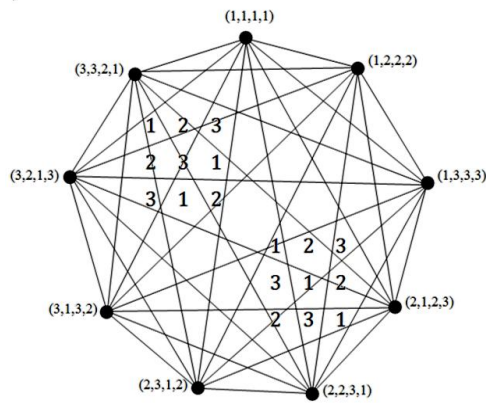




Andreia Cristina
Dias Morgado

Quadrados Latinos e Grafos





Universidade de Departamento de Matemática
Aveiro
Ano 2012

**Andreia Cristina
Dias Morgado**

Quadrados Latinos e Grafos

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática e Aplicações (ramo Ciências da Computação), realizada sob a orientação científica da Prof. Doutora Rosa Amélia Baptista Ferreira Soares Martins, Professora Auxiliar do Departamento de Matemática da Universidade de Aveiro.

Dedico este trabalho à minha Orientadora, Professora Doutora Rosa Amélia, pela sua orientação, apoio e disponibilidade.

À minha amiga e colega de Mestrado, Cecília Solange, pelo companheirismo e cooperação com que ultrapassamos as dificuldades sentidas.

Aos meus pais e namorado, pelo apoio e compreensão nos momentos mais difíceis, assim como, pela confiança e incentivo na realização e concretização desta etapa.

À família e amigos presentes ao longo desta caminhada pelo ânimo que sempre me transmitiram.

O júri

Presidente

Prof. Doutor Domingos Moreira Cardoso
Professor Catedrático da Universidade de Aveiro

Prof. Doutora Rosa Amélia Baptista Ferreira Soares Martins
Professora Auxiliar da Universidade de Aveiro (Orientadora)

Prof. Doutora Maria Manuel Torres
Professora Auxiliar da Faculdade de Ciências da Universidade de Lisboa

Palavras-chave

Quadrados Latinos; Quadrados Latinos Linha; MOLS; Grupos; Grafos; Grafos Completos; Fatorizações; Caminhos, circuitos e ciclos em grafos.

Resumo

O objetivo principal desta dissertação é o estudo da relação entre Quadrados Latinos e Grafos. Demonstra-se que o tipo e as características do Grafo refletem-se no tipo e características do Quadrado Latino associado.

No primeiro capítulo são apresentados os conceitos introdutórios e as principais características dos Quadrados Latinos.

As aplicações dos Quadrados Latinos à Teoria dos Grupo são tratadas no segundo capítulo.

Para finalizar, no terceiro capítulo, são apresentados alguns conceitos introdutórios da Teoria dos Grafos, sendo estes de extrema importância para a concretização do quarto capítulo onde se encontra a parte principal do trabalho, isto é, a relação entre Quadrados Latinos e Grafos.

Keywords

Latin Squares; Row Latin Squares; MOLS; Groups; Graphs; Complete Graphs; Factorizations; Paths, Circuits and Cycles in Graphs.

Abstract

The main objective of this dissertation is the study of the relationship between Latin squares and graphs. It is shown that the type and characteristics of the graph are reflected on the type and characteristics of the associated Latin square.

The first chapter presents introductory concepts and the main characteristics of Latin squares.

The applications of Latin squares to the group theory are discussed in the second chapter.

Finally, in the third chapter, we present some introductory concepts of Graph Theory, which are extremely important to the achievement of the fourth chapter where is the main part of the work, i.e., the relationship between Latin squares and graphs.

INTRODUÇÃO	I
1. QUADRADOS LATINOS	1
1.1. INTRODUÇÃO HISTÓRICA	1
1.2. EXEMPLO DE APLICAÇÃO	2
1.3. CONCEITOS BÁSICOS	3
1.4. QUADRADOS LATINOS MUTUAMENTE ORTOGONAIS	4
1.5. CONSTRUÇÃO DE CONJUNTOS COMPLETOS DE MOLS	7
1.6. ALGUNS RESULTADOS ADICIONAIS	13
2. GRUPOS E QUADRADOS LATINOS	17
2.1. INTRODUÇÃO	17
2.2. GRUPOS E QUADRADOS LATINOS	18
2.3. QUADRADOS LATINOS LINHA	21
2.4. CONJUNTOS DE QUADRADOS LATINOS LINHA ORTOGONAIS	22
3. GRAFOS	25
3.1. CONCEITOS BÁSICOS	26
4. GRAFOS E QUADRADOS LATINOS	33
4.1. QUADRADOS LATINOS E GRAFOS BIPARTIDOS	33
4.2. QUADRADOS LATINOS E FATORIZAÇÃO DE GRAFOS E DIGRAFOS	43
4.3. QUADRADOS LATINOS LINHA-COMPLETOS E CAMINHOS EM GRAFOS	54
4.4. GRAFOS FORTEMENTE REGULARES	66
BIBLIOGRAFIA	71
ANEXOS	73

INTRODUÇÃO

O objetivo principal desta dissertação é o estudo da relação entre *Quadrados Latinos* e *Grafos*. O tipo e as características do *Grafo* refletem-se no tipo e características do Quadrado Latino associado.

O tema da presente dissertação resulta de uma proposta apresentada em simultâneo a mim própria e a Cecília Solange Gomes Godinho, colega de Curso. Na época, tratando-se de um assunto novo para ambas, entendeu-se desenvolver em conjunto os temas presentes nos dois primeiros capítulos. Contudo, na presente dissertação as demonstrações dos resultados obtidos encontram-se em anexo.

Na concretização deste estudo escolhemos como base de trabalho o livro “*Discrete Mathematics Using Latin Squares*” de Charles F. Laywine e Gary L. Mullen.

Assim, os conceitos introdutórios serão apresentados no primeiro capítulo, onde se abordam os *Quadrados Latinos* e as suas principais características. No segundo capítulo exibem-se as aplicações dos *Quadrados Latinos* à *Teoria dos Grupos* e, no terceiro capítulo, serão apresentados alguns conceitos introdutórios da *Teoria dos Grafos*, sendo estes de extrema importância para a concretização do quarto capítulo onde se encontra a parte principal do trabalho, isto é, a relação entre *Quadrados Latinos* e *Grafos*.

Neste capítulo, as entradas de um *Quadrado Latino* podem ser interpretadas de várias formas. Se as interpretarmos como sendo as *arestas* de um *grafo* às quais são atribuídas cores ou símbolos, podemos utilizar o *quadrado latino* para estudar as *1-fatorizações* de *grafos bipartidos completos* e *grafos dirigidos completos* com e sem *lacetes*. Conforme o tipo de *grafo* que considerarmos, o tipo de *quadrado latino* associado a *1-fatorizações* será diferente e assim teremos que o número de *1-fatorizações* de um *grafo bipartido* de ordem n é dado pelo número de *quadrados latinos* de ordem n ; o número de *1-fatorizações* de um *grafo dirigido completo com lacetes* de ordem n é dado pelo número de *quadrados latinos* de ordem n com a *primeira linha fixa*; o número de *1-fatorizações* de um *grafo dirigido completo sem lacetes* de ordem n é dado pelo número de *quadrados latinos* de ordem n *unipotentes* com a *primeira linha fixa* e o número de *1-fatorizações* de um *grafo completo* (não dirigido) de ordem n , com n par, é dado pelo número de *quadrados latinos reduzidos, simétricos e unipotentes* de ordem n .

A existência de uma *1-fatorização* no *grafo* associado a um *quadrado latino* dar-nos-á, também, a informação sobre a existência ou não de *companheiro ortogonal* desse *quadrado latino*.

Contudo, os *quadrados latinos* dar-nos-ão outras informações se considerarmos as entradas como sendo os *vértices* de um *grafo*. Neste caso, cada linha do quadrado dar-nos-á sempre um

caminho hamiltoniano. E no caso de estarmos interessados em caminhos disjuntos, então teremos de exigir que o *quadrado latino* verifique a propriedade de ser “*linha-completo*”. Quando n é par prova-se construtivamente a existência de um *quadrado latino linha-completo* de ordem n .

Cada um desses *quadrados latinos linha-completos* de ordem n (com n par, ou seja, $n = 2m$) dá uma decomposição em $2m$ *caminhos hamiltonianos* disjuntos de um *grafo dirigido completo sem lacetes* de ordem $2m$ ou em m *caminhos hamiltonianos* disjuntos de um *grafo não dirigido completo* de ordem $2m$. Acrescentando um vértice aos *grafos* anteriormente referidos obtemos $2m$ *ciclos hamiltonianos* disjuntos de um *grafo dirigido sem lacetes* de ordem $2m+1$ e m *ciclos hamiltonianos* disjuntos de um *grafo não dirigido completo* de ordem $2m+1$.

As primeiras m linhas de um *quadrado latino* do tipo anteriormente referido dão-nos, também, a indicação de um *circuito de Euler* num *grafo completo não dirigido* de ordem $2m+1$.

Se pretendermos completar um *retângulo latino*, $r \times n$, de forma a obtermos um *quadrado latino* de ordem n teremos de considerar as suas entradas como *ausências de arestas* de um *grafo bipartido*, $K_{n,n}$, em que um dos conjuntos de vértices corresponde às n colunas e o outro corresponde aos n símbolos usados (se o símbolo k está ausente da coluna j existirá uma aresta de j para k).

No entanto, também se pode considerar as entradas do *quadrado latino* conjuntamente com a sua posição como representando vértices e adjacências de um *grafo fortemente regular*. Para este caso, existirão tantos vértices quantas as posições do *quadrado latino*.

E, se considerarmos, em vez de um *quadrado latino*, um conjunto de *quadrados latinos mutuamente ortogonais* (MOLS), podemos associar-lhe um *grafo fortemente regular* em que existirão tantos vértices quantas as posições dos *quadrados latinos* e a adjacência entre vértices estará associada à existência do mesmo símbolo em algum dos *quadrados* ou à posição que estes ocupam.

1. QUADRADOS LATINOS

1.1. INTRODUÇÃO HISTÓRICA

Os primeiros registos sobre *quadrados latinos* remontam a 1639 num jogo de cartas. Embora estes quadrados já fossem conhecidos pelo menos alguns séculos antes, *Leonhard Euler* (1707-1783) foi o primeiro matemático a explorar a *Teoria dos quadrados latinos*. Introduzindo o conceito de *Quadrado Latino*, em 1779, Euler chamou-lhe “*nova espécie de quadrado mágico*”. No entanto, ao contrário dos quadrados mágicos, os *quadrados latinos* não se preocupam com a aritmética e os símbolos que o compõem não têm de ser necessariamente números. O seu nome prende-se com o facto de os símbolos utilizados para o formarem serem os do alfabeto latino.

Euler primava pelo seu espírito genial de transformar “*pedras em ouro matemático*”. Entre as mais variadas descobertas, a *Teoria dos Grafos* nasce de um problema que lhe fora colocado em S. Petersburgo – as pontes de Königsberg. Bem como a *Teoria dos Quadrados Latinos* que Euler fundou em 1782 tendo como origem o problema dos 36 oficiais (que se diz ter-lhe sido proposto por Catarina, a Grande, czarina da Rússia). Para a resolução deste problema, Euler procurava dois *quadrados ortogonais* de ordem 6, não conseguindo encontra-los conjecturou que não havia pares de *quadrados latinos ortogonais* de ordem 6, 10, 14, 18, 22, ..., $4n + 2$.

Em 1900, *Gaston Tarry*, matemático amador que trabalhava como funcionário público na Argélia, confirma que não há nenhum par de quadrados latinos ortogonais de ordem 6.

Contudo, em 1960 *Raj Bose*, *Ernest Parker* e *Sharadchandra Shirikhande* provaram que existem realmente pares de quadrados latinos de ordem 10, 14, 18, 22, ..., $4n + 2$, com $n > 1$.

A *Teoria dos Quadrados Latinos* ainda se encontra em estudo, não tendo sido descoberto até à presente data três *quadrados latinos mutuamente ortogonais* de ordem 10.

Em 1925 *R. A. Fisher*, um eminente estatístico, sugeriu o uso de *quadrados latinos* nos projetos de ciências *estatísticas*. Desta forma, usou os *quadrados latinos* para revolucionar os métodos agrícolas durante o tempo em que esteve na Estação de Pesquisa Rothamsted em Hertfordshire, em Inglaterra.

Porém, existem várias situações onde o recurso à *Teoria dos Quadrados Latinos* é, sem dúvida, uma mais-valia, podendo assim trabalhá-los a nível de várias áreas dentro e fora da *combinatória*, envolvendo a *álgebra*, *geometria finita*, *estatística* e outras, como *teoria dos códigos* e *criptografia*.

No fim da década de 1970 foi inventado, em Nova Iorque, o tão conhecido *Sudoku* (“um só número”) – caso particular de um *quadrado latino*. Ganhou popularidade no Japão na década seguinte, antes de se tornar imensamente popular em 2005. Desta forma, todas as pessoas brincam com *quadrados latinos* – tal como os matemáticos.

1.2. EXEMPLO DE APLICAÇÃO

Muitas das motivações originais para o estudo da *teoria dos quadrados latinos* provém de experiências a nível da agricultura. Por exemplo, imagine-se que se quer plantar três variedades de plantas (0, 1 e 2) em três campos e em três meses, Abril, Maio e Junho, denotados respetivamente por, Ab, Ma e Ju. Uma forma possível de o conseguir é a seguinte:

Campo / Mês	Ab	Ma	Ju
A	0	1	2
B	0	1	2
C	0	1	2

Note-se que a variedade 0 só é testada no mês de Abril, a variedade 1 em Maio e a 2 em Junho. Uma melhor estratégia seria uma representação em que cada variedade é testada todos os meses e em todos os campos. Tal representação seria:

Campo / Mês	Ab	Ma	Ju
A	0	1	2
B	1	2	0
C	2	0	1

Suponha-se agora que se tem 3 tipos de fertilizantes (também denotados por 0,1 e 2). Da mesma forma, usar-se-á dois quadrados, um para representar a variedade de plantas e outro para representar a variedade de fertilizantes.

Será que é possível testar as nove combinações possíveis de variedades de planta/fertilizante exatamente uma vez?

A resposta é sim. Como o quadrado acima é um exemplo de um quadrado latino de ordem 3, a pergunta formulada tem resposta afirmativa, desde que exista um par de quadrados latinos com uma certa propriedade. De facto, quadrados desta forma apresentam uma estrutura combinatória muito singular, e dela derivam muitas propriedades e aplicações.

1.3. CONCEITOS BÁSICOS

Neste subcapítulo serão apresentadas algumas definições e resultados importantes para o desenvolvimento do estudo dos quadrados latinos.

Definição 1.1. (*Quadrado latino*): As matrizes quadradas de ordem n , cujas entradas pertencem a um conjunto com n elementos e onde cada elemento ocorre exatamente uma vez em cada linha e coluna, designam-se por quadrados latinos de ordem n .

Definição 1.2. (*Retângulo latino*): Dados dois inteiros r e n , com $r \leq n$, um *retângulo latino* é uma matriz com r linhas e n colunas, cujas entradas pertencem a um conjunto com n elementos e onde cada elemento ocorre exatamente uma vez em cada linha e não se repete por colunas.

Proposição 1.3.: Para qualquer $n > 1$ existe um quadrado latino de ordem n .

Note-se que este quadrado latino corresponde à tabela da adição em $(\mathbb{Z}_n, +)$. Tal facto leva a pensar na relação entre a *teoria dos quadrados latinos* e a *teoria dos grupos*, tornando-se posteriormente relevante abordar também este assunto.

Nota: No que se segue iremos considerar quadrados latinos de ordem n cujos elementos são $0, 1, \dots, n - 1$.

Definição 1.4. (*Quadrado latino reduzido ou normalizado*): Um quadrado latino designa-se por reduzido ou normalizado, se a primeira linha e coluna são da forma $0 \ 1 \ 2 \ \dots \ n - 1$.

Neste momento, torna-se relevante saber, dado $n > 1$, quantos quadrados latinos de ordem n existem. Para isso, denote-se por L_n o número de quadrados latinos distintos de ordem n e por l_n o número de quadrados latinos reduzidos de ordem n .

Teorema 1.5.: Para $n > 1$, L_n é dado por:

$$L_n = n! (n - 1)! l_n$$

No entanto, encontrar uma fórmula explícita para L_n a partir de n , isto é, $L_n = L_n(n)$ não é tarefa fácil, visto que é necessário calcular l_n , e este desafio torna-se um problema difícil, uma vez que não existe ainda relação explícita entre l_{n-1} e l_n . Para que se possa ter uma ideia da complexidade deste problema basta analisarmos a seguinte tabela:

n	l_n
2	1
3	1
4	4
5	56
6	9408
7	16942080
8	535281401856
9	377597570964258816
10	7580721483160132811489280
11	$\approx 5,36 \times 10^{33}$
12	$\approx 1,62 \times 10^{44}$
13	$\approx 2,51 \times 10^{56}$
14	$\approx 2,33 \times 10^{70}$
15	$\approx 1,5 \times 10^{86}$

Até hoje são apenas conhecidos valores exatos de l_n para $2 \leq n \leq 10$, e para $11 \leq n \leq 15$ existem apenas estimativas usando métodos probabilísticos e computacionais para tal.

1.4. QUADRADOS LATINOS MUTUAMENTE ORTOGONAIS

Definição 1.6. (*Quadrados latinos ortogonais*): Seja n um inteiro positivo. Dois quadrados latinos L' e L'' dizem-se ortogonais se os pares ordenados formados pelas entradas de L' e L'' na mesma posição aparecem todos sem repetição. Isto é, L' e L'' são considerados quadrados latinos ortogonais se para qualquer par de entradas (α, β) existe uma única posição (i, j) tal que $L'_{ij} = \alpha$ e $L''_{ij} = \beta$.

