorítmica do método simplex para redes (pressupondo que se conhece uma solução básica admissível inicial T_0 e os fluxos nos arcos não pertencentes a T_0 podem ser iguais aos respectivos minorantes ou às capacidades).

Algoritmo simplex para redes(segunda versão)

Dados de entrada: Rede \vec{R} , funções de custo $w : E(\vec{R}) \mapsto \mathbb{R}$ e de capacidade $c : E(\vec{R}) \mapsto \mathbb{R}_+$, vector de minorantes l para o fluxo nos arcos, e base admissível inicial T_0 , para a qual se supõe conhecidos os fluxos nos arcos não pertencentes a T_0 (os quais podem ser iguais aos respectivos minorantes ou às capacidades).

Resultados de saída: Fluxo f de custo mínimo.

1. Determinar o fluxo f para a solução básica admissível inicial T_0 e fazer $k \leftarrow 0$.
 2. Determinar uma solução dual y associada a T_k .
 3. Determinar
- $$\delta = \max\{y_i - y_j - w(ij) : f(ij) = l_{ij}\} \cup \{-(y_i - y_j - w(ij)) : f(ij) = c(ij)\}.$$
4. Se $\delta \leq 0$ então PARAR (o fluxo corrente é óptimo).
 5. Se $\delta = |y_u - y_v - w(uv)|$ determinar o ciclo C em $T_k + uv$ e proceder à marcação dos arcos deste ciclo, fazendo

$$m(ij) = \begin{cases} +\Delta, & \text{se } f(ij) = l_{ij} \text{ e } ij \text{ é concordante com } uv; \\ -\Delta, & \text{se } f(ij) = l_{ij} \text{ e } ij \text{ é contrário a } uv; \\ -\Delta, & \text{se } f(ij) = c(ij) \text{ e } ij \text{ é concordante com } uv; \\ +\Delta, & \text{se } f(ij) = c(ij) \text{ e } ij \text{ é contrário a } uv. \end{cases}$$

6. Determinar

$$\begin{aligned} \Delta &= \min\{c(ij) - f(ij) : m(ij) = +\Delta\} \cup \{f(ij) - l_{ij} : m(ij) = -\Delta\} \\ &= \begin{cases} c(xy) - f(xy) \\ \text{ou} \\ f(xy) - l_{xy} \end{cases} \end{aligned}$$

7. Se $\delta = +\infty$ então PARAR (o problema não tem óptimo finito).
 8. Para cada $ij \in E(\vec{R})$ fazer
- $$f(ij) \leftarrow \begin{cases} f(ij), & \text{se } ij \in E(\vec{R}) \setminus E(C); \\ f(ij) + \Delta, & \text{se } ij \in E(C) \wedge m(ij) = +\Delta; \\ f(ij) - \Delta, & \text{se } ij \in E(C) \wedge m(ij) = -\Delta. \end{cases}$$
9. Se $\delta = c(uv) - l_{uv}$ então voltar ao passo 3. Caso contrário, fazer $T_{k+1} \leftarrow (T_k - xy) + uv$, $k \leftarrow k + 1$ e voltar ao passo 2.
-

Exemplo 16.6. Vamos determinar um fluxo de custo mínimo na rede representada na Figura 16.13-(A) (onde em cada arco e o terno $(l(e), c(e), w(e))$ denota o minorante $l(e)$ para o fluxo, a capacidade do arco $c(e)$ e o custo unitário do fluxo $w(e)$, tomando para base inicial a árvore abrangente T representada na Figura 16.13-(B) (na qual se indicam os fluxos dos arcos básicos e não básicos)).

Solução. Considerando para solução básica admissível inicial a árvore abrangente T representada na Figura 16.13, onde se indicam os fluxos nos arcos básicos e não básicos (note-se que os fluxos nos arcos não básicos são $f(21) = 3$ e $f(65) = 4$), o custo do fluxo corrente vem dado por

$$\sum_{e \in E(\vec{R})} w(e)f(e) = 3 \times 3 + 4 \times 3 + 1 \times 2 - 1 \times 1 + 6 \times 5 + 2 \times 4 + 2 \times 3 = 66.$$

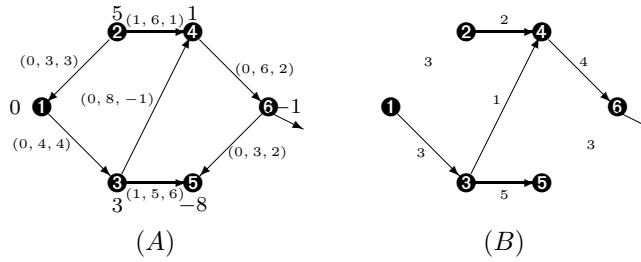


Figura 16.13: Rede (onde para cada arco e , os ternos $(l_e, c(e), w(e))$ denotam o minorante para o fluxo, a capacidade e o custo por unidade de fluxo) e base admissível com indicação dos fluxos nos arcos básicos e não básicos.

Antes de iniciarmos o processo iterativo vamos escolher para raiz da rede \vec{R} o vértice 6.

Iteração 1. Determinamos a solução dual associada à base T , resolvendo o sistema de equações lineares:

$$\begin{cases} y_6 = 0 \\ y_1 - y_3 = 4 \\ y_2 - y_4 = 1 \\ y_3 - y_4 = -1 \\ y_3 - y_5 = 6 \\ y_4 - y_6 = 2 \end{cases} \Rightarrow y = (5, 3, 1, 2, -5, 0).$$

Calculando $y_i - y_j - w(ij)$, para cada arco $ij \in E(\vec{R}) \setminus E(T)$, obtém-se os valores $y_2 - y_1 - w(21) = -5$ e $y_6 - y_5 - w(65) = 3$. Uma vez que

$$\begin{aligned} \delta &= \max\{y_i - y_j - w(ij) : f(ij) = l_{ij}\} \cup \{-(y_i - y_j - w(ij)) : f(ij) = c(ij)\} \\ &= \max\{5, -4\} = -(y_2 - y_1 - w(21)) = 5, \end{aligned}$$

junta-se o arco 21 à solução básica corrente, obtendo-se o ciclo representado na Figura 16.14-(A).

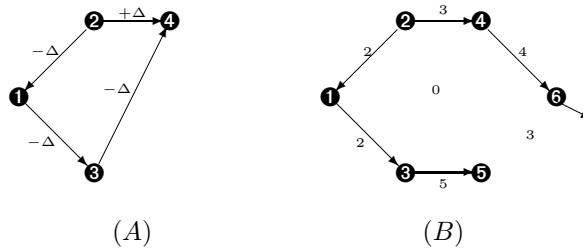


Figura 16.14: Segunda iteração do método simplex para redes.

Dado que $\Delta = \min\{f(21) - l_{21}, f(13) - l_{13}, f(34) - l_{34}, c(24) - f(24)\} = \min\{3 - 0, 3 - 0, 1 - 0, 6 - 2\} = f(34) - l_{34} = 1$, actualizando o fluxo, obtém-se nos arcos básicos e não básicos o fluxo representado na Figura 16.14-(B) (note-se que $f(34) = 0$ e $f(65) = 3$). Assim, o custo do fluxo corrente passa a ser 61.

Iteração 2. Considerando o sistema de equações associado à nova solução básica corrente T e resolvendo-o, vem

$$\left\{ \begin{array}{l} y_6 = 0 \\ y_1 - y_3 = 4 \\ y_2 - y_1 = 3 \\ y_2 - y_4 = 1 \\ y_4 - y_6 = 2 \\ y_3 - y_5 = 6 \end{array} \right. \Rightarrow y = (0, 3, -4, 2, -10, 0).$$

Calculando $y_i - y_j - w(ij)$, para cada arco $ij \in E(\vec{R}) \setminus E(T)$, obtém-se os valores $y_3 - y_4 - w(34) = -5$ e $y_6 - y_5 - w(65) = 8$. Dado que

$$\begin{aligned} \delta &= \max\{y_i - y_j - w(ij) : f(ij) = l_{ij}\} \cup \{-(y_i - y_j - w(ij)) : f(ij) = c(ij)\} \\ &= \max\{-5, -8\} = -5, \end{aligned}$$

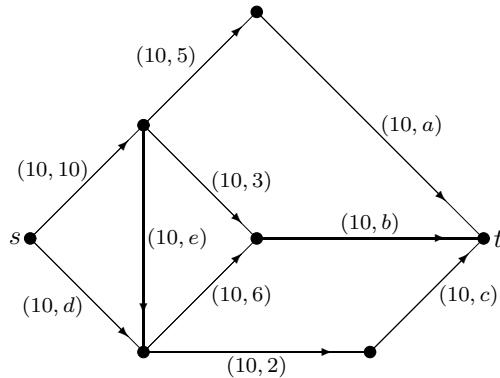
podemos concluir que a solução básica corrente é óptima. \square

16.3. Exercícios

16.1. Considere a rede \vec{R} representada na Figura 16.1 e responda às seguintes questões:

- (a) Indique se a função $f : E(\vec{R}) \mapsto \mathbb{R}$, tal que $f(sb) = f(ac) = f(ad) = f(dt) = 4, f(sa) = f(ct) = 5, f(bd) = f(dc) = 1$ e $f(ba) = 5$, é um fluxo em \vec{R} e, no caso afirmativo, determine o valor desse fluxo.
- (b) De entre os conjuntos de arcos a seguir indicados, qual ou quais constituem cortes- st ?
 - i. $E_1 = \{bd, dc, dt\}$;
 - ii. $E_2 = \{sa, ac, ad, bd\}$;
 - iii. $E_3 = \{sa, ba, ad, ac\}$;
 - iv. $E_4 = \{ac, ad, bd\}$.

16.2. Sabendo que a capacidade de cada um dos arcos da rede \vec{R} , a seguir representada, é constante e igual a 10, e que nos pares (x, y) indicados o valor de y corresponde ao valor que a função $f : E(\vec{R}) \mapsto \mathbb{R}_+$ toma no respectivo arco, determine os valores de a, b, c, d e e de modo que f seja um fluxo na rede.



Adicionalmente, indique os arcos que não estão saturados, relativamente ao fluxo apresentado na figura.

16.3. Considere a rede \vec{R} do exercício anterior e calcule a capacidade $c(P_s, P_t)$ do corte-*st* $\partial(P_s)$, tal que

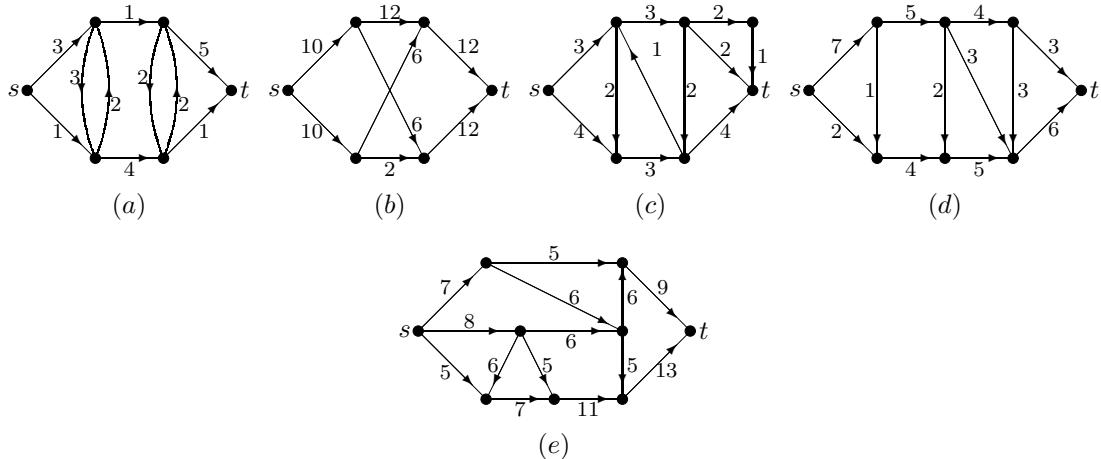
- (a) $P_s = \{s\}$;
- (b) $P_s = \{s\} \cup N_{\vec{R}}(s)$.

Adicionalmente, diga se algum destes cortes é corte mínimo.

16.4. Considere o fluxo f indicado na rede \vec{R} do Exercício 16.2.

- (a) Determine $\text{val}(f)$.
- (b) Identifique em \vec{R} um caminho de aumento relativamente a f .
- (c) A partir do caminho de aumento identificado na alínea anterior, determine um novo fluxo f' , tal que $\text{val}(f') > \text{val}(f)$.

16.5. Determine um fluxo máximo e um corte mínimo, para cada uma das redes a seguir representadas.

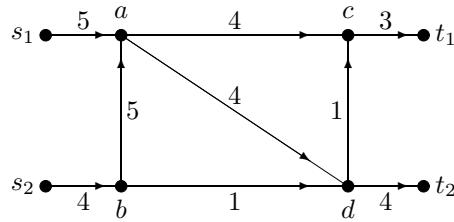


16.6. Seja \vec{R} uma rede com função de custo nos arcos $w : E(\vec{R}) \mapsto \mathbb{R}$, função de capacidade $c : E(\vec{R}) \mapsto \mathbb{R}_+$ e vector de minorantes para o fluxo nos arcos $l \in \mathbb{R}^{E(\vec{R})}$. Supondo que o fluxo admissível para esta rede definido pela função $f : E(\vec{R}) \mapsto \mathbb{R}_+$ é tal que o conjunto de arcos $\{e \in E(\vec{R}) : l_e < f(e) < c(e)\}$ determina um subgrafo de \vec{R} que contém pelo menos um ciclo C , prove que existe um árvore abrangente T que determina um fluxo f' tal que

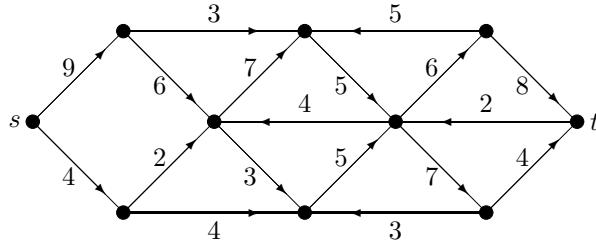
$$f'(e) \in \{l_e, c(e)\} \quad \forall e \in E(\vec{R}) \setminus E(T)$$

e, adicionalmente, $\sum_{e \in E(\vec{R})} w(e)f'(e) \leq \sum_{e \in E(\vec{R})} w(e)f(e)$.

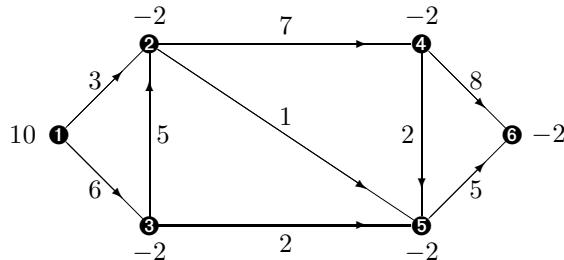
16.7. Considere a rede a seguir representada onde os vértices s_1 e s_2 injectam fluxo na rede e os vértices t_1 e t_2 consomem fluxo da rede (os pesos associados aos arcos indicam, naturalmente, as respectivas capacidades). Modifique esta rede, de modo adequado, para aplicação do algoritmo de Ford-Fulkerson para determinação do fluxo máximo.



- 16.8. Considerando a rede representada na figura a seguir, determine o respectivo fluxo máximo, justificando o resultado obtido.

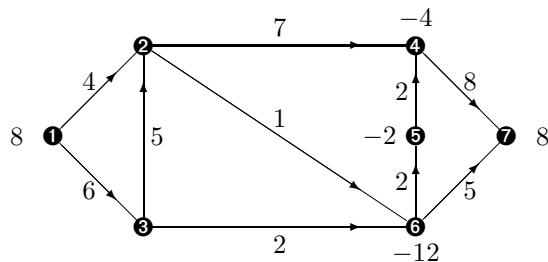


- 16.9. Considerando a rede representada no Exercício 16.8 e interpretando os pesos associados aos arcos como distâncias entre vértices, determine o caminho mais curto entre os vértices s e t , utilizando o algoritmo simplex para redes.
- 16.10. Considere a rede a seguir representada onde os pesos nos arcos indicam custos unitários de transporte de fluxo e os números negativos e positivos, associados aos vértices (sorvedouros e fonte), constituem os respectivos consumos e produção de fluxo.



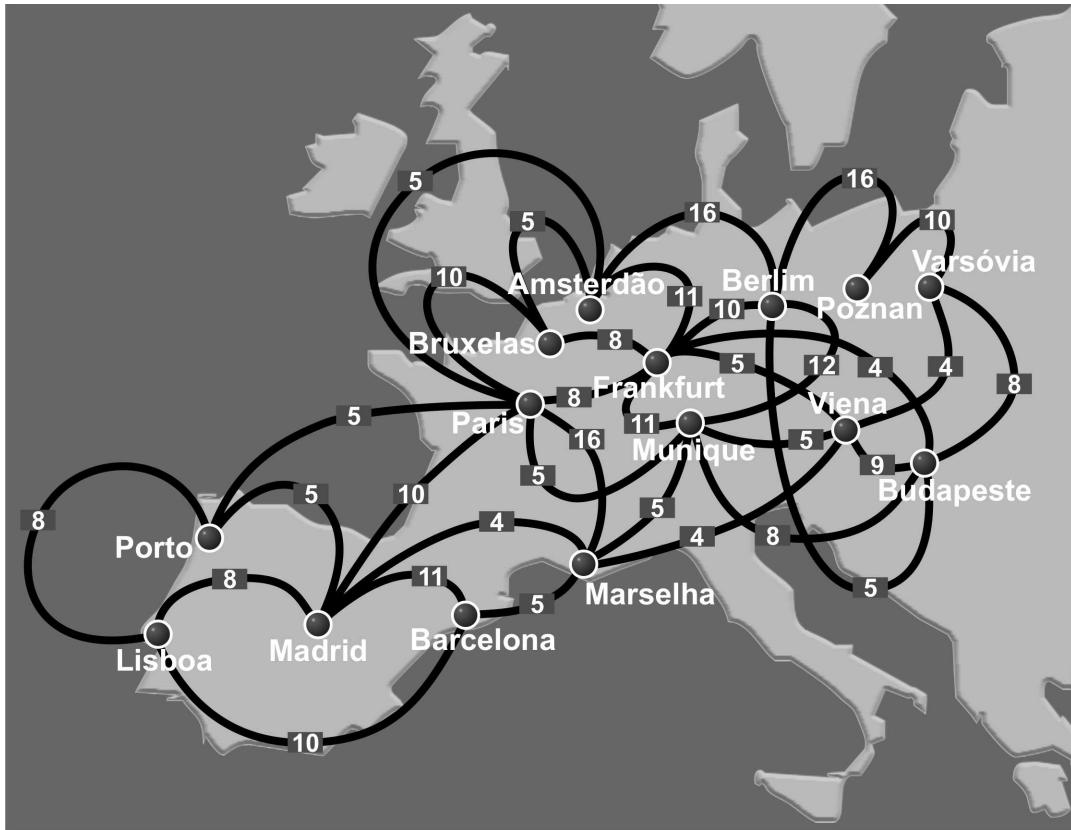
Determine o fluxo de custo mínimo.

- 16.11. Considere a rede a seguir representada, onde os pesos nos arcos indicam custos unitários de transporte de fluxo e os números positivos e negativos associados aos vértices (fontes e sorvedouros) constituem os respectivos consumos e produções de fluxo.



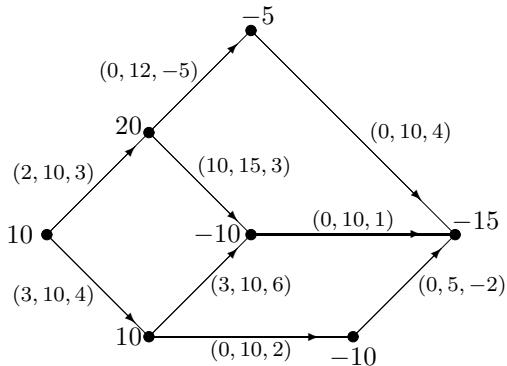
Determine o fluxo de custo mínimo.

- 16.12. Considere que uma empresa de transporte rodoviário de cargas tem a sua frota de camiões distribuída por várias cidades da Comunidade Europeia, fazendo ligações entre pares de cidades com camiões, cujas capacidades de carga, em toneladas, correspondem aos pesos indicados nas arestas representadas na figura a seguir.



Determine a carga máxima que é possível transportar entre o Porto e Poznań de tal forma que quando a carga muda de camião essa mudança é feita na totalidade, bem como o respectivo trajecto.

- 16.13. Considere a rede \vec{R} representada na figura a seguir, onde cada um dos ternos $(l_e, c(e), w(e))$ determina o minorante l_e para o fluxo no arco e , a respectiva capacidade $c(e)$ e o custo $w(e)$ por unidade de fluxo transportada no arco e . Tendo em conta as quantidades de fluxo produzidas e consumidas indicadas nos vértices, responda às seguintes questões:



- (a) Com recurso ao método das duas fases, determine uma solução básica admissível inicial.
- (b) A partir da solução básica admissível encontrada anteriormente, determine um fluxo de custo mínimo.
- 16.14. Considere a tabela de preços por tonelada transportada entre os pares de algumas das cidades representadas na figura do Exercício 16.12, conforme se apresenta a seguir, onde os índices linha e coluna representam as cidades: 1-Porto, 2-Lisboa, 3-Madrid, 4-Paris, 5-Bruxelas, 6-Amesterdão, 7-Frankfurt, 8-Berlin, 9-Viena, 10-Budapeste, 11-Varsóvia e 12-Poznań.

	1	2	3	4	5	6	7	8	9	10	11	12
1	—	80	150	435	—	—	—	—	—	—	—	—
2	80	—	180	—	—	—	—	—	—	—	—	—
3	150	180	—	315	—	—	—	—	—	—	—	—
4	435	—	315	—	75	125	145	—	—	—	—	—
5	—	—	—	75	—	55	95	—	—	—	—	—
6	—	—	—	125	55	—	110	170	—	—	—	—
7	—	—	—	145	95	110	—	130	180	245	—	—
8	—	—	—	—	—	170	130	—	—	—	—	100
9	—	—	—	—	—	—	180	—	—	70	—	—
10	—	—	—	—	—	—	245	—	70	—	240	—
11	—	—	—	—	—	—	—	—	—	240	—	75
12	—	—	—	—	—	—	—	100	—	—	75	—

Supondo que uma empresa fabrica um determinado produto nas cidades do Porto (20 toneladas/mês), Amesterdão (25 toneladas/mês) Budapest (15 toneladas/mes) e Poznań (20 toneladas/mes) e que o distribui pelas restantes cidades, nas quais existe um consumo mensal de 10 toneladas, determine as rotas de abastecimento mais económicas para esta distribuição.

- 16.15. Supondo que no problema anterior, nas cidades de Lisboa, Bruxelas, Viena e Berlim o consumo baixou para 5 toneladas, introduza as modificações necessárias para transformar a rede que modela este problema numa rede equilibrada e aplique, novamente, o método simplex para redes na respectiva resolução.

17

Emparelhamentos

O problema de partir o conjunto dos vértices de um grafo em pares de vértices adjacentes (ou outros subgrafos particulares), não só modela muitas aplicações práticas, como é de grande importância teórica, no contexto da teoria dos grafos. Tradicionalmente, este problema é designado por problema da determinação de um *emparelhamento perfeito*.

17.1. Emparelhamentos máximos e perfeitos

Seguem-se algumas definições formais e informais de conceitos associados à partição do conjunto de vértices de um grafo em pares de vértices adjacentes.

Definição 17.1 (Emparelhamento de um grafo). *Dado um grafo G , um subconjunto de arestas $M \subseteq E(G)$ sem lacetes que não contém duas arestas adjacentes designa-se por emparelhamento de G . Por sua vez, os dois extremos de uma aresta pertencente a um emparelhamento M dizem-se emparelhados por M .*

Por abuso de linguagem e em coerência com a definição mais geral de k -emparelhamento a introduzir mais adiante, também se considera um emparelhamento como sendo um subgrafo abrangente cujos vértices têm grau não superior a 1.

Diz-se que o emparelhamento M *satura* o vértice v (ou que v é *saturado* por M ou é *M -saturado*) se existe uma aresta de M incidente em v . Caso contrário, diz-se que o vértice v é *M -não-saturado* ou *M -livre* ou *exposto*.

Definição 17.2 (Emparelhamento perfeito e emparelhamento máximo). *Um emparelhamento M de um grafo G diz-se perfeito se satura todos os vértices de G . Por sua vez, diz-se que o emparelhamento M de um grafo G é um emparelhamento máximo se não existe nenhum emparelhamento M' em G , tal que $|M'| > |M|$.*

Como consequência desta definição, podemos concluir, imediatamente, que todo o emparelhamento perfeito é um emparelhamento máximo. Porém, o recíproco não é necessariamente verdadeiro.

Definição 17.3 (Caminho alternado e caminho de aumento). *Um caminho (ou um passeio) diz-se M -alternado ou, simplesmente, alternado se as suas sucessivas arestas estão, alternadamente, em M e em M^c (onde $M^c = E(G) \setminus M$). Se um caminho M -alternado, com pelo menos uma aresta, começa e termina em vértices não-saturados, dizemos que é um caminho de aumento, relativamente a M .*

O teorema a seguir, publicado por Berge¹ em 1957, caracteriza os emparelhamentos máximos em função da existência de caminhos de aumento.

¹Claude Berge (1926–2002), matemático francês que dedicou a maior parte da sua vida ao estudo da teoria dos grafos e da combinatória.

Teorema 17.1 (Berge). *Dado um grafo conexo G , um emparelhamento M é máximo se e só se não existe nenhum caminho de aumento relativamente a M .*

Demonstração. Seja M um emparelhamento máximo de G e suponha que existe um caminho P de aumento, relativamente a M . Para $M' = E(P) \setminus M$, vem que M' é um emparelhamento em G e $|M'| = |M| + 1$, o que constitui uma contradição (uma vez que, por hipótese, M é um emparelhamento máximo). Reciprocamente, seja M um emparelhamento de G que não é máximo e vamos admitir que G não contém nenhum caminho de aumento, relativamente a M . Sendo M' um emparelhamento máximo de G , por definição, $|M'| > |M|$. Considerando o subgrafo H , cujas arestas pertencem à diferença simétrica dos emparelhamentos M e M' e cujos vértices são exactamente os extremos destas arestas, ou seja, $E(H) = M \Delta M'$ e $V(H) = \{x : xy \in M \Delta M'\}$, podemos concluir que cada vértice de H tem grau um ou dois (uma vez que é extremo de não mais do que uma aresta de cada um dos emparelhamentos). Como consequência, cada componente de H é um ciclo de comprimento par ou um caminho com arestas alternadamente em M e em M' . Uma vez que $|M'| > |M|$, H contém mais arestas de M' do que de M e, consequentemente, dado que os ciclos contêm tantas arestas de M como de M' , existe pelo menos uma componente P de H que é um caminho que começa e termina numa aresta de M' . Logo, é claro que os vértices extremos de P são M -livres, não só em H , como também em G . Assim, considerando o caminho P em G , podemos concluir que P é um caminho de aumento, relativamente a M , o que constitui uma contradição. \square

Denotando por $\iota(G)$ o número de componentes com um número ímpar de vértices, as quais designamos por *componentes ímpares*, segue-se um teorema, publicado em 1947 por Tutte², que estabelece uma condição necessária e suficiente para a existência de emparelhamentos perfeitos. A demonstração que vamos utilizar, porém, foi publicada em 1975 por Lovász³.

Teorema 17.2 (Tutte). *Um grafo G admite um emparelhamento perfeito se e só se*

$$\forall_{S \subseteq V(G)} \iota(G - S) \leq |S|. \quad (17.1)$$

Demonstração. Seja G um grafo que admite um emparelhamento perfeito M e seja S um subconjunto de vértices de G . Para cada componente ímpar de $G - S$, sendo M' a parte de M pertencente a esta componente, podemos concluir que existe pelo menos um vértice M' -livre. Assim, existe pelo menos uma aresta do emparelhamento perfeito M , entre cada componente ímpar de $G - S$ e S . Como consequência, uma vez que o número de arestas de M incidentes em vértices de S é não superior a $|S|$, denotando por $\partial(S)$ o corte definido por S , podemos concluir que $\iota(G - S) \leq |\partial(S) \cap M| \leq |S|$. A prova recíproca vai ser feita por redução ao absurdo, supondo que existe um grafo G , sem qualquer emparelhamento perfeito, para o qual se verifica a condição (17.1). Antes de prosseguirmos, porém, convém observar que a adição de novas arestas não faz aumentar o número de componentes ímpares⁴ e, consequentemente, não põe em causa a condição (17.1). Assim, sem perda de generalidade, podemos assumir que G é um grafo maximal (no sentido da inclusão de arestas) que satisfaz (17.1) e não tem um emparelhamento perfeito, ou seja, para cada $xy \notin E(G)$ o grafo $G + xy$ tem um emparelhamento perfeito. Considerando o conjunto $T = \{v \in V(G) : d_G(v) = \nu(G) - 1\}$, para o qual, tendo em conta (17.1), $\iota(G - T) \leq |T|$, relativamente às componentes de $G - T$, temos dois casos.

Caso 1. Todos os componentes de $G - T$ são grafos completos e, neste caso, é fácil determinar em G um emparelhamento perfeito, o que contraria a hipótese.

²William Thomas Tutte (1917–2002), matemático inglês com trabalho relevante em teoria dos grafos, combinatória e criptografia.

³László Lovász, matemático húngaro nascido em 1948, com muitos resultados publicados nas áreas de optimização, teoria dos grafos, combinatória, etc.

⁴Observe-se, porém, que a adição de arestas pode aumentar o número de componentes pares. Por exemplo, ligando duas componentes ímpares por intermédio de uma aresta, obtém-se uma nova componente par.

Caso 2. Nem todas as componentes de $G - T$ são grafos completos. Então existem dois vértices $x, z \in V(G - T)$ à distância 2 (note-se que estes vértices não são adjacentes e têm pelo menos um vizinho comum y , ver Figura 17.1). É claro que $y \notin T$ e que existe um outro vértice $v \notin T$ não adjacente a y (caso contrário, $d_G(y) = \nu - 1$ e $y \in T$). Dado que G é maximal, o grafo $G + xz$ admite um emparelhamento perfeito M_{xz} e o grafo $G + vy$ admite um emparelhamento perfeito M_{vy} . Se $F = M_{xz} \Delta M_{vy}$, então as componentes do grafo formado pelas arestas de F são ciclos pares (note-se que $xz, vy \in F$).

Estamos agora em condições de construir um emparelhamento perfeito de G . Com efeito, as arestas comuns a M_{xz} e M_{vy} saturam todos os vértices que não são extremos de arestas de F . Por sua vez, em cada ciclo produzido por F que não contém xz nem vy , é possível escolher metade das suas arestas para se obter um emparelhamento que satura os respectivos vértices. Resta provar que podemos determinar mais um emparelhamento que satura os vértices dos ciclos pares que contêm xz e vy .

- Se xy e yv pertencem a dois ciclos distintos de F , então facilmente se obtém um emparelhamento nas condições pretendidas que não contém xz nem vy .
- Se xz e vy pertencem a um mesmo ciclo C de F , uma vez que $xz \notin M_{vy}$ e $vy \notin M_{xz}$, podemos concluir que as arestas deste ciclo são, sucessivamente, M_{xz} -alternadas e M_{vy} -alternadas. Por outro lado (por construção) sabe-se que $xy, zy \in E(G)$ (ver Figura 17.1). Logo, considerando de entre estas arestas aquela que divide C em dois subciclos pares, a partir dela, em cada subciclo, podemos construir um emparelhamento que a contém. É claro que a união das arestas dos emparelhamentos, assim obtidos, corresponde a um emparelhamento que satura todos os vértices de C e não contém xz nem vy . \square

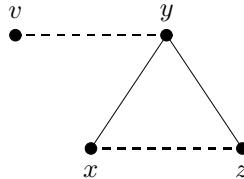


Figura 17.1: Ilustração da demonstração do teorema de Tutte (onde as linhas contínuas representam arestas de G , as linhas a tracejado representam arestas não pertencentes a G e a ausência de uma linha entre dois vértices significa que a aresta por eles definida pode existir ou não).

Como consequência imediata deste teorema, segue-se um resultado publicado em 1891 por Petersen⁵ (naturalmente, antes do teorema de Tutte ser conhecido).

Corolário 17.3 (Petersen). *Qualquer grafo 3-regular sem pontes tem um emparelhamento perfeito.*

Demonstração. Seja G um grafo 3-regular (também conhecido por grafo cúbico) sem pontes e $S \subseteq V(G)$. Uma vez que este resultado pode ser provado componente a componente, sem perda de generalidade, vamos assumir que G é conexo. Seja A o conjunto dos vértices de uma componente ímpar de $G - S$ e seja k o número de arestas de G entre S e A . É claro que a soma dos graus dos vértices da componente induzida por A é igual a $3|A| - k$ (que, necessariamente, é um número par). Uma vez que $|A|$ é ímpar, vem que k também é ímpar e, dado que G não tem pontes, $k \neq 1$, pelo que $k \geq 3$. Como consequência, o número de arestas que ligam S às restantes componentes ímpares de $G - S$ é não inferior de $3\iota(G - S)$. Porém, uma vez que o número de arestas que saem de S é não superior a $3|S|$, $3\iota(G - S) \leq 3|S|$, ou seja, $\iota(G - S) \leq |S|$. Assim, podemos concluir que os grafos cúbicos sem

⁵Julius Petersen (1839–1910), matemático dinamarquês que trabalhou essencialmente em teoria dos números, mas cujo nome ficou ligado a um grafo, com propriedades particulares, conhecido por grafo de Petersen.

pontes verificam a hipótese do teorema de Tutte e, como consequência, admitem emparelhamentos perfeitos. \square

Existem algumas generalizações da noção de emparelhamento de um grafo que, nesta altura, é útil introduzir. Antes, porém, deve observar-se que dado um grafo G e um emparelhamento M , o grafo $(V(G), M)$ é um subgrafo abrangente de G cujos vértices têm grau não superior a um. Por abuso de linguagem, algumas vezes, designaremos estes grafos abrangentes, simplesmente, por emparelhamentos.

Definição 17.4 (k -emparelhamento, k -factor). *Seja G um grafo e k um inteiro não negativo. Um subgrafo abrangente H de G diz-se um k -emparelhamento se para cada vértice v , $d_H(v) \leq k$. Adicionalmente, se*

$$\forall_{v \in V} d_H(v) = k,$$

o subgrafo H diz-se um k -emparelhamento perfeito ou k -factor. Por outro lado, um grafo G diz-se k -factorizável se existem k -factores disjuntos nas arestas, H_1, H_2, \dots, H_p , tais que

$$E(G) = E(H_1) \cup E(H_2) \cup \dots \cup E(H_p).$$

Observe que um 1-factor de um grafo G é um emparelhamento perfeito e um 1-emparelhamento de G é um emparelhamento (tendo em conta o abuso de linguagem anteriormente referido).

17.2. Emparelhamentos em grafos bipartidos

Quer pela sua maior simplicidade, quer pela sua grande aplicação prática, o problema da determinação de emparelhamentos (perfeitos ou não) em grafos bipartidos, ocupa lugar de destaque na teoria dos grafos. Seguem-se dois exemplos que evidenciam, precisamente, a aplicabilidade destes emparelhamentos.

1. Suponha que temos um conjunto finito de raparigas e um conjunto finito de rapazes cada um dos quais conhece um dado subconjunto de raparigas. Será que é possível casar todos os rapazes de tal forma que cada um se case com uma rapariga que conhece? Por exemplo, supondo que $X = \{g_1, g_2, g_3, g_4, g_5\}$ é o conjunto das raparigas e $Y = \{b_1, b_2, b_3, b_4\}$ é o conjunto dos rapazes, e ainda que b_1 conhece g_1, g_2 e g_3 ; b_2 conhece g_2 ; b_3 conhece g_2, g_3 e g_5 ; b_4 conhece g_4 e g_5 , uma solução possível consiste em casar b_1 com g_1 , b_2 com g_2 , b_3 com g_3 e b_4 com g_5 . Na linguagem da teoria dos grafos, o grafo bipartido G tal que $V(G) = X \cup Y$ e $E(G) = \{xy \in X \times Y : x \text{ conhece } y\}$ (ver Figura 17.2-(A)) modela este problema que, assim, consiste na determinação de um emparelhamento que satura todos os vértices de Y .
2. Uma universidade convida os professores P_1, P_2, P_3 e P_4 , para leccionarem disciplinas do conjunto $\{D_1, D_2, D_3, D_4, D_5\}$. Supondo que o professor P_1 está preparado para leccionar D_1 ; P_2 para leccionar D_1 e D_3 ; P_3 para leccionar D_1 e D_3 e P_4 para leccionar D_2, D_3, D_4 e D_5 , como se distribuem as disciplinas, de modo que cada professor leccione uma única disciplina de entre aquelas para as quais está preparado. Neste caso, considerando o grafo bipartido representado na Figura 17.2-(B), o objectivo é determinar um emparelhamento que sature todos os vértices do conjunto $\{P_1, P_2, P_3, P_4\}$.

O teorema que se segue, conhecido por teorema do casamento (por ter sido inicialmente formulado numa linguagem de casamentos) foi publicado, em 1930, por Hall⁶.

⁶Philip Hall (1904–1982), matemático inglês que trabalhou em álgebra, especialmente em teoria da representação.

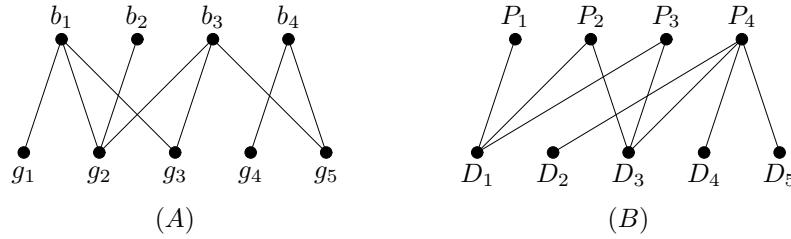


Figura 17.2: Exemplos de grafos bipartidos.

Teorema 17.4 (do casamento ou de Hall). *Seja G um grafo bipartido que admite a bipartição de vértices (X, Y) . Então, o grafo G contém um emparelhamento que satura todos os vértices de X se e só se*

$$\forall S \subseteq X \quad |N_G(S)| \geq |S|, \quad (17.2)$$

onde $N_G(S)$ denota o conjunto de todos os vértices adjacentes a pelo menos um vértice de S (ou seja, o conjunto de vizinhos de S).

Demonstração. Suponha que G contém um emparelhamento M que satura todos os vértices de X e $S \subseteq X$. Uma vez que os vértices de S são todos emparelhados por M com vértices distintos de $N_G(S)$, podemos concluir que $|N_G(S)| \geq |S|$. Reciprocamente, suponha que G é um grafo bipartido para o qual se verificam as desigualdades (17.2), mas que G não contém qualquer emparelhamento que sature todos os vértices de X . Sendo M^* um emparelhamento máximo em G , dado que M^* não satura todos os vértices de X , existe pelo menos um vértice $u \in X$ que é M^* -livre e um conjunto $Z \neq \emptyset$ dos vértices ligados a u por intermédio de um caminho M^* -alternado. Uma vez que M^* é um emparelhamento máximo, o Teorema-17.1 de Berge implica que u seja o único vértice M^* -livre em Z . Sendo $S = Z \cap X$ e $T = Z \cap Y$ (ver Figura 17.3), é claro que todos os vértices de $S \setminus \{u\}$ são emparelhados por M^* com vértices de T , pelo que

$$|T| = |S \setminus \{u\}| = |S| - 1 \quad \text{e} \quad T \subseteq N(S).$$

Na verdade, $T = N(S)$, uma vez que cada vértice de $N(S)$ está ligado a u por um caminho M^* -alternado. Como consequência, $|N(S)| = |S| - 1$, o que contradiz (17.2). \square

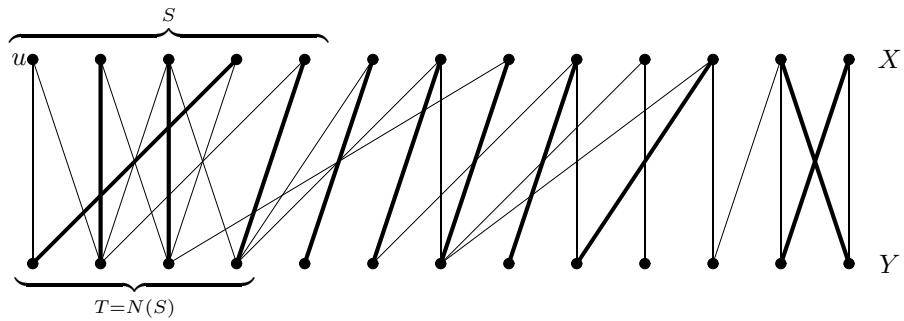


Figura 17.3: Ilustração da demonstração do teorema de Hall.

Corolário 17.5. *Se G é um grafo bipartido k -regular ($k > 0$), então G admite um emparelhamento perfeito.*

Demonstração. Seja G um grafo bipartido k -regular, com a bipartição de vértices (X, Y) . Uma vez que $k|X| = |E(G)| = k|Y|$, obtém-se $|X| = |Y|$. Considere o subconjunto de vértices $S \subseteq X$ e sejam

E_1 e E_2 os subconjuntos das arestas incidentes, respectivamente, em S e $N(S)$. Por definição de $N(S)$, $E_1 \subseteq E_2$ e, consequentemente,

$$k|N(S)| = |E_2| \geq |E_1| = k|S|,$$

ou seja, para cada $S \subseteq X$, $|N(S)| \geq |S|$. Logo, pelo teorema de Hall, G admite um emparelhamento M que satura todos os vértices de X . Adicionalmente, uma vez que $|X| = |Y|$, também se conclui que M satura todos os vértices de Y , ou seja, M é um emparelhamento perfeito. \square

Dado um grafo bipartido, o problema da determinação algorítmica de um emparelhamento que satura todos os vértices de subconjunto da bipartição, designa-se por *problema de afectação de tarefas* ou, no caso de grafos com custos nas arestas, por *problema de afectação óptima de tarefas*. Estes dois problemas serão analisados mais adiante (ainda neste capítulo).

17.2.1 Sistemas de representantes distintos

Uma aplicação interessante dos emparelhamentos, relaciona-se com a determinação de sistemas de representantes distintos que, informalmente, são subconjuntos de elementos pertencentes à união de conjuntos de uma certa família, de tal forma que cada conjunto dessa família contém um desses elementos que é o seu único representante. Segue-se a definição formal.

Definição 17.5 (Sistema de representantes distintos). *Seja E um conjunto finito não vazio e $\mathcal{A} = \{A_1, A_2, \dots, A_m\}$ uma família de subconjuntos não vazios de E (não necessariamente distintos). Um sistema de representantes distintos ou conjunto transversal de \mathcal{A} é um conjunto de elementos distintos de E , $\{e_1, e_2, \dots, e_m\}$, tal que $e_i \in A_i$.*

Exemplo 17.1. *Sendo $E = \{1, 2, 3, 4, 5, 6\}$, $A_1 = A_2 = \{1, 2\}$, $A_3 = A_4 = \{2, 3\}$ e $A_5 = \{1, 4, 5, 6\}$, vamos determinar um sistema de representantes distintos para cada uma das famílias $\mathcal{A} = \{A_1, A_2, A_3, A_5\}$ e $\mathcal{B} = \{A_1, A_2, A_3, A_4\}$.*

Solução. Relativamente a \mathcal{A} , dado que $1 \in A_1$, $2 \in A_2$, $3 \in A_3$ e $5 \in A_5$, conclui-se, imediatamente, que $\{1, 2, 3, 5\}$ é um conjunto transversal da família \mathcal{A} . Relativamente a \mathcal{B} , uma vez que $\bigcup_{A \in \mathcal{B}} A = \{1, 2, 3\}$, o número de elementos da união dos conjuntos da família é inferior ao número de conjuntos. Consequentemente, \mathcal{B} não admite um conjunto transversal. \square

Com base no exemplo anterior, concluímos que nem sempre existe um conjunto transversal. O problema da existência de um conjunto transversal pode ser formulado na linguagem dos grafos e resolvido com recurso ao teorema de Hall. Neste contexto, o teorema de Hall pode reescrever-se, como a seguir se indica.

Teorema 17.6 (Hall). *Seja E um conjunto finito e $\mathcal{A} = \{A_1, A_2, \dots, A_m\}$ uma família de subconjuntos não vazios de E . A família \mathcal{A} tem um sistema de representantes distintos se e só se a união de quaisquer k subconjuntos $A_{i_1}, A_{i_2}, \dots, A_{i_k}$ tem pelo menos k elementos, qualquer que seja $k \in \{1, 2, \dots, m\}$.*

Demonstração. Vamos definir um grafo bipartido G tal que $V(G) = \mathcal{A} \cup E$ e $E(G) = \{aA : a \in A, A \in \mathcal{A}\}$. Nestas condições, a existência de um conjunto transversal é equivalente à existência de um emparelhamento que satura todos os vértices em \mathcal{A} . Considerando o subconjunto de vértices $S = \{A_{i_1}, A_{i_2}, \dots, A_{i_k}\}$, obtém-se $|S| = k$ e $N_G(S) = A_{i_1} \cup A_{i_2} \cup \dots \cup A_{i_k}$. Logo, pelo teorema do casamento, o grafo G admite um emparelhamento que satura os vértices de \mathcal{A} se e só se para qualquer subfamília de k ($k \in \{1, 2, \dots, m\}$) elementos de \mathcal{A} ,

$$|A_{i_1} \cup A_{i_2} \cup \dots \cup A_{i_k}| \geq k.$$

\square

Existe uma estreita relação entre emparelhamentos e a noção de *cobertura de arestas por vértices* que, por simplicidade, também se designa *cobertura por vértices*.

Definição 17.6 (Cobertura por vértices e número de cobertura). *Dado um grafo G , designa-se por cobertura por vértices, um subconjunto de vértices $C \subseteq V(G)$, relativamente ao qual, cada aresta $e \in E(G)$ tem pelo menos um extremo em C . Se C é uma cobertura por vértices e não existe uma cobertura por vértices C' tal que $|C'| < |C|$, diz-se que C é uma cobertura por vértices mínima (ou de cardinalidade mínima), a sua cardinalidade designa-se por número de cobertura de G e denota-se por $\beta(G)$.*

Note-se que o conceito de cobertura por vértices aparece em muitas aplicações. Por exemplo, sendo H um grafo cujos vértices são salas e dois vértices são adjacentes se existe um corredor entre as respectivas salas, o qual pode ser iluminado por uma fonte de luz colocada à entrada de uma das salas, podemos concluir que um conjunto de fontes de luz que ilumine todos os corredores constitui um conjunto de cobertura de H .

Segue-se um teorema publicado em 1931, por König⁷, que em grafos bipartidos relaciona a cardinalidade de um emparelhamento máximo com a cardinalidade de uma cobertura por vértices de cardinalidade mínima.

Teorema 17.7 (König). *Num grafo bipartido a cardinalidade de um emparelhamento máximo é igual à cardinalidade de uma cobertura por vértices mínima.*

Demonstração. Seja G um grafo bipartido que admite a bipartição de vértices (X, Y) e seja M um emparelhamento máximo em G . Sem perda de generalidade, vamos assumir que G não tem vértices isolados. Considere o subconjunto de vértices $A \subseteq V(G)$, onde para cada $v \in A$ existe um caminho M -alternado que se inicia num vértice M -livre de X e termina em v e seja

$$B = (X \setminus A) \cup (Y \cap A).$$

Vamos provar que B é uma cobertura por vértices mínima e que $|B| = |M|$.

Inicialmente vamos mostrar, por redução ao absurdo, que B é uma cobertura por vértices. Assim, suponha que existe uma aresta $xy \in E$, com $x \in X$ e $y \in Y$, sem qualquer extremo em B . Por definição de B , $x \in A$ e $y \notin A$. Como consequência, $xy \notin M$ (uma vez que, se x é M -livre, então xy não pertence ao emparelhamento e se x é M -saturado, então existe $z \in Y \cap A$ tal que $xz \in M$, pelo que, mais uma vez $xy \notin M$). Porém, se $xy \in E(G) \setminus M$, então existe um caminho M -alternado (que passa por x) entre y e um vértice M -livre de X , pelo que $y \in A$, o que constitui uma contradição. Consequentemente, B é uma cobertura por vértices.

Uma vez que, em geral, qualquer cobertura por vértices contém pelo menos um extremo de cada uma das arestas de um emparelhamento arbitrário, a cardinalidade de uma cobertura por vértices é não inferior à cardinalidade de um emparelhamento. Logo, em particular, $|B| \geq |M|$ e, tendo em conta que M é um emparelhamento máximo, basta mostrar que $|B| = |M|$. Assim, para concluirmos esta igualdade, vamos provar a desigualdade $|B| \leq |M|$.

Com efeito, observe-se que todos os vértices de B são M -saturados, o que é consequência da definição de A , no caso dos vértices pertencentes a $X \setminus A$, e consequência da maximalidade de M , no caso dos vértices pertencentes a $Y \cap A$. Por outro lado, prova-se que qualquer aresta $xy \in M$, com $x \in X$ e $y \in Y$, não tem ambos os extremos em B , o que é equivalente a provar a implicação

$$y \in B \Rightarrow x \notin B.$$

Com efeito, se $y \in B$, então $y \in Y \cap A$ e $x \in A$ (por definição de A), pelo que $x \notin B$. Logo, $|B| \leq |M|$. \square

⁷Denes König (1884–1944), matemático húngaro com vários resultados em teoria dos grafos.

Como consequência imediata deste teorema, segue-se um resultado publicado, em 1917, por Frobenius⁸.

Teorema 17.8 (Frobenius). *Um grafo bipartido G admite um emparelhamento perfeito se e só se cada cobertura de arestas por vértice contém pelo menos $\nu(G)/2$ vértices.*

O próximo resultado, atribuído a König e a Egerváry⁹, conhecido por teorema húngaro, é também consequência do teorema de König.

Teorema 17.9 (König-Egerváry). *Dada uma matriz com entradas binárias 0 – 1, o maior número de entradas unitárias, com não mais do que uma em cada linha e coluna, é igual ao menor número de traços horizontais e verticais que cobrem todas as entradas unitárias da matriz.*

Demonstração. Seja $A = (a_{ij})$ uma matriz binária, com n linhas e m colunas, e seja G um grafo bipartido, com bipartição do conjunto dos vértices (X, Y) , onde os subconjuntos de vértices $X = \{x_1, \dots, x_n\}$ e $Y = \{y_1, \dots, y_m\}$ correspondem, respectivamente, às linhas e colunas de A , e

$$E(G) = \{x_i y_j : 1 \leq i \leq n \wedge 1 \leq j \leq m \wedge a_{ij} = 1\}.$$

Observe-se que aos subconjuntos de entradas com valor 1, com não mais do que uma entrada em cada linha e coluna, correspondem emparelhamentos no grafo G . Por outro lado, os conjuntos de traços verticais e horizontais que cobrem todas as entradas unitárias da matriz, definem linhas e colunas da matriz A , às quais correspondem coberturas por vértices em G . Sendo assim, a conclusão pretendida é consequência directa do teorema de König. \square

Exemplo 17.2. Dada a matriz binária

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

vamos determinar o maior número de entradas unitárias, com não mais do que uma em cada linha e coluna (o que é equivalente a determinar o menor número de traços verticais e horizontais que cobrem todas as entradas unitárias de A).

Solução. De acordo de Teorema 17.9, considere o grafo bipartido da Figura 17.4. A partir desta figura, com facilidade se determina o emparelhamento máximo $M = \{x_1 y_1, x_2 y_3, x_4 y_4\}$ e a cobertura por vértices obtida pela construção sugerida na prova do Teorema 17.7 $B = \{y_1, y_3, x_4\}$. Como consequência, podemos concluir que o maior número de entradas unitárias, com não mais do que uma em cada linha e coluna é igual a 3, conforme se apresenta na matriz a seguir.

$$\begin{pmatrix} \textcircled{1} & 0 & 1 & 0 & 0 \\ 1 & 0 & \textcircled{1} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & \textcircled{1} & 0 \end{pmatrix}.$$

De igual modo se conclui que o menor número de traços verticais e horizontais que cobrem todas as entradas unitárias de A é, também, igual a 3 (que correspondem à primeira e terceira colunas e à última linha). \square

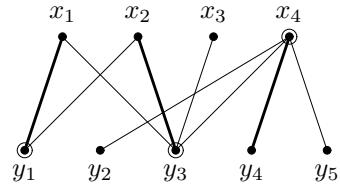


Figura 17.4: Grafo bipartido do Exemplo 17.2.

⁸Georg Frobenius (1849–1917), matemático alemão que trabalhou em várias áreas da matemática.

⁹Egerváry Jenő (1891–1958), matemático húngaro com trabalho relevante em optimização combinatória.

17.2.2 Uma aplicação à partição mínima de cpos em cadeias

Uma questão prática, relacionada com conjuntos parcialmente ordenados, diz respeito à determinação da partição de um conjunto parcialmente ordenado (cpo) em cadeias. Com efeito, de acordo com o teorema de Dilworth, sabe-se que um cpo se pode partir num número mínimo de cadeias que é igual à sua largura. No entanto, até agora, não se introduziu nenhum procedimento para se obter uma tal partição. É precisamente na determinação de uma dessas partições que vamos utilizar os emparelhamentos de grafos bipartidos. Antes porém, convém lembrar que dado um conjunto parcialmente ordenado $P = (X, \preceq_P)$, existem vários grafos (para além do diagrama de Hasse) que o representam.

Definição 17.7 (digrafos e grafos de comparabilidade). *Dado um conjunto parcialmente ordenado $P = (X, \preceq_P)$, designa-se por digrafo de comparabilidade de P , o digrafo $\overrightarrow{GC}(P)$, onde $V(\overrightarrow{GC}(P)) = X$ e $A(\overrightarrow{GC}(P))$ é tal que $\forall x, y \in X$*

$$(x, y) \in A(\overrightarrow{GC}(P)) \text{ sse } x \succ_P y;$$

Adicionalmente, designa-se por grafo de comparabilidade de P , o grafo $GC(P)$ que é obtido de $\overrightarrow{GC}(P)$ ignorando a orientação dos arcos.

Com facilidade se conclui que os digrafos de comparabilidade não admitem ciclos orientados. Na definição destes digrafos, em vez de $y \prec_P x$ escrevemos $x \succ_P y$ para que a associação pictórica com os arcos (x, y) se faça naturalmente.

A questão que nesta altura se levanta é a de saber como concluir se um dado grafo é (ou não) um grafo de comparabilidade. O teorema a seguir estabelece uma condição necessária e suficiente para que um grafo seja um grafo de comparabilidade de algum conjunto parcialmente ordenado.

Teorema 17.10 (Gilmore e Hoffman). *Um grafo simples G é um grafo de comparabilidade se e só se, para cada passeio fechado, $v_1, v_2, \dots, v_{2k+1}, v_1$, de comprimento ímpar, existe uma aresta entre x_j e x_{j+2} para algum j , com a adição considerada módulo $2k + 1$.*

A demonstração pode ser consultada em [10], páginas 367–369.

A figura a seguir exemplifica um grafo, que não é um grafo de comparabilidade, onde se assinala um passeio de comprimento 9 que não verifica as condições do Teorema 17.10.

Segue-se a descrição de um algoritmo para a determinação de uma partição mínima em cadeias de um conjunto parcialmente ordenado $P = (X, \preceq_P)$.

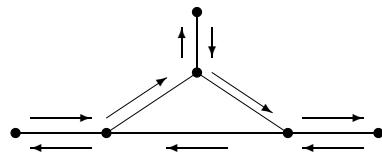


Figura 17.5: Grafo que não é de comparabilidade.

Algoritmo para determinação de uma partição mínima em cadeias de um cpo

Dados de entrada: cpo $P = (X, \preceq_P)$;

Resultados de saída: partição mínima em cadeias;

1. Dividir cada elemento $x \in X$ em x^+ e x^- , definindo-se os conjuntos X^+ e X^- tendo em vista a construção do grafo bipartido $GB(P) = (X^+, X^-, E)$ tal que $\forall x_i^+ \in X^+$ e $\forall x_j^- \in X^-$

$$x_i^+ x_j^- \in E \text{ se e só se } (x_i, x_j) \in A(\overrightarrow{GC}(P)),$$

para o qual, naturalmente, se verifica que $\forall x^+ \in X^+$ e $\forall x^- \in X^-$

$$d_{GB(P)}(x^+) = d_{\overrightarrow{GC}(P)}^+(x) \quad \text{e} \quad d_{GB(P)}(x^-) = d_{\overrightarrow{GC}(P)}^-(x).$$

2. Determinar um emparelhamento máximo, M , para $GB(P)$.
3. Determinar o grafo G_M , tal que

$$V(G_M) = X^+ \cup X^- \text{ e } E(G_M) = M \cup \{x^+x^- : x \in X\}.$$

4. Para cada componente de G_M , determinar o caminho orientado

$$x_{j_1}^- \rightarrow x_{j_1}^+ \rightarrow x_{j_2}^- \rightarrow x_{j_2}^+ \rightarrow \cdots \rightarrow x_{j_{k-1}}^- \rightarrow x_{j_{k-1}}^+ \rightarrow x_{j_k}^- \rightarrow x_{j_k}^+,$$

com $x_{j_i}^+x_{j_{i+1}}^- \in M \forall i \in \{1, \dots, k-1\}$.

5. Para cada um dos caminhos orientados determinados no passo anterior, determinar o correspondente caminho orientado em $\overrightarrow{GC}(P)$

$$x_{j_1} \rightarrow x_{j_2} \rightarrow \cdots \rightarrow x_{j_{k-1}} \rightarrow x_{j_k}$$

o qual, por sua vez, define a cadeia de P , $x_{j_1} \succ_P x_{j_2} \succ_P \dots \succ_P x_{j_k}$.

Note-se que, sendo M um emparelhamento para $GB(P)$ e G_M o grafo determinado no passo 3 do procedimento, conclui-se que $\Delta(G_M(P)) \leq 2$ e, consequentemente, cada componente de G_M ou é um caminho ou um ciclo. Contudo, a cada ciclo (caminho) de G_M corresponde um ciclo (caminho) em $GB(P)$ e também um ciclo (caminho) orientado em $\overrightarrow{GC}(P)$. Logo, podemos concluir que não existem ciclos em G_M e cada uma das suas componentes determina um caminho

$$x_{j_1}^- \rightarrow x_{j_1}^+ \rightarrow x_{j_2}^- \rightarrow x_{j_2}^+ \rightarrow \cdots \rightarrow x_{j_{k-1}}^- \rightarrow x_{j_{k-1}}^+ \rightarrow x_{j_k}^- \rightarrow x_{j_k}^+,$$

o qual, por sua vez, define o caminho orientado em $\overrightarrow{GC}(P)$

$$x_{j_1} \rightarrow x_{j_2} \rightarrow \cdots \rightarrow x_{j_{k-1}} \rightarrow x_{j_k}.$$

Assim, sendo M um emparelhamento, ao conjunto dos caminhos orientados determinados pelas componentes de G_M , corresponde uma partição de X em cadeias.

Exemplo 17.3. A partir do grafo bipartido $GB(P)$ representado na Figura 17.6 e que decorre do digrafo de comparabilidade $\overrightarrow{GC}(P)$, sabendo que

$$\begin{aligned} M_1 &= \{y^+z^-, z^+u^-, v^+w^-, w^+x^-\}, \\ M_2 &= \{y^+v^-, z^+u^-, v^+w^-, w^+x^-\}, \\ M_3 &= \{y^+w^-, z^+u^-, v^+z^-, w^+x^-\}, \end{aligned}$$

correspondem a emparelhamentos máximos em $GB(P)$, vamos determinar as correspondentes partições de P em cadeias.

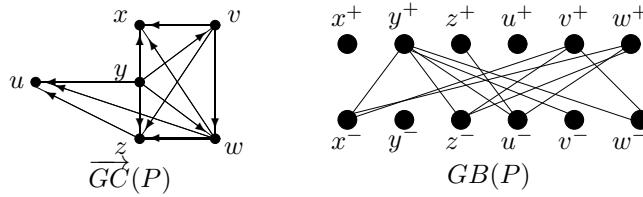
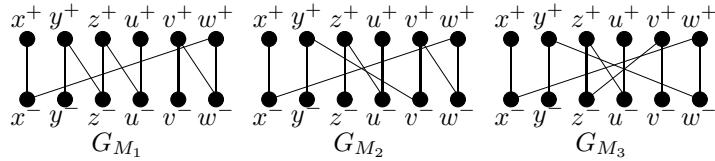


Figura 17.6: Digrafo de comparabilidade e garfo bipartido de um cpo P .

Figura 17.7: Grafos obtidos a partir de emparelhamentos máximos de $GB(P)$.

Solução. Definindo $G_{M_i} = M_i \cup \{a^+a^- : a \in X\}$, para $i \in \{1, 2, 3\}$, obtém-se os grafos bipartidos representados na Figura 17.7. Logo, vem que

- O grafo G_{M_1} tem como componentes $G_{M_1}^1$ que corresponde ao caminho de $GB(P)$

$$y^- \rightarrow y^+ \rightarrow z^- \rightarrow z^+ \rightarrow u^- \rightarrow u^+$$

e $G_{M_1}^2$ que corresponde ao caminho de $GB(P)$

$$v^- \rightarrow v^+ \rightarrow w^- \rightarrow w^+ \rightarrow x^- \rightarrow x^+.$$

- O grafo G_{M_2} tem como componentes $G_{M_2}^1$ que corresponde ao caminho de $GB(P)$

$$y^- \rightarrow y^+ \rightarrow v^- \rightarrow v^+ \rightarrow w^- \rightarrow w^+ \rightarrow x^- \rightarrow x^+$$

e $G_{M_2}^2$ que corresponde ao caminho de $GB(P)$

$$z^- \rightarrow z^+ \rightarrow u^- \rightarrow u^+.$$

- O grafo G_{M_3} tem como componentes $G_{M_3}^1$ que corresponde ao caminho de $GB(P)$

$$y^- \rightarrow y^+ \rightarrow w^- \rightarrow w^+ \rightarrow x^- \rightarrow x^+$$

e $G_{M_3}^2$ que corresponde ao caminho de $GB(P)$

$$v^- \rightarrow v^+ \rightarrow z^- \rightarrow z^+ \rightarrow u^- \rightarrow u^+.$$

Assim, podemos concluir que

- G_{M_1} determina as cadeias $y \prec_P z \prec_P u$ e $v \prec_P w \prec_P x$;
- G_{M_2} determina as cadeias $y \prec_P v \prec_P w \prec_P x$ e $z \prec_P u$;
- G_{M_3} determina as cadeias $y \prec_P w \prec_P x$ e $v \prec_P z \prec_P u$

e que, em todos os casos, se obtém uma partição de X em cadeias. \square

Teorema 17.11. Seja $P = (X, \preceq_P)$ um cpo. Então X admite uma partição em k cadeias se e só se existe um emparelhamento M em $GB(P)$ tal que $k = |X| - |M|$.

Demonstração. Suponha que X admite uma partição nas cadeias C_1, \dots, C_k , as quais determinam o grafo G_M , tal que $V(G_M) = V(GB(P))$ e $E(G_M) = \left(\bigcup_{j=1}^k E(C_j)\right) \cup \{x^-x^+, x \in X\}$. Logo, sendo

$C_j = x_{j_1} \rightarrow x_{j_2} \rightarrow \dots \rightarrow x_{j_{q-1}} \rightarrow x_{j_q}$, $E(C_j) = \{x_{j_1}^+ x_{j_2}^-, \dots, x_{j_{q-1}}^+ x_{j_q}^-\}^{10}$ e, uma vez que G_M não tem ciclos, podemos concluir que

$$\begin{aligned} |V(G_M)| - |E(G_M)| - k = 0 &\Leftrightarrow 2|X| - \sum_{j=1}^k |E(C_j)| - |X| - k = 0 \\ &\Leftrightarrow k = |X| - \sum_{j=1}^k |E(C_j)| \\ &\Leftrightarrow k = |X| - |M|, \end{aligned}$$

onde k denota o número de componentes e M é o emparelhamento de $GB(P)$ definido pelos arcos (quando existem) determinados pelas cadeias C_1, \dots, C_k . Reciprocamente, supondo que $GB(P)$ admite o emparelhamento

$$M = \{x_{i_1}^+ x_{j_1}^-, x_{i_2}^+ x_{j_2}^-, \dots, x_{i_k}^+ x_{j_k}^-\},$$

então o grafo G_M , definido por

$$V(G_M) = V(GB(P)) \text{ e } E(G_M) = M \cup \{x^- x^+ \mid x \in X\},$$

tem $|X| + |M|$ arestas e (uma vez que $|V(G_M)| = 2|X|$ e G_M não tem ciclos) $2|X| - (|X| + |M|) = |X| - |M|$ componentes. Cada uma destas componentes corresponde a uma cadeia de P e cada elemento de X pertence a uma (e só uma) componente. Consequentemente, estas componentes definem uma partição de X em $|X| - |M|$ cadeias. \square

17.2.3 Problema de afectação de tarefas

Teoricamente, com base no Teorema 17.1 (teorema de Berge), é fácil descrever um algoritmo que determine um emparelhamento máximo. Com efeito, este algoritmo pode descrever-se como a seguir se indica.

```

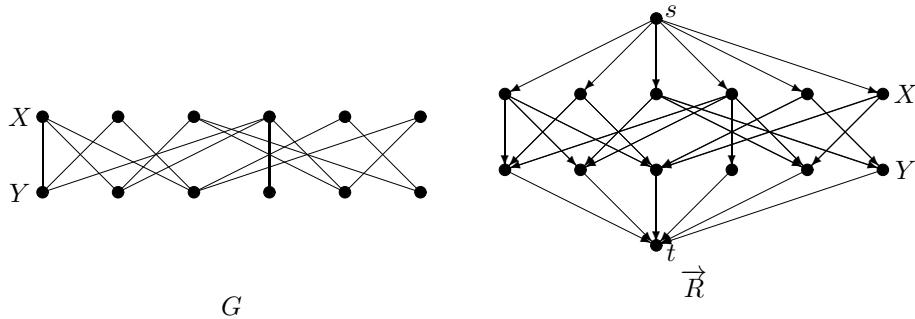
 $M \leftarrow$  um emparelhamento
enquanto existe um caminho  $M'$  de aumento (relativamente a  $M$ )
    fazer  $M \leftarrow M \Delta M'$ 
    devolver ( $M$ )

```

O principal problema deste algoritmo, porém, reside na determinação de um caminho de aumento. Com efeito, em geral uma tal tarefa exige um elevado número de operações, pelo que é computacionalmente pesada. No entanto, para grafos bipartidos, existem algoritmos muito eficientes para a determinação de emparelhamentos máximos. Um destes métodos, consiste na aplicação da determinação do fluxo máximo numa rede que se obtém por transformação (adequada) do grafo bipartido. O exemplo que se segue ilustra esta aplicação.

Exemplo 17.4. A partir de um grafo G , vamos construir uma rede \vec{R} cujo fluxo máximo determina um emparelhamento máximo em G .

Solução. Dada a bipartição (X, Y) do conjunto dos vértices de G , vamos transformar todas as arestas de G em arcos orientados de X para Y e introduzir dois vértices artificiais s e t , tais que s é a cauda de $|X|$ arcos que ligam s a cada um dos vértices de X e t é a cabeça de $|Y|$ arcos que ligam cada um dos vértices de Y a t . Finalmente, atribuímos a capacidade 1 a cada um dos arcos da rede obtida. Aplicando o algoritmo de Ford-Fulkerson a esta rede, obtém-se um fluxo máximo cujas quantidades de fluxo em cada arco pertencem a $\{0, 1\}$. É claro que as arestas de G associadas a arcos de \vec{R} com fluxo unitário, formam um emparelhamento máximo de G . A Figura 17.8 ilustra este procedimento. \square

Figura 17.8: Grafo G e respectiva rede obtida por transformação de G .

De entre os métodos conhecidos de determinação de emparelhamentos máximos em grafos bipartidos, um dos mais eficientes é, certamente, o *método húngaro* que procura um emparelhamento que satura todos os vértices de um dos subconjuntos da bipartição de vértices, se um tal emparelhamento existe, e determina um subconjunto S tal que $|N_G(S)| < |S|$, no caso contrário.

Algoritmo de afectação de tarefas – método húngaro.

Dados de entrada: grafo bipartido G (com bipartição do conjunto de vértices (X, Y)) e emparelhamento M .

Resultados: emparelhamento M que satura X , se um tal emparelhamento existe, ou subconjunto $S \subseteq X$, tal que $|S| > |N_G(S)|$, no caso contrário.

1. Se M satura os vértices de X , então PARAR. Caso contrário escolher um vértice M -livre $u \in X$, fazer $S \leftarrow \{u\}$ e $T \leftarrow \emptyset$.
2. Se $N_G(S) = T$, então PARAR ($|N_G(S)| < |S|$ e não existe um emparelhamento que sature os vértices de X). Caso contrário, escolher um vértice $y \in N_G(S) \setminus T$.
3. Se y é M -saturado, então determinar z tal que $yz \in M$, fazer $S \leftarrow S \cup \{z\}$, $T \leftarrow T \cup \{y\}$ e voltar ao passo 2. Caso contrário, sendo P o caminho M -alternado corrente entre u e y , fazer $M \leftarrow M \Delta E(P)$ e voltar ao passo 1.

Mais formalmente, segue-se o respectivo pseudocódigo que vamos designar por Algoritmo 17.1 MÉTODO HÚNGARO.

Exemplo 17.5. Com recurso à utilização do método húngaro, vamos determinar um emparelhamento perfeito (caso exista), para o grafo representado na Figura 17.9.

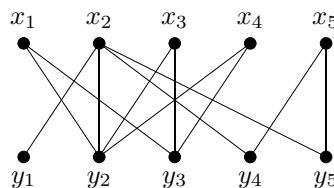


Figura 17.9: Grafo bipartido de Exemplo 17.5.

¹⁰Deve observar-se que $|C_j| = 1 \Rightarrow E(C_j) = \emptyset$.

Algoritmo 17.1: MÉTODO HÚNGARO($G = (X, Y, E), M$)

```

enquanto  $|M| \neq |X|$ 
     $u \leftarrow$  vértice  $M$ -livre de  $X$ 
     $S \leftarrow \{u\}; T \leftarrow \emptyset$ 
    repetir
        se  $N_G(S) = T$ 
        então devolver ( $S$ )a
        senão  $y \leftarrow$  elemento de  $N_G(S) \setminus T$ 
        se  $y$  é  $M$ -saturado
            então  $\begin{cases} z \leftarrow \text{vértice tal que } zy \in M \\ S \leftarrow S \cup \{z\}; T \leftarrow T \cup \{y\} \end{cases}$ 
        até  $y$  ser  $M$ -livre
         $P \leftarrow$  caminho- $(u, y)$   $M$ -alternado
         $M \leftarrow M \Delta E(P)$ 
    devolver ( $M$ )

```

^aNão existe um emparelhamento que sature os vértices de X .

Solução. Começando com um emparelhamento arbitrário, por exemplo, com uma aresta $M = \{x_1y_2\}$, obtém-se os seguintes passos:

1. Dado que M não satura todos os vértices de X , escolhemos um vértice M -livre $u \in X$, por exemplo, $u \leftarrow x_2$, fazemos $S \leftarrow \{x_2\}$ e $T \leftarrow \emptyset$.
2. Dado que $N_G(S) = \{y_1, y_2, y_4, y_5\} \neq T$, escolhemos $y \in N_G(S) \setminus T = \{y_1, y_2, y_4, y_5\}$, por exemplo, $y \leftarrow y_1$.
3. Dado que y é M -livre e $P \leftarrow x_2y_1$ é o caminho M -alternado corrente, fazemos $M \leftarrow M \Delta E(P) = \{x_1y_2, x_2y_1\}$.
1. Dado que M não satura todos os vértices de X , escolhemos um vértice M -livre $u \in X$, por exemplo, $u \leftarrow x_3$, fazemos $S \leftarrow \{x_3\}$ e $T \leftarrow \emptyset$.
2. Dado que $N_G(S) = \{y_2, y_3\} \neq T$, escolhemos $y \in N_G(S) \setminus T = \{y_2, y_3\}$, por exemplo, $y \leftarrow y_2$.
3. Dado que y é M -saturado, determinamos z tal que $yz \in M$, obtendo-se $z \leftarrow x_1$, fazemos $S \leftarrow S \cup \{x_1\} = \{x_1, x_3\}$ e $T \leftarrow T \cup \{y\} = \{y_2\}$.
2. Dado que $N_G(S) = \{y_2, y_3\} \neq T$, determinamos $y \in N_G(S) \setminus T = \{y_3\}$ e fazemos $y \leftarrow y_3$.
3. Dado que y é M -livre e $P \leftarrow x_3y_2x_1y_3$ é o caminho M -alternado corrente, fazemos $M \leftarrow M \Delta E(P) = \{x_1y_3, x_2y_1, x_3y_2\}$.
1. Dado que M não satura todos os vértices de X , escolhemos um vértice M -livre $u \in X$, por exemplo, $u \leftarrow x_4$, fazemos $S \leftarrow \{x_4\}$ e $T \leftarrow \emptyset$.
2. Dado que $N_G(S) = \{y_2, y_3\} \neq T$, escolhemos y em $N_G(S) \setminus T = \{y_2, y_3\}$, por exemplo, $y \leftarrow y_2$.
3. Dado que y é M -saturado, determinamos z tal que $yz \in M$, obtendo-se $z \leftarrow x_3$ (uma vez que $yz = y_2x_3 \in M$), fazemos $S \leftarrow S \cup \{x_3\} = \{x_3, x_4\}$ e $T \leftarrow T \cup \{y\} = \{y_2\}$.
2. Dado que $N_G(S) = \{y_2, y_3\} \neq T$, determinamos y em $N_G(S) \setminus T = \{y_3\}$, pelo que $y \leftarrow y_3$.

3. Dado que y é M -saturado, determinamos z tal que $yz \in M$, obtendo-se $z \leftarrow x_1$ (uma vez que $yz = y_3x_1 \in M$), fazemos $S \leftarrow S \cup \{x_1\} = \{x_1, x_3, x_4\}$ e $T \leftarrow T \cup \{y\} = \{y_2, y_3\}$.
2. Dado que $N_G(S) = \{y_2, y_3\} = T$, então PARAR.