Por exemplo, L' e L'' a seguir representados são dois quadrados latinos ortogonais de ordem 3:

$$L' = \begin{matrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{matrix} \quad \text{e} \quad L'' = \begin{matrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{matrix}$$

Uma forma imediata de verificar se dois quadrados latinos de ordem n são realmente ortogonais, consiste em determinar a matriz concatenada dos pares de símbolos que se obtém, para as entradas de ambos, e verificar se esta matriz tem ou não todas as n^2 entradas distintas.

Definição 1.7. (*Matriz Concatenada*): Dadas duas matrizes $n \times n$, $L' = (\alpha_{ij})$ e $L'' = (\beta_{ij})$, a matriz concatenada é a matriz $n \times n$, $C = (\alpha_{ij}, \beta_{ij})$, onde cada entrada é um par ordenado em que o primeiro elemento vem de L' e o segundo elemento vem de L'' . Denota-se por $C = L' \odot L''$.

Portanto, no exemplo anterior, construindo-se a matriz,

$$C = \begin{bmatrix} (\alpha, \alpha) & (\beta, \beta) & (\gamma, \gamma) \\ (\beta, \gamma) & (\gamma, \alpha) & (\alpha, \beta) \\ (\gamma, \beta) & (\alpha, \gamma) & (\beta, \alpha) \end{bmatrix}$$

verifica-se que todos os pares ordenados que representam as entradas da matriz C são distintos, podendo-se concluir que os quadrados latinos L' e L'' são realmente ortogonais.

Historicamente, o primeiro problema conhecido 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, cada um dos quais formado por 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 oficiais com a mesma patente ou pertencentes ao mesmo destacamento numa mesma linha ou coluna.

O problema dos trinta e seis oficiais é equivalente ao problema da existência de dois quadrados latinos ortogonais de ordem seis, em que um deles representa os destacamentos e o outro representa as patentes. 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 um matemático amador Francês, Tarry Gaston (1843-1913). 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 $n \equiv 2 \pmod{4}$, isto é, $n = 2(2k + 1)$.**

No entanto, esta conjectura é falsa. Com efeito, Raj Chandra Bose (1901-1987), Sharadchandra Shankar Shrikhande e Ernest Tilden Parker (1926-1991) demonstraram em 1960 a existência de quadrados latinos ortogonais de ordem n para todo o natural n , com exceção de $n = 2$ e $n = 6$.

Definição 1.8. (*Conjunto mutuamente ortogonal de quadrados latinos*): Seja $A = \{L_1, \dots, L_k\}$ um conjunto de quadrados latinos de ordem n . A diz-se um conjunto mutuamente ortogonal se para cada $i \neq j$, L_i é ortogonal a L_j . Os quadrados latinos de tal conjunto são denotados por MOLS (Mutually Orthogonal Latin Squares).

Vamos agora considerar o problema de encontrar conjuntos de MOLS cujas cardinalidades sejam as maiores possíveis. Para isto considere-se $N(n)$ como sendo o número máximo possível de MOLS de ordem n . De seguida, procurar-se-á um majorante para a função $N(n)$.

Proposição 1.9.: Para cada $n \geq 2$ $N(n) \leq n - 1$.

Definição 1.10. (*Conjunto completo de MOLS*): Um conjunto de $n - 1$ MOLS de ordem n é chamado um conjunto completo.

No exemplo abaixo apresenta-se um conjunto de MOLS de ordem 4.

Exemplo 1.11.: Considerem-se os quadrados latinos:

0	1	2	3	0	1	2	3	0	1	2	3
1	0	3	2	2	3	0	1	3	2	1	0
2	3	0	1	3	2	1	0	1	0	3	2
3	2	1	0	1	0	3	2	2	3	0	1

Por simples observação, verifica-se que eles formam um conjunto completo de MOLS. Note-se que $N(4) = 3$.

1.5. CONSTRUÇÃO DE CONJUNTOS COMPLETOS DE MOLS

1.5.1. CASO EM QUE n É POTÊNCIA DE UM NÚMERO PRIMO

▪ Interpretação Algébrica

Considere-se a construção de conjuntos de MOLS de ordem n tal que $n = p^m$, com p primo. Estas construções estão intimamente ligadas à *teoria dos corpos finitos* (o corpo finito mais simples é da forma \mathbb{Z}_p , em que p é primo e a adição e multiplicação são *mod* p).

O primeiro resultado mostra que para um $q = p^m$, pode-se facilmente construir um conjunto de MOLS de ordem q . Esta construção, de 1938, deve-se ao famoso estatístico-matemático indiano R. C. Bose (1901-1987) e a E. H. Moore (1896).

Inicialmente atribuem-se etiquetas às linhas e colunas de um quadrado latino $q \times q$, com q elementos, de um corpo finito F_q de ordem q . Por uma questão de simplificação. Assim, para o polinómio $f(x, y)$ com coeficientes em F_q , coloque-se o elemento $f(a, b)$ na intersecção da linha a com a coluna b do quadrado. Nestas condições, diz-se que o polinómio $f(x, y)$ representa o quadrado.

Vamos usar a construção acima descrita para construir um conjunto de MOLS de ordem 3.

Exemplo 1.12.: Vamos construir um conjunto completo de MOLS de ordem 3. Para isso, considere-se o corpo \mathbb{Z}_3 .

No caso em que $a = 1$, o polinómio da forma $ax + y$ é dado por $x + y$ e no caso em que $a = 2$, o polinómio correspondente é dado por $2x + y$. Seja L_1 o quadrado latino representado por $x + y$ e L_2 o quadrado latino representado por $2x + y$. Através destes polinómios é possível construir um conjunto completo de MOLS de ordem 3, em que L_1 e L_2 são dados por:

$$L_1 = \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \quad \text{e} \quad L_2 = \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

Não há mais polinómios da forma $ax + y$ com $a \in \mathbb{Z}_3 \setminus \{0\}$. Eles formam um conjunto completo de MOLS de ordem 3.

Segue-se o teorema fundamental deste capítulo:

Teorema 1.13.: Para q , potência de um número primo, o conjunto de polinómios da forma $f_a(x, y) = ax + y$ com $a \neq 0 \in F_q$ representa um conjunto completo de $q - 1$ MOLS de ordem q .

Considere-se o seguinte exemplo para $q = 4$:

Exemplo 1.14.: Para construir um conjunto completo de MOLS de ordem 4, considere-se o corpo $F_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$, onde α denota uma raiz de um polinómio irreduzível sobre F_2 , $x^2 + x + 1$ (de facto, $\alpha^2 + \alpha + 1 = 0$ é equivalente a $\alpha^2 + \alpha + 1 + \alpha + 1 = \alpha + 1$ e a $\alpha^2 = \alpha + 1$).

As operações em F_4 são as constantes nas tabelas:

Adição em F_4 :

	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Multiplicação em F_4 :

	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Aplicando o teorema acima, obtém-se os seguintes quadrados:

0	1	α	$\alpha+1$	0	1	α	$\alpha+1$	0	1	α	$\alpha+1$
1	0	$\alpha+1$	α	α	$\alpha+1$	0	1	$\alpha+1$	α	1	0
α	$\alpha+1$	0	1	$\alpha+1$	α	1	0	1	0	$\alpha+1$	α
$\alpha+1$	α	1	0	1	0	$\alpha+1$	α	α	$\alpha+1$	0	1

que são representados, respetivamente, pelos polinómios $x + y$, $\alpha x + y$, $(\alpha + 1)x + y$ de F_4 .

Note-se que se se trocar α , $\alpha + 1$ por 2 e 3 tem-se os mesmos MOLS do Exemplo 1.10..

1.5.2. CASO EM QUE n NÃO É POTÊNCIA DE UM NÚMERO PRIMO

Tendo efetivamente calculado $N(n)$ quando n é uma potência de um número primo, considere-se, agora, a construção de conjuntos de MOLS de ordem n , para um n arbitrário. Note-se que esta nova situação é muito diferente da anterior, pelo facto de se q não é primo, F_q é apenas um anel com unidade e não um corpo, não herdando as importantes propriedades da *teoria dos corpos finitos*; assim, tratar-se-á este problema de outra forma.

Para começar, lembre-se do problema proposto por Euler em 1779 dos 36 oficiais. É claro que este problema tem solução se, e somente se, existe um par de quadrados latinos de ordem 6 e, de facto, $n = 6$ é o primeiro número que não é primo, nem potência de um primo. Assim, se se tentar construir um par de MOLS de ordem 6 ter-se-ia de trabalhar sobre o anel \mathbb{Z}_6 que obviamente não é corpo, ou seja, tentar-se-ia trabalhar com a família de polinómios $ax + y$ para $a \neq 0 \in \mathbb{Z}_6$, não chegando a conclusão alguma, pois não se conseguiria cancelar os elementos da forma $(a - b) \neq 0 \in \mathbb{Z}_6$, uma vez que em \mathbb{Z}_6 os elementos invertíveis são apenas os que são primos com 6. Neste caso, apenas se tem o 1 e o 5, sendo \mathbb{Z}_6 um anel com característica 6 e com divisores de zero.

Euler não encontrou a solução para o problema dos 36 oficiais e falhou também em querer generalizar este facto em 1782.

Pela conjectura de Euler, $N(n) = 1$ para $n = 2(2k + 1)$, com $k \geq 0$. Sabe-se que este facto só é verdade para $k = 0, 1$, o que é intrigante, pois existem 408 quadrados latinos de ordem 6, e nenhum par deles é ortogonal!

Para números que não são potências de primos como $n = 10, 12, 15, 20, \dots$ utiliza-se uma estratégia natural, que se trata de uma espécie de “colagem” de MOLS de ordens menores. Para tal, usa-se o chamado produto de Kronecker de matrizes.

Definição 1.15. (*Produto de Kronecker*): Seja $A = (a_{ij})$ um quadrado latino de ordem m e $B = (b_{ij})$ um quadrado latino de ordem n . O produto de Kronecker de A por B é o quadrado $mn \times mn$, $A \otimes B$, dado por:

$$A \otimes B = \begin{pmatrix} (a_{11}, B) & (a_{12}, B) & \dots & (a_{1m}, B) \\ (a_{21}, B) & (a_{22}, B) & \dots & (a_{2m}, B) \\ \vdots & \vdots & \ddots & \vdots \\ (a_{m1}, B) & (a_{m2}, B) & \dots & (a_{mn}, B) \end{pmatrix}$$

onde para cada entrada a de A , (a, B) é uma matriz $n \times n$ dada por:

$$(a, B) = \begin{pmatrix} (a, b_{11}) & (a, b_{12}) & \dots & (a, b_{1n}) \\ (a, b_{21}) & (a, b_{22}) & \dots & (a, b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ (a, b_{n1}) & (a, b_{n2}) & \dots & (a, b_{nn}) \end{pmatrix}$$

Vejamos um exemplo do produto de Kronecker, para $m = 2$, $n = 3$:

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

O produto de Kronecker requer a construção de um quadrado de ordem 6 cujos elementos são pares ordenados¹:

$$\begin{array}{ccc|ccc} 00 & 01 & 02 & 10 & 11 & 12 \\ 01 & 02 & 00 & 11 & 12 & 10 \\ 02 & 00 & 01 & 12 & 10 & 11 \\ \hline 10 & 11 & 12 & 00 & 01 & 02 \\ 11 & 12 & 10 & 01 & 02 & 00 \\ 12 & 10 & 11 & 02 & 00 & 01 \end{array}$$

É claro que se pode trocar os símbolos 00,01,02,10,11,12 pelos símbolos 0,1,2,3,4,5 para obter um quadrado latino de ordem 6, cujos elementos sejam os símbolos usuais.

Agora, aplicando o produto de Kronecker na construção de conjuntos de MOLS, tem-se o seguinte Teorema:

Teorema 1.16.: Se existir um par de MOLS de ordem n e um par de MOLS de ordem m , então existe um par de MOLS de ordem mn .

Exemplo 1.17.: Neste exemplo, construir-se-á um par de MOLS, C_1 e C_2 de ordem 12 a partir de MOLS de ordem 4 e 3, respetivamente:

¹Por abuso de escrita usamos ij em vez de (i, j) .

$$A_1 = \begin{matrix} & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 2 \\ 1 & 2 & 3 & 0 & 1 \\ 2 & 3 & 2 & 1 & 0 \\ 3 & 2 & 1 & 0 & \end{matrix}$$

$$A_2 = \begin{matrix} & 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 0 & 1 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 & \end{matrix}$$

$$B_1 = \begin{matrix} & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & \end{matrix}$$

$$B_2 = \begin{matrix} & 0 & 1 & 2 \\ 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 2 & 1 & 2 & 0 \end{matrix}$$

$$C_1 = B_1 \otimes A_1$$

$$C_1 = \begin{array}{c|cccc|cccc|cccc}
00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 \\
01 & 00 & 03 & 02 & 11 & 10 & 13 & 12 & & & & \\
02 & 03 & 00 & 01 & 12 & 13 & 10 & 11 & & & & \\
03 & 02 & 01 & 00 & 13 & 12 & 11 & 10 & & & & \\
\hline
10 & 11 & 12 & 13 & 20 & & & & 00 & & & \\
11 & 10 & 13 & 12 & & & & & & & & \\
12 & 13 & 10 & 11 & & & & & & & & \\
13 & 12 & 11 & 10 & & & & & & & & \\
\hline
20 & & & & 00 & & & & 10 & & & \\
21 & & & & & & & & & & & \\
22 & & & & & & & & & & & \\
23 & & & & & & & & & & &
\end{array}$$

$$C_2 = B_2 \otimes A_2$$

$$C_2 = \begin{array}{c|cccc|cccc|cccc}
00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 \\
02 & 03 & 00 & 01 & 12 & 13 & 10 & 11 & & & & \\
03 & 02 & 01 & 00 & 13 & 12 & 11 & 10 & & & & \\
01 & 00 & 03 & 02 & 11 & 10 & 13 & 12 & & & & \\
\hline
20 & 21 & 22 & 23 & 00 & & & & 10 & & & \\
22 & 23 & 20 & 21 & & & & & & & & \\
23 & 22 & 21 & 20 & & & & & & & & \\
21 & 20 & 23 & 22 & & & & & & & & \\
\hline
10 & & & & 20 & & & & 00 & & & \\
12 & & & & & & & & & & & \\
13 & & & & & & & & & & & \\
11 & & & & & & & & & & &
\end{array}$$

Demonstrar-se-á, de seguida, alguns teoremas que garantem a existência de pelo menos um par de MOLS de ordem n .

Proposição 1.18. Se $n \equiv 0,1,3 \pmod{4}$, tem-se que $N(n) \geq 2$.

Resta analisar-se o caso $n \equiv 2 \pmod{4}$ (conjetura de Euler). Assim para $n = 2(2k + 1)$, a menor potência de um número primo na fatorização de n é 2, e sabe-se que $N(2) = 1$. Então, a utilização do produto de Kronecker não é válida para este caso. Porém, foi provado que $N(10) \geq 2$, $N(14) \geq 3$ e $N(18) \geq 3$.

Em 1960 foi provado por Bose, Shrikhande e Parker o caso geral, o que está enunciado abaixo:

Teorema 1.19. Para todo n , exceto 2 e 6, existe pelo menos um par de MOLS de ordem n , isto é, para todo n , exceto 2 e 6, $N(n) \geq 2$.

O método do produto de Kronecker pode ser aplicado na construção de mais do que um par de MOLS. Mais especificamente, tem-se o seguinte resultado, que é um complemento do Teorema 1.13..

Teorema 1.20. Seja $q_1 \times \dots \times q_r$ a fatorização de n em potências de números primos distintas com $q_1 < \dots < q_r$. Então, $N(n) \geq q_1 - 1$.

Motivado pela conjetura de Euler, MacNeish conjeturou em 1922 o seguinte resultado:

Conjetura 1.21. Se $q_1 \times \dots \times q_r$ é a fatorização de n em potências de números primos distintos com $q_1 < \dots < q_r$, então $N(n) = q_1 - 1$.

Porém, sabe-se hoje que esta conjetura é falsa para muitos valores de n , mas ainda há muitos outros valores em que permanece desconhecido se $N(n) = q_1 - 1$, onde q_1 é a menor potência de um número primo na fatorização de n . Por exemplo, para $n \leq 100$, a conjetura de McNeish está em aberto para $n = 63,77,99$.

Considere-se, agora, a tabela dos valores já obtidos para limite inferior de $N(n)$ para $n < 100$.

	0	1	2	3	4	5	6	7	8	9
0	-	-	1	2	3	4	1	6	7	8
10	2	10	5	12	3	4	15	16	3	18
20	4	5	3	22	4	24	4	26	5	28
30	4	30	31	5	4	5	5	36	4	4
40	7	40	5	42	5	6	4	46	5	48
50	6	5	5	52	4	5	7	7	5	58
60	4	60	4	6	63	7	5	66	5	6
70	6	70	7	72	5	5	6	6	6	78
80	9	80	8	82	6	6	6	6	7	88
90	6	7	6	6	6	6	7	96	6	8

A tabela acima menciona números não superiores a $N(n)$, onde a entrada na linha x e coluna y corresponde a $N(x + y)$. Nela, pode-se observar que a conjectura citada anteriormente está errada para muitos casos. Assim, existem casos onde o número de MOLS ultrapassou o valor dado pelo produto de Kronecker e pelo Teorema 1.13..

1.6. ALGUNS RESULTADOS ADICIONAIS

Termine-se este capítulo com alguns resultados que não sendo necessários ao desenvolvimento geral da *teoria* de MOLS, proporcionam resultados úteis e interessantes.

Considere-se a simples questão: Como é que se determina se um dado quadrado latino tem companheiro ortogonal? Ou alternativamente, dado um quadrado latino L , existirá um quadrado latino M ortogonal a L ?

Nem todos os quadrados latinos têm companheiro ortogonal.

Considere-se o seguinte quadrado latino de ordem 4:

$$L_1 = \begin{matrix} & 0 & 1 & 2 & 3 \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{matrix} 1 \\ 3 \\ 2 \\ 3 \end{matrix} & \begin{matrix} 3 \\ 0 \\ 0 \\ 2 \end{matrix} & \begin{matrix} 0 \\ 3 \\ 3 \\ 1 \end{matrix} & \begin{matrix} 2 \\ 2 \\ 1 \\ 0 \end{matrix} \end{matrix}$$

Se L_1 tem companheiro ortogonal, este terá de ser da seguinte forma:

$$L_2 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & a & b & c \\ d & e & f & g \\ h & i & j & k \end{matrix} \quad \text{ou} \quad L_3 = \begin{matrix} 0 & 1 & 2 & 3 \\ 3 & p & q & r \\ s & t & u & v \\ w & x & y & z \end{matrix}$$

Se $a = 3$, então o par (3,3) ocorrerá em simultâneo nas posições (1,4) e (2,2) do quadrado $L_1 \odot L_2$. Assim, $a = 0$ e consequentemente $b = 3$ e $c = 1$, para que L_2 seja latino. Então o par ordenado (2,1) ocorrerá na posição (2,4) após a sobreposição dos quadrados L_1 e L_2 , logo $d = 3$. Assim, $e = 2$ e $i = 3$ para se manter a propriedade de latino. Mas, desta forma o par (2,3) ocorrerá nas posições (3,1) e (4,2) de $L_1 \odot L_2$, o que contradiz a ortogonalidade.

Similarmente, L_3 não poderá ser completado de forma a obtermos um quadrado latino ortogonal a L_1 , pois se $p = 0$ então $q = 1$ e $r = 2$ para que L_3 seja latino. Mas, assim o par (2,2) ocorrerá nas posições (1,3) e (2,4) de $L_1 \odot L_3$, o que contradiz a ortogonalidade. Logo, $p = 2$ e consequentemente, $q = 1$ ($q = 0$ faria ocorrer (0,0) em duas posições de $L_1 \odot L_3$) e $r = 0$, para que L_3 e L_1 sejam ortogonais. Se $s = 2$ então o par (2,2) ocorrerá simultaneamente nas posições (1,3) e (3,1) da sobreposição dos quadrados latinos L_3 e L_1 , logo $s = 1$ e $N = 2$. No entanto, para este caso, o par (3,2) ocorrerá nas posições (2,2) e (4,1), contrariando a propriedade de ortogonal.

Pelo exemplo anterior, prova-se que nem sempre um quadrado latino possui um companheiro ortogonal.

Considere as n posições de um quadrado latino L de ordem n , que contêm o mesmo símbolo i , para $1 \leq i \leq n$. Então, as entradas do segundo quadrado latino, M , que correspondem a essas n posições devem ser todas distintas entre si ou L não será ortogonal a M .

Como i ocorre exatamente uma vez em cada coluna e linha de L , então os n símbolos de M correspondentes aos i símbolos em L também terão de ocorrer uma vez em cada linha e em cada coluna.

Um conjunto de n símbolos distintos que verifique esta propriedade é chamado de **transversal de um quadrado latino**.

Assim, segue-se o seguinte teorema:

Teorema 1.22.: Um quadrado latino de ordem n tem companheiro ortogonal se e só se contém n transversais disjuntos.

Exemplo 1.23.: Considerem-se os quadrados latinos L e M ortogonais:

$$L = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix} \quad M = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

Atente nas 3 posições do quadrado latino L , que contêm o mesmo símbolo/cor 0, 1 ou 2. Tal como se pode verificar, as entradas do segundo quadrado latino, M , que correspondem a essas 3 posições são todas distintas entre si (em símbolo/cor). Cada conjunto de 3 posições dessas é um transversal de M . M tem 3 transversais disjuntas. E reciprocamente, a cada símbolo/cor do quadrado M corresponde um transversal do quadrado L , que tem também 3 transversais disjuntas.

Conclui-se que como L e M são ortogonais, então contém 3 transversais disjuntas.

Poder-se-á, também, questionar se um dado conjunto de MOLS pode ser estendido a um conjunto maior.

Teorema 1.24.: Para $n \geq 3$, a existência de um conjunto de $n - 2$ MOLS de ordem n implica a existência de um conjunto completo de $n - 1$ MOLS de ordem n .

De facto, Shrikhande provou que para $n > 4$, a existência de um conjunto de $n - 3$ MOLS de ordem n implica a existência de um conjunto completo de $n - 1$ MOLS de ordem n .

Um quadrado latino L designa-se por **auto-ortogonal** se L é ortogonal ao seu transposto, L^T .

Sabe-se que para $n \neq 2,3,6$ existe um quadrado auto-ortogonal de ordem n .

Exemplo 1.25.: Considere-se o seguinte quadrado latino L e o seu transposto L^T :

$$L = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix} \quad e \quad L^T = \begin{matrix} 0 & 2 & 3 & 1 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \end{matrix}$$

Calculando $L \odot L^T = \begin{matrix} (0,0) & (1,2) & (2,3) & (3,1) \\ (2,1) & (3,3) & (0,2) & (1,0) \\ (3,2) & (2,0) & (1,1) & (0,3) \\ (1,3) & (0,1) & (3,0) & (2,2) \end{matrix}$, conclui-se que L e L^T são ortogonais.

Logo, L é auto-ortogonal.

2. GRUPOS E QUADRADOS LATINOS

2.1. INTRODUÇÃO

Neste capítulo pretende-se relacionar a *teoria dos quadrados latinos* com a *teoria dos grupos*. Veremos que toda a tabela de Cayley de um grupo finito é um quadrado latino, mas o recíproco não é verdadeiro.

Definição 2.1. (*Grupoide*): Um grupoide é um conjunto não vazio com uma lei de composição interna, (G, \odot) .

Definição 2.2. (*Grupo*): Dado um conjunto não vazio G e uma operação binária $*$ nele definida, diz-se que G é um grupo em relação à operação $*$ se os seguintes axiomas são satisfeitos:

- i. $*$ é associativa, isto é, $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$;
- ii. Existe um elemento neutro para a operação $*$, isto é, $\exists e \in G$ tal que $a * e = e * a = a$, $\forall a \in G$;
- iii. Existe elemento inverso para todo o elemento de G , isto é, $\forall a \in G$, $\exists a' \in G$ tal que $a * a' = a' * a = e$.

Diz-se que o grupo G é comutativo (ou abeliano) quando satisfaz a seguinte propriedade adicional: $a * b = b * a$, $\forall a, b \in G$.

Exemplo 2.3.:

De seguida, apresentam-se alguns exemplos de grupos:

- $(R, +)$, onde R denota o conjunto dos números reais e $+$ a adição usual;
- $(\mathbb{Z}_n, +)$, onde \mathbb{Z}_n denota o conjunto dos inteiros $\{0, 1, \dots, n - 1\}$ e $+$ denota a adição módulo n ;
- $(F_q, +)$, onde F_q denota o corpo finito de ordem q (q é potência de um número primo) e $+$ a adição em F_q .
- (R^*, \times) , onde R^* representa o conjunto dos números reais não nulos e \times a multiplicação usual.

Definição 2.4. (*Grupo finito*): Um grupo finito é um grupo que contém um número finito de elementos. Se esse número é n , diz-se que G tem ordem n .

Exemplo 2.5.:

$(\mathbb{Z}_n, +)$, onde \mathbb{Z}_n denota o conjunto dos inteiros \mathbb{Z}_n e $+$ denota a adição módulo n .

Se M é um conjunto com n elementos distintos, a função $f: M \rightarrow M$ é uma permutação de M se f é bijetiva (injetiva e sobrejetiva)ⁱⁱ.

Finalmente, se f e g são ambas permutações de um conjunto M , pode-se definir uma terceira permutação h , chamada composta de f com g . Esta define-se por $h(x) = f(g(x))$, para $x \in M$.

Pode denotar-se uma permutação f usando duas linhas, onde a primeira contém os elementos de M ($i = 1, 2, \dots, n$) e a segunda contém as imagens $f(i)$, ou usando apenas a segunda linha.

Definição 2.6. (*Grupo das permutações ou grupo simétrico completo*): O conjunto de todas as permutações de um conjunto com n elementos constitui um grupo com respeito à composição de funções e designa-se por S_n (este é um grupo não comutativo).

Exemplo 2.7.: Se $M = \{1, 2, 3, 4\}$, considere-se a permutação $f: M \rightarrow M$ definida por $f(1) = 3$, $f(2) = 2$, $f(3) = 4$, $f(4) = 1$. A sua representação é dada por, $f \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, ou simplesmente por $(3 \ 2 \ 4 \ 1)$.

2.2. GRUPOS E QUADRADOS LATINOS

Considere-se o grupo $G = (\mathbb{Z}_5, +)$. De seguida mostra-se a tabela da operação (Tabela de Cayley) de, G em que $+$ denota a adição módulo 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Assim, 1 e 4 são opostos, assim como o 2 e 3. Adicionalmente, como a tabela é simétrica sobre a diagonal principal, verificamos que o grupo $(\mathbb{Z}_5, +)$ é comutativo.

ⁱⁱ A função f diz-se injetiva se para $a, b \in M$, $f(a) = f(b)$ implica que $a = b$. Por outro lado, f diz-se sobrejetiva se para todo o $d \in M$, existir um $c \in M$ tal que $f(c) = d$.

Teorema 2.8.: A tabela de multiplicaçãoⁱⁱⁱ de um grupo finito $(G,*)$ de ordem n é um quadrado latino de ordem n .

O recíproco do Teorema 2.8 nem sempre é verdadeiro, isto é, existem quadrados latinos que não representam tabelas de grupos de ordem n .

Exemplo 2.9.: Considere-se o seguinte quadrado latino,

1	2	3	4	5
2	5	4	1	3
3	1	2	5	4
4	3	5	2	1
5	4	1	3	2

Ao analisar este quadrado latino, se o encararmos como uma tabela de uma operação $*$, concluímos que há elemento neutro, o 1, mas $4 * 2 = 3 \neq 1 = 2 * 4$, isto é, verifica-se que não existe oposto para cada elemento.

Portanto, conclui-se que este quadrado latino não representa a tabela de um grupo de ordem 5.

Teorema 2.10.: Um quadrado latino pode sempre ser encarado como a tabela de multiplicação de um monoide (grupoide com elemento neutro).

Ideia da demonstração:

Por exemplo, o seguinte quadrado latino pode ser encarado como a tabela da operação $*$ de um grupoide $G = \{a, b, c, d\}$, em que o elemento neutro é a .

	a	c	d	b
a	a	c	d	b
c	c	d	b	a
b	b	a	c	d
d	d	b	a	c

ⁱⁱⁱ Ou tabela da operação.

Este quadrado latino pode ser reescrito de modo que a primeira coluna seja igual à primeira linha (basta para isso permutar as linhas). Trocando-se as linhas 3 e 4, obtém-se:

	a	c	d	b
a	a	c	d	b
c	c	d	b	a
d	d	b	a	c
b	b	a	c	d

Suponha-se, sem perda de generalidade, que a primeira linha e a primeira coluna são $\{1, 2, \dots, N\}$. O elemento neutro da operação definida será 1.

Teorema 2.11.: Um quadrado latino é a tabela de Cayley de um grupo se e só se a composta de quaisquer duas linhas do quadrado latino (encaradas como permutações) é ainda uma linha do quadrado latino.

Exemplo 2.12.: Considere-se o seguinte quadrado latino,

$$\begin{array}{l}
 \varphi_1 \rightarrow 1 \ 2 \ 3 \ 4 \ 5 \\
 \varphi_2 \rightarrow 2 \ 5 \ 4 \ 1 \ 3 \\
 \varphi_3 \rightarrow 3 \ 1 \ 2 \ 5 \ 4 \\
 \varphi_4 \rightarrow 4 \ 3 \ 5 \ 2 \ 1 \\
 \varphi_5 \rightarrow 5 \ 4 \ 1 \ 3 \ 2
 \end{array}$$

Verifica-se que $\varphi_3 \circ \varphi_2 \neq \varphi_{3*2} = \varphi_1$.

$$\text{De facto, } \varphi_3 \circ \varphi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}.$$

A permutação resultante não é nenhuma linha do quadrado latino.

Conclusão: Este quadrado latino não é a tabela de Cayley de um grupo.

Para se averiguar se um quadrado latino tem a estrutura de grupo, tem que se testar no máximo as n^2 compostas possíveis de duas linhas. Note-se que isto é mais simples que testar as n^3 igualdades do tipo $a * (b * c) = (a * b) * c$.

Uma generalização do conceito de quadrado latino leva-nos ao de quadrado latino linha.

2.3. QUADRADOS LATINOS LINHA

Um quadrado latino linha é uma matriz quadrada de ordem n em que cada linha é uma permutação de n elementos. Observe-se que um quadrado latino é um quadrado latino linha, mas o recíproco nem sempre é verdadeiro.

Considere-se o seguinte quadrado latino linha R de ordem 3,

$$\begin{array}{ccc} 2 & 1 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

Cada linha de R pode ser vista como a imagem de uma permutação do conjunto $M = \{1,2,3\}$, isto é, $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Assim, $(f_1, f_2, f_3) := R$, e de forma análoga pode-se usar esta representação para qualquer quadrado latino linha.

Agora vamos converter o conjunto de todos os quadrados latinos linha de ordem n num grupo. Denote-se por RL_n o conjunto de todos os quadrados latinos linha de ordem n com entradas em $M = \{1,2, \dots, n\}$ e define-se a operação $\cdot : RL_n \times RL_n \rightarrow RL_n$ que, a cada par $(A, B) \in RL_n \times RL_n$, faz corresponder $AB \in RL_n$ do seguinte modo:

Para $A \in RL_n$, assumamos que $A = (f_1, \dots, f_n)$, onde para cada $i = 1, 2, \dots, n$, f_i é a permutação que representa a linha i do quadrado latino A . Analogamente, assumamos que $B \in RL_n$ é representado por $B = (g_1, \dots, g_n)$. Assim, o produto dos quadrados latinos linha A e B , designado por AB , é dado por:

$$AB = (h_1, h_2, \dots, h_n),$$

onde para cada $i = 1, 2, \dots, n$, h_i é a composta de f_i com g_i , dada por $h_i(x) = f_i(g_i(x))$, para todo $x \in M$.

Exemplo 2.13.: Considere-se os seguintes quadrados latinos,

$$\begin{array}{ccc}
 2 & 1 & 3 \rightarrow f_1 \\
 A = 2 & 3 & 1 \rightarrow f_2 \\
 3 & 1 & 2 \rightarrow f_3
 \end{array}
 \quad e \quad
 \begin{array}{ccc}
 1 & 2 & 3 \rightarrow g_1 \\
 B = 3 & 2 & 1 \rightarrow g_2 \\
 2 & 1 & 3 \rightarrow g_3
 \end{array}$$

O produto dos quadrados latinos linha A e B , designado por AB , é dado por:

$$\begin{array}{ccc}
 2 & 1 & 3 \rightarrow h_1=f_1 \circ g_1 \\
 AB = 1 & 3 & 2 \rightarrow h_2=f_2 \circ g_2 \\
 1 & 3 & 2 \rightarrow h_3=f_3 \circ g_3
 \end{array}$$

Teorema 2.14.: (RL_n, \cdot) é um grupo de ordem $(n!)^n$.

2.4. CONJUNTOS DE QUADRADOS LATINOS LINHA ORTOGONAIS

De seguida são apresentados alguns resultados úteis na construção de conjuntos de quadrados latinos linha mutuamente ortogonais, que se definem de forma análoga à de quadrados latinos mutuamente ortogonais.

Lema 2.15.: Sejam $R \in RL_n$ e $E = (e, \dots, e)$, onde e denota a permutação identidade. E e R são ortogonais se, e só se, R é um quadrado latino.

Lema 2.16.: Seja $\{A_1, \dots, A_m\}$ um conjunto de quadrados latinos linha mutuamente ortogonais. Assim, para qualquer quadrado latino linha X , o conjunto $\{A_1X, \dots, A_mX\}$ é um conjunto de quadrados latinos linha mutuamente ortogonais.

Teorema 2.17.: Sejam A e B dois quadrados latinos linha. A e B são ortogonais se e só se existe um quadrado latino L tal que $LA = B$.

Exemplo 2.18.: Dado um quadrado latino linha A , podemos usar o teorema anterior para construir um quadrado latino linha ortogonal a A .

$$\begin{array}{ccc}
 1 & 2 & 3 \\
 \text{Seja } A = 2 & 1 & 3 \text{ (quadrado latino linha).} \\
 3 & 1 & 2
 \end{array}$$

1 2 3

Se fizermos $L = \begin{matrix} 2 & 3 & 1 \end{matrix}$ (quadrado latino).

3 1 2

1 2 3

Será $LA = \begin{matrix} 3 & 2 & 1 \end{matrix}$.

2 3 1

A e $B = LA$ são quadrados latinos linha ortogonais.

(1,1) (2,2) (3,3)

Verificação: $A \odot B = \begin{matrix} (2,3) & (1,2) & (3,1) \end{matrix}$.

(3,2) (1,3) (2,1)

3. GRAFOS

Conforme é do conhecimento público, a *Teoria dos Grafos* teve a sua origem, relativamente recente, no século XVIII.