Observe-se, sendo $|S| = |\{x_1, x_3, x_4\}| = 3$ e $|N_G(S)| = |\{y_2, y_3\}| = 2$, pelo teorema de Berge (Teorema 17.1) podemos concluir que o grafo não admite um emparelhamento perfeito. \square

17.2.4 Problema de afectação óptima de tarefas

Supondo que temos um conjunto de n tarefas a distribuir por n trabalhadores e que conhecemos a apetência de cada trabalhador para cada tarefa (medida por um certo peso não negativo), o problema de afectar cada tarefa a cada trabalhador com o maior apetência global possível, pode formular-se como o problema da determinação de um *emparelhamento perfeito de peso máximo* num grafo bipartido completo K_{nn} , com pesos (não negativos) nas arestas. Este problema designa-se, também, por *problema de afectação óptima de tarefas*. Em certos casos, porém, existindo certos trabalhadores sem qualquer apetência para determinadas tarefas, muitas vezes não se consideram arestas que liguem estes trabalhadores a estas tarefas e, como consequência, o grafo em questão não é bipartido completo.

Dado um grafo bipartido arbitrário G , com pesos nas arestas e bipartição dos vértices (X, Y) tal que $|X| = |Y|$, para cada aresta $e \in E(G)$, denotando o respectivo peso por $w(e)$, quaisquer que sejam $x \in X$ e $y \in Y$, podemos definir a seguinte generalização da função de pesos nas arestas

$$w(x, y) = \begin{cases} w(xy), & \text{se } xy \in E(G); \\ 0, & \text{se } xy \notin E(G). \end{cases}$$

Adoptando esta generalização para função de pesos das arestas do grafo bipartido completo que se obtém de G , acrescentando tantas arestas quantas as necessárias, sem perda de generalidade, neste tipo de problemas podemos considerar apenas grafos bipartidos completos.

No que se segue, dado um grafo bipartido G , com bipartição do conjunto de vértices (X, Y) e pesos não negativos nas arestas, vamos designar por *função de etiquetação*, uma função $l : V(G) \rightarrow \mathbb{R}$ tal que

$$\forall_{x \in X} \forall_{y \in Y} l(x) + l(y) \geq w(x, y). \quad (17.3)$$

Adicionalmente, vamos denotar por E_l o subconjunto de arestas tal que

$$E_l = \{xy \in E(G) : l(x) + l(y) = w(x, y)\}$$

e por G_l um subgrafo abrangente de G tal que $E(G_l) = E_l$ (note-se que este grafo pode ter vértices isolados).

Por exemplo, dado o grafo bipartido G , com bipartição do conjunto de vértices (X, Y) e pesos não negativos nas arestas, a função particular l , definida por

$$\forall_{x \in X} l(x) = \max_{y \in Y} w(x, y) \quad \text{e} \quad \forall_{y \in Y} l(y) = 0, \quad (17.4)$$

é uma função de etiquetação para G .

Tendo presente esta notação, estamos em condições de introduzir o seguinte teorema.

Teorema 17.12. *Dado um grafo bipartido $G = (X, Y, E)$, com função de pesos não negativos nas arestas w , seja l uma função de etiquetação (pelo que verifica a condição (17.3)). Se o subgrafo G_l contém um emparelhamento perfeito M^* , então M^* é um emparelhamento de peso máximo para G .*

Demonstração. Seja G_l o subgrafo abrangente de G definido pela função de etiquetação l e M^* um emparelhamento perfeito de G_l . Uma vez que G_l é abrangente, M^* é também um emparelhamento perfeito para G . Logo, basta mostrar que tem peso máximo.

Por definição de grafo G_l e de emparelhamento perfeito vem

$$w(M^*) = \sum_{e \in M^*} w(e) = \sum_{v \in V} l(v).$$

Por outro lado, se M é um emparelhamento de G , então

$$w(M) = \sum_{e \in M} w(e) \leq \sum_{v \in V} l(v) = w(M^*),$$

onde se conclui que M^* tem peso máximo. \square

Teorema 17.13 (Egerváry). *Dado um grafo bipartido G com pesos nas arestas, seja \mathcal{L} o conjunto das suas funções de etiquetação l (ou seja, das funções $l : V(G) \mapsto \mathbb{R}$ que verificam a condição (17.3)) e seja $l_G = \sum_{v \in V(G)} l(v)$. Então, o peso total de um emparelhamento máximo em G vem dado por $l_G^* = \min_{l \in \mathcal{L}} l_G$.*

Demonstração. Considerando um emparelhamento máximo M em G , pelo Teorema 17.12, podemos concluir a desigualdade $w(M) \leq l_G^*$. Assim, basta mostrar que existe uma função de etiquetação l^* tal que $w(M) = l_G^*$.

Seja l^* uma das funções de etiquetação para as quais se verifica a igualdade $l_G^* = \min_{l \in \mathcal{L}} l_G$, F o subconjunto de arestas $uv \in E(G)$ tais que $l^*(u) + l^*(v) = w(uv)$ e W o subconjunto de vértices $v \in V(G)$ com etiquetas positivas (ou seja, tais que $l^*(v) > 0$). Se F contém um emparelhamento M^* que satura todos os vértices de W , então

$$w(M^*) = \sum_{e \in M^*} w(e) = \sum_{v \in W} l^*(v) = \sum_{v \in V(G)} l^*(v) = l_G^*.$$

Caso contrario, (pelo teorema de Hall) existe um subconjunto $S \subseteq W$ tal que $|N_G(S)| < |S|$. Neste caso, existe $\alpha > 0$ tal que a função de etiquetação l' , definida por

$$l'(v) = \begin{cases} l^*(v) - \alpha, & \text{se } v \in S; \\ l^*(v) + \alpha, & \text{se } v \in N_G(S); \\ l^*(v), & \text{caso contrario,} \end{cases}$$

verifica a desigualdade $l'_G < l_G^*$, o que contraria a minimalidade de l^* . \square

Com base neste resultado, Kuhn¹¹ (em 1955) e Munkres¹² (em 1957) desenvolveram um algoritmo para a resolução do problema de afectação óptima de tarefas. No entanto, a versão que vamos apresentar é mais simples e foi publicada por Edmonds¹³ (em 1967).

Algoritmo de Kuhn-Munkres.

Dados de entrada: grafo bipartido (completo) G com função de pesos não negativos nas arestas w , função de etiquetação l e emparelhamento M de G_l .

¹¹Harold Kuhn, matemático americano que nasceu em 1925 e trabalhou em teoria dos jogos. Em 1980 ganhou o prémio Jhon von Neumann.

¹²James Munkres, Professor do MIT com vários livros na área da topologia.

¹³Jack R. Edmonds, matemático canadiano com contribuições muito relevantes para a optimização combinatória. Em 1985 ganhou o prémio Jhon von Neumann.

Resultados: emparelhamento de peso máximo.

1. Se M é perfeito, então PARAR (M é um emparelhamento de peso máximo). Caso contrario, escolher um vértice M -livre $u \in X$, fazer $S \leftarrow \{u\}$ e $T \leftarrow \emptyset$.
2. Se $T \subsetneq N_{G_l}(S)$, então passar para o passo 3. Se $T = N_{G_l}(S)$, então calcular

$$\alpha = \min_{x \in S, y \in Y \setminus T} \{l(x) + l(y) - w(xy)\}$$

(note-se que $\alpha > 0$), actualizar a função de etiquetação, fazendo

$$l(v) \leftarrow \begin{cases} l(v) - \alpha, & \text{para } v \in S, \\ l(v) + \alpha, & \text{para } v \in T, \\ l(v), & \text{para os restantes vértices } v, \end{cases}$$

determinar o subgrafo abrangente G_l e um emparelhamento arbitrário M em G_l .

3. Escolher $y \in N_{G_l}(S) \setminus T$. Se y é M -saturado, então determinar z tal que $yz \in M$ e fazer $S \leftarrow S \cup \{z\}$, $T \leftarrow T \cup \{y\}$ e voltar ao passo 2. Caso contrario, sendo P o caminho- (u, y) de aumento, relativamente a M , em G_l , fazer $M \leftarrow M \Delta E(P)$ e voltar ao passo 1.

O Algoritmo 17.2 KUHN MUNKRES, a seguir apresentado, descreve este procedimento em pseudocódigo.

Exemplo 17.6. Vamos determinar um emparelhamento perfeito de peso máximo num grafo bipartido definido pela seguinte matriz de pesos:

$$\begin{array}{c} x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \\ \hline y_1 & 3 & 5 & 5 & 4 & 1 \\ y_2 & 2 & 2 & 0 & 2 & 2 \\ y_3 & 2 & 4 & 4 & 1 & 0 \\ y_4 & 0 & 1 & 1 & 0 & 0 \\ y_5 & 1 & 2 & 1 & 3 & 3 \end{array}$$

Solução. Considerando a função de etiquetação particular, l , definida em (17.4), obtém-se a tabela

v	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5
$l(v)$	3	5	5	4	3	0	0	0	0	0

onde se conclui que $E(G_l) = \{x_1y_1, x_2y_1, x_3y_1, x_4y_1, x_5y_5\}$. Escolhendo como emparelhamento inicial $M = \emptyset$, a partir destes dados, por aplicação do algoritmo de Kuhn-Munkres, obtém-se os seguintes passos:

Algoritmo 17.2: KUHN MUNKRES($G = ((X, Y), W), l$)

```

repetir
   $G_l \leftarrow \emptyset$ 
  para  $x \in X$  fazer
    para  $y \in Y$  fazer
      se  $l[x] + l[y] = W[x, y]$  então  $E(G_l) \leftarrow E(G_l) \cup \{xy\}$ 
    MÉTODO HÚNGARO( $((X, Y), G_l), M$ )
    se  $|M| = |X|$  então devolver ( $M$ )
     $u \leftarrow$  um vértice  $M$ -livre de  $X$ 
     $S \leftarrow \{u\}; T \leftarrow \emptyset$ 
    enquanto  $N_{G_l}(S) \neq T$ 
      fazer  $\begin{cases} y \leftarrow \text{um elemento de } N_{G_l}(S) \setminus T \\ \text{se } y \text{ é } M\text{-saturado} \\ \quad \text{então } \begin{cases} z \leftarrow \text{o outro extremo da aresta de } M \text{ incidente em } y \\ S \leftarrow S \cup \{z\}; T \leftarrow T \cup \{y\} \end{cases} \\ \text{senão } \begin{cases} P \leftarrow \text{arestas de um caminho-}(u, y) \text{ } M\text{-alternado} \\ M \leftarrow M \Delta P \end{cases} \\ \text{interromper} \end{cases}$ 
      se  $N_{G_l}(S) = T$ 
        então  $\begin{cases} \alpha \leftarrow \infty \\ \text{para } x \in S \text{ fazer} \\ \quad \text{para } y \in Y \setminus T \text{ fazer} \\ \quad \quad \text{se } \alpha > l[x] + l[y] - W[x, y] \text{ então } \alpha \leftarrow l[x] + l[y] - W[x, y] \\ \quad \quad \text{para } x \in S \text{ fazer } l[x] \leftarrow l[x] - \alpha \\ \quad \quad \text{para } y \in T \text{ fazer } l[y] \leftarrow l[y] + \alpha \end{cases}$ 
      até falso

```

1. Dado que M não é um emparelhamento perfeito, escolhemos (por exemplo) o vértice M -livre x_1 para u (ou seja, $u \leftarrow x_1$), fazemos $S \leftarrow \{x_1\}$ e $T \leftarrow \emptyset$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_1\}$, fazemos $y \leftarrow y_1$ e, uma vez que y_1 é M -livre (pelo que $P = x_1y_1$ é um caminho de aumento em G_l), fazemos $M \leftarrow M \Delta E(P) = \{x_1y_1\}$.
1. Dado que M não é um emparelhamento perfeito, escolhemos (por exemplo) o vértice M -livre x_2 para u (ou seja, $u \leftarrow x_2$) e fazemos $S \leftarrow \{x_2\}$ e $T \leftarrow \emptyset$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_1\}$, fazemos $y \leftarrow y_1$ e, uma vez que y_1 é M -saturado, fazemos $z \leftarrow x_1$, $S \leftarrow S \cup \{z\} = \{x_1, x_2\}$ e $T \leftarrow T \cup \{y\} = \{y_1\}$.
2. Dado que $T = N_{G_l}(S)$, determinamos $\alpha = \min_{x \in S, y \in Y \setminus T} \{l(x) + l(y) - W(xy)\} = 1$, actualizamos a função de etiquetação l

v	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5
$l(v)$	2	4	5	4	3	1	0	0	0	0

e determinamos o subgrafo abrangente G_l , para o qual se obtém $E(G_l) = \{x_1y_1, x_1y_2, x_1y_3, x_2y_1, x_2y_3, x_5y_5\}$.

3. Dado que $N_{G_l}(S) \setminus T = \{y_2, y_3\}$, fazemos $y \leftarrow y_2$ e, uma vez que y_2 é M -livre (pelo que $P = x_2y_1x_1y_2$ é um caminho de aumento em G_l), fazemos $M \leftarrow M \Delta E(P) = \{x_1y_2, x_2y_1\}$.
1. Dado que M não é um emparelhamento perfeito, escolhemos (por exemplo) o vértice M -livre x_3 para u (ou seja, $u \leftarrow x_3$) e fazemos $S \leftarrow \{x_3\}$ e $T \leftarrow \emptyset$.
2. Dado que $T = N_{G_l}(S)$, determinamos $\alpha = 1$, actualizamos a função de etiquetação l

v	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5
$l(v)$	2	4	4	4	3	1	0	0	0	0

e determinamos o subgrafo abrangente G_l , para o qual se obtém $E(G_l) = \{x_1y_1, x_1y_2, x_1y_3, x_2y_1, x_2y_3, x_3y_1, x_3y_3, x_5y_5\}$.

3. Dado que $N_{G_l}(S) \setminus T = \{y_1, y_3\}$, fazemos $y \leftarrow y_3$ e, uma vez que y_3 é M -livre (pelo que $P = x_3y_3$ é um caminho de aumento em G_l), fazemos $M \leftarrow M \Delta E(P) = \{x_1y_2, x_2y_1, x_3y_3\}$.
1. Dado que M não é um emparelhamento perfeito, escolhemos (por exemplo) o vértice M -livre x_4 para u (ou seja, $u \leftarrow x_4$) e fazemos $S \leftarrow \{x_4\}$ e $T \leftarrow \emptyset$.
2. Dado que $T = N_{G_l}(S)$, determinamos $\alpha = 1$, actualizamos a função de etiquetação l

v	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5
$l(v)$	2	4	4	3	3	1	0	0	0	0

e determinamos o subgrafo abrangente G_l , para o qual se obtém $E(G_l) = \{x_1y_1, x_1y_2, x_1y_3, x_2y_1, x_2y_3, x_3y_1, x_3y_3, x_4y_1, x_4y_5, x_5y_5\}$.

3. Dado que $N_{G_l}(S) \setminus T = \{y_1, y_5\}$, fazemos $y \leftarrow y_1$ e, uma vez que y_1 é M -saturado, fazemos $z \leftarrow x_2$, $S \leftarrow S \cup \{z\} = \{x_4, x_2\}$ e $T \leftarrow T \cup \{y\} = \{y_1\}$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_3, y_5\}$, fazemos $y \leftarrow y_5$ e, uma vez que y_5 é M -livre (pelo que $P = x_4y_5$ é um caminho de aumento em G_l), fazemos $M \leftarrow M \Delta E(P) = \{x_1y_2, x_2y_1, x_3y_3, x_4y_5\}$.
1. Dado que M não é um emparelhamento perfeito, escolhemos (por exemplo) o vértice M -livre x_5 para u (ou seja, $u \leftarrow x_5$) e fazemos $S \leftarrow \{x_5\}$ e $T \leftarrow \emptyset$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_5\}$, fazemos $y \leftarrow y_5$ e, uma vez que y_5 é M -saturado, fazemos $z \leftarrow x_4$, $S \leftarrow S \cup \{z\} = \{x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_5\}$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_1\}$, fazemos $y \leftarrow y_1$ e uma vez que y_1 é M -saturado, fazemos $z \leftarrow x_2$, $S \leftarrow S \cup \{z\} = \{x_2, x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_1, y_5\}$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_3\}$, fazemos $y \leftarrow y_3$ e, uma vez que y_3 é M -saturado, fazemos $z \leftarrow x_3$, $S \leftarrow S \cup \{z\} = \{x_2, x_3, x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_1, y_3, y_5\}$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.

3. Dado que $N_{G_l}(S) \setminus T = \{y_2\}$, fazemos $y \leftarrow y_2$ e, uma vez que y_2 é M -saturado, fazemos $z \leftarrow x_1$, $S \leftarrow S \cup \{z\} = \{x_1, x_2, x_3, x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_1, y_2, y_3, y_5\}$.
2. Dado que $T = N_{G_l}(S)$, determinamos $\alpha = 2$, actualizamos a função de etiquetação l

v	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5
$l(v)$	0	2	2	1	1	3	2	2	0	2

e determinamos o subgrafo abrangente G_l , para o qual se obtém $E(G_l) = \{x_1y_1, x_1y_2, x_1y_3, x_1y_4, x_2y_1, x_2y_3, x_3y_1, x_3y_3, x_4y_1, x_4y_5, x_5y_5\}$.

1. Dado que M não é um emparelhamento perfeito, escolhemos (por exemplo) o vértice M -livre x_5 para u (ou seja, $u \leftarrow x_5$) e fazemos $S \leftarrow \{x_5\}$ e $T \leftarrow \emptyset$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_5\}$, fazemos $y \leftarrow y_5$ e, uma vez que y_5 é M -saturado, fazemos $z \leftarrow x_4$, $S \leftarrow S \cup \{z\} = \{x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_5\}$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_1\}$, fazemos $y \leftarrow y_1$ e, uma vez que y_1 é M -saturado, fazemos $z \leftarrow x_2$, $S \leftarrow S \cup \{z\} = \{x_2, x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_1, y_5\}$.
2. Dado que $T \subsetneq N_{G_l}(S)$, passamos para o passo 3.
3. Dado que $N_{G_l}(S) \setminus T = \{y_3\}$, fazemos $y \leftarrow y_3$ e, uma vez que y_3 é M -saturado, fazemos $z \leftarrow x_3$, $S \leftarrow S \cup \{z\} = \{x_2, x_3, x_4, x_5\}$ e $T \leftarrow T \cup \{y\} = \{y_1, y_3, y_5\}$.
2. Dado que $T = N_{G_l}(S)$, determinamos $\alpha = 1$, actualizamos a função de etiquetação l

v	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5
$l(v)$	0	1	1	0	0	4	2	3	0	3

e determinamos o subgrafo abrangente G_l , para o qual se obtém $E(G_l) = \{x_1y_2, x_1y_4, x_2y_1, x_2y_3, x_2y_4, x_3y_1, x_3y_3, x_3y_4, x_4y_1, x_4y_2, x_4y_4, x_4y_5, x_5y_2, x_5y_4, x_5y_5\}$.

3. Dado que $N_{G_l}(S) \setminus T = \{y_4\}$, fazemos $y \leftarrow y_4$ e, uma vez que y_4 é M -livre (pelo que $P = x_5y_4$ é um caminho de aumento em G_l), fazemos $M \leftarrow M \Delta E(P) = \{x_1y_2, x_2y_1, x_3y_3, x_4y_5, x_5y_4\}$.
1. Dado que M é perfeito, PARAR.

Observe-se que, neste exemplo de aplicação, existem vários emparelhamentos perfeitos em G_l e, como consequência, vários emparelhamentos perfeitos de peso máximo em G (todos, naturalmente, com peso igual a 14). \square

17.3. Emparelhamentos em grafos arbitrários

No caso de grafos arbitrários, a determinação de um emparelhamento máximo é um problema bastante mais difícil do que no caso de grafos bipartidos. O resultado que se segue, conhecido por *lema da contracção de ciclos* (*cycle shrinking lemma*, na terminologia inglesa), constitui a base dos algoritmos que vamos propor para a determinação de emparelhamentos máximos em grafos arbitrários. Note-se que a contracção de um ciclo, corresponde à contracção sucessiva de todas as suas arestas, reduzindo-o a um único vértice.

Teorema 17.14 (Lema da contracção de ciclos). *Considere-se um grafo G , um emparelhamento M em G e um ciclo C de comprimento $2k + 1$ ($k \in \mathbb{N}$) que contém, exactamente, k arestas de M e um vértice M -livre. Se G^* é o grafo que se obtém de G após a contracção de C , então M é um emparelhamento máximo de G se e só se $M^* = M \setminus E(C)$ é um emparelhamento máximo de G^* .*

Demonstração. Suponha que M é um emparelhamento que não é máximo para o grafo G . Então, tendo em conta o teorema de Berge (Teorema 17.1), existe um caminho de aumento P , relativamente a M .

- Se o caminho P é disjunto do ciclo C , relativamente aos vértices (ou seja, $V(P) \cap V(C) = \emptyset$), então P é também um caminho de aumento em G^* , relativamente a M^* , e, consequentemente, M^* não é máximo em G^* .
- Se P não é disjunto do ciclo C , uma vez que C tem um único vértice M -livre, pelo menos um dos vértices extremos de P , x , não pertence a C . Seja z o primeiro vértice de P pertencente a C , quando se percorre o caminho P a partir de x . Então, o subcaminho- (x, z) de P é um caminho de aumento em G^* , relativamente ao emparelhamento M^* (note-se que o vértice obtido por contracção do ciclo C é M^* -livre), e, consequentemente, M^* não é máximo em G^* .

Reciprocamente, suponha que M^* não é máximo em G^* e seja N^* um emparelhamento em G^* tal que $|N^*| > |M^*|$. Voltando ao grafo G , reconstruindo-se o ciclo C , podemos concluir que o emparelhamento de G que corresponde ao emparelhamento N^* de G^* , não satura mais do que um vértice em C . Assim, podemos acrescentar k arestas de C a este emparelhamento, de modo a obter um emparelhamento N de cardinalidade $|N^*| + k$. Logo,

$$|N| = |N^*| + k > |M^*| + k = |M|,$$

e, como consequência, M também não é máximo em G . □

Definição 17.8 (Flor com caule). *Um passeio M -alternado $F = v_0v_1\dots v_t$ diz-se uma flor com caule, se t é ímpar, o vértice v_0 é M -livre, os vértices v_0, v_1, \dots, v_{t-1} são todos distintos e existe um índice par $i \in \{2, \dots, t-1\}$ tal que $v_i = v_t$. Por sua vez, o ciclo $v_iv_{i+1}\dots v_t$ designa-se por flor e o caminho $v_0v_1\dots v_i$ designa-se por caule.*

Na Figura 17.10, apresenta-se um exemplo de uma flor com caule.

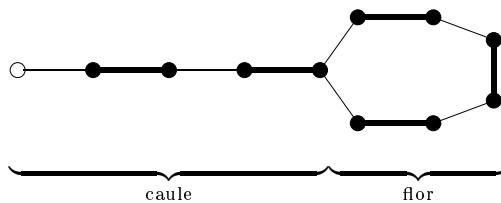


Figura 17.10: Flor com caule, onde os vértices não saturados são representados por \circ , os saturados por \bullet e as arestas do emparelhamento são representadas a negrito.

Teorema 17.15. *Dado um grafo G e um seu emparelhamento M , seja X o conjunto de todos os vértices M -livres de G e $P = v_0v_1\dots v_t$ um passeio M -alternado mais curto entre dois vértices distintos de X . Então ou P é um caminho de aumento ou existe $v_j \in V(P)$ tal que $v_0v_1\dots v_j$ é uma flor com caule.*

Demonstração. É claro que se P é um caminho, então é um caminho de aumento. Supondo que P não é um caminho, se j é o menor índice para o qual existe $i < j$, com $v_i = v_j$, então os vértices

v_0, v_1, \dots, v_{j-1} são todos distintos. Nestas condições, podemos concluir que $j - i$ é um número ímpar (uma vez que $j - i$ é o comprimento do ciclo que se inicia e termina em $v_i = v_j$ e, caso este ciclo tivesse comprimento par, o passeio M -alternado não seria o mais curto entre os dois vértices de X). Como consequência j e i têm paridade distinta. Caso i fosse ímpar teriam de existir duas arestas M -saturadas incidentes em $v_i = v_j$ o que é absurdo. Logo i é par e, consequentemente, (de acordo com a definição) $v_0v_1\dots v_j$ é uma flor com caule. \square

Algoritmo de determinação de um caminho de aumento

Dados de entrada: grafo G e emparelhamento M ;

Resultados: caminho de aumento em G , relativamente a M , caso exista;

Notação: X denota o conjunto de vértices M -livres em G ; se B é uma flor relativamente a M em G , então $G \circ B$ e $M \circ B$ são, respectivamente, o grafo que se obtém de G e o emparelhamento que se obtém de M , após a contracção de B .

1. Se não existe um passeio não trivial (ou seja, de comprimento positivo) M -alternado entre vértices de X , então PARAR (não existe um caminho de aumento em G , relativamente a M).
2. Determinar um passeio P não trivial M -alternado de comprimento mínimo entre dois vértices de X . Seja $P = v_0v_1\dots v_t$.
 - (a) Se P é um caminho então PARAR (P é um caminho de aumento em G , relativamente a M).
 - (b) Se j é tal que $P = v_0v_1\dots v_j$ é uma flor com caule e B é a respectiva flor, então executar este algoritmo, para o grafo $G \circ B$, tendo em vista a determinação de um caminho de aumento P , relativamente a $M \circ B$, em $G \circ B$, expandir P até se obter o caminho de aumento em G , relativamente a M , e PARAR.

Teorema 17.16. *Para qualquer grafo G existe um algoritmo que determina um emparelhamento máximo com uma complexidade computacional de $\mathcal{O}(\nu^2\epsilon)$.*

Demonstração. Considere-se o seguinte algoritmo de determinação de um emparelhamento máximo num grafo arbitrário G .

Algoritmo

1. $M \leftarrow \emptyset$,
2. Executar o algoritmo (anteriormente introduzido) de determinação de um caminho de aumento P , relativamente a M .
3. Se um tal caminho de aumento não existe, então PARAR (M é um emparelhamento máximo). Caso contrário, fazer $M \leftarrow M \Delta E(P)$ e voltar para o passo 2.

Uma vez que um passeio alternado entre dois vértices distintos de X pode ser determinado com uma complexidade de $\mathcal{O}(\epsilon)$, o grafo $G \circ B$ pode ser produzido com $\mathcal{O}(\epsilon)$ operações e a profundidade de recorrência é $\mathcal{O}(\nu)$, podemos concluir que a complexidade da determinação de um caminho de aumento é $\mathcal{O}(\nu\epsilon)$. Como consequência, tendo em conta que o passo 3 do algoritmo é executado, no pior caso, $\nu/2$ vezes, conclui-se que este algoritmo tem uma complexidade computacional de $\mathcal{O}(\nu^2\epsilon)$. \square

Para tornar este algoritmo (de determinação de um emparelhamento máximo) computacionalmente mais eficiente, é necessário melhorar o procedimento de determinação de um passeio alternado e o procedimento de contracção de uma flor, cuja complexidade (em ambos os casos) é $\mathcal{O}(\epsilon)$. Com este objectivo, vamos introduzir a seguinte estrutura de dados auxiliar.

Definição 17.9 (Floresta M -alternada). *Dado um grafo simples G e um seu emparelhamento M , seja X o conjunto de todos os vértices M -livres de G . Então, designa-se por floresta M -alternada, toda a floresta F que é subgrafo abrangente de G , tal que $M \subseteq E(F)$, onde cada componente ou contém exactamente um vértice M -livre (designado por raiz) ou é constituída por uma única aresta de M e onde cada caminho de F , com vértice extremo em X , é M -alternado.*

Adicionalmente, dada uma floresta M -alternada F de um grafo G , vamos denotar por

- $\text{pares}(F) = \{v \in V(G) : F \text{ contém um caminho-}(x, v) \text{ de comprimento par, com } x \in X\}$,
- $\text{ímpares}(F) = \{v \in V(G) : F \text{ contém um caminho-}(x, v) \text{ de comprimento ímpar, com } x \in X\}$,
- $\text{livres}(F) = \{v \in V(G) : F \text{ não contém nenhum caminho-}(x, v), \text{ com } x \in X\}$.

Na Figura 17.11, representa-se um exemplo de uma floresta M -alternada.

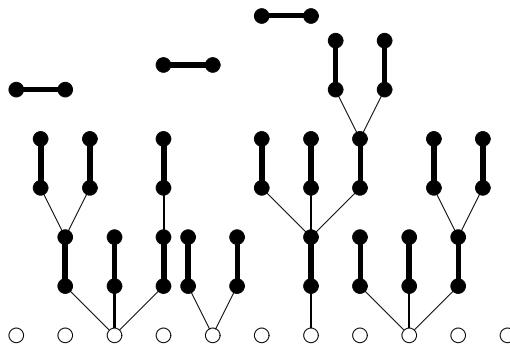


Figura 17.11: Exemplo de uma floresta M -alternada (onde os vértices não saturados são representados por \circ , os vértices saturados por \bullet e as arestas do emparelhamento são representadas a negrito).

Teorema 17.17 (Tutte-Berge). *Dado um grafo G , a cardinalidade de um emparelhamento máximo é igual a*

$$\min_{U \subseteq V(G)} \frac{1}{2} (|V(G)| + |U| - \iota(G - U)),$$

onde $\iota(H)$ denota o número de componentes ímpares do grafo H .

Demonstração. Denotando por $m(G)$ o cardinalidade de um emparelhamento máximo de G ,

$$\begin{aligned} m(G) &\leq |U| + m(G - U) \leq |U| + \frac{1}{2} (|V(G) \setminus U| - \iota(G - U)) \\ &= \frac{1}{2} (|V(G)| + |U| - \iota(G - U)). \end{aligned}$$

Reciprocamente, vamos mostrar, por indução sobre $\nu(G)$, que existe $U \subseteq V(G)$ tal que

$$m(G) \geq \frac{1}{2} (|V(G)| + |U| - \iota(G - U)), \quad (17.5)$$

tendo em conta que desigualdade (17.5) é trivialmente verdadeira, para $\nu(G) = 1$. Sem perda de generalidade, vamos assumir que G é conexo (caso contrário, a prova podia ser feita, separadamente, para cada componente) e que a desigualdade (17.5) se verifica para grafos com menos do que $\nu(G)$ vértices, com $\nu(G) > 1$.

- Se existe um vértice $v \in V(G)$ que é saturado por todos os emparelhamentos máximos de G , então $m(G) = m(G - v) + 1$ e, por hipótese de indução, existe $U' \subseteq V(G - v)$ tal que

$$\begin{aligned} m(G) &\geq \frac{1}{2} (|V(G - v)| + |U'| - \iota(G - v - U')) + 1 \\ &= \frac{1}{2} (|V(G)| - 1 + |U| - 1 - \iota(G - U)) + 1 \\ &= \frac{1}{2} (|V(G)| + |U| - \iota(G - U)), \end{aligned}$$

onde $U = U' \cup \{v\}$.

- Suponha que não existe nenhum vértice $v \in V(G)$ que seja saturado por todos os emparelhamentos máximos de G . Então, $m(G) < \frac{1}{2}\nu(G)$ e, neste caso, vamos mostrar que existe um emparelhamento de cardinalidade $\frac{1}{2}(\nu(G) - 1)$, o que implica o resultado pretendido (utilizando $U = \emptyset$). Como efeito, vamos assumir que tal não acontece, ou seja, que cada emparelhamento máximo de G não satura pelo menos dois vértices $u, v \in V(G)$. Seja M um emparelhamento máximo de G , relativamente ao qual existem dois vértices M -livres, u e v , que estão à distância mínima em G entre todos os pares de saturados por emparelhamentos máximos de G . Se $\text{dist}(u, v) = 1$, então u e v são adjacentes e podemos incluir a aresta uv no emparelhamento M , o que contradiz o facto de M ser máximo. Assim, podemos assumir que $\text{dist}(u, v) \geq 2$ e podemos escolher um vértice interior t de um caminho mais curto entre u e v . Por hipótese, existe pelo menos um emparelhamento máximo que não satura o vértice t . Seja N um emparelhamento escolhido de entre os emparelhamentos em tais condições (ou seja, que são máximos e não saturam t) de tal forma que maximiza $|M \cap N|$. Tendo em conta a minimalidade de $\text{dist}(u, v)$, podemos concluir que o emparelhamento N satura ambos vértices u e v (caso contrário, por exemplo, sendo u um vértice N -livre, $\text{dist}(u, t) < \text{dist}(u, v)$). Por outro lado, uma vez que M e N saturam o mesmo número de vértices, existe um vértice $x \neq t$ que é N -livre e M -saturado e, consequentemente, existe ainda um vértice y tal que $e = xy \in M$ (e, naturalmente, $e \notin N$). Tendo em conta a maximalidade de N , é claro que y é N -saturado, pelo que existe uma aresta $f = yz \in N$ (e, naturalmente, $f \notin M$). Finalmente, sendo $N' = (N \setminus \{f\}) \cup \{e\}$, N' é um emparelhamento máximo que não satura t tal que $|M \cap N'| > |M \cap N|$, o que é contraditório.

□

Antes de prosseguirmos com uma nova versão do algoritmo de determinação de um emparelhamento máximo, computacionalmente mais eficiente do que a versão apresentada na demonstração do Teorema 17.16, convém referir algumas propriedades de uma floresta M -alternada F .

- Qualquer vértice M -livre pertence a $\text{pares}(F)$;
- Se $v \in \text{ímpares}(F)$, então v é vértice extremo de exactamente uma aresta de M e exactamente uma aresta de $E(F) \setminus M$, ou seja, $d_F(v) = 2$;
- Se não existe nenhuma aresta de G entre $\text{pares}(F)$ e $\text{pares}(F) \cup \text{livres}(F)$, então
 - M é um emparelhamento máximo de G (como consequência do teorema de Tutte-Berge);
 - o conjunto $\text{pares}(F)$ é um conjunto independente¹⁴ de G ;
- Se $U = \text{ímpares}(F)$, então

$$\iota(G - U) \geq |V(G)| - 2|M| + |U| = |X| + |U| = |\text{pares}(F)|,$$

¹⁴Um subconjunto S de vértices de um grafo diz-se um independente se não existe nenhuma aresta desse grafo com extremos em S .

tendo em conta que a primeira desigualdade decorre, directamente, do teorema de Tutte-Berge, a segunda decorre da definição de vértice M -livre e a terceira é consequência da estrutura da floresta M -alternada F (uma vez que qualquer vértice ímpar é vértice intermédio de um caminho que se inicia num vértice par de X , prossegue com vértices alternadamente pares e ímpares e termina num vértice par).

Algoritmo de determinação de um emparelhamento máximo

Dados de entrada: grafo G e emparelhamento M ;

Resultados de saída: emparelhamento máximo M ;

Estruturas de dados: floresta M -alternada F ; listas de arestas de $E(G)$, de M e de F incidentes em cada vértice v , registo com uma aresta $e_v = vu$ tal que $u \in \text{pares}(F)$ (se tal aresta existe); listas de arestas de $E(G)$ incidentes no conjunto $\text{pares}(F)$ e no conjunto $\text{ímpares}(F)$;

Notação: X denota o conjunto de vértices M -livres em G e caminho- (X, v) denota um caminho- (x, v) em F , com $x \in X$.

1. Fazer $F \leftarrow M$ e, para cada vértice $v \in V(G)$, escolher uma aresta $e_v = vu$, onde $u \in \text{pares}(F)$ (se tal aresta existe).
2. Se para cada vértice $v \in \text{pares}(F) \cup \text{livres}(F)$ a respectiva aresta e_v não existe, então PARAR (o emparelhamento corrente, M , é máximo). Caso contrário, escolher um vértice $v \in \text{pares}(F) \cup \text{livres}(F)$, com aresta $e_v = vu$.
3. Se $v \in \text{livres}(F)$, então inserir a aresta e_v na floresta F . Sendo $w \in V(G)$ tal que $vw \in M$, para cada aresta $wx \in E(G)$, fazer $e_x \leftarrow wx$, e voltar ao passo 2.
4. Se $v \in \text{pares}(F)$ então determinar um caminho- (X, u) P e um caminho- (X, v) Q .
 - (a) Se P e Q são disjuntos nas arestas, então fazer $M \leftarrow M \Delta Z$ (note-se que $Z = E(P) \cup E(Q) \cup \{uv\}$ determina um caminho de aumento, relativamente a M), actualizar a estrutura de dados e voltar ao passo 2.
 - (b) Se P e Q não são disjuntos nas arestas, então
 - i. fazer B igual à flor contida em $P + Q + uv$;
 - ii. fazer $G \leftarrow G \circ B$, eliminar os lacetes produzidos e denotar por B o vértice produzido com a contracção da flor;
 - iii. para cada aresta $Bx \in E(G)$, fazer $e_x \leftarrow Bx$ e voltar ao passo 2.

Mostra-se que este algoritmo determina um emparelhamento máximo com uma complexidade computacional de $\mathcal{O}(\nu^3)$.

17.4. Emparelhamentos em grafos com pesos nas arestas

Tal como para os emparelhamentos em grafos sem pesos nas arestas, estudados na secção anterior, o algoritmo de determinação de um emparelhamento de peso mínimo que vamos apresentar, é baseado num procedimento de contracção de ciclos. Neste caso porém, utiliza-se também o procedimento inverso de expansão de ciclos (com o qual se reconstrói o ciclo anteriormente contraído).

Ao longo desta secção, assume-se que G é um grafo, $w : E(G) \mapsto \mathbb{Q}$ é uma função de pesos não negativos nas arestas (ou seja, $w(e) \geq 0 \forall e \in E(G)$) e G contém pelo menos um emparelhamento perfeito.

Definição 17.10 (Estrato de um conjunto C). Uma família \mathcal{C} de subconjuntos de um dado conjunto C designa-se por estrato de C se para cada par de conjuntos $T, U \in \mathcal{C}$ se verifica que $T \subseteq U$ ou $U \subseteq T$ ou $T \cap U = \emptyset$ e $C = \bigcup_{T \in \mathcal{C}} T$.

As principais ferramentas que vamos utilizar são um estrato \mathcal{C} do conjunto de vértices $V(G)$, a definir no algoritmo, cujos subconjuntos têm cardinalidade ímpar, e uma função $\pi : \mathcal{C} \mapsto \mathbb{Q}$ que verifica as seguintes condições:

- (i) $\pi(U) \geq 0$ se $U \in \mathcal{C}$ e $|U| \geq 3$,
- (ii) $\sum_{U \in U_e} \pi(U) \leq w(e)$, para cada $e \in E(G)$, onde $U_e = \{U \in \mathcal{C} : e \in \partial(U)\}$ e $\partial(U)$ denota o corte definido pelo subconjunto de vértices U (ou seja, o conjunto de arestas com um único extremo em U).

Observe-se que estas condições implicam que se M é um emparelhamento perfeito em G , então

$$w(M) \geq \sum_{U \in \mathcal{C}} \pi(U),$$

uma vez que

$$w(M) = \sum_{e \in M} w(e) \geq \sum_{e \in M} \sum_{U \in U_e} \pi(U) = \sum_{U \in \mathcal{C}} \pi(U) |M \cap \partial(U)| = \sum_{U \in \mathcal{C}} \pi(U).$$

Como consequência, dado um emparelhamento perfeito M^* , se a igualdade $w(M^*) = \sum_{U \in \mathcal{C}} \pi(U)$ se verifica, então M^* tem custo mínimo.

Antes da descrição algorítmica da determinação de um emparelhamento perfeito de peso mínimo (a qual se pode, facilmente, estender à determinação de um emparelhamento perfeito de custo máximo), vamos introduzir a notação necessária para esta descrição.

- Para cada aresta e , $w_\pi(e) = \sum_{e \in M} \sum_{U \in U_e} \pi(U)$ (observe-se que $w_\pi(e) \geq 0$ para $e \in E(G)$).
- E_π denota o conjunto de arestas $e \in E(G)$, tais que $w_\pi(e) = 0$, e G_π denota o subgrafo abrangente de G tal que $E(G_\pi) = E_\pi$.
- Assumindo que $\{v\} \in \mathcal{C} \forall v \in V(G)$, denota-se por \mathcal{C}^{max} a família de conjuntos de \mathcal{C} , maximais relativamente à relação de inclusão (observe-se que \mathcal{C}^{max} constitui uma partição do conjunto $V(G)$).
- G' denota o grafo obtido a partir G_π pela contracção de todos os conjuntos de \mathcal{C}^{max} , a qual denotamos por $G' = G_\pi \diamond \mathcal{C}^{max}$ (observe-se que os vértices de G' correspondem a conjuntos de \mathcal{C}^{max} e $xy \in E(G')$ se existe uma aresta de G que liga os conjuntos de vértices correspondentes a x e a y).
- Para cada $U \in \mathcal{C}$ tal que $|U| \geq 3$, vamos denotar por H_U o grafo obtido a partir do subgrafo de G induzido por U , isto é $G[U]$, por contracção do todos os subconjuntos próprios maximais de U que pertencem ao estrato \mathcal{C} .

Algoritmo para emparelhamentos perfeitos de peso mínimo

Dados de entrada: grafo G com função de pesos nas arestas w e com pelo menos um emparelhamento perfeito;

Resultados de saída: emparelhamento perfeito de custo mínimo M ;

Estruturas de dados: estrato \mathcal{C} do conjunto $V(G)$ com subconjuntos de cardinalidade ímpar; função $\pi : \mathcal{C} \mapsto \mathbb{Q}$ com as propriedades (i) e (ii) anteriormente referidas; emparelhamento M ; para cada $U \in \mathcal{C}$, com $|U| \geq 3$, C_U denota o ciclo que contém todos os vértices do grafo H_U .

1. Fazer $\mathcal{C} \leftarrow \{\{v\} : v \in V(G)\}$, $M \leftarrow \emptyset$ e $\pi(\{v\}) \leftarrow 0$, para cada $v \in V(G)$.
2. Fazer $G' \leftarrow G_\pi \diamond \mathcal{C}^{max}$ e X igual ao conjunto de vértices M -livres de G' .
3. Se G' contém um passeio M -alternado de comprimento positivo entre dois vértices de X , então
 - (a) determinar em G' um passeio M -alternado mais curto P , de comprimento positivo, entre dois vértices de X ;
 - (b) se P é um caminho, então $M \leftarrow M \Delta E(P)$ e passar para o passo 4;
 - (c) se P não é um caminho, então contém uma flor com caule e , sendo B uma destas flores, fazer $U \leftarrow V(C)$, $\mathcal{C} \leftarrow \mathcal{C} \cup U$, $\pi(U) \leftarrow 0$, $M \leftarrow M \setminus E(C)$, $C_U \leftarrow C$ e passar para o passo 4;
- senão
 - (a) fazer S igual ao subconjunto de $V(G')$ para o qual existe um passeio M -alternado, de comprimento ímpar, entre um vértice de X e um vértice de S ;
 - (b) fazer T igual ao subconjunto de $V(G')$ para o qual existe um passeio M -alternado, de comprimento par, entre um vértice de X e um vértice de S ;
 - (c) para cada $U \in \mathcal{C}$, fazer

$$\pi(U) \leftarrow \begin{cases} \pi(U) + \alpha, & \text{se } U \subseteq T; \\ \pi(U) - \alpha, & \text{se } U \subseteq S; \\ \pi(U), & \text{nos restantes casos,} \end{cases}$$

onde α é o maior valor para o qual π ainda verifica as condições (i) e (ii).

- (d) para cada $U \in \mathcal{C}$ tal que $\pi(U) = 0$,
 - i. fazer $\mathcal{C} \leftarrow \mathcal{C} \setminus \{U\}$ e proceder à respectiva expansão do grafo G' ;
 - ii. sendo v o único vértice M -saturado em C_U , fazer $M \leftarrow M \cup M_U$, onde M_U é o emparelhamento perfeito do caminho $C_U - v$.
 4. Se M é um emparelhamento perfeito de G' , então adicionar a M as arestas dos emparelhamentos perfeitos dos caminhos $C_U - v$, para cada $U \in \mathcal{C}^{max}$ onde, em cada um deles, v é o único vértice não saturado e PARAR. Caso contrário, passar para o passo 2.
-

Mostra-se que este algoritmo determina um emparelhamento perfeito de peso mínimo com uma complexidade computacional $\mathcal{O}(\nu^2\varepsilon)$.

No caso de se pretender determinar um emparelhamento perfeito de peso máximo, basta modificar o problema, alterando cada um dos pesos nas arestas, fazendo $w(e) \leftarrow W - w(e)$, onde W é uma constante com valor superior ao maior dos pesos, e aplicar o algoritmo anterior ao problema modificado.

Também se pode estender a aplicação deste algoritmo à determinação, em grafos arbitrários G , de emparelhamentos com o máximo número de arestas (não necessariamente perfeitos) e com peso mínimo (máximo). Com este objectivo, basta aplicar o algoritmo anterior a um grafo G^* , com função de pesos nas arestas w^* , que se obtém por modificação do grafo original G e da respectiva função de pesos nas arestas w , conforme a seguir se indica.

1. Fazer uma cópia G' e w' de G e w , respectivamente, tal que a cada $v \in V(G)$ corresponde $v' \in V(G')$ e $w'(xy) = w(x'y') \forall xy \in E(G)$.
2. Determinar o grafo G^* tal que $V(G^*) = V(G) \cup V(G')$ e $E(G^*) = E(G) \cup E(G') \cup \{vv' : v \in V(G)\}$.
3. Determinar a função de pesos nas arestas w^* tal que

$$w^*(e) = \begin{cases} w(e), & \text{se } e \in E(G); \\ w'(e), & \text{se } e \in E(G'); \\ \delta, & \text{nos outros casos,} \end{cases}$$

onde δ toma um valor suficientemente grande¹⁵ ($\delta = 0$) no caso de se pretender determinar um emparelhamento de peso mínimo (máximo).

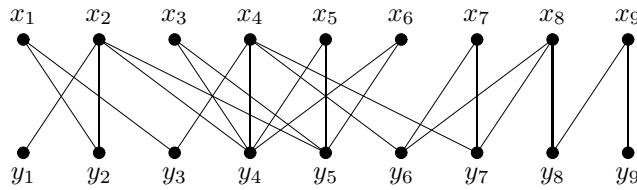
Por um lado, é claro que o grafo G^* admite um emparelhamento perfeito. Por outro lado, por aplicação do algoritmo anterior, determinado, em G^* , um emparelhamento perfeito de peso mínimo (máximo) M^* , vem que $M^* \cap E(G)$ é um emparelhamento de G de cardinalidade máxima com peso mínimo (máximo).

Resta referir que a complexidade computacional da aplicação do algoritmo para emparelhamentos perfeitos de peso mínimo (máximo), mesmo com estas modificações, mantém, evidentemente, a mesma ordem, ou seja, $\mathcal{O}(\nu^2\varepsilon)$.

17.5. Exercícios

- 17.1. Dada a família de subconjuntos do conjunto $X = \{0, 1, 2, \dots, 9\}$, $\mathcal{F} = \{\{1, 4, 7, 8, 9\}, \{2, 3, 9\}, \{0, 1, 4, 6\}, \{2, 3, 5\}, \{0, 5, 6, 7\}, \{0, 4, 7, 8\}, \{1, 4, 6, 8\}, \{2, 5, 9\}, \{1, 2, 3, 5\}\}$, determine um sistema de representantes distintos.
- 17.2. Sendo $G = (X, Y, E)$ um grafo bipartido, com pelo menos uma aresta, tal que $\min_{x \in X} d_G(x) \geq \max_{y \in Y} d_G(y)$, prove as seguintes proposições:
 - (a) $|X| \leq |Y|$;
 - (b) G admite um emparelhamento M tal que $|M| = |X|$.
- 17.3. Prove que, sendo G um grafo bipartido e $X \subseteq V(G)$ o subconjunto dos vértices de grau máximo, existe um emparelhamento M que satura todos os vértices de X .
- 17.4. Prove que um grafo bipartido p -regular admite p emparelhamentos perfeitos disjuntos nos arcos, ou seja, é 1-factorizável.
- 17.5. Considere o grafo bipartido representado na figura a seguir e determine um emparelhamento máximo utilizando o Algoritmo 17.1 MétodoHúngaro (página 462)

¹⁵Pode escolher-se, por exemplo, $\delta = \sum_{e \in E(G)} w(e) + 1$.



- 17.6. Determine um emparelhamento perfeito de peso máximo do grafo bipartido definido pela seguinte matriz de pesos

$$\begin{array}{cccccccc} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ y_1 & \left(\begin{array}{cccccccc} 1 & 2 & 1 & 3 & 5 & 5 & 4 & 1 \\ 2 & 3 & 2 & 4 & 0 & 1 & 2 & 2 \\ 2 & 4 & 1 & 4 & 1 & 3 & 0 & 1 \\ 0 & 1 & 1 & 2 & 2 & 3 & 0 & 0 \\ 1 & 2 & 1 & 3 & 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 1 & 1 & 2 & 0 & 2 \\ 3 & 0 & 1 & 4 & 2 & 1 & 1 & 1 \\ 2 & 1 & 2 & 3 & 2 & 1 & 0 & 3 \end{array} \right) \\ y_2 & \quad \\ y_3 & \quad \\ y_4 & \quad \\ y_5 & \quad \\ y_6 & \quad \\ y_7 & \quad \\ y_8 & \quad \end{array},$$

utilizando o Algoritmo 17.2 de Kuhn e Munkres (página 466).

- 17.7. Considere a matriz

$$A = \begin{pmatrix} 3 & 0 & 5 & 0 & 1 \\ 0 & 0 & 1 & 2 & 4 \\ 0 & 4 & 3 & 5 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 2 & 1 \end{pmatrix}$$

- (a) Determine o menor número de traços (verticais ou horizontais) que cobrem todos os zeros de A .
(b) Determine um emparelhamento perfeito de peso máximo num grafo bipartido completo definido pela matriz de pesos A .

- 17.8. Prove que um grafo bipartido G admite um emparelhamento perfeito se e só se uma cobertura por vértices mínima tem cardinalidade $\frac{1}{2}\nu(G)$.

- 17.9. Dado um grafo conexo arbitrário G suponha o seguinte jogo com dois jogadores: cada jogador escolhe alternadamente uma aresta $e \in E(G)$ ainda não escolhida de tal forma que as arestas já escolhidas (incluindo a aresta e) definam um caminho, perdendo o jogador que não for capaz de escolher uma aresta de acordo com estas regras. Prove que se G admite um emparelhamento perfeito, então existe uma estratégia ganhadora para o primeiro jogador.

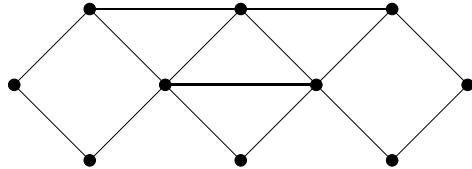
- 17.10. Um grafo G é *factor-crítico* se $G - v$ admite um emparelhamento perfeito qualquer que seja o vértice $v \in V(G)$. Prove que se um grafo é bipartido então não é factor-crítico.

- 17.11. Para cada número $k \in \mathbb{N}$, determine um grafo simples $2k$ -regular que não admite um emparelhamento perfeito.

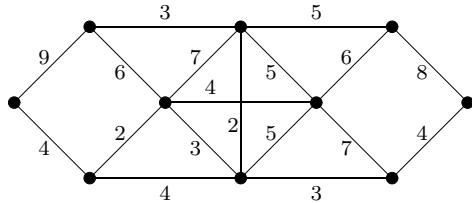
- 17.12. Represente um grafo conexo, G , sem vértices de corte que admite um emparelhamento perfeito tal que $\Delta(G) = 3$.

- 17.13. Demonstre que um grafo 3-regular admite um emparelhamento perfeito se e só se as suas arestas se podem decompor num conjunto de cópias de P_4 .

- 17.14. Dados dois inteiros positivos k e l tais que $1 \leq l \leq k$, sendo $Z(k, l)$ um grafo tal que $V(Z(k, l)) = \{1, 2, \dots, k\}$ e $E(Z(k, l)) = \{xy : |x - y| \geq l\}$, responda às seguintes questões:
- Represente o grafo $Z(8, 3)$.
 - Prove que se k é par e $2l \leq k$, então $Z(k, l)$ admite um emparelhamento perfeito.
 - Determine todos os valores de k e l , tais que $Z(k, l)$ admite um emparelhamento perfeito.
 - Mostre que $Z(k, l)$ é bipartido se e só se $2l \geq k$.
 - Determine o número cromático $\chi(Z(k, l))$.
- 17.15. Mostre que uma árvore admite no máximo um 1-factor
- 17.16. Prove que o grafo de Petersen não é 1-factorizável.
- 17.17. Seja G um grafo simples de ordem par, tal que
- $$d_G(x) + d_G(y) \geq \nu(G) - 1 \quad \forall x, y \in V(G).$$
- Prove que G admite um 1-factor.
- 17.18. Seja $R(m, n)$ o grafo simples cujos vértices são os pares ordenados de inteiros (z_1, z_2) , tais que $1 \leq z_1 \leq m$ e $1 \leq z_2 \leq n$, onde dois vértices (z_1, z_2) e (\bar{z}_1, \bar{z}_2) são adjacentes se $z_1 = \bar{z}_1$ e $|z_2 - \bar{z}_2| = 1$ ou $z_2 = \bar{z}_2$ e $|z_1 - \bar{z}_1| = 1$. Mostre que $R(m, n)$ admite um 1-factor se e só se mn é par.
- 17.19. Seja G um grafo que não admite um 1-factor e seja M um emparelhamento máximo. Prove que qualquer aresta incidente num vértice não saturado por M faz parte de um emparelhamento máximo.
- 17.20. Determine um emparelhamento máximo do grafo a seguir representado (utilizando o algoritmo apresentado na página 473).



- 17.21. Determine um emparelhamento perfeito de peso mínimo no grafo a seguir representado (utilizando o algoritmo da página 475).



18

Grafos de Euler e Grafos de Hamilton

A origem da teoria dos grafos é, em geral, associada ao *problema das pontes de Königsberg* (cidade da Prússia que agora se designa por Kaliningrad). Parte desta cidade localizava-se em duas ilhas do rio Pregel as quais estavam ligadas às margens e uma à outra através de sete pontes, conforme a Figura 18.1 documenta.

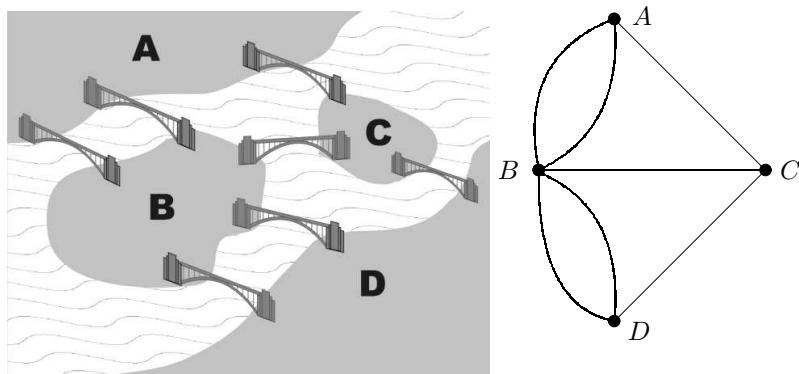


Figura 18.1: Pontes de Königsberg em 1736 e respectivo grafo.

Consta que os habitantes de Königsberg gostavam de dar passeios de modo a atravessar todas as pontes e que alguns andavam particularmente aborrecidos pelo facto de não encontrarem um trajecto (com partida e chegada a um mesmo lugar) que lhes permitisse atravessar apenas uma vez cada uma das pontes. O matemático suíço Leonhard Euler (1707-1783) ao tomar conhecimento deste problema resolveu-o (indicando a impossibilidade da existência de um tal percurso, numa memória que publicou em São Petersburgo em 1736) modelando-o pelo grafo representado na Figura 18.1. O problema dual do *problema das pontes de Königsberg*, é o de saber se um nadador poderia nadar neste mesmo rio e local de modo a passar por baixo de todas as pontes sem repetir nenhuma.

Um problema com ingredientes semelhantes ao problema das pontes de Königsberg foi formulado e resolvido (em 1857) pelo matemático irlandês Sir William Hamilton (1805-1865). Este problema que consiste em percorrer todos os vértices do dodecaedro representado na Figura 18.2, passando uma única vez em cada um, com partida e chegada no mesmo vértice, foi designado por *viagem à volta do mundo*.

Hamilton resolveu este problema observando que quando o viajante chega a um dado vértice, percorrendo uma certa aresta, tem três opções: ou (L) continua pela aresta da esquerda, ou (R) continua pela aresta da direita, ou (1) fica no vértice (o que acontece quando percorre um ciclo). A partir desta observação, definiu um conjunto de procedimentos à custa de operações com L e R , representando, por exemplo, por L^2R o procedimento de voltar duas vezes seguidas à esquerda e posteriormente à direita. Adicionalmente, considerou que duas sequências de operações têm o mesmo resultado se, a partir de um mesmo vértice, ambas conduzem a esse vértice. Este produto, embora não seja comutativo (uma vez que $LR \neq RL$) é um produto associativo (por exemplo, $(LL)R = L(LR)$). Devido ao facto das faces serem pentagonais é claro que $R^5 = L^5 = 1$ e, por outro lado, com facilidade se verifica que $LR^3L = R^2$. Com base nestas conclusões, vem

$$\begin{aligned} 1 &= R^5 = R^2R^3 = (LR^3L)R^3 = (LR^3)^2 = (L(LR^3L)R)^2 = (L^2R^3LR)^2 \\ &= (L^2(LR^3L)RLR)^2 = (L^3R^3LRLR)^2 \\ &= LLLRRRLRLRLLLRRRLRLR. \end{aligned}$$

A sequência obtida contém 20 operações e nenhuma subsequência dá resultado 1 (pelo que não determina subciclos), logo representa um ciclo de Hamilton. Note-se ainda que este ciclo se pode iniciar em qualquer dos 20 vértices do dodecaedro.

Neste capítulo, vamos fazer o estudo detalhado deste tipo de circuitos, sobre as implicações que a sua existência tem na estrutura de um grafo e sobre os principais algoritmos para a respectiva determinação, no contextos dos problemas de optimização combinatória.

18.1. Grafos de Euler

Seguem-se as definições formais de trajecto e circuito que contém todas as arestas de um grafo.

Definição 18.1 (Trajecto e circuito de Euler). *Um trajecto designa-se por trajecto de Euler se contém todas as arestas do grafo. Por sua vez, designa-se por circuito de Euler, todo o circuito que contém todas as arestas do grafo.*

Desta definição decorre que um circuito de Euler é um trajecto de Euler fechado. Também se podem definir trajectos e circuitos de Euler em grafos orientados (utilizando, nesse caso, as noções de trajecto e circuito orientado).

Definição 18.2 (Grafo euleriano e semi-euleriano). *Um grafo diz-se euleriano (ou grafo de Euler) se admite um circuito de Euler e diz-se semi-euleriano se admite um trajecto de Euler.*

É claro que todo o grafo euleriano é também semi-euleriano.

Com base nestes conceitos, o problema das pontes de Königsberg reduz-se à questão de saber se o grafo representado na Figura 18.1 é ou não euleriano. Embora, actualmente, com base no Teorema 18.1, a apresentar mais adiante, a resolução deste problema seja muito simples, Euler resolveu-o fazendo pesquisa exaustiva.

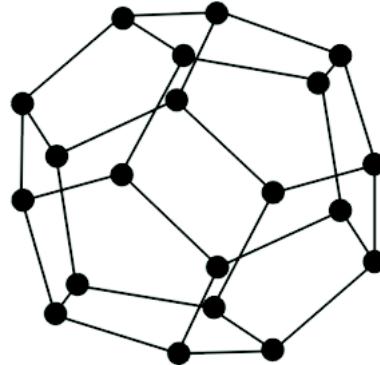


Figura 18.2: Dodecaedro (poliedro regular com 20 vértices de grau 3, 12 faces pentagonais e 30 arestas).

Exemplo 18.1. Vamos demonstrar que se um grafo G é euleriano, então todos os vértices têm grau par.

Solução. Seja G um grafo euleriano e C um dos seus circuitos. Escolha-se um vértice u para vértice inicial e final do circuito C . Percorrendo o circuito C , cada vez que passamos por um vértice $v \neq u$ percorremos duas novas arestas incidentes em v donde, uma vez que o circuito utiliza todas as arestas, o grau de v é par. Analogamente, quando passamos pelo vértice u percorremos duas arestas incidentes em u . Juntando a todas estas arestas percorridas a primeira e a última aresta incidentes em u , podemos concluir que todos os vértices de G têm grau par. \square

Exemplo 18.2. Vamos demonstrar que se $\delta(G) \geq 2$, então G ou contém um lacete ou um biciclo (duas arestas paralelas) ou um ciclo de comprimento superior a 2 (devendo observar-se que quando G é simples, resta apenas a última alternativa).

Solução. Seja G um grafo tal que $\delta(G) \geq 2$. Se G contém um lacete ou duas arestas paralelas a proposição verifica-se. Logo, vamos assumir que G não contém nenhum lacete nem arestas paralelas, ou seja, G é simples. Se G não contém nenhum ciclo, então cada componente é uma árvore e pelo Teorema 15.2 contém vértices de grau um, o que constitui uma contradição. \square

Para procurar um ciclo num digrafo \vec{G} que tenha como vértice inicial e final o vértice $v \in V(\vec{G})$, podemos utilizar o algoritmo de pesquisa em largura com pequenas modificações, conforme o pseudo-código do Algoritmo 18.1 CICLO. Deve observar-se que este algoritmo devolve o ciclo mais curto que contém v , caso um tal ciclo exista.

Algoritmo 18.1: CICLO(\vec{G}, v)

```

para  $x \in V(\vec{G})$  fazer Antecessor[ $x$ ]  $\leftarrow 0$ 
Cabeça  $\leftarrow 1$ ; Cauda  $\leftarrow 1$ ; Fila[1]  $\leftarrow v$ 
enquanto Cabeça  $\leq$  Cauda  $\wedge$  Antecessor[v] = 0
    fazer  $\begin{cases} w \leftarrow \text{Fila}[Cabeça]; Cabeça \leftarrow Cabeça + 1 \\ \text{para } x \in \Gamma(w) \\ \quad \text{fazer se } \text{Antecessor}[x] = 0 \\ \quad \quad \text{então } \begin{cases} \text{Antecessor}[x] \leftarrow w \\ Cauda \leftarrow Cauda + 1; \text{Fila}[Cauda] \leftarrow x \end{cases} \end{cases}$ 
    se Antecessor[v] = 0
        então devolver (“Não existe”)
        fazer  $\begin{cases} C \leftarrow \{v\}; w \leftarrow \text{Antecessor}[v] \\ \text{enquanto } w \neq v \\ \quad \text{fazer } C \leftarrow C \cup \{w\}; w \leftarrow \text{Antecessor}[w] \\ \text{devolver } (C) \end{cases}$ 
    senão

```

Exemplo 18.3. Seja G um grafo e C um circuito de G . Vamos demonstrar que para cada vértice $v \in V(G)$, a paridade do grau de v em G é a mesma que em $G - E(C)$.

Solução. O Exemplo 18.1 implica que no grafo $H = (V, E(C))$ todos os vértices têm grau par (tendo em conta que se trata de um grafo euleriano eventualmente com vértices isolados). Uma vez que

$$\forall_{v \in V} d_G(v) = d_{G-E(C)}(v) + d_H(v)$$

e $d_H(v)$ é par, então $d_G(v)$ e $d_{G-E(C)}(v)$ têm a mesma paridade. \square

O teorema que se segue é conhecido como teorema de Euler (dada a sua relação com a resolução do problema das sete pontes de Königsberg, obtida por Euler em 1736). A sua primeira demonstração, porém, foi publicada por Carl Hierholzer¹ em 1873.

Teorema 18.1 (Euler-Hierholzer). *Um grafo conexo não trivial é euleriano se e só se nenhum dos seus vértices tem grau ímpar.*

Demonstração. Utilizando o Exemplo 18.1, podemos concluir que se um grafo é euleriano então não tem vértices de grau ímpar. Assim, resta provar a implicação reciproca que demonstraremos por redução ao absurdo.

Suponha que G é um grafo conexo, não trivial, sem vértices de grau ímpar que não é euleriano e ainda que qualquer subgrafo de G (com menos arestas) não tem esta propriedade. Uma vez que todos os vértices têm grau par, tendo em conta o Exemplo 18.2, podemos concluir que G contém um circuito.

Seja C um circuito de G com comprimento máximo. Uma vez que G não é euleriano, C não é um circuito de Euler. Como consequência, o grafo $G - E(C)$ tem uma componente G' com $\varepsilon(G') > 0$. Do Exemplo 18.3 decorre que o grafo conexo G' não tem vértices de grau ímpar. Porém, uma vez que $\varepsilon(G') < \varepsilon(G)$, G' admite um circuito de Euler C' . Adicionalmente, dado que G é conexo, existe um vértice $v \in V(C) \cap V(C')$, o qual podemos escolher para vértice inicial (e final) do circuito $C \cup C'$ que, naturalmente, tem mais arestas do que as de C , o que constitui uma contradição (tendo em conta a maximalidade de C). \square

Exemplo 18.4. *Vamos demonstrar que um grafo conexo é semi-euleriano se e só se não tem mais do que dois vértices de grau ímpar.*

Solução. Se G contém um trajecto de Euler com vértices inicial e final coincidentes, então este trajecto é um circuito de Euler e pelo Teorema 18.1, todos os vértices têm grau par. Se os vértices inicial e final do trajecto são distintos, então ligando-os por uma nova aresta e , obtém-se um grafo $G + e$ que é euleriano e, novamente pelo Teorema 18.1, todos os vértices de $G + e$ têm grau par. Logo, no grafo G apenas os vértices extremos da aresta e têm grau ímpar.

Reciprocamente, seja G um grafo conexo com não mais do que dois vértices de grau ímpar. Uma vez que em qualquer grafo o número de vértices de grau ímpar é par, temos dois casos – o número de vértices de grau ímpar é zero ou dois. No primeiro caso (ausência de vértices de grau ímpar), o Teorema 18.1 implica que G tenha um circuito (que é também um trajecto) de Euler. No segundo caso, existindo dois vértices de grau ímpar, podemos ligar estes vértices por uma nova aresta e e o grafo obtido, $G + e$, não tem vértices de grau ímpar. Logo, aplicando o Teorema 18.1, o grafo $G + e$ tem um circuito de Euler C , donde $C - e$ é um trajecto de Euler para G . \square

Exemplo 18.5. *De entre as imagens apresentadas na Figura 18.3, quais as que podem ser decaladas sem levantar a caneta e sem repetir qualquer das linhas?*

Solução. Na linguagem da teoria dos grafos a pergunta é: quais destes grafos são semi-eulerianos.

G_1 : Como este grafo contém componentes conexas não nulas, então não é semi-euleriano, apesar de todos os vértices terem grau par.

G_2 : Trata-se de um grafo conexo onde todos os vértices têm grau par, logo existe um circuito (e um trajecto) de Euler.

G_3 : Este grafo é conexo e tem exactamente dois vértices de grau ímpar. Logo contém um trajecto de Euler (embora não contenha nenhum circuito de Euler) que se inicia num dos vértices de grau ímpar e termina no outro.

¹Carl Fridolin Bernhard Hierholzer (1840–1871) foi um matemático alemão.

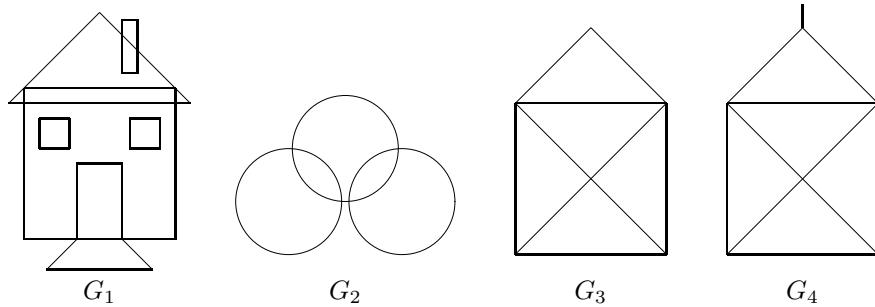


Figura 18.3: Quatro imagens consideradas no Exemplo 18.5.

G_4 : Trata-se de um grafo conexo, mas com quatro vértices de grau ímpar, logo não contém qualquer circuito nem trajecto de Euler.

Como consequência, a resposta é positiva apenas para G_2 e G_3 . \square

18.1.1 Algoritmos de Hierholzer e de Fleury

No próximo exemplo demonstra-se que um circuito de Euler (caso exista) admite uma decomposição em circuitos (ciclos, no caso de grafos simples) e é precisamente neste facto que se baseia o algoritmo de determinação de um circuito de Euler num grafo, conhecido por *algoritmo de Hierholzer*.

Exemplo 18.6. Vamos demonstrar que se um grafo G não tem vértices de grau ímpar então o conjunto das suas arestas pode partitarse em subconjuntos que determinam circuitos (ciclos, se G é simples) C_1, C_2, \dots, C_m , ou seja, cada um destes circuitos é disjunto nas arestas e

$$E(G) = E(C_1) \cup E(C_2) \cup \dots \cup E(C_m).$$

Solução. Vamos fazer a prova por indução sobre o número das arestas ε , tendo em conta que se $\varepsilon = 1$ e o grafo G não tem vértices de grau ímpar, então a única aresta é um lacete e o resultado verifica-se.

Suponhamos que o resultado é verdadeiro para todos os grafos com menos do que ε arestas e seja G um grafo com ε arestas e sem vértices de grau ímpar. Observe que os vértices isolados não têm qualquer importância para o resultado que se pretende provar, pelo que, sem perda de generalidade, podemos assumir que G não tem vértices isolados. Neste caso, o menor grau é não inferior a 2. Do Exemplo 18.2 decorre que G contém um circuito C . Uma vez que o grafo $G^* = G - E(C)$, tem menos do que ε arestas e, pela Exemplo 18.3, G^* não tem vértices de grau ímpar então, por hipótese de indução, existe um número, por exemplo $m - 1$, de circuitos disjuntos nas arestas, C_1, C_2, \dots, C_{m-1} , tais que

$$E(G^*) = \bigcup_{i=1}^{m-1} E(C_i).$$

Então, denotando por C_m o ciclo C (ou seja, $C_m = C$), podemos concluir que $E(G) = \bigcup_{i=1}^m E(C_i)$. \square

Descrição do algoritmo de Hierholzer.

Dados de entrada: Grafo conexo G .

Resultados de saída: Circuito de Euler \mathcal{E} , caso exista.

1. Escolher um vértice $v \in V(G)$ e determinar um circuito (ciclo) \mathcal{E} que se inicie e termine em v . Fazer $G \leftarrow G - E(\mathcal{E})$.

2. Repetir (a) ... (d) até que G seja um grafo nulo (sem arestas).
 - (a) Determinar $v \in V(\mathcal{E})$ com pelo menos uma aresta de G incidente.
 - (b) Determinar um circuito (ciclo) C que se inicie e termine em v , caso exista; caso contrário PARAR - o grafo não é euleriano.
 - (c) Juntar os circuitos \mathcal{E} e C e denotar o circuito resultante por \mathcal{E} .
 - (d) Fazer $G \leftarrow G - E(C)$.
 3. Devolver o circuito de Euler \mathcal{E} .
-
-

Segue-se o pseudocódigo do Algoritmo 18.2 HIERHOLZER. Neste pseudocódigo utiliza-se a notação $\mathcal{E} + C$ para a operação de junção dos circuitos \mathcal{E} e C com um vértice comum v .

Algoritmo 18.2: HIERHOLZER(G)

```

 $v \leftarrow$  elemento arbitrário de  $V(G)$ 
 $\mathcal{E} \leftarrow \text{CICLO}(G, v); G \leftarrow G - E(\mathcal{E})$ 
enquanto  $|E(G)| > 0$ 
  fazer
     $v \leftarrow 0$ 
    para  $w \in V(\mathcal{E})$ 
      fazer se  $N_G(w) \neq \emptyset$  então  $v \leftarrow w$ ; interromper
      se  $v = 0$  então devolver ("O grafo não é euleriano")
       $C \leftarrow \text{CICLO}(G, v)$ 
       $\mathcal{E} \leftarrow \mathcal{E} + C; G \leftarrow G - E(C)$ 
  devolver ( $\mathcal{E}$ )

```

Um outro algoritmo igualmente eficiente para a determinação de circuitos de Euler é o *algoritmo de Fleury* publicado em 1883, cuja estratégia consiste em juntar ao trajecto corrente uma nova aresta que se possível não seja uma ponte. Segue-se a descrição deste algoritmo.

Descrição de algoritmo de Fleury.

Dados de entrada: Grafo conexo G .

Resultados de saída: Circuito de Euler \mathcal{E} , caso exista.

1. Escolher $v \in V(G)$ e fazer $NArestas \leftarrow 0$.
 2. Repetir (a) ... (d) até $E = \emptyset$.
 - (a) Se $N_G(v) = \emptyset$, então PARAR – o grafo não é euleriano.
 - (b) Escolher uma aresta $e = vw$ que, se possível, não seja uma ponte.
 - (c) Adicionar e ao circuito:
 $NArestas \leftarrow NArestas + 1, \mathcal{E}[NArestas] \leftarrow e$.
 - (d) Actualizar as variáveis: $E \leftarrow E \setminus \{e\}, v \leftarrow w$.
 3. Devolver o circuito de Euler \mathcal{E} .
-

Este algoritmo é representado, em pseudocódigo, pelo Algoritmo 18.3 FLEURY. Para verificar se uma aresta é uma ponte utiliza-se Algoritmo 14.1 DISTBFS.

Algoritmo 18.3: FLEURY(G)

```

 $v \leftarrow$  vértice arbitrário de  $V(G)$ 
 $N\text{arestas} \leftarrow 0$ 
enquanto  $|E(G)| > 0$ 
    se  $|N_G(v)| = 0$  então devolver (“O grafo não é euleriano”)
     $v \leftarrow 0$ 
    para  $w \in N_G(v)$ 
        fazer se DISTBFS( $G - vw, v, w) < \infty$ 
        então  $v \leftarrow w$ ; interromper
    se  $v = 0$  então  $v \leftarrow$  vértice arbitrário de  $N_G(v)$ 
     $e \leftarrow$  aresta arbitrária  $vw$ ;  $G \leftarrow G - e$ 
     $N\text{arestas} \leftarrow N\text{arestas} + 1$ ;  $\mathcal{E}[N\text{arestas}] \leftarrow e$ 
devolver ( $\mathcal{E}$ )

```

É claro que o algoritmo de Fleury determina um trajecto. O teorema que se segue mostra que, se possível, este trajecto é um circuito de Euler.

Teorema 18.2. Se G é um grafo euleriano então o trajecto de G determinado pelo algoritmo de Fleury é um circuito de Euler.

Demonstração. Seja G um grafo euleriano e seja

$$\mathcal{E} = v_0e_1v_1 \dots e_nv_n$$

o trajecto de G determinado pelo algoritmo de Fleury.

Uma vez que v_n tem grau zero em $G_n = G - E(\mathcal{E})$ e todos vértices em G têm grau par, $v_n = v_0$, ou seja, \mathcal{E} é um circuito. Vamos mostrar, por redução ao absurdo, que o circuito \mathcal{E} é euleriano. Assim, suponha que \mathcal{E} não é um circuito de Euler e seja S o conjunto de vértices de G com grau positivo em G_n . Observe que, por definição, o conjunto S é não vazio, $S \cap V(\mathcal{E}) \neq \emptyset$ (uma vez que G é euleriano) e $v_n = v_0 \in S^c = V(G) \setminus S$. Seja m o maior inteiro tal que $v_m \in S$ e $v_{m+1} \in S^c$. Uma vez que \mathcal{E} termina em S^c , então e_{m+1} é a única aresta do corte $\partial(S, S^c)$ no grafo $G_m = G - \{e_1, \dots, e_{m-1}\}$, ou seja, é uma ponte neste grafo (ver Figura 18.4).

Seja e uma aresta arbitrária distinta de e_{m+1} , incidente em v_m no grafo G_n (note-se que tal aresta existe, tendo em conta a definição de S). É claro que e também é uma ponte em G_m (uma vez que o algoritmo escolhe uma ponte se e só se não pode escolher uma aresta que não seja uma ponte) e, como consequência, e é uma ponte em $G_m[S]$. Mas $G_m[S] = G_n[S]$ e, dado que todos os vértices de $G_n[S]$ têm grau par, o grafo $G_m[S]$ não pode ter uma ponte, o que constitui uma contradição. \square

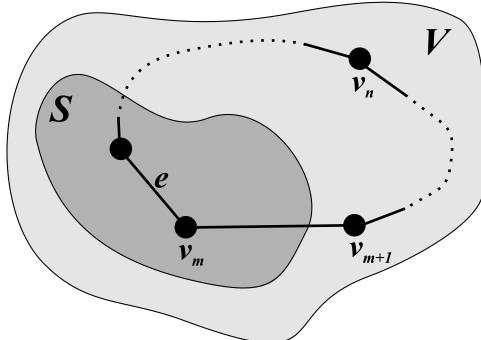


Figura 18.4: Ilustração da demonstração do Teorema 18.4.

18.1.2 Problema do carteiro chinês

Neste problema, um carteiro levanta a correspondência numa estação de correios, faz a respectiva distribuição e regressa ao ponto de partida. Assumimos que o carteiro deve percorrer todas as ruas da respectiva área de distribuição pelo menos uma vez. Sujeito a estas condições, pretendemos determinar o percurso que deve fazer o carteiro de modo a andar o menos possível. A designação de *problema do*

carteiro chinês deve-se ao facto de ter sido primeiramente formulado pelo matemático chinês Mei-Ko Kwan em 1962.

Podemos formular este problema na linguagem dos grafos com pesos (não negativos) nas arestas, da seguinte forma: considere-se o grafo correspondente à rede de ruas da área de distribuição do carteiro e associe-se a cada aresta o peso igual ao comprimento da rua a que se refere. Neste grafo, define-se o peso do passeio $v_0e_1, v_1e_2, \dots, e_nv_0$ como sendo a soma dos pesos de suas arestas, ou seja, $\sum_{i=1}^n w(e_i)$. Assim, o objectivo é encontrar um passeio fechado que contenha todas as arestas e tenha peso mínimo, o qual será designado por *passeio óptimo para o carteiro chinês*. É claro que se o grafo considerado é de Euler, então um passeio é óptimo para o carteiro chinês se e só se é um circuito de Euler e, neste caso, o problema resolve-se por aplicação do algoritmo de Hierholzer ou de Fleury. No caso contrário, porém, o problema é mais complicado, uma vez que o carteiro terá de passar mais do que uma vez por algumas ruas e temos de escolher quais. Para resolver este problema, vamos introduzir a operação de duplicação de arestas.

Definição 18.3 (Duplicação de uma aresta). *Dado um grafo G e uma função de pesos nas arestas $w : E(G) \rightarrow \mathbb{R}$, a duplicação da aresta $e \in E(G)$, com peso $w(e)$, consiste em adicionar ao grafo uma nova aresta com os mesmos vértices extremos de e e o mesmo peso (ou seja, consiste em criar uma aresta paralela a e com o mesmo peso).*

Utilizando a operação de duplicação de arestas, o problema do carteiro chinês pode reformular-se como a seguir se indica.

Seja G um grafo com pesos não negativos nas arestas.

- (i) Com recurso à duplicação de arestas, determinar um supergrafo G^* do grafo G que seja euleriano e tal que o somatório

$$\sum_{e \in E(G^*) - E(G)} w(e)$$

tenha o menor valor possível.

- (ii) Determinar um circuito de Euler para o grafo G^* .

Note-se que a resolução de (ii) não tem qualquer dificuldade. Com efeito, basta utilizar um dos algoritmos anteriormente apresentados, o algoritmo de Hierholzer ou de Fleury. Edmonds e Johnson, em 1973, publicaram um algoritmo eficiente para a resolução de (i).

Seja V^- o conjunto de vértices de grau ímpar num grafo G (é claro que $|V^-|$ é par) e seja M o conjunto de arestas que definem caminhos entre vértices de V^- . Então, denotando por $G^+(M)$ o grafo obtido a partir de G por duplicação das arestas contidos em M , temos o seguinte resultado.

Teorema 18.3. *Dado um grafo G com pesos nas arestas, existe um conjunto de caminhos M em G que emparelham os vértices de grau ímpar tal que o peso de M é mínimo e o circuito de Euler do grafo $G^+(M)$ é uma solução óptima para o problema do carteiro chinês.*

Demonstração. Observe-se que as arestas duplicadas (ou seja, as arestas de M) não contêm nenhum ciclo. Caso contrário, tendo em conta o Exemplo 18.3 e o teorema de Euler-Hierholzer, eliminadas as arestas deste ciclo, o grafo teria um circuito de Euler com menor peso.

Seja v_1 um vértice de grau ímpar no grafo G . Então, qualquer passeio fechado óptimo \mathcal{C} passa por uma das arestas incidentes em v_1 mais do que uma vez. Seja $e_1 = v_1v_2$ a aresta repetida durante a construção do passeio óptimo \mathcal{C} . Se v_2 tem grau ímpar em G , então $v_1e_1v_2$ é um caminho de M que liga vértices de grau ímpar em G . Se v_2 tem grau par em G entao, com a duplicação de e_1 , v_2 passa a ter grau ímpar e, tal como anteriormente, qualquer passeio fechado óptimo passa por uma das arestas incidentes em v_2 mais do que uma vez. Este procedimento repete-se até que todos os vértices de grau ímpar estejam ligados por passeios formados pelas arestas repetidas pertencentes a M . Acrescentando

estas arestas ao grafo original obtemos um novo grafo onde todos os vértices têm grau par. Assim, admitindo que M é o conjunto de arestas que definem os caminhos entre os pares de vértices de grau ímpar que no seu conjunto têm peso mínimo, obtém-se o pretendido. \square

No caso particular de um grafo G com exactamente dois vértices u e v de grau ímpar, a solução de (i) é equivalente à determinação de um caminho mais curto e à duplicação das arestas desse caminho.

Exemplo 18.7. Vamos resolver o problema do carteiro chinês para o grafo definido pela seguinte matriz de pesos:

$$W(G) = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\ v_1 & \infty & 2 & \infty & \infty & \infty & \infty & 2 \\ v_2 & 2 & \infty & 3 & \infty & \infty & \infty & 5 & 4 \\ v_3 & \infty & 3 & \infty & 8 & \infty & 6 & 3 & \infty \\ v_4 & \infty & \infty & 8 & \infty & 5 & 2 & \infty & \infty \\ v_5 & \infty & \infty & \infty & 5 & \infty & 7 & \infty & \infty \\ v_6 & \infty & \infty & 6 & 2 & 7 & \infty & 9 & \infty \\ v_7 & \infty & 5 & 3 & \infty & \infty & 9 & \infty & 2 \\ v_8 & 2 & 4 & \infty & \infty & \infty & \infty & 2 & \infty \end{pmatrix}.$$

Solução. Tendo em conta a Figura 18.5, onde se representa o grafo que modela este problema, é fácil verificar que apenas os vértices v_4 e v_8 têm grau ímpar.

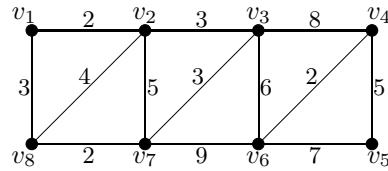


Figura 18.5: Grafo que modela o problema do carteiro chinês do Exemplo 18.7.

Determinado o caminho mais curto entre eles, com recurso (por exemplo) ao algoritmo de Dijkstra,

$$\text{DIJKSTRA}(G = (\{v_1, \dots, v_8\}, W(G)), v_4, v_8),$$

podemos concluir que o comprimento de um caminho (v_4, v_8) mais curto é 13 e um destes caminhos é $v_8v_7v_3v_4$ (o outro caminho com igual peso é $v_8v_7v_6v_4$).

Duplicando as arestas deste caminho, obtemos o grafo euleriano representado na Figura 18.6.

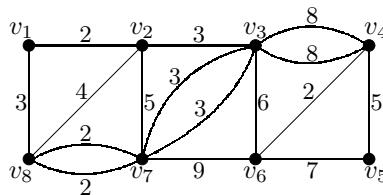


Figura 18.6: Grafo euleriano obtido a partir do grafo representado na Figura 18.5 por duplicação das arestas de um caminho mais curto entre v_4 e v_8 .

A soma dos pesos das arestas de um circuito de Euler deste grafo é igual a 72 e um destes circuitos é, por exemplo,

$$v_1v_2v_3v_4v_3v_6v_4v_5v_6v_7v_3v_7v_8v_2v_7v_8v_1,$$

sendo claro que este circuito determina um passeio óptimo para o carteiro chinês. \square

Descrição de algoritmo de Edmonds e Johnson.

Dados de entrada: Um grafo G com pesos das arestas.

Resultados de saída: Circuito de Euler do grafo euleriano G^* tal que $V(G^*) = V(G)$, $E(G) \subseteq E(G^*)$ e o conjunto de arestas $E(G^*) \setminus E(G)$ tem peso mínimo.

1. Utilizando um algoritmo de determinação de caminhos mais curtos, determinar a matriz $D(G) = (d_{ij})$ de dimensão $|V^-| \times |V^-|$ tal que d_{ij} é o peso de um caminho de peso mínimo entre os vértices v_i e v_j (para $v_i, v_j \in V^-$).
 2. Determinar um emparelhamento com peso mínimo no grafo completo com conjunto de vértices V^- e peso em cada uma das arestas $v_i v_j$ igual a d_{ij} .
 3. Sendo M o conjunto das arestas que correspondem aos caminhos de peso mínimo definidos pelo emparelhamento óptimo, duplicar as arestas de M para obter o grafo $G^+(M)$.
 4. Determinar circuito de Euler no grafo $G^* = G^+(M)$.
-

Exemplo 18.8. Vamos resolver o problema do carteiro chinês para o grafo definido pela seguinte matriz de pesos:

$$W(G) = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\ v_1 & \infty & 2 & \infty & \infty & \infty & \infty & 2 \\ v_2 & 2 & \infty & 3 & \infty & \infty & 2 & 5 \\ v_3 & \infty & 3 & \infty & 8 & \infty & 6 & 3 \\ v_4 & \infty & \infty & 8 & \infty & 5 & 2 & \infty \\ v_5 & \infty & \infty & \infty & 5 & \infty & 7 & \infty \\ v_6 & \infty & 2 & 6 & 2 & 7 & \infty & 9 \\ v_7 & \infty & 5 & 3 & \infty & \infty & 9 & \infty \\ v_8 & 2 & 4 & \infty & \infty & \infty & 2 & \infty \end{pmatrix}.$$

Solução. Tendo em conta a Figura 18.7 que representa o grafo que modela este problema, é fácil concluir que v_2, v_4, v_6 e v_8 são os vértices de grau ímpar.

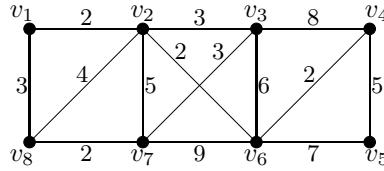


Figura 18.7: Grafo que modela o problema do carteiro chinês do Exemplo 18.8.

Na Figura 18.8 apresenta-se uma tabela com os pesos e os caminhos de peso mínimo entre os diferentes pares de vértices de grau ímpar, bem como o grafo completo com este vértices e estes pesos nas arestas.

Determinando o emparelhamento de peso mínimo no grafo completo representado na Figura 18.8, obtém-se as arestas v_2v_8 e v_4v_6 . Como consequência, de acordo com a tabela da Figura 18.8, o conjunto $M = \{v_2v_8, v_4v_6\}$ tem peso 6 e, duplicando as arestas de M , obtém-se o grafo representado na Figura 18.9.

Uma vez que a soma dos pesos das arestas do circuito de Euler deste grafo é igual a 67 e um destes circuitos é

$$v_1 v_2 v_3 v_4 v_3 v_6 v_4 v_5 v_6 v_4 v_6 v_3 v_7 v_6 v_2 v_7 v_8 v_2 v_8 v_1 ,$$

Extremos de caminho	Peso	Caminho
v_2 e v_4	4	$v_2v_6v_4$
v_2 e v_6	2	v_2v_6
v_2 e v_8	4	v_2v_8
v_4 e v_6	2	v_4v_6
v_4 e v_8	8	$v_4v_6v_2v_8$
v_6 e v_8	6	$v_6v_2v_8$

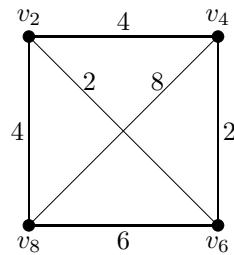


Figura 18.8: Determinação do grafo completo com pesos não negativos nas arestas, correspondente ao conjunto de vértices V^- do Exemplo 18.8.

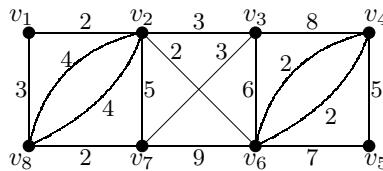


Figura 18.9: Grafo euleriano obtido a partir o grafo representado na Figura 18.7, por duplicação das arestas do conjunto $M = \{v_2v_8, v_4v_6\}$.

podemos concluir que é também um passeio óptimo para o carteiro chinês.

Observe que, embora a área de distribuição do carteiro tenha mais uma rua do que no Exemplo 18.8, o passeio óptimo tem menos peso! \square

18.2. Grafos de Hamilton

Segue-se a definição formal de caminho e ciclo que passa por todos os vértices de um grafo.

Definição 18.4 (Caminho e ciclo de Hamilton). *Um caminho que contém todos os vértices de um grafo diz-se um caminho de Hamilton (ou hamiltoniano). Por sua vez, um ciclo que contém todos os vértices de um grafo, designa-se por ciclo de Hamilton (ou hamiltoniano).*

Também se podem definir caminhos e ciclos de Hamilton para grafos orientados (utilizando, nesse caso, a noção de caminho e ciclo orientado).

Como exemplo, para além do ciclo de Hamilton que é possível obter no grafo definido pelo dodecaedro (anteriormente referido), considere-se um tabuleiro de xadrez e associe-se a cada um dos seus 64 quadrados um vértice de um grafo G cujas arestas ligam os vértices correspondentes a quadrados entre os quais é possível efectuar um movimento de cavalo. Neste grafo existem ciclos de Hamilton que correspondem a movimentos sucessivos de um cavalo de forma a que todos os quadrados (pretos e brancos) sejam visitados uma única vez. Na figura da página 327 representa-se um dos ciclos de Hamilton possíveis para o referido grafo.

Definição 18.5 (Grafo hamiltoniano e grafo semi-hamiltoniano). *Um grafo que admite um ciclo de Hamilton designa-se por grafo hamiltoniano (ou grafo de Hamilton). Um grafo que admite um caminho de Hamilton diz-se um grafo semi-hamiltoniano.*

Contrariamente ao que acontece no caso dos circuitos eulerianos não se conhece nenhuma condição necessária e suficiente computacionalmente efectiva para a existência de um ciclo de Hamilton. No entanto, podem apresentar-se, separadamente, condições necessárias e condições suficientes. Recordando

que o número de componentes conexas de um grafo H se denota por $\text{cc}(H)$, temos a seguinte condição necessária para um grafo ser hamiltoniano.

Teorema 18.4. *Se um grafo G é hamiltoniano, então qualquer que seja o subconjunto não vazio de vértices $S \subseteq V(G)$,*

$$\text{cc}(G - S) \leq |S|. \quad (18.1)$$

Demonstração. Seja \mathcal{C} um ciclo de Hamilton em G . Então, para cada subconjunto não vazio $S \subseteq V(G)$

$$\text{cc}(\mathcal{C} - S) \leq |S|,$$

uma vez que, eliminando k vértices de um ciclo se obtém k partes desse ciclo. Finalmente, dado que $\mathcal{C} - S$ é um subgrafo abrangente de $G - S$, vem

$$\text{cc}(G - S) \leq \text{cc}(\mathcal{C} - S) \leq |S|. \quad \square$$

Este teorema pode ser utilizado apenas para demonstrar que alguns grafos não são hamiltonianos. Com efeito, existem grafos não hamiltonianos, como é o caso do grafo de Petersen (ver Figura 14.4, na página 385), para os quais qualquer que seja o subconjunto de vértices S se verifica a desigualdade (18.1), o que significa que a validade desta desigualdade para todo o subconjunto de vértices S não é uma condição suficiente para o respectivo grafo ser hamiltoniano.

Teorema 18.5. *Seja G um grafo simples e sejam $u, v \in V(G)$ dois vértices não adjacentes tais que*

$$d_G(u) + d_G(v) \geq \nu(G).$$

Então, o grafo G é hamiltoniano se e só se $G + uv$ é hamiltoniano.

Demonstração. Observe-se que adicionando arestas a um grafo hamiltoniano esse grafo mantém-se hamiltoniano. Logo, se G é hamiltoniano, então $G + uv$ é também hamiltoniano. Reciprocamente, suponha que existe um grafo G que satisfaz hipótese de teorema e $G + uv$ é hamiltoniano, mas G não é hamiltoniano. Então qualquer ciclo de Hamilton de $G + uv$ contém a aresta uv . Como consequência, em G existe um caminho de Hamilton $u = v_1, v_2, \dots, v_\nu = v$. Note-se que não existe nenhum índice i tal que

$$uv_{i+1} \in E(G) \quad \text{e} \quad v_i v \in E(G),$$

caso contrário existiria em G o ciclo de Hamilton

$$v_1 v_2, \dots, v_i, v_\nu, v_{\nu-1}, \dots, v_{i+1}, v_1,$$

(ver Figura 18.10). Logo, sendo $k = d_G(u)$ e $N_G(u) = \{v_{j_1}, \dots, v_{j_k}\}$, não existe um índice j_i tal que

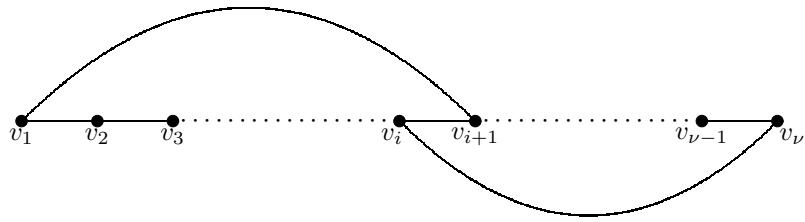


Figura 18.10: Ciclo de Hamilton $v_1 v_2, \dots, v_i, v_\nu, v_{\nu-1}, \dots, v_{i+1}, v_1$.

$v_{j_i-1} \in N_G(v)$. Consequentemente, existem $d_G(u) + 1$ vértices que não são adjacentes a v (contando com o próprio vértice v), ou seja, $d_G(v) \leq \nu(G) - (d_G(u) + 1)$, o que é equivalente a $d_G(v) + d_G(u) \leq \nu(G) - 1$, contrariando a hipótese. \square

Como corolário imediato podemos obter um resultado clássico publicado por Ore em 1960².

Corolário 18.6 (Teorema de Ore). *Seja G um grafo simples com $\nu(G) \geq 3$. Se*

$$\forall_{u,v \in V(G)} d_G(u) + d_G(v) \geq \nu(G),$$

então G é hamiltoniano.

Demonstração. Vamos fazer esta prova por redução ao absurdo. Suponhamos que o teorema é falso e seja G um grafo não hamiltoniano com $\nu(G) \geq 3$, satisfazendo a hipótese do teorema. Acrescentando tantas arestas quantas as necessárias, podemos supor que G é um grafo maximal com esta propriedade, significando isso que, se acrescentarmos mais uma aresta, o grafo passa a ser hamiltoniano. Como G não é completo (caso contrário seria hamiltoniano) existe um par de vértices não adjacentes u e v . Uma vez que $G + uv$ é hamiltoniano, utilizando o Teorema 18.5, concluímos que G também é hamiltoniano, o que constitui uma contradição. \square

Um outro corolário imediato é o resultado clássico publicado por Dirac³ em 1952.

Corolário 18.7 (Teorema de Dirac). *Se G é um grafo simples tal que $\nu(G) \geq 3$ e $\delta(G) \geq \frac{1}{2}\nu(G)$, então G é hamiltoniano.*

Demonstração. Uma vez que para cada vértice $v \in V(G)$ se obtém $d_G(v) \geq \frac{1}{2}\nu(G)$, então

$$\forall_{u,v \in V(G)} d_G(u) + d_G(v) \geq \nu(G).$$

Logo, pelo Corolário 18.6, G é hamiltoniano. \square

Exemplo 18.9. *Vamos demonstrar que os grafos apresentados na Figura 18.11 são hamiltonianos.*



Figura 18.11: Exemplos de grafos hamiltonianos.

Solução. Uma vez que para o grafo G se verifica

$$\forall_{u,v \in V(G)} d_G(u) + d_G(v) \geq 5,$$

pelo Corolário 18.6, podemos concluir que G é hamiltoniano. Analogamente, uma vez que para o grafo H se verifica

$$\forall_{v \in V(H)} d_H(v) \geq \frac{7}{2},$$

então, pelo teorema de Dirac, o grafo H é hamiltoniano. \square

²Øystein Ore (1899–1968), matemático norueguês que trabalhou em teoria dos grafos, teoria dos anéis e teoria dos corpos.

³Gabriel Andrew Dirac (1925–1984), matemático (que foi professor na Dinamarca), filho da mulher do físico teórico e fundador da mecânica quântica (prêmio Nobel da Física em 1933) Paul Dirac.

Exemplo 18.10. Seja $C(G)$ o grafo que se obtém de G , ligando sucessivamente por uma aresta os pares de vértices não adjacentes cuja soma dos graus é não inferior a $\nu = \nu(G)$, enquanto tais pares de vértices existirem. Vamos demonstrar que $C(G)$ fica bem definido.

Solução. Sejam G_1 e G_2 os grafos obtidos por adição (respeitando o critério definido) das sequências de arestas e_1, \dots, e_m e f_1, \dots, f_n , respectivamente. Suponhamos que $\{e_1, \dots, e_m\} \neq \{f_1, \dots, f_n\}$. Seja $e_{k+1} = uv$ a primeira aresta da sequência e_1, \dots, e_m tal que $e_{k+1} \notin \{f_1, \dots, f_n\}$ e seja $H = G \cup \{e_1, e_2, \dots, e_k\}$. O modo como se escolhe $e_{k+1} = uv$, implica que os vértices u e v sejam não adjacentes e a que soma dos respectivos graus em H seja não inferior a ν . Porém, uma vez que H é também um subgrafo de G_2 a soma dos graus de u e v é também não inferior a ν em G_2 . Logo, a aresta $e_{k+1} = uv$ faz parte da sequência f_1, f_2, \dots, f_n , o que é contraditório. Analogamente se prova que todas as arestas da sequência f_1, f_2, \dots, f_n , pertencem ao conjunto $\{e_1, \dots, e_m\}$. Logo, $G_1 = G_2$. \square

Deve observar-se que se um grafo G verifica a hipótese do teorema de Dirac, então $C(G)$ é o grafo completo $K_{\nu(G)}$.

Teorema 18.8. Um grafo simples G é hamiltoniano se e só se $C(G)$ é hamiltoniano.

Demonstração. Seja e_1, e_2, \dots, e_n uma sequência de arestas adicionadas a G para obter $C(G)$. Seja $G_0 = G$ e seja $G_i = G_{i-1} + e_i$ para $i = 1, \dots, n$. O Teorema 18.5 implica que, para todo $i \in \{1, \dots, n\}$, o grafo G_i é hamiltoniano se e só se G_{i-1} é hamiltoniano. Como consequência, G_n é hamiltoniano se e só se G_0 é hamiltoniano. \square

Note-se que, para $n \geq 3$, o grafo completo K_n é hamiltoniano, concluindo-se que se $C(G)$ é um grafo completo, então G é hamiltoniano (para $\nu(G) \geq 3$).

Definição 18.6 (Grafo linha de um grafo). Dado um grafo G , designa-se por grafo linha de G e denota-se por $L(G)$ o grafo que se obtém de G considerando $E(G)$ como conjunto dos vértices e onde dois vértices $e_1, e_2 \in E(G)$ são adjacentes se e só se as arestas e_1 e e_2 são incidentes num mesmo vértice de G .

É claro que a um circuito de Euler num grafo G corresponde um ciclo de Hamilton em $L(G)$. Consequentemente, G é euleriano se e só se $L(G)$ é hamiltoniano. No exemplo a seguir, provam-se algumas propriedades adicionais dos grafos linha.

Exemplo 18.11. Vamos demonstrar que

- (a) o grafo linha de um grafo de Euler é um grafo euleriano,
- (b) o grafo linha de um grafo de Hamilton é um grafo hamiltoniano,
- (c) o grafo linha de um grafo de Hamilton não é necessariamente euleriano.

Solução.

- (a) Observe-se que todo o caminho P em G se transforma num caminho em $L(G)$ entre a primeira e a última arestas de P . Como consequência, se G é conexo, então $L(G)$ também é conexo.

Logo, basta mostrar que se em G todos os vértices têm grau par, então em $L(G)$ acontece o mesmo. Seja $e = uv$ em vértice de $L(G)$ (ou seja, e é uma aresta de G), então

$$d_{L(G)}(e) = d_G(u) + d_G(v) - 2,$$

isto é, o grau de e em $L(G)$ é par.

- (b) Se G é um grafo de Hamilton, então podemos desenhá-lo como um polígono que contém todos os vértices de grafo, possivelmente com algumas diagonais. Por sua vez, no grafo linha de G , o polígono transforma-se num polígono, porém, geralmente, este polígono não é um ciclo de Hamilton em $L(G)$ – podendo existir outros vértices que correspondem às diagonais do polígono em G .

Suponha que, sendo v o vértice extremo comum a duas arestas sucessivas e_1 e e_2 do polígono de G , existem arestas $e_{i_1}, e_{i_2}, \dots, e_{i_m}$ incidentes em v . Tal significa que $L(G)$ tem um subgrafo completo induzido pelos vértices $e_{i_1}, e_{i_2}, \dots, e_{i_m}$ e que todos estes vértices são adjacentes aos vértices e_1 e e_2 . Logo, percorrendo os vértices de $L(G)$, pela sequência correspondente à sequência de arestas do polígono de G , mas fazendo desvios entre dois destes vértices consecutivos de modo a percorrer todos os subgrafos completos que vão aparecendo (e são induzidos por vértices ainda não percorridos), obtém-se um ciclo de Hamilton em $L(G)$.

- (c) Como exemplo de um tal grafo, podemos considerar $G = K_4 - e$ (ver Figura 18.12). O grafo linha $L(G)$ tem dois vértices de grau ímpar e, como consequência, não é euleriano. \square

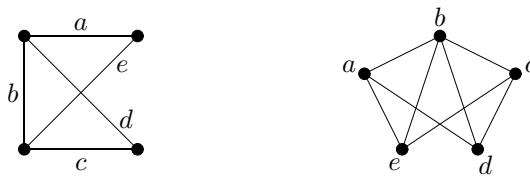


Figura 18.12: Os grafos $K_4 - e$ e $L(K_4 - e)$.

18.2.1 Código de Gray

Segue-se uma aplicação directa, muito simples, dos ciclos de Hamilton. Certos instrumentos contadores representam números reais por sequências de dígitos de comprimento fixo (como, por exemplo, os conta-quilómetros dos automóveis). Com estes dispositivos, na maioria dos casos, os números vão variando com a modificação de um único dígito. Porém, em certas situações, a mudança do número obriga à troca de vários dígitos, como no caso da passagem de 189.999 para 190.000, operação que provoca alguns problemas mecânicos de difícil resolução. Nestas passagens, qualquer avaria (mesmo que pontual) no dispositivo mecânico pode provocar erros consideráveis. Para evitar estes erros, podemos definir uma sequência de números de tal forma que de um número para outro apenas se troca um dígito. Com estas sequências, uma avaria pontual (ausência atempada de resposta do dispositivo mecânico) apenas provoca o erro de uma unidade. No caso destas sequências se referirem a representações binárias de números, elas são conhecidas por códigos de Gray. Um grafo, cujos vértices são os n -uplos $(x_{n-1}, x_{n-2}, \dots, x_1, x_0)$, de zeros e uns, tais que dois vértices são adjacentes se diferem num único dígito designa-se, usualmente, por n -cubo e denota-se por Q_n (deve observar-se que, neste n -cubo, existem 2^n vértices, cada um dos quais associado a um número, entre 0 e $2^n - 1$, representado numa base binária). Na Figura 12.11 (página 342) apresentam-se os k -cubos, com $k = 0, 1, 2, 3$.

Um código de Gray corresponde a um ciclo de Hamilton no n -cubo Q_n e a existência de um tal ciclo fica garantida pelo teorema que se segue.

Teorema 18.9. *Se $n \geq 2$, então o grafo Q_n é hamiltoniano.*

Demonstração. A prova será feita por indução sobre n , tendo em conta que, para $n = 2$, Q_2 é um ciclo com 4 arestas, pelo que o resultado é verdadeiro (uma vez que se pode obter o ciclo de Hamilton $(00, 01, 11, 10, 00)$).

Supondo que existe o ciclo de Hamilton em Q_n , $(v_0, v_1, \dots, v_{2^n-2}, v_{2^n-1}, v_0)$, é claro que $(0v_0, 0v_1, \dots, 0v_{2^n-2}, 0v_{2^n-1}, 1v_{2^n-1}, 1v2^n - 2, \dots, 1v_1, 1v_0, 0v_0)$ é um ciclo de Hamilton em Q_{n+1} . \square

Na prática, para a codificação e descodificação dos números, é necessário conhecer a posição de cada vértice no ciclo de Hamilton que define o código de Gray. Um modo fácil de o conseguir, consiste em construir o código de Gray de comprimento 2^{n+1} , a partir do código de Gray de comprimento 2^n , tal como se procedeu na demonstração do Teorema 18.9, primeiro percorrendo a sequência de vértices do caminho de Hamilton de Q_n , entre 0 e $2^n - 1$, colocando um 0 na posição mais à esquerda e, posteriormente, percorrendo o mesmo caminho pela ordem inversa, colocando 1 nessa mesma posição. O teorema a seguir indica um modo sistemática para a obtenção das diferentes representações do código de Gray com cadeias binárias de n dígitos.

Teorema 18.10. *Considerem-se os vértices do ciclo de Hamilton de Q_n (construído tal como anteriormente se indicou), etiquetados com $0, 1, 2, 3, \dots, 2^n - 2, 2^n - 1$, segundo a ordem pela qual são visitados. Se 2^k (com $0 \leq k \leq n - 1$) é a maior potência de 2 que divide $p \in \{1, 2, \dots, 2^n - 1\}$, então no p -ésimo número binário representado, α_p , o dígito que se modifica (em relação ao vértice anterior, i.e., em relação ao vértice de ordem $p - 1$) é o k -ésimo a partir da direita.*

Demonstração. Esta prova vai ser feita por indução sobre n , tendo em conta que para $n = 2$ se obtém a sequência representada na tabela a seguir.

p	α_p	k	2^k
0	00		
1	01	0	1
2	11	1	2
3	10	0	1

Supondo que a afirmação anterior é verdadeira para $2 \leq n \leq N$, vamos analisar o comportamento da sequência de números binários para $n = N + 1$.

Para os primeiros p números representados, com $0 \leq p \leq 2^N - 1$, vem

$$\alpha_p = 0a_{N-1}a_{N-2}\dots a_1a_0.$$

Logo, por hipótese de indução, se 2^k é a maior potência de 2 que divide p , então, na passagem de α_{p-1} para α_p é o k -ésimo dígito binário (a contar da direita) que se modifica. Para $p = 2^N$, o dígito que se modifica é o N -ésimo, pelo que a afirmação continua válida. Por sua vez, para $p = 2^N + \tau$, com $0 \leq \tau \leq 2^N - 1$, verifica-se que α_p coincide com $\alpha_{p-2\tau-1}$ em todos os dígitos à excepção do dígito mais à esquerda (que para α_p tem o valor 1 e para $\alpha_{p-2\tau-1}$ tem o valor 0). Se 2^k a maior potência de 2 que divide $p = 2^N + \tau$, então $p = 2^k(2^{N-k} + q)$, com $\tau = 2^kq$ e $p - 2\tau - 1 = 2^N - \tau - 1 = 2^k(2^{N-k} - q) - 1$, donde se pode concluir que 2^k é a maior potência de 2 que divide $(p - 2\tau - 1) + 1 = p - 2\tau$. Como consequência, o k -ésimo dígito (a contar da direita) do número $\alpha_{p-2\tau}$ alterou-se em relação a $\alpha_{p-2\tau-1}$, pelo que o k -ésimo dígito (a contar da direita) de α_p alterou-se em relação a α_{p-1} (uma vez que, com excepção do dígito mais à esquerda, os dígitos de α_p coincidem com os de $\alpha_{p-2\tau-1}$, e os de α_{p-1} coincidem com os de $\alpha_{(p-1)-2(\tau-1)-1} = \alpha_{p-2\tau}$). \square

A tabela a seguir dá-nos a sequência de representações binárias produzidas pelo código de Gray, para $n = 4$ (com indicação, na primeira coluna, da ordem segundo a qual o código produz cada uma das cadeias de dígitos binários obtidas).

p	α_p	p	α_p
0	0000	8	1100
1	0001	9	1101
2	0011	10	1111
3	0010	11	1110
4	0110	12	1010
5	0111	13	1011
6	0101	14	1001
7	0100	15	1000

Com o processo de construção anteriormente referido, podemos obter as regras de codificação e descodificação que o teorema a seguir indica.

Teorema 18.11. *O código de Gray obtido pelo ciclo de Hamilton que percorre o n-cubo, conforme anteriormente se referiu, admite as seguintes regras de codificação e descodificação:*

1. Se $p = b_{n-1} \dots b_0$, onde b_0, \dots, b_{n-1} são dígitos binários, então

$$\alpha_p = a_{n-1} \dots a_0,$$

com $a_j = b_j + b_{j+1} \pmod{2}$, convencionando-se que $b_n = 0$, para $j = 0, \dots, n-1$, ocupa a p -ésima posição.

2. Se $\alpha_p = a_{n-1} \dots a_0$, onde a_0, \dots, a_{n-1} são dígitos binários, então $p = b_{n-1} \dots b_0$, com

$$b_i = \sum_{j=i}^{n-1} a_j \pmod{2}, \text{ para } i = 0, \dots, n-1.$$

Demonstração. Vamos fazer a prova de 1 por indução sobre n (número de dígitos binários das cadeias produzidas pelo código), tendo em conta que para $n = 1$ a regra 1 é trivialmente válida.

Suponha que a regra 1 é válida para $1 \leq n \leq N$ e que dispomos de um código com cadeias binárias de comprimento $N+1$. Sendo α_p uma dessas cadeias, se $p \leq 2^N - 1$, então (a menos do zero mais à esquerda) a representação de α_p coincide com a representação produzida pelo código de comprimento N . Logo, por hipótese de indução, a regra é válida.

Suponha que $p \geq 2^N$ e seja $p' = 2^{N+1} - 1 - p$ (i.e., $p = 2^{N+1} - 1 - p'$). Então, podemos concluir que a regra 1 se verifica para p' , uma vez que $p' = 2^{N+1} - 1 - p \leq 2^{N+1} - 1 - 2^N = 2^N(2-1) - 1 = 2^N - 1$. Porém, os dígitos binários das cadeias que representam $\alpha_p = a_N \dots a_0$ e $\alpha'_p = a'_N \dots a'_0$, estão relacionados da seguinte forma:

$$\begin{aligned} a_j &= a'_j, \text{ para } j = 0, \dots, N-1, \\ a_N &= 1, \\ a'_N &= 0, \end{aligned}$$

pelo que $a_N = a'_N + 1$. Por outro lado, tendo em conta que $p + p' = 2^{N+1} - 1 = 11 \dots 111$, sendo $p = b_N \dots b_0$ e $p' = b'_N \dots b'_0$, obtém-se $b_i = b'_i + 1 \pmod{2}$ (ou seja, se $b'_i = 0$, então $b_i = 1$ e se $b'_i = 1$, então $b_i = 0$). Como consequência, $a_i = a'_i = b'_i + b'_{i+1} \pmod{2} = b_i + b_{i+1} \pmod{2}$, para $i = 0, \dots, N-1$. Adicionalmente, $a_N = a'_{N+1} \pmod{2} = b'_N + b'_{N+1} + 1 \pmod{2} = b_N + b_{N+1} \pmod{2}$ (uma vez que $b'_N = 0$, $b'_{N+1} = 0$, $b_N = 1$ e $b_{N+1} = 0$). Deste modo fica completa a prova de 1.

A prova de 2 obtém-se invertendo 1. Com efeito, tendo em conta a sequência de somas $0 = b_0 + b_1 \pmod{2}, a_1 = b_1 + b_2 \pmod{2}, \dots, a_N = b_N + b_{N+1} \pmod{2}$, vem

$$\begin{aligned} a_i &= b_i + b_{i+1} \pmod{2} \\ &\Downarrow \\ a_i + a_{i+1} &= b_i + b_{i+1} + b_{i+1} + b_{i+2} = b_i + b_{i+2} \pmod{2} \\ &\Downarrow \\ a_i + a_{i+1} + a_{i+2} &= b_i + b_{i+2} + b_{i+2} + b_{i+3} = b_i + b_{i+3} \pmod{2} \\ &\Downarrow \\ &\vdots \\ &\Downarrow \\ a_i + a_{i+1} + \dots + a_N &= b_i + b_{N+1} = b_i \pmod{2} \text{ (uma vez que } b_{N+1} = 0\text{).} \end{aligned}$$

Logo, $b_i = \sum_{j=1}^N a_j \pmod{2}$, para $i = 0, \dots, N$, conforme se pretendia demonstrar. \square

18.2.2 Problema do caixeiro viajante

O problema do caixeiro viajante que usualmente se denota por TSP (iniciais de *Traveling Salesman Problem*), consiste em determinar um percurso que permita visitar uma conjunto de cidades, passando uma única vez em cada cidade e voltando à cidade de origem, com custo (ou tempo) total mínimo. Na terminologia da teoria dos grafos, dado um grafo completo com pesos não negativos nas arestas, este problema reduz-se à determinação de um ciclo de Hamilton de peso mínimo. Não existe perda de generalidade ao definir-se o problema para o grafo completo, uma vez que, sendo G um grafo arbitrário com pesos não negativos nas arestas definidos pela função $w_G : E(G) \mapsto \mathbb{R}^+$, a determinação de um ciclo de Hamilton de peso mínimo em G é equivalente à resolução do TSP para o grafo completo K com função de pesos $w_K : E(K) \mapsto \mathbb{R}^+ \cup \{\infty\}$ tal que

$$w_K(e) = \begin{cases} w_G(e), & \text{se } e \in E(G); \\ \infty, & \text{se } e \notin E(G). \end{cases}$$

O TSP é fácil de formular e, em geral, não é necessário grande talento para a obtenção de ciclos de Hamilton de peso aceitável (quando existem), mesmo para grandes problemas. No entanto, a determinação da solução do problema tem resistido à obtenção de "bons" algoritmos de resolução. Trata-se assim de um problema que contém todos os condimentos que têm atraído muitos matemáticos ao longo dos séculos – formulação simples e dificuldade de resolução. Existem também razões de carácter prático que contribuem para a importância do TSP, dado que muitos problemas da vida real se podem formular como casos particulares do TSP.

Uma abordagem imediata para a resolução do TSP consiste na pesquisa exaustiva de todos os ciclos de Hamilton do grafo e na escolha de um que apresente peso mínimo. A seguir descreve-se um algoritmo que utiliza esta pesquisa exaustiva.

Algoritmo de resolução do TSP por pesquisa exaustiva

Dados de entrada: grafo G de ordem n , com matriz de custos $W = (w_{ij})$;

Resultados de saída: ciclo de Hamilton de peso mínimo C ;

1. Fazer $PesoMin = \infty$;
2. Para todas as permutações π de $[n]$ fazer
 - (a) $Peso \leftarrow w_{\pi(n)\pi(1)} + \sum_{i=1}^{n-1} w_{\pi(i)\pi(i+1)}$;
 - (b) Se $Peso < PesoMin$ então $PesoMin \leftarrow Peso$ e $C \leftarrow \pi$;
3. Devolver C .

Um grafo completo de ordem n tem $(n - 1)!$ ciclos de Hamilton, os quais podem ser agrupado em pares de ciclos que diferem apenas no sentido em que são percorridos (com efeito, se a permutação do conjunto de vértices $[1, 2, \dots, n-1, n]$ define um ciclo de Hamilton então a permutação $[n, n-1, \dots, 2, 1]$ também define). No caso de grafos não orientados, ou seja, no caso simétrico em que $w_{ij} = w_{ji}$, existem "apenas" $\frac{1}{2}(n - 1)!$ ciclos de Hamilton. No entanto, mesmo para valores de n não muito grandes, este número continua a ser muito elevado. Por exemplo, para $n = 12$ obtém-se $\frac{1}{2} \cdot 11! = 19.958.400$ ciclos hamiltonianos candidatos a ciclos de peso mínimo. Assim, esta pesquisa exaustiva tem um custo computacional muito elevado. Alternativamente ao método de pesquisa exaustiva que exige um esforço computacional que cresce exponencialmente com n , é comum, na prática, a utilização de

métodos heurísticos com os quais, embora não se tenha a garantia de optimalidade, as experiências computacionais realizadas sugerem a obtenção de soluções próximas da solução óptima de modo eficiente.

Vamos introduzir uma técnica de "branch and bound"⁴ para a determinação de uma solução óptima do TSP, introduzida por Little, Marty, Sweeney e Karel em 1963. Esta técnica apresenta a vantagem de, em muitos casos, a solução óptima ser obtida sem se analisarem exaustivamente todos os ciclos de Hamilton. Por questões de simplicidade, utilizaremos W^* para denotar a matriz de pesos não negativos de um digrafo com os elementos diagonais modificados para $w_{ii}^* = \infty$, $i = 1, \dots, \nu$, a qual vamos designar por matriz de pesos modificada. Antes de prosseguirmos, convém ainda introduzir o seguinte resultado mais ou menos evidentes mas de grande utilidade.

Teorema 18.12. *Dado um digrafo definido pela matriz de pesos modificada $W^* = (w_{ij}^*)$, seja*

$$\begin{aligned}\hat{w}_r &= \min\{w_{rj}^*, j \in [\nu]\}, \\ \bar{w}_s &= \min\{w_{is}^*, i \in [\nu]\},\end{aligned}$$

para $r, s = 1, \dots, \nu$. Seja \hat{w} o vector coluna cujas componentes são \hat{w}_r , para $r = 1, \dots, \nu$, \bar{w}^T o vector linha cujas componentes são \bar{w}_s , para $s = 1, \dots, \nu$ e \hat{e} o vector coluna cujas componentes são todas iguais a 1. Denote-se por $W^* - \hat{w}\hat{e}^T$ ($W^* - \hat{e}\bar{w}^T$) a matriz que se obtém de W^* subtraindo \hat{w}_i a todas as entradas da i -ésima linha, para $i = 1, \dots, \nu$ (\bar{w}_j^T a todas as entradas da j -ésima coluna, para $j = 1, \dots, \nu$). Se $P(W^*)$ é o peso de uma solução óptima para o TSP do digrafo definido pela matriz W^* , então

$$P(W^*) = \sum_{i=1}^{\nu} \hat{w}_i + P(W^* - \hat{w}\hat{e}^T)$$

$$(P(W^*) = \sum_{j=1}^{\nu} \bar{w}_j + P(W^* - \hat{e}\bar{w}^T)).$$

Demonstração. Tendo em conta que qualquer que seja o vértice i uma solução óptima utiliza necessariamente um dos arcos com cauda em i (e também um dos arcos com cabeça em i), pelo menos o menor dos pesos destes arcos está presente nessa solução óptima e, consequentemente, o resultado verifica-se. \square

Note-se que nos digrafo onde existem pares ordenados de vértices sem os correspondentes arcos, podemos assumir que o arco em falta tem peso infinito. Por sua vez, os grafos não orientados podem encarar-se como grafos orientados nos quais entre cada par de vértices adjacentes existe um par de arcos com o mesmo peso (da aresta original) e sentidos opostos.

O algoritmo de Little, Marty, Sweeney e Karel, que a seguir se descreve, em cada iteração determina um minorante para a peso óptimo (com base no Teorema 18.12) e quando termina devolve um ciclo de Hamilton de peso mínimo. Como veremos, o processo iterativo desenvolve-se ao longo de uma árvore de decisão, onde cada vértice corresponde à decisão de considerar a inclusão (ou não) de um dado arco num ciclo em construção e à determinação do minorante obtido com essa decisão. A ramificação (produção na árvore de decisão de duas novas arestas que conduzem a outros tantos vértices, um dos quais relativo à inclusão de um dado arco no ciclo e outro à situação contrária) deve ser feita a partir do vértice corrente que é o que tem um minorante mais favorável de entre os vértices não ramificados. Com esta estratégia, caso se obtenha um ciclo de Hamilton com peso coincidente com o minorante, podemos concluir que esse ciclo é uma solução óptima para o TSP. Ao longo do algoritmo, vamos denotar por C e \bar{C} o par de caminhos tais que C é a parte conhecida (corrente) do ciclo de Hamilton eventualmente a determinar e \bar{C} , com início no vértice final de C e fim no vértice inicial de C , é a parte desconhecida. Quando $|E(C)| = \nu(\vec{G})$, podemos concluir que C define um ciclo de Hamilton.

⁴Designação inglesa que caracteriza uma família de algoritmos de optimização discreta.

Algoritmo de Little, Marty, Sweeney e Karel

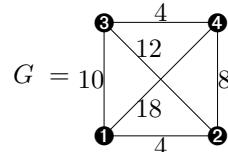
Dados de entrada: Matriz de pesos modificada $W^* = (w_{ij}^*)$ de um digrafo \vec{G} ;

Resultados de saída: Ciclo de Hamilton C de peso mínimo;

1. Fazer $Min \leftarrow 0$ e $E(C) = \emptyset$.
2. (a) Determinar \hat{w} , fazer $W^* \leftarrow W^* - \hat{w}\hat{e}^T$ e $Min \leftarrow Min + \sum_{i=1}^{\nu} \hat{w}_i$.
(b) Determinar \bar{w} , fazer $W^* \leftarrow W^* - \hat{e}\bar{w}^T$ e $Min \leftarrow Min + \sum_{i=1}^{\nu} \bar{w}_j$.
3. Considerar um dos arcos ij cuja entrada em W^* tem peso corrente nulo e proceder à ramificação a partir do vértice corrente da árvore de decisão, analisando no ramo (a) a possibilidade deste arco fazer parte do ciclo de Hamilton e o caso contrário no ramo (b):
 - (a) Neste ramo $E(C) \leftarrow E(C) \cup \{ij\}$ e a linha correspondente ao vértice i e a coluna correspondente ao vértice j são eliminadas da matriz W^* . Adicionalmente, para evitar o aparecimento de subciclos, os pesos dos arcos que ligam o vértice final (neste caso j) do caminho C (designado por caminho corrente) a qualquer dos vértices já percorridos tomam o valor ∞ .
 - (b) Neste ramo ($ij \notin E(C) \cup E(\bar{C})$) a entrada w_{ij}^* passa a ter o valor ∞ .
4. Escolher para vértice corrente da árvore de decisão a folha da árvore com menorante (Min) mais favorável.
5. Repetir os passos anteriores (com exceção do primeiro) até se obter um ciclo de Hamilton C .
6. Devolver o ciclo de Hamilton C e o menorante Min .

Exemplo 18.12. Vamos aplicar o algoritmo de Little, Marty, Sweeney e Karel ao TSP associado ao grafo G definido pela matriz de pesos:

$$W = \begin{pmatrix} \infty & 4 & 10 & 18 \\ 4 & \infty & 12 & 8 \\ 10 & 12 & \infty & 4 \\ 18 & 8 & 4 & \infty \end{pmatrix}$$



Solução.

1. $Min \leftarrow 0$; $E(C) \leftarrow \emptyset$.
2. ($E(C) = \emptyset$ e $Min = 0$)
$$\hat{w} \leftarrow \begin{pmatrix} 4 \\ 4 \\ 4 \\ 4 \end{pmatrix}, W \leftarrow \begin{pmatrix} \infty & 0 & 6 & 14 \\ 0 & \infty & 8 & 4 \\ 6 & 8 & \infty & 0 \\ 14 & 4 & 0 & \infty \end{pmatrix} \text{ e } Min \leftarrow 16;$$

$$\bar{w} \leftarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, W \leftarrow \begin{pmatrix} \infty & 0 & 6 & 14 \\ 0 & \infty & 8 & 4 \\ 6 & 8 & \infty & 0 \\ 14 & 4 & 0 & \infty \end{pmatrix} \text{ e } Min \leftarrow 16.$$

Árvore de decisão:

16

3. ($E(C) = \emptyset$ e $Min = 16$) Considerando o arco 12, temos as seguintes alternativas:

(a) $E(C) = \{12\}$, a linha 1 e a coluna 2 são eliminadas da matriz W e a entrada w_{21} passa a

$$\infty, \text{ obtendo-se a matriz } W \leftarrow \begin{array}{c|ccc} & \textcircled{1} & \textcircled{3} & \textcircled{4} \\ \textcircled{2} & \infty & 8 & 4 \\ \textcircled{3} & 6 & \infty & 0 \\ \textcircled{4} & 14 & 0 & \infty \end{array}, \text{ para a qual}$$

$$\hat{w} \leftarrow \begin{pmatrix} 4 \\ 0 \\ 0 \end{pmatrix}, W \leftarrow \begin{array}{c|ccc} & \textcircled{1} & \textcircled{3} & \textcircled{4} \\ \textcircled{2} & \infty & 4 & 0 \\ \textcircled{3} & 6 & \infty & 0 \\ \textcircled{4} & 14 & 0 & \infty \end{array}, \bar{w} \leftarrow \begin{pmatrix} 6 \\ 0 \\ 0 \end{pmatrix}, W \leftarrow \begin{array}{c|ccc} & \textcircled{1} & \textcircled{3} & \textcircled{4} \\ \textcircled{2} & \infty & 4 & 0 \\ \textcircled{3} & 0 & \infty & 0 \\ \textcircled{4} & 8 & 0 & \infty \end{array}$$

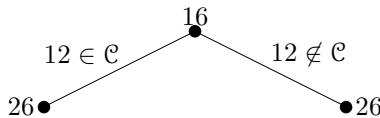
e $Min \leftarrow 26$.

(b) $12 \notin E(C) \cup E(\overline{C})$ e então obtém-se a matriz $W \leftarrow \begin{array}{c|cccc} & \infty & \infty & 6 & 14 \\ & 0 & \infty & 8 & 4 \\ & 6 & 8 & \infty & 0 \\ & 14 & 4 & 0 & \infty \end{array}$, para a qual

$$\hat{w} \leftarrow \begin{pmatrix} 6 \\ 0 \\ 0 \\ 0 \end{pmatrix}, W \leftarrow \begin{array}{c|cccc} \infty & \infty & 0 & 8 \\ 0 & \infty & 8 & 4 \\ 6 & 8 & \infty & 0 \\ 14 & 4 & 0 & \infty \end{array}, \bar{w} \leftarrow \begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \end{pmatrix}, W \leftarrow \begin{array}{c|cccc} \infty & \infty & 0 & 8 \\ 0 & \infty & 8 & 4 \\ 0 & 4 & \infty & 0 \\ 8 & 0 & 0 & \infty \end{array}$$

e $Min \leftarrow 26$.

Árvore de decisão:



2. ($E(C) = \{12\}$, $W = \begin{array}{c|ccc} & \textcircled{1} & \textcircled{3} & \textcircled{4} \\ \textcircled{2} & \infty & 4 & 0 \\ \textcircled{3} & 0 & \infty & 0 \\ \textcircled{4} & 8 & 0 & \infty \end{array}$ e $Min = 26$) Considerando o arco 24, temos as seguintes alternativas:

(a) $E(C) = \{12, 24\}$, a linha que corresponde ao vértice 2 e a coluna que corresponde ao vértice 4 são eliminadas da matriz W e a entrada w_{41} passa a ∞ , obtendo-se a matriz

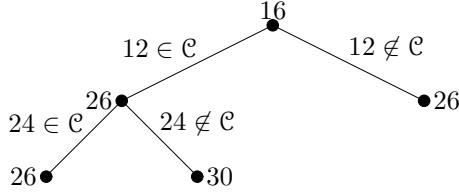
$$W \leftarrow \begin{array}{c|cc} & \textcircled{1} & \textcircled{3} \\ \textcircled{3} & 0 & \infty \\ \textcircled{4} & \infty & 0 \end{array}, \text{ para a qual}$$

$$\hat{w} \leftarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \bar{w} \leftarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

e $Min \leftarrow 26$.

(b) $24 \notin E(C) \cup E(\bar{C})$ e então obtém-se a matriz $W \leftarrow \begin{array}{c} \textcircled{1} \quad \textcircled{3} \quad \textcircled{4} \\ \textcircled{2} \quad (\infty \quad 4 \quad \infty) \\ \textcircled{3} \quad (0 \quad \infty \quad 0) \\ \textcircled{4} \quad (8 \quad 0 \quad \infty) \end{array}$ e
 $\hat{w} \leftarrow \begin{pmatrix} 4 \\ 0 \\ 0 \end{pmatrix}, W \leftarrow \begin{array}{c} \textcircled{1} \quad \textcircled{3} \quad \textcircled{4} \\ \textcircled{2} \quad (\infty \quad 0 \quad \infty) \\ \textcircled{3} \quad (0 \quad \infty \quad 0) \\ \textcircled{4} \quad (8 \quad 0 \quad \infty) \end{array}, \bar{w} \leftarrow \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ e $Min \leftarrow 30$.

Árvore de decisão:



2. ($E(C) = \{12, 24\}$, $W = \begin{array}{c} \textcircled{1} \quad \textcircled{3} \\ \textcircled{3} \quad (\infty \quad \infty) \\ \textcircled{4} \quad (\infty \quad 0) \end{array}$ e $Min = 26$) Considerando o arco 31, temos as seguintes alternativas:

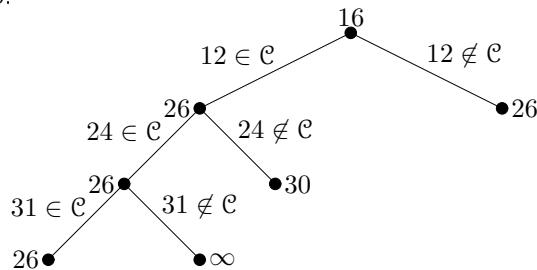
(a) $E(C) = \{12, 24, 31\}$, a linha que corresponde ao vértice 3 e a coluna que corresponde ao vértice 1 são eliminadas da matriz W , obtendo-se a matriz $W \leftarrow \begin{array}{c} \textcircled{1} \quad \textcircled{3} \\ \textcircled{4} \quad (0) \end{array}$, para a qual

$$\hat{w} \leftarrow (0), \bar{w} \leftarrow (0),$$

e $Min \leftarrow 26$. Note-se que o arco 43 completa o ciclo de Hamilton $3 \rightarrow 1 \rightarrow 2 \rightarrow 4 \rightarrow 3$, mantendo o peso 26.

(b) $31 \notin E(C) \cup E(\bar{C})$ e então obtém-se $W \leftarrow \begin{array}{c} \textcircled{1} \quad \textcircled{3} \\ \textcircled{3} \quad (\infty \quad \infty) \\ \textcircled{4} \quad (\infty \quad 0) \end{array}$ e $Min \leftarrow \infty$ (neste caso, não é possível obter um ciclo de Hamilton).

Árvore de decisão:



Uma vez que todas as folhas da árvore de decisão distintas da que corresponde ao ciclo de Hamilton determinado têm um minorante não inferior a 26, podemos concluir que a solução encontrada é óptima. \square

Segue-se um método heurístico, relativamente eficiente, que nos casos em que a sua execução termina obtém uma solução optima para o TSP. Para fundamentar a aplicação deste método a um grafo arbitrário G com matriz de pesos nas arestas W , convém introduzir o resultado a seguir, onde p denota uma função de penalidade nos vértices $p : V(G) \mapsto \mathbb{R}$.

Teorema 18.13. Seja G um grafo com matriz de pesos nas arestas $W = (w_{ij})$, p uma função de penalidade nos vértices e G' o grafo que se obtém de G alterando a matriz de pesos nas arestas para $W' = (w'_{ij})$, tal que

$$w'_{ij} = w_{ij} + p(i) + p(j),$$

Então, qualquer solução óptima do TSP para o grafo G' determina uma solução óptima do TSP para G .

Demonstração. Observe-se que para qualquer ciclo de Hamilton com arestas e_1, e_2, \dots, e_ν , o seu peso é

$$\sum_{i=1}^{\nu} W'(e_i) = \sum_{i=1}^{\nu} W(e_i) + 2 \sum_{v \in V(G)} p(v).$$

Então o peso de um ciclo para o grafo G' é igual o peso para o grafo G mais uma constante, com valor $2 \sum_{v \in V(G)} p(v)$, que não depende do ciclo. Como consequência, um ciclo de peso mínimo para G' é também um ciclo de peso mínimo para G . \square

Algoritmo de premiar e punir para a determinação de um caminho de Hamilton de peso mínimo entre dois vértices

Dados de entrada: grafo G com matriz de pesos nas arestas W e dois vértices $v_0, v_1 \in V(G)$;

Resultados de saída: caminho de Hamilton T entre v_0 e v_1 de peso mínimo;

Notação: valor de penalidade p e variação da penalidade Δp ;

1. Fazer $p(v) \leftarrow 0$ para cada $v \in V(G)$.
2. Determinar, com recurso de algoritmo de Kruskal, uma árvore abrangente de peso mínimo T para o grafo G com a matriz de pesos W' .
3. Se T é um caminho, então PARAR (T é um caminho de Hamilton de peso mínimo). Caso contrário, utilizando o Teorema 18.13, para cada $v \in V(G)$ fazer:
 - (premiar) se $v \notin \{v_0, v_1\}$ e $d_T(v) = 1$, então $p(v) \leftarrow p(v) - p$,
 - (punir) se $v \notin \{v_0, v_1\}$ e $d_T(v) > 2$ ou $v \in \{v_0, v_1\}$ e $d_T(v) > 1$, então $p(v) \leftarrow p(v) + p$.
4. Se $p > \Delta p$, então modificar o valor de penalidade ($p \leftarrow p - \Delta p$) e em qualquer caso voltar a 2.

Mais precisamente, este procedimento é apresentado com recurso ao pseudocódigo Algoritmo 18.4 TSPPREMIAREPUNIR. Neste algoritmo, assume-se que os valores de p e Δp são pré-definidos.

Algoritmo 18.4: TSPPREMIAREPUNIR(G, W, v_0, v_1)

```

para todo  $v \in V(G)$  fazer  $p[v] \leftarrow 0$ 
repetir
  para todo  $v \in V(G)$  fazer
    para todo  $w \in V(G)$  fazer  $W'[v, w] \leftarrow W[v, w] + p[v] + p[w]$ 
    Kruskal( $G, W', v_0$ )
     $ok \leftarrow$  verdadeiro
    para todo  $v \in \{v_0, v_1\}$ 
      fazer se  $d_T(v) > 1$  então  $p[v] \leftarrow p[v] + p$ ;  $ok \leftarrow$  falso
    para todo  $v \in V \setminus \{v_0, v_1\}$ 
      fazer {se  $d_T(v) > 2$  então  $p[v] \leftarrow p[v] + p$ ;  $ok \leftarrow$  falso
             se  $d_T(v) < 2$  então  $p[v] \leftarrow p[v] - p$ ;  $ok \leftarrow$  falso}
      se  $p > \Delta p$  então  $p \leftarrow p - \Delta p$ 
    até  $ok$ 
devolver ( $T$ )

```

Exemplo 18.13. Vamos determinar um ciclo de comprimento mínimo que passe por todas as cidades de Portugal, relativamente ao grafo representado na Figura 14.8, com recurso ao algoritmo de premiar e punir.

Solução. Observe-se que no mapa da Figura 14.8 existem vértices (cidades) de grau 2 como, por exemplo, a Covilhã. Como consequência, cada ciclo de Hamilton utiliza necessariamente a aresta Covilhã–Guarda. Assim, vamos remover esta aresta e determinar um caminho abrangente de comprimento mínimo entre a Covilhã e a Guarda. É claro que este caminho é também um árvore abrangente onde os vértices relativos à Covilhã e à Guarda têm grau 1 e os restantes têm grau 2. Logo, em cada iteração do algoritmo procuramos, com recurso ao algoritmo de Kruskal, uma árvore abrangente de comprimento mínimo e com raiz na Covilhã, penalizando todos vértices de grau maior do que o necessário e premiando os vértices de grau menor do que o necessário. Neste exemplo, na primeira iteração, vamos utilizar um valor de penalização (ou prémio) $p = 80$, o qual vai decrescer de $\Delta p = 5$ unidades em cada uma das iterações seguintes. Na Figura 18.13, representam-se os resultados decorrentes de todas as iterações, verificando-se que ao fim de 14 iterações se obtém um ciclo de Hamilton com o comprimento mínimo de 2.127 km. \square

Deve observar-se que o valor de penalização tem influência decisiva no número de iterações necessárias e até na convergência do método. No caso do exemplo anterior, a utilização de um valor de penalização constante igual a 10 em cada iteração (isto é, $p = 10$ e $\Delta p = 0$) implicaria a execução de 40 iterações. Por outro lado, para certos valores de penalização o algoritmo não converge.

Geralmente, recomenda-se a utilização de um valor de penalização aproximadamente igual à média dos pesos das arestas do grafo.

18.3. Exercícios

18.1. Indique os valores de n para os quais o grafo K_n é euleriano.

18.2. Indique os valores de m e n para os quais o grafo $K_{m,n}$ é euleriano.

18.3. Considere o grafo representado na figura a seguir e responda.

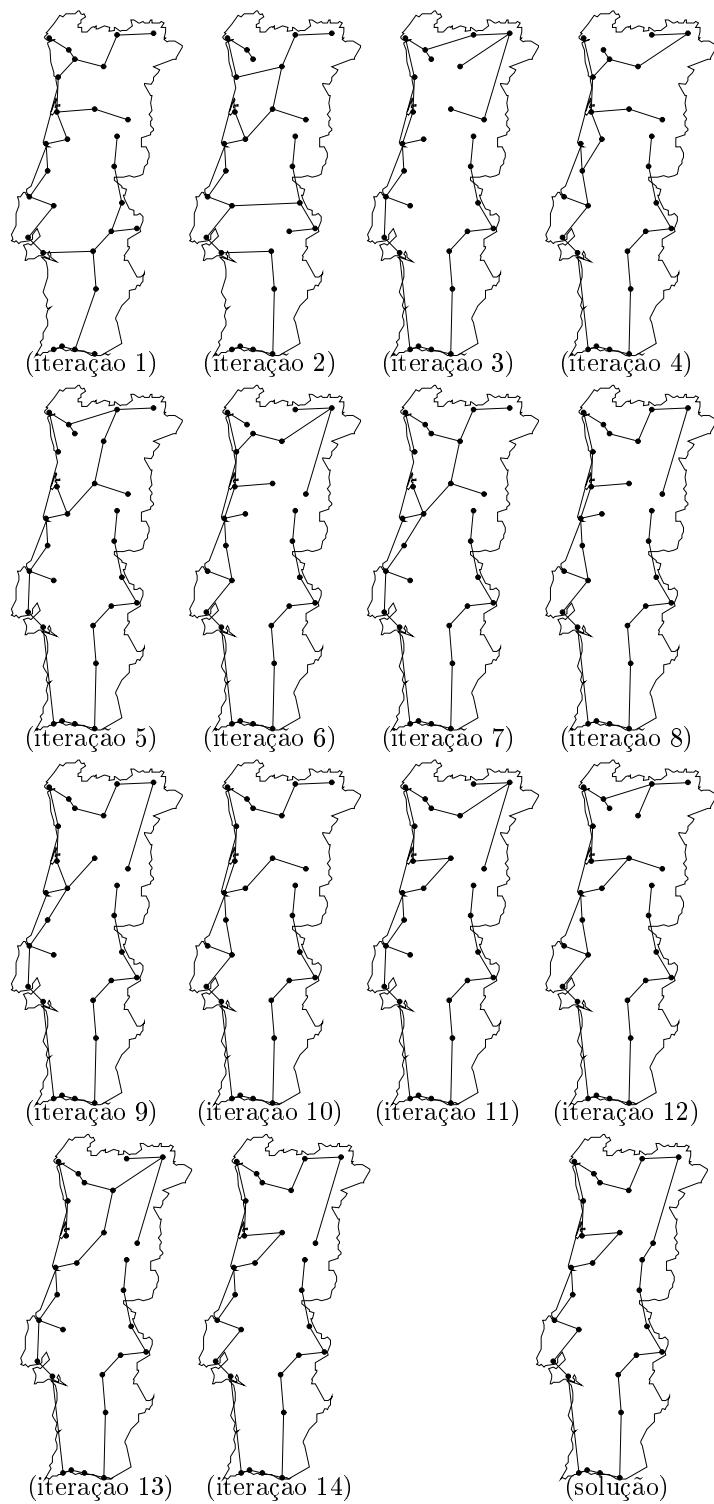
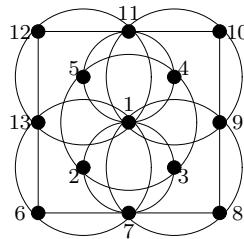


Figura 18.13: Exemplo de resolução do TSP pelo método de premiar e punir.

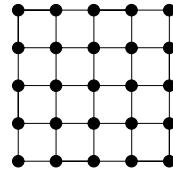


- (a) Verifique que se trata de um grafo euleriano.
- (b) Determine um circuito de Euler, utilizando o Algoritmo 18.2 (algoritmo de Hierholzer, página 484).
- (c) Determine um circuito de Euler, utilizando o Algoritmo 18.3 (algoritmo de Fleury, página 485).
- 18.4. Determine um passeio fechado óptimo para o problema do carteiro chinês associado ao grafo definido pela matriz de pesos

$$W(G) = \begin{pmatrix} 0 & 5 & \infty & \infty & \infty & 6 & \infty & \infty & \infty \\ 5 & 0 & 6 & \infty & \infty & 5 & 6 & \infty & \infty \\ \infty & 6 & 0 & 6 & \infty & \infty & \infty & 6 & \infty \\ \infty & \infty & 6 & 0 & 4 & \infty & \infty & 10 & 7 \\ \infty & \infty & \infty & 4 & 0 & \infty & \infty & \infty & 4 \\ \infty & 5 & \infty & \infty & \infty & 0 & 7 & \infty & \infty \\ \infty & 6 & \infty & \infty & \infty & 7 & 0 & 18 & \infty \\ \infty & \infty & 6 & 10 & \infty & \infty & 18 & 0 & 9 \\ \infty & \infty & \infty & 7 & 4 & \infty & \infty & 9 & 0 \end{pmatrix},$$

utilizando o algoritmo de Edmonds e Johnson (página 488).

- 18.5. Considere o grafo representado na figura a seguir e resolva o problema do carteiro chinês, assumindo que todas as arestas têm o mesmo peso.



- 18.6. Seja G o grafo de Petersen (grafo representado na Figura 14.4, página 385))
- (a) Determine um subconjunto de arestas de G , $E' \subset E(G)$, de cardinalidade mínima, de tal forma que o subgrafo $G - E'$ admita um trajecto de Euler.
- (b) Prove que G é um grafo não hamiltoniano.
- 18.7. Sendo G um grafo hamiltoniano e $X \subset V(G)$ um subconjunto não vazio de vértices, prove a desigualdade $cc(G - X) \leq |X|$.
- 18.8. Tendo em conta que um grafo é orientável se admite uma orientação das suas arestas de tal forma que o digrafo obtido é fortemente conexo, indique qual ou quais das seguintes afirmações são verdadeiras.
- (a) Qualquer grafo hamiltoniano é orientável.
- (b) Cada grafo orientável é Hamiltonian.

- 18.9. De acordo com o teorema de Ore (Corolário 18.6, página 491), um grafo, G , simples de ordem $\nu(G) \geq 3$, para o qual se verifica

$$\forall_{u,v \in V(G)} d_G(u) + d_G(v) \geq \nu(G),$$

é um grafo hamiltoniano. Prove que se esta propriedade for substituída por $\forall_{u,v \in V(G)} d_G(u) + d_G(v) \geq \nu(G) - 1$, então o grafo pode ser não hamiltoniano.

- 18.10. Seja G um grafo simples de ordem $\nu(G) \geq 3$. Prove que para todo o par de vértices não adjacentes $x, y \in V(G)$ se verifica a desigualdade $d_G(x) + d_G(y) \geq \nu(G)$, então G é hamiltoniano.

- 18.11. Considere a sequência de números binários produzida pelo código de Gray com 8 bites.

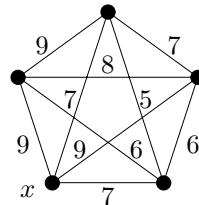
- (a) Indique a ordem em que aparece o número binário 10110011 na sequência;
- (b) Indique o número binário que ocupa o lugar 156 na sequência.

- 18.12. Resolva o TSP associado ao grafo definido pela matriz de pesos nas arestas

$$W(G) = \begin{pmatrix} 0 & 28 & 31 & 28 & 22 & 36 & 50 & 67 & 40 & 74 \\ 28 & 0 & 31 & 40 & 41 & 64 & 74 & 80 & 63 & 101 \\ 31 & 31 & 0 & 14 & 53 & 53 & 53 & 50 & 42 & 83 \\ 28 & 40 & 14 & 0 & 50 & 41 & 39 & 41 & 28 & 69 \\ 22 & 41 & 53 & 50 & 0 & 40 & 61 & 86 & 53 & 78 \\ 36 & 64 & 53 & 41 & 40 & 0 & 24 & 58 & 22 & 39 \\ 50 & 74 & 53 & 39 & 61 & 24 & 0 & 37 & 11 & 30 \\ 67 & 80 & 50 & 41 & 86 & 58 & 37 & 0 & 36 & 60 \\ 40 & 63 & 42 & 28 & 53 & 22 & 11 & 36 & 0 & 41 \\ 74 & 101 & 83 & 69 & 78 & 39 & 30 & 60 & 41 & 0 \end{pmatrix},$$

utilizando o algoritmo de Little, Marty, Sweeney e Karel (página 498).

- 18.13. Com recurso ao Algoritmo 18.4 (algoritmo de premiar e punir, página 502), determine um caminho de Hamilton de comprimento mínimo entre os vértices v_8 e v_9 do grafo definido no Exercício 18.4.
- 18.14. Considere o grafo representado na figura a seguir.



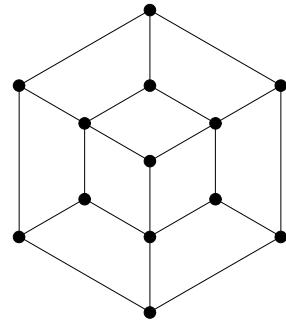
- (a) Determine o número de ciclos de Hamilton.
- (b) Determine o número de árvores abrangentes do subgrafo obtido depois de se ter eliminado o vértice marcado com x .
- (c) De entre as árvores abrangentes determinadas na alínea anterior quantas fazem parte de ciclos hamiltonianos de $G - x$?
- (d) Determine uma árvore abrangente de peso mínimo do subgrafo $G - x$ e demonstre que o peso (ou comprimento) da solução óptima do TSP associado a este subgrafo é de pelo menos 32.

18.15. Prove que se G é um grafo hamiltoniano, então qualquer que seja o subconjunto de vértices $S \subseteq V$, $\text{cc}(G - S) \leq |S|$.

18.16. Dado um grafo G , demonstre que se $\delta(G) \geq \frac{1}{2}\nu(G)$ então G é hamiltoniano.

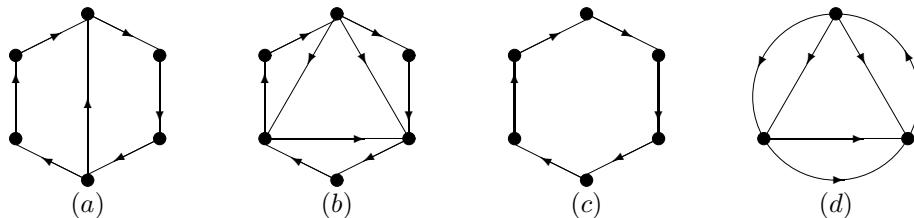
18.17. Demonstre que se G é um grafo bipartido de ordem ímpar, então é não hamiltoniano.

18.18. Mostre que o grafo a seguir representado é um grafo não hamiltoniano.



18.19. Determine qual ou quais dos seguintes digrafos são:

- (a) Fortemente conexos;
- (b) Eulerianos (digrafos que admitem circuitos de Euler orientados);
- (c) Hamiltonianos (digrafos que admitem ciclos de Hamilton orientados).



18.20. Considerando os grafos simples G de ordem ν , determine o menor e o maior número de arestas de tal forma que G

- (a) seja conexo;
- (b) seja desconexo;
- (c) tenha exactamente c componentes conexos.
- (d) seja hamiltoniano;
- (e) seja não hamiltoniano.
- (f) não contenha P_k – caminho com k arestas.