Dentre os primeiros cientistas a trabalhar nesta área se destacam L. Euler, G. Kirchhoff e A. Cayley. A *teoria dos grafos* tem extensiva utilização em matemática aplicada, pois demonstra ser uma poderosa ferramenta para a modelagem de diversas situações reais em, entre outros, física, química, biologia, engenharia e investigação operacional.

O primeiro e mais famoso problema em *Teoria dos Grafos* foi resolvido por Euler em 1736, e derivou da resolução dos problemas que os habitantes de Königsberg (cidade da antiga Prússia conhecida, também, por Kaliningrad) enfrentavam nas suas deslocações pelas pontes que ligavam a cidade entre as duas ilhas do rio Pregel e entre estas ilhas e as margens opostas do referido rio. O desafio que se colocava a estes habitantes era o de descobrirem um percurso com início e fim num mesmo local sem se repetir a passagem em nenhuma dessas pontes.

Sentindo-se atraído por este desafio Leonard Euler (1707-1783) demonstrou a impossibilidade da existência de tal percurso fundamentando essa conclusão com o grafo representado na Figura 1.

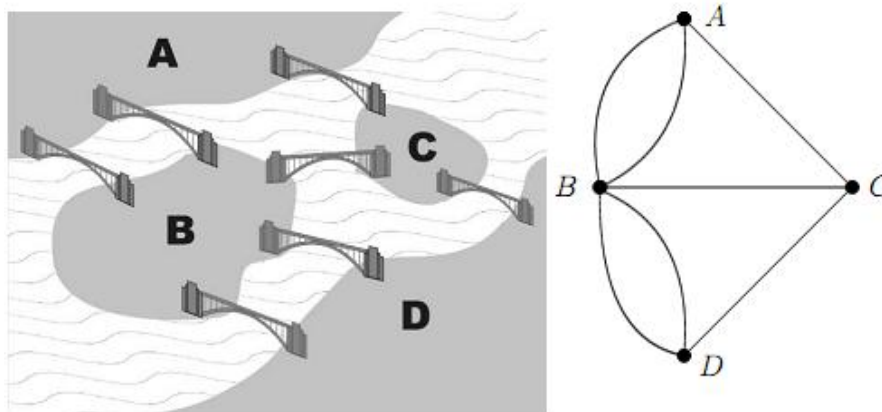


Figura 1 – Pontes de Königsberg em 1736 e respetivo grafo.

Assistiu-se posteriormente à formulação de novos e interessantes desafios e respetivas abordagens. Naquele que foi designado por “Viagem à Volta do Mundo”, Sir William Hamilton (1805-1865), demonstrou a existência de um trajeto com início e fim no mesmo vértice passando uma única vez por todos os vértices do dodecaedro representado na Figura 2.



Figura 2 – Dodecaedro (poliedro regular com 20 vértices de grau 3, 12 faces pentagonais e 30 arestas).

No “Problema das 4 cores”, um outro desafio de natureza combinatória, mas desta vez no âmbito da cartografia, a questão era descobrir o menor número de cores a utilizar num mapa sem que países com fronteira comum tivessem a mesma cor. Francis Guthrie, em 1852, estava convicto que 4 seriam as cores necessárias e suficientes. No entanto, em 1878, Cayley defendia, na “London Mathematical Society”, que este era um problema em aberto.

Desde então, novos e motivadores desafios de carácter combinatório e respetivas abordagens, conceitos e resultados, transformaram a *teoria dos grafos* numa área da matemática extremamente motivadora.

3.1. Conceitos Básicos

Neste capítulo introduzem-se definições e notações básicas da *teoria dos Grafos* e respetiva notação, uma vez que quer as terminologias quer as notações não são únicas.

Definição 3.1. (*Grafo simples e não orientado*): Um *grafo* é um conjunto não vazio V com uma relação binária simétrica E nele definida. Os elementos de V serão designados por vértices e os elementos de E (que são pares não ordenados de vértices) serão designados por arestas.

Designaremos por $G = (V, E)$ um *grafo* em que o conjunto de vértices é V e o conjunto de arestas é E .

Os *grafos* são muitas vezes representados por figuras planas constituídas por pontos representando vértices e linhas representando arestas.

Exemplo 3.2.: Seja $G = (V, E)$ onde $V = \{a, b, c, d\}$ e $E = \{\{a, b\}\{b, c\}\{c, d\}\{a, c\}\}$. Então, G pode ser representado por:

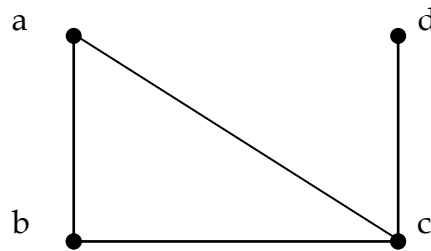


Figura 3 – Representação de um grafo.

Definição 3.3. (*Subgrafo*): Um *subgrafo* de $G = (V, E)$ é um *grafo* cujo conjunto de vértices é um subconjunto V' de V e o conjunto de arestas é um subconjunto de E constituído por pares de elementos de V' .

Definição 3.4. (*Subgrafo gerador*): Um *subgrafo gerador* de G é um subgrafo de G que contém todos os vértices de G .

Dois vértices são *adjacentes* ou *vizinhos* quando são extremidades de uma aresta. Analogamente, duas arestas distintas incidentes no mesmo vértice são chamadas *adjacentes*.

O número de vértices de um grafo designa-se por *ordem* do grafo.

O número de arestas que incidem em cada vértice designa-se por *grau* desse vértice.

Definição 3.5. (*Grafo regular*): Um *grafo* diz-se *regular* se todos os seus vértices tiverem o mesmo grau, isto é, de todos os seus vértices tiverem o mesmo número de arestas a incidir nele.

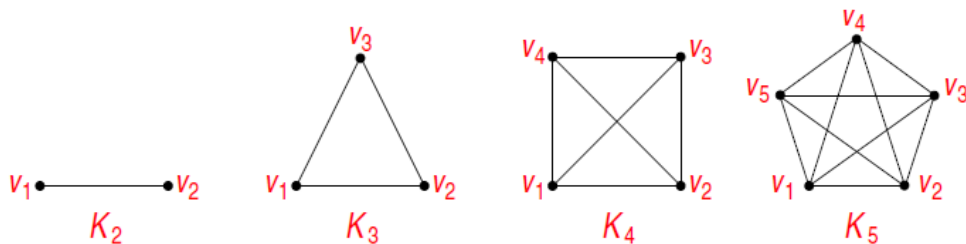


Figura 4 – Grafos completos com 2, 3, 4, e 5 vértices são grafos regulares.

Definição 3.6. (*Grafo fortemente regular*): Um *grafo fortemente regular* é um *grafo regular* em que para todos os pares de vértices adjacentes existe um número λ fixo de vértices adjacentes a ambos, e para qualquer par de vértices não adjacentes existe um número fixo μ de vértices adjacentes a ambos.

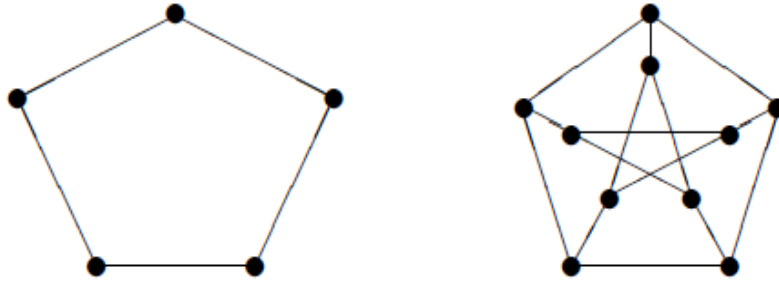


Figura 5 – Grafos fortemente regulares com parâmetros $(5; 2; 0; 1)$ e $(10; 3; 0; 1)$, respectivamente.

Um *grafo fortemente regular* (n, r, λ, μ) é um *grafo regular* de ordem n , em que todos os vértices tem grau r e parâmetros λ e μ .

Definição 3.7. (*Grafo completo*): Designa-se por *grafo completo* (nulo) de ordem n e denota-se por K_n um grafo com n vértices adjacentes dois a dois (não adjacentes, ou seja, sem qualquer aresta).

Definição 3.8. (*Grafo bipartido*): Um *grafo bipartido* é um grafo $G = (V, E)$ onde o conjunto de vértices V pode ser particionado em dois subconjuntos $U = \{U_1, U_2, \dots, U_m\}$ e $W = \{W_1, W_2, \dots, W_n\}$ tais que toda a aresta é do tipo $\{U_i, W_j\}$, ou seja, não há nenhuma aresta a unir vértices do mesmo subconjunto.

Definição 3.9. (*Grafo bipartido completo*): Um *grafo bipartido* em que $|U| = |W| = n$ é *completo* se cada vértice de U se encontra ligado a cada vértice de W e é representado por $K_{n,n}$.

Definição 3.10. (*Fatorização de grafos*): Um grafo $G = (V, E)$ admite uma *t-fatorização* se o seu conjunto de arestas, E , admite uma partição em l *t-fatores* disjuntos.

Um *t-fator* de um grafo $G = (V, E)$ é um subgrafo gerador *t-regular*.

Em particular, um *1-fator* de um grafo $G = (V, E)$ é um grafo cujo conjunto de vértices é o próprio conjunto V (*subgrafo gerador*) e cujo conjunto das arestas é um subconjunto de E , tal que em cada vértice incide exatamente uma aresta desse subconjunto.

Se E pode ser particionado em subconjuntos disjuntos de modo que cada subconjunto corresponda a um *1-fator* de G , G diz-se *1-fatorizável*.

Exemplo 3.11.: Assim, o exemplo que de segue retrata o descrito acima para o caso de $l=2$ e $t=2$.

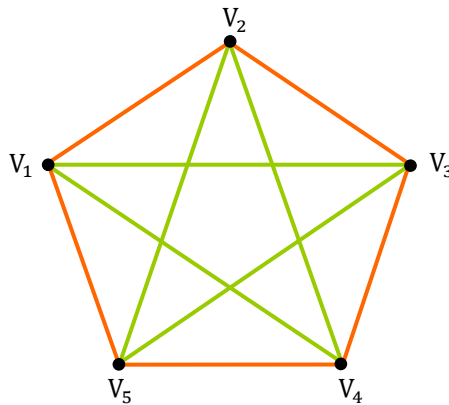


Figura 6 – Grafo completo de ordem 5 com uma *2-fatorização*.

O grafo K_5 admite uma *2-fatorização* em dois *2-fatores*:

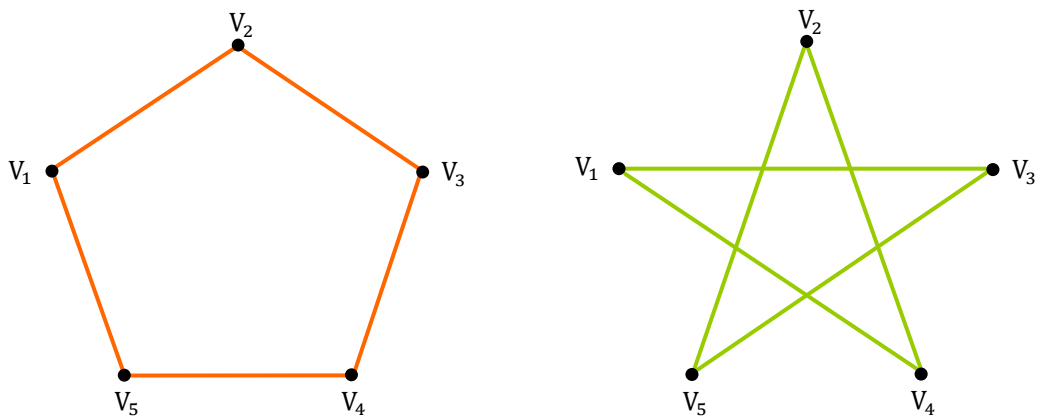


Figura 7 – Decomposição em dois *2-fatores* do grafo K_5 .

O exemplo seguinte ilustra o caso de um grafo bipartido *1-fatorizável* em dois *1-fatores*:

Exemplo 3.12.: O conjunto de arestas do *grafo* seguinte admite uma partição em 2 subconjuntos tais que em cada vértice incidem exatamente duas arestas, uma de cada subconjunto. A cada subconjunto de arestas corresponde um *1-fator*.

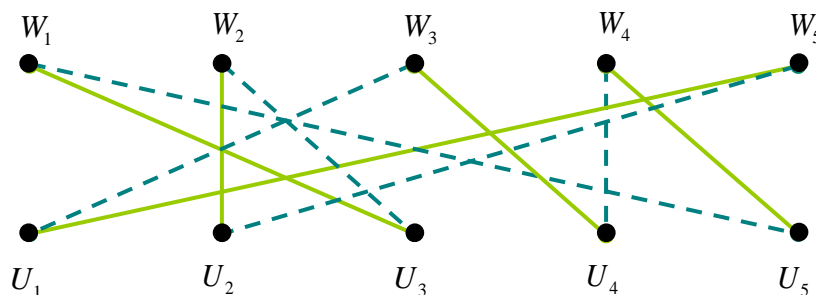


Figura 8 – Grafo G e a sua *1-fatorização*.

Definição 3.13. (*Matriz de adjacência de um grafo*): Uma *matriz* cujas entradas mostram a *adjacência* entre vértices de um grafo é conhecida como *matriz de adjacência do grafo*.

Se apenas estamos interessados na existência ou ausência de aresta, a matriz será de 1's e 0's. Se, para além, da existência de aresta estivermos interessados na sua cor, distância ou custo que representa, a matriz de adjacência terá outros símbolos em vez do 1.

Definição 3.14. (*Grafos dirigidos ou digrafos*): Um *grafo dirigido* ou *digrafo* é um conjunto não vazio V com uma relação binária não necessariamente simétrica E nele definida. Os elementos de $E \subseteq V^2$ (que são pares ordenados de vértices) serão designados por arcos.

Interprete-se um *lacete*, que é uma aresta que sai de um vértice para o mesmo vértice, como representando simultaneamente duas arestas, uma para dentro e outra para fora do vértice.

Definição 3.15. (*Grafos dirigidos completos*): Designa-se por \overrightarrow{K}_n o *grafo dirigido completo com lacetes* em n vértices, ou seja, o grafo que possui uma aresta dirigida do vértice V_i para o vértice V_j , para qualquer par (V_i, V_j) de vértices não necessariamente distintos.

Designa-se por \overrightarrow{K}'_n , um *grafo dirigido completo sem lacetes*.

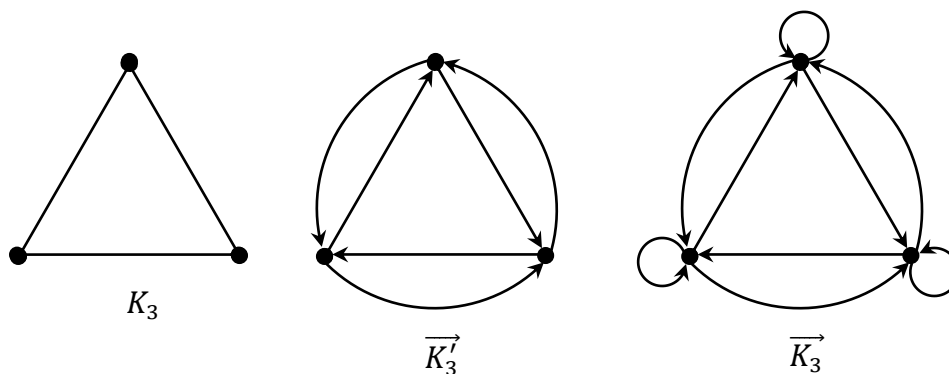


Figura 9 – Grafos completos com três vértices

Definição 3.16. (*Passeio*): Designa-se por *passeio* num grafo G , entre dois vértices x e y , toda a sequência de vértices e arestas $x = v_1, v_1v_2, v_2, \dots, v_{k-1}, v_{k-1}v_k, v_k = y$, com eventual repetição de vértices e arestas.

Definição 3.17. (*Trajeto e Circuito*): Um *trajeto* num grafo G entre dois vértices é um *passeio* entre esses mesmos vértices sem arestas repetidas (podendo, no entanto, existir vértices repetidos).

Um *trajeto* designa-se por **trajeto de Euler** se contém todas as arestas do grafo.

Os *trajetos fechados* (onde o vértice final coincide com o inicial) designam-se por *circuitos*.

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 **trajeto de Euler fechado**.

Definição 3.18. (*Caminho e Ciclo*): Um *caminho* entre dois vértices é um *trajeto* sem vértices repetidos.

Um caminho que contém todos os vértices de um grafo será chamado de *caminho Hamiltoniano*.

Um *ciclo* é um caminho fechado, ou seja, inicia e termina no mesmo vértice.

Um ciclo que contém todos os vértices de um grafo será chamado de *ciclo Hamiltoniano*.

Também se podem definir de modo análogo *trajetos*, *circuitos*, *caminhos* e *ciclos* em grafos orientados.

Exemplo 3.19.: Considere-se o seguinte *grafo*:

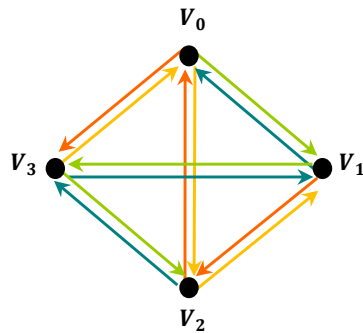


Figura 10 – Quatro caminhos Hamiltonianos

Cada cor (verde, laranja, azul e amarelo) corresponde a um *caminho Hamiltoniano* no *grafo dirigido*, isto é, V_0, V_1, V_3, V_2 , V_1, V_2, V_0, V_1 , V_2, V_3, V_1, V_0 e V_3, V_0, V_2, V_1 são os quatro *caminhos Hamiltonianos* do *grafo*.

Definição 3.20. (*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 *trajeto 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 1 é ou não *Euleriano*.

Exemplo 3.21: Demonstrar-se-á que, se um *grafo* G é *Euleriano*, então todos os vértices têm grau par.

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, vem que 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.

4. Grafos e Quadrados Latinos

4.1. Quadrados Latinos e Grafos Bipartidos

Uma conexão entre a estrutura relativamente simples de um grafo e a estrutura mais intrincada de um quadrado latino não é inicialmente óbvia.

A interpretação de cada símbolo que ocorre num quadrado latino como uma cor associada a uma aresta de um grafo tornará mais natural essa ligação, como veremos.

Considerando que um *grafo* G consiste num conjunto não vazio de elementos, V , que designaremos por vértices e num subconjunto E de pares de vértices, que designaremos por arestas, como vimos anteriormente, e sabendo que, um *grafo bipartido* é um grafo $G = (V, E)$ onde o conjunto de vértices V pode ser particionado em dois subconjuntos $U = \{U_1, U_2, \dots, U_m\}$ e $W = \{W_1, W_2, \dots, W_n\}$ tais que toda a aresta é do tipo $\{U_i, W_j\}$, ou seja, não há nenhuma aresta a unir vértices do mesmo conjunto.

Suponha-se que $|U| = |W|$ e que U e W representam respetivamente, as linhas (i) e colunas (j) de um quadrado latino L de ordem n .

Se o símbolo na posição (i, j) de L é k , então uma aresta de cor $k = 1, 2, \dots, n$ unirá os vértices U_i e W_j , e como L é um quadrado latino, claramente $L = (V, E)$ é um grafo bipartido especial, porque é completo e em cada vértice incide uma aresta de cada cor.

2 1 3

Exemplo 4.1.: Dado o *quadrado latino* $L = \begin{matrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{matrix}$, este pode ser representado através do

1 3 2

seguinte grafo bipartido:

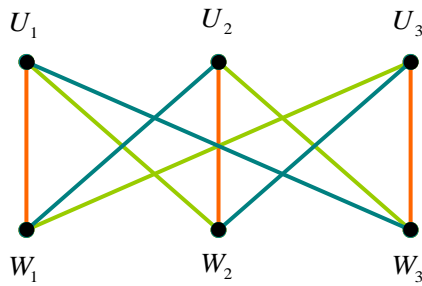


Figura 11 – Grafo bipartido de um quadrado latino.

onde, 1 – verde, 2 – laranja e 3 – azul e $U = \{U_1, U_2, U_3\}$ e $W = \{W_1, W_2, W_3\}$ correspondem às linhas e colunas de L , respectivamente.

Assim, o grafo bipartido associado a um quadrado latino de ordem n é um $K_{n,n}$ em que cada aresta é colorida com uma das n cores presentes no quadrado latino e em cada vértice incide exatamente uma aresta de cada cor.

Um quadrado latino linha de ordem n pode ser representado por um grafo bipartido completo em que $|U| = |W| = n$ e tal que em cada vértice correspondente às linhas incide exatamente uma aresta de cada cor. Contudo, nos vértices correspondentes às colunas podem incidir arestas da mesma cor.

2 1 3

Exemplo 4.2.: Dado o quadrado latino linha $L = \begin{matrix} 2 & 3 & 1 \\ 1 & 3 & 2 \end{matrix}$, este pode ser representado através do

1 3 2

grafo bipartido:

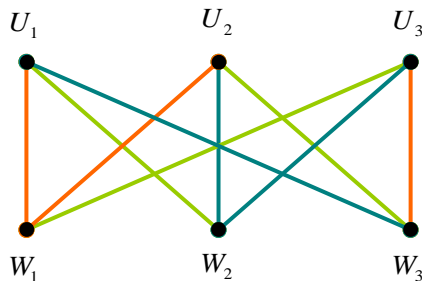


Figura 12 – Grafo bipartido de um quadrado latino linha.

onde, 1 – verde, 2 – laranja e 3 – azul e $U = \{U_1, U_2, U_3\}$ e $W = \{W_1, W_2, W_3\}$ correspondem às linhas e colunas de L , respectivamente.

O exemplo seguinte poderá espelhar uma situação real se se considerar os W_i uma fonte de abastecimento do produto i (por exemplo, gás, água e luz) e os U_i os estabelecimentos que as recebem.

Exemplo 4.3.: Dado o *quadrado latino linha* $L = \begin{matrix} & 1 & 2 & 3 \\ 1 & 2 & 3 & \\ & 1 & 2 & 3 \end{matrix}$, este pode ser representado através do grafo bipartido:

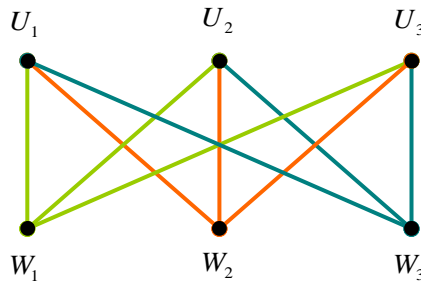


Figura 13 – Grafo bipartido de um quadrado latino linha.

onde, 1 – verde, 2 – laranja e 3 – azul e $U = \{U_1, U_2, U_3\}$ e $W = \{W_1, W_2, W_3\}$ correspondem às linhas e colunas de L , respectivamente.

De acordo com o definido anteriormente, um grafo admite uma *t-fatorização* se o seu conjunto de arestas, admite uma partição em l *t-fatores* disjuntos, sendo um *t-fator* de um grafo um subgrafo gerador *t-regular*.

Um *1-fator* de um grafo é um grafo cujo conjunto de vértices é o próprio conjunto V e cujo conjunto das arestas é um subconjunto de E , tal que em cada vértice incide exatamente uma aresta desse subconjunto. Se E pode ser particionado em subconjuntos disjuntos de modo que cada subconjunto corresponda a um *1-fator* diz-se *1-fatorizável*.

Contudo, o *grafo bipartido* associado a um *quadrado latino linha* não é necessariamente *1-fatorizável* como mostra o exemplo 4.2..

Podemos assim concluir:

Teorema 4.4.: Um quadrado latino L de ordem n é equivalente a uma *1-fatorização* de um $K_{n,n}$.

Demonstração. Seja L um quadrado latino de ordem n . Representemos por $U = \{U_1, U_2, \dots, U_n\}$ as linhas de L e por $W = \{W_1, W_2, \dots, W_n\}$ as colunas de L .

Consideremos um grafo cujo conjunto de vértices é $V = U \cup W$.

Se em L o símbolo na posição (i, j) é k , então uma aresta de cor k ligará U_i a W_j . Assim, o grafo é bipartido, completo, e em cada vértice incide uma aresta de cada cor.

Lembrando que L é um quadrado latino, cada símbolo k origina um 1 -fator monocromático, isto é, um 1 -fator cujas arestas são todas da mesma cor.

Reciprocamente, consideremos G um $K_{n,n}$ cujas arestas são coloridas, cada uma com uma de n cores, de modo que exista uma 1 -fatorização de G em n 1 -fatores monocromáticos.

Atendendo à regra de construção de quadrados latinos à custa de grafos do tipo $K_{n,n}$, considere-se o símbolo k na posição (i, j) de um quadrado $n \times n$, se existe uma aresta de cor k a unir os vértices U_i e W_j (o que é sempre possível uma vez que o grafo é do tipo $K_{n,n}$); claramente, cada linha e coluna contém cada símbolo exatamente uma vez (pois se se supuser que na linha i , k aparece duas vezes, isso significa que no vértice U_i incidem duas arestas de cor k , o que contraria a hipótese de o grafo ser 1 -fatorizável; analogamente para as colunas). ■

O teorema que se segue dá uma interpretação em termos de *teoria dos grafos* da condição necessária e suficiente para a existência de *companheiro ortogonal* de um *quadrado latino*.

Mas agora estamos interessados numa 1 -fatorização do grafo bipartido associado, tal que cada 1 -fator, em vez de ser monocromático como no Teorema 4.4., tem agora uma aresta de cada cor.

Tal como foi referido no capítulo introdutório um *quadrado latino de ordem n* tem *companheiro ortogonal* se e só se contém n *transversais disjuntas*, isto é, considerando as n posições de um quadrado latino de ordem n , que contêm o mesmo símbolo i , para $1 \leq i \leq n$, as entradas do segundo quadrado latino, correspondentes a essas n posições devem ser todas distintas entre si.

Teorema 4.5.: Um *quadrado latino L de ordem n* , tem um *companheiro ortogonal* se e só se existe uma 1 -fatorização do grafo associado $K_{n,n}$ tal que cada 1 -fator contém uma aresta de cada cor.

Demonstração. Um *quadrado latino* que possua um *companheiro ortogonal* pode ser decomposto em n *transversais disjuntas*. Como cada *transversal* contém uma entrada em cada linha e coluna, as arestas associadas a cada posição formam um *1-fator* do *grafo bipartido*.

Como cada símbolo ocorre em cada *transversal*, cada *1-fator* contém uma aresta de cada cor.

Reciprocamente, se um *quadrado latino* for construído a partir de um *grafo bipartido*, com uma *1-fatorização* nas condições descritas, então os n *1-fatores* originarão um conjunto de *transversais disjuntas* (cada *1-fator* origina um *transversal*) que coletivamente contêm todas as n^2 posições do quadrado.

Portanto, cada *quadrado latino* construído à custa de um *grafo bipartido* deste tipo possui um *quadrado latino companheiro ortogonal*. ■

O exemplo que segue retrata o teorema anterior.

Exemplo 4.6.: Consideremos o *quadrado latino* $L = \begin{matrix} & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 2 & 3 \end{matrix}$ que pode ser representado através do *grafo bipartido*:

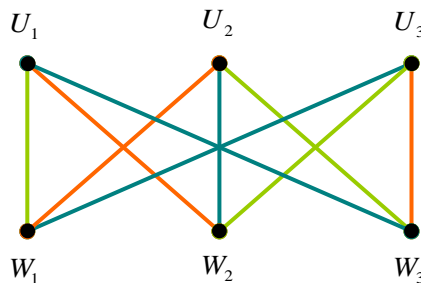


Figura 14 – Grafo bipartido de um quadrado latino.

onde, 1 – verde, 2 – laranja e 3 – azul e $U = \{U_1, U_2, U_3\}$ e $W = \{W_1, W_2, W_3\}$ correspondem às linhas e colunas de L , respectivamente.

Seja $M = \begin{matrix} & 1 & 2 & 3 \\ 1 & 3 & 1 & 2 \\ 2 & 2 & 3 & 1 \\ 3 & 1 & 2 & 3 \end{matrix}$ o *companheiro ortogonal* de L que pode ser representado através do *grafo bipartido*:

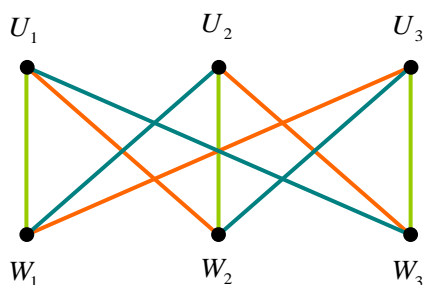


Figura 15 – Grafo bipartido do companheiro ortogonal do quadrado latino anterior.

onde, 1 – verde, 2 – laranja e 3 – azul e $U = \{U_1, U_2, U_3\}$ e $W = \{W_1, W_2, W_3\}$ correspondem às linhas e colunas de M , respectivamente.

Os três 1 -fatores do grafo completo bipartido $K_{3,3}$ associado a L , em que cada aresta é de sua cor são:

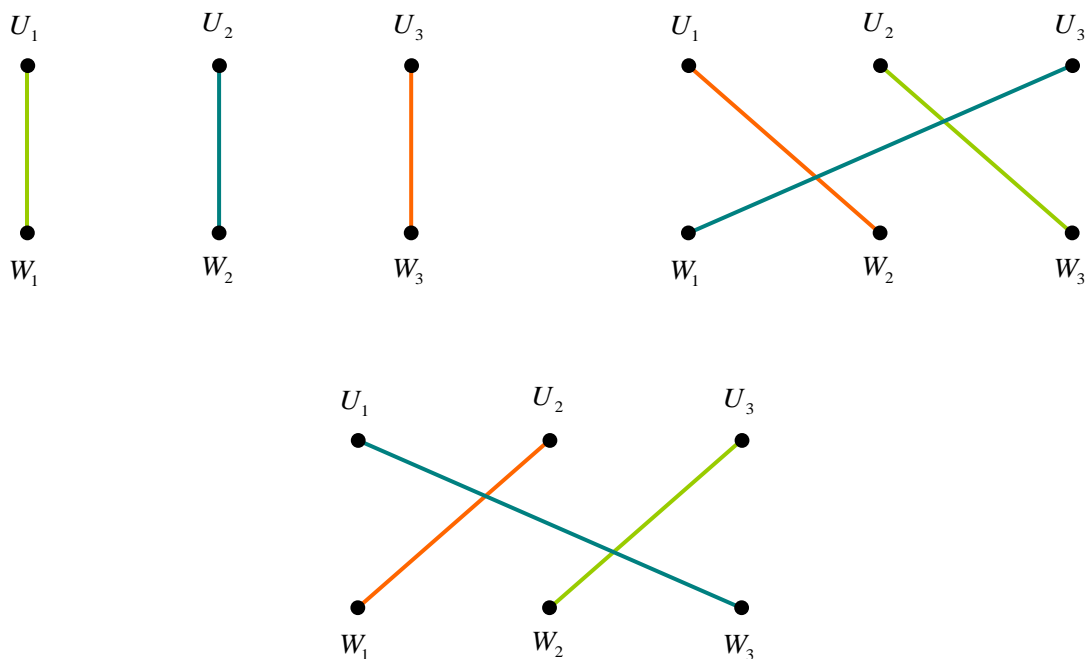


Figura 16 – Três 1 -fatores do grafo completo bipartido $K_{3,3}$ associado a L .

Cada um destes 1 -fatores corresponde a um dos três 1 -fatores monocromáticos do grafo $K_{3,3}$ associado a M , companheiro ortogonal de L , o primeiro ao verde, o segundo ao laranja e o terceiro ao azul.

O que podemos concluir para o caso de um quadrado latino que não tem companheiro ortogonal? O exemplo seguinte realça esse aspecto.

Exemplo 4.7.: Consideremos o quadrado latino $L = \begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}$ que pode ser representado através do grafo bipartido:

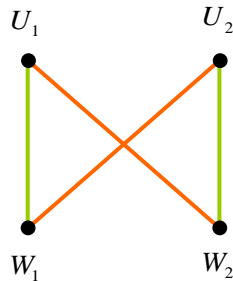


Figura 17 – Grafo bipartido do quadrado latino L.

onde, 1 – verde e 2 – laranja e $U = \{U_1, U_2\}$ e $W = \{W_1, W_2\}$ correspondem às linhas e colunas de L, respectivamente.

A 1-fatorização do grafo $K_{2,2}$ associado a L, só tem 1-fatores monocromáticos. Pois não existem 1-fatores em que cada aresta seja de sua cor.

Se associarmos da mesma forma um grafo bipartido a um retângulo latino de r linhas e n colunas, onde $r \leq n$, o grafo obtido é representado por $K_{r,n}$ em que cada aresta é colorida com uma das n cores, tal que em cada vértice incide uma aresta de cada cor (n arestas no caso dos r vértices correspondentes às linhas, r arestas no caso dos n vértices correspondentes às colunas), como se pode observar no exemplo que se segue:

1 3 4 2 5

Exemplo 4.8.: Dado o retângulo latino $R = \begin{matrix} 4 & 1 & 3 & 5 & 2 \\ 2 & 4 & 5 & 1 & 3 \end{matrix}$, este pode ser representado através do

2 4 5 1 3

grafo bipartido:

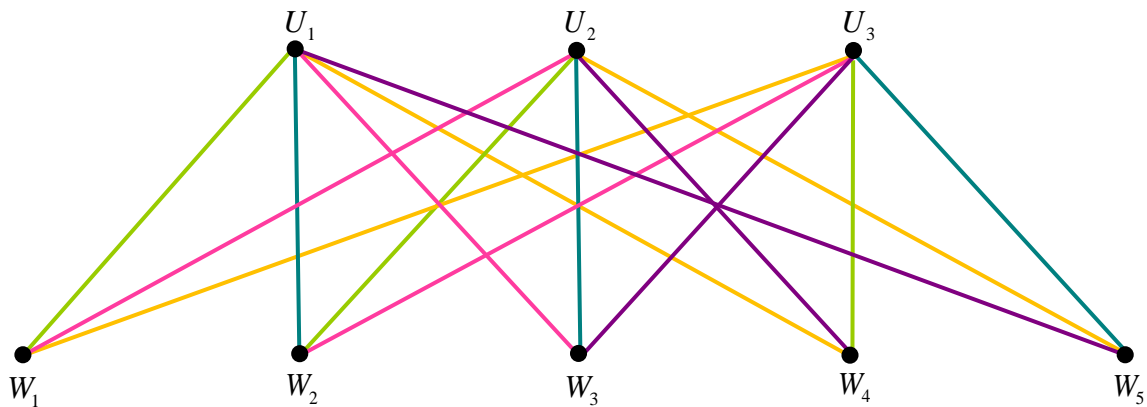


Figura 18 – Grafo bipartido de um retângulo latino.

onde, 1 – verde, 2 – amarelo, 3 – azul, 4 – rosa, 5 – violeta e $U = \{U_1, U_2, U_3\}$ e $W = \{W_1, W_2, W_3, W_4, W_5\}$ correspondem às linhas e colunas de R , respetivamente.