19

Independentes, Cliques e Colorações

Muitos problemas práticos podem formular-se com recurso à teoria dos grafos, como problemas de determinação de conjuntos independentes de vértices ou cliques, ou ainda, como problemas de coloração de vértices ou arestas, relativamente aos quais, muitas vezes, o principal objectivo é o de chegar à maior ou menor das cardinalidades em jogo. No entanto, estes problemas são, em geral, difíceis de resolver quando a ordem e dimensão dos grafos é elevada. Assim, torna-se conveniente tirar partido de todas as propriedades apresentadas pelos casos particulares ou aproximar as respectivas cardinalidades por majorantes e minorantes adequados. Este capítulo inclui uma boa parte das propriedades básicas relacionadas com a determinação de conjuntos independentes de vértices e cliques, com a determinação de colorações de vértices, com a determinação de colorações de arestas e a determinação de majorantes e minorantes para as cardinalidades que lhes estão associadas. Adicionalmente, ao longo do capítulo, apresentam-se várias aplicações.

19.1. Conjuntos independentes e cliques

Convém, nesta altura, introduzir os conceitos de conjunto independente de vértices (ou estável), independente maximal, independente máximo (ou estável máximo) e número de independência (ou número de estabilidade) que são conceitos muito utilizados em aplicações práticas.

Definição 19.1 (Conjunto independente e número de independência). *Um subconjunto de vértices $S \subseteq V(G)$ diz-se um conjunto independente (ou estável) de G se entre quaisquer dois vértices distintos de S não existe uma aresta, ou seja, se induz um subgrafo nulo. O conjunto independente de vértices $S \subseteq V(G)$ diz-se maximal se qualquer que seja o vértice $v \in V(G) \setminus S$, $S \cup \{v\}$ não é um conjunto independente. Um conjunto independente de vértices de G de cardinalidade máxima diz-se um independente máximo (ou estável máximo) de G e a sua cardinalidade designa-se por número de independência (ou número de estabilidade) e denota-se por $\alpha(G)$.*

Como exemplo de aplicação do conceito de conjunto independente de vértices de um grafo, suponha que pretende armazenar várias substâncias químicas em diferentes salas. É claro que é aconselhável armazenar em salas diferentes as substâncias químicas que são incompatíveis entre si (ou seja, aquelas que na presença umas das outras podem provocar reacções com consequências indesejáveis). Seja G um grafo cujos vértices são as substâncias químicas e onde dois vértices são adjacentes se e só se as correspondentes substâncias são incompatíveis. Logo, qualquer conjunto de vértices representando substâncias compatíveis forma um conjunto independente de vértices em G .

Exemplo 19.1. Vamos determinar todos os conjuntos independentes, independentes maximais e o número de independência do grafo G representado na Figura 19.1.

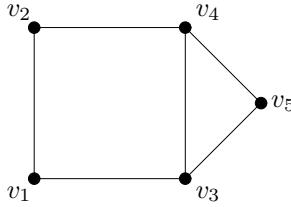


Figura 19.1: Grafo simples G com $\alpha(G) = 2$.

Solução. Por definição, o conjunto vazio e todos os conjuntos singulares de vértices são conjuntos independentes, logo

$$\emptyset, \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\}$$

são conjuntos independentes. Um subconjunto de vértices de cardinalidade dois $\{x, y\}$ é independente se e só se $xy \notin E(G)$, logo

$$\{v_1, v_4\}, \{v_1, v_5\}, \{v_2, v_3\}, \{v_2, v_5\} \quad (19.1)$$

são conjuntos independentes. Por verificação exaustiva, podemos concluir que não existe nenhum conjunto independente de cardinalidade três (e, como consequência, também não existem conjuntos independentes de cardinalidade superior a 3). Logo, entre todos os conjuntos independentes determinados, os maximais (que são os que não estão contidos em qualquer outro) são os representados em (19.1). Consequentemente, o número de independência de G é $\alpha(G) = 2$. \square

Os grafos onde todos os conjuntos independentes de vértices maximais são independentes máximos, como é o caso do grafo representado na Figura 19.1, designam-se por *grafos bem cobertos*.

Antes de considerarmos outro exemplo de aplicação da determinação de independentes máximos em grafos, vamos introduzir o conceito de distância de Hamming entre duas sequências de dígitos. Assim, dadas duas sequências de m dígitos, $x = x_1x_2\dots x_m$ e $y = y_1y_2\dots y_m$, cada um dos quais pertence a um mesmo conjunto de n símbolos, designa-se por *distância de Hamming* entre x e y e denota-se por $d_{Ham}(x, y)$, o número de posições em que x e y diferem. Por exemplo, dadas as palavras de 10 letras do nosso alfabeto:

bombástico e *fantástica*,

conclui-se que a distância de Hamming entre elas é igual a 5, uma vez que as duas palavras têm letras distintas nas posições 1, 2, 3, 4 e 10. Esta métrica é muito utilizada em *teoria dos códigos*, com vista à determinação de códigos que sejam imunes a um certo nível de ruído.

Designa-se por *grafo de Hamming* com parâmetros (m, n) e denota-se por $H(m, n)$ o grafo cujos vértices são as sequências de m dígitos pertencentes a um conjunto de n símbolos e onde dois vértices são adjacentes se as correspondentes sequências estão a uma distância de Hamming igual a 1.

Exemplo 19.2. Vamos transformar a determinação de um quadrado latino de ordem n na determinação de um independente máximo de um grafo de Hamming e, com base nesta transformação, determinar um quadrado latino de ordem três.

Solução. Sendo $X = (x_{ij})$ um quadrado latino de ordem n sobre o conjunto de símbolos $[n]$ e denotando cada entrada $x_{ij} = k$ por x_{ijk} , com $i, j, k \in [n]$, é claro que em X não podem existir duas entradas determinadas por $x_{i_1j_1k_1}$ e $x_{i_2j_2k_2}$ cuja distância de Hamming entre as sequências de

três índices $(i_1 j_1 k_1)$ e $(i_2 j_2 k_2)$ seja igual a 1. Logo, construindo o correspondente grafo de Hamming, $H(3, n)$, que é um grafo de ordem n^3 tal que

$$\begin{aligned} V(G) &= \{(ijk) : i, j, k \in [n]\}, \\ E(G) &= \{(i_1 j_1 k_1)(i_2 j_2 k_2) : d_{Ham}((i_1 j_1 k_1), (i_2 j_2 k_2)) = 1\}, \end{aligned}$$

conclui-se que a determinação de um quadrado latino X de ordem n é equivalente à determinação de um independente máximo de $H(3, n)$.

1. Com efeito, uma vez que de entre as possíveis sequências de índices ijk , com $i, j, k \in [n]$, existem no máximo n^2 pares de índices distintos, podemos concluir, imediatamente, que $\alpha(H(3, n)) \leq n^2$.
2. Por outro lado, admitindo que existe um quadrado latino L de ordem n (o que é sempre possível de obter, utilizando, por exemplo, as técnicas introduzidas na secção 8.6) é claro que o conjunto de sequências de três índices $\{ijk : L_{ij} = k\}$ tem cardinalidade n^2 (que é igual ao número de entradas de L) e define em $H(3, n)$ um conjunto independente de vértices.

Tendo em conta os pontos 1 e 2, $\alpha(H(3, n)) = n^2$.

Concretizando esta redução da determinação de quadrados latinos à determinação de independentes máximos de grafos de Hamming, para $n = 3$, considerando o grafo de Hamming $H(3, 3)$ (que tem ordem 27), conforme anteriormente se referiu, vem

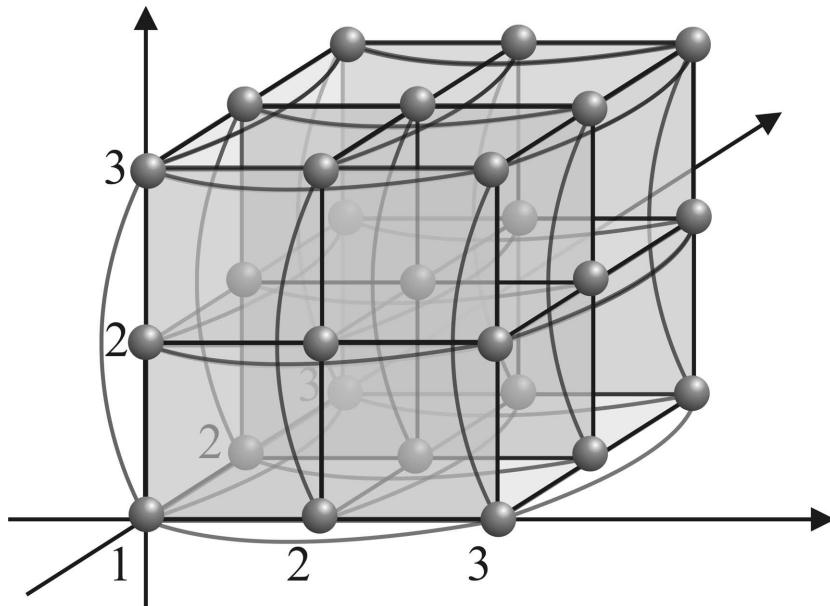


Figura 19.2: O grafo de Hamming $H(3, 3)$.

$$\begin{aligned} V(G) &= \{(111), (112), (113), (121), (122), (123), (131), (132), (133), (211), (212), (213), (221), (222), \\ &\quad (223), (231), (232), (233), (311), (312), (313), (321), (322), (323), (331), (332), (333)\}, \end{aligned}$$

$$\begin{aligned} E(G) &= \{(111)(112), (111)(113), (111)(121), (111)(131), (111)(211), (111)(311), (112)(113), \\ &\quad (112)(122), (112)(132), (112)(212), (112)(312), (113)(123), (113)(213), (113)(313), \\ &\quad (121)(122), (121)(123), (121)(131), (121)(221), (121)(321), (122)(123), (122)(222), \\ &\quad (122)(322), (123)(133), (123)(223), (123)(323), (131)(132), (131)(133), (132)(332), \\ &\quad (133)(233), (133)(333), (211)(212), (211)(213), (211)(221), (211)(231), (211)(311), \end{aligned}$$

$(212)(213), (212)(222), (212)(232), (212)(312), (213)(223), (213)(233), (213)(223),$
 $(213)(233), (213)(313), (221)(222), (221)(223), (221)(231), (221)(321), (222)(223),$
 $(222)(232), (222)(322), (223)(323), (231)(232), (231)(233), (231)(331), (232)(233),$
 $(232)(332), (233)(333), (311)(312), (311)(313), (311)(321), (311)(331), (312)(313),$
 $(312)(322), (312)(323), (312)(332), (313)(323), (313)(333), (321)(322), (321)(322),$
 $(321)(323), (321)(331), (322)(323), (322)(332), (323)(333), (331)(332), (331)(333),$
 $(332)(333)\}.$

Analizando este grafo, obtém-se, por exemplo, os conjuntos independentes máximos

$$\begin{aligned} S_1 &= \{(111), (122), (133), (212), (223), (231), (313), (321), (332)\}, \\ S_2 &= \{(111), (122), (133), (213), (221), (232), (312), (323), (331)\}, \end{aligned}$$

cada um dos quais define, naturalmente, um quadrado latino de ordem 3 \square

Segue-se um resultado que relaciona os conceitos de conjunto independente de vértices e conjunto de cobertura por vértices (ver Definição 17.6).

Teorema 19.1. *Dado um grafo G , um subconjunto de vértices $S \subseteq V(G)$ é independente se e só se $T = V(G) \setminus S$ é um conjunto de cobertura por vértices.*

Demonstração. Um subconjunto $S \subseteq V(G)$ é um independente se e só se não existem vértices adjacentes em S . Logo, qualquer aresta de G é incidente num vértice de $T = V(G) \setminus S$, pelo que T é um conjunto de cobertura. \square

O teorema a seguir, demonstrado por Gallai¹ em 1959, relaciona o número de independência de um grafo G , $\alpha(G)$, com o seu número de cobertura por vértices $\beta(G)$ (ver secção 17.2.1).

Teorema 19.2 (Gallai). *Dado um grafo G ,*

$$\alpha(G) + \beta(G) = \nu(G).$$

Demonstração. Seja S um conjunto independente máximo para o grafo G . Pelo Teorema 19.1, $V(G) \setminus S$ é um conjunto de cobertura por vértices e, consequentemente,

$$|V(G) \setminus S| = \nu(G) - \alpha(G) \geq \beta(G).$$

De modo semelhante se conclui que, sendo T um conjunto de cobertura mínima de arestas por vértices de G , $V(G) \setminus T$ é um conjunto independente de vértices de G e, consequentemente,

$$|V(G) \setminus T| = \nu(G) - \beta(G) \leq \alpha(G).$$

Tendo em conta as desigualdades obtidas, obtém-se $\nu(G) = \alpha(G) + \beta(G)$. \square

Definição 19.2 (Cliques e número de clique). *Dado um grafo G , um subconjunto de vértices $K \subseteq V(G)$ diz-se uma clique de G se entre quaisquer dois vértices distintos pertencentes a K existe uma aresta, ou seja, se K induz um subgrafo completo. Uma clique K diz-se maximal se qualquer que seja $v \in V(G) \setminus K$ o conjunto de vértices $K \cup \{v\}$ não é uma clique. Uma clique de G de cardinalidade máxima designa-se por clique máxima e a sua cardinalidade por número de clique de G e denota-se por $\omega(G)$.*

Exemplo 19.3. *Vamos determinar todas as cliques, cliques maximais e o número de clique para o grafo representado na Figura 19.1.*

¹ Tibor Gallai (1912–1992), foi um matemático húngaro que trabalhou em teoria dos grafos.

Solução. Por definição, o conjunto vazio e todos os subconjuntos singulares de vértices são cliques, logo os subconjuntos

$$\emptyset, \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\}$$

são cliques. Um subconjunto de vértices de cardinalidade dois $\{x, y\}$ é uma clique se e só se $xy \in E(G)$, logo os subconjuntos

$$\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}, \{v_3, v_5\}, \{v_4, v_5\}$$

são cliques. Uma vez que os subconjuntos de vértices de cardinalidade três $\{x, y, z\}$ são cliques se e só se formam triângulos (isto é, $xy, xz, yz \in E(G)$), podemos concluir que o subconjunto

$$\{v_3, v_4, v_5\}$$

é uma clique. Por observação directa da figura que representa o grafo, podemos concluir ainda que não existe nenhuma clique de cardinalidade quatro (ou mais). Adicionalmente, de entre todas as cliques, as quatro maximais (que são as que não estão contidos em qualquer outra) são:

$$\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_4\}, \{v_3, v_4, v_5\}.$$

Logo, é claro que o número de clique para este grafo é $\omega(G) = 3$. □

Tendo em conta as definições de conjunto independente de vértices e clique e de número de independência e número de clique, conclui-se imediatamente que se um conjunto de vértices T é independente para um grafo G , então o mesmo conjunto é uma clique para o grafo complementar G^c e, adicionalmente, $\alpha(G) = \omega(G^c)$. Consequentemente, o problema da determinação de um independente máximo é equivalente ao problema da determinação de uma clique máxima.

19.2. Coloração de vértices

A coloração de vértices em grafos, embora seja usualmente associada ao problema clássico da coloração de mapas, a estudar no capítulo seguinte (Secção 20.4), modela muitos problemas de aplicação actuais. Com efeito, os problemas de coloração de vértices em grafos aparecem, hoje em dia, em modelos de elaboração de horários, atribuição de frequências de rádio a diferentes estações emissoras, etc. Com estes modelos, em geral, o objectivo é a atribuição de cores aos vértices de um grafo de tal forma que não existam vértices adjacentes com a mesma cor. Mais geralmente, segue-se a definição de coloração e coloração própria dos vértices de um grafo.

Definição 19.3 (Coloração de vértices e coloração própria de vértices). *Dado um grafo arbitrário G , designa-se por k -coloração dos vértices de G uma função sobrejectiva*

$$c : V(G) \mapsto \{1, \dots, k\}.$$

A coloração c diz-se própria se para cada $xy \in E(G)$ se verifica $c(x) \neq c(y)$.

Como consequência, uma k -coloração própria dos vértices de um grafo G sem lacetes é equivalente à partição do conjunto dos seus vértices em k subconjuntos independentes (V_1, V_2, \dots, V_k) , alguns dos quais podem ser vazios. Em geral, quando nada se diz em contrário, designamos as k -colorações próprias simplesmente por k -colorações. É claro que um grafo sem lacetes G admite uma k -coloração se e só se o seu grafo de suporte admite uma k -coloração. Como consequência, para problemas de coloração de vértices em grafos, basta considerar grafos simples. Note-se que um grafo simples admite uma 1-coloração se e só se é um grafo nulo (isto é, sem arestas) e admite uma 2-coloração se e só se é bipartido.

Dado um grafo arbitrário G , a determinação de uma coloração de vértices própria pode facilmente obter-se recorrendo, por exemplo, ao seguinte algoritmo:

Algoritmo guloso (*greedy*) para coloração de vértices*Dados de entrada:* grafo G ;*Resultados de saída:* uma coloração própria dos vértices de G ;Seja $V(G) = \{v_1, v_2, \dots, v_{\nu(G)}\}$.Para $i = 1, 2, \dots, \nu(G)$ colorir v_i com a menor cor possível.

Porém, para um valor fixo de k , verificar se um grafo admite uma k -coloração própria pode tornar-se muito mais difícil, em particular, se pretendermos determinar o menor k para o qual tal acontece.

Definição 19.4 (Número cromático). *O menor k para o qual o grafo G admite uma k -coloração própria designa-se por número cromático de G e denota-se por $\chi(G)$.*

Exemplo 19.4. Vamos determinar $\chi(G)$, $\omega(G)$ e $\Delta(G)$ para os seguintes grafos simples G :

1. grafo completo K_n ,
2. ciclo de comprimento par C_{2n} ,
3. ciclo de comprimento ímpar C_{2n+1} .

Solução.

1. Se G é o grafo completo K_n , então $V(G)$ é uma clique. Assim, $\omega(G) = n$, todos os vértices do grafo têm um mesmo grau, pelo que $\Delta(G) = n - 1$, e uma vez que quaisquer dois vértices são adjacentes, todos têm cores distintas, donde $\chi(G) = n$. Como consequência,

$$\omega(G) = \chi(G) = \Delta(G) + 1.$$

2. Se G é um ciclo do comprimento par, C_{2n} , então $\omega(G) = 2$, $\Delta(G) = 2$ e $\chi(G) = 2$. Logo,

$$\omega(G) = \chi(G) < \Delta(G) + 1.$$

3. Se G é um ciclo do comprimento ímpar, C_{2n+1} , então $\omega(G) = 2$, $\Delta(G) = 2$ e $\chi(G) = 3$. Consequentemente,

$$\omega(G) < \chi(G) = \Delta(G) + 1. \quad \square$$

O teorema a seguir estabelece a validade geral do minorante e do majorante determinados para o número cromático do caso particular dos grafos do exemplo anterior.

Teorema 19.3. Dado um grafo arbitrário G ,

$$\omega(G) \leq \chi(G) \leq \Delta(G) + 1.$$

Demonstração. No grafo G existe um subgrafo induzido $H \cong K_{\omega(G)}$ cuja coloração própria dos vértices exige $\omega(G)$ cores (ver Exemplo 19.4). Logo, $\omega(G) \leq \chi(G)$. Por outro lado, o algoritmo guloso (*greedy*) não utiliza mais do que $\Delta(G) + 1$ cores. Logo, $\chi(G) \leq \Delta(G) + 1$. \square

Definição 19.5 (Grafo perfeito). *Designa-se por grafo perfeito todo o grafo G tal que para cada $U \subseteq V(G)$*

$$\chi(G[U]) = \omega(G[U]).$$

O teorema do grafo perfeito, publicado em 1972 por Lovász [68], estabelece que um grafo é perfeito se e só se o seu complementar é um grafo perfeito. Adicionalmente, se G é um grafo perfeito então, tendo em conta o Teorema 19.10 (mais adiante), qualquer que seja o subgrafo induzido H , podemos concluir que $\nu(H) \leq \alpha(G)\omega(G)$ (note-se que neste caso $\chi(H) = \omega(H)$). Na verdade, em alternativa ao teorema do grafo perfeito, Lovász provou que um grafo G é perfeito se e só se qualquer que seja o subgrafo induzido H , $\nu(H) \leq \alpha(H)\omega(H)$.

A famosa conjectura do grafo perfeito, proposta por Berge em 1966, afirma que G é um grafo perfeito se e só se nem G nem o seu complementar contém qualquer ciclo induzido de comprimento ímpar maior ou igual a 5. Os grafos tais que nem eles nem os complementares contêm ciclos induzidos de comprimento ímpar maior ou igual a 5 designam-se por *grafos de Berge*. Já se sabia que (como facilmente se conclui²) todos os grafos perfeitos são grafos de Berge, o recíproco, porém, onde se clama que todos os grafos de Berge são grafos perfeitos, só muito recentemente se provou³.

São exemplos de grafos perfeitos, os grafos bipartidos, os *grafos intervalares* (que são grafos cujos vértices são intervalos e dois vértices são adjacentes se os correspondentes intervalos têm intersecção não vazia) e os *grafos de comparabilidade* de conjuntos parcialmente ordenados (ver Definição 17.7). Em relação a estes casos, de acordo com o teorema do grafo perfeito, é claro que são ainda perfeitos os respectivos grafos complementares.

Dado uma conjunto parcialmente ordenado $P = (X, \preceq_P)$ e sendo $GC(P)$ o seu grafo de comparabilidade, deve observar-se ainda que, de acordo com a definição de comprimento e largura de um conjunto parcialmente ordenado, $\text{comprimento}(P) = \omega(GC(P)) - 1$, e $\text{largura}(P) = \alpha(GC(P))$. Por outro lado, apesar da determinação do número de independência e, consequentemente, a determinação do número de clique ser, em geral, um problema *NP*-completo, tal não acontece no caso dos grafos de comparabilidade que são grafos perfeitos para os quais existem algoritmos polinomiais para a determinação do número de independência e do número de clique.

Seguem-se mais alguns resultados sobre o número cromático de um grafo.

Teorema 19.4. Qualquer que seja o grafo G ,

$$\chi(G) \leq \max_{U \subseteq V(G)} \delta(G[U]) + 1.$$

Demonstração. Suponha que G tem ordem n e seja

$$k = \max_{U \subseteq V(G)} \delta(G[U]).$$

Seja v_ν um vértice de G tal que $d_G(v_\nu) \leq k$ e $H_{\nu-1} = G - \{v_\nu\}$. Por hipótese, $H_{\nu-1}$ tem um vértice de grau não superior a k . Seja $v_{\nu-1}$ um desses vértices e seja $H_{\nu-2} = H_{\nu-1} - \{v_{\nu-1}\}$, isto é, $H_{\nu-2} = G - \{v_\nu, v_{\nu-1}\}$. Continuando este processo, obtém-se uma sequência de vértices de G , v_ν, \dots, v_1 , tal que v_j é adjacente a um máximo de k vértices de entre os vértices v_{j-1}, \dots, v_1 . Consequentemente, para os colorir, no máximo, são necessárias $k + 1$ cores. \square

Se G é um grafo conexo não regular, então

$$\max_{U \subseteq V(G)} \delta(G[U]) \leq \Delta(G) - 1$$

e, consequentemente, a partir do Teorema 19.4, podemos concluir a desigualdade $\chi(G) \leq \Delta(G)$. O teorema de Brooks (1941) [18], a seguir, estende esta desigualdade aos grafos conexos regulares que não são completos nem ciclos de comprimento ímpar.

²Ver Exercício 19.3.

³Esta prova foi apresentada num Encontro Científico realizado entre 30 de Outubro e 3 de Novembro de 2002, no *American Institute of Mathematics*, em Palo Alto, Califórnia, num artigo assinado por Maria Chudnovsky, Neil Robertson, Paul Seymour e Robin Thomas. A versão preliminar deste artigo, distribuída pelos participantes, tinha 148 páginas.

Teorema 19.5 (Brooks). *Sendo G um grafo conexo, se G não é completo nem um ciclo de comprimento ímpar, então $\chi(G) \leq \Delta(G)$.*

Demonstração. No caso de G ser não regular já se concluiu que $\chi(G) \leq \Delta(G)$, pelo que resta fazer a prova para o caso regular. Adicionalmente, sem perda de generalidade, vamos assumir que G é pelo menos 2-conexo⁴ e que $\Delta(G) \geq 3$, uma vez que um grafo regular tal que $\Delta(G) = 2$, nas condições da hipótese, é um ciclo de comprimento par, logo com número cromático igual a 2. Assim, basta considerar o caso dos grafos Δ -regulares, com $\Delta \geq 3$, 2-conexos, os quais vamos dividir em grafos 3-conexos e em grafos que não são 3-conexos.

- Suponha que G é 3-conexo, com $n = \nu(G)$. Uma vez que $G \neq K_n$, é possível escolher um vértice v_n com dois vizinhos mutuamente não adjacentes, v_1 e v_2 (ver Figura 19.3), verificando-se que $G - \{v_1, v_2\}$ é conexo, $v_1 v_2 \notin E(G)$, mas $v_1 v_n, v_2 v_n \in E(G)$. Logo, defina-se recursivamente em $G - \{v_1, v_2\}$ a sequência de vértices v_{n-1}, v_{n-2}, \dots de tal forma que cada vértice v_i é adjacente a pelo menos um vértice da subsequência v_{i+1}, \dots, v_n (o que pode ser feito, caso contrário $G - \{v_1, v_2\}$ não seria conexo). Depois de se atribuir a mesma cor aos vértices v_1 e v_2 , podemos colorir, sequencialmente, os vértices v_3, v_4, \dots, v_{n-1} , utilizando no máximo Δ cores (dado que cada vértice v_i é adjacente a no máximo $\Delta - 1$ vértices previamente coloridos em v_1, v_2, \dots, v_{i-1}). Finalmente, sendo v_n adjacente aos vértices v_1 e v_2 (que têm a mesma cor) e a no máximo $\Delta - 2$ outros vértices, resta pelo menos uma das Δ cores para colorir v_n .

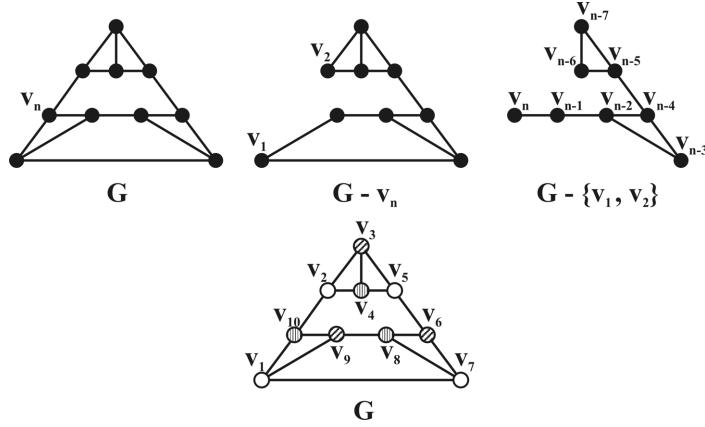


Figura 19.3: Ilustração da demonstração do teorema de Brooks.

- Suponha que G é 2-conexo mas não é 3-conexo e sejam u e v_n dois vértices tais que $G - \{u, v_n\}$ não é conexo. Então, o grafo $G - \{v_n\}$ é 1-conexo, mas não 2-conexo, pelo que tem pelo menos dois blocos e, pelo menos, dois destes blocos são blocos extremos (ver Definição 13.6), o que significa que cada um deles contém exactamente um vértice de corte. Assim, o vértice v_n é adjacente a pelo menos um vértice (que não é de corte) em cada bloco extremo, caso contrário haveria pelo menos um bloco extremo com um vértice de corte em G (o que contradiz o facto de G ser 2-conexo). Assim, sendo v_1 e v_2 dois vértices adjacentes a v_n , pertencentes a blocos extremos distintos (em $G - \{v_n\}$), escolhendo a sequência de vértices v_{n-1}, v_{n-2}, \dots tal como no caso 3-conexo e o mesmo modo de coloração dos vértices chegamos ao mesmo resultado. \square

⁴No caso dos grafos 1-conexos (ver Definição 13.5), G , sendo $G = G_1 \cup \dots \cup G_p$, onde G_1, \dots, G_p são os seus blocos (ver Definição 13.6), $\chi(G) = \max\{\chi(G_j), j = 1, \dots, p\}$.

À primeira vista tudo indica que a existência de grafos com elevado número cromático está directamente relacionada com a existência, nesses grafos, de subgrafos completos de elevada cardinalidade. O teorema a seguir, publicado por Zykov⁵ em 1949, porém, contraria uma tal relação, ao garantir a existência de grafos com cintura superior a três (i.e., sem triângulos) e com número cromático arbitrário.

Teorema 19.6 (Zykov). *Para cada $k \in \mathbb{N}$, existe um grafo G_k tal que $g(G_k) > 3$ e $\chi(G_k) = k$.*

Demonstração. Vamos fazer a prova por indução sobre k , sabendo que para $k = 1$ o resultado é trivialmente verdadeiro. Seja $k > 1$ e suponha que o resultado é verdadeiro para G_1, \dots, G_{k-1} . Considerem-se cópias disjuntas destes grafos e seja $V = V(G_1) \times \dots \times V(G_{k-1})$ o conjunto de novos vértices definidos pelos $(k-1)$ -uplos de vértices obtidos pela selecção de um vértice de cada um dos grafos G_1, \dots, G_{k-1} . Assim, G_k é obtido de G_1, \dots, G_{k-1} e V , ligando cada vértice de V aos $k-1$ vértices que lhe correspondem em G_1, \dots, G_{k-1} , um em cada G_i , pelo que

$$\chi(G) \leq k. \quad (19.2)$$

Por outro lado, em G_1 existe um vértice v_1 com uma certa cor c_1 , em G_2 existe um vértice v_2 com uma cor $c_2 \neq c_1$ (dado que $\chi(G_2) = 2$), em G_3 existe um vértice v_3 com uma cor $c_3 \notin \{c_1, c_2\}$ (dado que $\chi(G_3) = 3$), etc. Consequentemente, o vértice $v \in V$ adjacente a v_1, \dots, v_{k-1} , tem de ter uma cor distinta de c_1, \dots, c_{k-1} , pelo que

$$\chi(G) \geq k. \quad (19.3)$$

Tendo em conta as desigualdades (19.2) e (19.3) conclui-se que $\chi(G_k) = k$. \square

Teorema 19.7 (Gaddum e Nordthaus). *Dado um grafo G de ordem $\nu = \nu(G)$, verifica-se a desigualdade*

$$\chi(G^c) + \chi(G) \leq \nu + 1.$$

Demonstração. Vamos fazer a prova por indução sobre o número de vértices, tendo em conta que o resultado é trivialmente verdadeiro para grafos de ordem 1 e 2. Suponha que o resultado é verdadeiro para grafos com menos vértices do que os de G e que $\nu(G) \geq 2$. Sendo G' o subgrafo obtido de G por eliminação de um vértice x , vem

$$\chi(G) \leq \chi(G') + 1, \quad (19.4)$$

$$\chi(G^c) \leq \chi(G'^c) + 1 \quad (19.5)$$

Se a igualdade se verifica em (19.4) e em (19.5), então $d_G(x) \geq \chi(G')$ e $d_{G^c}(x) \geq \chi(G'^c)$. Consequentemente,

$$\chi(G^c) + \chi(G) = \chi(G') + \chi(G'^c) + 2 \leq d_{G^c}(x) + d_G(x) + 2 = \nu(G) + 1.$$

Suponha-se que a igualdade não se verifica simultaneamente em (19.4) e (19.5). Então $\chi(G^c) + \chi(G) \leq \chi(G'^c) + \chi(G') + 1 \leq \nu(G') + 1 + 1 = \nu(G) + 1$. \square

Para se concluir que o majorante determinado no Teorema 19.7 é atingido, basta exhibir o par de grafos complementares, G e G^c , representados na Figura 19.4 para os quais se obtém $\chi(G) = 5$ e $\chi(G^c) = 4$, pelo que $\chi(G^c) + \chi(G) = 9 = \nu(G) + 1$.

Corolário 19.8. *Dado um grafo arbitrário G de ordem $\nu = \nu(G)$, verifica-se a desigualdade*

$$\chi(G)\chi(G^c) \leq \left\lfloor \left(\frac{\nu + 1}{2} \right)^2 \right\rfloor.$$

⁵Alexander Alexandrovitch Zykov, matemático russo.

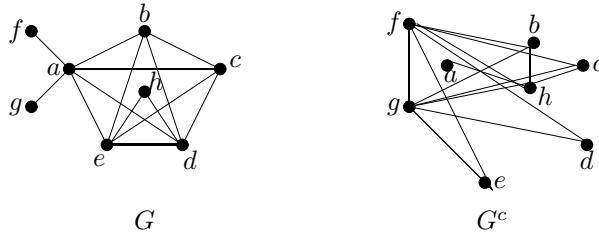


Figura 19.4: Grafos para os quais o majorante do Teorema 19.7 é atingido.

Demonstração.

$$\begin{aligned} 4\chi(G)\chi(G^c) &\leq 4\chi(G)\chi(G^c) + (\chi(G) - \chi(G^c))^2 = (\chi(G) + \chi(G^c))^2 \\ &\leq (\nu + 1)^2. \end{aligned}$$

□

Tal como anteriormente, também se verifica que o majorante é atingido, dado que para o grafo G representado na Figura 19.4 se obtém

$$20 = \chi(G)\chi(G^c) \leq \left\lfloor \left(\frac{\nu(G) + 1}{2} \right)^2 \right\rfloor = 20.$$

O teorema a seguir estabelece um minorante e um majorante para o número cromático de um grafo em função do número de vértices e arestas.

Teorema 19.9. *Para qualquer grafo conexo G de ordem $\nu = \nu(G)$ e $\varepsilon = \varepsilon(G)$,*

$$\left\lceil \frac{\nu^2}{\nu^2 - 2\varepsilon} \right\rceil \leq \chi(G) \leq \left\lfloor \sqrt{2\varepsilon} + 1 \right\rfloor. \quad (19.6)$$

Demonstração. Vamos provar primeiro a desigualdade esquerda e depois a desigualdade direita.

- Prova da desigualdade esquerda. Seja $\chi(G) = k$ e sejam S_1, \dots, S_k os conjuntos de vértices com as cores c_1, \dots, c_k . Ordenando os vértices convenientemente e denotando os conjuntos de índices associados aos vértices de S_i , para $i = 1, \dots, k$, por $J(S_i)$, verifica-se que a matriz de adjacência de G , A_G , toma o seguinte aspecto:

$$A_G = \begin{pmatrix} J(S_1) & J(S_2) & \cdots & J(S_k) \\ J(S_1) & 0 & \cdots & \cdots \\ J(S_2) & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ J(S_k) & \cdots & \cdots & 0 \end{pmatrix}.$$

Seja ν_i o número de vértices do conjunto S_i ($\nu_i = |S_i|$), para $i = 1, \dots, k$ e seja N_0 e N_1 , respectivamente, o número de entradas nulas e entradas unitárias da matriz A_G . Então, por um lado, tendo em conta a desigualdade de Chebyshev (ver Exemplo 2.12),

$$N_0 \geq \sum_{i=1}^k \nu_i^2 \geq \frac{\left(\sum_{i=1}^k \nu_i \right)^2}{k} = \frac{\nu^2}{k}$$

e, por outro lado, $N_1 = 2\varepsilon$, uma vez que a soma das componentes unitárias de cada linha (ou coluna) da matriz corresponde ao grau do vértice que lhe está associado. Consequentemente, o número total de entradas da matriz A_G vem dado por

$$\nu^2 = N_0 + N_1 \geq \frac{\nu^2}{k} + 2\varepsilon \Leftrightarrow \chi(G) = k \geq \frac{\nu^2}{\nu^2 - 2\varepsilon}.$$

- Prova da desigualdade direita. Uma vez que o conjunto de vértices $V(G)$ se parte em $\chi(G)$ conjuntos independentes, entre cada par dos quais existe pelo menos uma aresta, podemos concluir as desigualdades

$$\varepsilon \geq \frac{\chi(G)(\chi(G) - 1)}{2} \Rightarrow 2\varepsilon > (\chi(G) - 1)^2,$$

onde se obtém a desigualdade pretendida. \square

Note-se que o triângulo verifica ambas as desigualdades (19.6) na forma de igualdade.

Teorema 19.10. *Dado um grafo arbitrário G de ordem $\nu = \nu(G)$, verificam-se as seguintes desigualdades:*

$$\chi(G) + \alpha(G) - 1 \leq \nu \leq \chi(G)\alpha(G).$$

Demonstração. Sendo G tal que $V(G) = \{v_1, \dots, v_\nu\}$ e considerando a coloração própria dos vértices de G , com $\chi(G)$ cores,

$$c : V(G) \mapsto \{1, \dots, \chi(G)\},$$

podemos definir a relação de ordem parcial $\preceq_G \subset V(G) \times V(G)$ tal que

$$v_i \preceq_G v_j \text{ sse } c(v_i) = c(v_j) \wedge i \leq j.$$

Nestas condições, é imediato que a largura do conjunto parcialmente ordenado obtido é igual a $\chi(G)$ e o comprimento é não superior a $\alpha(G) - 1$. Logo, por aplicação do Corolário 7.19 (que é consequência do lema de Dilworth), vem

$$\nu \leq \alpha(G)\chi(G).$$

Adicionalmente, supondo que aos vértices de um estável máximo, S , é atribuída uma cor, então aos restantes $\nu - \alpha(G)$ vértices poder-se-ão atribuir $\nu - \alpha(G)$ cores, pelo que $\chi(G) \leq \nu - \alpha(G) + 1 \Leftrightarrow \chi(G) + \alpha(G) - 1 \leq \nu$. \square

No caso do Teorema 19.10, deve observar-se que a desigualdade da esquerda se verifica na forma de igualdade para os grafos cujos vértices podem ser partidos em dois subconjuntos V_1 e V_2 tais que um é uma clique, o outro um conjunto independente de vértices e existe uma aresta entre qualquer vértice de V_1 e qualquer vértice de V_2 . Por sua vez, a desigualdade da direita verifica-se, por exemplo, para grafos completos. Vamos terminar esta secção com um algoritmo para a determinação de uma k -coloração dos vértices de um grafo G , com k mínimo.

Algoritmo de coloração dos vértices de um grafo G

Dados de entrada: grafo G ;

Resultados de saída: coloração dos vértices de G ;

1. Determinar o conjunto \mathcal{W} de todos os conjuntos independentes maximais do grafo G , pelo que,

$$\bigcup_{W \in \mathcal{W}} W = V(G).$$

2. Determinar um subconjunto $\mathcal{W}^* \subseteq \mathcal{W}$ de cardinalidade mínima, tal que $\mathcal{W}^* = \{W_1, W_2, \dots, W_k\}$ e $\bigcup_{i=1}^k W_i = V(G)$.
3. Partir $V(G)$ nas cores C_1, C_2, \dots, C_k , de tal modo que

$$\begin{aligned}C_1 &= W_1, \\C_2 &= W_2 \setminus W_1, \\C_3 &= W_3 \setminus (W_1 \cup W_2), \\&\dots \\C_k &= W_k \setminus (W_1 \cup \dots \cup W_{k-1}).\end{aligned}$$

Na próxima secção, introduzem-se os procedimentos para a determinação de todos os conjuntos independentes maximais (passo 1 do algoritmo) e para a determinação da subfamília \mathcal{W}^* (passo 2 do algoritmo).

19.2.1 Uma aplicação das funções booleanas

Vamos aplicar a teoria das funções booleanas (ver Secção 10.4) na determinação da família de todos os conjuntos independentes de vértices maximais de um grafo G e também na determinação de uma subfamília com o menor número de conjuntos cuja união contenha $V(G)$.

Observe-se que cada função booleana n -ária pode ser representada (definida) por uma 2-coloração (não necessariamente própria) dos vértices de um n -cubo, atribuindo as cores 0 e 1 aos respectivos vértices (ver exemplo a seguir).

Exemplo 19.5. Vamos colorir os vértices de Q_2 com duas cores, considerando a função booleana $f(x_1, x_2) = x_1 \vee x_2$.

Solução. Tendo em conta que $f(0, 0) = 0$ e $f(0, 1) = f(1, 0) = f(1, 1) = 1$, obtém-se a coloração dos vértices apresentada na Figura 19.5, onde os vértices de cor branca correspondem ao valor 0 e os de cor negra ao valor 1 (deve observar-se que esta coloração não é própria). \square

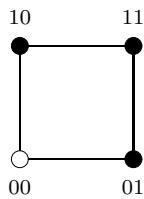


Figura 19.5: Coloração dos vértices de Q_2 a partir da função booleana $f(x_1, x_2) = x_1 \vee x_2$.

Para a determinação de colorações próprias de vértices com um número mínimo de cores, recorrendo à utilização de funções booleanas, é particularmente importante relembrar as funções booleanas monótonas (ver Definição 10.9), o vector reduzido minimal (Definição 10.11) e o Teorema 10.11 da representação de formas disjuntivas reduzidas mínimas de funções booleanas monótonas. Adicionalmente, é especialmente útil para a redução de uma função booleana à sua forma disjuntiva reduzida mínima ter presente as propriedades das álgebras de Boole

$$a + a = a, \quad a + ab = a, \quad (a + b)(a + c) \cdots (a + d) = a + (bc \cdots d)$$

e as respectivas propriedades duais

$$aa = a, \quad a(a + b) = a; \quad ab + ac + \cdots + ad = a(b + c + \cdots + d).$$

O algoritmo que a seguir se indica determina todos os conjuntos independentes maximais de um grafo G , com base na teoria das funções booleanas monótonas. Com efeito, com este algoritmo, a partir da matriz de incidência aresta vértice do grafo G , define-se uma função booleana que posteriormente é representada na forma disjuntiva reduzida mínima, a qual nos permite determinar todos os conjuntos independentes maximais de vértices de G .

Algoritmo para determinar todos os conjuntos independentes maximais de um grafo

Dados de entrada: matriz de incidência, $M_G = (m_{ij})$, de um grafo G ;

Resultados de saída: família de todos os conjuntos independentes maximais de G ;

1. A partir de matriz M_G , definir a função booleana

$$f_G(x_1, \dots, x_\nu) = \prod_{j=1}^{\varepsilon} \sum_{i=1}^{\nu} m_{ij} x_i.$$

2. Reduzir f_G à forma disjuntiva reduzida mínima.
3. Tendo em conta que cada um dos termos da forma disjuntiva reduzida mínima de f_G define uma cobertura mínima de G e que todos os termos definem todas as coberturas, determinar os correspondentes conjuntos independentes maximais de G .

Uma vez determinada a família de todos os conjuntos independentes maximais de um grafo G , estamos interessados em obter uma subfamília destes conjuntos, com um número mínimo de elementos cuja união seja $V(G)$. Com este objectivo, vamos recorrer ao algoritmo a seguir indicado, o qual, dada uma família \mathcal{F} de conjuntos cuja união é F , que designamos por *cobertura de F* , determina todas as *subcoberturas minimais* de F (ou seja, todas as subfamílias de conjuntos de \mathcal{F} cuja união é F , relativamente a cada uma das quais, retirando um elemento, a respectiva união deixa de ser F). Assim, conhecidas todas estas subcoberturas minimais de F , podemos escolher uma de menor cardinalidade.

Algoritmo de determinação de todas as subcoberturas minimais de uma cobertura de um conjunto

Dados de entrada: família de conjuntos $\mathcal{W} = \{W_1, W_2, \dots, W_k\}$;

Resultados de saída: todas as subcoberturas minimais do conjunto $\{w_1, w_2, \dots, w_n\} = \bigcup_{j=1}^k W_j$;

1. A partir de família \mathcal{W} , determinar a matriz $\mathbf{B} = (b_{ij})$ de dimensão $n \times k$ tal que

$$b_{ij} = \begin{cases} 1, & \text{se } w_i \in W_j, \\ 0, & \text{caso contrário.} \end{cases}$$

2. A partir de matriz \mathbf{B} , definir a função booleana

$$f_W(x_1, x_2, \dots, x_k) = \prod_{i=1}^n \sum_{j=1}^k b_{ij} x_j.$$

3. Reduzir f_W à forma disjuntiva reduzida mínima.
 4. Escolher um termo com o menor número de factores de entre os termos da forma disjuntiva reduzida mínima de f_W (os quais, no seu conjunto, representam todas as subcoberturas mínimas da cobertura \mathcal{W}).
-
-

Exemplo 19.6. Vamos determinar uma coloração própria dos vértices do grafo representado na Figura 19.6, com recurso a um número mínimo de cores.

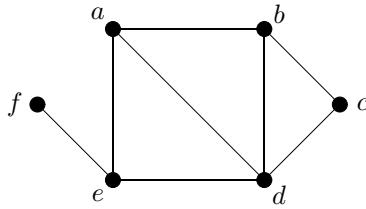


Figura 19.6: Grafo do Exemplo 19.6

Solução. Segue-se a aplicação do algoritmo introduzido na secção anterior.

1. Começando por determinar todos os conjuntos independentes maximais de vértices, vamos definir a função booleana

$$f_G(a, b, c, d, e, f) = (a + b)(a + d)(a + e)(b + c)(b + d)(c + d)(d + e)(e + f),$$

cujos factores correspondem aos extremos de todas as arestas. Seguidamente, reduzindo-se esta função à sua forma disjuntiva reduzida mínima, obtém-se

$$\begin{aligned} f_G(a, \dots, f) &= (a + bde)(b + c)(d + bce)(e + f) \\ &= (ab + bde + ac + bcde)(de + bce + df + bcef) \\ &= abde + bde + acde + bcde + abce + bcde + bcde + abce + bcde \\ &\quad + abdf + bdef + acdf + bcdef + abcef + bcdef + abcef + bcdef \\ &= bde + acde + abce + abdf + bdef + acdf \\ &= bde + acde + abce + abdf + acdf \\ &= \text{(sequência de 5 grafos)} \end{aligned}$$

onde a última expressão obtida é substituída pela sequência dos grafos nos quais os vértices que correspondem aos conjuntos de cobertura minimais, definidos por cada um dos termos, são pintados a preto. Logo, tal como se indica na Figura 19.7, obtém-se cinco pares de conjuntos independentes maximais e de cobertura minimais (os vértices assinalados a preto definem conjuntos de cobertura minimais e os assinalado a branco conjuntos independentes maximais).

2. Denotando estes conjuntos independentes maximais do grafo G por $W_1 = \{a, c, f\}$, $W_2 = \{b, f\}$, $W_3 = \{d, f\}$, $W_4 = \{c, e\}$ e $W_5 = \{b, e\}$, vamos determinar todas as subcoberturas mínimas da

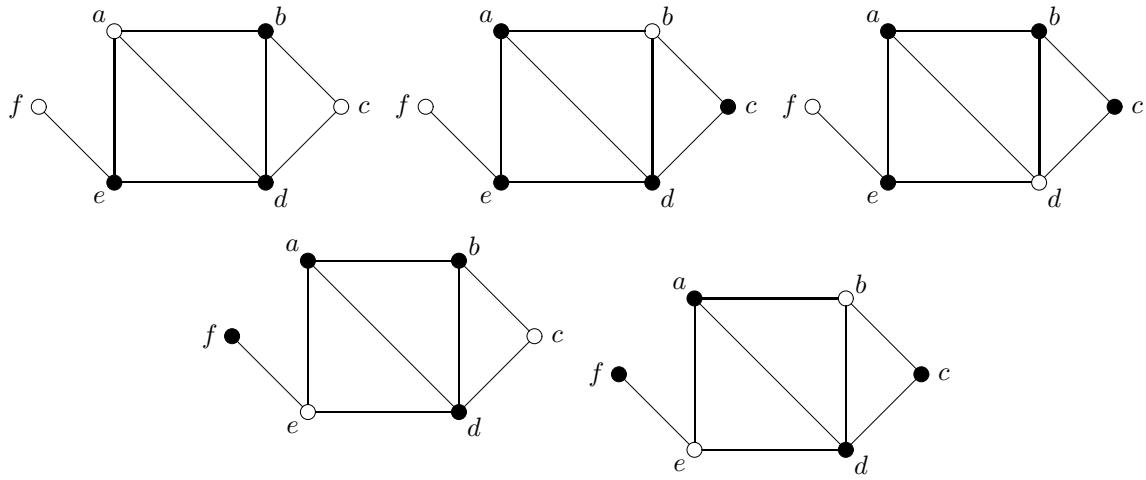


Figura 19.7: Representação de todos os conjuntos independentes maximais e de cobertura mínimas do grafo da Figura 19.6.

cobertura $\{W_1, \dots, W_5\}$. Assim, uma vez que a matriz \mathbf{B} é tal que

$$\mathbf{B} = \begin{pmatrix} & W_1 & W_2 & W_3 & W_4 & W_5 \\ a & 1 & 0 & 0 & 0 & 0 \\ b & 0 & 1 & 0 & 0 & 1 \\ c & 1 & 0 & 0 & 1 & 0 \\ d & 0 & 0 & 1 & 0 & 0 \\ e & 0 & 0 & 0 & 1 & 1 \\ f & 1 & 1 & 1 & 0 & 0 \end{pmatrix},$$

obtém-se a função booleana

$$f_W(x_1, x_2, x_3, x_4, x_5) = (x_1)(x_2 + x_5)(x_1 + x_4)(x_3)(x_4 + x_5)(x_1 + x_2 + x_3).$$

Reduzindo esta função booleana à forma disjuntiva reduzida mínima

$$\begin{aligned} f_W &= (x_1x_3)(x_2 + x_5)(x_4 + x_1x_5)(x_1 + x_2 + x_3) \\ &= (x_1x_3)[(x_2 + x_5)(x_2 + x_1) + (x_3)(x_2 + x_5)](x_4 + x_1x_5) \\ &= (x_1x_3)[(x_2 + x_5x_1) + (x_3)(x_2 + x_5)](x_4 + x_1x_5) \\ &= (x_1x_3)[(x_2x_4 + x_5x_1) + (x_3)(x_2 + x_5)(x_4 + x_1x_5)] \\ &= x_1x_3x_5 + x_1x_2x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_4x_5 + x_1x_2x_3x_5 + x_1x_3x_5 \\ &= x_1x_3x_5 + x_1x_2x_3x_4 \end{aligned}$$

podemos concluir que os conjuntos $W_1 = \{a, c, f\}$, $W_3 = \{d, f\}$ e $W_5 = \{b, e\}$ constituem uma subcobertura mínima da cobertura $\mathcal{W} = \{W_1, W_2, W_3, W_4, W_5\}$.

- Finalmente, com recurso ao algoritmo de coloração de vértices de um grafo, obtém-se a coloração definida pelos subconjuntos de vértices

$$\begin{aligned} C_1 &= W_1 = \{a, c, f\} \\ C_2 &= W_3 \setminus W_1 = \{d\} \\ C_3 &= W_5 \setminus (W_1 \cup W_3) = \{b, e\} \end{aligned}$$

□

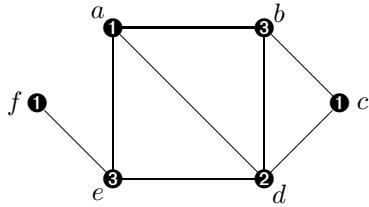


Figura 19.8: Coloração dos vértices do grafo do Exemplo 19.6.

19.2.2 Polinómios cromáticos

Um dos problemas muito estudados diz respeito à determinação do número de diferentes colorações de vértices de um grafo com recurso a um número fixo de cores. Whitney⁶ [105] em 1932 mostrou que o número de colorações próprias distintas dos vértices de um grafo, em função do número de cores, é uma função polinomial. Por sua vez, Birkhoff⁷ e Lewis⁸ [14], num estudo realizado em 1946, baptizaram esta função de polinómio cromático.

Dado um grafo G e um conjunto de λ cores, vamos definir a função $f(G, \lambda)$ como sendo o número de colorações (próprias) de vértices que é possível realizar em G utilizando λ cores. Logo, se $\lambda < \chi(G)$, então $f(G, \lambda) = 0$ e

$$\chi(G) = \min_{\lambda \in \mathbb{N}: f(G, \lambda) > 0} \lambda.$$

É fácil concluir que $f(K_\nu, \lambda) = \lambda(\lambda - 1) \cdots (\lambda - (\nu - 1))$ e $f(K_\nu, \lambda) > 0$, para $\nu \leq \lambda \in \mathbb{N}$. Com efeito, começando por escolher um vértice arbitrário, podemos colori-lo com qualquer das λ cores, para o segundo vértice escolhido a sua coloração pode ser feita com qualquer das $\lambda - 1$ cores que restam, etc. Por exemplo,

$$f(K_3, \lambda) = \lambda(\lambda - 1)(\lambda - 2) \quad (19.7)$$

$$f(K_\nu^c, \lambda) = \lambda^\nu. \quad (19.8)$$

É precisamente a função $f(G, \lambda)$ que se designa por *polinómio cromático* de G . No que se segue, todas as colorações são colorações próprias, as quais são designadas, simplesmente, por colorações.

Teorema 19.11. *Se G é um grafo simples, então $\forall e \in E(G)$*

$$f(G, \lambda) = f(G \setminus e, \lambda) - f(G/e, \lambda),$$

onde $G \setminus e$ e G/e denotam os grafos obtidos de G depois das operações de eliminação e contracção (ver Definição 15.3) da aresta e , respectivamente.

Demonstração. Seja $e = uv \in E(G)$. Tendo em atenção que $f(G \setminus e, \lambda)$ denota o número de colorações de $G \setminus e$ com recurso a λ cores, podemos concluir que esse número é igual à soma do número de colorações de $G \setminus e$, com u e v recebendo a mesma cor (o qual é igual ao número de colorações de G/e) mais o número de colorações de $G \setminus e$, com u e v recebendo cores distintas (o qual é igual ao número de colorações de G). Logo, $f(G \setminus e, \lambda) = f(G, \lambda) + f(G/e, \lambda)$. \square

É imediato concluir que dados dois grafos disjuntos G e H , denotando a sua união por $G + H$, $f(G + H, \lambda) = f(G, \lambda)f(H, \lambda)$.

Exemplo 19.7. Denotando por C_r um ciclo com r vértices, por P_s um caminho com s vértices e por kH a união de k cópias de H , vamos determinar o polinómio cromático do grafo C_4 , utilizando dois métodos distintos.

⁶Hassler Whitney (1907–1989), matemático americano que trabalhou em teoria das singularidades.

⁷George David Birkhoff (1884–1944), matemático americano que trabalhou em teoria ergódica.

⁸H. W. Lewis, matemático americano que trabalhou em teoria dos polinómios.

Solução. Método 1:

$$\begin{aligned}
 f(C_4, \lambda) &= f(G \setminus xy, \lambda) - f(G/xy, \lambda) \\
 &= f(P_4, \lambda) - f(K_3, \lambda) \\
 &= f(P_4 \setminus wz, \lambda) - f(P_4/wz) - f(K_3, \lambda) \\
 &= f(2K_2, \lambda) - f(P_3, \lambda) - f(K_3, \lambda) \\
 &= f(2K_2, \lambda) - (f(P_3 \setminus yw, \lambda) - f(P_3/yw, \lambda)) - f(K_3, \lambda) \\
 &= f(2K_2, \lambda) - f(K_2 + K_1, \lambda) + f(K_2, \lambda) - f(K_3, \lambda) \\
 &= (f(K_2, \lambda))^2 - f(K_2, \lambda)f(K_1, \lambda) + f(K_2, \lambda) - f(K_3, \lambda) \\
 &= (\lambda(\lambda-1))^2 - \lambda(\lambda-1)\lambda + \lambda(\lambda-1) - \lambda(\lambda-1)(\lambda-2) \\
 &= \lambda^4 - 4\lambda^3 + 6\lambda^2 - 3\lambda.
 \end{aligned}$$

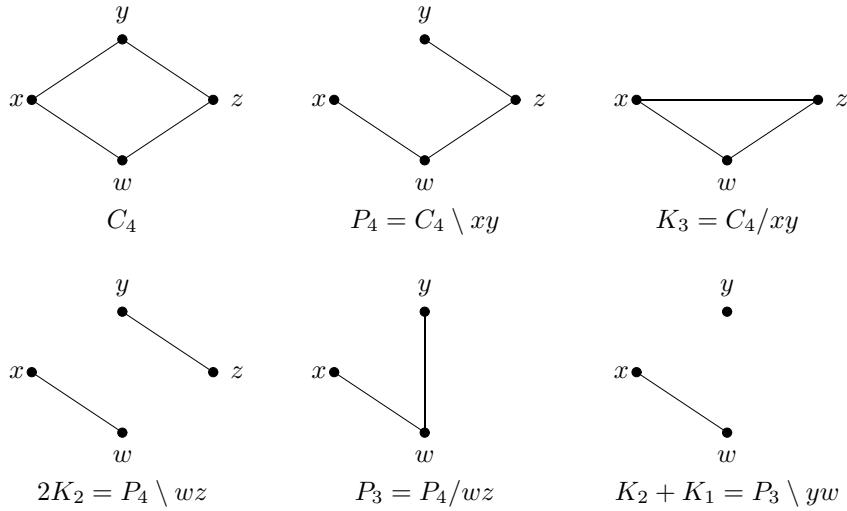


Figura 19.9: Grafos C_4 , P_4 , K_3 , $2K_2$, P_3 e $K_2 + K_1$.

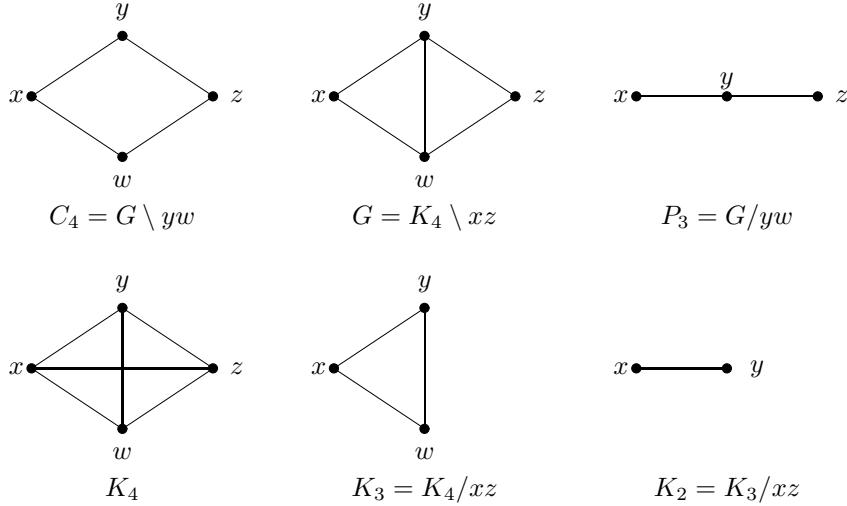
$$\begin{aligned}
 \text{Método 2: } f(G \setminus yw, \lambda) &= f(G, \lambda) + f(G/yw, \lambda) = f(K_4 \setminus xz, \lambda) + f(P_3, \lambda) \\
 &= f(K_4, \lambda) + f(K_4/xz, \lambda) + f(K_3 \setminus xz, \lambda) \\
 &= f(K_4, \lambda) + f(K_3, \lambda) + f(K_3, \lambda) + f(K_3/xz, \lambda) \\
 &= f(K_4, \lambda) + 2f(K_3, \lambda) + f(K_2, \lambda) \\
 &= \lambda^4 - 4\lambda^3 + 6\lambda^2 - 3\lambda.
 \end{aligned}$$

□

Note-se que a função $f(C_4, \lambda)$, determinada no exemplo anterior, é um polinómio mónico de grau 4 com coeficientes inteiros, no qual o coeficiente de λ^3 é igual a $-\varepsilon(G)$, o termo constante é nulo e os coeficientes alternam em sinal. Com o Teorema 19.12, a seguir, fica claro que estas características não são coincidência.

Teorema 19.12. *Dado um grafo simples G de ordem $\nu = \nu(G)$ e $\varepsilon = \varepsilon(G)$, $f(G, \lambda)$ é um polinómio mónico de grau ν em λ com coeficientes inteiros e termo constante nulo. Adicionalmente, cada coeficiente alterna em sinal e o coeficiente de $\lambda^{\nu-1}$ é $-\varepsilon$.*

Demonstração. Vamos fazer a prova por indução sobre o número de arestas ε , tendo em conta que para $\varepsilon = 0$ o resultado é trivialmente verdadeiro ($f(K_\nu^c, \lambda) = \lambda^\nu$). Suponhamos que o resultado é

Figura 19.10: Grafos C_4 , $K_4 \setminus xz$, P_3 , K_4 , K_3 e K_2 .

verdadeiro para grafos com menos do que ε arestas, com $\varepsilon \geq 1$ e seja G um grafo de ordem ν , com ε arestas e $e \in E(G)$. Então,

$$\begin{aligned} f(G \setminus e, \lambda) &= \lambda^\nu - a_{\nu-1}\lambda^{\nu-1} + a_{\nu-2}\lambda^{\nu-2} + \cdots + (-1)^{\nu-1}a_1\lambda \\ f(G/e, \lambda) &= \lambda^{\nu-1} - b_{\nu-2}\lambda^{\nu-1-1} + b_{\nu-3}\lambda^{\nu-1-2} + \cdots + (-1)^{\nu-1-1}b_1\lambda \end{aligned}$$

onde $a_1, \dots, a_{\nu-1}$ e $b_1, \dots, b_{\nu-2}$ são inteiros não negativos, $a_{\nu-1} = \varepsilon - 1$ e $b_{\nu-2} = \varepsilon - 1$. Dado que $f(G, \lambda) = f(G \setminus e, \lambda) - f(G/e, \lambda)$,

$$f(G, \lambda) = \lambda^\nu - (a_{\nu-1} + 1)\lambda^{\nu-1} + (a_{\nu-2} + b_{\nu-2})\lambda^{\nu-2} - \cdots + (-1)^{\nu-1}(a_1 + b_1)\lambda.$$

Tendo em conta que $a_{\nu-1} + 1 = \varepsilon$, podemos concluir que $f(G, \lambda)$ tem todas as propriedades pretendidas. \square

Ainda de acordo com o Teorema 19.12, podemos concluir que dado um grafo simples G , todas as raízes de $f(G, \lambda)$ são não negativas. Com efeito, uma vez que os coeficientes do polinómio cromático alternam em sinal, para $\lambda < 0$ todos os termos de $f(G, \lambda)$ têm o mesmo sinal (positivo se ν é par, negativo se ν é ímpar).

Teorema 19.13. Se G é um grafo simples de ordem $\nu = \nu(G)$, com $\varepsilon = \varepsilon(G)$ arestas e k componentes, então

$$f(G, \lambda) = \lambda^\nu - \varepsilon\lambda^{\nu-1} + \cdots + (-1)^{\nu-j}a_j\lambda^j + \cdots + (-1)^{\nu-k}a_k\lambda^k,$$

onde $a_j > 0$, para $k \leq j \leq \nu$, com $a_\nu = 1$ e $a_{\nu-1} = \varepsilon$.

Demonstração. Vamos fazer a prova por indução sobre o número de arestas ε , tendo em conta que para $\varepsilon = 0$, $f(G, \lambda) = \lambda^\nu$ e $k = \nu$. Suponha que o resultado é verdadeiro para grafos simples com menos arestas do que as de G , $\varepsilon = \varepsilon(G) > 0$ e o número de componentes de G é k . Sendo e uma aresta de G , $G \setminus e$ tem k ou $k + 1$ componentes, G/e tem k componentes e, por hipótese de indução,

$$\begin{aligned} f(G \setminus e, \lambda) &= \lambda^\nu - (\varepsilon - 1)\lambda^{\nu-1} + \cdots + (-1)^{\nu-j}b_j\lambda^j + \cdots + (-1)^{\nu-k}b_k\lambda^k \\ f(G/e, \lambda) &= \lambda^{\nu-1} + \cdots - (-1)^{\nu-j}c_j\lambda^j + \cdots - (-1)^{\nu-k}c_k\lambda^k \end{aligned}$$

onde todos os escalares b_j e c_j são positivos com a possível exceção de b_k que pode ser nulo. Logo, o resultado obtém-se fazendo $f(G, \lambda) = f(G \setminus e, \lambda) - f(G/e, \lambda)$. \square

Conclui-se assim que 0 é raiz do polinómio cromático de qualquer grafo simples G e tem multiplicidade igual ao número de componentes conexas de G . Por outro lado, se G tem pelo menos uma aresta, então 1 é também uma raiz do polinómio cromático $f(G, \lambda)$ (uma vez que, nestas condições, o número de colorações dos vértices de G com recurso a uma única cor é igual a zero). Na verdade, se G contém o subgrafo completo K_n , então $\chi(G) \geq n$ e, consequentemente, $0, 1, 2, \dots, n - 1$ são raízes do polinómio cromático $f(G, \lambda)$.

Teorema 19.14. *Um grafo simples G é uma árvore de ordem ν se e só se $f(G, \lambda) = \lambda(\lambda - 1)^{\nu-1}$.*

Demonstração. Vamos fazer a prova da condição necessária, ou seja, da implicação:

$$\text{se } G \text{ é uma árvore então } f(G, \lambda) = \lambda(\lambda - 1)^{\nu-1},$$

por indução sobre ν , tendo em conta que para $\nu = 1$ o resultado é trivialmente verdadeiro. Suponha que o resultado é verdadeiro para árvores com menos do que ν vértices e que $\nu \geq 2$. Seja G uma árvore de ordem ν e seja $e \in E(G)$ uma aresta pendente. Então, $f(G, \lambda) = f(G \setminus e, \lambda) - f(G/e, \lambda)$ e $G \setminus e$ é uma floresta com duas componentes, uma de ordem 1 e outra de ordem $\nu - 1$. Logo, $f(G \setminus e, \lambda) = \lambda(\lambda(\lambda - 1)^{\nu-2}) = \lambda^2(\lambda - 1)^{\nu-2}$ e, consequentemente,

$$\begin{aligned} f(G, \lambda) &= \lambda^2(\lambda - 1)^{\nu-2} - \lambda(\lambda - 1)^{\nu-2} \\ &= (\lambda^2 - \lambda)(\lambda - 1)^{\nu-2} \\ &= \lambda(\lambda - 1)^{\nu-1}. \end{aligned}$$

Reciprocamente, suponha que G é um grafo simples tal que $f(G, \lambda) = \lambda(\lambda - 1)^{\nu-1}$. Então,

$$f(G, \lambda) = \lambda^\nu - (\nu - 1)\lambda^{\nu-1} + \cdots + (-1)^{\nu-1}\lambda$$

e, consequentemente, G tem ν vértices e $\nu - 1$ arestas. Adicionalmente, o último termo, $(-1)^{\nu-1}\lambda$, assegura que G é conexo (tendo em conta o Teorema 19.13). Logo, G é uma árvore. \square

O Teorema 19.14 tem como consequência a existência de grafos não isomorfos com o mesmo polinómio cromático. Por exemplo, $K_{1,3}$ e P_4 não são isomorfos e têm o mesmo polinómio cromático $\lambda(\lambda - 1)^3$ (logo, o número de colorações dos vértices com λ cores é igual). Por outro lado, dado o polinómio cromático de um grafo simples conexo G de ordem $\nu = \nu(G)$,

$$f(G, \lambda) = \lambda^\nu - \varepsilon(G)\lambda^{\nu-1} + \cdots + (-1)^{\nu-j}a_j\lambda^j + \cdots + (-1)^{\nu-1}a_1\lambda,$$

da demonstração do Teorema 19.13 decorre a igualdade $a_j = b_j + c_j$, com $c_j \geq 0$, pelo que $a_j \geq b_j$, para todo o j (note-se que a_j denota o valor absoluto do j -ésimo coeficiente do polinómio cromático de G , enquanto b_j denota o valor absoluto do j -ésimo coeficiente do polinómio cromático do grafo que se obtém de G eliminando uma aresta). Assim, eliminando tantas arestas quantas as necessárias para se obter uma árvore abrangente T , obtém-se

$$f(T, \lambda) = \lambda^\nu - \varepsilon(T)\lambda^{\nu-1} + \cdots + (-1)^{\nu-j}d_j\lambda^j + \cdots + (-1)^{\nu-1}d_1\lambda,$$

com $d_j \leq a_j$, para todo o j . Porém, uma vez que (de acordo com o Teorema 19.14) $f(T, \lambda) = \lambda(\lambda - 1)^{\nu-1}$, $d_j = \binom{\nu-1}{j-1}$ e, consequentemente, podemos concluir o seguinte corolário dos Teoremas 19.13 e 19.14:

Corolário 19.15. *Se G é um grafo simples conexo com polinómio cromático*

$$f(G, \lambda) = \lambda^\nu - \varepsilon\lambda^{\nu-1} + \cdots + (-1)^{\nu-j}a_j\lambda^j + \cdots + (-1)^{\nu-1}a_1\lambda,$$

então $a_j \geq \binom{\nu-1}{j-1}$, para $1 \leq j \leq \nu$, com $a_\nu = 1$ e $a_{\nu-1} = \varepsilon$.

Seguem-se mais alguns resultados sobre polinómios cromáticos de famílias particulares de grafos simples.

Teorema 19.16. *Se C_ν é um ciclo, com $\nu = \nu(C_\nu)$ vértices, então*

$$f(C_\nu, \lambda) = (\lambda - 1)^\nu + (-1)^\nu(\lambda - 1). \quad (19.9)$$

Demonstração. Vamos fazer a prova por indução sobre o número de vértices. Se $\nu = 3$, então C_3 é o grafo completo K_3 , donde

$$f(C_3, \lambda) = \lambda(\lambda - 1)(\lambda - 2) = (\lambda - 1)^3 - (\lambda - 1).$$

Para $\nu > 3$, considere uma aresta e de C_ν .

- Eliminando a aresta e de C_ν obtém-se uma árvore cujo polinómio cromático (de acordo com o Teorema 19.14) é $f(C_\nu \setminus e, \lambda) = \lambda(\lambda - 1)^{\nu-1}$.
- Contraindo a aresta e de C_ν obtém-se um ciclo com $\nu - 1$ vértices que, por indução, tem como polinómio cromático $f(C_{\nu-1}, \lambda) = (\lambda - 1)^{\nu-1} - (-1)^\nu(\lambda - 1)$.

Logo,

$$\begin{aligned} f(C_\nu, \lambda) &= \lambda(\lambda - 1)^{\nu-1} - (\lambda - 1)^{\nu-1} + (-1)^\nu(\lambda - 1) \\ &= (\lambda - 1)^\nu + (-1)^\nu(\lambda - 1). \end{aligned}$$

□

Teorema 19.17. *Se G é a união de dois subgrafos simples, G_1 e G_2 , cuja intersecção é um grafo completo K_n , então*

$$f(G, \lambda) = \frac{f(G_1, \lambda)f(G_2, \lambda)}{\lambda(\lambda - 1) \cdots (\lambda - (n - 1))}.$$

Demonstração. Primeiro, podemos colorir os vértices de G_1 com recurso a λ cores de $f(G_1, \lambda)$ modos distintos. Seguidamente, podemos escolher cada uma das $\lambda(\lambda - 1) \cdots (\lambda - (n - 1))$ colorações possíveis para o subgrafo completo $G_1 \cap G_2$ e estende-la a G_2 . Consequentemente, temos $f(G_2, \lambda)/\lambda(\lambda - 1) \cdots (\lambda - (n - 1))$ modos de estender cada uma destas colorações particulares a todo o grafo G . □

19.2.3 Colorações parciais e Sudoku

Dado um grafo simples, G , designa-se por *coloração parcial* de G toda a coloração própria de um subconjunto de vértices $W \subseteq V(G)$, ou seja, toda a função $\kappa : W \rightarrow \{1, \dots, k\}$, tal que $ij \in E(G[W]) \Rightarrow \kappa(i) \neq \kappa(j)$. Assim, dado um grafo simples, G , com uma coloração parcial κ , uma questão que se coloca é a de saber se esta coloração pode ser estendida a uma coloração própria de todos os vértices do grafo. Ao longo desta secção, designamos uma tal extensão por *extensão cromática* de κ .

Existem muitos problemas práticos que podem ser modelados como problemas de determinação de uma extensão cromática de uma coloração parcial, como é o caso, por exemplo, do problema de afectação de frequências de transmissão a novas estações emissoras de rádio, supondo que já existem outras estações com frequências de transmissão atribuídas. Com efeito, a atribuição de frequências de transmissão a estações emissoras deve ser feita de modo que não haja sobreposição, o que, em geral, acontece quando existem postos transmissores que, não estando suficientemente afastados, têm a mesma frequência atribuída. Assim, considerando um grafo G , cujos vértices são as estações de rádio e onde dois vértices são adjacentes se a distância que separa os correspondentes postos transmissores é não superior a d (distância mínima exigida para não haver sobreposição), podemos considerar as frequências de transmissão como cores a atribuir aos vértices e as frequências já atribuídas como uma coloração parcial $\kappa : W \rightarrow \{1, \dots, k\}$. Como consequência, a distribuição de frequências pelas novas estações corresponde à determinação de uma extensão cromática de κ .

Antes de prosseguirmos, embora no Capítulo 20 se analisem, com mais detalhe, os conceitos mais gerais de menor combinatório e menor topológico, por agora, convém referir que um grafo que se obtém de um outro grafo G por operações de contracção de zero ou mais arestas (ver Definição 15.3) se designa por *contracção* de G . É fácil verificar que a relação de contracção de zero ou mais arestas é uma relação de ordem parcial no conjunto dos grafos.

Dado um grafo G , um subconjunto não vazio de vértices $W \subseteq V(G)$ e uma coloração parcial $\kappa : W \rightarrow \{1, \dots, k\}$, vamos considerar um caso especial de contracção de grafos, a designar por κ -contracção. Esta contracção obtém-se de G a partir de uma coloração arbitrária (não necessariamente própria) dos vértices em $V(G) \setminus W$, com recurso a $\lambda \geq k$ cores, contraindo todas as arestas cujos extremos têm a mesma cor e eliminando posteriormente lacetes e arestas paralelas ou com ambos os extremos em W eventualmente produzidas por esta operação de contracção. Note-se que para se fazerem estas contracções, as arestas a contrair têm no máximo um vértice extremo em W (ou seja, pertencem ao corte $\partial(W)$ ou ao subgrafo induzido por $V(G) \setminus W$) e as κ -contracções produzidas ficam com uma coloração própria dos seus vértices. Assim, dada uma coloração arbitrária dos vértices de G , respeitando a coloração parcial κ , a κ -contracção que lhe corresponde diz-se uma κ -contracção de G e, por sua vez, dadas duas κ -contracções de G , G_1 e G_2 , se G_2 se pode obter de G_1 por uma κ -contracção, diz-se que G_2 é uma κ -contracção de G_1 e escreve-se $G_2 \preceq_\kappa G_1$ (ou $G_2 \prec_\kappa G_1$, se $G_2 \neq G_1$).