Vamos agora utilizar um grafo que nos ajude a resolver o problema de completar um *retângulo latino* de forma a obter-se um *quadrado latino*, também ele *latino*. Interessar-nos-á evidenciar no grafo associado as ausências de símbolos nas colunas do retângulo latino.

Qualquer *retângulo latino* $r \times n$, com $r \leq n$, pode ser completado de modo a obter um *quadrado latino de ordem* n , pela adição de $n - r$ linhas.

Para esta finalidade alteraremos um pouco a representação precedente de um *retângulo latino* por um *grafo bipartido completo*.

Agora, identificar-se-á um *retângulo latino*, R , de $r \times n$, por um *grafo bipartido* $G(R)$ com $|U| = |W| = n$, onde U e W representam, respetivamente, as colunas de R e os n elementos do *retângulo latino* e em que a aresta $\{U_i, W_j\}$ está presente se a coluna i de R não contém o símbolo j .

Em cada vértice incidem $n - r$ arestas.

O próximo exemplo ilustra a construção descrita acima no caso de $r = 3$ e $n = 5$.

Exemplo 4.9.: Considere-se o seguinte *retângulo latino*:

$$R = \begin{matrix} & 1 & 3 & 4 & 2 & 5 \\ 1 & & & & & \\ 2 & & & & & \\ 3 & & & & & \end{matrix}$$

O grafo associado ao mesmo será representado por:

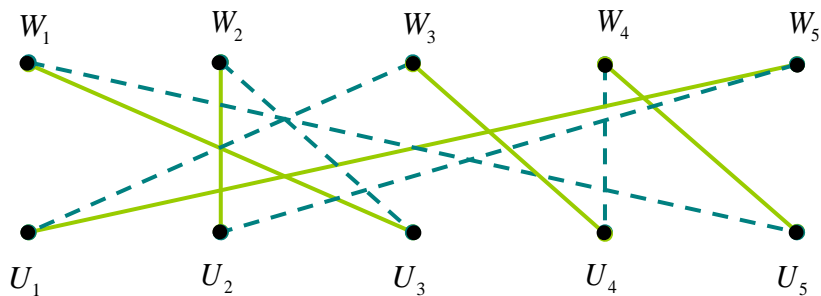


Figura 19 – 1-fatorização de um grafo bipartido $G(R)$.

Adicionar uma nova linha a R é equivalente a determinar um 1 -fator do grafo bipartido associado.

No exemplo acima a linha $(3 \ 5 \ 2 \ 4 \ 1)$ corresponde ao 1 -fator do grafo $G(R)$, ilustrado na figura anterior, considerando o tracejado azul dos U_i para os W_j .

Na 1 -fatorização do grafo bipartido associado desta forma ao retângulo latino, cada um dos $n - r$ 1 -fatores gera uma nova linha adicional no retângulo latino.

Tomando estas linhas adicionais obtemos um quadrado latino.

$$R = \begin{matrix} & 1 & 3 & 4 & 2 & 5 \\ & 4 & 1 & 3 & 5 & 2 \\ 2 & 4 & 5 & 1 & 3 & \\ & 3 & 5 & 2 & 4 & 1 \\ & 5 & 2 & 1 & 3 & 4 \end{matrix}$$

Para provar que o quadrado resultante é um quadrado latino recorre-se ao seguinte lema:

Lema 4.10.: Num retângulo latino R , $r \times n$, com $r \leq n$, existem pelo menos k símbolos que não aparecem em todas as colunas de qualquer conjunto de $k \leq n$ colunas, embora possam aparecer em algumas delas.

Demonstração. Seja S_i , $i = 1, 2, \dots, n$ o conjunto dos $n - r$ símbolos ausentes na coluna i de R . Cada símbolo ocorre exatamente uma vez em cada linha de R , com um total de r ocorrências, portanto cada símbolo está ausente em $n - r$ colunas. Neste caso, estar ausentes nas colunas implicará estar presente nos S_i 's.

Se k , $1 \leq k \leq n$, colunas são selecionadas, os S_i 's associados conterão no máximo $k(n - r)$ símbolos, ou seja, cada S_i tem $n - r$ símbolos e adicionando as k colunas temos o total de $k(n - r)$ símbolos, não necessariamente distintos.

Uma vez que cada símbolo ocorre exatamente $n - r$ vezes no conjunto de todos os S_i 's, porque cada símbolo tem de ocorrer uma e uma só vez em cada uma das linhas que faltam, nenhum símbolo ocorre mais do que $n - r$ vezes entre os k S_i 's selecionados e pelo menos k dos $k(n - r)$ símbolos presentes nos k S_i 's selecionados são distintos. O Lema diz que no grafo $G(R)$ qualquer conjunto de k U_i 's é *coletivamente adjacente*^{iv} a pelo menos k dos W_j 's onde $k \leq n$. ■

Observação: O lema anterior não é aplicável a *retângulos latinos linha*, pois apenas temos de garantir o facto de os elementos serem distintos por linha.

No exemplo anterior se tomarmos $k = 3$ as colunas 1, 2 e 3 admitem quatro símbolos distintos ausentes, a saber: 5, 3, 1, 2. O Lema garante que há pelo menos 3 símbolos distintos ausentes de alguma de 3 colunas escolhidas arbitrariamente, num quadrado latino.

Lema 4.11.: Sejam $r < n$ inteiros positivos. Dado um *retângulo latino* R , $r \times n$, podemos sempre adicionar-lhe uma linha de forma a obtermos um *retângulo latino* R' , $(r + 1) \times n$.

A demonstração deste Lema usa o Lema 4.10. e o método de indução sobre o conjunto dos vértices, U , do grafo $G(R)$ associado ao *retângulo latino*.

Uma vez que a determinação de cada 1 -fator origina uma nova linha do *retângulo latino*, a repetição do processo $n - r$ vezes completa a 1 -fatorização de $G(R)$ estendendo assim o *retângulo* a um *quadrado latino*. Desta forma surge o seguinte corolário:

Corolário 4.12.: Se $r < n$, qualquer *retângulo latino* $r \times n$ pode ser completado num *quadrado latino de ordem* n , pela adição de $n - r$ linhas.

Observação: Dado um *retângulo latino* $r \times n$, com r linhas e n colunas onde $r \leq n$, existem sempre $(n - r)!$ formas de se obter um *quadrado latino* e $(n!)(n - r)!$ formas de se obter um *quadrado latino linha*.

^{iv} Um conjunto de vértices diz-se coletivamente adjacente a outro se cada vértice do primeiro conjunto tem ligação a cada vértice do segundo.

4.2. Quadrados Latinos e Fatorização de Grafos e Digrafos Completos

No que se segue iremos determinar o número de 1 -fatorizações de grafos e digrafos completos não bipartidos, utilizando quadrados latinos como matriz de adjacência de tais grafos.

Recorde-se que a matriz de adjacência de um grafo é uma matriz cujas entradas mostram a adjacência entre vértices desse mesmo grafo.

Para começar, considere-se o quadrado latino $L = \begin{matrix} & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}$ que pode, enquanto matriz,

decompor-se em $L = L_1 + L_2 + L_3 + L_4$, com

$$L_1 = \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}, \quad L_2 = \begin{matrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{matrix}, \quad L_3 = \begin{matrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{matrix}, \quad L_4 = \begin{matrix} 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 4 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{matrix}.$$

Cada matriz L_1, \dots, L_4 é a matriz de adjacência de um digrafo (grafo dirigido), como se pode observar na figura, supondo que a cada símbolo está associada uma cor:

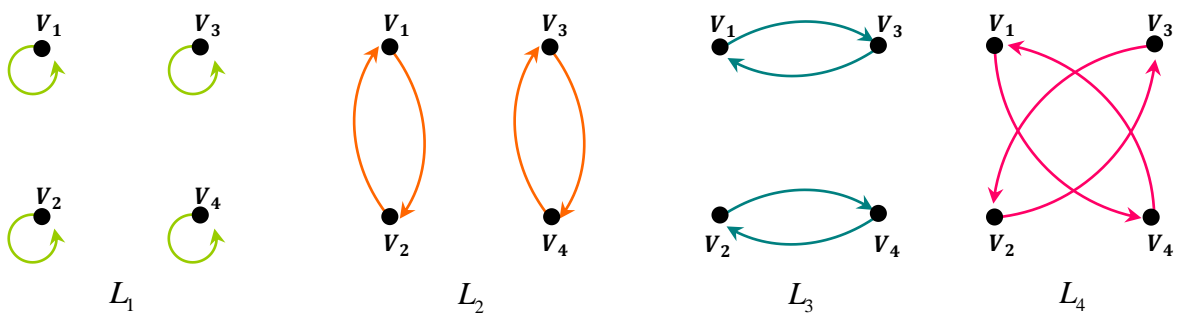


Figura 20 – 1-fatorização de um grafo dirigido completo

Enquanto a adição das quatro matrizes origina um *quadrado latino de ordem quatro*, a sobreposição dos *quatro grafos* associados origina um *grafo* com as seguintes propriedades:

1. Tem uma aresta dirigida do vértice V_i para o vértice V_j , para $i, j = 1, 2, 3, 4$ (ou seja, é um *digrafo completo*)
2. A cada aresta está associada uma de quatro cores;
3. Existe exatamente uma aresta de cada cor que entra/sai em/de cada vértice.

Interprete-se um *lacete*, que é uma aresta que sai de um vértice para o mesmo vértice, como sendo simultaneamente uma aresta para dentro e para fora do vértice.

Para *quadrados latinos linha* verificam-se as duas primeiras propriedades acima enunciadas, porém não é verificado o facto de existir exatamente uma aresta de cada cor que entra/sai em/de cada vértice, como observaremos no exemplo abaixo.

Exemplo 4.13.: Considerando o *quadrado latino linha* $L = \begin{matrix} 2 & 1 & 3 \\ 1 & 2 & 3 \\ 3 & 2 & 1 \end{matrix}$ e tomando 1 – verde, 2 – laranja e 3 – azul, obtemos o seguinte *grafo dirigido*:

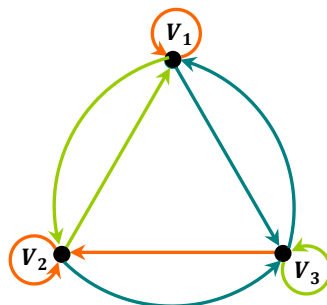


Figura 21 – Grafo dirigido representante de um quadrado latino linha

Designa-se por $\overrightarrow{K_n}$, o *grafo dirigido completo com lacetes* com n vértices, ou seja, o *grafo* que possui uma aresta dirigida do vértice V_i para o vértice V_j , para qualquer par (V_i, V_j) de vértices não necessariamente distintos.

Exemplo 4.14.: Dado o *quadrado latino* $L = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}$, este pode ser representado através do

grafo:

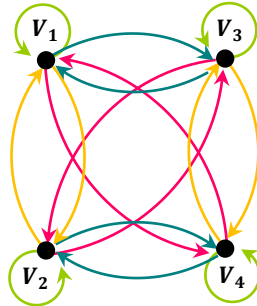


Figura 22 – Grafo dirigido completo com lacetes.

onde cada número corresponderá à respectiva cor: 1 – verde, 2 – amarelo, 3 – azul e 4 – rosa.

No caso dos *grafos dirigidos*, um *1-fator* será um subgrafo gerador associado a um subconjunto de arestas tais que, para cada vértice, há uma e apenas uma aresta desse subconjunto tanto a entrar como a sair dele.

Como no caso dos *grafos não dirigidos*, uma *1-fatorização* é uma partição do conjunto das arestas em *1-fatores*.

A figura 22 mostra uma *1-fatorização* de \vec{K}_4 associada a um *quadrado latino* L cada cor corresponde a um *1-fator*.

Assuma-se que as arestas que constituem um *1-fator* tomem a cor i se correspondem às posições ocupadas pelo símbolo i no *quadrado latino*. Reciprocamente, todo o *quadrado latino de ordem* n pode ser interpretado como uma *1-fatorização* de \vec{K}_n com os vértices etiquetados.

Observe-se que uma permuta de etiquetas de vértices reposicionará os símbolos e originará um *quadrado latino* diferente.

Por outro lado, a definição de *l*-fatorização não distingue as fatorizações associadas aos quadrados

$$M_1 \text{ e } M_2 \text{ onde } M_1 = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix} \text{ e } M_2 = \begin{matrix} 3 & 2 & 1 & 4 \\ 2 & 3 & 4 & 1 \\ 1 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 \end{matrix}.$$

Aqui, M_2 pode ser derivado de M_1 trocando os símbolos 1 e 3.

As duas *l*-fatorizações são equivalentes porque uma pode ser obtida a partir da outra por permutação das cores atribuídas aos *l*-fatores.

Antes de formular o teorema seguinte, recorde-se que um *quadrado latino reduzido* é um quadrado no qual a primeira linha e coluna estão na sua ordem natural. E vamos representar por \overrightarrow{F}_n o número de *l*-fatorizações de \overrightarrow{K}_n .

Teorema 4.15.: O número de *l*-fatorizações de \overrightarrow{K}_n é dada por $\overrightarrow{F}_n = \frac{L_n}{n!} = (n-1)! l_n$, onde L_n e l_n são, respetivamente, o número de *quadrados latinos* e o número de *quadrados latinos reduzidos* de ordem n .

Demonstração. Para qualquer *l*-fatorização existem $n!$ formas de atribuir as n cores aos *fatores*, e cada atribuição origina um único *quadrado latino*. Assim, $\overrightarrow{F}_n = \frac{L_n}{n!}$.

No teorema 1.5. vimos que $L_n = n!(n-1)! l_n$, assim $\overrightarrow{F}_n = \frac{L_n}{n!} = \frac{n!(n-1)! l_n}{n!} = (n-1)! l_n$. ■

Corolário 4.16.: O número de *l*-fatorizações de \overrightarrow{K}_n corresponde ao número de *quadrados latinos de ordem n com a primeira linha fixa*.

Demonstração: Existem $n!$ formas para escolher uma linha de um *quadrado latino de ordem n*, por isso, existem $\frac{L_n}{n!}$ *quadrados latinos com a primeira linha fixa*. ■

Exemplo 4.17.: Considere-se os seguintes *grafos dirigidos*:

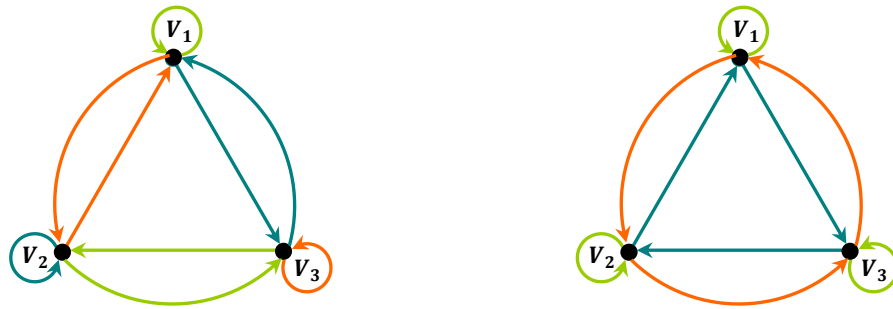


Figura 23 – Duas 1 -fatorizações $\overrightarrow{K_3}$

Se tomarmos verde – 1, laranja – 2 e azul – 3, obtemos os seguintes *quadrados latinos com a*

primeira linha fixa $L_1 = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix}$ e $L_2 = \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$. São estes os dois únicos *quadrado latinos*

com a primeira linha fixa, de ordem 3, que se podem construir.

Desta forma, podemos observar que o número de 1 -fatorizações de $\overrightarrow{K_3}$ corresponde ao número de *quadrados latinos de ordem 3 com a primeira linha fixa*.

Fixar a primeira linha no quadrado latino significa criar uma convenção de cores para as arestas que saem do primeiro vértice, o que implica uma atribuição de cores a todas as arestas do *grafo*. Como se trata de um *quadrado latino*, cada cor corresponderá às arestas de um 1 -fator. O *quadrado latino* traduz uma 1 -fatorização. Se permutarmos cores, a *fatorização* é a mesma, mas o *quadrado latino* resultante teria a *primeira linha “desarrumada”*.

Por isso, na contagem das 1 -fatorizações, basta considerar os *quadrados latinos* que têm a *primeira linha fixa*.

Considere-se agora $\overrightarrow{K'_n}$, um *grafo dirigido completo sem lacetes*.

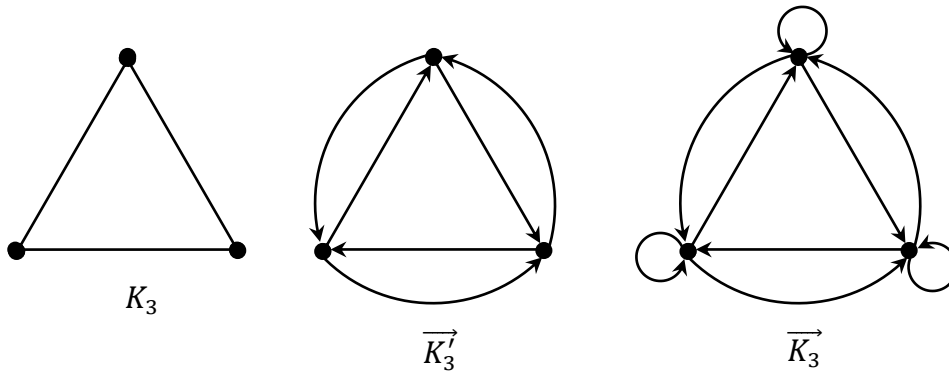


Figura 24 – Grafos completos com três vértices

Assinale-se com cores os 1 -fatores de uma 1 -fatorização de modo que a aresta que sai do vértice i para o vértice j tem a cor k_{ij} , com $k_{ij} \in \mathbb{Z}_n$ tal que $k_{ij} \equiv j - i \pmod{n}$ com $i = 1, \dots, n$.

Exemplo 4.18.: Por exemplo, se $n = 3$ e $i, j = 1, 2, 3$, ou seja, em \vec{K}_3 as arestas com cor 1 (azul) são $[V_1, V_2]$, (pois $2 - 1 = 1$), $[V_2, V_3]$, (pois $3 - 2 = 1$) e $[V_3, V_1]$, (pois $1 - 3 = -2$ e $-2 \equiv 1 \pmod{3}$); as arestas com a cor 2 (verde) são $[V_1, V_3]$, (pois $3 - 1 = 2$), $[V_3, V_2]$, (pois $2 - 3 = -1$ e $-1 \equiv 2 \pmod{3}$) e $[V_2, V_1]$, (pela razão anterior) e obtém-se o seguinte grafo:

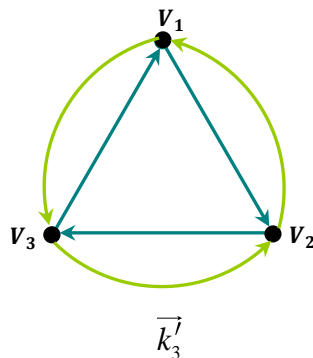


Figura 25 – Grafo dirigido, \vec{K}_3 .

O subgrafo gerador cujas arestas têm uma dada cor constitui um 1 -fator do grafo \vec{K}_3 .

Aqui a cor zero indica a ausência de lacetes.

Se a aresta dirigida de cor k unir os vértices V_i e V_j , a matriz obtida pela colocação de um k na posição (i, j) é um *quadrado latino de ordem n , com a primeira linha ordenada e zeros na diagonal principal*.

$$\begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

Se fizermos a coloração das arestas de uma 1 -fatorização de um $\overrightarrow{K_n}$ como, se descreveu, a sua *matriz de adjacência* é um *quadrado latino* em que os elementos da *primeira linha* estão na sua ordem natural $(0, 1, 2, \dots, n - 1)$ e os elementos da *diagonal* são todos iguais a zero.

Um *quadrado latino com um único símbolo na diagonal principal* é chamado de **unipotente**.

Podemos sempre permutar as linhas do *quadrado latino* obtido (*unipotente com a primeira linha fixa*) de modo que a primeira coluna fique na sua ordem natural, obtendo-se assim um *quadrado latino reduzido*, ou seja, um *quadrado latino reduzido* pode ser sempre obtido a partir de um *quadrado latino unipotente* cuja *primeira linha* está na sua *ordem natural* e, reciprocamente, dado um *quadrado latino reduzido*, existirá uma permutação das suas linhas que deixa a *primeira linha* na sua *ordem natural* e coloca na *diagonal principal* sempre o *mesmo elemento*, obtendo-se desta forma um *quadrado latino unipotente*.

Exemplo 4.19.: A permutação $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ aplicada às linhas transforma o quadrado latino

$$\begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \\ 2 & 0 & 3 & 1 \\ 3 & 2 & 1 & 0 \end{matrix} \quad \text{em} \quad \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 3 & 1 \\ 1 & 3 & 0 & 2 \\ 3 & 2 & 1 & 0 \end{matrix}$$

O primeiro quadrado é um *quadrado latino reduzido* e o segundo é um *quadrado latino unipotente com a primeira linha fixa*. Além disso, podemos dizer que o segundo *quadrado latino* é a *matriz de adjacência* da seguinte 1 -fatorização de $\overrightarrow{K_4}$, grafo da direita, onde 1 corresponde à cor azul, 2 à cor verde e 3 à cor laranja.

Se aplicássemos a mesma convenção de cores ao primeiro quadrado latino iríamos obter o grafo da esquerda que nem é $\overrightarrow{K_4}$ nem $\overleftarrow{K_4}$.

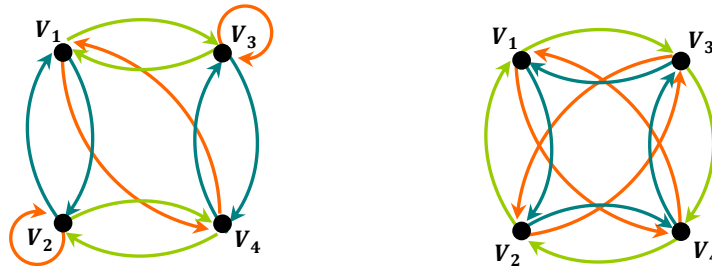


Figura 26 – Representação de grafos associados aos quadrados acima mencionados.

O seguinte teorema é consequência natural do que se observou anteriormente.

Teorema 4.20.: São iguais os seguintes números:

- I. O número de 1 -fatorizações de $\overrightarrow{K_n}$;
- II. O número de *quadrados latinos unipotentes de ordem n com a primeira linha fixa*;
- III. O número de *quadrados latinos reduzidos de ordem n* .

Regressemos agora aos grafos não dirigidos, mas também não bipartidos.

Finalmente, considere-se K_n , o grafo completo (não dirigido) de n vértices (convencionalmente, tais grafos não têm lacetes – são grafos simples, não multigrafos). Como iremos ver, colorindo os 1 -fatores de uma 1 -fatorização, se ela existir, obtém-se um quadrado latino unipotente simétrico.

Para começar, considere-se a questão da existência de 1 -fatorizações.

Teorema 4.21: Existe uma 1 -fatorização de K_n se e só se n é par.

Demonstração. i) Cada 1 -fator consiste numa coleção de arestas disjuntas que, coletivamente, incidem em todos os vértices, uma vez em cada.

Como cada aresta une dois vértices, o número total de vértices tem de ser par.

ii) Suponhamos que $n = 2m$ e que os vértices têm as etiquetas $\{V_\infty, V_0, V_1, V_2, \dots, V_{2m-2}\}$. Então, utilizando a adição *módulo* $2m - 1$, com a exceção de $\infty + i = \infty$ para todo o V_i , etiqueta de vértice, os $2m - 1$ *1-fatores* $F_i, i = 0, 1, \dots, 2m - 2$, são dados por:

$$F_i = \{(V_\infty, V_i), (V_{i+1}, V_{i-1}), (V_{i+2}, V_{i-2}), \dots, (V_{i+(m-1)}, V_{i-(m-1)})\}, \text{ ou seja,}$$

$$F_i = \{(V_\infty, V_i)\} \cup \{(V_j, V_k) \text{ com } j \neq i \text{ e } j + k \equiv 2i \pmod{(2m - 1)}\}$$

Em cada *1-fator* F_i a soma (*módulo* $2m - 1$) das etiquetas de dois vértices adjacentes é $2i$ exceto se um deles corresponde à etiqueta V_∞ . Nesse caso o vértice adjacente tem a etiqueta V_i . ■

Se for atribuída uma cor às arestas de cada *1-fator*, a *matriz de adjacência* resultante é um *quadrado latino simétrico* (porque o grafo é *não dirigido*) com *zeros na diagonal principal* (pois não há *lacetes*). Além disso, se os vértices estiverem ordenados $V_\infty, V_0, V_1, V_2, \dots, V_{2m-2}$, e as cores estiverem atribuídas de modo que a cor $i + 1$ seja usada para o *1-fator* que contém a aresta do vértice V_∞ para o vértice $V_i, i = 0, 1, \dots, 2m - 2$, as primeiras linha e coluna estão na sua ordem natural.

O seguinte *quadrado latino* é obtido a partir da *1-fatorização* de K_4 descrita anteriormente, como se pode ver na figura seguinte:

Para $n = 4$ e $m = 2$, temos:

Cor azul $F_0 = \{(V_\infty, V_0), \{V_1, V_2\}\} \longrightarrow j + k \equiv 0 \pmod{3}$
 Cor laranja $F_1 = \{(V_\infty, V_1), \{V_0, V_2\}\} \longrightarrow j + k \equiv 2 \pmod{3}$
 Cor verde $F_2 = \{(V_\infty, V_2), \{V_0, V_1\}\} \longrightarrow j + k \equiv 4 \pmod{3} \text{ ou } j + k \equiv 1 \pmod{3}$

Considerando os seguinte *1-fatores*:

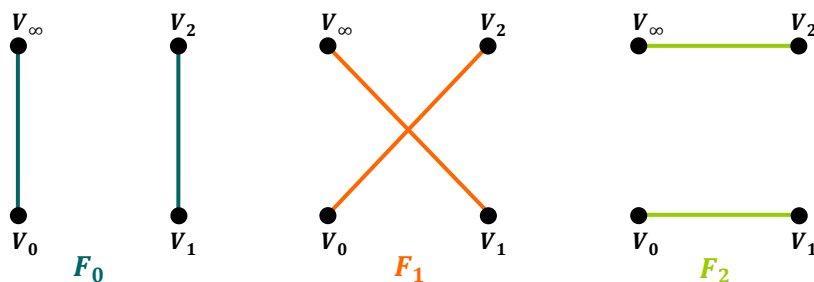


Figura 27 – Três *1-fatores* de K_4

O grafo correspondente será:

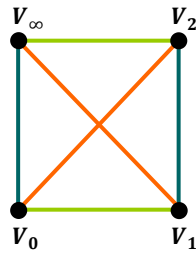


Figura 28 – Uma 1-fatorização de K_4

Sendo o respetivo *quadrado latino*:

$$L = \begin{matrix} & \begin{matrix} V_\infty & V_0 & V_1 & V_2 \end{matrix} \\ \begin{matrix} V_\infty \\ V_0 \\ V_1 \\ V_2 \end{matrix} & \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \end{matrix}$$

O *quadrado latino* resultante é o único *quadrado latino reduzido, simétrico e unipotente*.

Considere-se agora o seguinte *quadrado latino reduzido, simétrico e unipotente* é obtido a partir da 1-fatorização de K_6 descrita anteriormente, como se pode ver na figura seguinte:

Para $n = 6$ e $m = 3$, temos:

Cor verde $F_0 = \{\{V_\infty, V_0\}, \{V_1, V_4\}, \{V_2, V_3\}\} \longrightarrow j + k \equiv 0(\text{mod } 5)$

Cor laranja $F_1 = \{\{V_\infty, V_1\}, \{V_0, V_2\}, \{V_3, V_4\}\} \longrightarrow j + k \equiv 2(\text{mod } 5)$

Cor azul $F_2 = \{\{V_\infty, V_2\}, \{V_0, V_4\}, \{V_1, V_3\}\} \longrightarrow j + k \equiv 4(\text{mod } 5)$

Cor rosa $F_3 = \{\{V_\infty, V_3\}, \{V_0, V_1\}, \{V_2, V_4\}\} \longrightarrow j + k \equiv 6(\text{mod } 5)$

Cor violeta $F_4 = \{\{V_\infty, V_4\}, \{V_0, V_3\}, \{V_1, V_2\}\} \longrightarrow j + k \equiv 8(\text{mod } 5)$

Assim teremos os seguinte 1-fatores:

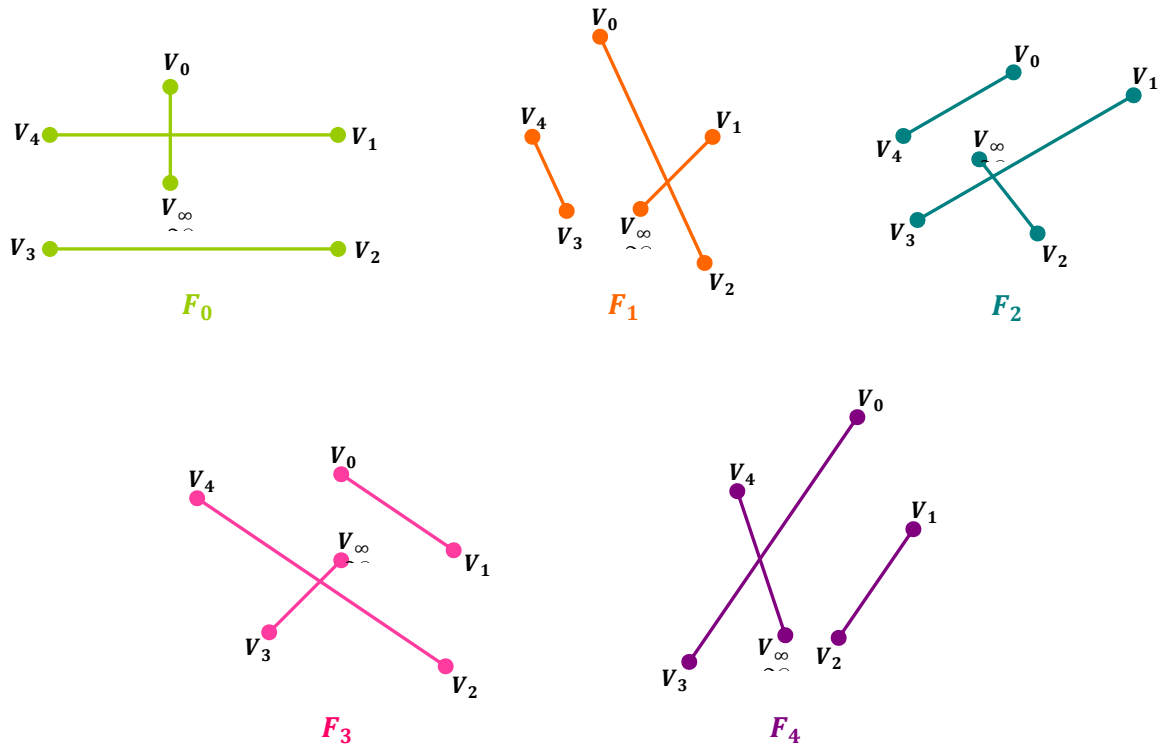


Figura 29 – Cinco 1-fatores de K_6

Cujo grafo será representado por:

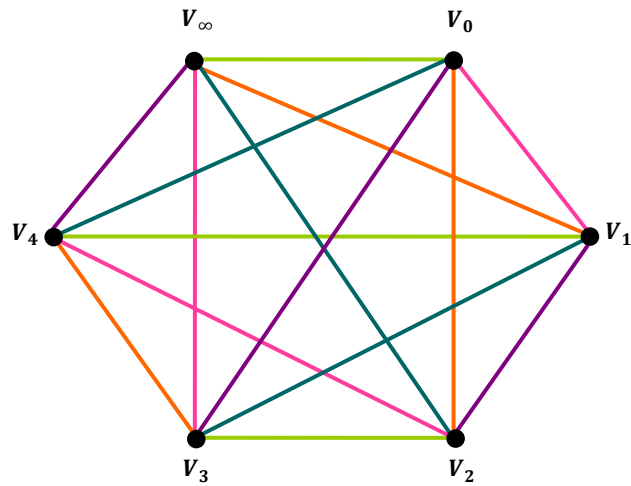


Figura 30 – Uma 1-fatorização de K_4

Sendo o respetivo *quadrado latino*:

$$L_1 = \begin{matrix} & V_\infty & V_0 & V_1 & V_2 & V_3 & V_4 \\ \begin{matrix} V_\infty \\ V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \end{matrix} & \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 4 & 2 & 5 & 3 \\ 2 & 4 & 0 & 5 & 3 & 1 \\ 3 & 2 & 5 & 0 & 1 & 4 \\ 4 & 5 & 3 & 1 & 0 & 2 \\ 5 & 3 & 1 & 4 & 2 & 0 \end{pmatrix} \end{matrix}$$

Utilizando esta forma de etiquetar e ordenar os vértices e as regras de atribuição das cores, qualquer l -fatorização de K_{2m} originará um *quadrado latino reduzido, simétrico e unipotente*.

Daqui surge o teorema seguinte:

Teorema 4.22: O número de l -fatorizações de K_{2m} é igual ao número de *quadrados latinos reduzidos, simétricos e unipotentes*.

4.3. Quadrados Latinos Linha-Completos e Caminhos em Grafos

Pretende-se agora decompor um *grafo dirigido* em *caminhos*, sendo que um *caminho* é uma sequência de vértices $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ distintos, tal que para qualquer par de vértices sucessivos v_{i_j} e $v_{i_{j+1}}$, existe uma aresta dirigida de v_{i_j} para $v_{i_{j+1}}$.

Se a sequência $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ inclui todos os vértices do *grafo*, o *caminho* é chamado de *Hamiltoniano* ou caminho de *Hamilton*.

Primeiro, observemos que dado um *caminho de Hamilton* num *grafo dirigido com n vértices*, a sequência de vértices que define o *caminho* é uma permutação dos n símbolos que representam os vértices. Depois, se se tomar um *grafo dirigido completo sem lacetes*, \overrightarrow{K}_n , qualquer decomposição em *caminhos Hamiltonianos disjuntos* dá-nos exatamente n *caminhos* (cada *caminho* “gasta” $n - 1$ arestas do *grafo* e o total de arestas é $n(n - 1)$).

No que se segue vamos utilizar um certo tipo de *quadrados latinos* que passamos a definir.

Um *quadrado latino de ordem n* diz-se *linha-completo* (“row complete”) se, dado um qualquer par ordenado de elementos diferentes (α, β) de entre os $n(n - 1)$ pares possíveis de símbolos presentes no *quadrado latino*, existe uma linha i e uma coluna j tais que α e β ocorrem respetivamente na posição (i, j) e $(i, j + 1)$ do *quadrado latino*.

De forma análoga, se qualquer par ordenado de símbolos diferentes ocorre em posições adjacentes em alguma coluna, o *quadrado latino* diz-se *coluna-completo* (“column complete”).

Se for simultaneamente *linha-completo* e *coluna-completo* diz-se apenas **completo**.