Denotando por \mathcal{G}_κ o conjunto de todas as κ -contracções de G , no qual se faz distinção entre grafos isomorfos que decorrem da contracção de diferentes conjuntos de arestas, definidos por diferentes colorações não próprias dos vértices em $V(G) \setminus W$, é claro que a cada coloração arbitrária (não necessariamente própria) dos vértices de G que respeite a coloração parcial κ , corresponde a única κ -contracção em \mathcal{G}_κ que se obtém de G contraindo as arestas com extremos da mesma cor. Desta forma, a κ -contracção obtida fica com uma extensão cromática de κ . Reciprocamente, a cada κ -contracção $H \prec_\kappa G$, com uma extensão cromática da coloração parcial κ , corresponde a única coloração não própria dos vértices de G que se determina deixando inalteradas as cores dos vértices pertencentes a $V(H)$ e colorindo os restantes vértices de forma que os vértices extremos de cada uma das arestas de G contraídas para se obter H fiquem com as mesmas cores. Adicionalmente, é imediato concluir que a relação binária \preceq_κ , definida em \mathcal{G}_κ , é uma relação de ordem parcial e, consequentemente, $(\mathcal{G}_\kappa, \preceq_\kappa)$ é um conjunto parcialmente ordenado (cpo), onde \mathcal{G}_κ se designa por *conjunto das κ -contracções de G* e $(\mathcal{G}_\kappa, \preceq_\kappa)$ por *conjunto parcialmente ordenado das κ -contracções de G* . É claro que o subgrafo induzido por W é isomorfo aos elementos minimais de $(\mathcal{G}_\kappa, \preceq_\kappa)$.

Exemplo 19.8. Considerando o grafo G representado

na Figura 19.11, com a coloração parcial

$$\kappa : W = \{1, 3\} \rightarrow \{\text{branco, preto}\},$$

vamos determinar o conjunto parcialmente ordenado $C = (\mathcal{G}_\kappa, \preceq_\kappa)$.

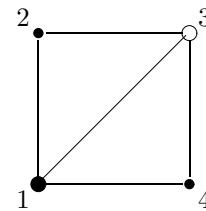
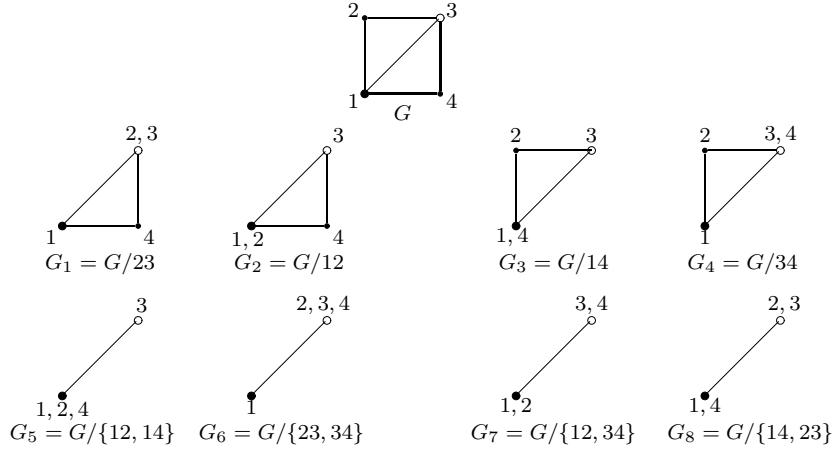
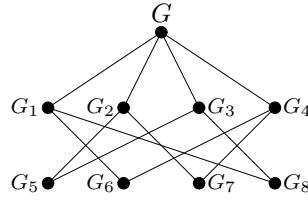


Figura 19.11: Grafo G com uma coloração parcial definida em $W = \{1, 3\} \subset V(G)$.

Solução. Com base na Figura 19.12, onde constam todas

as κ -contracções de G definidas pela coloração parcial $\kappa : W = \{1, 3\} \rightarrow \{\text{branco, preto}\}$, representada na Figura 19.11, com facilidade se conclui que o conjunto parcialmente ordenado C tem o diagrama de Hasse que se indica na Figura 19.13. \square

Figura 19.12: Conjunto das κ -contracções do grafo G representado na Figura 19.11.Figura 19.13: Diagrama de Hasse do cpo C do Exemplo 19.8.

Teorema 19.18. Dado um grafo simples G de ordem $\nu = \nu(G)$ e um subconjunto de vértices $W \subseteq V(G)$, seja $\kappa : W \rightarrow \{1, \dots, k\}$, onde $|W| = w$, uma coloração parcial. Se $f_\kappa(G, \lambda)$ é o número de extensões cromáticas de κ , utilizando $\lambda \geq k$ cores, então $f_\kappa(G, \lambda)$ é um polinómio em λ , mónico, de grau $\nu - w$, com coeficientes inteiros.

Demonstração. Dado um grafo simples G de ordem ν e um subconjunto de vértices $W \subseteq V(G)$, seja $\kappa : W \rightarrow \{1, \dots, k\}$, com $|W| = w$, uma coloração parcial de G e seja $C = (\mathcal{G}_\kappa, \preceq_\kappa)$ o cpo das κ -contracções de G . Para cada κ -contracção $G' \in \mathcal{G}_\kappa$, seja $f_\kappa(G', \lambda)$ o número de extensões cromáticas em G' da coloração parcial κ , utilizando λ cores e seja $q_\kappa(G', \lambda)$ o número de todas as colorações (não necessariamente próprias) dos vértices de G' , utilizando λ cores e respeitando as cores já atribuídas aos vértices de W pela coloração parcial κ . Nestas condições, é claro que $q_\kappa(G', \lambda) = \lambda^{\nu' - w}$, onde ν' denota a ordem do grafo G' . Uma vez que $\lambda \geq k$, sabe-se que qualquer coloração dos vértices de G (não necessariamente própria), respeitando as cores já atribuídas aos vértices de W , define uma coloração própria para a única κ -contracção $G' \in \mathcal{G}_\kappa$ que se obtém, contraindo todas as arestas cujos vértices extremos têm a mesma cor. Como consequência,

$$q_\kappa(G, \lambda) = \lambda^{\nu - w} = \sum_{G' \preceq_\kappa G} f_\kappa(G', \lambda).$$

Por aplicação do teorema da inversão de Möbius (Teorema 7.29), vem

$$f_\kappa(G, \lambda) = \sum_{G' \preceq_\kappa G} \mu(G', G) \lambda^{\nu' - w}, \quad (19.10)$$

onde ν' denota a ordem da κ -contracção G' . É claro que o segundo membro desta igualdade é um polinómio em λ , mónico, de grau $\nu - w$, com coeficientes inteiros. \square

Assim, de acordo com o Teorema 19.18, dado um grafo G , um subconjunto de vértices $W \subseteq V(G)$ e uma coloração parcial $\kappa : W \rightarrow \{1, \dots, k\}$, o número de extensões cromáticas de κ em G , utilizando $\lambda \geq k$ cores, é um polinómio em λ que designamos por *polinómio das extensões cromáticas* de κ no grafo G e denotamos por $f_\kappa(G, \lambda)$. Note-se que, em (19.10), os valores da função de Möbius podem ser determinados, recursivamente, a partir da fórmula (7.10)

Exemplo 19.9. Vamos determinar o polinómio das extensões cromáticas da coloração parcial representada na Figura 19.11, utilizando $\lambda \geq 2$ cores.

Solução. A coloração parcial $\kappa : W = \{1, 3\} \rightarrow \{\text{branco, preto}\}$, representada na Figura 19.11, determina o cpo $C = (\mathcal{G}_\kappa, \preceq_\kappa)$, cujo diagrama de Hasse é o da Figura 19.13, onde $\mathcal{G}_\kappa = \{G, G_1, G_2, \dots, G_8\}$. De acordo com o Teorema 19.18,

$$\begin{aligned} f_\kappa(G, \lambda) &= \sum_{G' \preceq_\kappa G} \mu(G', G) \lambda^{\nu' - 2} \\ &= \sum_{j=5}^8 \mu(G_j, G) + \left(\sum_{i=1}^4 \mu(G_i, G) \right) \lambda + \mu(G, G) \lambda^2. \end{aligned}$$

Logo, aplicando a equação recursiva (7.10), obtém-se

$$\begin{aligned} \mu(G_5, G) &= -(\mu(G_5, G_5) + \mu(G_5, G_2) + \mu(G_5, G_4)) \\ \mu(G_5, G_5) &= 1 \\ \mu(G_5, G_2) &= -\mu(G_5, G_5) = -1 \\ \mu(G_5, G_4) &= -\mu(G_5, G_5) = -1 \end{aligned}$$

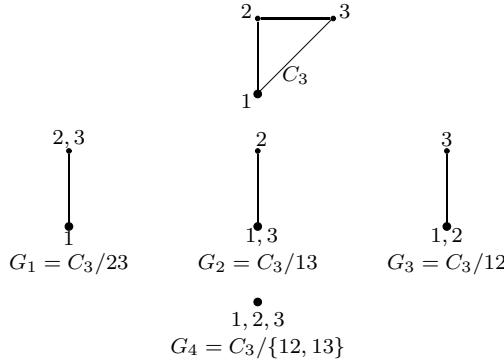
pelo que $\mu(G_5, G) = -(1 - 1 - 1) = 1$ e de modo idêntico se determina $\mu(G_6, G) = \mu(G_7, G) = \mu(G_8, G) = 1$, $\mu(G_1, G) = \mu(G_2, G) = \mu(G_3, G) = \mu(G_4, G) = -1$ e $\mu(G, G) = 1$. Consequentemente,

$$f_\kappa(G, \lambda) = 4 - 4\lambda + \lambda^2. \quad \square$$

Este tipo de abordagem pode ser utilizada na determinação de polinómios cromáticos de grafos. Com efeito, dado um grafo G e considerando uma coloração parcial $\kappa : W \rightarrow \{1\}$, onde W é um conjunto com um único vértice, é imediato concluir que $f(G, \lambda) = \lambda f_\kappa(G, \lambda)$.

Exemplo 19.10. Com recurso à coloração parcial de um único vértice de C_3 , κ , e a partir da determinação do respectivo polinómio das extensões cromáticas, $f_\kappa(C_3, \lambda)$, vamos determinar o polinómio cromático de C_3 , $f(C_3, \lambda)$.

Solução. Considerando a coloração parcial $\kappa : W = \{1\} \rightarrow \{\text{preto}\}$, o conjunto das κ -contracções, \mathcal{G}_κ , é constituído pelos grafos C_3, G_1, G_2, G_3 e G_4 , representados na Figura 19.14, a partir do qual é fácil determinar o cpo das contracções de C_3 definidas por κ , $C = (\mathcal{G}_\kappa, \preceq_\kappa)$. Logo, de acordo com o

Figura 19.14: Conjunto \mathcal{G}_κ das κ -contracções, com $\kappa : W = \{1\} \rightarrow \{\text{preto}\}$.

Teorema 19.18, vem

$$\begin{aligned}
 f_\kappa(C_3, \lambda) &= \sum_{G' \preceq_\kappa C_3} \mu(G', C_3) \lambda^{\nu' - 1} \\
 &= \mu(G_4, C_3) + (\mu(G_3, C_3) + \mu(G_2, C_3) + \mu(G_1, C_3))\lambda + \mu(C_3, C_3)\lambda^2 \\
 &= -(\mu(G_4, G_4) + \mu(G_4, G_3) + \mu(G_4, G_2) + \mu(G_4, G_1)) + \\
 &\quad + (-\mu(G_3, G_3) - \mu(G_2, G_2) - \mu(G_1, G_1))\lambda + \lambda^2 \\
 &= -(1 - 1 - 1 - 1) + (-1 - 1 - 1)\lambda + \lambda^2 \\
 &= 2 - 3\lambda + \lambda^2 = (\lambda - 1)(\lambda - 2).
 \end{aligned}$$

Como consequência, obtém-se (comparar com as fórmulas (19.7) e (19.9))

$$f(C_3, \lambda) = \lambda f_\kappa(C_3, \lambda) = \lambda(\lambda - 1)(\lambda - 2). \quad \square$$

Mais geralmente, podemos introduzir o seguinte resultado cuja prova fica como exercício (ver Exercício 19.20).

Teorema 19.19. *Dado um grafo simples G , um subconjunto de vértices $W \subseteq V(G)$, se $\mathcal{K}_{W; \lambda}$ é o conjunto de todas as colorações parciais $\kappa : W \rightarrow \{1, \dots, \lambda\}$ de G , então*

$$f(G, \lambda) = \sum_{\kappa \in \mathcal{K}_{W; \lambda}} f_\kappa(G, \lambda).$$

Como consequência, do Teorema 19.19 decorre o seguinte corolário.

Corolário 19.20. *Dado um grafo simples G e um subconjunto de vértices $W \subseteq V(G)$, induzindo o subgrafo completo $K_w = G[W]$, onde $w = |W|$, se $\bar{\kappa} : W \rightarrow \{1, \dots, w\}$ é uma coloração parcial de G , então*

$$f(G, \lambda) = f_{\bar{\kappa}}(G, \lambda) \prod_{i=0}^{w-1} (\lambda - i).$$

Demonstração. Seja $\mathcal{K}_{W; \lambda}$ o conjunto de todas as colorações parciais de G determinadas pelas colorações próprias dos vértices em $W \subseteq V(G)$, utilizando $\lambda \geq w$ cores, cujo número é $|\mathcal{K}_{W; \lambda}| = f(K_w, \lambda) = \lambda(\lambda - 1) \cdots (\lambda - (w - 1))$. Tendo em conta o Teorema 19.19 e o facto do número de

extensões cromáticas em G obtidas a partir de qualquer coloração própria dos vértice em W ser constante, dada a coloração parcial particular $\bar{\kappa} : W \rightarrow \{1, \dots, w\}$, vem

$$f(G, \lambda) = \sum_{\kappa \in \mathcal{K}_{W; \lambda}} f_\kappa(G, \lambda) = f(K_w, \lambda) f_{\bar{\kappa}}(G, \lambda) = f_{\bar{\kappa}}(G, \lambda) \prod_{i=0}^{w-1} (\lambda - i).$$

□

Exemplo 19.11. Vamos determinar o polinómio cromático do grafo G representado na Figura 19.11.

Solução. De acordo com o Exemplo 19.8, $f_{\bar{\kappa}}(G, \lambda) = \lambda^2 - 4\lambda + 4$ e na coloração parcial $\bar{\kappa} : W = \{1, 3\} \rightarrow \{\text{preto, branco}\}$ considerada, W induz K_2 . Logo, aplicando o Corolário 19.20, vem

$$f(G, \lambda) = f(K_2, \lambda) f_{\bar{\kappa}}(G, \lambda) = \lambda(\lambda - 1)(\lambda^2 - 4\lambda + 4) = \lambda(\lambda - 1)(\lambda - 2)^2.$$

□

Relativamente ao número de extensões cromáticas de uma coloração parcial, ainda podemos referir o seguinte resultado.

Teorema 19.21. Dado um grafo simples G e um subconjunto de vértices $W \subset V(G)$, seja $\kappa : W \rightarrow \{1, \dots, k\}$ uma coloração parcial, onde $k = \chi(G) - 2$. Se existe uma extensão cromática de κ , utilizando $\chi(G)$ cores, então o número destas extensões é não inferior a 2.

Demonstração. Uma vez que de entre as cores determinadas por uma extensão cromática da coloração parcial κ (a todos os vértices de G), existem duas que não são utilizadas por κ , podemos troca-las entre si, sem que a coloração dos vértices de G deixe de ser própria e de ser uma extensão cromática de κ . □

Como consequência imediata deste teorema, podemos concluir que dado um grafo simples G e um subconjunto de vértices $W \subseteq V(G)$, se a coloração parcial $\kappa : W \Rightarrow \{1, \dots, k\}$ admite uma única extensão cromática, então $k \geq \chi(G) - 1$.

Uma aplicação muito popular da determinação de extensões cromáticas de colorações parciais está relacionada com a completação de quadrados latinos parcialmente conhecidos, mais particularmente, com o *Sudoku* cuja designação é a abreviatura japonesa de *suuji wa dokushin ni kagiru* que significa os dígitos devem permanecer únicos. Trata-se de um puzzle publicado pela primeira vez, no final de 1970, na revista americana *Math Puzzles and Logic Problems*, com a designação *Number Place* e mais tarde levado para o Japão onde, rapidamente, atingiu grande popularidade. Desde há vários anos, é proposto, frequentemente, aos leitores de muitos jornais e revistas em todo o mundo, consistindo numa grelha com 9×9 entradas, a qual deve ser totalmente preenchida com números inteiros entre 1 e 9. As entradas desta grelha estão agrupados em 3×3 blocos, cada um dos quais com 3×3 entradas (conforme a Tabela 19.1 exemplifica).

Inicialmente, algumas das entradas estão já preenchidas e o jogo (puzzle) consiste em preencher as restantes entradas, de tal forma que em cada linha, coluna e bloco, não existam números repetidos. Assim, o objectivo é a determinação de um quadrado latino com a particularidade de em cada um dos 3×3 blocos também não existirem entradas repetidas. Mais geralmente, esta grelha com $n^2 \times n^2$ entradas (e $n \times n$ blocos, com $n \times n$ entradas cada) designa-se por *Sudoku* de ordem n e denota-se por S_n . Com ela, dado um conjunto de entradas inicialmente preenchidas, pretendemos preencher as restantes com inteiros entre 1 e n^2 de modo a obter um quadrado latino com a propriedade adicional de não conter entradas repetidas em cada um dos seus $n \times n$ blocos. Na Tabela 19.1, representa-se um *Sudoku* de ordem 3, S_3 , com 17 entradas inicialmente preenchidas.

Dado um *Sudoku* de ordem n , S_n , designa-se por *grafo do Sudoku* S_n e denota-se por $G(S_n)$, o grafo cujos vértices são as entradas (i, j) de S_n , com $1 \leq i, j \leq n^2$, e onde dois vértices são adjacentes se correspondem a entradas na mesma linha ou coluna ou bloco, ou seja, (i_1, j_1) é adjacente a (i_2, j_2) se $i_1 = i_2$ ou $j_1 = j_2$ ou ainda $[i_1/n] = [i_2/n]$ e $[j_1/n] = [j_2/n]$. As entradas de S_n inicialmente

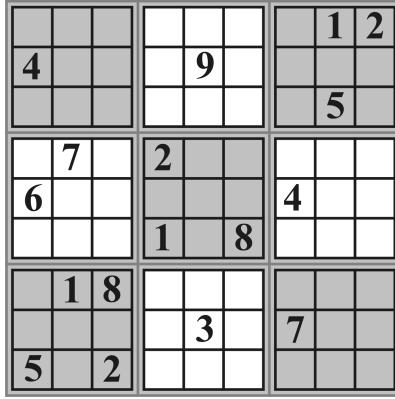


Tabela 19.1: Sudoku com 17 entradas inicialmente preenchidas.

preenchidas correspondem a uma coloração parcial κ de $G(S_n)$, com pelo menos $n^2 - 1$ cores, e o problema do preenchimento das restantes entradas (puzzle Sudoku) corresponde ao problema da determinação de uma extensão cromática de κ com recurso a n^2 cores.

Teorema 19.22. *Qualquer que seja $n \in \mathbb{N}$, sendo S_n um Sudoku de ordem n , $\chi(G(S_n)) = n^2$.*

Demonstração. Uma vez que cada $n \times n$ bloco de S_n dá origem a uma clique em $G(S_n)$ e quaisquer k vértices, com $k > n^2$, não pertencem a uma mesma linha ou coluna ou bloco, podemos concluir que $\omega(G(S_n)) = n^2$ e, consequentemente, $\chi(G(S_n)) \geq n^2$. Logo, resta provar que é possível colorir propriamente os vértices de $G(S_n)$, com n^2 cores. Por facilidade de notação, vamos indexar os vértices do grafo do Sudoku $G(S_n)$ por (i, j) , com $0 \leq i, j \leq n^2 - 1$. Assim, fazendo $i = nt_i + d_i$, com $0 \leq t_i, d_i \leq n - 1$, e $j = nt_j + d_j$, com $0 \leq t_j, d_j \leq n - 1$, e

$$\kappa(i, j) = nd_i + t_i + nt_j + d_j \pmod{n^2},$$

vamos provar que se trata de uma coloração própria dos vértices de $G(S_n)$, para o que basta provar que, com ela, vértices adjacentes têm cores distintas.

Sejam (i_1, j_1) e (i_2, j_2) dois vértices tais que $\kappa(i_1, j_1) = \kappa(i_2, j_2)$.

- Se $i_1 = i_2 = i$, então

$$\kappa(i, j_1) = \kappa(i, j_2) \Leftrightarrow nt_{j_1} + d_{j_1} = nt_{j_2} + d_{j_2} \pmod{n^2} \Leftrightarrow j_1 = j_2.$$

- De igual modo se prova que se $j_1 = j_2$, então $i_1 = i_2$.

- Suponhamos que $\lfloor i_1/n \rfloor = \lfloor i_2/n \rfloor$ (o que é equivalente a $\lceil (i_1+1)/n \rceil = \lceil (i_2+1)/n \rceil$) e $\lfloor j_1/n \rfloor = \lfloor j_2/n \rfloor$ (o que é equivalente a $\lceil (j_1+1)/n \rceil = \lceil (j_2+1)/n \rceil$). Sendo $i_1 = nt_{i_1} + d_{i_1}$ e $i_2 = nt_{i_2} + d_{i_2}$, com $0 \leq d_{i_1}, d_{i_2} \leq n - 1$, e sendo $j_1 = nt_{j_1} + d_{j_1}$ e $j_2 = nt_{j_2} + d_{j_2}$, com $0 \leq d_{j_1}, d_{j_2} \leq n - 1$, podemos concluir que $t_{i_1} = t_{i_2}$ e $t_{j_1} = t_{j_2}$. Logo, uma vez que

$$\begin{aligned} \kappa(i_1, j_1) = \kappa(i_2, j_2) &\Leftrightarrow nd_{i_1} + d_{j_1} = nd_{i_2} + d_{j_2} \pmod{n^2} \\ &\Rightarrow d_{j_1} = d_{j_2} \pmod{n} \\ &\Rightarrow d_{j_1} = d_{j_2}, \end{aligned}$$

podemos concluir a igualdade $(i_1, j_1) = (i_2, j_2)$. □

Quando se preenche um Sudoku de ordem 3, uma questão frequente é a de saber se a partir das entradas inicialmente preenchidas existe uma solução e se essa solução é única. Adicionalmente, outra questão relevante é qual o número mínimo de entradas inicialmente preenchidas de forma a obter-se uma única solução. Actualmente, conhecem-se dezenas de milhar de puzzles Sudoku, S_3 , com 17 entradas inicialmente preenchidas que apresentam uma única solução (como é o caso do exemplo apresentado na Tabela 19.1) (ver <http://www.csse.uwa.edu.au/~gordon/sudokumin.php>). Porém, continua em aberto o problema de saber se existe algum Sudoku, S_3 , com 16 entradas inicialmente preenchidas que tenha uma única solução [57].

19.3. Coloração de arestas

Para muitas aplicações práticas é mais interessante estudar a coloração de arestas do que a coloração de vértices.

Definição 19.6 (Coloração de arestas, coloração própria de arestas e índice cromático). *Uma k -coloração das arestas de um grafo G sem lacetes é uma função*

$$c' : E(G) \rightarrow \{1, \dots, k\}.$$

Uma k -coloração das arestas de G diz-se própria se para qualquer par de arestas $xy, xz \in E(G)$ (arestas adjacentes), $c'(xy) \neq c'(xz)$. O menor k para o qual existe uma k -coloração própria das arestas de G designa-se por índice cromático de G e denota-se por $\chi'(G)$.

É claro que se o grafo G é não nulo, então $\chi'(G) = \chi(L(G))$, onde $L(G)$ denota o grafo linha de G . Um resultado publicado por Vizing em 1964 estabelece limites muito apertados para a coloração de arestas de grafos arbitrários.

Teorema 19.23 (Vizing). *Dado um grafo simples G , verificam-se as desigualdades*

$$\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1. \quad (19.11)$$

Demonstração. Uma vez que a primeira desigualdade é trivialmente verdadeira, apenas vamos provar a segunda por indução sobre as arestas do grafo G , tendo em conta que se $\varepsilon(G) = 0$, é claro que $\chi'(G) \leq \Delta(G) + 1$. Suponha $\Delta(G) > 0$ e que (19.11) se verifica para grafos com menos arestas do que $\varepsilon(G)$. Qualquer que seja a aresta $uv \in E(G)$, por hipótese de indução, existe uma coloração das arestas de $G - uv$ com recurso a no máximo $\Delta(G) + 1$ cores. Adicionalmente, as arestas incidentes em u utilizam no máximo $d_G(u) \leq \Delta(G)$ cores. Logo, pelo menos uma das $\Delta(G) + 1$ cores (por exemplo a cor azul) não é utilizada e, para qualquer outra cor (por exemplo, vermelha) existe um passeio (eventualmente trivial), único, maximal, com início no vértice u e arestas alternadamente vermelhas e azuis. Este passeio é um caminho que vamos designar por *caminho alternadamente vermelho e azul, com início em u* .

- Vamos fazer a prova por partes, supondo que G não admite uma coloração de arestas com $\Delta(G) + 1$ cores.
 - (a) Então, dada uma aresta $xy \in E(G)$ e uma coloração arbitrária de $G - xy$ relativamente à qual (por exemplo) a cor azul não aparece nas arestas incidentes em x e (por exemplo) a cor vermelha não aparece nas arestas incidentes em y , o caminho alternadamente azul e vermelho com início em y termina em x (caso contrário, poderíamos trocar as cores vermelha e azul entre si e colorir a aresta xy com a cor azul, o que seria contraditório).
 - (b) Se $xv_0 \in E(G)$, então (por hipótese de indução) $G - xv_0$ admite uma coloração c_0 de arestas com não mais do que $\Delta(G) + 1$ cores. Seja a cor azul a cor em falta de entre as cores de

c_0 utilizadas pelas arestas incidentes em x e seja, v_0, v_1, \dots, v_k a sequência maximal de vizinhos distintos de x em G tais que a cor $c_0(xv_i)$ não aparece nas arestas incidentes em v_{i-1} , para $i = 1, \dots, k$. Para cada um dos grafos $G_i = G - xv_i$, vamos definir a coloração de arestas c_i , fazendo

$$c_i(e) = \begin{cases} c_0(xv_{j+1}), & \text{se } e = xv_j \text{ e } j \in \{0, \dots, i-1\}, \\ c_0(e), & \text{no caso contrário.} \end{cases}$$

Note-se que em cada uma destas colorações, c_1, \dots, c_k , as cores que não aparecem nas arestas incidentes em x coincidem com as cores de c_0 nas mesmas condições.

- (c) Seja o vermelho a cor de c_0 que não aparece nas arestas incidentes no vértice v_k . É claro que o vermelho é também a cor de c_k que não aparece nas arestas incidentes em v_k . Se esta cor não aparece nas arestas incidentes em x , então podemos colorir xv_k de vermelho e estender c_k a todas as arestas de G , o que é contraditório. Consequentemente, existe uma aresta vermelha incidente em x para qualquer das colorações c_0, \dots, c_k . Com efeito, pela maximalidade de k ,

$$c_0(xv_i) \text{ é a cor vermelha para algum } i \in \{1, \dots, k-1\}. \quad (19.12)$$

- (d) Seja P o caminho de G_k , alternadamente azul e vermelho, com início em v_k , relativamente à coloração c_k (ver Figura 19.15). De acordo com (a), o caminho P termina em x com

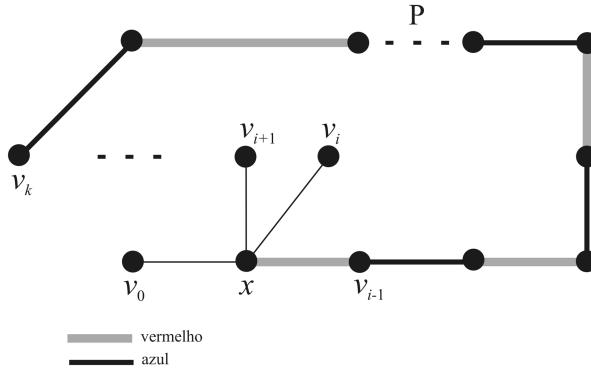


Figura 19.15: Coloração das arestas de P com as cores de c_k .

uma aresta vermelha (relativamente a c_k), uma vez que as arestas incidentes em x não têm a cor azul. Adicionalmente, dado que a cor vermelha corresponde a $c_k(xv_i) = c_0(xv_{i-1})$, xv_{i-1} é precisamente a aresta de P que incide em x . Contudo, para a coloração c_0 e, consequentemente, para c_{i-1} , a cor vermelha não aparece nas arestas incidentes em v_{i-1} (tendo em conta (19.12) e a escolha de v_i). Seja P' o caminho de G_{i-1} , alternadamente azul e vermelho, com início em v_{i-1} (relativamente à coloração c_{i-1}). Uma vez que P' é unicamente determinado, trata-se da parte do caminho P que se inicia em v_{i-1} e passa pelas restantes arestas de P , até v_k , continuando (eventualmente) para x . Deve observar-se que as arestas deste caminho são coloridas com as mesmas cores, tanto relativamente a c_{i-1} , como relativamente a c_k . Porém, relativamente a c_0 e, consequentemente, relativamente a c_{i-1} , não existe uma aresta vermelha incidente em v_k (de acordo com (c)). Logo, P' termina em v_k , o que contradiz (a). \square

O teorema de Vizing divide os grafos finitos em duas classes, de acordo com o seu índice cromático. Os grafos G para os quais $\chi'(G) = \Delta(G)$ pertencem à *classe 1* e os grafos H para os quais $\chi'(H) = \Delta(H) + 1$ pertencem à *classe 2*. Deve observar-se ainda que, de acordo com a definição de coloração de arestas, um conjunto de arestas com a mesma cor é um emparelhamento. Como consequência, dado um grafo arbitrário G e sendo $M \subseteq E(G)$ um emparelhamento máximo de G , podem concluir-se as desigualdades

$$|M| \geq \frac{\varepsilon(G)}{\chi'(G)} \geq \frac{\varepsilon(G)}{\Delta(G) + 1}. \quad (19.13)$$

No caso de grafos bipartidos, temos o seguinte teorema, publicado por König em 1916.

Teorema 19.24 (König). *Se G é um grafo bipartido então $\chi'(G) = \Delta(G)$.*

Demonstração. Vamos fazer a prova por indução sobre o número de arestas do grafo, sabendo que quando esse número é nulo, $\Delta(G) = 0$ e $\chi'(G) = 0$, pelo que o resultado se verifica. Suponha que G tem pelo menos uma aresta e que o resultado é verdadeiro para grafos com menos arestas do que as de G . Seja $xy \in E(G)$ e seja H o grafo que se obtém de G eliminando a aresta xy . Por hipótese de indução, $\chi'(H) = \Delta(H)$.

- Se $\Delta(H) = \Delta(G) - 1$, então é claro que $\chi'(G) = \Delta(G)$.
- Se $\Delta(G) = \Delta(H)$, uma vez que tanto o grau de x como o de y em H é no máximo $\Delta(G) - 1$, podemos concluir que de entre as cores utilizadas para colorir as arestas de H existe pelo menos uma cor que não aparece nas arestas de H incidentes em x e pelo menos uma cor que não aparece nas arestas de H incidentes em y .
 - Caso se trate da mesma cor, podemos atribui-la à aresta xy , obtendo-se o resultado pretendido.
 - Caso se trate de cores distintas, admitindo, por exemplo, que a cor azul não aparece nas arestas incidentes em x e a cor vermelha não aparece nas arestas incidentes em y , iniciando um caminho de máximo comprimento a partir de x com arestas de cores alternadamente vermelha e azul, nunca atingiremos o vértice y (uma vez que passamos alternadamente do subconjunto independente de vértices que contém x para o subconjunto independente de vértices que contém y e reciprocamente, no primeiro caso sempre por arestas de cor vermelha e no segundo com arestas de cor azul). Logo, procedendo à troca entre si das cores que aparecem ao longo deste caminho, não só a coloração de arestas se mantém própria, como a cor vermelha (que já não fazia parte das cores das arestas incidentes em y) deixa também de fazer parte das cores das arestas incidentes em x , pelo que pode ser utilizada para colorir a aresta xy sem que o número de cores se altere. \square

A coloração de arestas de grafos bipartidos tem aplicação na produção de quadrados latinos. Com efeito, denotando o conjunto dos índices das linhas de um quadrado latino L de ordem n , por $I = \{i_1, \dots, i_n\}$ e o conjunto dos índices das colunas por $J = \{j_1, \dots, j_n\}$, qualquer coloração das arestas do grafo bipartido completo $K_{nn} = (I, J, E)$, com n cores, determina um quadrado latino L . Note-se que, de acordo com o Teorema 19.24, $\chi'(K_{nn}) = n$. Logo, identificando os n símbolos do quadrado latino L com as n cores utilizadas na coloração das arestas, conclui-se que não existem dois símbolos iguais na mesma linha ou coluna, dado que tal equivaleria à existência de duas arestas com a mesma cor incidentes num mesmo vértice.

Exemplo 19.12. *Vamos determinar um quadrado latino de ordem 3, a partir de uma 3-coloração própria das arestas do grafo bipartido completo K_{33} .*

Solução. Na Figura 19.16, onde as letras indicam cores, representa-se uma 3-coloração das arestas de $K_{3,3}$. Como consequência, a partir desta 3-coloração de arestas, obtém-se o quadrado latino

$$L = \begin{array}{c} \begin{matrix} & j_1 & j_2 & j_3 \\ i_1 & b & c & a \\ i_2 & c & a & b \\ i_3 & a & b & c \end{matrix} \\ \left(\begin{matrix} i_1 \\ i_2 \\ i_3 \end{matrix} \right) \end{array}.$$

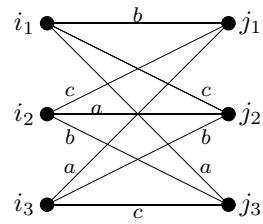


Figura 19.16: Grafo $K_{3,3}$ com uma 3-coloração própria de arestas

Segue-se um teorema atribuído a Tait⁹, mas cuja demonstração foi publicada por Petersen¹⁰ em 1898 [77].

Teorema 19.25 (Tait). *Sendo G um grafo cúbico, $\chi'(G) = 3$ se e só se G tem um subgrafo abrangente 2-regular que é formado pela união de ciclos de comprimento par.*

Demonstração. Se H é um subgrafo abrangente de G que é 2-regular, formado pela união de ciclos de comprimento par, então podemos colorir as arestas de $E(G) \cap E(H)$ com duas cores e as restantes arestas de G com uma terceira cor. Reciprocamente, se G admite uma coloração de arestas com três cores, então as arestas pintadas com duas das cores formam (necessariamente) um subgrafo abrangente de G que é 2-regular e é formado pela união de ciclos de comprimento par. \square

O resultado a seguir pode obter-se como corolário imediato do teorema de Tait.

Corolário 19.26. *Se G é um grafo cúbico que admite um ciclo de Hamilton, então $\chi'(G) = 3$.*

Demonstração. Seja G é um grafo cúbico (logo de ordem par) que admite um ciclo de Hamilton C . Uma vez que $\nu(G) = |V(C)| = |E(C)|$, $|E(C)|$ é par. Logo, podemos concluir que G admite um subgrafo abrangente 2-regular formado por um único ciclo de comprimento par e, como consequência, por aplicação do Teorema 19.25, $\chi'(G) = 3$. \square

Note-se que é muito fácil colorir as arestas de um grafo cúbico hamiltoniano, G , utilizando três cores. Com efeito, sendo $C = (x_1, x_2, \dots, x_{2k}, x_1)$ um ciclo de Hamilton em G , podemos atribuir a cor 1 às arestas $x_{2j-1}x_{2j}$, para $j = 1, \dots, k$, a cor 2 à aresta $x_{2k}x_1$ e às arestas $x_{2j}x_{2j+1}$, para $j = 1, \dots, k-1$ e a cor 3 às restantes.

19.3.1 Números de Ramsey para grafos simples

Em qualquer conjunto de seis pessoas que se encontram casualmente, podemos afirmar que existem três pessoas que se conhecem mutuamente ou existem três pessoas que não se conhecem. Com efeito, para se tirar esta conclusão, considerando o grafo simples completo de ordem 6, K_6 , onde os vértices denotam as pessoas, e atribuindo a cor A a cada aresta cujos vértices extremos correspondem a pessoas que se conhecem e a cor B no caso contrário, basta provar que existe um triângulo com arestas da mesma cor. Com este objectivo, escolhendo um vértice arbitrário $v \in V(K_6)$, é claro que v tem grau 5 e, consequentemente, pelo menos três arestas incidentes em v têm a mesma cor que, sem perda de generalidade, vamos supor ser A . Sendo vx, vy e vz arestas com cor A , se xy, xz e yz têm cor B então o resultado obtém-se, caso contrário, existe pelo menos uma aresta, por exemplo xy com cor A e, consequentemente, as arestas vx, vy e xy têm a cor A .

No resultado que acabamos de enunciar, não é por acaso que se consideraram 6 pessoas e não 5 ou 7. Com efeito, o número seis é o mínimo possível para uma tal proposição ser verdadeira, uma vez que, no caso de K_5 , a coloração das arestas do pentágono que limita K_5 com uma cor e todas as restantes arestas (diagonais do pentágono) com a outra cor, não produz qualquer triângulo monocromático.

⁹ Peter Guthrie Tait (1831-1901), foi um escocês que ficou particularmente conhecido pelo livro que publicou em co-autoria com Kelvin, na área da física-matemática.

¹⁰ Julius Petersen (1839-1910), matemático dinamarquês, com várias contribuições para a teoria dos grafos e que é especialmente conhecido pelo grafo, com o seu nome (ver Figura 14.4) que introduziu em 1892.

Este resultado, aliás, é um caso particular de resultados mais gerais que decorrem da *Teoria de Ramsey*¹¹. Segundo esta teoria, dado um grafo simples G de ordem não inferior a 6 existe uma clique de cardinalidade 3 ou um conjunto independente de cardinalidade 3 (note-se que podemos considerar o grafo com arestas apenas entre os vértices correspondentes a pessoas que se conhecem, pelo que, a ausência de aresta corresponde a eliminar do grafo completo as arestas com cor B). Mais geralmente, segue-se a definição de número de Ramsey.

Definição 19.7 (Número de Ramsey). *Designa-se por número de Ramsey e denota-se por $R(p, q)$, o menor inteiro positivo tal que colorindo as arestas do grafo simples completo K_ν , com $\nu = R(p, q)$, utilizando as cores A e B, existe um subgrafo K_p com arestas de cor A ou um subgrafo K_q com arestas de cor B.*

De acordo com esta definição, tendo em conta que as cores A e B partem as arestas de K_ν em dois subgrafos complementares, G e G^c , de ordem ν , podemos definir o número de Ramsey $R(p, q)$, como sendo o menor inteiro positivo ν tal que qualquer grafo G de ordem não inferior a ν contém uma clique de cardinalidade p ou um conjunto independente de cardinalidade q , ou seja, $\omega(G) \geq p$ ou $\alpha(G) \geq q$.

Ainda de acordo com a definição de número de Ramsey, é claro que quaisquer que sejam os inteiros positivos p e q , $R(p, q) = R(q, p)$ e $R(1, q) = 1 = R(p, 1)$. O teorema a seguir garante a existência dos números de Ramsey, $R(p, q)$, para todos os pares de inteiros positivos $p, q \geq 2$.

Teorema 19.27. *Dados dois inteiros positivos $p, q \geq 2$, $R(p, 2) = p$, $R(2, q) = q$ e*

$$R(p, q) \leq R(p, q - 1) + R(p - 1, q), \quad (19.14)$$

Demonstração. Vamos começar por provar as igualdades $R(p, 2) = p$ e $R(2, q) = q$ e posteriormente, vamos provar, por indução, a desigualdade (19.14).

1. Dado o grafo completo de ordem p (q), colorindo as suas arestas com duas cores, todas as arestas de K_p (K_q) têm a mesma cor ou existem duas arestas com cores distintas e, neste último caso, existe o subgrafo monocromático K_2 , pelo que $R(p, 2) \leq p$ ($R(2, q) \leq q$). Porém, é claro que colorindo as arestas do grafo simples completo de ordem $p - 1$ ($q - 1$) com uma única cor não se obtém nenhum dos subgrafos monocromáticos K_p ou K_2 , pelo que $R(p, 2) = p$ ($R(2, q) = q$).
2. A prova da desigualdade (19.14) implica a existência de números de Ramsey $R(p, q)$, para todos os inteiros positivos $p, q \geq 2$. Vamos fazer esta prova por indução, tendo em conta as igualdades $R(p, 2) = p$ e $R(2, q) = q$ e admitindo que os números de Ramsey $R(p, q - 1)$ e $R(p - 1, q)$ existem para $p, q > 2$. Assim, considerando um grafo simples completo de ordem $\nu = R(p, q - 1) + R(p - 1, q)$ e colorindo as suas arestas com as cores azul ou vermelha, se $v \in K_\nu$ (pelo que v tem grau $\nu - 1$), então temos um dos seguintes casos:
 - (a) o vértice v tem pelo menos $R(p, q - 1)$ arestas vermelhas que lhe são incidentes;
 - (b) o vértice v tem pelo menos $R(p - 1, q)$ arestas azuis que lhe são incidentes.

Em (a) seja $X \subset V(K_\nu)$ o subconjunto dos $R(p, q - 1)$ vizinhos de v . Por hipótese de indução, X induz um grafo simples completo que contém K_p com arestas azuis ou K_{q-1} com arestas vermelhas. Neste último caso, juntando as arestas incidentes em v às arestas de K_{q-1} , obtém-se K_q com arestas vermelhas. De igual modo se prova em (b) que se obtém um subgrafo simples completo que contém K_q com arestas vermelhas ou K_p com arestas azuis. \square

A desigualdade (19.14) do Teorema 19.27, garante a existência de números de Ramsey $R(p, q)$, com $p, q \geq 2$, conforme o Corolario 19.28 estabelece.

¹¹ Esta teoria, com início num artigo publicado em 1929 por Ramsey [78], no contexto da teoria dos conjuntos, é hoje intensamente investigada em diferentes áreas da Matemática, entre as quais a teoria dos grafos

Corolário 19.28. Dados dois inteiros positivos p_1 e p_2 , existe um inteiro positivo mínimo, $R(p_1, p_2)$, tal que para $\nu \geq R(p_1, p_2)$, se colorirmos as arestas de K_ν , com as cores 1 ou 2, então existe $i \in \{1, 2\}$ e um subgrafo de K_ν , completo, K_{p_i} , com arestas de cor i .

Demonstração. De acordo com a definição, sabe-se que $R(1, p_2) = 1$ e $R(p_1, 1) = 1$ e, de acordo o Teorema 19.27, se $p_1, p_2 \geq 2$, então $R(2, p_2) = p_2$ e $R(p_1, 2) = p_1$. Nos restantes casos, sendo $p_1, p_2 > 2$, admitindo a existência de números de Ramsey $R(x, p_2)$, com $x < p_1$, e $R(p_1, y)$, com $y < p_2$, por indução, aplicando o Teorema 19.27, podemos concluir a existência de $R(p_1, p_2)$. \square

Note-se que estes resultados de existência de números de Ramsey $R(p, q)$, para os inteiros positivos p e q , não nos indicam o seu valor exacto que, aliás, é desconhecido para a esmagadora maioria dos pares (p, q) . Por exemplo, tendo em conta a desigualdade (19.14), embora se possa concluir a desigualdade $R(4, 3) \leq R(3, 3) + R(4, 2) = 6 + 4 = 10$, $R(4, 3) = 9$, conforme se prova no exemplo a seguir.

Exemplo 19.13. Vamos provar a igualdade $R(4, 3) = 9$.

Solução. Vamos provar que a coloração das arestas de K_9 com duas cores, azul e vermelha, produz um subgrafo K_4 , com arestas azuis, ou um subgrafo K_3 , com arestas vermelhas, e que o mesmo não acontece com K_8 .

- Considerando K_9 , com as arestas coloridas com cores azul e vermelha, podemos concluir que existe um vértice $v \in V(K_9)$ no qual incidem pelo menos 6 arestas azuis ou pelo menos 4 arestas vermelhas. Caso contrário, em todos os vértices incidem não mais de 5 arestas azuis e não mais de 3 arestas vermelhas, pelo que, em cada um deles, fica, pelo menos, uma aresta por colorir, o que é contraditório. Assim, temos dois casos possíveis.
 - Existem 6 arestas azuis incidentes em v e, consequentemente, sendo $Y \subseteq X = \{x : vx \in E(K_9) \text{ e tem cor azul}\}$ um subconjunto de vértices de cardinalidade 6, Y induz o subgrafo K_6 no qual existe um triângulo de arestas azuis ou um triângulo de arestas vermelhas. Logo, K_6 contém um triângulo de arestas azuis que juntamente com v forma K_4 com arestas azuis ou contém um triângulo com arestas vermelhas.
 - Existem 4 arestas vermelhas incidentes em v e, consequentemente, sendo $Y \subseteq X = \{x : vx \in E(K_9) \text{ e tem cor vermelha}\}$ um subconjunto de vértices de cardinalidade 4 que induz K_4 , ou todas as arestas deste subgrafo são azuis ou tem pelo menos uma aresta vermelha que, conjuntamente com as arestas incidentes em v , forma um triângulo vermelho.
- Seja $V(K_8) = \{1, 2, \dots, 8\}$ e disponha estes vértices de forma circular e crescente (no sentido dos ponteiros do relógio, por exemplo). Vamos colorir as arestas ij , com $j > i$, de vermelho se $j - i \in \{1, 4, 7\}$ e de azul nos outros casos, ou seja, se $j - i \in \{2, 3, 5, 6\}$. Nestas condições, não existe qualquer triângulo com arestas vermelhas. Caso contrário, sendo i o vértice de menor índice de um tal triângulo, ele contém necessariamente dois dos vértices $i + 1, i + 4, i + 7$ que estão ligados, entre si, por arestas azuis, o que é contraditório. Por outro lado, supondo que existe um subgrafo K_4 com arestas azuis, sendo i o vértice de menor índice deste subgrafo, os seus vizinhos são três dos quatro vértices $i + 2, i + 3, i + 5, i + 6$. Porém, a aresta que liga $i + 2$ e $i + 3$ é vermelha, assim como a aresta que liga os vértices $i + 5$ e $i + 6$, o que é contraditório.

\square

Note-se que, de acordo com este exemplo e com a definição de $R(4, 3)$, podemos concluir que para qualquer grafo G de ordem 9, $\omega(G) \geq 4$ ou $\alpha(G) \geq 3$ (ou, tendo em conta que $R(3, 4) = R(4, 3)$, $\alpha(G) \geq 4$ ou $\omega(G) \geq 3$).

Antes de passarmos ao próximo exemplo que estabelece o valor exacto de mais um número de Ramsey, convém introduzir o conceito de *resíduo quadrático módulo p*, onde p é um número primo

maior que dois, e que é um inteiro m não divisível por p (i.e., $p \nmid m$) relativamente ao qual existe $x \in \{1, \dots, p-1\}$ tal que $x^2 \equiv m \pmod{p}$.

Exemplo 19.14. Vamos provar a igualdade $R(4, 4) = 18$.

Solução. Tendo em conta a desigualdade (19.14), é claro que

$$R(4, 4) \leq R(4, 3) + R(3, 4) = 9 + 9 = 18.$$

Por outro lado, vamos considerar o grafo completo K_{17} , tal que $V(K_{17}) = \{0, 1, \dots, 16\}$, e colorir as suas arestas ij , com $j > i$, de cor azul se $i - j$ é um resíduo quadrático módulo 17 e de cor vermelha no caso contrário. Nestas condições, as arestas vermelhas são as arestas ij , com $j > i$, tais que $j - i \in \{1, 2, 4, 8, 9, 13, 15, 16\}$. Com esta coloração das arestas, conclui-se a não existência de um subgrafo de K_{17} isomorfo a K_4 com arestas da mesma cor. \square

Já vimos que $R(2, 2) = 2$, $R(3, 3) = 6$ e $R(4, 4) = 18$. Porém, até ao momento, não se conhecem os valores exactos de $R(p, p)$, para $p \geq 5$, e a sua investigação tem-se revelado muito difícil. Seguem-se alguns minorantes e majorantes para números de Ramsey.

Teorema 19.29. Dado os inteiros $p, q \geq 2$, verificam-se as desigualdades:

- (a) $R(p, q) \leq \binom{p+q-2}{p-1}$;
- (b) $R(p, p) \leq 4^{p-1}$;
- (c) $R(p, p) \geq 2^{p/2}$.

Demonstração. Vamos provar cada uma das desigualdades pela ordem que aparecem no enunciado do teorema.

- (a) Vamos fazer esta prova por indução, tendo em conta que para $p = 2$ ($q = 2$), $R(2, q) = q = \binom{q}{1}$ ($R(p, 2) = p = \binom{p}{1}$). Assumindo que a desigualdade se verifica para $R(p, q-1)$ e $R(p-1, q)$, vem

$$\begin{aligned} R(p, q) &\leq R(p, q-1) + R(p-1, q) \\ &\leq \binom{p+q-3}{p-1} + \binom{p+q-3}{p-2} \\ &= \binom{p+q-2}{p-1}, \end{aligned} \tag{19.15}$$

onde a igualdade (19.15) decorre da identidade combinatória (4.21) do Exemplo 4.26.

- (b) Tendo em conta a desigualdade (a), vem

$$R(p, p) \leq \binom{2p-2}{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j}^2 \tag{19.16}$$

$$\begin{aligned} &\leq \left(\sum_{j=0}^{p-1} \binom{p-1}{j} \right)^2 \\ &= (2^{p-1})^2 \\ &= 4^{p-1}, \end{aligned} \tag{19.17}$$

onde a igualdade (19.16) decorre da identidade combinatória do Exemplo 4.27 e a igualdade (19.17) decorre da identidade combinatória (4.19).

- (c) Seja \mathcal{G}_n o conjunto dos grafos cujo conjunto de vértices é $V = \{1, 2, \dots, n\}$. Uma vez que a desigualdade se verifica para $p = 2$ ($R(2, 2) = 2 \geq 2^{2/2}$), sem perda de generalidade, podemos considerar $p > 2$ e, dado que $R(3, 3) = 6$, podemos considerar $n \geq 4$. Então, $|\mathcal{G}_n| = 2^{\binom{n}{2}}$ e o número de subgrafos completos induzidos por um subconjunto de vértices $P \subseteq V$ de cardinalidade p é $2^{\binom{n}{2} - \binom{p}{2}}$. Tendo em conta que existem $\binom{n}{p}$ subconjuntos P distintos, o número total de subgrafos completos de ordem p em \mathcal{G}_n é não superior a $\binom{n}{p} 2^{\binom{n}{2} - \binom{p}{2}}$ e a proporção de subgrafos K_p no conjunto \mathcal{G}_n é $\binom{n}{p} 2^{-\binom{p}{2}}$. Porém,

$$\binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p!} \leq \frac{n^p}{2^{p-1}} < \frac{2^{p^2/2}}{2^{p-1}},$$

se $n < 2^{p/2}$ e, consequentemente, para estes valores de n , a proporção de subgrafos K_p é inferior a $1/2$. Com efeito,

$$\begin{aligned} 2^{p^2/2-p+1} 2^{-\binom{p}{2}} &= 2^{(p^2-2p+2)/2} 2^{-\binom{p}{2}} \\ &= 2^{((p-1)^2+1-p(p-1))/2} \\ &= 2^{((p-1)(p-1-p)+1)/2} \\ &= \frac{1}{2^{p/2-1}} \\ &< \frac{2}{n} \quad (\text{tendo em conta a desigualdade } n < 2^{p/2}) \\ &\leq \frac{1}{2} \quad (\text{uma vez que } n \geq 4). \end{aligned}$$

Com argumentos semelhantes se conclui que a proporção de conjuntos independentes de cardinalidade p é inferior a $\frac{1}{2}$ e, consequentemente, existe pelo menos um grafo em \mathcal{G}_n que não tem uma clique de cardinalidade p nem um conjunto independente de cardinalidade p . Logo, $R(p, p) \geq 2^{p/2}$. \square

Os números de Ramsey podem generalizar-se para colorações de arestas com mais do que duas cores, de acordo com o teorema que se segue.

Teorema 19.30 (Ramsey [78]). *Dados os inteiros positivos p_1, p_2, \dots, p_k , existe um inteiro positivo mínimo, $R(p_1, p_2, \dots, p_k)$, tal que, para $\nu \geq R(p_1, \dots, p_k)$, colorindo as arestas de K_ν com as cores $1, 2, \dots, k$, existe $i \in \{1, \dots, k\}$ e um subgrafo de K_ν , completo, K_{p_i} , com arestas de cor i .*

Demonstração. Vamos fazer a prova por indução sobre k , tendo em conta que para $k = 1$ o resultado é trivialmente verdadeiro e para $k = 2$ decorre do Corolário 19.28. Assim, suponha $k > 2$ e que o resultado se verifica para $k - 1$, ou seja, existe um inteiro positivo mínimo, $R(p_1, \dots, p_{k-1})$, tal que para $n \geq R(p_1, \dots, p_{k-1})$, colorindo as arestas de K_n com as cores $1, \dots, k-1$, existe $i \in \{1, \dots, k-1\}$ e um subgrafo de K_n , completo, K_{p_i} , com arestas de cor i . Assim, sendo $p = R(p_1, p_2, \dots, p_{k-1})$ e $q = p_k$, de acordo com o Corolário 19.28, existe um número positivo mínimo $R(p, q)$, tal que para $\nu \geq R(p, q)$, a coloração das arestas de K_ν , com as cores A ou B , produz pelo menos um dos seguintes casos:

- (a) existe um subgrafo de K_ν , completo, K_p , com arestas de cor A ;
- (b) existe um subgrafo de K_ν , completo, K_q , com arestas de cor B .

Vamos considerar A , não como uma cor específica, mas como o conjunto de $k - 1$ cores possíveis, $\{1, 2, \dots, k - 1\}$, e $B = k$. Como consequência, obtém-se um subgrafo de K_ν , completo, K_{p_k} , com

arestas de cor k (de acordo com (b)) ou K_p , com arestas coloridas com uma das cores tiradas do conjunto $\{1, \dots, k-1\}$ (de acordo com (a)). Neste último caso, por hipótese de indução, existe $i \in \{1, \dots, k-1\}$ e um subgrafo de K_p e, consequentemente, de K_ν , completo, K_{p_i} , com arestas de cor i . \square

19.4. Exercícios

- 19.1. Uma escola tem as seguintes sete disciplinas para oferecer num curso de verão: Matemática (M), Inglês (I), Português (P), História (H), Ciências (C), Geografia (G) e Religião e Moral (R). Os 12 alunos que vão frequentar este curso efectuaram as seguintes escolhas:

António (M), (C), (P).

Bruno (M), (C), (G).

Carla (I), (P).

Daniela (M), (I), (C).

Eduardo (I), (R).

Filipe (I), (H).

Gaspar (M), (C).

Hélder (I), (P).

Ilda (I), (R).

Joana (M), (C), (G).

Luís (I), (P).

Sofia (G), (R).

Admitindo que todas as disciplinas têm aulas com a mesma duração e sabendo que se pretende determinar um horário que minimize o número de intervalos de tempo para funcionamento das disciplinas, sem que qualquer dos alunos tenha sobreposição de aulas de disciplinas que escolheu, responda às seguintes questões:

- (a) Modele este problema como um problema de coloração de vértices de um grafo G .
- (b) Determine a solução óptima, ou seja, $\chi(G)$ e uma coloração dos vértices com $\chi(G)$ cores.

- 19.2. Dado um grafo simples k -regular, G , prove que se G admite um vértice de corte então $\chi'(G) > k$.

- 19.3. Prove que todo o grafo perfeito é um grafo de Berge (ou seja, é um grafo tal que nem ele nem o complementar contém um ciclo induzido de comprimento ímpar não inferior a 5).

- 19.4. Prove que os grafos de comparabilidade de conjuntos parcialmente ordenados são grafos perfeitos.

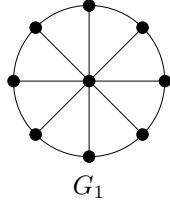
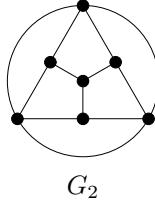
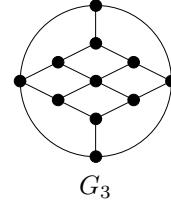
- 19.5. Por aplicação do algoritmo guloso (greedy) para coloração de vértices, determine uma coloração dos vértices do grafo representado na Figura 19.4.

- 19.6. Determine o polinómio cromático do grafo representado na Figura 19.1 tendo em conta que, de acordo com o Exemplo 19.7,

$$f(C_4, \lambda) = \lambda^4 - 4\lambda^3 + 6\lambda^2 - 3\lambda.$$

- 19.7. Determine o polinómio cromático de $K_{2,3}$.

- 19.8. Considerando o grafo G representado na Figura 19.4 com a coloração parcial $\kappa : W \rightarrow \{1, 2, 3, 4, 5\}$, onde $W = \{a, b, c, d, e\} \subset V(G)$ e $\kappa(a) = 1, \kappa(b) = 2, \kappa(c) = 3, \kappa(d) = 4$ e $\kappa(e) = 5$, determine o polinómio das extensões cromáticas de κ , $f_\kappa(G, \lambda)$.
- 19.9. Prove a desigualdade $R(n + 2, 3) > 3n$, para $n > 1$.
- 19.10. Supondo que as arestas de K_6 são coloridas utilizando unicamente duas cores, demonstre as seguintes proposições:
- Existem pelo menos dois triângulos monocromáticos.
 - Existe pelo menos um ciclo C_4 monocromático.
- 19.11. Prove que o teorema de Vizing (a desigualdade (19.11)) é apenas válido para grafos simples.
- 19.12. Considere um grafo G , tal que $|E(G)| \geq |V(G)|$.
- Prove que G contém pelo menos um ciclo.
 - Verifique a veracidade da afirmação: cada vértice de G pertence a pelo menos um ciclo.
 - Supondo que G é o grafo K_{2m+1} e que as suas arestas são coloridas arbitrariamente com recurso a m cores, mostre que existe um ciclo monocromático.
- 19.13. Represente um dos grafos G de menor ordem que não é perfeito e é tal que $\chi(G) = \omega(G)$.
- 19.14. Determine o número cromático dos grafos a seguir representados:

 G_1  G_2  G_3

- 19.15. Determine o número mínimo de cores necessárias para a colorir propriamente as faces de um cubo.
- 19.16. Um tratador de cobras mantém cinco cobras (A, B, C, D, E) guardadas em caixas no seu apartamento. Algumas atacam as outras, pelo que não podem ser guardadas na mesma caixa. Na tabela a seguir, as entradas com asterisco indicam que as cobras que lhe correspondem não podem estar juntas. Qual o menor número de caixas necessárias para guardar todas as cobras?

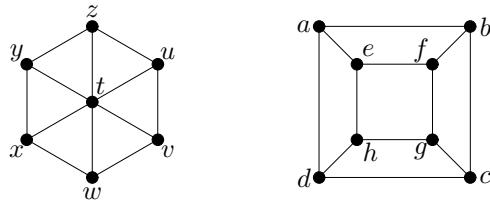
	A	B	C	D	E
A	—	*	*	*	*
B	*	—	*	—	—
C	*	*	—	*	—
D	*	—	*	—	*
E	*	—	—	*	—

- 19.17. Para cada λ , determine o número de colorações próprias dos vértices dos grafos a seguir indicados, com recurso a λ cores.
- Grafo completo K_6 .
 - Grafo $K_{1,5}$ (estrela).

- (c) Grafo linha de P_6 .
 (d) Grafos $K_{1,n}$, $K_{2,n}$ e $K_{3,n}$.

- 19.18. Determine os polinómios cromáticos dos grafos P_4 , $K_{1,3}$, C_4 , K_4 e verifique que cada um destes polinómios tem a forma $\lambda^4 - \varepsilon\lambda^3 + a\lambda^2 - b\lambda$, onde ε o correspondente número de arestas e $a, b \in \mathbb{N}$.
- 19.19. Determine o polinómio cromático de C_5 .
- 19.20. Prove o Teorema 19.19.
- 19.21. Determine o índice cromático do cubo Q_3 e do octaedro.
- 19.22. Prove que um grafo tem número cromático 2 se e só se não contém ciclos de comprimento ímpar.
- 19.23. Prove que todo o grafo G contém um subgrafo abrangente bipartido H tal que $d_H(x) \geq \frac{1}{2}d_G(x) \forall x \in V(G) = V(H)$. Adicionalmente, deduza a desigualdade $\varepsilon(H) \geq \frac{1}{2}\varepsilon(G)$.
- 19.24. É possível atribuir duas cores aos vértices de um grafo G de tal forma que no máximo metade da vizinhança de cada vértice v contém as mesmas cores que v ?
- 19.25. Dê um exemplo de um grafo G tal que $\Delta(G) = \chi'(G) = \varepsilon(G)$ e de um grafo H tal que $\Delta(H) < \chi'(H) < \varepsilon(H)$.
- 19.26. Determine o índice cromático do grafo de Petersen.
- 19.27. Dado um grafo arbitrário G , prove as desigualdades $\Delta(G) \leq \chi'(G) \leq 2\Delta(G) - 1$.
- 19.28. Dado um grafo simples G , prove a desigualdade $\chi'(G) \leq \Delta(G) + 1$.
- 19.29. Prove que cada grafo $2k$ -regular contém um 2-factor e, a partir deste resultado, prove também que se G é um grafo sem lacetes, então $\chi'(G) \leq 3 \left\lceil \frac{\Delta(G)}{2} \right\rceil$.
- 19.30. Dado um grafo bipartido G tal que $\delta(G) \geq 1$, prove que o número de estabilidade de G , $\alpha(G)$, é igual à cardinalidade de um conjunto de cobertura de vértices por arestas (ou seja, conjunto de arestas que cobrem todos os vértices do grafo) de cardinalidade mínima.

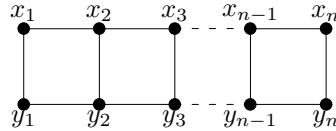
- 19.31. Considere os grafos representados na figura a seguir e responda às seguintes questões:
- Determine dois conjuntos independentes (de vértices) maximais com cardinalidades distintas.
 - Determine $\alpha(G)$, para cada um dos grafos G representados.
 - Determine o número de estabilidade dos grafos $K_{1,3}$, $K_{2,3}$, $K_{2,4}$, $K_{4,4}$, $K_{4,6}$ e $K_{m,n}$;
 - Sabendo que I é um conjunto independente (de vértices) de G , indique o tipo de grafos induzidos pelos subconjuntos não vazios de I em G^c ?



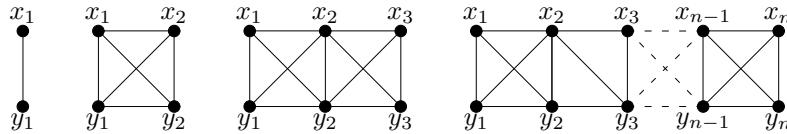
- 19.32. Considere um grafo não nulo G e prove que $I \subseteq V(G)$ é um estável de G se e só se $V(G) \setminus I$ é um conjunto de cobertura (de arestas por vértices) de G .

19.33. Seja G o grafo representado na figura a seguir.

- (a) Determine $\varepsilon(G)$ e o polinómio cromático $P_G(\lambda)$.
- (b) Dado o inteiro não negativo n , seja a_n o número de modos de seleccionar n arestas em $E(G)$ sem que existam arestas com um extremo comum. Formule e resolva uma equação de recorrência para a_n .



19.34. Considere os grafos representados na figura a seguir e seja a_n o número de subconjuntos do conjunto $\{x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n\}$ que constituem conjuntos independentes. Formule e resolva a equação de recorrência para a_n .



19.35. Sabendo que um grafo G , sem lacetes, é "crítico para a coloração de vértices", se $\chi(G) > \chi(G - v) \forall v \in V(G)$, responda:

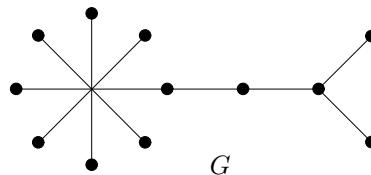
- (a) Prove que os ciclos com um número ímpar de vértices são "críticos para a coloração de vértices", enquanto os ciclos com um número par de vértices não são "críticos para a coloração de vértices".
- (b) Determine os valores de $n \in \mathbb{N}$ para os quais K_n é "crítico para a coloração de vértices".
- (c) Se um grafo G é "crítico para a coloração de vértices", então G é conexo.
- (d) Prove que se G é "crítico para a coloração de vértices", então $d_G(v) \geq \chi(G) - 1 \forall v \in V$.

19.36. Tendo em conta que dado um grafo G e um subconjunto de vértices $\emptyset \neq S \subset V(G)$, $\partial(S)$ denota o corte definido por S , ou seja, $\partial(S) = \{xy \in E(G) : x \in S \wedge y \in V(G) \setminus S\}$, prove que um grafo H é k -aresta-conexo se e só para todo o subconjunto não vazio de vértices $U \subset V(H)$, $|\partial(U)| \geq k$.

19.37. Considerando um grafo arbitrário G , prove as desigualdades $\chi(G) \leq \chi'(G) \leq \Delta(G) + 1$. Adicionalmente, no caso particular do k -cubo, Q_k , prove a igualdade $\chi'(Q_k) = k = \chi(Q_k)$.

19.38. Determine os valores de $\chi(G)$ e $\chi'(G)$ para cada um dos seguintes grafos:

- (a) K_9 ;
- (b) $K_{5,6}$;
- (c) K_{10} ;
- (d) grafo representado na figura a seguir.



19.39. Considere um grafo $\Omega(n)$ cujos vértices são os n -uplos de componentes $+1$ ou -1 tal que dois vértices são adjacentes se os correspondentes vectores são ortogonais, ou seja, considerando os n -uplos como sequências de dígitos 1 e -1 , dois vértices são adjacentes se e só se a distância de Hamming (ver definição na pag. 508) entre as sequências que lhes correspondem é igual a $n/2$. Tendo em conta que, nestas condições, uma clique de cardinalidade n corresponde a uma matriz de Hadamard de ordem n (ver Definição 9.10 na pag. 263), responda às seguintes questões:

- (a) Prove a desigualdade $\omega(\Omega(n)) \leq n$;
- (b) Prove que se n é uma potência de 2 , então $\omega(\Omega(n)) = n$.

20

Grafos Planares e Generalizações

Exemplos muito comuns de grafos planares são os que se referem à representação de mapas de estradas. Com efeito, os mapas de estradas, na ausência de viadutos, são grafos que apresentam a particularidade de se poderem representar numa folha de papel sem que as arestas se cruzem, uma vez que aos cruzamentos e entroncamentos correspondem vértices. Quando um grafo, G , admite uma representação numa superfície, S , sem que existam arestas que se intersectem, diz-se que G é *realizável* (mergulhável) em S .

Definição 20.1 (Grafo planar, grafo não-planar e grafo plano). *Um grafo diz-se planar se admite uma realização (mergulho ou imersão) no plano e, nesse caso, essa realização designa-se por grafo plano, caso contrário diz-se não-planar.*

Note-se que, apesar de um grafo poder aparecer representado no plano com arestas que se cruzam, isso não significa que não seja planar, uma vez que pode existir outro modo de o representar sem que o cruzamento de arestas ocorra. Assim, há que distinguir entre o grafo abstracto (onde os conjuntos de vértices e arestas são entidades abstractas) da sua realização numa superfície.

Uma vez que a projecção estereográfica converte figuras do plano em figuras da esfera e reciprocamente (ver o exemplo da Figura 20.1), podemos afirmar que um grafo é planar se e só se é realizável na esfera.

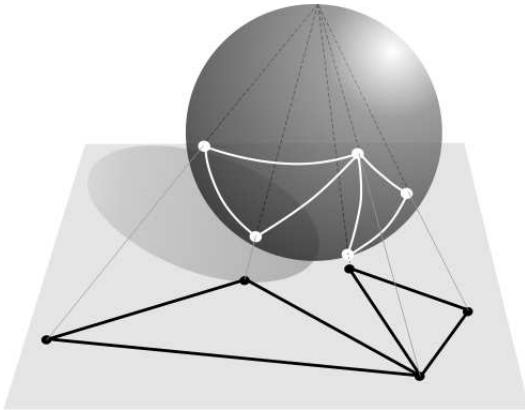


Figura 20.1: Exemplificação da projecção estereográfica

20.1. O ponto de vista topológico

Nesta secção, excepção feita ao plano (que não é compacto), vamos considerar unicamente realizações de grafos em variedades compactas de dimensão dois, orientáveis. Uma *variedade compacta* de dimensão dois, é uma superfície S com as seguintes propriedades:

1. cada ponto de S tem uma vizinhança homeomorfa¹ a uma bola aberta;

¹Um conjunto A é homeomorfo a um conjunto B se existe uma aplicação contínua com inversa contínua entre A e

2. toda a cobertura de S , com bolas abertas, tem uma subcobertura finita.

Adicionalmente, dizemos que uma superfície S é *orientável* se é possível definir um referencial tridimensional (com dois eixos no plano tangente à superfície) que se desloque ao longo de qualquer curva fechada representada em S , sem alterar o sentido dos eixos quando regressa ao ponto inicial. Caso contrário, dizemos que S é *não-orientável*. Por exemplo, a fita de Möbius, representada na figura a seguir, é exemplo de uma superfície não-orientável.

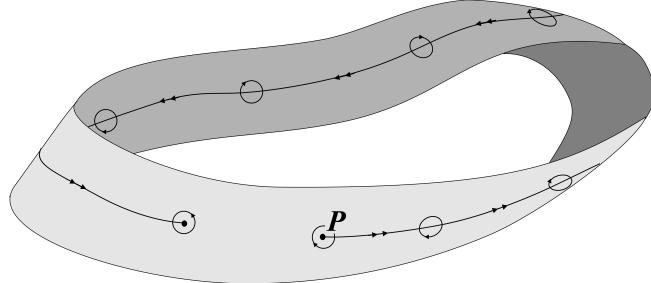


Figura 20.2: Ilustração da não orientabilidade da fita de Möbius.

No nosso caso, porém, apenas vamos considerar superfícies orientáveis sem bordo, como são a esfera que se denota por S_0 (não tem buracos, i.e., tem genus 0), torus S_1 (um buraco, i.e., genus 1), torus duplo S_2 (dois buracos, i.e., genus 2), torus triplo S_3 (três buracos, i.e., genus 3), etc., ou superfícies topologicamente equivalentes a estas². Estas superfícies, que genericamente se designam por *superfícies de Riemann fechadas*, denotam-se por S_g , onde g indica o genus da superfície.

20.1.1 Realização de grafos em superfícies orientáveis

A realização de um grafo G numa superfície S_g , que usualmente se designa por *mapa* em S_g e se denota por $M(G)$, implica que cada vértice de G corresponda a um ponto de S_g e cada aresta corresponda a uma curva simples (ver definição mais adiante), ligando dois vértices sem que nenhum par de curvas se intersecte num ponto, com eventual exceção dos respectivos pontos extremos (vértices). Assim, do ponto de vista topológico, um grafo é um mapa $M(G)$ que corresponde a uma realização numa superfície S_g de um certo grafo G e que é definido por um conjunto finito de curvas simples de S_g , que denotamos por $E_{M(G)}$ (e também se designam por arestas), de tal forma que quaisquer duas destas curvas têm intersecção vazia ou numa das suas extremidades, denominando-se o conjunto destas extremidades (que também se designam por vértices) por $V_{M(G)}$. Neste contexto, dizemos que um grafo, G , é conexo, se quaisquer dois vértices de uma sua realização $M(G)$ se podem ligar por uma curva ou por concatenação de várias curvas (arestas) de $E_{M(G)}$.

Uma curva em \mathbb{E}^2 (espaço euclidiano de dimensão dois) é um subconjunto $C \subset \mathbb{E}^2$, para o qual existe uma aplicação contínua injetiva $c : [0, 1] \rightarrow \mathbb{E}^2$ tal que $c([0, 1]) = C$. Se c é apenas injetiva em B .

² Esquematicamente, duas superfícies são topologicamente equivalentes se uma se pode transformar na outra deformando-se elasticamente (i.e. sem quebrar ou rasgar de modo a criar um novo buraco).

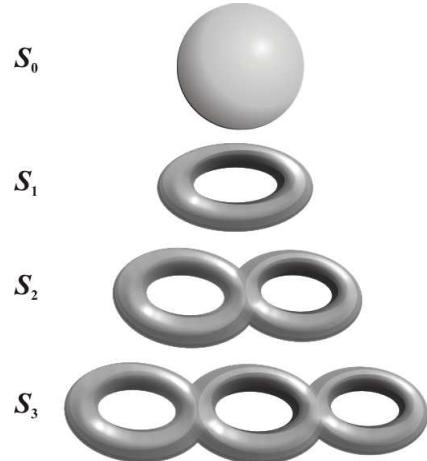


Figura 20.3: Esfera, torus, torus duplo e torus triplo.

$[0, 1]$ e $c(0) = c(1)$, diz-se que C é uma *curva fechada de Jordan*. Nestas condições, uma curva é um subconjunto de \mathbb{E}^2 homeomorfo ao intervalo $[0, 1]$ e uma curva fechada de Jordan é um subconjunto de \mathbb{E}^2 homeomorfo à circunferência. Qualquer destas curvas, C , se designa por *curva simples* e a respectiva aplicação, c , por *parametrização* de C . Adicionalmente, $C \subset \mathbb{E}^2$ diz-se um *conjunto separador* de \mathbb{E}^2 (ou conjunto que separa \mathbb{E}^2), se $\mathbb{E}^2 \setminus C$ tem mais do que uma componente conexa (i.e., subconjunto conexo³ maximal, no sentido da inclusão), caso contrário diz-se não-separador. Camille Jordan⁴ enunciou em 1897 o teorema de separação para \mathbb{E}^2 que a seguir se apresenta, o qual, no entanto, só mais tarde, 1905, veio a ser provado por Oswald Veblen⁵.

Teorema 20.1 (da curva fechada de Jordan). *Se C é uma curva fechada de Jordan em \mathbb{E}^2 , então C separa \mathbb{E}^2 .*

Embora este teorema estabeleça um resultado intuitivamente verdadeiro, a sua demonstração foi muito difícil de obter e cai fora do âmbito deste livro. Os mais curiosos, podem consultá-la, por exemplo, em [6].

Como consequência imediata, do Teorema 20.1 decorre que se C é uma curva fechada de Jordan em \mathbb{E}^2 , então $\mathbb{E}^2 \setminus C$ é a união disjunta de dois conjuntos abertos, $d_{int}(C)$ (domínio interior a C) e $d_{ext}(C)$ (domínio exterior a C), tais que $d_{int}(C)$ é limitado, $d_{ext}(C)$ é ilimitado e, tanto $d_{int}(C)$ como $d_{ext}(C)$ são conexos por arcos. Por outro lado, toda a curva que liga um ponto de $d_{int}(C)$ a um ponto de $d_{ext}(C)$ tem pelo menos um ponto comum com C .

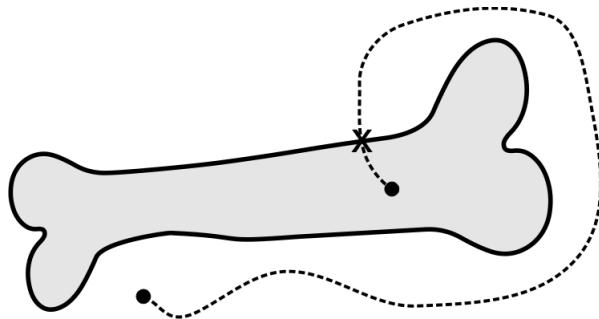


Figura 20.4: Representação de uma curva fechada de Jordan C e de uma curva simples com extremos em $d_{int}(C)$ e $d_{ext}(C)$, respectivamente.

No caso de uma superfície S (orientável ou não), em geral, não basta uma curva fechada de Jordan para separar S , sendo o *genus* de S , precisamente, o maior número de curvas fechadas de Jordan disjuntas que constituem um conjunto não-separador. Por exemplo, é fácil ver que na esfera qualquer curva fechada de Jordan constitui um conjunto separador, enquanto no torus existem curvas fechadas de Jordan não-separadoras (mas quaisquer duas curvas fechadas de Jordan disjuntas formam um conjunto separador). Nesta definição de genus de uma superfície, baseada no maior número de curvas fechadas de Jordan não-separadoras, é absolutamente essencial considerá-las disjuntas, uma vez que, por exemplo, no torus, é possível representar duas curvas fechadas de Jordan que constituem um conjunto não-separador, as quais, no entanto, se intersectam num ponto.

³Dizemos que um conjunto X é conexo por arcos se entre quaisquer dois pontos existe uma curva simples totalmente contida em X e, para os objectivos que nos interessam, por enquanto, basta saber que todo o conexo por arcos é um conjunto conexo (embora o recíproco, em geral, não seja verdadeiro). Para clarificação destes conceitos, consultar, por exemplo, [66].

⁴Marie Ennemond Camille Jordan (1838-1922), matemático francês que foi um dos fundadores da teoria das funções e que trabalhou em álgebra, topologia, equações diferenciais e cristalografia.

⁵Oswald Veblen (1880-1960), matemático americano de origem norueguesa que trabalhou em geometria diferencial.

A realização de um grafo H numa superfície S_g proporciona a partição dessa superfície nas componentes conexas de $S_g \setminus E_{M(H)}$ que se designam por *regiões*. Sendo $M(G)$ uma realização de um grafo G em S_g , designa-se por *célula* ou *face*, toda a componente conexa do complementar de $E_{M(G)}$ em S_g homeomorfa a uma bola aberta de \mathbb{E}^2 . Uma realização diz-se celular (alguns autores preferem a designação 2-cellular) se todas as regiões criadas por essa realização são células ou faces.

Podemos desde já adiantar (conforme Teorema 20.21, mais adiante) que todas as realizações em S_g se podem converter em realizações celulares em $S_{g'}$, para algum $g' \leq g$. Por simplicidade, de agora em diante, designaremos também por grafo uma sua realização e utilizaremos indiferentemente a notação G ou $M(G)$, fazendo-se a respectiva distinção de acordo com o contexto.

O conjunto das faces criadas por uma realização celular de G em S_g denota-se por $F_g(G)$. Como regra prática para a detecção de faces (ou células) de um grafo, G , realizado numa superfície S_g , pode adoptar-se a seguinte:

Uma região de G é uma face (ou célula) se e só se a sua fronteira é contractível a um ponto, ou seja, se e só se é possível "reduzi-la", continuamente, até a transformar num ponto.

Na Figura 20.5, apenas a primeira realização de um grafo G , de entre as apresentadas, é uma realização celular.

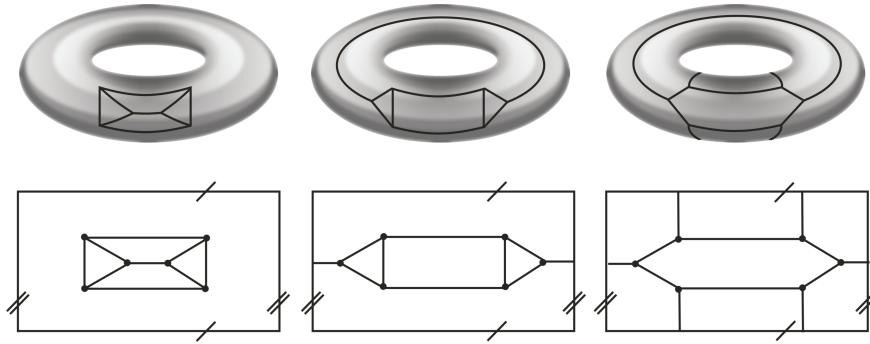


Figura 20.5: Três realizações de um grafo G no torus, onde só a primeira é celular.

20.1.2 Menores e menores topológicos

Como veremos, mais adiante, os conceitos de menor e de menor topológico estão intimamente relacionados com a caracterização de grafos planares. Na década de 1980, Robertson e Seymour desenvolveram a teoria dos menores de grafos e publicaram duas dezenas de artigos sobre esta teoria. Pela sua grande complexidade e importância no contexto deste capítulo, entre os resultados obtidos, coligidos em [84], destacamos a prova da conjectura de Wagner,⁶ publicada em [102], segundo a qual *em toda a coleção infinita de grafos finitos existem dois grafos tais que um é menor de outro*.

Por definição, uma classe de grafos \mathcal{C} diz-se *fechada para menores* se para todo o grafo $G \in \mathcal{C}$ qualquer menor de G pertence também a \mathcal{C} . Assim, dada uma família de grafos $\{G_1, G_2, \dots\}$, se definirmos a classe de grafos \mathcal{C} como sendo o conjunto dos grafos que não têm nenhum dos grafos G_1, G_2, \dots como menor, é claro que esta classe é fechada para menores, pelo que, os grafos G_1, G_2, \dots caracterizam \mathcal{C} como a classe de grafos com menores proibidos G_1, G_2, \dots . Reciprocamente, também se pode concluir que toda a classe de grafos fechada para menores pode ser caracterizada por menores proibidos (desde que se possam listar todos os grafos que não pertencem à família). Da conjectura de Wagner, agora teorema (depois da prova obtida por Robertson e Seymour), decorre o seguinte resultado:

⁶Klaus Wagner (1910-2000), matemático alemão.

Teorema 20.2 (Robertson e Seymour). *Toda a classe de grafos fechada para menores pode ser caracterizada por uma família finita de menores proibidos.*

Tendo em conta que se um grafo é realizável numa superfície S , então os seus menores também são, segue-se um corolário que é consequência imediata do Teorema 20.2.

Corolário 20.3. *Para cada variedade compacta de dimensão dois, superfície S orientável ou não-orientável, existe uma lista finita de grafos L , tal que um grafo arbitrário G é realizável em S se e só se nenhum dos grafos de L é menor de G .*

Nesta altura, convém relembrar as seguintes operações sobre grafos:

1. *eliminação* de arestas;
2. *eliminação* de vértices;
3. *contracção* de arestas;
4. *subdivisão* de arestas.

Dado um grafo G , seja $e \in E(G)$ e $E' = \{e_1, \dots, e_k\} \subset E(G)$.

1. A operação de eliminação da aresta e que se denota por $G - e$ corresponde à obtenção do grafo H tal que $V(H) = V(G)$ e $E(H) = E(G) \setminus \{e\}$. Mais geralmente, considerando o subconjunto de arestas E' , $G - E'$ corresponde ao grafo obtido de G por eliminação sucessiva (independentemente da ordem) das arestas e_1, \dots, e_k . Note-se que esta operação já foi introduzida na Secção 12.5, na sequência da Definição 12.19.
2. De modo semelhante se define a operação de eliminação de vértices, tendo em conta que, neste caso, ao eliminar-se um vértice (ou conjunto de vértices) também se eliminam (automaticamente) as arestas que lhe(s) é (são) incidente(s).
3. A operação de contracção de e em G denota-se por G/e e, de acordo com a Definição 15.3 do Capítulo 15, corresponde ao grafo obtido pela sobreposição dos vértices extremos de e e pela eliminação dos lacetos e arestas paralelas, eventualmente produzidas. Mais geralmente, dado um subconjunto de arestas, E' , G/E' corresponde ao grafo obtido após a contracção sucessiva (independentemente da ordem) das arestas e_1, \dots, e_k .
4. Designa-se por subdivisão de uma aresta e , a inserção de um vértice em e (o qual, naturalmente, passa a ter grau dois). Esta operação de subdivisão de zero ou mais arestas de um grafo G , também se designa por subdivisão ou *expansão* de G (pelo que, qualquer grafo é também uma subdivisão ou expansão de si próprio).

Definição 20.2 (Menor e menor topológico). *Dado um grafo G , designa-se por menor (ou menor combinatório) de G , toda a contracção de um subgrafo de G . Por sua vez, designa-se por menor topológico de G , todo o grafo H que admite uma subdivisão (ou expansão) que é um subgrafo de G , ou seja, H é um menor topológico de G se existe um subgrafo de G que é uma subdivisão (ou expansão) de H .*

De acordo com esta definição, um menor de um grafo G é um grafo obtido a partir de G , primeiro eliminando subconjuntos (eventualmente vazios) de arestas e vértices e depois contraindo zero ou mais arestas. Logo, todo o subgrafo de um grafo é também um seu menor e, consequentemente, todo o grafo é menor de si próprio. O mesmo acontece para os menores topológicos, ou seja, todo o subgrafo de um grafo é também um seu menor topológico e, consequentemente, todo o grafo é um menor topológico de si próprio.

A Figura 20.6 exemplifica a subdivisão de arestas de um grafo, obtendo-se um grafo \hat{G} que é uma subdivisão de G , pelo que, neste caso, G é um menor topológico de \hat{G} .

Das definições de menor e menor topológico, decorre que todo o menor topológico de um grafo G é também um menor de G . Porém, o recíproco, em geral, não é verdadeiro. Por exemplo, K_5 é um menor do grafo de Petersen (grafo representado na Figura 14.4), uma vez que é uma contracção do grafo de Petersen, mas não é um menor topológico, uma vez que o grafo de Petersen não contém uma subdivisão de K_5 .

Dados dois grafos X e Y , se X é um menor de Y , denota-se esse facto por $X \preceq Y$, provando-se facilmente que esta relação, \preceq , é uma relação de ordem parcial no conjunto dos grafos finitos e que o mesmo acontece relativamente à relação de menor topológico (ou seja, ambas as relações são reflexivas, anti-simétricas e transitivas).

Um conjunto parcialmente ordenado, (P, \preceq) , diz-se *bem-pré-ordenado* ou que tem uma *boa-pré-ordem*⁷ se em toda a sequência infinita (p_1, p_2, \dots) de elementos de P , existem dois elementos, p_i e p_j , tais que $i < j$ e $p_i \preceq p_j$, o que equivale a afirmar que (P, \preceq) não contém uma cadeia infinitamente descendente, nem uma anticadeia infinita (ver Definição 7.26).

Existem várias propriedades de grafos que são fechadas para menores, conforme se exemplifica a seguir.

- Um grafo diz-se *série-paralelo* se pode ser obtido a partir de uma única aresta, após uma sequência de zero ou mais operações de extensão em paralelo (cada uma das quais consiste na adição de uma nova aresta em paralelo a uma já existente) e operações de extensão em série (cada uma das quais consiste na subdivisão de uma aresta).

Se G é um grafo série-paralelo, então todos os seus menores são série-paralelo.

- Sabe-se que todo o grafo é realizável em \mathbb{R}^3 . Porém, podemos impor restrições adicionais relativamente a esta realização.

- Por exemplo, um grafo é *realizável sem ciclos ligados* se admite uma realização onde não existem ciclos disjunto que passem um por dentro do outro (tal como acontece numa cadeia de anéis).
- Outro exemplo, um grafo é *realizável sem nós* se admite uma realização sem ciclos que se entrelaçam a si próprios.

Estes dois exemplos mostram duas propriedades topológicas dos grafos que são fechadas para menores.

Relativamente aos grafos série-paralelo, em 1952, Dirac [32] provou o seguinte teorema:

Teorema 20.4 (Dirac). *Um grafo é série-paralelo se e só se não tem K_4 como menor.*

Relativamente aos grafos realizáveis sem ciclos ligados, Horst Sachs [89] provou que todo o grafo que admite um grafo da família de Petersen (representada na Figura 20.7) como menor não é realizável sem ciclos ligados. Reciprocamente, conjecturou que todo o grafo que não admite uma realização sem ciclos ligados tem um dos grafos da família de Petersen como menor. Em 1995 Robertson, Seymour e Thomas [86] provaram a conjectura de Sachs.

Teorema 20.5 (Robertson, Seymour e Thomas). *Um grafo é realizável sem ciclos ligados se e só se nenhum dos seus menores é um dos sete grafos representados na Figura 20.7.*

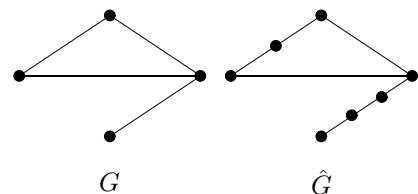


Figura 20.6: Grafo \hat{G} obtido por subdivisão de arestas de G .

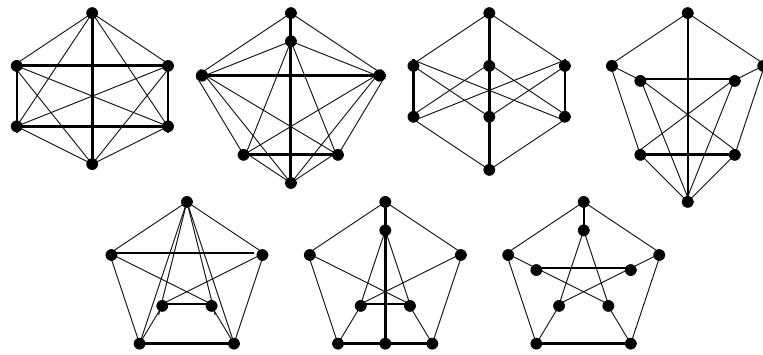


Figura 20.7: Família de Petersen

Note-se que os Teoremas 20.4 e 20.5 são casos particulares do Teorema 20.2. Para além do Teorema 20.2, Robertson e Seymour também provaram que para todo o grafo H , existe um algoritmo com complexidade $\mathcal{O}(\nu^3)$ (ver Apêndice A) que, dado um grafo G de ordem ν , verifica se H é ou não um menor de G . Assim, apesar de em geral não se conhecer um procedimento para a determinação de menores proibidos de famílias de grafos, nem se conhecer um majorante para o número de tais menores proibidos, podemos tirar a seguinte conclusão:

Para toda a família de grafos \mathcal{F} , fechada para menores, existe um algoritmo cúbico que verifica se um grafo arbitrário G pertence a \mathcal{F} . Logo, caso se conheça a lista, L , dos menores proibidos que caracterizam \mathcal{F} , para uma tal verificação, basta testar se existe um grafo em L que é menor de G .

Como consequência, é claro que podemos testar em $\mathcal{O}(\nu^3)$ se um grafo G de ordem ν é série-paralelo, bastando verificar, de acordo com o Teorema 20.4, se K_4 é um seu menor. Adicionalmente, também podemos testar em $\mathcal{O}(\nu^3)$ se G é realizável sem ciclos ligados, bastando verificar, de acordo com o Teorema 20.5, se algum dos grafos da família de Petersen (representada na Figura 20.7) é um seu menor. Para a realização de grafos em superfícies orientadas arbitrárias, com excepção da esfera, não se conhecem conjuntos de menores proibidos que caracterizem os grafos realizáveis em S_g . No caso particular do torus, os testes computacionais efectuados têm revelado a existência de milhares de menores proibidos para a família dos grafos realizáveis em S_1 .

20.2. Grafos planares

Dada um grafo plano, que se pode obter pela projecção estereográfica de uma realização na esfera de um grafo planar, para além das faces limitadas, existe uma face exterior ao grafo (i. e., a porção de espaço que o envolve) que se designa por *face ilimitada*.

O teorema que se segue, consta (sem prova) numa carta enviada por Euler, em 1750, a Goldbach. As primeiras demonstrações foram obtidas por Legendre (em 1794), l'Huilier (em 1811 - 1812) e Cauchy (em 1813).

Teorema 20.6 (da fórmula de Euler). *Se G é um grafo conexo e planar, então, para qualquer realização plana,*

$$|F_0(G)| = \varepsilon(G) - \nu(G) + 2.$$

⁷Convém lembrar que, tal como se referiu na Subsecção 7.3.5 do Capítulo 7, uma relação de pré-ordem (*quasi-order* na terminologia inglesa) é uma relação reflexiva e transitiva. Como consequência, toda a relação de ordem parcial é uma relação de pré-ordem.

Demonstração. Vamos fazer a prova por indução sobre o número de arestas, tendo em conta que o resultado é verdadeiro para grafos conexos planos não nulos com zero ($0 - 1 + 2 = 1$) ou uma aresta ($1 - 2 + 2 = 1$).

Sendo G_n um grafo com n arestas, em geral, para $n > 1$, o grafo G_n obtém-se a partir de G_{n-1} acrescentando uma aresta a $E(G_{n-1})$, de uma das seguintes formas:

1. a nova aresta incide em vértices de G_{n-1} (ou seja, liga dois vértices $x, y \in V(G_{n-1}) = V(G_n)$);
2. a nova aresta liga um vértice de G_{n-1} a um novo vértice (pelo que $x \in V(G_{n-1}) = V(G_n) \setminus \{y\}$).

Seja $n > 1$ e, por hipótese de indução, vamos supor que a fórmula de Euler é válida para grafos conexos planos com menos que n arestas.

Em 1, a nova aresta vai provocar o aparecimento de um novo ciclo, consequentemente, uma nova face, pelo que $|F_0(G_n)| = |F_0(G_{n-1})| + 1$. Assim, dado que $\varepsilon(G_n) = \varepsilon(G_{n-1}) + 1$ e $V(G_n) = V(G_{n-1})$, conclui-se que a fórmula de Euler continua válida para G_n .

Em 2, a nova aresta não provoca o aparecimento de nenhuma face, pelo que $|F_0(G_n)| = |F_0(G_{n-1})|$. Uma vez que $\varepsilon(G_n) = \varepsilon(G_{n-1}) + 1$ e $\nu(G_n) = \nu(G_{n-1}) + 1$, conclui-se que a fórmula de Euler também se verifica para G_n . \square

20.2.1 Propriedades dos grafos planares

Embora o Teorema 20.6 seja válido para quaisquer grafos conexos e planares (simples ou não), tal não acontece com o corolário que a seguir se apresenta. Antes, porém, convém introduzir o conceito de grau de uma face de um grafo planar. Dado um grafo planar G e uma face $f \in F_0(G)$, designa-se por *grau* de f , o número de arestas da sua fronteira, considerando-as duplamente quando se trata de arestas de corte (como é o caso da aresta xy indicada na Figura 20.8, que conta duas vezes para o grau 10 da face K).

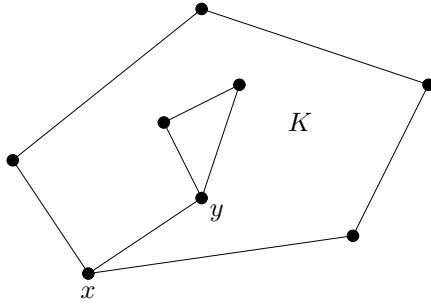


Figura 20.8: Exemplo de grafo planar com uma aresta de corte

Corolário 20.7 (do teorema que estabelece a fórmula de Euler). *Se G é um grafo simples, conexo e planar, com mais do que uma aresta, então $\varepsilon(G) \leq 3\nu(G) - 6$.*

Demonstração. Dado um grafo simples, conexo e planar, com mais do que uma aresta, considere-se uma sua realização plana G . Uma vez que cada face de G tem grau não inferior a 3, podemos concluir que a soma dos graus das $|F_0(G)|$ faces é não inferior a $3|F_0(G)|$. Por outro lado, esta soma dos graus de todas as faces é igual a $2\varepsilon(G)$ (dado que cada aresta conta duas vezes para esta soma). Logo, $3|F_0(G)| \leq 2\varepsilon(G)$ e, combinando esta desigualdade com a fórmula de Euler, obtém-se

$$3(\varepsilon(G) - \nu(G) + 2) \leq 2\varepsilon(G) \Leftrightarrow \varepsilon(G) \leq 3\nu(G) - 6.$$

\square

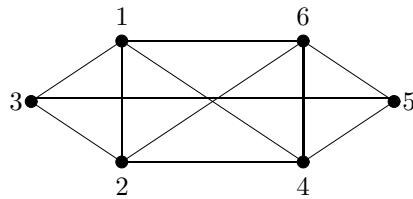


Figura 20.9: Exemplo de um grafo não-planar que verifica a desigualdade do Corolário 20.7.

Como consequência imediata deste corolário, podemos concluir que o grafo completo de ordem 5 (K_5) é não-planar, uma vez que $\varepsilon(K_5) = 10 > 9 = 3\nu(K_5) - 6$. Note-se, porém, que existem grafos não-planares, G , que verificam a desigualdade $\varepsilon(G) \leq 3\nu(G) - 6$, conforme a Figura 20.9 exemplifica.

Um outro modo de utilizar o Corolário 20.7 para se concluir sobre a eventualidade de um grafo simples ser não-planar, consiste em produzir alterações no grafo (as quais devem manter invariante a propriedade de ser planar ou não) e tentar mostrar que o grafo obtido não satisfaz o Corolário 20.7. Uma das alterações mais usuais utiliza a contracção de uma das arestas do grafo G em estudo, fazendo decrescer o número de arestas de uma unidade e $3\nu(G) - 6$ de 3 unidades, donde, em certos casos, a desigualdade do Corolário 20.7 pode deixar de se verificar.

Designa-se por *triangulação do plano* (ou *plana*) qualquer grafo simples, plano, onde todas as faces (incluindo a face ilimitada) têm fronteira triangular (ou seja, K_3). Verifica-se que qualquer triangulação do plano, G , tal que $\nu(G) \geq 4$, é um grafo, pelo menos 3-conexo (ver Definição 13.5). Designa-se por grafo *planar-maximal* todo o grafo simples planar que deixa de ser se lhe acrescentarmos uma aresta.

Teorema 20.8. *Um grafo simples, plano, de ordem não inferior a 3, é um grafo planar-maximal se e só se é uma triangulação do plano.*

Demonstração. Seja G um grafo simples, plano, de ordem não inferior a 3.

- Se G é uma triangulação do plano, então é um grafo simples, conexo, plano e $3|F_0(G)| = 2\varepsilon(G)$, donde, aplicando a fórmula de Euler, se obtém

$$3(\varepsilon(G) - \nu(G) + 2) = 2\varepsilon(G) \Leftrightarrow \varepsilon(G) = 3\nu(G) - 6.$$

Nestas condições, se acrescentarmos uma aresta e ao grafo G , de tal forma que $G + e$ se mantenha simples, então $\varepsilon(G + e) = \varepsilon(G) + 1 > 3\nu(G) - 6 = 3\nu(G + e) - 6$. Logo, de acordo com o Corolário 20.7, $G + e$ é não-planar.

- Se G não é uma triangulação do plano, então ou não é conexo (e, nesse caso, também não é planar-maximal) ou existe uma face $f \in F_0(G)$ cuja fronteira contém dois vértices que podem ser ligados por uma aresta e de modo a obter-se um grafo simples, $G + e$, que ainda é planar.

□

O corolário a seguir que, tal como o Corolário 20.7, só é valido para grafos simples, vai permitir concluir que o grafo bipartido completo $K_{3,3}$ é não-planar.

Corolário 20.9 (do teorema que estabelece a fórmula de Euler). *Se G é um grafo simples, conexo, bipartido e plano, com mais do que uma aresta, então $\varepsilon(G) \leq 2\nu(G) - 4$.*

Demonstração. Esta prova é idêntica à do Corolário 20.7, tendo em conta que, desta vez (de acordo com o Teorema 12.4), qualquer ciclo de um grafo bipartido tem comprimento par. Logo, cada face de um grafo simples, conexo, bipartido e plano, G , tem grau não inferior a 4. Como consequência,

$$4|F_o(G)| \leq 2\varepsilon(G) \Leftrightarrow 4(\varepsilon(G) - \nu(G) + 2) \leq 2\varepsilon(G) \Leftrightarrow \varepsilon(G) \leq 2\nu(G) - 4.$$

□

Deste corolário decorre, imediatamente, a não-planaridade de $K_{3,3}$, uma vez que $\varepsilon(K_{3,3}) = 9 > 8 = 2\nu(K_{3,3}) - 4$.

Em alternativa à condição necessária de planaridade estabelecida no Corolário 20.7, pode ainda concluir-se (com uma prova semelhante) que se um grafo simples conexo G de ordem n ($n \geq 3$) é planar e $g(G) < \infty$, então $\varepsilon(G) \leq \frac{g(G)(\nu(G)-2)}{g(G)-2}$. Com base nesta última desigualdade, podemos concluir que o grafo de Petersen (representado na Figura 14.4) é não-planar. Com efeito, sendo G o grafo de Petersen, dado que $g(G) = 5$, obtém-se

$$\varepsilon(G) = 15 > \frac{40}{3} = \frac{g(G)(\nu(G)-2)}{g(G)-2}.$$

Uma vez que qualquer subgrafo de um grafo planar é também planar e, por sua vez, qualquer supergrafo de um grafo não-planar é também não-planar e ainda que um grafo é planar se e só se o grafo simples de suporte (i.e., aquele que se obtém eliminando arestas paralelas e lacetes) é planar, tendo em conta os Corolários 20.7 e 20.9, podemos concluir que qualquer grafo que contenha K_5 ou $K_{3,3}$ como seu menor (combinatório ou topológico) é não-planar.

Teorema 20.10. *Todo o grafo simples, conexo e planar tem, pelo menos, um vértice de grau não superior a cinco.*

Demonstração. Dado um grafo simples conexo planar, seja G uma sua realização plana. Denotando por n_i o número de vértices de grau i (com $\delta(G) \leq i \leq \Delta(G)$), obtém-se as igualdades:

$$2\varepsilon(G) = \sum_{i=\delta(G)}^{\Delta(G)} in_i \quad \text{e} \quad \nu(G) = \sum_{i=\delta(G)}^{\Delta(G)} n_i.$$

Fazendo as respectivas substituições na desigualdade obtida no Corolário 20.7, vem

$$\frac{1}{2} \sum_{i=\delta(G)}^{\Delta(G)} in_i \leq 3 \sum_{i=\delta(G)}^{\Delta(G)} n_i - 6 \Leftrightarrow \frac{1}{2} \sum_{i=\delta(G)}^{\Delta(G)} n_i(6-i) \geq 6.$$

Logo, existe pelo menos um vértice com grau inferior a 6. □

Particularizando o resultado anterior para os grafos bipartidos planares, com facilidade se conclui a existência, nestes grafos, de pelo menos um vértice de grau não superior a três (ver Exercício 20.5).

20.2.2 Teorema de Kuratowski

O critério de planaridade fornecido pelo teorema de Kuratowski que, na sua versão original, estabelece que um grafo G é planar se e só se não admite K_5 nem $K_{3,3}$ como menores topológicos, foi generalizado por Wagner à não admissibilidade de K_5 ou $K_{3,3}$ como menores de G , ou seja, G é planar se e só se não admite K_5 nem $K_{3,3}$ como menores combinatórios. Assim, com base neste resultado, é possível utilizar o algoritmo cúbico, referido no final da Subsecção 20.1.2, para a verificação da planaridade de grafos. Nesta secção, apresentaremos um teorema que estabelece a equivalência entre os dois critérios e a sua validade, como condição necessária e suficiente de planaridade. Antes porém, vamos introduzir três lemas que serão de grande utilidade para a respectiva demonstração.

Lema 20.11. *Seja H um grafo não-planar que não contém um subgrafo contractível a K_5 ou $K_{3,3}$ e considere que H tem o mínimo número de arestas de entre os grafos com esta propriedade. Então H é 3-conexo.*

Demonstração. Seja H um grafo não-planar que não contém qualquer subgrafo contractível a K_5 ou $K_{3,3}$ e com o mínimo número de arestas de entre os grafos com esta propriedade. Adicionalmente, suponha que H não é 3-conexo e sejam $u, v \in V(H)$ tais que $H - \{u, v\}$ é desconexo. Então H é a união de dois grafos, H_1, H_2 , que se intersectam nos vértices u e v e, possivelmente, na aresta uv . Adicionando a aresta uv a cada um destes grafos (se ela ainda não lhes pertence), ou pelo menos um dos grafos resultantes, H'_1 ou H'_2 , é não-planar ou são ambos planares. No primeiro caso, obtém-se um grafo não-planar que não contém qualquer subgrafo contractível a K_5 ou $K_{3,3}$ com menos arestas do que as de H , o que é contraditório. No segundo caso, H'_1 e H'_2 admitem uma realização plana com a aresta uv na face ilimitada. Como consequência, podemos juntar estes grafos, sobrepondo a aresta uv e produzindo uma realização plana de H , o que também constitui uma contradição. \square

Lema 20.12. *Se H é um grafo 3-conexo distinto de K_4 , então existe $e \in E(H)$ tal que G/e é ainda 3-conexo.*

Demonstração. Suponha que H é um grafo 3-conexo distinto de K_4 e que não existe qualquer aresta $e \in E(H)$ cuja contracção produza um grafo ainda 3-conexo. Então, escolhendo uma aresta arbitrária uv , existe um vértice w tal que $H - \{u, v, w\}$ é um subgrafo desconexo com componentes H_1, H_2, \dots . Adicionalmente, cada um dos vértices u, v e w é adjacente a pelo menos um vértice de cada uma das componentes H_1, H_2, \dots (caso contrário, um subconjunto próprio de $\{u, v, w\}$ desconexa H). Escolhendo-se agora uv e w de tal forma que uma das componentes de $H - \{u, v, w\}$, H_1 , tenha o menor número possível de vértices, se $z \in V(H_1)$ é adjacente a w , então podemos aplicar os mesmos argumentos, agora à aresta wz . Assim, existe um vértice $y \in V(H)$ tal que $H - \{w, z, y\}$ é desconexo e tem como componentes H'_1, H'_2, \dots . Seja H'_1 uma componente que não contém u e, consequentemente, não contém v (uma vez que u e v são adjacentes). Porém, H'_1 contém pelo menos um vértice adjacente a z , mas não contém u, v ou w , pelo que H'_1 está completamente contida em H_1 . Porém, uma vez que H'_1 também não contém z , podemos concluir que é um subgrafo de H_1 com menos vértices do que $|V(H_1)|$, o que constitui uma contradição. \square

O facto de um grafo G ser contractível a um grafo H , não significa que G contenha um subgrafo que seja uma expansão (ou subdivisão) de H e, consequentemente, não significa que H seja, necessariamente, um menor topológico de G . Por exemplo, tal como já se referiu, o grafo de Petersen (representado na Figura 14.4) é contractível a K_5 mas não contém um subgrafo que seja uma expansão de K_5 , pelo que K_5 não é um menor topológico do grafo de Petersen. No entanto, o lema a seguir, garante-nos que a contractibilidade de um grafo G a K_5 ou $K_{3,3}$ implica que G tenha como menor topológico um grafo $H \in \{K_5, K_{3,3}\}$.

Lema 20.13. *Se o grafo H contém um subgrafo contractível a K_5 ou $K_{3,3}$, então H contém uma subdivisão de K_5 ou $K_{3,3}$.*

Demonstração. Vamos considerar os dois casos possíveis.

1. Suponha que H contém um subgrafo contractível a $K_{3,3}$. Então existe um subgrafo de H que contém seis subgrafos induzidos conexos H_1, H_2, H_3 e H'_1, H'_2, H'_3 e arestas entre cada H_i e cada H'_j , para todo o i e todo o j , mas não existem arestas entre quaisquer dois grafos de entre H_1, H_2, H_3 e entre quaisquer dois grafos de entre H'_1, H'_2, H'_3 . Escolhendo-se adequadamente as nove arestas, em cada subgrafo obtém-se três caminhos que terminam num único vértice, os quais, conjuntamente com as nove arestas correspondem a uma subdivisão de $K_{3,3}$.
2. Suponha que H contém um subgrafo contractível a K_5 e sejam H_1, \dots, H_5 os subgrafos induzidos que determinam os vértices de K_5 . Em cada H_i existem duas possibilidades: (a) ou as quatro arestas que ligam os restantes subgrafos a H_i são incidentes nos vértices extremos de quatro caminhos de H_i , com zero ou mais arestas que se intersectam num único vértice; (b) ou são incidentes nos vértices extremos de quatro caminhos, com zero ou mais arestas, dos quais dois

se intersectam num vértice u e outros dois num vértice v , existindo um caminho entre u e v . Se o caso (a) ocorre em todos os subgrafos H_j , com $j = 1, \dots, 5$, então obtém-se uma subdivisão de K_5 . Caso contrário, sendo H_1 o subgrafo que contém os vértices u e v do caso (b), podemos concluir que H_1 conjuntamente com os restantes subgrafos contêm um subgrafo contractível a $K_{3,3}$, o que corresponde ao caso 1. \square

Na sua versão original, o teorema de Kuratowski, publicado em 1930 [63], contempla unicamente menores topológicos. A versão que considera menores mais gerais (menores combinatórios) foi publicada mais tarde, por Wagner em 1937 [103]. O teorema a seguir, estabelecendo a equivalência entre as duas abordagens, é idêntico ao apresentado em [30], mas com uma demonstração influenciada pela segunda das provas que constam em [108].

Teorema 20.14 (Kuratowski, Wagner). *Sendo G um grafo, são equivalentes as seguintes afirmações:*

1. G é planar;
2. G não contém K_5 nem $K_{3,3}$, como menores combinatórios;
3. G não contém K_5 nem $K_{3,3}$, como menores topológicos.

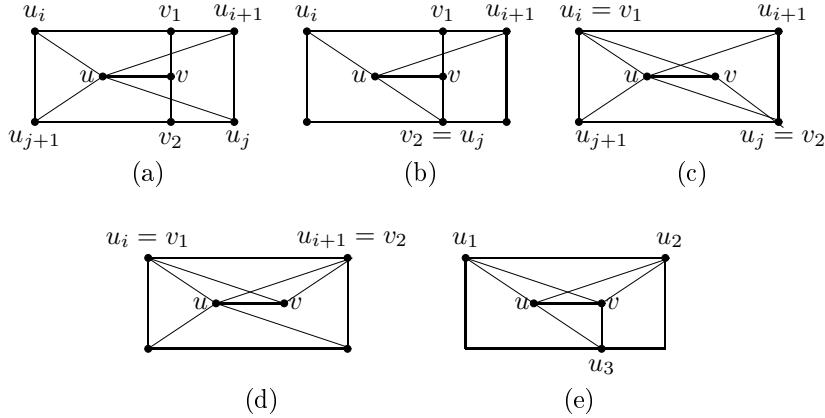


Figura 20.10: Os casos da demonstração do Teorema 20.14.

Demonstração.

- (1 \Rightarrow 2) Se G é um grafo planar, então qualquer dos seus menores simples, G' , é um grafo planar e, pelo Corolário 20.7, $\varepsilon(G') \leq 3\nu(G') - 6$. Logo, uma vez que K_5 não é plano ($10 = \varepsilon(K_5) > 3\nu(K_5) - 6 = 9$), conclui-se que K_5 não é um menor de G . Identicamente, no caso de G admitir como menor um grafo bipartido simples, G' , do Corolário 20.9 decorre a desigualdade $\varepsilon(G') \leq 2\nu(G') - 4$ e, uma vez que $K_{3,3}$ não a satisfaz ($9 = \varepsilon(K_{3,3}) > 2\nu(K_{3,3}) - 4 = 8$), conclui-se que não é um menor de G .
- (2 \Rightarrow 3) Dado que qualquer menor topológico de um grafo G é também um menor combinatório, se G não admite K_5 nem $K_{3,3}$ como menor combinatório, então também não admite K_5 nem $K_{3,3}$ como menor topológico.

(3 \Rightarrow 1) Vamos provar esta implicação por redução ao absurdo, supondo que G é um grafo não-planar que não contém K_5 nem $K_{3,3}$ como menores topológicos (i.e., G não contém qualquer subgrafo H que seja uma expansão de K_5 ou $K_{3,3}$). Logo, de acordo com o Lema 20.13, G não contém um subgrafo H contractível a K_5 ou $K_{3,3}$. Vamos supor que G é o grafo com menor número de arestas de entre os grafos nestas condições. Então, de acordo com o Lema 20.11, G é 3-conexo e uma vez que G é distinto de K_4 (dado ser não-planar), por aplicação do Lema 20.12, podemos escolher uma aresta $uv \in E(G)$, tal que G/uv é ainda 3-conexo. Adicionalmente, pela minimalidade de G sabemos que G/uv é planar. Seja F uma realização plana de G/uv e $w \in V(F)$ o vértice correspondente à aresta contraída uv . Então o conjunto das faces que partilham w na sua fronteira, formam uma região R do plano que tem um ciclo C na sua fronteira. Vamos tentar repor os vértices u e v , no interior da região R , ligando-os adequadamente aos vértices do ciclo C , começando pelo vértice u , considerando os seus vizinhos em C são os vértices $u_1, u_2, \dots, u_k, u_{k+1} = u_1$, dispostos, sequencialmente, por esta ordem. Vamos agora considerar os vários casos possíveis de acordo com o posicionamento dos vizinhos de v no ciclo C . Notes-se que v tem pelo menos dois vizinhos em C (dado que G é 3-conexo e u é vizinho de v).

- a) Se existem vizinhos de v , v_1 e v_2 , um estritamente entre u_i e u_{i+1} e outro entre u_j e u_{j+1} , com $i \neq j$, então existe um subgrafo contractível ao grafo $K_{3,3}$ induzido pelo subconjunto de vértices $\{u, v_1, v_2\} \cup \{v, u_i, u_{i+1}\}$ (ver Fig. 20.10-(a)).
- b) Se existe um vizinho de v , v_1 , nas condições do item anterior e um vizinho $v_2 = u_j$, com $j \notin \{i, i+1\}$, então (eliminando a aresta uv_2) as conclusões são idênticas às do item anterior (ver Fig. 20.10-(b)).
- c) Nos restantes casos, após eventual contracção de arestas, todos os vizinhos de v no ciclo C são também vizinhos de u .
 - (i) Se existem dois vizinhos de v em C não-adjacentes, por exemplo, $v_1 = u_i$ e $v_2 = u_j$, com $i \neq j \pm 1$, então obtém-se $K_{3,3}$ no subconjunto de vértices $\{u, v_1, v_2\} \cup \{v, u_{i+1}, u_{j+1}\}$, eliminando naturalmente as arestas uv_1 e uv_2 (ver Fig. 20.10-(c)).
 - (ii) Se os vizinhos de v em C são todos adjacentes entre si, então ou existem apenas dois, por exemplo, $v_1 = u_i$ e $v_2 = u_{i+1}$ e, nesse caso, é possível representar v e todas as arestas necessárias no interior do triângulo u, u_i, u_{i+1}, u (ver Fig. 20.10-(d)), o que é contraditório com o facto de G ser não-planar; ou existem pelo menos três deles e o ciclo é um triângulo $u_1 u_2 u_3$ (ver Fig. 20.10-(e)), pelo que os vértices u, v, u_1, u_2, u_3 formam K_5 . \square

20.2.3 Dualidade em grafos e digrafos planares

Vamos começar por introduzir a definição de dual (ou dual geométrico) de um grafo planar.

Definição 20.3 (Dual de um grafo planar). *Dado um grafo planar G que, sem perda de generalidade, se admite realizado no plano, designa-se por dual (ou dual geométrico⁸) de G e denota-se por G^* o grafo obtido de G por aplicação do seguinte procedimento:*

1. A cada face de G faz-se corresponder um vértice de G^* .
2. A cada aresta $e \in E(G)$ faz-se corresponder uma aresta $e^* \in E(G^*)$ que liga duas faces (vértices de $V(G^*)$) vizinhas, cruzando a aresta e .

A Figura 20.11, exemplifica a obtenção do dual geométrico de um grafo plano, apresentando o mapa da Polónia (como grafo plano) e o seu dual geométrico sobrepostos.

⁸Esta designação é utilizada para se distinguir este dual do dual combinatório a introduzir mais adiante.

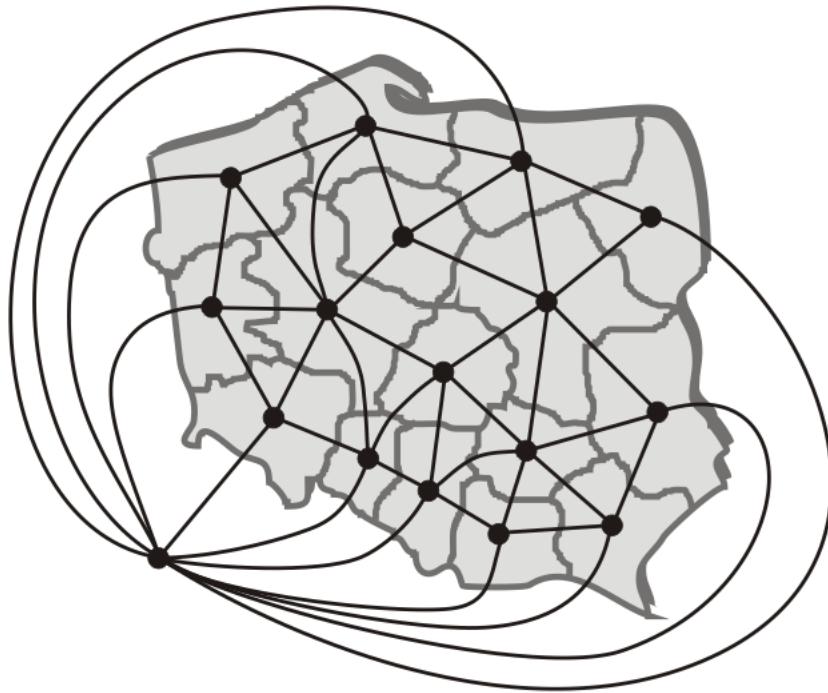


Figura 20.11: Exemplo de um par de grafos planos duais (sendo um deles o mapa da Polónia) que aparecem sobrepostos.

No caso de grafos orientados, \vec{G} , com exceção dos lacetes, cujo sentido é arbitrário, o sentido de cada um dos arcos, $a^* \in A(\vec{G}^*)$, é determinado dividindo o ciclo orientado \vec{C} que limita a face correspondente ao vértice incidente v^* em \vec{C}^+ e \vec{C}^- (consoante os arcos estejam no sentido positivo ou negativo). Se $a \in \vec{C}^+$, então o arco de $A(\vec{G}^*)$ que o intersecta tem cauda em v^* , caso contrário esse arco tem cabeça em v^* .

Teorema 20.15. *Sendo G um grafo plano e G^* o correspondente dual geométrico, podemos concluir o seguinte:*

1. G^* é conexo;
2. se G é conexo, então $(G^*)^* = G$;
3. se G é conexo, então G^* contém um vértice de corte se e só se G contém um vértice de corte.

Demonstração.

1. Uma vez que podemos passar de uma face f_i para qualquer outra face f_j de G ao longo das arestas de G^* , conclui-se que existe um caminho entre quaisquer dois vértices, v_i^* e v_j^* , de $V(G^*)$.
2. Por construção de G^* , sabe-se que $\nu(G^*) = |F_0(G)|$ e $\varepsilon(G^*) = \varepsilon(G)$. Uma vez que cada aresta da fronteira de cada elemento de $F_0(G^*)$ é atravessada por uma aresta de G , é claro que cada face de G^* contém, pelo menos, um vértice de G . Adicionalmente, tendo em conta que G é conexo, por aplicação da fórmula de Euler, pode concluir-se que $|F_0(G^*)| = |V(G)|$, pelo que cada elemento de $F_0(G^*)$ contém, exactamente, um vértice de G . Consequentemente, partindo-se de

G^* e aplicando o procedimento de construção do dual geométrico de G^* , obtém-se a construção inicial, i.e., $(G^*)^* = G$.

3. Seja v um vértice de corte em G , o qual proporciona a decomposição de G em subgrafos conexos $G = G_1 \cup G_2$, com $G_1 \cap G_2 = \{v\}$. Sendo $f \in F_0(G)$ a face ilimitada de G , para se passar das faces de G_1 para as faces de G_2 , é necessário atravessar a face f . Consequentemente, todos os caminhos entre um vértice de G^* contido numa face de G_1 e um vértice de G^* contido numa face de G_2 , passam pelo vértice de G^* relativo a f , o que implica que ele seja um vértice de corte de G^* . O recíproco, é igualmente verdadeiro, tendo em conta o item 2. \square

Lema 20.16. *Dado um grafo plano G e o seu dual geométrico G^* , verificam-se as seguintes propriedades:*

- (1) *Se C é um ciclo de G e $E_C = E(C)$ é o correspondente conjunto de arestas, então E_C^* é um corte de G^* , ou seja, existe $X^* \subset V(G^*)$ tal que $E_C^* = \partial(X^*)$.*
- (2) *Se $F \subseteq G$ é uma floresta e $E_F = E(F)$ é o correspondente conjunto de arestas, então $G^* - E_F^*$ é um grafo conexo.*

Demonstração. Com efeito, a propriedade (1) decorre directamente do teorema da curva fechada de Jordan e a propriedade (2) obtém-se por indução sobre o número de arestas da floresta (removendo uma aresta pendente da floresta). \square

Dado um grafo G , diz-se que G^{cb} é o *dual combinatório* de G , se existe uma função $\varphi : E(G) \rightarrow E(G^{cb})$ tal que C é um ciclo de G se e só se $\varphi(E(C))$ é um corte (ou co-circuito) de G^{cb} . Com base nesta definição, é fácil provar que, sendo G^{cb} o dual combinatório de G e $e \in E(G)$, se e^{cb} é a aresta que em G^{cb} corresponde a e , então $G^{cb} - e^{cb}$ é o dual combinatório de G/e e G^{cb}/e^{cb} é o dual combinatório de $G - e$.

Teorema 20.17. *Seja G um grafo plano, 2-conexo e H o dual geométrico de G , ou seja, $H = G^*$. Então H é o dual combinatório de G , ou seja, $H = G^{cb}$.*

Demonstração. Uma vez que H é o dual geométrico de G , definindo-se a função $\varphi : E(G) \rightarrow E(H)$, tal que $\varphi(e) = e^*$, tendo em conta o Lema 20.16, conclui-se imediatamente que C é um ciclo de G se e só se $\varphi(E(C))$ é um corte de H . Logo, $H = G^{cb}$. \square

Como consequência dos Teoremas 20.15 e 20.17, podemos ainda concluir que sendo G um grafo plano, 2-conexo, não só $G^* = G^{cb}$, como G é o dual geométrico e, consequentemente, combinatório de G^* .

Adicionalmente, se H admite um dual combinatório H^{cb} , então todo o menor de H admite um dual combinatório, podendo demonstrar-se que K_5 e $K_{3,3}$ não admitemiais combinatórios. Consequentemente, o teorema de Kuratowski implica a parte não trivial do critério de planaridade que o teorema de Whitney [105, 106] (a seguir) estabelece.

Teorema 20.18 (Whitney). *Seja G um grafo 2-conexo. Então G é planar se e só se admite um dual combinatório. Adicionalmente, sendo G^{cb} o dual combinatório de G , então G tem uma realização plana com dual geométrico G^* isomorfo a G^{cb} . Em particular, G^{cb} é planar e G é o dual combinatório de G^{cb} .*

A demonstração deste teorema pode ser consultada em [70] (pag. 45).

Voltando ao problema das sete pontes de Königsberg que, como se sabe, não tem solução, podemos colocar a seguinte questão:

É possível a um nadador passar por baixo de todas as pontes sem repetir nenhuma e voltar ao sítio de onde partiu?

Considerando que o nadador pode sair e entrar na água, desde que o faça nos pontos extremos da porção de rio representada na figura, ou seja, antes ou depois de todas as pontes (por exemplo, pode sair do rio no ponto em que se encontra na figura, andar a pé por uma das margens e voltar a entrar no extremo oposto, depois de todas as pontes), esta versão do problema das sete pontes de Königsberg resolve-se construindo o dual geométrico G^* do grafo da Figura 18.1 e investigando se G^* é ou não euleriano. Mesmo não permitindo que o nadador saia da água, é possível verificar se o problema tem solução, analisando um grafo obtido depois de uma ligeira modificação de G^* (Exercício 20.21). Outra questão relacionada com este problema, consiste em saber se é possível ao nadador partir de um ponto deste rio e chegar a outro ponto, passando por baixo de cada uma das pontes uma única vez (Exercício 20.20).

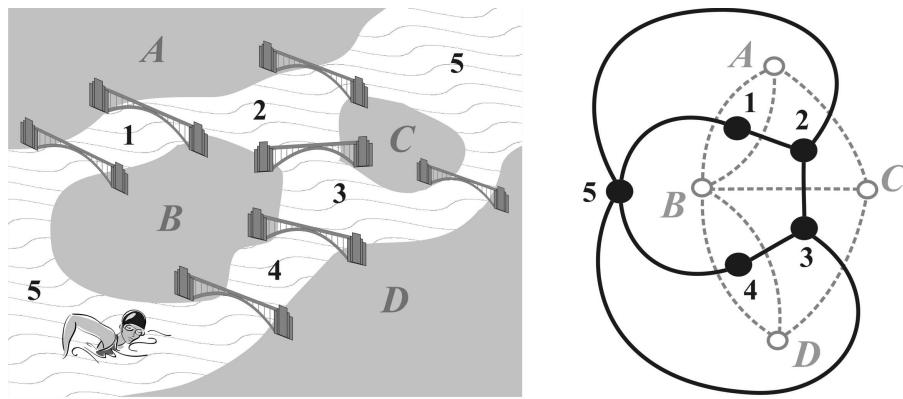


Figura 20.12: Dual do grafo de Euler para o problema das sete pontes de Königsberg.

20.2.4 Grafos platônicos

Um grafo simples, diz-se *platônico* se é constituído por um único vértice ou, tendo mais que uma aresta, é conexo, plano, regular e todas as faces têm o mesmo grau. São grafos platônicos, o grafo constituído por um vértice isolado (K_1), os grafos cílicos (que correspondem aos polígonos regulares) e os grafos formados pelas arestas dos cinco poliedros convexos regulares: o tetraedro, o hexaedro (ou cubo), o octaedro, o dodecaedro e o icosaedro. Note-se que um *polígono regular* é uma figura poligonal fechada limitada por um número finito de segmentos (arestas), com igual comprimento e com os mesmos ângulos. Existe um número infinito de polígonos regulares, aos quais correspondem grafos cílicos.

O teorema a seguir estabelece a existência de apenas cinco poliedros convexos regulares distintos com mais do que duas faces (aos quais correspondem cinco grafos platônicos).

Teorema 20.19. *Existem somente cinco grafos platônicos distintos de K_1 e dos grafos cílicos.*

Demonstração. Seja G um grafo simples, conexo, plano e d -regular, onde cada face tem grau f . Uma vez que $G \neq K_1$, podemos concluir que $d > 0$ e, dado que $\varepsilon(G) > 1$, $d > 1$. Adicionalmente, uma vez que G não é um grafo cíclico, conclui-se que $d > 2$, ou seja, $d \geq 3$ e, é claro, $f \geq 3$. Logo,

$$f|F_0(G)| = 2\varepsilon(G) = d\nu(G) \Rightarrow \varepsilon(G) = \frac{d\nu(G)}{2},$$

e $|F_0(G)| = \frac{2\varepsilon(G)}{f}$. Como consequência, uma vez que G é plano, por aplicação da fórmula de Euler,

obtém-se

$$\begin{aligned}
 \frac{2\varepsilon(G)}{f} = \frac{d\nu(G)}{2} - \nu(G) + 2 &\Leftrightarrow \frac{d\nu(G)}{f} = \frac{d\nu(G)}{2} - \nu(G) + 2 \\
 &\Leftrightarrow \nu(G)\left(\frac{d}{f} + 1 - \frac{d}{2}\right) = 2 \\
 &\Leftrightarrow \nu(G)(2d + 2f - fd) = 4f
 \end{aligned} \tag{20.1}$$

Da igualdade (20.1) decorre a inequação

$$2d + 2f - fd > 0 \Leftrightarrow -2d - 2f + fd + 4 < 4 \Leftrightarrow (f - 2)(d - 2) < 4,$$

que, para $f \geq 3$ e $d \geq 3$, apresenta como soluções apenas os pares de valores (d, f) : $(3, 3)$, $(3, 4)$, $(3, 5)$, $(4, 3)$ e $(5, 3)$, aos quais correspondem, respectivamente, o tetraedro, hexaedro, dodecaedro, octaedro e icosaedro. \square

Utilizando a igualdade (20.1) que é equivalente à igualdade $\nu(G) = \frac{4f}{2f+2d-fd}$, podemos obter a tabela a seguir, onde se apresentam os graus dos vértices (d), os graus das faces (f), o número de vértices, o número de arestas e o número de faces, para cada um dos poliedros convexos regulares associados aos grafos platónicos distintos de K_1 e dos grafos cílicos, os quais designamos por grafos platónicos não triviais.

d	f	$\nu(G)$	$\varepsilon(G)$	$ F_0(G) $	Designação
3	3	4	6	4	Tetraedro
3	4	8	12	6	Hexaedro
3	5	20	30	12	Dodecaedro
4	3	6	12	8	Octaedro
5	3	12	30	20	Icosaedro

Na Figura 20.13 representam-se os cinco grafos platónicos não triviais. Na primeira linha o tetraedro, hexaedro e o octaedro e na segunda linha o dodecaedro e o icosaedro (que é o grafo dual do dodecaedro).

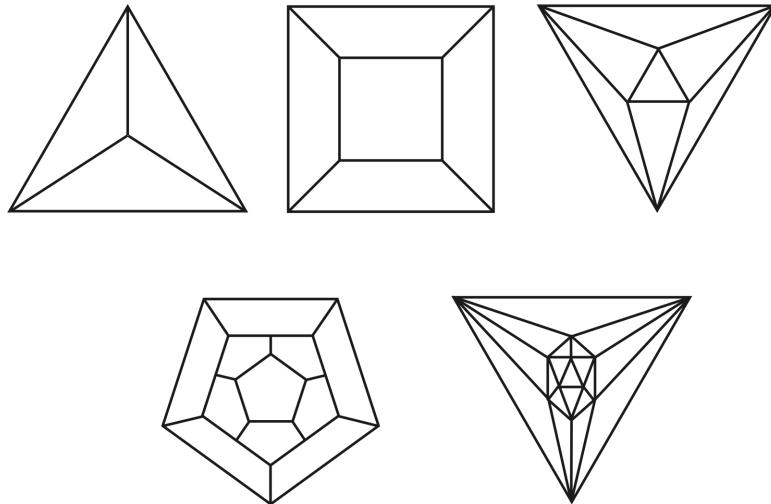


Figura 20.13: Grafos platónicos.

20.3. Grafos com genus positivo

Designa-se por *genus de um grafo* G e denota-se por g_G (não confundir com a cintura de G que se denota por $\varepsilon(G)$), o menor genus das superfícies S_0, S_1, S_2, \dots , em que G é realizável. Como consequência, dado um grafo planar G , $g_G = 0$.

Teorema 20.20. *Todo o grafo tem genus.*

Demonstração. Seja G um grafo. Se G é planar, então $g_G = 0$. Suponha que G não é planar e, mesmo assim, desenhe-se esse grafo no plano e transfira-se, por projeção estereográfica, esse desenho para a esfera (superfície S_0). Seguidamente, adicionem-se tantas *ansas* tubulares quantas as necessárias para que, fazendo passar as arestas que intersectam outras arestas através dessas *ansas* tubulares (uma em cada), não existam arestas cruzadas (i.e. não existam arestas que se intersectem em pontos distintos dos vértices). Sendo p o número de *ansas* tubulares adicionadas, é claro que $p \leq \varepsilon(G)$. Deformando, continuamente, a superfície obtida é possível produzir um *torus* com p buracos, S_p , onde G se realiza. Consequentemente, tendo em conta que S_p pertence à sequência $S_0, S_1, \dots, S_p, S_{p+1}, \dots, S_{\varepsilon(G)}$, conclui-se que G tem genus $g_G \leq p$. \square

A Figura 20.14 exemplifica a demonstração do teorema anterior.

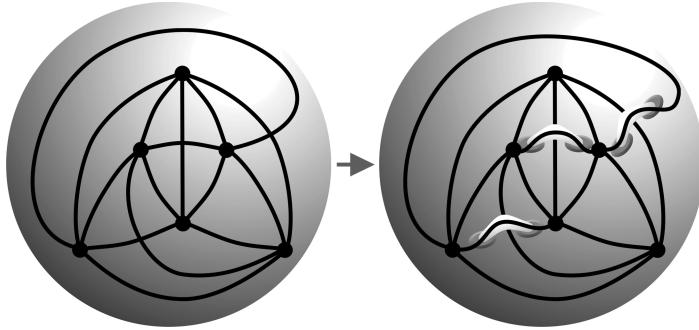


Figura 20.14: Figura que ilustra a introdução de ansas que suportam arestas de um grafo não-planar representado na esfera.

Deve observar-se que uma esfera com p *ansas* tubulares é topologicamente equivalente (i.e., homeomorfa) a um *torus* com p buracos e é claro que se um grafo, G , tem genus g_G , então G pode realizar-se em qualquer superfície S_g , com $g \geq g_G$. A questão que se coloca agora é a de saber se todo o grafo conexo, finito, com pelo menos uma aresta, admite uma realização celular. Para responder a essa questão, convém analisar, com mais detalhe, as realizações de grafos em superfícies.

Dado um grafo conexo G , com pelo menos uma aresta, para cada vértice $v \in V(G)$, seja π_v uma permutação cíclica das arestas incidentes em v . Considere-se uma aresta $e_1 = v_1v_2$ e um passeio fechado $P = v_1e_1v_2e_2v_3 \dots v_ke_kv_1$, que é determinado por $\pi_{v_{i+1}}(e_i) = e_{i+1}$, para $i = 1, \dots, k$, com $e_{k+1} = e_1$ (onde k é mínimo). Uma vez que G é finito, P não pode ser infinito sem repetição de uma aresta. Sendo $\pi = \{\pi_v : v \in V(G)\}$, designamos P por π -passeio. Para cada π -passeio fechado consideramos um polígono no plano, com k lados (onde k é o comprimento do π -passeio) disjunto dos restantes polígonos, e designamo-lo por π -polígono. Considerando agora todos os π -polígonos, cada aresta de G aparece exactamente em dois π -polígonos (cujos correspondentes lados vamos designar por gémeo) e este facto determina orientações dos lados dos π -polígonos. Identificando, em cada polígono, cada lado com o seu lado gémeo, obtém-se uma realização celular de um grafo isomorfo a G . Com esta construção, verifica-se que a superfície obtida é orientável e que todo o grafo conexo, com pelo menos uma aresta, admite uma realização celular em alguma superfície orientável.

Teorema 20.21. Se G é um grafo conexo com genus g , então qualquer realização de G em S_g é celular.

O teorema a seguir, por sua vez, reduz o problema da determinação do genus de um grafo arbitrário ao problema da determinação do genus de grafos 2-conexos.

Teorema 20.22 ([8]). O genus de um grafo conexo é a soma dos genera⁹ dos seus blocos.

Ambos os teoremas acabados de enunciar (Teorema 20.21 e Teorema 20.22), têm demonstrações que podem ser consultadas em [70] (o primeiro na pag. 95 e o segundo na pag. 113).

20.3.1 Fórmula de Euler generalizada

No que se segue, sem perda de generalidade, assumimos que se G é um grafo conexo com genus g , então G é realizável em S_g de tal forma que através de cada buraco de S_g passa pelo menos um anel, formado por vértices e arestas de G , que não é contractível em S_g . Com efeito, se G tem genus g , então G não admite qualquer realização em nenhuma das superfícies S_0, S_1, \dots, S_{g-1} . Consequentemente, cada buraco de S_g é essencial para a realização de G . Logo, cada buraco deve ser atravessado por, pelo menos, uma aresta de G , de tal forma que ligada a outras arestas forme um anel nas condições referidas. Em alternativa, poder-se-ão obter anéis não contractíveis que contornem buracos. Esta situação, porém, é topologicamente equivalente à anterior. Note-se que cortar uma superfície, S_g , ao longo de g anéis não contractíveis cada um dos quais atravessa ou contorna um buraco distinto produz, em ambos os casos, uma superfície topologicamente equivalente a uma esfera à qual faltam $2g$ círculos.

Teorema 20.23 (l'Huilier¹⁰). Se G é um grafo conexo com genus g , então

$$\nu(G) + |F_g(G)| - \varepsilon(G) = 2(1 - g). \quad (20.2)$$

Demonstração. Seja G um grafo conexo de genus g . Então G é realizável em S_g de tal forma que para cada buraco de S_g existe um anel, não contractível, formado pela concatenação de arestas. Corte-se o torus ao longo de cada um destes g anéis, dupliquem-se os anéis e, consequentemente, as arestas e vértices que definem as fronteiras das regiões circulares que se formaram e coleem-se círculos, de modo a tapar todos estas regiões. Por deformação contínua da superfície deste modo obtida, pode construir-se uma superfície esférica, S_0 , que lhe é topologicamente equivalente, onde o grafo conexo produzido, H , se realiza. Consequentemente, aplicando a fórmula de Euler a H , vem $\nu(H) + |F_0(H)| - \varepsilon(H) = 2$. Tendo em conta que os novos vértices, que agora aparecem em H , $V(H) \setminus V(G)$, são os que se produziram com a duplicação de ciclos provocada pelos cortes efectuados em cada um dos g anéis e tendo em conta que nos ciclos o número de arestas é igual ao número de vértices, obtém-se $\nu(H) - \nu(G) = \varepsilon(H) - \varepsilon(G)$. Por outro lado, dado que as novas faces em H são as limitadas pelos $2g$ anéis, conclui-se que $|F_0(H)| = |F_g(G)| + 2g$. Logo, fazendo $x = \nu(H) - \nu(G) = \varepsilon(H) - \varepsilon(G)$, vem

$$\begin{aligned} \nu(G) + |F_g(G)| - \varepsilon(G) &= (\nu(H) - x) + (|F_0(H)| - 2g) - (\varepsilon(H) - x) \\ &= \nu(H) + |F_0(H)| - \varepsilon(H) - 2g \\ &= 2 - 2g. \end{aligned}$$

□

A Figura 20.15 ilustra a demonstração do Teorema 20.23.

Sendo G um grafo com genus g , ou seja, cuja superfície orientável de menor genus na qual se realiza é S_g , a quantidade $2(1 - g)$ que aparece no segundo membro da Fórmula de Euler generalizada (20.2),

⁹Plural de genus.

¹⁰Embora muitas publicações designem este resultado por fórmula de Heawood ou por segunda fórmula de Euler, ele foi publicado pela primeira vez por l'Huilier em 1812–1813.

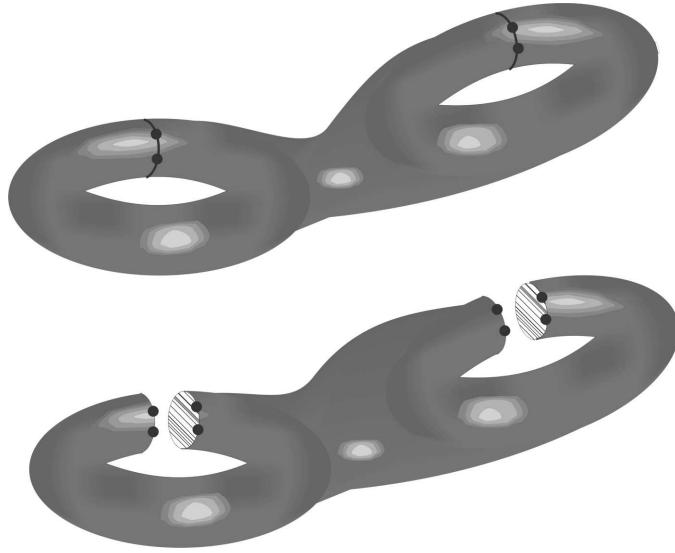


Figura 20.15: Transformação do duplo torus numa superfície homeomorfa à superfície esférica.

designa-se por *característica de Euler* da superfície S_g . A vantagem da utilização deste parâmetro na classificação de superfícies, em relação ao genus, é que pode ser definido também para superfícies não orientáveis.

Supondo que G é um grafo simples conexo tal que $\nu(G) \geq 3$, então

$$3|F_{g_G}(G)| \leq 2\varepsilon(G)$$

e, por aplicação do Teorema 20.23, $g_G \geq \frac{1}{6}\varepsilon(G) - \frac{1}{2}(\nu(G) - 2)$. Consequentemente, tendo em conta que g_G é inteiro, obtém-se

$$g_G \geq \left\lceil \frac{1}{6}\varepsilon(G) - \frac{1}{2}(\nu(G) - 2) \right\rceil. \quad (20.3)$$

Teorema 20.24 (Heawood). *Se $n \geq 3$, então $g_{K_n} \geq \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil$.*

Demonstração. Uma vez que $n \geq 3$ e K_n é conexo, tendo em conta a desigualdade (20.3),

$$\begin{aligned} g_{K_n} &\geq \left\lceil \frac{1}{6}|E(K_n)| - \frac{1}{2}(|V(K_n)| - 2) \right\rceil \\ &= \left\lceil \frac{n(n-1)}{12} - \frac{n-2}{2} \right\rceil = \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil. \end{aligned} \quad \square$$

A desigualdade recíproca,

$$g_{K_n} \leq \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil \quad (20.4)$$

e, consequentemente, a igualdade, embora tenha sido conjecturada por Heawood em 1890, apenas foi provada em 1968 [79]. A respectiva demonstração, porém, é bastante mais elaborada.

Como consequência da desigualdade (20.4), tendo em conta a desigualdade (20.3) e que, sendo H um supergrafo do grafo conexo G , $g_H \geq g_G$ e ainda que para $n = \nu(G)$, K_n é um supergrafo de G , se

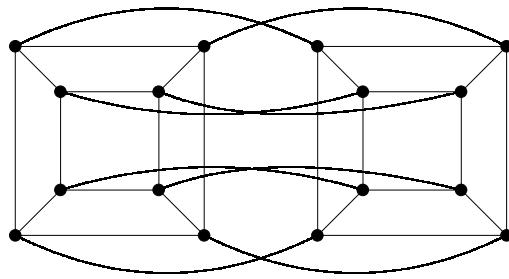


Figura 20.16: Grafo 1-platónico com vértices e faces de grau 4.

$n \geq 4$, então

$$\left\lceil \frac{1}{6}\varepsilon(G) - \frac{1}{2}(n-2) \right\rceil \leq g_G \leq \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil.$$

Embora, nem sempre estes minorante e majorante sejam boas aproximações para g_G , existem grafos para os quais eles coincidem. Por exemplo, se G é um grafo simples, conexo, de ordem 52 e dimensão 1.321, 1.322, 1.323, 1.324, 1.325 ou 1.326, então

$$196 = \left\lceil \frac{1}{6}\varepsilon(G) - \frac{1}{2}(n-2) \right\rceil \leq g_G \leq \frac{(n-3)(n-4)}{12} = 196.$$

20.3.2 Grafos g -platónicos

Um grafo simples G diz-se g -platónico se tem genus g , é conexo, regular e na sua realização em S_g , toda a aresta está na fronteira de duas faces e todas as faces têm o mesmo grau. Nestas condições, os grafos platónicos são grafos 0-platónicos. Denotando por d o grau dos vértices e por f o grau das faces de um grafo G , da definição de grafo g -platónico decorre que se G é g -platónico, então $\varepsilon(G) = \frac{d\nu(G)}{2}$ e $|F_g(G)| = \frac{d\nu(G)}{f}$. Por outro lado, se $g > 0$, então $d \geq 3$ e $f \geq 3$.

Teorema 20.25. *Sendo d o grau dos vértices e f o grau das faces de um grafo 1-platónico, verifica-se que o par (d, f) é igual a $(3, 6)$ ou $(4, 4)$ ou $(6, 3)$ ¹¹.*

Demonstração. Seja G um grafo 1-platónico, $d \geq 3$, $f \geq 3$, $\varepsilon(G) = \frac{d\nu(G)}{2}$, $|F_1(G)| = \frac{d\nu(G)}{f}$ e $|\nu(G)| + |F_1(G)| - \varepsilon(G) = 2(1-g)$. Então,

$$\nu(G) + \frac{d\nu(G)}{f} - \frac{d\nu(G)}{2} = 2(1-g) = 0 \Leftrightarrow \nu(G)(2f + 2d - df) = 0.$$

Uma vez que a ordem de G é positiva, conclui-se a igualdade

$$2f + 2d - df = 0 \Leftrightarrow df - 2d - 2f + 4 = 4 \Leftrightarrow (f-2)(d-2) = 4$$

e, consequentemente, que apenas os pares (d, f) : $(3, 6)$, $(4, 4)$ e $(6, 3)$ verificam esta igualdade, com $d \geq 3$ e $f \geq 3$. \square

Na Figura 20.16, representa-se um grafo 1-platónico cujo grau dos vértices e das faces é igual a 4.

Teorema 20.26. *Se existe um grafo g -platónico, G , tal que $g > 1$, então $\nu(G) = \frac{4f(g-1)}{d(f-2)-2f}$, onde d denota o grau dos vértices e f o grau das faces.*

¹¹Embora só existam grafos 1-platónicos com os pares (d, f) indicados, o seu número não é finito.

Demonstração. Se G é um grafo g -platónico, com $g > 1$, então

$$\varepsilon(G) = \frac{d\nu(G)}{2}, \quad |F_g(G)| = \frac{d\nu(G)}{f} \quad \text{e} \quad \nu(G) + |F_g(G)| - \varepsilon(G) = 2((1-g)).$$

Logo,

$$\begin{aligned} \nu(G) + \frac{d\nu(G)}{f} - \frac{d\nu(G)}{2} &= 2(1-g) \Leftrightarrow \nu(G)(2f + 2d - df) = 4f(1-g) \\ &\Leftrightarrow \nu(G) = \frac{4f(g-1)}{d(f-2)-2f}. \end{aligned}$$

□

Como corolário imediato deste teorema, conclui-se que, para cada $g > 1$, existe um número finito de grafos g -platónicos. Com efeito, sendo $g > 1$, se não existem grafos g -platónicos, então o resultado é verdadeiro para g . Supondo que existe um grafo g -platónico G , cujo grau dos vértices é d e cujo grau das faces é f , uma vez que $g > 1$, $d \geq 3$ e $f \geq 3$,

$$\nu(G) > 0 \Rightarrow \frac{4f(g-1)}{d(f-2)-2f} > 0 \Leftrightarrow df - 2d - 2f > 0 \Leftrightarrow df - 2d - 2f + 4 > 4,$$

ou seja, conclui-se a desigualdade $(d-2)(f-2) > 4$. Como consequência, o estudo reduz-se aos seguintes casos:

1. Se $f = 3$, então $(d-2)(3-2) > 4 \Rightarrow d \geq 7 \Rightarrow \nu(G) = \frac{12(g-1)}{d-6} \leq 12(g-1)$.
2. Se $f = 4$, então $(d-2)(4-2) > 4 \Rightarrow d \geq 5 \Rightarrow \nu(G) = \frac{16(g-1)}{2d-8} \leq 8(g-1)$.
3. Se $f = 5$, então $(d-2)(5-2) > 4 \Rightarrow d \geq 4 \Rightarrow \nu(G) = \frac{20(g-1)}{3d-10} \leq 10(g-1)$.
4. Se $f = 6$, então $(d-2)(6-2) > 4 \Rightarrow d \geq 4 \Rightarrow \nu(G) = \frac{24(g-1)}{4d-12} \leq 6(g-1)$.
5. Se $f \geq 7$, então $(d-2)(f-2) > 4 \Rightarrow d \geq 3 \Rightarrow$

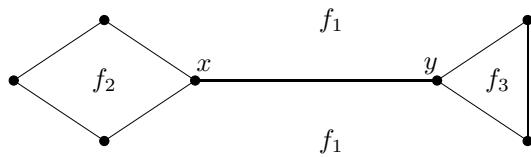
$$\nu(G) = \frac{4f(g-1)}{d(f-2)-2f} \leq \frac{4f(g-1)}{3(f-2)-2f} \leq \frac{4f(g-1)}{f-6} \leq 28(g-1).$$

Logo, todos os grafos g -platónicos (com $g > 1$) têm ordem não superior a $28(g-1)$, pelo que o seu número é finito.

20.4. Mapas e colorações

Um dos mais velhos problemas relacionados com a Teoria dos Grafos, diz respeito à *coloração de mapas*. Com este problema, pretende-se saber qual o menor número de cores necessárias para pintar um mapa de modo que não existam países com fronteira comum pintados com a mesma cor. Uma forma de modular este problema (ignorando situações particulares em que os países se distribuem por diferentes componentes conexas e ainda a possibilidade de existência de fronteiras pontuais) consiste em considerar o mapa como uma realização plana de um grafo planar G , ou seja, considerar o mapa planar $M(G)$ e pintar as respectivas faces, utilizando cores distintas para faces com uma aresta comum, ou ainda, de um modo equivalente, determinar uma coloração dos vértices do respectivo dual (ver Figura 20.11). Assim, o conceito de dualidade desempenha um papel preponderante na coloração de mapas, uma vez que torna equivalente a coloração de faces ou vértices de grafos planos.

Mais formalmente, uma k -coloração das faces de um mapa plano G é uma atribuição de cores: $1, \dots, k$, às faces de G , de modo que faces incidentes na mesma aresta tenham cores distintas. Desta forma, grafos com arestas de corte, como o indicado na Figura 20.17, não admitem k -colorações das sua faces, uma vez que a face ilimitada incide duplamente em cada aresta de corte. Por exemplo, na Figura 20.17, a face f_1 incide duas vezes na aresta de corte xy .

Figura 20.17: Mapa planar com uma aresta de corte xy .

20.4.1 Teorema das quatro cores

Desde muito cedo se conjecturou que 4 cores bastariam para resolver o problema da coloração das faces (ou vértices) de grafos planos. O cartógrafo inglês, Francis Guthrie, já em 1852 reclamava a suficiência de quatro cores para distinguir os países num mapa plano e foi, precisamente, nesse ano (1852) que Augustus De Morgan, numa carta que enviou a William Rowan Hamilton, afirmou ter tomado conhecimento deste problema que designou por *problema das quatro cores*, através de um seu aluno, Frederick Guthrie (irmão de Francis Guthrie). Nessa carta, De Morgan mostrava a necessidade de quatro cores, para o que basta exibir um mapa adequado (como é o caso do representado na Figura 20.18).

Mais tarde, numa publicação de 1879 [25], Cayley referiu-se ao problema das quatro cores como um problema em aberto e apresentou várias das dificuldade relacionadas com a sua resolução. Nesse mesmo ano, Kempe [59] propôs uma pretensa solução que só em 1890 foi refutada por Heawood, no seu primeiro trabalho escrito [56], onde provou a suficiência de cinco cores para a coloração de vértices de grafos planares. O Teorema 20.27 estabelece o resultado obtido por Heawood, com base no método utilizado, 11 anos antes, por Kempe.

Teorema 20.27 (Heawood). *Todo o grafo planar, não, sem lacetes, admite uma coloração de vértices com cinco cores.*

Demonstração. A prova vai ser feita por indução sobre o número de vértices de grafos simples planos (note-se, no entanto, que a existência de arestas paralelas não influencia o número de cores em causa).

Seja G um grafo simples, plano, não nulo e suponha que o resultado é verdadeiro para grafos, nestas condições, com menor número de vértices do que $\nu(G)$.

Tendo em conta o Teorema 20.10, existe um vértice $v \in V(G)$ tal que $d_G(v) \leq 5$ e, por hipótese de indução, $G[V(G) \setminus \{v\}]$ admite uma coloração de vértices com 5 cores. Se nem todas as 5 cores são utilizadas nos vértices adjacentes a v , então uma das que ficam livres pode ser utilizada em v e, consequentemente, o resultado verifica-se. Suponha que todos os vértices adjacentes a v , v_1, v_2, v_3, v_4, v_5 têm cores distintas (as quais vamos identificar por 1, 2, 3, 4, 5 e supor distribuídas segundo uma ordem contrária aos ponteiros do relógio). Seja $V_{1;3}$ o conjunto dos vértices que podem ser alcançados a partir de v_1 , por um trajecto que utiliza, unicamente, vértices com cores 1 e 3 (note-se que $v_1 \in V_{1;3}$). Se $V_{1;3}$ é um conjunto singular, ou seja, é constituído unicamente por v_1 , tal significa que v_1 não tem vértices adjacentes com cor 3, donde podemos atribuir esta cor 3 a v_1 e, subsequentemente, a cor 1 a v . Supondo que $V_{1;3}$ tem mais do que um vértice, podemos trocar estas duas cores, entre si, em $V_{1;3}$,



Figura 20.18: Exemplo de um mapa para o qual são necessárias quatro cores para colorir as faces.

sem que vértices adjacentes deixem de ter cores distintas. Se $v_3 \notin V_{1;3}$, então, após troca de cores, nenhum dos vértices adjacentes a v tem a cor 1, pelo que a podemos utilizar para v .

Suponha que $v_3 \in V_{1;3}$ e seja $v_1, u_1, \dots, u_k, v_3$ um caminho (entre v_1 e v_3) com cores, alternadamente, 1 e 3. Acrescentando a v este caminho, obtém-se um ciclo, $C_{1;3}$, homeomorfo a uma curva fechada de Jordan C que, naturalmente, divide o plano em duas componentes conexas por caminhos e, de acordo com esta construção, é claro que v_2 e v_4 pertencem a componentes distintas. Seja $V_{2;4}$ o conjunto dos vértices alcançados, a partir de v_2 , por trajectos que utilizam, unicamente, as cores 2 e 4 (note-se que $v_2 \in V_{2;4}$). Nestas condições, nenhum destes trajectos cruza o ciclo $C_{1;3}$, pelo que $V_{2;4}$ está contido na componente conexa definida pela curva fechada de Jordan C que contém v_2 . Consequentemente, $v_4 \notin V_{2;4}$ e, trocando as cores 2 e 4, entre si, a cor 2 fica disponível para o vértice v . \square

Existe uma relação interessante entre a coloração de faces de mapas planos e ciclos de Hamilton, conforme o teorema a seguir, atribuído a Tait, indica.

Teorema 20.28 (Tait). *Se um mapa plano tem um ciclo de Hamilton, então admite uma 4-coloração das suas faces.*

Demonstração. Seja G um mapa plano hamiltoniano e C um ciclo de Hamilton. Então este ciclo é homeomorfo a uma curva fechada de Jordan que também vamos denotar por C . É claro que as faces situadas no domínio interior (exterior) de C estão separadas por arestas que ligam vértices de C e, consequentemente, podemos colori-las alternadamente com as cores 1 e 2 (3 e 4). \square

Este teorema está na base de uma outra tentativa falhada para a resolução do problema das quatro cores (a adicionar à de Kempe), apresentada em 1880 por Tait que, por essa altura, conjecturava que todos os grafos cúbicos, 2-conexos (ou seja, sem vértices de corte), planares, admitiam um ciclo de Hamilton e, consequentemente, por aplicação do Teorema 20.28, admitiriam uma 4-coloração das suas faces. Note-se que, tendo em vista colorir as faces de um mapa plano, podemos transformá-lo num mapa cúbico plano, introduzindo novas faces, conforme a Figura 20.19 ilustra, sendo fácil concluir que qualquer coloração das faces do grafo modificado define uma coloração das faces do grafo original (bastando manter as cores nas faces originais). Assim, caso todos os grafos cúbicos, 2-conexos, planares admitissem um ciclo de Hamilton, tal como Tait conjecturou, com recurso a esta operação de transformação de mapas planos em mapas cúbicos planos, o problema das quatro cores ficava resolvido. Porém, a conjectura de Tait foi refutada em 1946, por Tutte que, por essa altura, exibiu o grafo cúbico 2-conexo, plano, não-hamiltoniano representado na Figura 20.20 (trata-se de um grafo com 69 arestas, 46 vértices e 25 faces).

Relativamente aos grafos cúbicos, 2-conexos, não-hamiltonianos, deve observar-se ainda que, já em 1891, Petersen tinha encontrado um grafo cúbico, 2-conexo, não-hamiltoniano (o famoso grafo de Petersen, representado na Figura 14.4). No entanto, o grafo de Petersen não serve de contra-exemplo para a conjectura de Tait, uma vez que é não-planar.

Ambas as tentativas (não conseguidas) de resolução do problema das quatro cores tiveram contributos positivos. Kempe introduziu o conceito que actualmente se designa por cadeia de Kempe (o qual corresponde a um subgrafo conexo maximal, com vértices coloridos, unicamente, com duas cores) que foi utilizada por Heawood na demonstração do Teorema 20.27 e que é utilizada na redutibilidade de configurações a que se recorre na prova do teorema das quatro cores, obtida por Appel e Haken [4, 5].



Figura 20.19: Transformação de um mapa plano num mapa plano cúbico.

Por outro lado, Tait mostrou (com o teorema que se segue) que o problema da coloração dos vértices de triangulações planas com quatro cores é equivalente à coloração das arestas do correspondente grafo dual com apenas com três cores. Note-se que colorir as arestas do grafo dual de uma triangulação plana com três cores é equivalente a etiquetar as arestas que constituem as fronteiras triangulares de cada face com as cores das arestas duais que as cruzam de tal forma que cada triângulo contenha as três cores.

Convém observar que o dual de um grafo simples, conexo, cúbico e plano é uma triangulação do plano, ou seja, um grafo planar-maximal, pelo que, colorir as faces de um grafo, conexo, cúbico e plano é equivalente a colorir os vértices de uma triangulação do plano.

Teorema 20.29 (Tait). *Sendo G uma triangulação do plano, $\chi(G) \leq 4$ se e só se as arestas de G podem ser etiquetadas com três etiquetas distintas de tal modo que na fronteira de cada face existam as três etiquetas.*

Demonstração. Suponha que G admite a coloração de vértices $f : V(G) \rightarrow \{(0,0), (1,0), (0,1), (1,1)\}$ e que, a partir dela, se define a etiquetação de arestas determinada pela aplicação $\psi : E(G) \rightarrow \{(1,0), (0,1), (1,1)\}$ tal que se $uv \in E(G)$, então $f(u) = (u_x, u_y)$, $f(v) = (v_x, v_y)$ e

$$\psi(uv) = f(u) + f(v) = (u_x + v_x \pmod{2}, u_y + v_y \pmod{2}).$$

Nestas condições, $\psi(uv)$ associa às arestas de cada triângulo as etiquetas $(1,0)$, $(0,1)$ e $(1,1)$.

Reciprocamente, seja $\psi : E(G) \rightarrow \{(1,0), (0,1), (1,1)\}$ uma função de etiquetação das arestas de G de tal forma que cada face contenha as três etiquetas. Seja v_1 um vértice arbitrário e seja $f : V(G) \rightarrow \{(0,0), (1,0), (0,1), (1,1)\}$ tal que

$$f(x) = \sum_{e \in P_{v_1 x}} \psi(e) \pmod{2},$$

onde $P_{v_1 x}$ é um caminho (ou passeio) arbitrário entre v_1 e x . Assim, resta provar que a função f está bem definida, ou seja, o seu valor é independente do caminho (ou passeio) escolhido entre v_1 e x (o que é equivalente a afirmar que o seu valor é nulo para $x = v$, considerando qualquer circuito) e ainda que $f(x) \neq f(y)$ se $xy \in E(G)$. Um vez que a segunda parte é imediata, vamos provar apenas a primeira parte.

Seja C um ciclo arbitrário de G , pelo que ou é um triângulo ou o domínio interno da curva de Jordam que lhe está associada está dividido em triângulos T_i . Então, procedendo à adição módulo 2 das etiquetas das arestas que constituem os triângulos, obtém-se $(1,0) + (0,1) + (1,1) = (0,0)$ e, sendo T o conjunto dos triângulos do domínio interno de C (incluindo os que têm uma aresta em C), vem

$$0 = \sum_{e \in E(T)} \psi(e) = \sum_{e \in E(C)} \psi(e) + \sum_{e \in E(T) \setminus E(C)} \psi(e).$$

Dado que as arestas de $E(T) \setminus E(C)$ estão associadas a dois triângulos (logo contam duas vezes), podemos concluir que $\sum_{e \in E(T) \setminus E(C)} \psi(e) = 0$ e, consequentemente, $\sum_{e \in E(C)} \psi(e) = 0$. \square

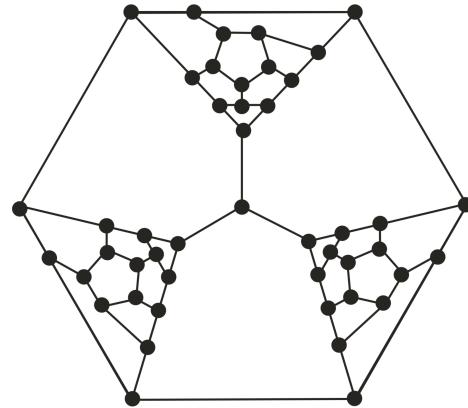


Figura 20.20: Contra-exemplo de Tutte para a conjectura de Tait.

Além de apresentar um contra-exemplo para a conjectura de Tait, Tutte provou [97] que todo o grafo planar, 4-conexo, é hamiltoniano (e, consequentemente, admite uma coloração das faces com quatro cores). Esta é, aliás, uma das várias condições suficientes (mas não necessárias) para um grafo ser hamiltoniano. Por sua vez, o próximo teorema, obtido por Grinberg [49], é uma das poucas condições necessárias (relativamente simples) para um grafo ser hamiltoniano, a qual pode ser utilizada para se concluir que certos grafos não admitem ciclos de Hamilton (o que não é o caso, porém, do grafo de Tutte representado na Figura 20.20 que, apesar de ser não-hamiltoniano, verifica esta condição necessária).

Teorema 20.30 (Grinberg). *Seja G é um grafo plano com um ciclo de Hamilton C , $F_0^{int}(C)$ e $F_0^{ext}(C)$ os subconjuntos de faces de G pertencentes, respectivamente, ao domínio interior e exterior da curva fechada de Jordan determinada por C . Se f_i^{int} e f_i^{ext} são o número de faces de grau i existentes, respectivamente, em $F_0^{int}(C)$ e $F_0^{ext}(C)$, então*

$$\sum_i (i-2)(f_i^{int} - f_i^{ext}) = 0,$$

onde o somatório é estendido a todos os graus das faces de G .

Demonstração. Suponha que o grafo G é realizado na esfera, pelo que C separa a superfície esférica em duas componentes conexas, uma que contém as faces do subconjunto $F_0^{int}(C)$ e outra que contém as faces do subconjunto $F_0^{ext}(C)$, as quais continuaremos a designar, respectivamente, por domínio interior e exterior de C . Sendo $E(G) = E(C) \cup E_{int}(C) \cup E_{ext}(C)$, onde $E_{int}(C)$ e $E_{ext}(C)$ denotam os subconjuntos de arestas que não estão em $E(C)$ e pertencem, respectivamente, ao domínio interior e exterior de C (pelo que $|E(G)| = |E(C)| + |E^{int}(C)| + |E^{ext}(C)|$), com facilidade se conclui que $|F_0^{int}| = |E^{int}(C)| + 1$ e $|F_0^{ext}| = |E^{ext}(C)| + 1$. Logo,

$$|F_0^{int}(C)| = \sum_i f_i^{int} = |E^{int}(C)| + 1 \quad (20.5)$$

$$|F_0^{ext}(C)| = \sum_i f_i^{ext} = |E^{ext}(C)| + 1 \quad (20.6)$$

e, por outro lado,

$$\sum_i i f_i^{int} = |E(C)| + 2|E^{int}(C)| \quad (20.7)$$

$$\sum_i i f_i^{ext} = |E(C)| + 2|E^{ext}(C)| \quad (20.8)$$

Combinando as igualdades (20.5) e (20.7) e as igualdades (20.6) e (20.8), obtém-se

$$\sum_i (i-2)f_i^{int} = |E(C)| - 2 \text{ e } \sum_i (i-2)f_i^{ext} = |E(C)| - 2$$

e, consequentemente, $\sum_i (i-2)(f_i^{int} - f_i^{ext}) = 0$. □

Como consequência deste teorema, Grinberg construiu vários contra-exemplos para a conjectura de Tait.

Em 1958, Grötzsch [52] obteve o resultado que a seguir se enuncia, conhecido por *teorema das três cores*.

Teorema 20.31 (Grötzsch). *Todo o grafo planar, sem lacetes e sem triângulos admite uma coloração de vértices com três cores.*

Uma vez que dado um par de mapas planares duais, G e G^* , os circuitos de G com c arestas são transformados em cortes de G^* (com o mesmo número de arestas, naturalmente), o teorema das três cores (de Grötzsch), pode ser reescrito na seguinte forma:

Teorema 20.32 (Grötzsch, 1958). *Todo o mapa planar, sem arestas de corte e sem cortes de cardinalidade 3 admite uma coloração das suas faces com 3 cores.*

Em 1963, Grünbaum [50] generalizou o teorema de Grötzsch, publicando o seguinte resultado:

Teorema 20.33 (Grünbaum). *Todo o mapa planar, sem arestas de corte e com não mais do que três cortes de cardinalidade três admite uma 3-coloração das suas faces.*

Porém, a suficiência de quatro cores para colorir as faces de um mapa planar arbitrário, só mais recentemente (1977), foi computacionalmente provada por Kenneth Appel e Wolfgang Haken [4, 5] e este resultado é conhecido por *teorema das quatro cores*. Tendo em conta a análise anterior, para se provar o teorema das quatro cores é suficiente provar que qualquer grafo planar-maximal (triangulação do plano) tem número cromático não superior a 4. Com este objectivo, a estratégia consiste em considerar contra-exemplos mínimos, ou seja, contra-exemplos de menor ordem que naturalmente admitem colorações com 5 cores e provar que são redutíveis, ou seja, eliminando um vértice admitem uma coloração com quatro cores (pela sua minimalidade) e, posteriormente, repondo o vértice e reorganizando as cores, é possível utilizar não mais do que quatro cores, o que é contraditório. Esta operação designa-se por *redução* e tais configurações por *configurações redutíveis*. Por exemplo, admitindo que um hipotético contra-exemplo G tem um vértice de grau 4, utilizando cadeias de Kempe, é fácil concluir que bastam quatro cores para colorir os vértices de G . Uma outra parte da prova, consiste em mostrar que todo o grafo plano contém uma destas configurações redutíveis, ou seja, estas configurações são *inevitáveis*, uma vez que qualquer grafo plano contém pelo menos uma delas. Assim, se provarmos que o conjunto de configurações inevitáveis é constituído unicamente por configurações redutíveis, provamos o teorema das quatro cores.

Já sabemos que basta considerar triangulações do plano (as quais correspondem aos duais de grafos simples, conexos, cúbicos e planos). Adicionalmente, uma vez que já sabemos que a presença de vértices de grau não superior a quatro implica a redutibilidade, podemos considerar apenas grafos planos cujo menor grau é cinco.

Designa-se por *contra-exemplo minimal* para o teorema das quatro cores, todo o grafo plano 5-crítico para a coloração de vértices (ou seja, que não admite uma coloração com quatro cores, mas qualquer dos seus subgrafos próprios tem número cromático não superior a quatro). Por sua vez, os contra-exemplos minimais para o teorema das quatro cores que são triangulações planas designam-se por *triangulações minimais*. Uma configuração é um grafo plano cujos vértices externos formam um anel de comprimento não inferior a quatro, contém vértices internos e todas as faces limitadas têm fronteira triangular. Como consequência, se um grafo plano, G , é uma configuração, então é conexo, sem pontes nem vértices de grau um e $\nu(G) \geq 4$. A Figura 20.21 representa uma configuração não trivial conhecida por *diamante de Birkhoff*.

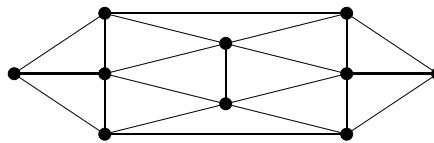


Figura 20.21: Diamante de Birkhoff.

Designa-se por comprimento do um anel de uma configuração, o comprimento do anel formado pelos vértices externos da configuração. Logo, o diamante de Birkhoff é uma configuração cujo anel

tem comprimento 6. Por sua vez, designa-se por núcleo de uma configuração o subgrafo induzido por todos os vértices internos.

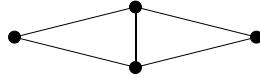


Figura 20.22: Núcleo do diamante de Birkhoff.

Uma triangulação do plano designa-se por *triangulação internamente 6-conexa* se nessa triangulação, todo o anel de comprimento não superior a cinco consiste ou nos vértices de um triângulo ou nos vizinhos de um vértice de grau cinco.

Relativamente às triangulações minimais, podemos destacar as seguintes propriedades:

- (a) Não contêm vértices de grau quatro (conforme anteriormente se concluiu).
- (b) Não admitem anéis de comprimento 4, conforme prova de Birkhoff [13].
- (c) Não admitem um anel de comprimento cinco cujo domínio interior da curva fechada de Jordan que lhe esta associada contenha mais do que um vértice, conforme prova de Birkhoff [13].
- (d) Não contêm diamantes de Birkhoff (podendo esta prova ser consultada em [42], pag. 180-183).

Verifica-se assim que todas as configurações cujo anel tem comprimento quatro ou cujo anel tem comprimento cinco, com mais do que um vértice interno, são configurações redutíveis.

O estudo da redutibilidade de configurações com anéis de comprimento 6 (como é o caso do diamante de Birkhoff), desenvolvido por Arthur Bernhart em 1947 [11], juntamente com os resultados de Birkhoff, constituem os fundamentos da verificação exaustiva de 1476 configurações, efectuada por Appel e Haken [4, 5] com recurso a computador. O próprio Birkhoff já havia concluído que uma configuração cujo anel tem comprimento 6, com pelo menos 4 vértices internos e tal que todos os vértices internos têm grau 5, contém o diamante de Birkhoff e, consequentemente, de acordo com (e), não pode ocorrer numa triangulação minimal. Por sua vez, as propriedades (b) e (c) das triangulações minimais, permitem concluir, ainda, que toda a triangulação minimal é internamente 6-conexa e foi precisamente esta conclusão que levou Robertson, Sanders, Seymour e Thomas em 1994 [83] a restringirem a sua atenção, unicamente, nas triangulações internamente 6-conexas e a apresentarem uma nova demonstração com verificação exaustiva de apenas 633 configurações.

20.4.2 Colorações em superfícies de genus positivo

Vamos denotar por $\chi(S_g)$ o maior número cromático dos grafos com genus g , ou seja, $\chi(S_g) = \max\{\chi(G) : G \text{ tem genus } g\}$. Sendo assim, o teorema das quatro cores implica que se tenha $\chi(S_0) = 4$ (note-se que K_4 é planar). Por outro lado, uma vez que K_5 admite uma realização no torus, é claro que $\chi(S_1) \geq 5$. Deve observar-se ainda que dados dois grafos G e H , tais que H é um subgrafo de G , o número cromático de H é não superior ao de G , ou seja, $\chi(G) \geq \chi(H)$, pelo que, em particular, se $K_n \subseteq G$, então $\chi(G) \geq n$. Tendo em conta que do Teorema 20.24 e da desigualdade (20.4), obtida em [79], decorre a igualdade $g_{K_n} = \lceil \frac{(n-3)(n-4)}{12} \rceil$. Uma vez que $\chi(K_p) = p$, podemos concluir que $\forall n > 0$

$$\chi(S_n) \geq \left\lceil \frac{7 + \sqrt{1 + 48n}}{2} \right\rceil.$$

Com efeito, para $p = \left\lfloor \frac{7+\sqrt{1+48n}}{2} \right\rfloor$, vem

$$\begin{aligned} g_{K_p} &= \left\lceil \frac{\left(\left\lfloor \frac{7+\sqrt{1+48n}}{2} \right\rfloor - 3 \right) \left(\left\lfloor \frac{7+\sqrt{1+48n}}{2} \right\rfloor - 4 \right)}{12} \right\rceil \\ &= \left\lceil \frac{\left\lfloor \frac{7+\sqrt{1+48n}}{2} - 3 \right\rfloor \left\lfloor \frac{7+\sqrt{1+48n}}{2} - 4 \right\rfloor}{12} \right\rceil \end{aligned} \quad (20.9)$$

$$\leq \left\lceil \frac{\left\lfloor \frac{-1+1+48n}{4} \right\rfloor}{12} \right\rceil \quad (20.10)$$

$$= n. \quad (20.11)$$

Logo, K_p é realizável em S_n e, consequentemente,

$$\chi(S_n) \geq \chi(K_p) = p = \left\lfloor \frac{7 + \sqrt{1 + 48n}}{2} \right\rfloor. \quad (20.12)$$

Note-se que a igualdade (20.9) se obtém, tendo em conta que para qualquer $m \in \mathbb{Z}$, $\lfloor x \rfloor - m = \lfloor x - m \rfloor$ e a desigualdade (20.10) decorre da desigualdade $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor$.

Em 1890, Heawood conjecturou a identidade $\chi(S_n) = \left\lfloor \frac{7+\sqrt{1+48n}}{2} \right\rfloor \forall n > 0$, tendo apenas provado a desigualdade recíproca da desigualdade (20.12). Combinando estas duas desigualdades, completa-se a prova da conjectura de Heawood.

Teorema 20.34. $\forall g \geq 0 \quad \chi(S_g) = \left\lfloor \frac{7+\sqrt{1+48g}}{2} \right\rfloor$.

Demonstração. Uma vez que, de acordo com o teorema das quatro cores, $\chi(S_0) = 4$ e, para $g = 0$, se obtém

$$\left\lfloor \frac{7 + \sqrt{1 + 48g}}{2} \right\rfloor = \left\lfloor \frac{7 + \sqrt{1 + 0}}{2} \right\rfloor = 4 = \chi(S_0),$$

resta fazer a prova para $g > 0$.

Tendo em conta a desigualdade (20.12), sabe-se que $\chi(S_g) \geq \left\lfloor \frac{7+\sqrt{1+48g}}{2} \right\rfloor$, para $g \geq 1$. Como consequência, se $g \geq 1$, então $\chi(S_g) \geq 7$. Sendo G um grafo com genus $g \geq 1$, tal que $\chi(G) = k \geq 7$, dado que $\nu(G) \geq 3$, cada face de G é limitada por, pelo menos, 3 arestas, donde $3|F_g(G)| \leq 2\varepsilon(G)$. Assim, aplicando a fórmula de Euler generalizada, $\nu(G) + |F_g(G)| - \varepsilon(G) = 2(1 - g)$, vem

$$\varepsilon(G) \leq 3\nu(G) - 6(1 - g). \quad (20.13)$$

Se G' um subgrafo de G que é k -crítico para a coloração de vértices, então $\delta(G') \geq k - 1$ ¹². Tendo em conta (20.13), $\delta(G')\nu(G') \leq 6\nu(G') - 12(1 - g)$ e, consequentemente, $(k - 1)\nu(G') \leq 6\nu(G') - 12(1 - g)$. Dado que esta última desigualdade é equivalente a $(k - 7)\nu(G') + 12(1 - g) \leq 0$, se $7 \leq k \leq \nu(G')$, então $(k - 7)k + 12(1 - g) \leq 0 \Leftrightarrow k^2 - 7k + 12(1 - g) \leq 0$, donde

$$k \leq \frac{7 + \sqrt{49 - 48(1 - g)}}{2} = \frac{7 + \sqrt{1 + 48g}}{2} \Leftrightarrow k \leq \left\lfloor \frac{7 + \sqrt{1 + 48g}}{2} \right\rfloor. \quad \square$$

Deve observar-se que a demonstração deste teorema vai contra a nossa intuição de que seria mais simples determinar $\chi(S_0)$ do que $\chi(S_n)$, para $n > 0$. Com efeito, embora se tenham obtido ambos os resultados, as técnicas até ao momento utilizadas para se chegar à determinação do primeiro são bem mais elaboradas do que as utilizadas na determinação do segundo.

¹²Note-se que se $v \in V(G')$ é um vértice k -crítico para a coloração de vértices, então $\chi(G' - \{v\}) = \chi(G') - 1 \leq d_G(v)$. Logo, se G' é k -crítico para a coloração de vértices, então $\chi(G') - 1 \leq \delta(G')$.

20.4.3 Conjecturas de Hadwiger e Hajós

Como consequência do teorema das quatro cores, todo o grafo simples G com número cromático $\chi(G) = 5$ é não-planar, donde, de acordo com o Teorema 20.14, é contractível a $K_{3,3}$ ou a K_5 . Uma vez que apenas o último destes grafos tem número cromático 5 (note-se que $K_{3,3}$ é bipartido e, consequentemente, admite uma bicoloração), podemos questionar se todos os grafos simples com número cromático 5 têm um subgrafo contractível a K_5 , ou seja, têm K_5 como menor combinatório. Em 1943, Hadwiger [53] formulou a conjectura que a seguir se indica e que, na sua forma geral, continua em aberto.

Conjectura 20.35 (Hadwiger). *Dado um grafo simples, G , para todo o inteiro positivo p ,*

$$\chi(G) \geq p \Rightarrow K_p \preceq G,$$

onde $S \preceq T$ denota que S é um menor de T .

Esta conjectura é trivialmente verdadeira para $p \leq 2$. Para $p = 3$, decorre da implicação de que se G não contém K_3 como menor, então G não contém ciclos (pelo que é uma floresta), logo G é bipartido e, consequentemente, admite uma bicoloração, i.e., $\chi(G) < 3$. O próprio Hadwiger fez a prova [53] da validade da conjectura no caso particular de $p = 4$, que é precisamente o que o teorema a seguir estabelece.

Teorema 20.36 (Hadwiger). *Dado um grafo simples G , $\chi(G) \geq 4 \Rightarrow K_4 \preceq G$.*

Demonstração. Vamos fazer a prova da implicação equivalente, $K_4 \not\preceq G \Rightarrow \chi(G) < 4$, por indução sobre o número de vértices, tendo em conta que a implicação se verifica, trivialmente, para grafos de ordem não superior a 3.

Seja G um grafo simples de ordem $\nu > 3$, não contractível a K_4 , e suponha que a implicação se verifica para grafos simples de ordem inferior ν . Suponha ainda (sem perda de generalidade) que G é conexo e contém ciclos. Seja $C = v_1, v_2, \dots, v_k, v_1$ um ciclo de menor comprimento em G e seja H o subgrafo induzido pelos vértices que não estão em C , ou seja, $H = G[V(G) \setminus \{v_1, v_2, \dots, v_k\}]$ e sejam H_1, \dots, H_m , as componentes conexas de H . Vamos dividir esta prova em 3 partes.

1. Vamos provar, inicialmente, que se existe um vértice de C sem vizinhos em H , então $\chi(G) < 4$, pelo que, a implicação se verifica. Com efeito, suponha que existe um vértice v_j em C que não tem vizinhos em H (ou seja, $d_G(v_j) = 2$). Por hipótese de indução, $G - \{v_j\}$ admite uma coloração de vértices com três cores que se pode estender a G , uma vez que $d_G(v_j) = 2$. Assim, de agora em diante, vamos assumir que qualquer vértice de C tem pelo menos um vizinho em H .
2. Vamos provar que, para cada j , o número de vértices de C adjacentes a vértices de H_j é não superior a 2. Suponha que para algum j , existem 3 vértices de C , v_{i_1}, v_{i_2} e v_{i_3} , adjacentes a vértices de H_j , então é possível contrair H_j a um único vértice v e o ciclo C ao triângulo $v_{i_1}, v_{i_2}, v_{i_3}$ e estes 4 vértices induzem K_4 , o que contradiz a hipótese. Logo, qualquer das componentes H_j tem, no máximo, dois vizinhos em C .
3. Na última parte desta prova consideramos o caso em que (a) existe uma componente H_j com um único vizinho em C e o caso em que (b) todas as componentes de H têm exactamente dois vizinhos em C .
 - (a) Seja H_j uma componente de H , com um único vizinho em C , v_i . Então v_i é um vértice de corte para G , donde, sendo G_1 e G_2 as componentes de $G - \{v_i\}$, por hipótese de indução, os subgrafos induzidos $G[V(G_1) \cup \{v_i\}]$ e $G[V(G_2) \cup \{v_i\}]$ admitem uma coloração de vértices com três cores, a qual pode ser estendida a G .

- (b) Neste caso, é possível provar que não existem duas componentes H_i e H_j , relativamente às quais, se $v_{i_1}, v_{i_2} \in V(C)$ são os vizinhos de H_i e $v_{j_1}, v_{j_2} \in V(C)$ os vizinhos de H_j , então $i_1 < j_1 < i_2 < j_2$. Com efeito, caso existissem todos estes vizinhos, seria possível contrair o ciclo C e as componentes H_i e H_j , conjuntamente, de modo a obter K_4 , o que contraria a hipótese. Logo, existem dois vértices de C adjacentes, v_r e v_{r+1} , vizinhos de, pelo menos, uma componente H_i . Nestas condições, podemos dividir o grafo G em dois subgrafos, G_1 e G_2 , sendo $G_1 = G[V(H_i) \cup \{v_r, v_{r+1}\}]$ e $G_2 = [V(G) \setminus V(H_i)]$ e é claro que ambos têm em comum apenas a aresta $v_r v_{r+1}$. Por hipótese de indução, tanto G_1 como G_2 admitem uma coloração de vértices com três cores, a qual pode ser estendida a G , desde que se escolham adequadamente as cores de modo que v_r tenha a mesma cor em G_1 e G_2 e o mesmo aconteça a v_{r+1} . \square

Conforme provaremos no Exemplo 20.1, se a conjectura de Hadwiger é verdadeira para um inteiro positivo particular p , então também é verdadeira para todos os inteiros positivos inferiores a p . Como consequência, caso exista um inteiro positivo p , para o qual a conjectura de Hadwiger é falsa, podemos concluir que ela é falsa para todos os inteiros superiores a p .

Exemplo 20.1. *Vamos provar que se a conjectura de Hadwiger é verdadeira para $p = q$, então também é verdadeira para $p < q$.*

Solução. Suponha que a conjectura é verdadeira para $p = q$ e $\chi(G) \geq q - 1$. Então, considerando o grafo $G \oplus v$, com $v \notin V(G)$ e tal que

$$V(G \oplus v) = V(G) \cup \{v\} \text{ e } E(G \oplus v) = E(G) \cup \{xv : x \in V(G)\},$$

$$\chi(G \oplus v) = \chi(G) + 1 \geq q \text{ e, uma vez que por hipótese } K_q \preceq G \oplus v, K_{q-1} \preceq G. \quad \square$$

Com base na implicação

$$(\chi(G) \geq p \Rightarrow K_p \preceq G) \Rightarrow (\chi(G) \geq p - 1 \Rightarrow K_{p-1} \preceq G)$$

que se provou no Exemplo 20.1, podemos concluir que a validade da conjectura de Hadwiger para $p \geq 5$, implica o teorema das 4 cores que estabelece que se G é planar, então $\chi(G) \leq 4$. Com efeito, para $p = 5 + k$, vem

$$\begin{aligned} (\chi(G) \geq 5 + k \Rightarrow K_{5+k} \preceq G) &\Rightarrow (\chi(G) \geq 5 + k - 1 \Rightarrow K_{5+k-1} \preceq G) \\ &\Rightarrow (\chi(G) \geq 5 + k - 2 \Rightarrow K_{5+k-2} \preceq G) \\ &\vdots \\ &\Rightarrow (\chi(G) \geq 5 \Rightarrow K_5 \preceq G). \end{aligned}$$

Logo, se G é planar, então G não contém um subgrafo contractível a K_5 (i.e., K_5 não é um menor de G) e, tendo em conta a última das implicações obtidas, $\chi(G) < 5$.

Segue-se o teorema da equivalência de Wagner [104] que relaciona a conjectura de Hadwiger, para $p = 5$, com o teorema das quatro cores.

Teorema 20.37 (Wagner). *A conjectura de Hadwiger, para o caso particular de $p = 5$, é equivalente ao teorema das quatro cores.*

Demonstração. De acordo com a análise anterior, podemos concluir que a validade da conjectura de Hadwiger, no caso particular de $p = 5$, implica o teorema das quatro cores. Para provarmos o recíproco, vamos partir do teorema das quatro cores e assumir que G é um grafo simples, não-contractível a K_5 , mas $\chi(G) = 5$. Então G é não-planar e, assumindo que G tem o mínimo número de arestas de entre

os grafos com esta propriedade (pelo que, qualquer subgrafo com menos arestas admite uma coloração de vértices com 4 cores), de acordo com o Lema 20.11, G é 3-conexo, donde, se $S \subset V(G)$ é um subconjunto de vértices de cardinalidade mínima que desconexa G , então $|S| = 3$. Supondo que $G - S$ tem componentes H_1, \dots, H_k , com $k \geq 2$, vamos considerar os subgrafos $G_i = G[S \cup V(H_i)]$, para $i = 1, \dots, k$ (note-se que para cada $i \in \{1, \dots, k\}$, existe pelo menos uma aresta entre S e H_i). Sendo $T \subseteq S$ um subconjunto independente maximal (em S), então $T = S$ ou $G[S - T] \in \{K_1, K_2\}$. Assim, os vértices de qualquer subgrafo G_i podem ser coloridos com 4 cores, de tal forma que todos os vértices em T têm a mesma cor c e os vértices em $S - T$ têm cores distintas de c (note-se que sendo T um conjunto independente maximal em S , todos os vértices de $S - T$ são adjacentes a um vértice em T). Consequentemente, qualquer coloração de vértices em $G[S]$ produz a mesma partição de S e, consequentemente, é possível colorir os vértices de cada subgrafo G_i , com 4 cores e de tal forma que as cores dos vértices em S permaneçam as mesmas em todos os subgrafos G_i , para $i = 1, \dots, k$. Logo, esta coloração é extensível a G , o que é contraditório com a hipótese de se ter $\chi(G) = 5$. \square

A prova da conjectura de Hadwiger para $p = 6$, decorre de um estudo sobre grafos não-contractíveis a K_6 , desenvolvido por Robertson, Seymour e Thomas [85], onde, assumindo a validade do teorema das quatro cores, se conclui que tais grafos admitem uma coloração dos vértices com 5 cores e, consequentemente, que a conjectura de Hadwiger é verdadeira para $p = 6$.

Uma variante da conjectura de Hadwiger, proposta por Hajós em 1961 [54], contempla a subdivisão em vez da contracção de grafos, ou seja, considera menores topológicos em vez de menores combinatórios.

Conjectura 20.38 (Hajós). *Dado um grafo simples G , se $\chi(G) = p$, então K_p é um menor topológico de G .*

Apesar da semelhança, as duas conjecturas são muito diferentes. Com facilidade se conclui que para $p \leq 2$, a conjectura de Hajós é verdadeira e a prova para o caso particular de $p = 3$ decorre do facto de todo o grafo com número cromático 3 conter um ciclo ímpar (caso contrário, seria bipartido) que é uma subdivisão de K_3 . Dirac, em 1952 [32], provou a validade da conjectura de Hajós, para o caso particular de $p = 4$ e, apesar da prova obtida por Catlin, em 1979 [24], de que esta conjectura é falsa para $p > 6$, continua por provar se é verdadeira ou falsa, para $p \in \{5, 6\}$.

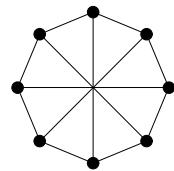
Teorema 20.39 (Catlin). *A conjectura de Hajós é falsa para $p \geq 7$.*

Demonstração. Vamos começar por provar que a conjectura é falsa para $p = 7$. Com efeito, vamos considerar o contra-exemplo apresentado por Catlin, $H = L(3C_5) - \{x, y\}$, onde $3C_5$ é o grafo que se obtém de C_5 , substituindo cada aresta por 3 arestas paralelas, $L(3C_5)$ denota o respectivo grafo linha e x e y são dois vértices não adjacentes de $L(3C_5)$. Dado que H contém K_6 e, a partir de qualquer dos vértices, $v \notin V(K_6)$, não existem 6 caminhos disjuntos nas arestas entre v e os vértices de K_6 , K_6 é o subgrafo completo de maior ordem que é menor topológico de H . Por outro lado, uma vez que $\alpha(H) = 2$, de acordo com o Teorema 19.10, $\chi(H) \geq \lceil \frac{13}{2} \rceil = 7$. Sendo fácil obter uma coloração dos vértices de H com 7 cores, podemos concluir que $\chi(H) = 7$ e H não contém K_7 como menor topológico. O resto da prova decorre, directamente, da seguinte implicação (a provar): se G é um contra-exemplo para a conjectura de Hajós, então $G \oplus v$, onde $v \notin V(G)$, $V(G \oplus v) = V(G) \cup \{v\}$ e $E(G \oplus v) = E(G) \cup \{uv : u \in V(G)\}$, é também um contra-exemplo para a conjectura de Hajós. Com efeito, se $\chi(G) = p$ e G não contém K_p como menor topológico, então $\chi(G \oplus v) = p + 1$ e $G \oplus v$ não contém K_{p+1} como menor topológico. Logo, a conjectura de Hajós é falsa para $p \geq 7$. \square

20.5. Exercícios

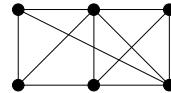
20.1. Determine um menor topológico isomorfo a $K_{3,3}$ de cada um dos seguintes grafos:

- (a) Grafo representado na Figura 20.16;
 (b) Grafo representado na figura a seguir.



- 20.2. Mostre que $K_{3,3}$ tem um menor topológico isomorfo a K_4 .
- 20.3. Mostre que o 4-cubo, Q_4 , tem um menor isomorfo a K_5 . Como consequência, demonstre que o k -cubo é não planar se e só se $k > 3$
- 20.4. Mostre que o grafo de Petersen tem $K_{3,3}$ como menor topológico.
- 20.5. Prove que se G é um grafo bipartido e plano, então $\delta(G) \leq 3$.
- 20.6. Dado um grafo G dos vértices e arestas de um poliedro, que é um grafo simples, conexo, planar, cujo menor grau é maior ou igual a 3, responda às seguintes questões:
- Prove que $|\varepsilon(G)| \neq 7$.
 - Prove que se G tem 11 faces, então $|\varepsilon(G)| \neq 30$.
- 20.7. Dado um conjunto de n circunferências representadas no plano de tal forma que quaisquer duas se intersectam em dois pontos e não existe um ponto que seja intersecção de mais do que duas circunferências, determine o número de regiões em que estas n circunferências dividem o plano.
- 20.8. Considere uma circunferência representada no plano, conjuntamente com n ($n \in \mathbb{N}$) rectas que se intersectam duas a duas num único ponto do interior do círculo limitado pela circunferência. Supondo que não existem três rectas que se intersectem no mesmo ponto, determine o número de regiões definidas pelas rectas e pela circunferência.
- 20.9. Prove que o grafo de Petersen (representado na Figura 14.4, página 385) é não-planar.
- 20.10. Supondo que G é uma triangulação do plano (ou seja, um grafo planar onde todas as faces têm grau 3) e sendo n_i o número de vértices de grau i , para $i = \delta(G), \dots, \Delta(G)$, prove que
- $$\sum_{i=\delta(G)}^{\Delta(G)} (6-i)n_i = 12.$$
- 20.11. Dado um grafo, G , simples, conexo, planar, com mais do que uma aresta, prove que G tem pelo menos três vértices de grau não superior a 5.
- 20.12. Seja G um grafo simples, planar e conexo.
- Mostre que se $\varepsilon(G) = 3\nu(G) - 6$, então G é triangular.
 - Prove que o poliedro convexo, com 12 vértices e 20 faces é composto unicamente por triângulos.
- 20.13. Existe algum grafo planar bipartido com 7 vértices e 11 arestas?
- 20.14. Prove a equivalência das seguintes afirmações:

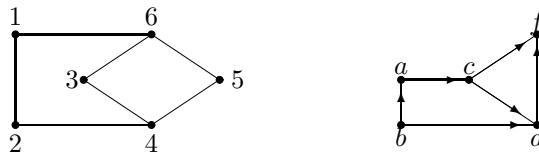
- (a) G é um grafo planar maximal;
- (b) G é uma triangulação do plano;
- (c) $\varepsilon(G) = 3\nu(G) - 6$ e G é planar.
- 20.15. Dado um grafo conexo G de ordem $\nu(G) \geq 11$, sem lacetes, prove que G ou G^c é não-não-planar.
- 20.16. Mostre que o grafo representado na figura a seguir é planar e aplique a fórmula de Euler para a determinação do número de faces.



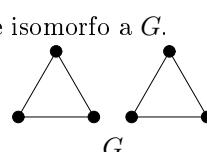
- 20.17. Prove que se G é um grafo planar de ordem $n \geq 3$, tal que $g(G) < \infty$ (onde $g(G)$ denota a cintura de G), então

$$|E(G)| \leq \frac{g(G)(n-2)}{g(G)-2}. \quad (20.14)$$

- 20.18. Determine os duais do grafo e digrafo planar, a seguir representados.



- 20.19. Dado um grafo planar G , tal que $f_0 = |V(G)|$, $f_1 = |E(G)|$ e $f_2 = |F_0(G)|$, sendo G^* o respectivo dual, prove que $|V(G^*)| = f_2$, $|E(G^*)| = f_1$ e $|F_0(G^*)| = f_0$.
- 20.20. Considere o problema das 7 pontes de Königsberg, descrito no início do capítulo 18, e prove que é possível a um nadador nadar entre dois pontos do rio passando por baixo de cada ponte uma única vez (ver Figura 20.12, página 562), ou seja, construa um grafo H que represente este problema e prove que H é semi-euleriano (ver Definição 18.2).
- 20.21. Considere o grafo H do Exercício 20.20 e responda às seguintes questões:
- (a) Quais as diferenças entre o grafo H e o dual do grafo proposto por Euler para o problema das 7 pontes de Königsberg?
- (b) Prove que não é possível a um nadador passar por baixo de todas as pontes sem repetir nenhuma e voltar ao ponto de partida, ou seja, prove que H não é euleriano.
- 20.22. Seja G o grafo desconexo planar que se representa na figura a seguir.
- (a) Represente o dual de G , G^* , e o dual de G^* , $(G^*)^*$.
- (b) Prove que se G é desconexo e planar, então G^* é conexo.
- (c) Prove que, em geral, $(G^*)^*$ não é isomorfo a G .



- 20.23. Considere um poliedro com faces triangulares e pentagonais tais que, cada triângulo faz fronteira unicamente com pentágonos e cada pentágono faz fronteira unicamente com triângulos, onde cada vértice tem grau p e seja G o grafo dos vértices e arestas deste poliedro.
- Prove a igualdade $\frac{1}{\varepsilon(G)} = \frac{1}{p} - \frac{7}{30}$.
 - Deduza que o grau dos vértices é $p = 4$ e ainda que existem 20 triângulos e 12 pentágonos.
 - Descreva o grafo dual de G .
- 20.24. Prove que um grafo G de ordem n e genus g tem no máximo $3(n - 2 + 2g)$ arestas.
- 20.25. Determine o genus de um grafo constituído unicamente por dois blocos extremos G_1 e G_2 , tais que $G_1 = K_5$ e $G_2 = K_{3,3}$.

Apêndices



A

Notação Assimptótica

Quando consideramos "grandes" objectos de natureza combinatória ou outra, nem sempre é necessário determinar o valor exacto de uma dada quantidade (especialmente quando a fórmula exacta não é conhecida ou, sendo conhecida, é complicada). Nesses casos, muitas vezes, basta conhecer apenas um valor aproximado. É precisamente para este tipo de problemas que se utiliza a notação assimptótica.

A notação assimptótica foi introduzida por Paul Bachmann em 1894 e, actualmente, tem utilização generalizada. A sua popularização deve-se essencialmente a Edmund Landau e, por esse motivo, é conhecida por notação de Landau.

Neste texto consideramos apenas os casos em que n é uma variável inteira que toma valores arbitrariamente grandes ($n \rightarrow \infty$). Também se poderia considerar os casos que envolvem variáveis convergentes para valores finitos, os quais, porém, estão fora do nosso contexto.

Note-se que, ao longo do livro, utilizamos algumas vezes argumentos de natureza assimptótica. Por exemplo, a fórmula (6.18) constitui uma expressão assimptótica para os números de Fibonacci e as fórmulas (6.1) e (6.2) são expressões assimptóticas para os números factoriais.

A.1. Notação "O-grande" (\mathcal{O})

O primeiro símbolo considerado é \mathcal{O} (ler "O-grande")¹. Utilizando este símbolo, podemos expressar o ritmo com que uma dada função cresce (ou decresce) comparativamente com o ritmo com que uma outra função cresce (decresce).

Definição A.1 (Notação assimptótica \mathcal{O}). *Dadas duas funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, diz-se que a função $f(n)$ é de ordem não superior à função $g(n)$ (quando $n \rightarrow \infty$) e escreve-se $f(n) = \mathcal{O}(g(n))$ se e só se*

$$\exists c > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n > n_0 \quad |f(n)| \leq c|g(n)|.$$

Exemplo A.1. Dada a função $f : \mathbb{N} \rightarrow \mathbb{R}$ tal que $f(n) = n^2$, verifique qual ou quais as fórmulas verdadeiras de entre as que a seguir se indicam².

- (a) $f(n) = \mathcal{O}(n)$,
- (b) $f(n) = \mathcal{O}(n^2)$,
- (c) $f(n) = \mathcal{O}(n^3)$.

¹Inicialmente Bachmann e Landau utilizaram como notação a letra grega omicron maiúscula. Porém, como a forma gráfica desta letra grega é idêntica à letra latina "O", a designação "O-grande" acabou por se popularizar.

²Nestas expressões e ao longo deste capítulo, utilizaremos uma notação menos formal, por exemplo $f(n) = \mathcal{O}(n^2)$ que significa $f(n) = \mathcal{O}(g(n))$, onde g é tal que para cada $n \in \mathbb{N}$, $g(n) = n^2$.

Solução.

- (a) Para se ter $f(n) = \mathcal{O}(n)$ é necessário que exista uma constante c tal que para n suficientemente grande se verifica a desigualdade $n^2 \leq cn$. Uma vez que uma tal constante não existe, concluímos que $f(n) \neq \mathcal{O}(n)$.
- (b) Com efeito, $f(n) = \mathcal{O}(n^2)$ uma vez que a desigualdade $n^2 \leq cn^2$ se verifica, com $c = 1$, para todo $n \in \mathbb{N}$.
- (c) Com efeito, $f(n) = \mathcal{O}(n^3)$ uma vez que a desigualdade $n^2 \leq cn^3$ se verifica, com $c = 1$, para todo $n \in \mathbb{N}$. \square

A expressão $\mathcal{O}(f(n)) = \mathcal{O}(g(n))$ significa que todas as funções que são $\mathcal{O}(f(n))$ também são $\mathcal{O}(g(n))$ (por exemplo, $\mathcal{O}(n^2) = \mathcal{O}(n^3)$).

Atenção. Note-se que a relação de igualdade assimptótica não é uma relação simétrica. Por exemplo, podemos escrever $f(n) = \mathcal{O}(n^2)$ mas não $\mathcal{O}(n^2) = f(n)$. De modo idêntico se verifica que $\mathcal{O}(n^2) = \mathcal{O}(n^3)$, mas $\mathcal{O}(n^3) \neq \mathcal{O}(n^2)$. Para uma mais fácil compreensão deste conceito, podemos considerar $\mathcal{O}(f(n))$ como o conjunto de todas as funções de ordem não superior a $f(n)$. Nesta linha, alguns autores propõem que a expressão $f(n) = \mathcal{O}(n^2) = \mathcal{O}(n^3)$ se escreva na forma $f(n) \in \mathcal{O}(n^2) \subseteq \mathcal{O}(n^3)$. Na verdade, esta última notação é mais intuitiva e coerente com a ausência de simetria, porém, a notação de Landau tem já uma utilização praticamente universal e por esta razão é também a adoptada neste texto³.

Seguem-se alguns exemplos que põem em evidência certas propriedades do símbolo \mathcal{O} .

Exemplo A.2. Vamos mostrar que para qualquer par de funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$ se verifica:

- (a) $f(n) = \mathcal{O}(f(n))$;
- (b) se $f(n) = \mathcal{O}(g(n))$ então $f(n) = \mathcal{O}(\alpha g(n))$ para qualquer constante $\alpha \neq 0$;
- (c) $f(n) + g(n) = \mathcal{O}(\max\{|f(n)|, |g(n)|\})$;
- (d) se existe $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ então $f(n) = \mathcal{O}(g(n))$ se e só se $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| < \infty$.

Solução.

- (a) Uma vez que para cada $n \in \mathbb{N}$ e para $c = 1$ se verifica $|f(n)| \leq c|f(n)|$, então $f(n) = \mathcal{O}(f(n))$.
- (b) Se $f(n) = \mathcal{O}(g(n))$, então existe uma constante $c > 0$ e $n_0 \in \mathbb{N}$ tal que para qualquer $n > n_0$, $|f(n)| \leq c|g(n)|$. Porém, esta última desigualdade é equivalente à desigualdade $|f(n)| \leq \frac{c}{|\alpha|}|\alpha g(n)|$ que, por sua vez, implica $f(n) = \mathcal{O}(\alpha g(n))$.
- (c) Uma vez que para cada $n \in \mathbb{N}$ se verificam as desigualdades $|f(n)| \leq \max\{|f(n)|, |g(n)|\}$ e $|g(n)| \leq \max\{|f(n)|, |g(n)|\}$, vem que $|f(n) + g(n)| \leq |f(n)| + |g(n)| \leq 2 \max\{|f(n)|, |g(n)|\}$ o que, por definição, equivale à igualdade $f(n) + g(n) = \mathcal{O}(\max\{|f(n)|, |g(n)|\})$.
- (d) Suponhamos que $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ existe (sendo finito ou infinito). Se $f(n) = \mathcal{O}(g(n))$, então existe uma constante $c > 0$ tal que para n suficientemente grande, $\left| \frac{f(n)}{g(n)} \right| < c$ e, consequentemente, $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| \leq c < \infty$. Reciprocamente, se $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = c < \infty$, então para qualquer $\varepsilon > 0$ e n suficientemente grande, $\left| \frac{f(n)}{g(n)} \right| < c + \varepsilon$ e esta desigualdade equivale à desigualdade $|f(n)| < (c + \varepsilon)|g(n)|$. Logo, $f(n) = \mathcal{O}(g(n))$. \square

³Note-se que existem também outras notações assimptóticas, como por exemplo na notação de Hardy segundo a qual a expressão $f(n) = \mathcal{O}(g(n))$ toma a forma $f(n) \lesssim g(n)$ e expressão $f(n) = o(g(n))$ (com notação a introduzir mais adiante) toma a forma $f(n) \ll g(n)$.

A propriedade (d), deste exemplo, simplifica a verificação da relação $f(n) = \mathcal{O}(g(n))$, nos casos em que podemos calcular (ou estimar) o $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$. Deve observar-se que algumas vezes, mesmo não existindo este limite, pode verificar-se a igualdade assintótica $f(n) = \mathcal{O}(g(n))$, conforme a seguir se exemplifica.

Exemplo A.3. Vamos dar exemplos de pares de funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$ para os quais $f(n) = \mathcal{O}(g(n))$, embora o $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ não exista.

Solução. Os exemplos que se seguem são dois casos típicos, um que envolve funções com valores nulos e outro que considera uma função cujos valores oscilam sistematicamente.

(a) Seja

$$f(n) = \begin{cases} n, & \text{para } n = 2k \\ 0, & \text{para } n = 2k + 1 \end{cases} \quad \text{e} \quad g(n) = \begin{cases} 5n, & \text{para } n = 2k \\ 0, & \text{para } n = 2k + 1. \end{cases}$$

Então, para qualquer $n \in \mathbb{N}$, verifica-se a desigualdade $|f(n)| \leq |g(n)|$, pelo que $f(n) = \mathcal{O}(g(n))$.

Porém, o quociente $\frac{f(n)}{g(n)}$ não tem significado para valores ímpares de n e, consequentemente, o $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ não existe. \square

(b) Seja $h(n) = \operatorname{sen}(n)$. Uma vez que $|\operatorname{sen}(n)| \leq 1$, podemos concluir a igualdade $\operatorname{sen}(n) = \mathcal{O}(1)$, mas $\lim_{n \rightarrow \infty} |\operatorname{sen}(n)|$ não existe. \square

Exemplo A.4. Vamos provar que $\log n = \mathcal{O}(\sqrt{n})$ e $\sqrt{n} \neq \mathcal{O}(\log n)$.

Solução. Recorrendo ao Exemplo A.2-(d), vamos começar por determinar o $\lim_{n \rightarrow \infty} \frac{\log n}{\sqrt{n}}$. Aplicado a regra de l'Hôpital, obtém-se

$$\lim_{n \rightarrow \infty} \frac{\log n}{\sqrt{n}} = \lim_{n \rightarrow \infty} \frac{n^{-1}}{\frac{1}{2}n^{-\frac{1}{2}}} = \lim_{n \rightarrow \infty} \frac{2}{\sqrt{n}} = 0 < \infty.$$

Como consequência, $\log n = \mathcal{O}(\sqrt{n})$.

Por sua vez, determinando $\lim_{n \rightarrow \infty} \frac{\sqrt{n}}{\log n}$, aplicando, novamente, a regra de l'Hôpital, vem

$$\lim_{n \rightarrow \infty} \frac{\sqrt{n}}{\log n} = \lim_{n \rightarrow \infty} \frac{\frac{1}{2}n^{-\frac{1}{2}}}{n^{-1}} = \lim_{n \rightarrow \infty} \frac{1}{2}\sqrt{n} = \infty,$$

onde $\sqrt{n} \neq \mathcal{O}(\log n)$. \square

Exemplo A.5. Sendo $w : \mathbb{N} \rightarrow \mathbb{R}$ um polinómio $w(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0$, com $a_k \neq 0$, vamos provar a igualdade $w(n) = \mathcal{O}(n^k)$.

Solução. Dado que para $n \in \mathbb{N}$ e $l \leq k$, se verifica a desigualdade $n^l \leq n^k$, então

$$\begin{aligned} |w(n)| &= |a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0| \\ &\leq |a_k| n^k + |a_{k-1}| n^{k-1} + \cdots + |a_1| n + |a_0| \\ &\leq (|a_k| + |a_{k-1}| + \cdots + |a_1| + |a_0|) n^k, \end{aligned}$$

e, consequentemente, por definição, $w(n) = \mathcal{O}(n^k)$. \square

As expressões assintóticas podem tomar formas mais elaboradas do que as anteriormente consideradas. Por exemplo, a expressão assintótica $f(n) = g(n) + \mathcal{O}(h(n))$ é equivalente à expressão assintótica $f(n) - g(n) = \mathcal{O}(h(n))$.

Exemplo A.6. Vamos mostrar que $(n+1)^3 = n^3 + \mathcal{O}(n^2)$.

Solução. Uma vez que $(n+1)^3 - n^3 = 3n^2 + 3n + 1$ é um polinómio de grau dois, tendo em conta o Exemplo A.5, vem que $(n+1)^3 - n^3 = \mathcal{O}(n^2)$. \square

Exemplo A.7. Vamos detectar o erro existente na seguinte afirmação:

Seja $S(n) = 1 + 2 + 3 + \dots + n$. Uma vez que cada termo desta soma é não superior a n , generalizando o Exemplo A.2-(c), vem que para a soma dos n termos se obtém $S(n) = \mathcal{O}(\max\{1, 2, \dots, n\}) = \mathcal{O}(n)$.

Observe-se ainda que de acordo com o Exemplo 2.8, $S(n) = \frac{1}{2}n^2 + \frac{1}{2}n$ e, consequentemente, tendo em conta o Exemplo A.1-(a), $S(n) \neq \mathcal{O}(n)$.

Solução. É claro que o Exemplo A.2-(c) pode ser generalizado para qualquer número finito de termos. Com efeito, para todo $k \in \mathbb{N}$,

$$f_1(n) + f_2(n) + \dots + f_k(n) = \mathcal{O}(\max\{|f_1(n)|, |f_2(n)|, \dots, |f_k(n)|\}).$$

Porém, não é possível utilizar esta fórmula com n termos (como é o caso de $S(n)$), uma vez que quando se utiliza notação assimptótica, por definição, pressupõe-se que $n \rightarrow \infty$. Logo, $S(n) \neq \mathcal{O}(n)$. \square

Deve observar-se que nem todas as funções admitem uma comparação assimptótica, com recurso ao símbolo \mathcal{O} , conforme o exemplo a seguir ilustra.

Exemplo A.8. Vamos dar um exemplo de duas funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, para as quais $f(n) \neq \mathcal{O}(g(n))$ e $g(n) \neq \mathcal{O}(f(n))$.

Solução. Considerem-se as funções

$$f(n) = \begin{cases} n, & \text{para } n = 2k \\ n^2, & \text{para } n = 2k + 1 \end{cases} \quad \text{e} \quad g(n) = \begin{cases} n^2, & \text{para } n = 2k \\ n, & \text{para } n = 2k + 1. \end{cases}$$

Neste caso, para n par não existe uma constante c tal que $f(n) \leq cg(n)$ e para n ímpar não existe uma constante c' tal que $g(n) \leq c'f(n)$. \square

A.2. A notação "o-pequeno" (o)

A notação "o-pequeno" é utilizada para indicar que uma dada função é de ordem inferior a outra (dizendo-se também que é negligenciável relativamente a outra).

Definição A.2. (Notação assimptótica o). Dadas duas funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, diz-se que a função $f(n)$ é de ordem inferior à função $g(n)$ (quando $n \rightarrow \infty$) e escreve-se $f(n) = o(g(n))$ se e só se

$$\forall_{c>0} \exists_{n_0 \in \mathbb{N}} \forall_{n > n_0} |f(n)| < c|g(n)|.$$

O exemplo que se segue ilustra algumas propriedades da notação assimptótica "o-pequeno".

Exemplo A.9. Vamos mostrar que para qualquer par de funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$ se verifica:

- (a) $f(n) \neq o(f(n))$;
- (b) se $f(n) = o(g(n))$ então $f(n) = o(\alpha g(n))$ para qualquer constante $\alpha \neq 0$;
- (c) se $f(n) = o(g(n))$ então $f(n) = \mathcal{O}(g(n))$;

$$(d) \text{ se existe } o \lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|, \text{ então } f(n) = o(g(n)) \text{ se e só se } \lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 0.$$

Solução.

- (a) Considerando, por exemplo, $c = \frac{1}{2}$, é claro que $|f(n)| \leq \frac{1}{2}|f(n)|$ não se verifica para nenhum valor de n .
- (b) Suponha que $f(n) = o(g(n))$ e seja $c > 0$ uma constante. De acordo com a definição da notação assimptótica "o-pequeno", existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$, $|f(n)| < c|\alpha| \cdot |g(n)|$ e esta desigualdade é equivalente à desigualdade $|f(n)| < c|\alpha g(n)|$. Consequentemente, $f(n) = o(\alpha g(n))$.
- (c) Assumindo que $f(n) = o(g(n))$ e que $c > 0$ é uma constante, podemos concluir que para n suficientemente grande se verifica a desigualdade $|f(n)| < c|g(n)|$, pelo que $f(n) = \Theta(g(n))$.
- (d) Suponha que $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ existe.
Se $f(n) = o(g(n))$, então para cada constante $c > 0$ arbitrariamente pequena e n suficientemente grande, $\left| \frac{f(n)}{g(n)} \right| < c$. Logo, $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 0$.
Reciprocamente, se $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 0$, então para qualquer constante $c > 0$ e n suficientemente grande, obtém-se a desigualdade $\left| \frac{f(n)}{g(n)} \right| < c$ que é equivalente à desigualdade $|f(n)| < c|g(n)|$. Logo, $f(n) = o(g(n))$. \square

Em certos textos utiliza-se a notação assimptótica ω que se define da seguinte forma: $f(n) = \omega(g(n))$ se e só se $g(n) = o(f(n))$. Assim, se $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ existe, então $f(n) = \omega(g(n))$ se e só se $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = \infty$.

A.3. Outras notações assimptóticas

Relembrando que a notação assimptótica Θ significa "de ordem não superior", deve referir-se que também existe a notação assimptótica "de ordem não inferior" – que utiliza a letra grega Ω .

Definição A.3 (Notação assimptótica Ω). *Dadas duas funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, diz-se que a função $f(n)$ é de ordem não inferior à função $g(n)$ (quando $n \rightarrow \infty$) e escreve-se $f(n) = \Omega(g(n))$ se e só se*

$$\exists_{c>0} \exists_{n_0 \in \mathbb{N}} \forall_{n > n_0} |f(n)| \geq c|g(n)|.$$

Note-se que $f(n) = \Omega(g(n))$ se e só se $g(n) = \Theta(f(n))$.

Existe ainda um outro símbolo assimptótico, de uso comum, a letra grega Θ que é utilizada para designar "é da mesma ordem".

Definição A.4 (Notação assimptótica Θ). *Dadas duas funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, diz-se que a função $f(n)$ é da mesma ordem que a função $g(n)$ (quando $n \rightarrow \infty$) e escreve-se $f(n) = \Theta(g(n))$ se e só se*

$$\exists_{c_1, c_2 > 0} \exists_{n_0 \in \mathbb{N}} \forall_{n > n_0} c_1|g(n)| \leq |f(n)| \leq c_2|g(n)|.$$

Note-se que, de acordo com esta definição, $f(n) = \Theta(g(n))$ se e só se $f(n) = \Theta(g(n))$ e $f(n) = \Omega(g(n))$.

Exemplo A.10. *Vamos mostrar que $\log n! = \Theta(n \log n)$, onde o logaritmo log tem base $a > 1$.*

Solução. Uma vez que a função \log é monótona crescente, verifica-se que para todo $n \in \mathbb{N}$

$$\log n! = \log 1 + \log 2 + \dots + \log n \leq n \log n,$$

e, consequentemente, $\log n! = \mathcal{O}(n \log n)$. Por outro lado, observando a Figura A.1, podemos concluir que a soma de todos os rectângulos é igual ao somatório $\sum_{k=1}^n \log k$ e a área limitada inferiormente pelo eixo horizontal e superiormente pela curva (gráfico da função $\log(x)$) vem dada por $\int_1^n \log x dx$. Logo,

$$\begin{aligned} \log n! &= \log 1 + \log 2 + \dots + \log n \geq \\ &\geq \int_1^n \log x dx = \left. \frac{x \ln x - x}{\ln 2} \right|_1^n = n \log n - (n-1) \log e \end{aligned}$$

e uma vez que $\frac{1}{2}n \log n \geq (n-1) \log e$ (para n suficientemente grande), obtém-se $n \log n - (n-1) \log e \geq \frac{1}{2}n \log n$ e, consequentemente, $\log n! = \Omega(n \log n)$. Note-se que a solução deste exemplo pode também ser obtida com recurso à desigualdades de Stirling (ver Teorema 6.1). \square

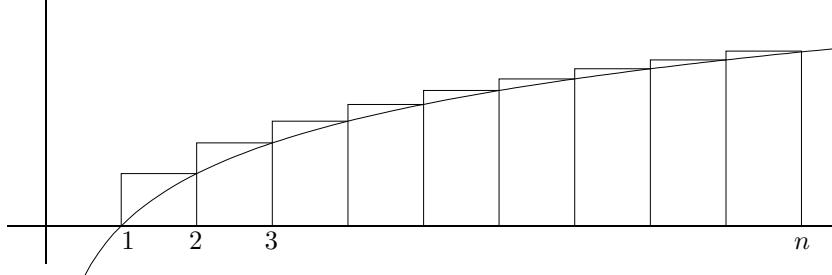


Figura A.1: Aproximação de $\sum_{k=1}^n \log k$.

Definição A.5 (Notação assimptótica \sim). *Dadas duas funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, diz-se que a função $f(n)$ é assimptoticamente (ou aproximadamente) igual à função $g(n)$ (quando $n \rightarrow \infty$) e escreve-se $f(n) \sim g(n)$ se e só se*

$$\forall \varepsilon > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n > n_0 \quad (1 - \varepsilon)g(n) \leq f(n) \leq (1 + \varepsilon)g(n).$$

Exemplo A.11. Vamos mostrar que para qualquer par de funções $f, g, h : \mathbb{N} \rightarrow \mathbb{R}$ se verifica:

- (a) $f(n) \sim f(n)$ (isto é, a relação \sim é reflexiva);
- (b) se $f(n) \sim g(n)$, então $g(n) \sim f(n)$ (isto é, a relação \sim é simétrica);
- (c) se $f(n) \sim g(n)$ e $g(n) \sim h(n)$, então $f(n) \sim h(n)$ (isto é, a relação \sim é transitiva⁴);
- (d) se $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)}$ existe, então $f(n) \sim g(n)$ se e só se $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$.

Solução.

- (a) Uma vez que $(1 - \varepsilon)f(n) \leq f(n) \leq (1 + \varepsilon)f(n)$ se verifica para todo $\varepsilon \in (0, 1)$ e todo $n \in \mathbb{N}$, então $f(n) \sim f(n)$.

⁴ As propriedades (a)-(c) garantem que relação \sim é uma relação de equivalência.

- (b) Se $f(n) \sim g(n)$, então para qualquer $\varepsilon > 0$ e n suficientemente grande, $(1 - \varepsilon)g(n) \leq f(n) \leq (1 + \varepsilon)g(n)$, o que é equivalente a $\frac{1}{1+\varepsilon}f(n) \leq g(n) \leq \frac{1}{1-\varepsilon}f(n)$. Escolhendo η como sendo o menor de entre $1 - \eta = \frac{1}{1+\varepsilon}$ e $1 + \eta = \frac{1}{1-\varepsilon}$, obtém-se $(1 - \eta)g(n) \leq f(n) \leq (1 + \eta)g(n)$. Logo, uma vez que para todo $\eta > 0$ existe ε para o qual as desigualdades anteriores se verificam, $g(n) \sim f(n)$.
- (c) Assumindo que se verificam as relações $f(n) \sim g(n)$ e $g(n) \sim h(n)$, podemos concluir que, para $\varepsilon, \eta > 0$, $(1 - \varepsilon)g(n) \leq f(n) \leq (1 + \varepsilon)g(n)$ e $(1 - \eta)h(n) \leq g(n) \leq (1 + \eta)h(n)$. Consequentemente,

$$\begin{aligned} f(n) &\leq (1 + \varepsilon)g(n) \leq (1 + \varepsilon)(1 + \eta)h(n) \leq (1 + \xi)h(n) \\ f(n) &\geq (1 - \varepsilon)g(n) \geq (1 - \varepsilon)(1 - \eta)h(n) \geq (1 - \xi)h(n) \end{aligned}$$

onde $\xi = \varepsilon + \eta + \varepsilon\eta$. Uma vez que para qualquer $\xi > 0$ existem ε e η para os quais as desigualdades anteriores se verificam, $f(n) \sim h(n)$.

- (d) Se $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)}$ existe, então $f(n) \sim g(n)$ é equivalente às desigualdades

$$-\varepsilon \leq \frac{f(n)}{g(n)} - 1 \leq \varepsilon$$

que são válidas para qualquer $\varepsilon > 0$. Logo, $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$. □

Exemplo A.12. Vamos mostrar que $f(n) \sim g(n)$ se e só se $f(n) = g(n)(1 + o(1))$.

Solução. Em primeiro lugar, deve observar-se que $f(n) = g(n)(1 + o(1))$ é equivalente a $f(n) - g(n) = o(g(n))$, uma vez que $g(n)o(1) = o(g(n))$.

Escrever $f(n) \sim g(n)$ é equivalente a afirmar que para qualquer $\varepsilon > 0$ e n suficientemente grande se verificam as desigualdades $(1 - \varepsilon)g(n) \leq f(n) \leq (1 + \varepsilon)g(n)$ o que, por sua vez, é equivalente a $-\varepsilon g(n) \leq f(n) - g(n) \leq \varepsilon g(n)$, ou seja, $|f(n) - g(n)| \leq \varepsilon |g(n)|$. A última desigualdade obtida significa precisamente que $f(n) - g(n) = o(g(n))$. □

Para sintetizar, na Tabela A.1 indica-se a existência ou não das diferentes relações assimptóticas, para um par de funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$, para o qual $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$ existe e $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = c$.

	$c = 0$	$c \in (0, 1)$	$c = 1$	$c \in (1, \infty)$	$c = \infty$
$f(n) = \Theta(g(n))$	sim	sim	sim	sim	não
$f(n) = \Omega(g(n))$	não	sim	sim	sim	sim
$f(n) = \Theta(g(n))$	não	sim	sim	sim	não
$f(n) \sim g(n)$	não	não	sim	não	não
$f(n) = o(g(n))$	sim	não	não	não	não
$f(n) = \omega(g(n))$	não	não	não	não	sim

Tabela A.1: Existência das diferentes relações assimptóticas

A.4. Teorema da recorrência universal

Uma estratégia muito comum no desenvolvimento de algoritmos, consiste em dividir o problema inicial em subproblemas de menor dimensão, cujos resultados são adequadamente combinados para se obter o resultado final (são exemplos deste tipo de algoritmos, os que se designam em língua inglesa por *divide and conquer*). A análise destes algoritmos conduz-nos a equações de recorrência particulares, cujos métodos de resolução vamos estudar. Com este objectivo, vamos começar com um exemplo simples.

Exemplo A.13. Suponha que a solução de um problema de tamanho n se obtém resolvendo dois problemas de tamanhos $\lfloor \frac{n}{2} \rfloor$ e $\lceil \frac{n}{2} \rceil$, respectivamente, e que posteriormente quando se combinam os resultados obtidos (para se determinar o resultado do problema original) isso tem um custo αn , onde α é uma constante. Assumindo que a solução deste problema, mas com tamanho 1, tem um custo fixo β . O custo $t(n)$ necessário para resolver o problema verifica a equação de recorrência

$$t(n) = t\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + t\left(\left\lceil \frac{n}{2} \right\rceil\right) + \alpha n, \quad t(1) = \beta.$$

Vamos analisar esta equação.

Solução. Sendo $n = 2^k$ e assumindo que k é inteiro, se $a_k = t(2^k)$, então podemos rescrever a equação de recorrência na forma

$$a_k = 2a_{k-1} + \alpha 2^k, \quad a_0 = \beta. \quad (\text{A.1})$$

A última equação obtida, trata-se de uma equação de recorrência linear que pode ser resolvida utilizando os métodos do Capítulo 5. Uma vez que a equação característica associada tem raiz 2, a solução da equação homogénea é da forma $a_k^{(1)} = c2^k$. Porém, dado que 2 é também a base da potência existente no lado direito da equação, a solução particular desta equação toma a forma $a_k^{(2)} = Ck2^k$, sendo fácil determinar $C = \alpha$. Logo, a solução geral da equação (A.1) vem dada por $a_k = c2^k + \alpha k2^k$ e, a partir de condição inicial, obtém-se $c = \beta$. Como consequência,

$$a_k = \beta 2^k + \alpha k 2^k.$$

Voltando à notação inicial, para $n = 2^k$, vem que

$$t(n) = \beta n + \alpha n \log_2 n. \quad (\text{A.2})$$

□

Note-se que a expressão (A.2) é a solução da equação de recorrência do Exemplo A.13, apenas para valores de n que são potências de 2. Para os restantes valores de n , podemos afirmar que a solução tem ordem não inferior a $n \log n$, ou seja,

$$t(n) = \Theta(n \log n).$$

Esta última igualdade é consequência da monotonicidade de t (o que se pode demonstrar por indução), da suavidade da função $n \log_2 n$, e de alguns resultados de análise matemática. O teorema a seguir, cuja demonstração se pode encontrar em [28], generaliza este resultado.

Teorema A.1 (da recorrência universal). *Para $\alpha \geq 0$, $\beta > 0$, $n \in \mathbb{N}$ e $f : \mathbb{N} \rightarrow \mathbb{R}_+$, seja*

$$t(n) = \begin{cases} \alpha t\left(\frac{n}{\beta}\right) + f(n), & \text{se } n \geq \beta, \\ \Theta(1), & \text{se } n = 1, 2, \dots, \beta - 1. \end{cases}$$

Nestas condições,

- se $f(n) = \mathcal{O}(n^{\log_\beta \alpha - \varepsilon})$ (onde $\varepsilon > 0$), então $t(n) = \Theta(n^{\log_\beta \alpha})$;
- se $f(n) = \Theta(n^{\log_\beta \alpha})$, então $t(n) = \Theta(n^{\log_\beta \alpha} \log n)$;
- se $f(n) = \mathcal{O}(n^{\log_\beta \alpha + \varepsilon})$ e $\alpha f\left(\frac{n}{\beta}\right) \leq cf(n)$ (onde $\varepsilon > 0$ e $0 < c < 1$), então $t(n) = \Theta(f(n))$.

O teorema da recorrência universal só é valido nos casos em que n é dividido em partes iguais. No caso mais geral, o teorema de Akra-Bazzi é uma ferramenta mais poderosa para análise de algoritmos deste tipo.

Teorema A.2 (Akra-Bazzi). *Dada uma constante $k \in \mathbb{N}$, sejam $a_i \geq 0$ e $b_i \in (0, 1)$ ($i = 1, 2, \dots, k$) constantes, $f : \mathbb{N} \rightarrow \mathbb{R}_+$, $f'(x) = \mathcal{O}(x^c)$ (onde f' denota a derivada de f e c é uma constante), $h_i(n) = \mathcal{O}\left(\frac{n}{\log^2 n}\right)$ e*

$$t(n) = \begin{cases} \sum_{i=1}^k a_i t(b_i n + h_i(n)) + f(n), & \text{se } n \geq n_0, \\ \Theta(1), & \text{se } n = 1, 2, \dots, n_0 - 1. \end{cases}$$

Então

$$t(n) = \Theta\left(n^p \left(1 + \int_1^n \frac{f(x)}{x^{p+1}} dx\right)\right),$$

onde p é definido pela equação $\sum_{i=1}^k a_i b_i^p = 1$.

Note-se que sendo o argumento de t , $\lfloor b_i n \rfloor$, ou seja, assumindo que pretendemos determinar $t(\lfloor b_i n \rfloor)$, fazendo $\lfloor b_i n \rfloor = b_i n + h_i(n)$, vem que $h_i(n) \in [0, 1)$ e, consequentemente, $h_i(n) = \mathcal{O}(1) = \mathcal{O}\left(\frac{n}{\log^2 n}\right)$. Logo, nestas condições, $h_i(n)$ verifica a hipótese do teorema de Akra-Bazzi. Adicionalmente, deve observar-se que $h_i(n)$ é negligenciável relativamente a $b_i n$.

Exemplo A.14. Vamos determinar uma solução assintótica da seguinte equação de recorrência:

$$t(n) = \frac{1}{2}t\left(\left\lfloor \frac{1}{4}n \right\rfloor\right) + \frac{1}{2}t\left(\left\lceil \frac{3}{4}n \right\rceil\right) + n^2$$

Solução. Neste caso, utilizando a notação do teorema de Akra-Bazzi, vem que $k = 2$, $a_1 = a_2 = \frac{1}{2}$, $b_1 = \frac{1}{4}$, $b_2 = \frac{3}{4}$, $h_1(n) = \frac{1}{4}n - \lfloor \frac{1}{4}n \rfloor = \mathcal{O}(1)$, $h_2(n) = \frac{3}{4}n - \lceil \frac{3}{4}n \rceil = \mathcal{O}(1)$, $f(n) = n^2$, $f'(n) = 2n = \mathcal{O}(n)$ e, finalmente, p vem definido por

$$\frac{1}{2}\left(\frac{1}{4}\right)^p + \frac{1}{2}\left(\frac{3}{4}\right)^p = 1$$

(devendo observar-se que, de acordo com esta equação, $p = 0$). Assim, calculando

$$\int_1^n \frac{f(x)}{x^{p+1}} dx = \int_1^n \frac{x^2}{x} dx = \frac{1}{2}n^2 - \frac{1}{2},$$

obtém-se

$$t(n) = \Theta\left(n^0 \left(1 + \frac{1}{2}n^2 - \frac{1}{2}\right)\right) = \Theta(n^2).$$

□

A.5. Exercícios

A.1. Determine qual ou quais das seguintes expressões assintóticas se verifica(m).

- (a) $2^{n+1} = \mathcal{O}(2^n)$,
- (b) $(n+1)! = \mathcal{O}(n!)$,
- (c) qualquer que seja a função $f : \mathbb{N} \rightarrow \mathbb{R}$, $f(n) = \mathcal{O}(n) \Rightarrow (f(n))^2 = \mathcal{O}(n^2)$,
- (c) qualquer que seja a função $f : \mathbb{N} \rightarrow \mathbb{R}$, $f(n) = \mathcal{O}(n) \Rightarrow 2^{f(n)} = \mathcal{O}(2^n)$.

A.2. Mostre que a relação assintótica definida por \mathcal{O} é transitiva, isto é

$$\text{se } f(n) = \mathcal{O}(g(n)) \text{ e } g(n) = \mathcal{O}(h(n)) \text{ então } f(n) = \mathcal{O}(h(n)).$$

- A.3. Sejam f_1, f_2, g_1, g_2 funções positivas (isto é, $f_1, f_2, g_1, g_2 : \mathbb{N} \rightarrow \mathbb{R}_+$) e suponha que \diamond denota uma das operações $+, -, \cdot, /$. Mostre que a proposição

| se $f_1(n) = \mathcal{O}(g_1(n))$ e $f_2(n) = \mathcal{O}(g_2(n))$, então $f_1(n) \diamond f_2(n) = \mathcal{O}(g_1(n) \diamond g_2(n))$
é verdadeira para $\diamond \in \{+, \cdot\}$ e é falsa para $\diamond \in \{-, /\}$.

- A.4. Com a notação assimptótica definida por \mathcal{O} ordene (por exemplo, $\mathcal{O}\left(\frac{1}{n}\right) = \mathcal{O}(1) = \mathcal{O}(n) = \mathcal{O}(n^2)$) as seguintes funções:

$$\frac{n}{\ln n}, n^{1+\varepsilon}, (1+\varepsilon)^n, \ln n, (n + \ln^2 n)^5,$$

onde $0 < \varepsilon < 1$.

- A.5. Mostre que para quaisquer constantes $a, b > 1$ a relação assimptótica $\log_a n = \Theta(\log_b n)$ se verifica.

- A.6. Mostre que para qualquer $k \in \mathbb{N}$ se verifica a seguinte relação assimptótica⁵

$$\sum_{i=1}^n i^k = \Theta(n^{k+1}).$$

- A.7. Mostre que $2^n = o(n!) = o(n^n)$.

- A.8. Escolha a notação assimptótica $f(n) = \mathcal{X}(g(n))$, para os pares de funções a seguir indicados, substituindo \mathcal{X} pelo símbolo assimptótico adequado de forma que a respectiva relação assimptótica seja verdadeira.

- (a) $f(n) = n$ e $g(n) = 2n$;
- (b) $f(n) = n \ln n$ e $g(n) = \frac{n^2}{\ln n}$;
- (c) $f(n) = (n+1)!$ e $g(n) = n!$
- (d) $f(n) = \binom{2n}{n}$ e $g(n) = 4^n$;
- (e) $f(n) = \mathcal{O}(n)$ e $g(n) = (f(n))^2$.

- A.9. Para cada uma das relações assimptóticas a seguir explicitadas, mostre que é verdadeira para todo o par de funções $f, g : \mathbb{N} \rightarrow \mathbb{R}$ ou mostre que é falsa para qualquer par destas funções ou apresente um exemplo para o qual a relação é verdadeira e um exemplo para o qual ela é falsa.

- (a) $f(n) = \mathcal{O}((f(n))^2)$;
- (b) $f(n) = o(g(n))$ e $f(n) = \Omega(g(n))$;
- (c) $f(n) \neq \mathcal{O}(g(n))$ e $g(n) \neq \mathcal{O}(f(n))$;
- (d) $f(n) = \Omega(g(n))$ e $f(n) = \omega(g(n))$;
- (e) $f(n) = \mathcal{O}(2^{\ln f(n)})$.

- A.10. Demonstre as seguintes relações assimptóticas:

- (a) $2^{2n} = \mathcal{O}(5^n)$;
- (b) $n + \sqrt{n} = \mathcal{O}(n)$;
- (c) $n^k 2^n = \mathcal{O}(4^n)$ onde $k \in \mathbb{N}$ é uma constante.

⁵ Esta propriedade também se verifica para todos os valores reais de k tais que $k > -1$.

A.11. Melhore o resultado do Exemplo A.10 de forma a obter a igualdade assimptótica $\ln n! \sim n \ln n$.

A.12. Sendo $f, g : \mathbb{N} \rightarrow \mathbb{R}_+$ duas funções positivas, demonstre as seguintes proposições verdadeiras:

- (a) $f(n) = \Theta(g(n))$ se e só se $\ln f(n) = \ln g(n) + \mathcal{O}(1)$;
- (b) se $f(n) = \Theta(g(n))$, então não necessariamente $\ln f(n) = \mathcal{O}(\ln g(n))$;
- (c) se $f(n) = \Theta(g(n))$ e $g(n) \rightarrow \infty$, então $\ln f(n) \sim \ln g(n)$.

A.13. Utilizando teorema de Stirling, demonstre a seguinte fórmula de Stirling:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e} \right)^n.$$

A.14. Assumindo $t(1) = 1$, determine uma solução assimptótica para cada um das seguintes equações de recorrência:

- (a) $t(n) = t(\lfloor \frac{n}{2} \rfloor) + n$;
- (b) $t(n) = 2t(\lfloor \frac{n}{2} \rfloor) + n$;
- (c) $t(n) = 3t(\lfloor \frac{n}{2} \rfloor) + n$;
- (d) $t(n) = t(\lfloor \frac{n}{3} \rfloor) + t(\lfloor \frac{n}{2} \rfloor) + n$;
- (e) $t(n) = t(\frac{n}{3}) + n \ln n$;
- (f) $t(n) = 3t(\frac{n}{5}) + \ln^2 n$;

B

Notação

Símbolo	Significado	Página
\mathbb{N}	Conjunto dos números naturais; $\mathbb{N} = \{1, 2, \dots\}$	6
\mathbb{N}_0	Conjunto dos números inteiros não negativos; $\mathbb{N}_0 = \{0, 1, 2, \dots\}$	27
\mathbb{Z}	Conjunto dos números inteiros	6
\mathbb{Q}	Conjunto dos números racionais	6
\mathbb{R}	Conjunto dos números reais	6
\mathbb{B}	Conjunto dos algarismos binários; $\mathbb{B} = \{0, 1\}$	57
$[n]$	Conjunto dos números naturais não superiores a n ; $[n] = \{1, 2, \dots, n\}$	27
\emptyset	Conjunto vazio	6
$\mathcal{P}(A)$	Conjunto das partes do conjunto A	18
$x \in A$	x pertence ao conjunto A	6
$A \subseteq B$	A está contido em B	6
$A \subset B$	A está contido em B e $A \neq B$ (também se utiliza a notação $A \subsetneq B$)	6
$A \cup B$	União dos conjuntos A e B	12
$A \cap B$	Intersecção dos conjuntos A e B	12
$A \setminus B$	Diferença entre os conjuntos A e B	12
$A \Delta B$	Diferença simétrica entre os conjuntos A e B	12
A^c	Complementar do conjunto A	12
$ A $	Cardinalidade do conjunto A	26
$\neg p$	Negação da proposição p : "não p "	9
$p \vee q$	Disjunção das proposições p e q : " p ou q "	9
$p \wedge q$	Conjunção das proposições p e q : " p e q "	9
$p \Rightarrow q$	Implicação, " p implica q "	8
$p \Leftrightarrow q$	Equivalência das proposições p e q : " p se e só se q "	9
$p \dot{\vee} q$	Ou exclusivo das proposições p e q : " p ou q mas não ambos"	278
$p \dot{\wedge} q$	Não-ou ("nor") das proposições p e q	278
$p \bar{\wedge} q$	Não-e ("nand") das proposições p e q	278
$\lfloor x \rfloor$	O maior número inteiro não superior a x , para $x \in \mathbb{R}$	49
$\lceil x \rceil$	O menor número inteiro não inferior a x , para $x \in \mathbb{R}$	92
$n!$	Factorial de n ; $n! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1$	41
$n!!$	Factorial duplo de n ; $n!! = n(n-2)(n-4) \cdots$	128
$(n)_k$	Coeficiente factorial; $(n)_k = n(n-1)(n-2) \cdots (n-k+1)$	72

Símbolo	Significado	Página
$\binom{n}{k}$	Número binomial; $\binom{n}{k} = \frac{(n)_k}{k!}$	72
$\binom{n}{t_1, \dots, t_r}$	Número multinomial; $\binom{n}{t_1, \dots, t_r} = \frac{n!}{t_1! t_2! \dots t_r!}$	78
$[n]_k$	Número de Stirling de primeira espécie	136
$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$	Número de Stirling de segunda espécie	138
$\langle n \rangle_k$	Número de Euler de primeira ordem	141
$\langle \rangle_k$	Número de Euler de segunda ordem	141
B_n	Número de Bell, para $n \in \mathbb{N}$	107
C_n	Número de Catalan, para $n \in \mathbb{N}$	146
F_n	Número de Fibonacci, para $n \in \mathbb{N}$	98
L_n	Número de Lucas, para $n \in \mathbb{N}$	134
Φ	Número de ouro	134
$\downarrow A$	Menor subconjunto inferior que contém A , $\{y \in X : \exists_{a \in A} y \preceq a\}$	161
$\uparrow A$	Menor subconjunto superior que contém A , $\{y \in X : \exists_{a \in A} a \preceq y\}$	161
$x \wedge y$	Ínfimo de x e y	156
$x \vee y$	Supremo de x e y	156
\overline{X}	Fecho de X	172
$\dim(P)$	Dimensão do cpo P	188
$\mathcal{I}(X)$	Conjunto dos subconjuntos inferiores de X	161
$\mathcal{J}(X)$	Conjunto dos elementos irredutíveis de X	170
$\inf A$	Ínfimo do conjunto A	156
$\sup A$	Supremo do conjunto A	156
V_x	Vizinhança mínima de x	172
$d n$	d divide n	19
D_n^*	Conjunto dos divisores de n	201
D_n	Conjunto dos divisores positivos de n ; também utilizada para Grupo diedral	19 319
$\text{mdc}(n, m)$	Máximo divisor comum entre m e n	201
$\text{mmc}(n, m)$	Mínimo múltiplo comum entre m e n	201
\mathbb{Z}_m	Conjunto dos inteiros módulo m	209
$\varphi(n)$	Função de Euler	204
$\mu(n)$	Função de Möbius (clássica)	207
$\mu(x, y)$	Função de Möbius (no contexto dos cpos)	190
\sqcup	Soma da álgebra de Boole	273
\sqcap	Produto da álgebra de Boole	273
$'$	Complementação da álgebra de Boole	273
\sqsubseteq	Relação de ordem parcial definida numa álgebra de Boole	285
\succeq	Relação de ordem parcial definida nos n -uplos binários, menores de grafos, etc.	158
A_G	Matriz de adjacência do grafo G	332
$E(G)$	Conjunto das arestas (dos arcos) do grafo (digrafo) G	329
$G[\widehat{E}]$	Subgrafo induzido pelas arestas \widehat{E} ($\widehat{E} \subset E(G)$)	340
$G[\widehat{V}]$	Subgrafo induzido pelos vértices \widehat{V} ($\widehat{V} \subset V(G)$)	339
K_n	Grafo completo com n vértices	339
$K_{n,m}$	Grafo bipartido completo	340
$L(G)$	Grafo linha do grafo G	492

Símbolo	Significado	Página
M_G	Matriz de incidência do grafo G	332
$V(G)$	Conjunto dos vértices do grafo G	329
$d_G(v)$	Grau do vértice v relativamente ao grafo G	331
$\text{diam}(G)$	Diâmetro do grafo G	379
$g(G)$	Cintura do grafo G	338
g_G	Genus do grafo G	548
$F_g(G)$	Conjunto das faces de uma realização celular do grafo G numa superfície de genus g	550
$e_G(v)$	Excentricidade do vértice v relativamente ao grafo G	379
$r(G)$	Raio de um grafo G	379
G/e	Contracção da aresta e no grafo G	404
$G//e$	Fusão de extremos da aresta e no grafo G	404
$G - e$	Eliminação da aresta e do grafo G	340
\cong	Isomorfismo entre grafos	335
$\alpha(G)$	Número de independência (ou de estabilidade) do grafo G	507
$\beta(G)$	Número de cobertura do grafo G	455
$N_G(v)$	Conjunto dos vértices adjacentes ao vértice v do grafo G	330
$\Delta(G)$	Máximo grau dos vértices do grafo G	331
$\delta(G)$	Mínimo grau dos vértices do grafo G	331
$\varepsilon(G)$	Número de arestas (arcos) do grafo (digrafo) G (isto é, $\varepsilon(G) = E(G) $)	331
$\nu(G)$	Número de vértices do grafo G (isto é, $\nu(G) = V(G) $)	331
$\tau(G)$	Número de árvores abrangentes do grafo G	404
ψ_G	Função de incidência aresta vértice do grafo G	329
$\chi(G)$	Número cromático do grafo G	512
$f(G, \lambda)$	Polinómio cromático do grafo G	522
\mathcal{G}_κ	Conjunto das κ -contracções do grafo G	527
$f_\kappa(G, \lambda)$	Polinómio das extensões cromáticas de κ em G	529
$\mathcal{K}_{W, \lambda}$	Conjunto de todas as colorações parciais $\kappa : W \rightarrow \{1, \dots, \lambda\}$	530
$\chi'(G)$	Índice cromático do grafo G	533
$\omega(G)$	Número de clique do grafo G	510
G^*	Dual (ou dual geométrico) do grafo planar G	559
G^{cb}	Dual combinatório do grafo G	561
\mathcal{O}	Notação assimptótica "O-grande"	585
Ω	Notação assimptótica Ω	589
Θ	Notação assimptótica Θ	589
o	Notação assimptótica "o-pequeno"	588
ω	Notação assimptótica ω	589
\sim	Notação assimptótica \sim	590

Bibliografia

- [1] M. Abramowitz e I. A. Stegun (eds.), *Handbook of mathematical functions, with formulas, graphs, and mathematical tables*, Dover, 1972.
- [2] M. Aigner, *Discrete mathematics*, American Mathematical Society, 2000.
- [3] I. Anderson, *A first course in discrete mathematics*, Springer, SUMS, 2001.
- [4] K. Appel e W. Haken, *Every planar map is four colorable, part i: Discharging*, Illinois J. Math. **21** (1977), 429–490.
- [5] ———, *Every planar map is four colorable, part ii: Reducibility*, Illinois J. Math. **21** (1977), 491–567.
- [6] M. A. Armstrong, *Basic topology*, 5a ed., Springer, New York, 1997.
- [7] L. M. Batten, *Combinatorics of finite geometries*, Cambridge University Press, 1997.
- [8] J. Battle, F. Harary, Y. Kodama e J. W. T. Youngs, *Additivity of the genus of a graph*, Bull. Amer. Math. Soc. **68** (1962), 565–568.
- [9] L. W. Beineke e R. J. Wilson (eds.), *Graph connections - relationships between graph theory and other areas of mathematics*, Clarendon Press, 1997.
- [10] C. Berge, *Graphs and hypergraphs*, North-Holland, 1991.
- [11] A. Bernhart, *Six rings in minimal five color maps*, Am. J. Math. **69** (1947), 391–412.
- [12] N. L. Biggs, *Discrete mathematics*, 2a ed., Oxford University Press, 2002.
- [13] G. D. Birkhoff, *The reducibility of maps*, Am. J. Math **35** (1913), 115–128.
- [14] G. D. Birkhoff e D. Lewis, *Chromatic polynomials*, Trans. Amer. Math. Soc. **60** (1946), 355–451.
- [15] M. Bóna, *A walk through combinatorics, an introduction to enumeration and graph theory*, World Scientific, 2002.
- [16] B. Bollobás, *Graph theory - an introductory course*, Springer, 1979.
- [17] ———, *Modern graph theory*, Springer, 1998.
- [18] R. L. Brooks, *On colouring the nodes of a network*, Proceedings of the Cambridge Philosophical Society **37** (1941), 194–197.
- [19] R. A. Brualdi, *Introductory combinatorics*, Prentice Hall, Inc., 2004.

- [20] F. S. Budnick, *Finite mathematics with applications*, McGraw-Hill, New York, 1985.
- [21] L. M. Butten, *Combinatorics of finite geometries*, Cambridge University Press, 1997.
- [22] P. J. Cameron, *Combinatorics - topics, techniques and algorithms*, Cambridge University Press, 1994.
- [23] D. M. Cardoso e D. A. Catalano, *Elementos de matemática*, Cadernos de Matemática da Universidade de Aveiro, CM 06/D-01, Aveiro, 2006.
- [24] P. Catlin, *Hajos' graph-coloring conjecture: variations and counterexamples*, J. of Combin. Theory, Ser. B **26** (1979), 268–274.
- [25] A. Cayley, *On the colouring of maps*, Proceedings of the Royal Geographical Society **1** (1879), 259–261.
- [26] L. Comtet, *Advanced combinatorics: The art of finite and infinite expansions*, Kluwer Academic Publishers, 1974.
- [27] J. H. Conway e R. K. Guy, *The book of numbers*, Springer-Verlag, 1974.
- [28] T. H. Cormen, C. E. Leiserson, R. L. Rivest e C. Stein, *Introduction to algorithms*, 2a ed., McGraw-Hill, 2001.
- [29] D. A. Davey e H. A. Priestley, *Introduction to lattice and order*, Cambridge University Press, 1994.
- [30] R. Diestel, *Graph theory*, Springer, 1997.
- [31] J. Dieudonné, *A formação da matemática contemporânea*, Publicações Dom Quixote, Lisboa, 1990.
- [32] G. A. Dirac, *A property of 4-chromatic graphs and some remarks on critical graphs*, J. of London Math. Soc. **27** (1952), 85–92.
- [33] P. Erdős, Chao Ko e R. Rado, *Extremal problem among subsets of a set*, Quart. J. Math. Oxford Ser. (2) **12** (1961), 313–318.
- [34] M. J. Erickson, *Introduction to combinatorics*, John Wiley & Sons, New York, 1999.
- [35] H. Eves, *Introdução à história da matemática*, Editora da Universidade Estadual de Campinas - UNICAMP, Campinas, 1997.
- [36] R. Loja Fernandes e M. Ricou, *Introdução à álgebra*, IST Press, Lisboa, 2004.
- [37] P. C. Fishburn, *Interval orders and interval graphs*, John Wiley & Sons, New York, 1985.
- [38] A. J. Franco de Oliveira, *Lógica e aritmética*, 2a ed., Gradiva – Publicações, Lda, 1991.
- [39] ———, *Geometria euclidiana*, Universidade Aberta, 1995.
- [40] M. Fréchet e K. Fan, *Invitation to combinatorial topology*, Dover Publications, Inc, 2003.
- [41] P. J. Freitas, *Topicos de Álgebra superior*, Univeridade de Lisboa, 2004.
- [42] R. Fritsch e G. Fritsch, *The four-color theorem: History, topological foundations, and idea of proof*, Springer, Lisboa, 1998.

- [43] A. Garcia e Y. Lequin, *Álgebra: um curso de introdução*, IMPA – Projeto Euclides, Livros Técnicos e Científicos Editora S.A., Rio de Janeiro, 1988.
- [44] L. J. Gerstein, *Introduction to mathematical structures and proofs*, Springer, New York, 2001.
- [45] P. C. Gilmore e A. J. Hoffman, *A characterization of comparability graphs and interval graphs*, Can. J. Math. **16** (1964), 539–548.
- [46] A. Gonçalves, *Introdução à álgebra*, IMPA – Projeto Euclides, Livros Técnicos e Científicos Editora S.A., Rio de Janeiro, 1979.
- [47] R. L. Graham, D. E. Knuth e O. Patashnik, *Concrete mathematics: A foundation for computer science*, 2a ed., Addison-Wesley, Reading, Massachusetts, 1994.
- [48] R. P. Grimaldi, *Discrete and combinatorial mathematics (an applied introduction)*, Addison-Wesley, Reading, Massachusetts, 1998.
- [49] Ya. E. Grinberg, *Plane homogeneous graphs of degree three without hamilton circuits*, Latvia Math. **4** (1968), 51–58.
- [50] B. Grünbaum, *Grötzsch's theorem on 3-colorings*, Michigan Math. J. **10** (1963), 303–310.
- [51] J. Gross e J. Yellen, *Graph theory and its applications*, CRC Press, 1999.
- [52] H. Grötzsch, *Ein Dreifarbensatz für Dreikreisfreie Netze auf der Kugel*, Halle-Wittenberg Math. Naturforsch. Reith **8** (1958), 108–119.
- [53] H. Hadwiger, *über eine klassifikation der streckenkomplexe*, Vierteljahrsschriften der Naturforschungsgesellschaft Zürich **88** (1943), 133–142.
- [54] G. Hajós, *über eine konstruktion nicht n-färbbarer graphen*, Wissenschaftliche Zeitschrift der Martin-Luther-Universität Halle-Wittenberg. Mathematisch-Naturwissenschaftliche Reihe **10** (1961), 116–117.
- [55] F. Harary, *Graph theory*, Addison-Wesley, Reading, 1969.
- [56] P. J. Heawood, *Map-color theorem*, Quart. J. Pure Appl. Math. **24** (1890), 332–338.
- [57] A. M. Herzberg e M. R. Murty, *Sudoku squares and chromatic polynomials*, Notices of the AMS **54** (2007), 708–717.
- [58] C. Jordan, *Calculus of finite differences*, 3a ed., Chelsea, New York, 1965.
- [59] A. B. Kempe, *On the geographical problem of the four colors*, American J. Math. **2** (1879), 193–200.
- [60] B. Kisačanin, *Mathematical problems and proofs: Combinatorics, number theory and geometry*, Plenum Press, New York, 1998.
- [61] D. E. Knuth, *The art of computer programming, vol. 1: Fundamental algorithms*, 3 ed., Addison-Wesley, Reading, Massachusetts, 1997.
- [62] D. L. Kreher e D. R. Stinson, *Combinatorial algorithms: Generation, enumeration, and search*, CRC Press, Boca Raton, 1999.
- [63] K. Kuratowski, *Sur le problème des courbes gauches en topologie*, Fundamenta Mathematicae **15** (1930), 271–283.

- [64] S. K. Lando, *Lectures on generating functions*, Student Mathematical Library, vol. 23, American Mathematical Society, 2003.
- [65] R. Lidl e G. Pilz, *Applied abstract algebra*, Springer, 1997.
- [66] E. L. Lima, *Espaços métricos*, IMPA, 1993.
- [67] L. Lovász, J. Pelikán e V. Vesztergombi, *Discrete mathematics: Elementary and beyond*, Springer, 2003.
- [68] L. Lovász, *Normal hypergraphs and the perfect graph conjecture*, Discrete Mathematics **2** (1972), 253–267.
- [69] ———, *Combinatorial problems and exercises*, North Holland, Amsterdam, 1979.
- [70] B. Mohar e C. Thomassen, *Graphs and surfaces*, John Hopkins University Press, 2001.
- [71] A. J. Monteiro e I. T. Matos, *Álgebra – um primeiro curso*, Escolar Editora, Lisboa Codex, 1995.
- [72] J. L. Mott, A. Kandel e T. P. Baker, *Discrete mathematics for computer scientists*, Reston Publishing Company, Inc., A Prentice-Hall Company, Reston, Virginia, 1983.
- [73] J. R. Munkres, *Topology*, Prentice Hall, Inc, 2000.
- [74] P. A. J. Oliveira, *O teorema de Fermat-Euler-Silva*, Boletim da SPM **45** (2001), 65–72.
- [75] M. T. F. Oliveira Martins, *Tópicos fundamentais de matemática*, Textos de Matemática, Série A, no. 3, Universidade de Coimbra, 1999.
- [76] K. R. Parthasarathy, *Basic graph theory*, McGraw-Hill, New Delhi, 1994.
- [77] J. Petersen, *Sur le théorème de Tait*, L'Intermédiaire des Mathématiciens **5** (1998), 225–227.
- [78] F. P. Ramsey, *On a problem of formal logic*, Proc. London Math. Soc. (1930), no. 30, 264–286.
- [79] G. Ringel e J. W. T. Youngs, *Solution of the Heawood map-coloring problem*, Proc. Nat. Acad. Sci. USA (1968), no. 60, 438–445.
- [80] J. Riordan, *Combinatorial identities*, John Wiley & Sons, New York, 1979.
- [81] ———, *An introduction to combinatorial analysis*, John Wiley & Sons, New York, 1980.
- [82] F. S. Roberts, *Applied combinatorics*, Prentice Hall, Inc, 1984.
- [83] N. Robertson, D. P. Sanders, P. D. Seymour e R. Thomas, *The four-colour theorem*, J. Comb. Theory B **70** (1994), 2–44.
- [84] N. Robertson e P. D. Seymour, *Graph theory*, 3rd ed., Springer, 2005.
- [85] N. Robertson, P. D. Seymour e R. Thomas, *Hadwiger's conjecture for K_5 -free graphs*, Combinatorica (1993), no. 13, 279–361.
- [86] ———, *Sachs' linkless embedding conjecture*, J. Comb. Theory B **64** (1995), 185–227.
- [87] S. Roman, *The umbral calculus*, Academic Press, 1984.
- [88] K. H. Rosen, *Exploring discrete mathematics with MAPLE*, International Editions, Mathematics & Statistics Series, McGraw-Hill, New York, 1997.

- [89] H. Sacchs, *On spatial representations of finite graphs, finite and infinite sets*, vol. 37, (A. Hajnal, L. Lovász and V. T. Sós, eds) Colloq. Math. Soc. János Bolyai, North-Holland, Budapest, 1984.
- [90] V. N. Sachkov, *Combinatorial methods in discrete mathematics*, Cambridge University Press, 1996.
- [91] ———, *Probabilistic methods in combinatorial analysis*, Cambridge University Press, 1997.
- [92] B. S. W. Schröder, *Ordered sets: an introduction*, Birkhäuser, 2002.
- [93] A. Shen e N. K. Vereshchagin, *Basic set theory*, Student Mathematical Library, vol. 17, American Mathematical Society, 2002.
- [94] J. M. S. Simões Pereira, *Matemática discreta: Tópicos de combinatória*, Editora Luz da Vida, 2006.
- [95] R. P. Stanley, *Enumerative combinatorics*, Cambridge Studies in Advanced Mathematics 49, vol. I, Cambridge University Press, 1997.
- [96] ———, *Enumerative combinatorics*, Cambridge Studies in Advanced Mathematics 62, vol. 2, Cambridge University Press, 1999.
- [97] W. T. Tutte, *How to draw a graph*, Proc. London Mathematica Society (1963), no. 13, 743–767.
- [98] J. H. van Lint e R. M. Wilson, *A course in combinatorics*, Cambridge University Press, 1994.
- [99] D. J. Velleman, *How to prove it: a structured approach*, Cambridge University Press, Cambridge, 1998.
- [100] E. B. Vinberg, *A course in algebra*, Graduate studies in mathematics, vol. 56, American Mathematical Society, 2003.
- [101] V. G. Vizing, *On an estimate of the chromatic class of a p-graph*, Metody Diskret. Analiz. **3** (1964), 25–30, (Russian).
- [102] K. Wagner, *Graphentheorie*, B. J. Hochscultaschenbucher 248/248a, Mammheim, 1870.
- [103] ———, *über eine eigenschaft der ebenen komplex*, Math. Ann. (1937), 570–590.
- [104] ———, *beweis einer abschwächung der hadwiger-vermutung*, Math. Ann. (1964), 139–141.
- [105] H. Whitney, *Non-separable and planar graphs*, Trans. Amer. Math. Soc. **34** (1932), 339–362.
- [106] ———, *Planar graph*, Fund. Math. **21** (1933), 73–84.
- [107] A. S. Wiitala, *Discrete mathematics – a unified approach*, McGraw-Hill, New York, 1987.
- [108] R. A. Wilson, *Graphs, colourins and the four-coulor theorem*, Oxford University Press, Oxford, 2002.
- [109] R. J. Wilson, *Introduction to graph theory*, Oliver and Boyd, Edinburgh, 1972.
- [110] A. A. Zykov, *On some properties of linear complexes (in russian)*, Mat. Sbornik N. S. (1949), 163–188, (tradução publicada em inglês em: AMS Translations Series I, Vol. 7, Algebraic Topology (1962) 418-449).

Índice

- aberto, 172–180
absorção, 163, 164, 271–277
adjacência, 335
alcance de um quantificador, 16
Alexandroff, Pavel Sergeevich, 172–175, 177, 179
alfabeto grego, 3
álgebra
 das funções booleanas, 290, 291
 das partes de um conjunto, *ver* álgebra de subconjuntos
 de Boole, 169, 271, 273–278, 285–290, 300, 301, 370, 518, 598
 infinita, 288, 301
de n -uplos binários, 274, 286, 287, 290
de subconjuntos, 271–273, 286, 287, 289, 300
dos valores lógicos, 271–274, 277, 278, 286, 300
algoritmo
 AHSTS, 244
 de Bellman-Ford, 393–396, 398, 432
 de coloração de vértices, 517
 de de la Loubere, 229, 230, 232
 de Dijkstra, 387–391, 393, 395, 396, 398, 432, 487
 de Edmonds e Johnson, 486, 488
 de Euclides, 202, 203
 de Fleury, 484–486
 de Floyd, 396
 de fluxo máximo, *ver* algoritmo de Ford-Fulkerson
 de Ford-Fulkerson, 428, 429, 432
 de fusão de vértices, 362, 364, 366
 de Gabow, 371
 de Hierholzer, 483, 484, 486
 de Horner, 214, 215
 de Kosaraju, 371
 de Kruskal, 413–417, 501
 de Kuhn-Munkres, 464, 466
 de Leifman, 371, 372, 374–376
 de Little, Marty, Sweeney e Karel, 497, 498
 de pesquisa
 em largura, 347, 349, 361, 371, 385
 em profundidade, 347, 348, 361
 de Prüfer, *ver* código de Prüfer
 de premiar e punir, 501
 de Prim, 413, 415–417, 421
 de Quine-McCluskey, 291
 de Tarjan, 371
 guloso, 413
 de coloração de vértices, 512
 simplex, 438
análise combinatória, 71
anel, 209, 210, 213, 216, 220, 234
 associativo, 215
 com elemento unidade, 214, 215
 comutativo, 209, 213, 215
 de polinómios, 224
anti-simetria, 163, 185, 286
anticadeia, 180–184, 186, 187, 189, 194, 195, 200, 552
aplicação, *ver* função
 de Frobenius, 217
Appel, Kenneth, 570, 573, 574
arco, 329, 332, 379
 não saturado, 425
 saturado, 425
arco-conexidade, 370
aresta, 329, 332, 333, 337, 339, 340, 360, 379, 548
 de corte, *ver* ponte
aresta-conexidade, 368
arestas
 adjacentes, 330
 paralelas, 330, 336, 339, 354, 364
arranjos
 com repetição, 71, 72
 sem repetição, *ver* arranjos simples

- simples, 72, 73, 75
 árvore, 401–409, 411–413, 418, 419
 abrangente, 403–407, 409–412, 414, 420
 de custo mínimo, 401, 413–418, 421
 binária, 421
 associatividade, 163, 209, 271–274, 276, 277, 287, 305, 306
 átomo, 170, 285–291, 301
 automorfismo, 336
 de um grupo, 306
 axioma, 4
 das paralelas, 5
 de separação T_0 , 172
 de separação T_1 , 172, 173
 axiomas, 4, 5
 da geometria, 245, 246, 249, 251, 258
 de Euclides, 4, 246
 de separação, 172, 173
 do plano afim, 246
 do plano projectivo, 246, 248
- Bachmann, Paul, 585
 base
 de uma álgebra de Boole, 273, 274, 277, 285, 286, 288
 de um espaço vectorial, 218
 de um sistema de numeração, 280, 281
 de uma topologia, 176–178
 fortemente admissível, 440
 irreduzível, 178
 mínima de uma topologia, 177
- Bell, Eric Temple, 107, 127, 144, 145
 Bellman, Richard, 393
 Berge, Claude, 449, 513
 Bernhart, Arthur, 574
 Bernstein, Felix, 30
 BFS, *ver* algoritmo de pesquisa em largura
 bijecção, 23–30, 34, 57–59, 68, 80, 105, 289, 306, 335, 336, 405
 binómio
 de Newton, 128
 bipartição, 342, 358, 361
 Birkhoff, David George, 522
 Birkhoff, Garret, 171
 bloco, 369
 de um design, 237–241, 243–245, 248, 249, 265–268
 de uma partição, 20, 21
 extremo, 369
 bola aberta, 547, 550
- Boole, George, 271–278, 285–290, 300, 301, 598
 breadth-first search, *ver* algoritmo de pesquisa em largura
 Brouwer, L.E.J., 32
 Burnside, William, 310
 cabeça, 330, 332
 cadeia, 180–184, 189, 194, 195, 200, 457–460, 552
 de Kempe, 573
 caixa preta, 282, 283
 cálculo
 proposicional, 10, 39, 40, 271, 276, 277
 caminho, 336, 357, 358, 379, 402, 404, 407, 506
 alternado, 449, 453, 455, 462, 466, 469–471, 475
 de aumento, 427, 449, 450, 460, 465–470, 473
 de Hamilton, 489, 494, 501, 505
 de peso mínimo, 498, 501
 fechado, *ver* ciclo
 mais curto, 379, 387, 388, 390
- Cantor, Georg, 26–29, 31
 capacidade, 423–425, 429, 432, 433, 437, 438, 442, 444, 445
 de um corte, 426–428, 431
- característica
 de Euler, 566
 de um corpo, 216–218
- cardinalidade, 26–28
 Catalan, Eugène Charles, 127, 145–150
 Cauchy, Augustin-Louis, 31, 83, 310
 cauda, 330, 332
 caule, 469
 Cayley, Arthur, 306, 401, 411, 569
 célula
 de um grafo, *ver* face de um grafo
- centro
 de um grafo, 379, 381
- Chebyshev, Pafnutiy, 45, 46, 338
- ciclo, 337, 381, 401, 402, 405–407, 409, 414, 415, 419
 de Hamilton, 480, 489, 490, 492–498, 500–502, 505, 506, 536, 570
 de peso mínimo, 497
 de uma permutação, 136–138
- cintura, 338, 381, 384, 385
- circuito, 337, 338, 340, 360
 com memória, 278
 combinatório, 278, 279, 285
 de Euler, 480–489, 492, 506
 lógico, 278–280, 282–285, 291, 301

- sequencial, 278
circunferência, 549
classe
 de equivalência, 20–22, 26, 357
 de grafos
 fechada para menores, 550, 553
lateral, 307, 308
 à direita, 307
 à esquerda, 307
clique, 510, 537
 máxima, 510, 511
cobertura
 por vértices, 455, 456, 510, 519, 543
 mínima, 455, 456, 477, 510, 519–521
código
 de Gray, 493–495
 de Morse, 133, 134
 de Prüfer, 411–413, 420
coeficiente factorial, 72
coloração
 de arestas, 533
 própria, 533
 de mapas, 511, 568
 de vértices, 511
 própria, 511
 parcial, 526, 528, 531, 532, 542
combinação linear, 218
combinações
 com repetição, 77, 78
 simples, 72, 74, 79, 88
complementar de um conjunto, 11, 12
complementaridade, 272–274, 276, 277, 287
complementação, 11, 12, 273, 598
componente, 357
 conexa, 357–362, 364, 365
 fortemente conexa, 370, 371, 374–376
composição
 de funções, 24, 25
 de relações, 24
comprimento
 de um caminho, 337, 352
 de um ciclo, 337, 338
 de um circuito, 338, 340
 de um cpo, 182, 183, 194, 195, 200
 de um passeio, 337
comutatividade, 163, 209, 271–274, 276, 277, 286
condição inicial
 da equação de recorrência, 94–104, 106–109,
 124–126
 de indução, 42–48
conexidade, 368, 370
conexão, 357, 369
 forte, 369
 fraca, 369
configuração redutível, 573
conjectura, 5
 de Wagner, 550
 de Goldbach, 5
 de Hadwiger, 576
 de Hajós, 578
conjugaçāo, 309
conjunção, 9–11, 42, 272, 277, 278, 291–293, 597
conjunto, 6, 7
 aberto, *ver* aberto
 centralizador, 309
 com repetição, 77, 78
 conexo, 549
 por arcos, 549
 contável, *ver* conjunto numerável
 das arestas, 329
 das faces, 550
 das partes, 18, 57, 65, 271, 597
 de chegada, 22
 de estacionaridade, 309
 de partida, 22
 de todas as colorações parciais, 530
 dos arcos, 329
 dos números inteiros, 6
 dos números naturais, 6
 dos números racionais, 6
 dos números reais, 6
 dos vértices, 329, 335, 357
enumerável, *ver* conjunto numerável
extremal, 194, 195
fechado, *ver* fechado
finito, 27, 49, 57
independente, 507–511, 517–521, 535, 537, 540,
 543, 544
 maximal, *ver* independente maximal
 máximo, *ver* independente máximo
inferior, 161, 170, 171, 183
infinito, 27
numerável, 28–30
parcialmente ordenado, 19, 155–162, 166, 168,
 174, 175, 177, 178, 180–189, 194, 197–
 200, 457–459, 517, 552
 das κ -contracções de um grafo, 527
potência, *ver* conjunto das partes
quociente, 21, 26
separador, 549

- superior, 161, 179, 183
 totalmente ordenado, 19, 181
 transversal, *ver sistema de representantes dis-tintos*
 universal, 6–8, 18
 vazio, 6, 18, 22, 28, 597
 conjuntos
 comparáveis, 156
 disjuntos, 62
 equipotentes, 26, 27, 29
 homeomorfos, 548, 549, 570
 iguais, 3, 6
 contracção
 de um grafo, 527
 de arestas, 404, 522, 527, 551
 contradição, 10, 11, 13, 27, 30, 32
 contradomínio, 22
 de função, 25
 de relação, 18
 corpo, 209, 210, 212, 213, 215–221, 235
 de decomposição, 221, 222
 de decomposição de um polinómio, 213, 214, 221, 222
 de Galois, 216, 219, 220, 222, 252, 254, 255, 259, 262, 268
 finito, 209, 212, 213, 216–218, 220, 222, 227
 corte, 425
 mínimo, 427, 428, 431, 445
 corte-uv, 425
 contra-exemplo minimal, 573
 cpo, *ver conjunto parcialmente ordenado*
 critério
 de Dantzig, 435
 de Eisenstein, 223, 224
 cubo, 342, 343, 493, 562
 curva, 548
 fechada de Jordan, 549, 572
 simples, 548, 549
 custo
 de um caminho, 379
 Daniel da Silva, 65, 67, 211
 Dantzig, George, 435
 De Morgan, Augustus, 39–41, 64, 277, 569
 Dedekind, Richard, 29, 31
 depth-first search, *ver algoritmo de pesquisa em profundidade*
 derivada formal de um polinómio, 221
 desencontros, 80, 106
 design, 237–239, 241–243, 245, 248, 249, 252, 265, 267–269
 1-design, 237–239, 241, 242, 267, 268
 2-design, 242, 243, 248, 249, 251, 256, 258, 266, 268, 269
 de Hadamard, 266
 simétrico, 242, 248, 249, 263, 266, 267, 270
 t-design, 241, 242
 desigualdade
 de Chebyshev, 45, 46, 338
 de Fischer, 242
 destino
 de uma rede, 423, 425, 426, 432, 433
 DFS, *ver algoritmo de pesquisa em profundidade*
 diagrama
 de Hasse, 156–167, 174–180, 185, 186, 198, 457
 de Venn, 11–13
 diamante de Birkhoff, 573, 574
 diâmetro
 de um grafo, 379–381, 384, 385, 391, 393, 399
 diferença
 de conjuntos, 11, 12
 simétrica, 11, 12
 dígito
 de transporte, 281, 282, 285
 digrafo, *ver grafo orientado*
 Dijkstra, Edsger W., 387
 Dilworth, Robert, 180, 182, 183, 200
 dimensão
 de Dushnik-Miller, 188
 de um cpo, 188
 de um espaço vectorial, 216, 218, 220, 221
 de um grafo, 331, 332, 343, 352, 353, 358
 Dirac, Gabriel Andrew, 491
 Dirichlet, J.P.G.L., 49
 disjunção, 9–11, 272, 277, 278, 291–293, 364, 597
 exclusiva, 278–280, 283, 597
 distância
 de Hamming, 508
 entre vértices, 337, 340, 379–383, 386, 388, 390–392, 399
 distributividade, 271–274, 276, 277, 287
 divisibilidade, *ver relação de divisibilidade*
 divisor, 156, 158, 160, 165, 201, 202, 204, 207, 215, 222–224, 300, 308
 comum, 201, 202, 204, 205, 210, 215, 223
 de zero, 215
 primo, 204
 dodecaedro, 480, 562, 563
 dominância, 272–277
 domínio, 22

- de função, 22, 23, 25
de integridade, 215
de relação, 18
euclidiano, 215
exterior, 549
interior, 549
dual, 559
combinatório, 559, 561
de um grafo planar, 559
geométrico, *ver* dual
duplicação
de uma aresta, 486
Dürer, Albrecht, 228
- e-não, *ver* incompatibilidade
Edmonds, Jack R., 464
Egerváry, Jenő, 456
Eisenstein, Ferdinand Gotthold, 223
elemento
invertível, 209–211, 227, 235
irreduzível, 170, 171, 179, 180, 199
maximal, 156, 161, 175, 181, 183, 184
minimal, 156, 157, 175, 177, 183, 184
mínimo, 170
neutro, 305, 309
nulo, 209, 235
unidade, 209, 213–215
elementos comparáveis, 155–157, 180–184, 186–188
eliminação
de arestas, 404, 522, 551
de vértices, 551
emparelhamento, 449, 450, 452, 453, 455, 460
máximo, 449, 450, 455, 456, 458, 460, 461, 464, 465, 468–473
perfeito, 449–454, 456, 461, 463–468, 473–478
de peso máximo, 463
de peso mínimo, 475
equação
característica, 96, 99, 101
de recorrência
homogénea, 95, 97–99, 101–103
homogénea associada, 108
linear não homogénea, 102–104, 108, 109
não linear, 106–109, 124
equipotência, 26
equivalecia, 9, 16, 278, 597
Erdős, Paul, 181, 346
esfera, 548
espaço
afim, 246
de Alexandroff, 173–175, 177
de Fréchet, 173
de Khalimsky, 177
de Kolmogorov, 173
euclidiano, 245, 548
projectivo, 237, 246, 254, 259, 260, 262
topológico, 171–180
topológico T_0 , 172–175, 177–179
topológico T_1 , 172–175
topológico finito, 171, 173–176
vectorial, 218, 220, 259–261
esquema de Horner, *ver* algoritmo de Horner
estabilizador, 309, 311
estável, *ver* conjunto independente
estrato de um conjunto, 474, 475
estrela, 361
estrutura
cíclica, 314, 316, 317
de incidência, 244, 245, 249, 251, 252, 258, 263
dual, 244
etiquetação, 335
de arestas, 335
de vértices, 335
Euclides, 4, 5, 31, 202, 246
Eudoxo de Cnido, 31
Euler, Leonhard, 31, 127, 141–144, 150, 204, 205, 210, 211, 226, 479, 482
excentricidade
de um vértice, 379–381, 386, 391, 393, 398, 399
expansão
de um grafo, 551
expressão
dual, 275, 287
equivalente, 10, 11
lógica, 9, 34
extensão
cromática, 526, 531, 532
de separação de um polinómio, 214
de um corpo, 210
de uma função, 25
linear, 184–187, 198, 200
extremo, *ver* vértice extremo de uma aresta
face, 568
de um grafo, 550
ilimitada, 553, 568
factorial, 127

- duplo, 128
- falso, 8
- família
 - de conjuntos, 14
 - de Petersen, 552, 553
 - de Sperner, 194
 - disjunta, 14, 15
 - dois a dois disjunta, 14, 15
 - intersectante, 195, 196, 200
- fechado, 172–180
- fecho
 - de um conjunto, 172, 176, 179
 - de um elemento, 172
- Fermat, Pierre, 71, 211, 217
- Fibonacci, 98, 127, 130–135, 150
- fila, 350
- Fischer, Ernst Sigismund, 242
- fita de Möbius, 548
- flor, 469, 470, 473
 - com caule, 469, 470, 475
- floresta, 401, 403, 407, 408, 410
 - abrangente, 406, 407, 409
- Floyd, Robert W., 396
- fluxo, 423, 424, 460
 - de custo mínimo, 432, 433, 437, 438, 440–442, 448
 - máximo, 423, 425, 427–432, 436, 445, 446, 460
- folha, 403, 411, 418
- Fontana, Niccollo, 71
- forma
 - conjuntiva, 300
 - disjuntiva
 - mínima, 291
 - reduzida, 292
 - reduzida mínima, 293, 518–521
 - mínima, 291
 - normal, 291
 - conjuntiva, 291
 - disjuntiva, 291, 294
- fórmula
 - bem formada, 10
 - da linguagem proposicional, 10
- binomial de Newton, 86
- da inversão de Möbius, 193
 - clássica, 208
- da linguagem proposicional, 10
- de Cauchy, 83
- de Daniel da Silva, 65, 67
- de Euler, 553–555, 560, 562, 565, 575, 580
 - generalizada, 565
- para grafos planos, 553
- segunda, 565
- de Heawood, 565
- de Stirling, 127, 595
- de Sylvester, 65
- multinomial, 86, 91
- Fraenkel, Abraham, 32
- Frege, Gottlob, 31
- Frobenius, Georg, 217, 310, 456
- função, 22
 - bijectiva, *ver* bijecção
 - booleana, 290, 291, 301, 518
 - monótona, 291–293, 518
 - continua, 178, 179
 - de capacidade, *ver* capacidade
 - de etiquetação, 463–468
 - de Euler, 204, 205, 210, 322
 - de incidência, 329
 - de Möbius, 190–192, 204, 207, 208
 - versão clássica, 207
 - de peso, 311
 - delta de Kronecker, 189
 - injectiva, 22–30, 34
 - inversa, 22, 26
 - isótona, 159, 161, 199
 - sobrejectiva, 23–28, 34, 58, 76
 - zeta de um cpo, 189
- funções iguais, 23
- fusão
 - de extremos de uma aresta, 404
 - de vértices, 362, 363
- Gallai, Tibor, 346, 510
- Gaston, Tarry, 226
- Gauss, Carl Friedrich, 43, 223
- genus, 564
 - de um grafo, *ver* genus, 581
 - de uma superfície, 548
- geometria, 245, 246, 249–251, 253
 - afim, 246, 258
 - euclidiana, 246
 - finita, 245
 - projectiva, 190, 246
- Gödel, Kurt, 5, 32, 33
- Goldbach, Christian, 5
- grafo, 329
 - autocomplementar, 335, 359
 - bem coberto, 508
 - bipartido, 340, 342, 352, 353, 452–458, 460, 461, 463–465, 468, 476–478

- completo, 340, 341, 463
com custos nas arestas, 387
com pesos nas arestas, 379, 486
complementar, 332, 335, 339
completo, 339, 341
conexo, 357–360, 362, 368, 382, 384, 402–406,
 409, 414, 416, 419, 506
cúbico, 339, 451, 536, 570
de Berge, 513
de comparabilidade, 457, 513
de Euler, 480–482, 484–489, 492, 493, 502,
 506
de Hamilton, 489–493, 506, 536
de Hamming, 508, 509
de Hoffman-Singleton, 385
de Kneser, 353, 385
de Moore, 385
de Petersen, 353, 385, 490, 552, 556, 570
de Turan, 419
desconexo, 357
do Sudoku, 531
dos blocos, 369
euleriano, *ver* grafo de Euler
factor-crítico, 477
finito, 331
fortemente conexo, 370
g-platônico, 567
hamiltoniano, *ver* grafo de Hamilton
infinito, 331
intervalar, 513
k-aresta-conexo, 368
k-conexo, 368
linha, 492, 493
mergulhável, *ver* grafo realizável
não etiquetado, 335
não orientado, 329, 333, 334
não-planar, 547, 555–557, 559, 564, 570, 576,
 577, 579, 580
nulo, 339
orientado, 329, 331, 334, 369–371, 374, 375
perfeito, 512
planar, 547, 550, 553, 554, 556, 558, 559, 564,
 568, 569, 572, 579, 580
planar-maximal, 555
plano, 547, 553, 559–561, 568, 572, 573
platônico, 562, 567
 não trivial, 563
realizável, 547, 551–553, 564, 565, 575
 na esfera, 547
 sem ciclos ligados, 552
sem nós, 552
regular, 339, 343, 352, 353, 381, 384, 453, 536
semi-euleriano, 480, 482
semi-hamiltoniano, 489
série-paralelo, 552
simples, 330, 335–339, 341–344, 349–351, 354,
 358, 360, 364
trivial, 331, 357, 359
grafos
 iguais, 331, 335
 isomorfos, 335, 336
 não isomorfos, 341, 342, 354
grau
 de um vértice, 331, 333, 335, 336, 339, 343,
 359, 371
 de uma face, 554
grelha, 58, 59, 74–76, 86–88, 91, 152
grupo, 225, 305, 307–309, 315
 abeliano, 209, 306
 cíclico, 307, 320, 322
 comutativo, 209, 210, 235
 de simetrias, 319
 diedral, 319–323
 finito, 305, 309, 311
 multiplicativo, 210, 221
 quociente, 308
 simétrico, 306
grupóide, 225
Guthrie, Francis, 569
Guthrie, Frederick, 569
Hadamard, Jacques, 263
Haken, Wolfgang, 570, 573, 574
Hall, Philip, 452
Hamilton, William Rowan, 479, 569
Hardy, Godfrey Harold, 586
Hasse, Helmut, 156–167, 174–180, 185, 186, 198
Heawood, 569
hexaedro, 562, 563
Hierholzer, Carl, 482
Hilbert, David, 32, 33
hipótese
 de indução, 42, 44–48
homomorfismo
 entre grupos, 306
Hopcroft, John, 347
Horner, William George, 214, 215
icosaedro, 562, 563
idempotência, 163, 276, 277, 286, 287
igualdade

- de grafos, 331
- imagem, 22
 - de função, 23
 - de relação, 18
 - recíproca, 22
 - de função, 23, 24
 - de relação, 18
- implicação, 7, 8, 12, 20, 35, 37, 39–42, 47, 48, 278
- incompatibilidade, 278, 302, 597
- independente
 - maximal, 507, 508, 517–521, 543
 - máximo, 507–511, 517
- índice
 - cromático, 533
 - cíclico, 314–320, 322, 323
 - de um subgrupo, 308
- ínfimo, 156, 157, 161–163, 165, 169, 170
- interior
 - de um conjunto, 172
- intersecção
 - de conjuntos, 11, 12, 14, 15, 62, 64, 271, 597
 - generalizada, 14, 15
 - não vazia, 11, 12, 21
- intervalo, 165, 173, 187, 189, 200
- isomorfismo
 - entre álgebras de Boole, 271, 289, 300
 - entre conjuntos parcialmente ordenados, 159–161
 - entre grafos, 335, 336, 339
 - entre grupos, 306, 307
 - entre reticulados, 166, 167, 171
- jogo solitário, 218, 219
- Jordan, Camille, 549
- König, Denes, 455
- Karnaugh, Maurice, 291
- k*-emparelhamento, 452
- Kempe, Alfred, 569, 570
- k*-factor, 452
- Khayyam, Omar, 87
- Kneser, Martin, 353
- Kuhn, Harold, 464
- lacete, 330–332, 336, 339, 354, 361, 364
- Landau, Edmund, 585
- largura
 - de um cpo, 182, 183, 189, 194, 200, 517
- lei
 - de contraposição, 11, 13, 39
 - de De Morgan, 10, 14, 39–41, 64, 277
- generalizada, 15
- do terceiro excluído, 32
- Leibnitz, Gottfried, 31
- Leifman, L. Ya., 371
- lema
 - da contracção de ciclos, 468, 469
 - de Burnside, 310–312, 317
 - de Dilworth, 180–183, 200, 517
 - de Sperner, 194
 - de Zorn, 184
- Leonardo de Pisa, *ver* Fibonacci
- Lewis, H. D., 522
- linguagem proposicional, 7, 9, 10
- lista
 - de adjacência, 334
 - de arestas, 334
 - de sucessores, 334, 362, 363
- Loubere, Antoine de la, 229
- Lovász, László, 450, 513
- Lucas, 134, 150
- maior
 - grau dos vértices, 331, 338, 354
- majorante, 156–158, 162, 163, 165
- Mantel, W., 338
- mapa, 548, 568
 - de Karnaugh, 291
 - de Portugal, 391, 392, 399, 417
 - planar, 569
- matriz
 - de adjacência, 332–334, 362, 364, 365, 367, 374, 376, 386
 - de atingibilidade, 370, 371
 - de distâncias, 390
 - de Hadamard, 237, 263–267, 269
 - normalizada, 265, 266
 - de incidência, 332–334, 519
 - de um design, 238, 239, 242, 266, 267
 - de pesos, 488
 - simétrica, 333
- Maurólico, Francesco, 42
- máximo divisor comum, 201, 202, 204, 205, 300
 - de polinómios, 215, 223
- Mei-Ko Kwan, 486
- menor, 551–553, 556–559, 561, 564, 565, 568, 569, 576–579
 - combinatório, *ver* menor
 - grau dos vértices, 331, 338, 354
 - topológico, 551, 552, 556–559, 578, 579
- método

- das duas fases, 436, 448
de de la Loubere, *ver* algoritmo de de la Loubere
de Horner, *ver* algoritmo de Horner
de previsão, 102
heurístico, 497
húngaro, 461, 462
simplex para redes, 437, 439–443
mínimo múltiplo comum, 201, 300
 de polinómios, 215
minitermo, 290
minorante, 156–158, 170, 182
Möbius, August Ferdinand, 190, 204, 207, 208
monoide
 comutativo, 209
Morse, Samuel, 133, 134
multidigrafo, 331
multigrafo, 331, 334, 336
múltiplo, 205, 206, 219, 233
 comum, 201
 de polinómios, 215
Munkers, James, 464
- nand, *ver* incompatibilidade
negação, 9, 16, 41, 272, 277, 278, 283, 597
 conjunta, *ver* incompatibilidade
nem-nem, *ver* rejeição
Neumann, John von, 32
Newton, Isaac, 31, 86, 128
nor, *ver* rejeição
notação
 assimptótica, 334, 585
 de Hardy, 586
 de Landau, 585, 586
número
 binário, 280, 281, 284, 285
 cardinal, 26, 28
 cromático, 512–516, 542, 543
 de Catalan, 421
 de clique, 510, 511, 513
 de cobertura, 455, 510
 de estabilidade, *ver* número de independência
 de independência, 507, 508, 510, 511, 513, 543
 de ouro, 130, 134, 135, 150
 de Ramsey, 536–540
 decimal, 281, 302
 hexadecimal, 281
 primo, 127, 203, 204, 210, 211, 216, 217, 219–223, 227, 228, 234, 235
números
 binomiais, 72, 79, 87, 127–129, 133, 146
 generalizados, 127, 129, 141
 de Bell, 107, 127, 144, 145
 de Catalan, 127, 145–150
 de Euler, 127, 141
 de primeira ordem, 141, 142
 de segunda ordem, 143, 144
 de Fibonacci, 98, 127, 130–135, 150
 de Lucas, 134, 150
 de Stirling, 127, 136
 de primeira espécie, 136, 137, 141
 de segunda espécie, 138–140
 multinomiais, 78–80, 86, 88
 triangulares, 127
 n-uplo, *ver* sequência
octaedro, 562, 563
órbita, 309, 311, 312, 317
ordem
 da equação de recorrência, *ver* profundidade
 das frames, 174
 de especialização, 174–179
 de um corpo, 218
 de um grafo, 331–333, 339, 343, 352, 353, 358
 de um grupo, 305, 306
 de um plano afim, 251, 252, 254, 258
 de um plano projectivo, 247, 248, 251, 252, 254, 262–264, 268
Ore, Øystein, 491
origem
 de uma rede, 423, 425, 426, 429, 432, 433
ou exclusivo, 11, *ver* disjunção exclusiva
ou-não, *ver* rejeição
overflow, 285
- par ordenado, 17
paradoxo
 de Russel, 31
 de Zenão, 31
 do barbeiro, 32
parametrização de uma curva, 549
Parker, Ernest Tilden, 226
partição
 de um conjunto, 20–22, 127, 136, 138–140, 144
 do conjunto dos vértices, *ver* bipartição dos vértices
Pascal, Blaise, 71, 87
passeio, 336, 337
 óptimo, 486
passo

- de indução, 42–45, 47, 48
 pentágono, 581
 permutação, 80, 90, 93, 94, 106, 136–138, 141–144,
 306, 313, 315, 352
 com repetição, 77, 78
 inversa, 306
 permutações, 72
 simples, *ver* permutação
 peso, 379
 de um caminho, 488
 de um passeio, 486
 fechado, 486
 de uma aresta, 486, 488
 Petersen, Julius, 353, 451, 536
 pilha, 349, 372
 plano, 245
 afim, 244, 246, 251–259, 262, 268
 finito, 250, 251
 do Fano, 246, 248, 251, 259, 269
 projectivo, 244, 246–248, 251, 252, 254, 259,
 260, 262–264, 268
 finito, 247, 251
 poliedro, 562, 581
 polinómio
 cromático, 522
 das extensões cromáticas, 529
 irreduzível, 215, 216, 220–225, 235
 mónico, 213
 padrão, 315, 316
 primitivo, 223
 primo, *ver* polinómio irreduzível
 reduzível, 215, 220, 223, 224
 separável, 221
 sobre um anel, 213
 polinómios
 relativamente primos, 215
 Pólya, George, 314–317
 polígono, 562
 regular, 562
 ponte, 360, 361, 369, 402, 404, 405, 452, 554, 568,
 569
 ponto
 do infinito, 246
 fixo, 80, 312
 pontos
 colineares, 245–247, 253
 porta lógica, 278–280, 283, 291, 301, 302
 poset, *ver* conjunto parcialmente ordenado
 Prüfer, Ernst Heinz, 411
 predicado, 6, 7
- princípio
 da adição, 62–64, 75, 86–89, 98
 da bijecção, 57, 61, 62, 105
 da dualidade
 das álgebras de Boole, 275, 276, 291
 dos reticulados, 162, 167, 168, 179
 da gaiola dos pombos, 49, 50, 354
 da inclusão-exclusão, 80
 da multiplicação, 60–64, 71–76, 89, 94, 106
 generalizada, 72, 78, 79
 da multiplicação generalizada, 60, 61
 de conservação do fluxo, 424, 425, 432, 434
 de Dirichlet, 49
 de inclusão mútua, 12, 13, 20
 de inclusão-exclusão, 57, 62, 64, 67, 68
 de indução, 41–43, 47, 48
 completa, 47
- problema
 da afectação de tarefas, 454, 460
 da afectação óptima de tarefas, 454, 463
 das pontes de Königsberg, 479, 480, 482, 561
 das quatro cores, 569
 de Dedekind, 293
 do caixeiro viajante, 496–498, 500, 501, 503,
 505
 do carteiro chinês, 486–489, 504
 dos trinta e seis oficiais, 226
- produto
 cartesiano, 17, 155, 165, 249, 342
 da álgebra de Boole, 273, 598
 de convolução, 189
 de reticulados, 165, 166, 199
 directo
 de conjuntos parcialmente ordenados, 191
 profundidade, 95, 96
 projecção estereográfica, 547, 553, 564
 proposição, 7, 8, 11, 13, 33
 atómica, 8–10
 composta, 8–10
 condicional, 8
- propriedade
 da dupla complementaridade, 14, 276
 da idempotência, 276, 286
 de associatividade, 11, 14
 de distributividade, 11, 13
 de dupla negação, 11
 de idempotência, 11
 do elemento neutro, 276
- pseudoconjunto, *ver* conjunto com repetição
 pseudocódigo, 344, 345, 348–350

- Bellman-Ford, 394
BFS, 350
Ciclo, 481
ComponenteDFS, 361–363
de Floyd, 397
de Leifman, 373
de Prim, 416
DFS, 348
DFS1, 349
Dijkstra, 389, 390
DistBFS, 386
EliminaAresta, 409
Fleury, 485
Ford-Fulkerson, 430
FundeComponente, 364, 365, 367
FundeVértices, 364, 367
Hierholzer, 484
InsereAresta, 408
InvPrufer, 412
Kruskal, 414
KuhnMunkres, 466
MétodoHúngaro, 462
NCC, 362
OrdenarVértices, 349
Prufer, 411
RaizNova, 408
TesteDeSequênciaGráfica, 344, 345
TSPPremiarEPunir, 502
- quadrado
latino, 225–228, 235, 236, 254, 508, 509, 531
normalizado, 226–228, 236
ordem, 225–227, 236
mágico, 228, 229, 232, 236
ordem, 228, 229
perfeito, 229–233
- quadrados latinos
mutuamente ortogonais, 254–259, 262, 263, 268
ortogonais, 226, 227, 229, 254
- quantificador, 15, 16
existencial, 15, 16
universal, 15, 16
- quasigrupo, 225
- raio
de um grafo, 379, 380, 384, 391, 393, 399
- raiz
de uma árvore, 407
de um polinómio, 213, 235
racional, 213, 235
- realização
2-cellular, 550
celular, 550, 565
de um grafo, 547
- recorrência, 93
recta, 245–254, 256–264, 268
de Khalimsky, 177
digital, 177
projectiva, 259
- rectas
paralelas, 246, 251, 252, 254, 256–258
rede, 423–447, 460
de transporte, 379, 423
equilibrada, 433
quilibrada, 448
- reflexividade, 163, 286
reflexão, 313, 319, 320
- região
de um grafo, 550
- regra
de l'Hôpital, 587
- rejeição, 11, 33, 278, 302, 597
- relação
anti-simétrica, 18, 19, 155, 174, 285
binária, 17–19, 21, 22
de adjacência, 330, 335, 336
de conexidade, 357
de congruência, 21, 208, 212
módulo um polinómio, 216
de divisibilidade, 156, 157, 160, 165
de equivalência, 20–22, 25, 357
de incidência, 245, 263, 330, 335
de blocos, 244
de isomorfismo, 335
de ordem, 19
de ordem fraca, 185
de ordem intervalar, 185
de ordem linear, 19, 156, 184, 186, 188
de ordem parcial, 19, 27, 155, 156, 159, 162, 163, 171, 174, 178–182, 184–186, 188, 194, 197–199, 285, 322
de ordem semi-transitiva, 185
de ordem total, 19, 156, 181, 185
de pertença, 18
de pertença de pontos a blocos, *ver* relação
da incidência de blocos
de pré-ordem, 174, 553
de quase-ordem, 185–187
de recorrência, 93–95, 125
inversa, 18, 22

- reflexiva, 18–20, 22, 155, 162, 174, 184, 285
- semi-transitiva, 185, 199
- simétrica, 18–20, 22
- transitiva, 18–20, 22, 155, 174, 285
- unívoca, 22
- representação
 - de um cpo, 189
- restrição
 - de ordem parcial, 184
 - de uma função, 25, 30
- resíduo quadrático módulo p , 538
- reticulado, 155, 161–171, 174, 178–180, 186, 198, 199
 - complementado, 169, 272
 - completo, 169, 170, 174
 - de Boole, 169
 - diamante, 167–169
 - distributivo, 167–171, 179, 180, 199, 272
 - finito, 169–171, 179, 180, 199
 - modular, 168
 - pentágono, 167, 168
 - subreticulado, 164, 165, 168, 171
- rotação, 313, 314, 318–320, 322
- Russel, Bertrand, 31
- Schröder, Ernst, 30
- Segner, Johann Andreas von, 146
- segundo membro
 - da equação de recorrência, 102–106, 108
- semigrau
 - de entrada, 331, 371
 - de saída, 331, 371
- sequência, 24, 60, 71–75, 77, 78, 80, 99, 336
 - binária, 57–60, 62, 68, 74, 77, 125, 165, 274, 287, 289, 342–345, 598
 - de Fibonacci, 98
 - de graus de vértices, 343, 344, 346, 355
 - gráfica, 343–346, 355
- Shrikhande, S.S., 226
- sistema
 - de equações, 97
 - lineares, 100, 102, 105
 - de numeração, 280
 - árabe, 98
 - binário, 280, 282, 284
 - decimal, 98, 280, 281
 - hexadecimal, 280
 - hindu, 98
 - não posicional, 280
 - octal, 280, 281
- posicional, 280, 281
- romano, 280
- de representantes distintos, 454, 476
- de Steiner, 243, 248
- de triplos de Steiner, 243, 244, 258, 268
- parcial, 243
- Skolem, Thoralf, 32
- solução
 - básica admissível, 433, 436–439, 441–443, 448
 - degenerada, 440
 - inteira não negativa, 59, 75
 - inteira positiva, 75
- soma
 - da álgebra de Boole, 273, 598
 - lógica, 272
 - módulo dois, 278–280
 - telescópica, 131, 132
- somador
 - completo, 282–285
 - parcial, 282–285
- Sperner, Emanuel, 194
- Stirling, James, 127, 128, 136–141, 145, 595
- Stone, Marshall H., 289
- subárvore, 408
- subconjunto, 6, 7, 12, 17, 18, 21, 22, 25, 28–30, 34, 35
 - próprio, 6, 29
- subcorpo, 210, 217
 - primitivo, 217, 218
- subdivisão
 - de arestas, 551
 - de um grafo, 551
- subgrafo, 339–341, 369
 - abrangente, 339–341
 - de suporte, *ver* subgrafo abrangente
 - induzido, 339, 357
 - pelas arestas, 340
 - próprio, 339
- subgrupo, 306–309
 - normal, 308
- subminitermo, 290
- subsequências, 181
- sucessão, 24
- Sudoku, 526, 531–533
- superfície, 549
 - de Riemann fechada, 548
 - não-orientável, 548
 - orientável, 548
 - sem bordo, 548
- superfícies

- topologicamente equivalentes, 548
supergrafo, 339
supremo, 156, 157, 161–163, 165, 169, 170
Sylvester, James, 65, 263
Szekeres, George, 181
- tabela
de operação, 209, 210, 218–220, 222, 225
de verdade, 8–11, 34
dos valores lógicos, 8
- tabuleiro
de xadrez, 353, 489
- Tait, Peter Guthrie, 536, 570
- Tarjan, Robert, 347
- Tarski, Alfred, 30
- Tartaglia, *ver* Fontana, Niccolò
- tautologia, 10, 11, 13, 33, 34, 39, 40
- teorema
clássico da inversão de Möbius, 208
da curva fechada de Jordan, 549
da fórmula de Euler, 553
da inversão de Möbius, 193, 234, 529
da recorrência universal, 592
da representação de Birkhoff, 171
da representação de Stone, 289
da versão clássica da inversão de Möbius, 208
das quatro cores, 569, 573
das três cores, 572
de Akra-Bazzi, 593
de Berge, 450, 460, 463, 469
de Bose, 259
de Brooks, 513, 514
de Burnside-Pólya, 317
de Cantor, 27, 28
de Catlin, 578
de Cayley, 306, 406, 411
de Daniel da Silva, 211
de Dedekind e Cantor, 29
de Dilworth, 182, 183, 189, 457
de Dirac, 491, 492, 552
de Dirichlet, 49
de Egerváry, 464
de Erdős-Ko-Radó, 195, 196
de Erdős-Szekeres, 181
de Euler, 206, 211
de Euler-Hierholzer, 482, 486
de Ford e Fulkerson, 425, 428
de Frobenius, 456
de Gaddum e Nordthaus, 515
de Gallai, 510
- de Gauss, 223
de Gilmore e Hoffman, 457
de Grimberg, 572
de Grünbaum, 573
de Hadamard, 266
de Hadwiger, 576
de Hall, 453, 454, 464
de Heawood, 566, 569
de König, 455, 456, 535
de König-Egerváry, 456
de Kuratowski, 556, 558
de Lagrange, 308
de l’Huillier, 565
de Mantel, 338
de Mirsky, 183
de Ore, 491
de Pólya, 314, 316
de Ramsey, 540
de Robertson e Seymour, 551
de Robertson, Seymour e Thomas, 552
de Schröder-Bernstein, 30
de separação, 549
de Stirling, 595
de Szpilrajn, 184
de Tait, 536, 570, 571
de Tarski, 30
de Tutte, 450–452
de Tutte-Berge, 471
de Vizing, 533
de Wagner, 558, 577
de Whitney, 561
de Zykov, 515
do casamento, *ver* teorema de Hall
do fluxo máximo corte mínimo, *ver* teorema
de Ford e Fulkerson
do grafo perfeito, 513
fundamental da aritmética, 204, 234
húngaro, *ver* teorema de König-Egerváry
pequeno de Fermat, 211, 217
- teoria
de Ramsey, 537
dos códigos, 508
tetraedro, 562, 563
topologia, 171–180
 digital, 155, 174, 176
 finita, 171, 172
torre de Hanoi, 118
torus, 548
 duplo, 548
 triplo, 548

- trajecto, 336, 337
 de Euler, 480, 482, 485
 fechado, *ver* circuito
 trajectória, *ver* órbita
 transitividade, 163, 183–185, 286, 288
 transposição, 83, 352
 transposição
 simples, 83, 84
 triangulação, 571
 do plano, 555, 571
 internamente 6-conexa, 574
 minimal, 573
 plana, *ver* triangulação do plano
 triângulo, 337, 338, 343, 581
 de Pascal, 87, 129, 133
 TSP, *ver* problema do caixeiro viajante
 Tutte, William Thomas, 450, 570
- união
 de conjuntos, 11, 12, 14, 15, 62, 64, 65, 271
 generalizada, 14
- valência, *ver* grau
 valor
 do fluxo, 424
 variedade compacta, 547, 551
 variável
 proposicional, 8–10
 vector
 reduzido minimal, 518
 reduzido mínimo, 292, 293
 vectores
 linearmente independentes, 218
 Velben, Oswald, 549
 Venn, 11–13
 verdadeiro, 8, 9, 26
 vértice, 329, 332, 548
 atingível, 370
 central, 379, 380, 383, 391, 393
 de corte, 361, 369, 560
 destino, 424
 extremo de uma aresta, 330, 334–336, 339,
 340, 347, 357, 548
 final, 336, 337
 fonte, 423, *ver* vértice origem
 initial, 336, 337
 intermédio, 336
 isolado, 334, 340, 359
 origem, 424
 sorvedouro, 423, *ver* vértice destino
 vértice-conexidade, 370
- vértices
 adjacentes, 330, 339, 340, 343
 conexos, 357, 360
 mutuamente atingíveis, 370
 viagem à volta do mundo, 479
 vizinhança, 330, 547
 aberta, 172, 173, 177
 aberta mínima, 174, 177
 mínima, 172, 177, 178
 vizinho, 337
- Wagner, Klaus, 550
 Weierstrass, Karl, 31
 Whitney, Hassler, 522
- xor, *ver* disjunção exclusiva
- Yang Hui, 87
- Zenão de Eléia, 31
 Zermelo, Ernst, 32
 Zykov, Alexander Alexandrovitch, 515