Num *quadrado latino linha-completo de ordem n*, cada par (α, β) de símbolos diferentes ocorre exatamente uma vez em posições adjacentes em alguma linha do *quadrado latino* – isto porque, por um lado, há no total $n(n - 1)$ pares (α, β) de símbolos diferentes e, por outro lado, há n linhas no *quadrado latino* e em cada linha existem $n - 1$ posições adjacentes.

Se cada par ocorre pelo menos uma vez em posições adjacentes, em alguma linha, então terá de ocorrer no máximo uma vez, ou seja, **ocorre exatamente uma vez**.

Estes tipos de *quadrados latinos* têm várias aplicações estatísticas, como por exemplo no teste de uma dieta ou medicamento em pessoas ou animais. Este poderá ser influenciado por tratamentos anteriores ou pelo número de vezes que este é aplicado, isto é, os resultados do tratamento i , poderão ser influenciados pelo $i - 1$. Desta forma, através do uso de *quadrados linha-completos* poder-se-á minimizar os efeitos secundários testando todas as possibilidades de aplicação. O *quadrado latino linha-completo* assegura que cada tratamento é imediatamente precedido exatamente uma vez por todos os outros tratamentos.

Exemplo 4.23.: Considere-se o seguinte *quadrado latino linha-completo*,

$$L = \begin{array}{cccc} 0 & 1 & 3 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 3 & 1 & 0 \\ 3 & 0 & 2 & 1 \end{array}$$

tomando a 1ª linha – verde, 2ª linha – laranja, 3ª linha – azul e a 4ª linha – amarelo, obtemos o seguinte *grafo dirigido*:

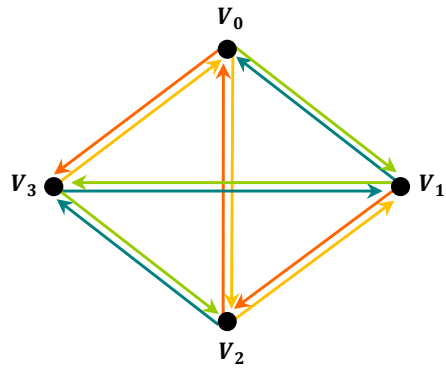


Figura 31 – Quatro *caminhos Hamiltonianos* de um \overline{K}_4

Cada linha deste *quadrado latino* dá-nos um *caminho Hamiltoniano*.

Teorema 4.24.: Se existe um *quadrado latino linha-completo de ordem n* , então existe uma decomposição de \overline{K}_n em n *caminhos Hamiltonianos disjuntos*, e reciprocamente.

O problema da existência de *quadrados latinos* deste tipo (*linha-completo*) foi resolvido, no caso em que n é par, por Williams, Dénes e Keedwell.

O próximo teorema mostra como se podem construir *quadrados latinos linha-completo* de ordem par.

Teorema 4.25.: Seja L um *quadrado latino de ordem $2m$* com a *primeira linha* dada por $0, 1, 2m - 1, 2, 2m - 2, 3, 2m - 3, \dots, m - 1, m + 1, m$ e a linha k , $k = 2, \dots, 2m$ obtida pela adição de $1 \pmod{2m}$ a cada elemento da linha anterior. Então, L é um *quadrado latino linha-completo*.

Demonstração. O *quadrado L* é claramente *latino*, visto que, cada linha e coluna consistem nos inteiros $0, 1, \dots, 2m - 1$. E cada símbolo apenas ocorre uma vez em cada linha, assim como em cada coluna devido ao método de construção utilizado ser baseado na adição de $1 \pmod{2m}$.

Queremos mostrar, então, que dados quaisquer dois símbolos α e β , estes são adjacentes em alguma linha.

Considerando as diferenças, *módulo $2m$* , entre as sucessivas entradas na *primeira linha*, obtém-se $1, 2m - 2, 3, 2m - 4, 5, 2m - 6, \dots, 2m - 1$, todas elas distintas. A partir da construção, se l_{ij} é a entrada na posição (i, j) de L , $l_{i,j+1} - l_{ij} = l_{1,j+1} - l_{1j}$ para $i = 2, \dots, 2m$ e $j = 1, \dots, 2m - 1$.

Assim, como estas diferenças $(1, 2m - 2, 3, 2m - 4, 5, 2m - 6, \dots, 2m - 1)$ surgem em todas as linha do *quadrado latino*, então podemos dizer que este é *linha-completo*.

Como cada símbolo ocorre uma vez em cada coluna, a diferença entre qualquer símbolo α e o seu vizinho do lado direito é diferente para cada ocorrência de α . ■

No exemplo 4.23. o quadrado latino:

$$L = \begin{matrix} & 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 0 & 3 \\ 1 & 2 & 3 & 1 & 0 \\ 2 & 3 & 0 & 2 & 1 \\ 3 & 0 & 1 & 3 & 2 \end{matrix}$$

foi construído segundo o teorema acima enunciado.

Exemplo 4.26.: Considere-se o seguinte *quadrado latino linha-completo*,

$$L = \begin{matrix} & 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 0 & 3 \\ 1 & 2 & 3 & 1 & 0 \\ 2 & 3 & 0 & 2 & 1 \\ 3 & 0 & 1 & 3 & 2 \end{matrix}$$

Cada linha deste *quadrado latino* dá-nos um *caminho Hamiltoniano*, como podemos observar a seguir, onde a 1ª linha surge a *verde*, a 2ª a *laranja*, a 3ª a *azul* e a 4ª a *amarelo*.

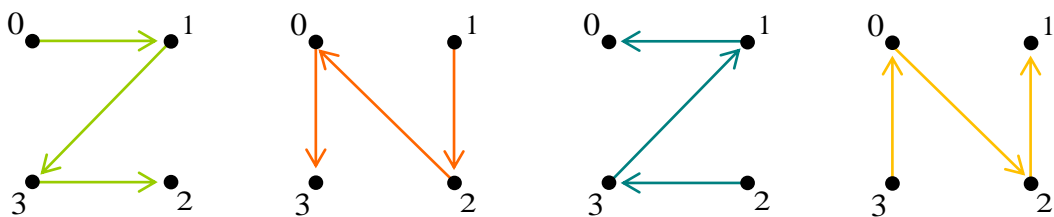


Figura 32 – *Caminhos Hamiltonianos* das linhas de L

Observação: Ao trocar as duas últimas linhas de L , obtém-se um quadrado latino completo:

$$L' = \begin{matrix} & 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 0 & 3 \\ 1 & 2 & 3 & 1 & 0 \\ 2 & 3 & 0 & 2 & 1 \\ 3 & 0 & 1 & 3 & 2 \end{matrix}$$

Teorema 4.27.: Seja L um *quadrado latino linha-completo*, construído segundo o teorema 4.25 e seja L' um *quadrado latino* em que a primeira coluna é idêntica à primeira linha de L , então L' é completo.

Demonstração. A reordenação das linhas não altera a sua “completude” no sentido em que o novo *quadrado latino* mantém-se *linha-completo*. Em L' as diferenças entre entradas sucessivas da primeira coluna são distintas e, além disso, $l'_{i+1,1} - l'_{i1} = l'_{i+1,j} - l'_{ij}$, onde l'_{ij} é a entrada da posição (i, j) de L' .

Em todas as colunas as entradas sucessoras a qualquer símbolo α serão ainda distintas porque α ocorre só uma vez em cada linha. ■

Podemos, assim, concluir que todo o *grafo dirigido completo de ordem par n* , tem n *caminhos Hamiltonianos* disjuntos.

A decomposição de um *grafo dirigido completo* em *caminhos Hamiltonianos disjuntos* será restringida ao caso em que o número de vértices é par. No entanto, há autores (Archdeacon et al.) que mostram que em alguns casos a decomposição pode ser feita também para um número ímpar de vértices.

Contudo, sabe-se que não existe nenhum *quadrado latino linha-completo* de ordem 3, 5 ou 7, mas existe de ordem 9. Esses autores conjecturaram que existem *quadrados latinos linha-completo* de ordem $n > 2$ se e só se n não é primo.

Suponhamos, agora que se deseja fechar os *caminhos Hamiltonianos* retornando em cada caso ao vértice inicial, isto é, transformar um *caminho Hamiltoniano* num *ciclo*. Isto pode ser facilmente conseguido pela adição de um novo vértice, etiquetado de $2m$. Este vértice irá permitir a união do último vértice ao vértice inicial do anterior caminho, dando origem a um *ciclo Hamiltoniano*. Assim, o caminho $v_{i_0}, v_{i_1}, \dots, v_{i_{2m-1}}$ em $\overrightarrow{K'_{2m}}$ será transformado em $v_{i_0}, v_{i_1}, \dots, v_{i_{2m-1}}, v_{i_{2m}}, v_{i_0}$, que representa um ciclo *Hamiltoniano* em $\overrightarrow{K'_{2m+1}}$.

No contexto dos *quadrados latinos linha-completos*, o fecho dos *caminhos* pode ser representado pela adição da $(2m + 1)^{a}$ coluna, a cada uma das $2m$ existentes. Portanto, o *quadrado latino* L origina um retângulo L'' do tipo $2m \times (2m + 1)$.

Nos *ciclos Hamiltonianos* as linhas são interpretadas como permutações circulares, por isso, cada linha proporciona o ciclo descrito anteriormente.

Exemplo 4.28.: Assim, se considerarmos o *quadrado latino*

$$L = \begin{matrix} & 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 0 & 3 \\ 1 & 2 & 3 & 1 & 0 \\ 2 & 3 & 0 & 2 & 1 \\ 3 & 0 & 1 & 3 & 2 \end{matrix}$$

do exemplo anterior, podemos transformá-lo no retângulo 4×5 : $L'' = \begin{matrix} & 0 & 1 & 3 & 2 & 4 \\ 0 & 1 & 2 & 0 & 3 & 4 \\ 1 & 2 & 3 & 1 & 0 & 4 \\ 2 & 3 & 0 & 2 & 1 & 4 \\ 3 & 0 & 1 & 3 & 2 & 4 \end{matrix}$ para que

os *caminhos Hamiltonianos* anteriormente observados, passem a *ciclos Hamiltonianos*.

Este retângulo dá a decomposição de $\overrightarrow{K_5}$ em *ciclos Hamiltonianos* que se mostra na figura:

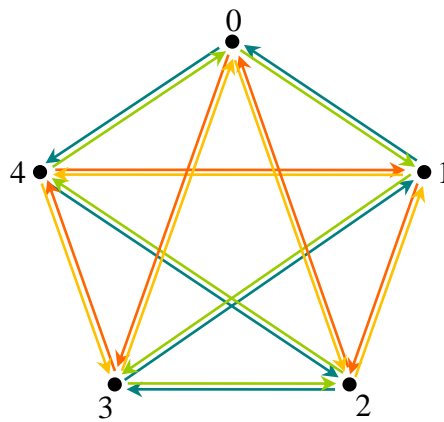


Figura 33 – Ciclos Hamiltonianos disjuntos de $\overrightarrow{K_5}$.

Teorema 4.29.: Existe uma decomposição de:

- I. $\overrightarrow{K'_{2m}}$ em $2m$ *caminhos Hamiltonianos disjuntos*;
- II. $\overrightarrow{K'_{2m+1}}$ em $2m$ *ciclos Hamiltonianos disjuntos*.

O número de *ciclos Hamiltonianos* é igual ao número de *caminhos* conforme decorre da construção e da forma de etiquetar os vértices dos respectivos *grafos*.

Recorrendo aos *caminhos* anteriormente exemplificados no exemplo 4.28. observamos que a 1ª e 3ª linha correspondem a caminhos inversos, assim como a 2ª e 4ª.

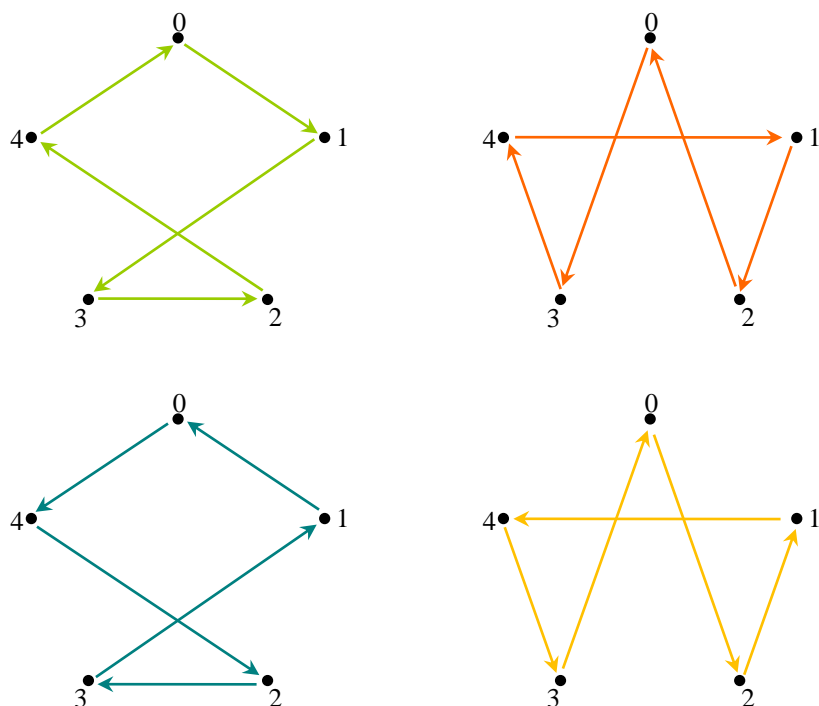


Figura 34 – Ciclos hamiltonianos das linhas de L

Surgindo, desta forma, o seguinte lema:

Lema 4.30.: As últimas m linhas do *quadrado latino completo* L de ordem $2m$ são as primeiras m linhas na ordem inversa.

Demonstração. Definindo a primeira linha como sendo

$$0, 1, 2m - 1, 2, 2m - 2, 3, 2m - 3, \dots, m - 1, m + 1, m,$$

as restantes linhas $(2, 3, \dots, 2m)$ serão obtidas adicionando uma unidade aos elementos da linha precedente.

Adicionando $m \pmod{2m}$ a todos os elementos da primeira linha obtenho a linha $m + 1$ dada por:

$$m, m + 1, m - 1, m + 2, m - 2, \dots, 2m - 1, 1, 0$$

que é a primeira linha na sua ordem inversa.

Adicionando $1 \pmod{2m}$ aos elementos das linhas 1 e $m + 1$ obtemos as linha 2 e $m + 2$, verificando que a linha $m + 2$ é a linha 2 na sua ordem inversa.

Assim, através de adições sucessivas obtemos a linha $m + k$ que corresponderá à linha k , para $k \leq m$, na sua ordem inversa. ■

Do lema anterior podemos concluir que dois *caminhos orientados inversos* de $\overrightarrow{K'_{2m}}$ corresponderão a um *caminho* de K_{2m} , obtendo-se assim o seguinte teorema:

Teorema 4.31.: Existe uma decomposição de:

- I. K_{2m} em m *caminhos Hamiltonianos disjuntos*;
- II. K_{2m+1} em m *ciclos Hamiltonianos disjuntos*.

Demonstração. As primeiras m linhas do *quadrado latino linha-completo* L fornecem os *caminhos*.

As mesmas m linhas do retângulo ao qual foi adicionado o símbolo $2m$ como sendo o elemento de ordem $2m + 1$, fornecem-nos os *ciclos*. ■

Prosseguindo o estudo vamos agora associar os *quadrados latino* a *trajetos* e *circuitos de Euler*.

Relembremos que um *trajeto de Euler* tem de conter todas as arestas do *grafo*. Por sua vez, designa-se por *circuito de Euler*, todo o *circuito* que contém todas as arestas do *grafo*.

Assim, um *circuito de Euler* é um *trajeto de Euler* fechado.

Um *grafo* diz-se *Euleriano* se admite um *circuito de Euler* e diz-se *Semi-euleriano* se admite um *trajeto de Euler*. É sabido que um *grafo* é *Euleriano* se e só se todos os vértices têm grau par.

Obviamente K_{2m+1} verifica essa condição mas K_{2m} não. Iremos demonstrar de forma construtiva a existência de um *circuito de Euler* para K_{2m+1} , ordenando os *caminhos Hamiltonianos* “colando” o vértice final de cada um ao vértice inicial do seguinte e fechando no final dos m *caminhos*, formando desta forma um *circuito Euleriano*.

Utilizando o retângulo L'' , obtido no teorema 4.29. pela adição de uma coluna constante ao *quadrado latino linha-completo* L , obtemos o seguinte teorema:

Teorema 4.32.: Um *circuito Euleriano* de K_{2m+1} é dado pelas m primeiras linhas do retângulo L'' .

Demonstração. Sejam os elementos das primeiras m linhas de L'' ordenadas linearmente, isto é, à sequências dos elementos da 1ª linha segue-se a sequência da 2ª linha, ..., até à sequência da linha

de ordem m , ou seja, para $i < m$, a posição (i, j) é o antecessor imediato de $(i, j + 1)$ e $(i, 2m + 1)$ é o antecessor imediato de $(i + 1, 1)$.

Para fechar o circuito a posição $(m, 2m + 1)$ é o antecessor imediato de $(1, 1)$. Ficando assim com as primeiras m linhas a originar um *circuito Euleriano*.

De facto, o número total de arestas será $m(2m+1)$.

Cada aresta do *grafo* (*não dirigido*) aparece uma só vez nas m primeiras linhas do retângulo L'' . Em cada linha há $2m$ arestas, logo nas m primeiras linhas teremos $m \times 2m$ arestas. Por cada mudança de linha temos uma nova aresta, ou seja, mais $m - 1$ arestas. Para fecharmos o caminho teremos mais uma aresta que unirá o ultimo vértice da linha m ao primeiro da linha 1. Assim, no total serão $2m^2 + m$. ■

Exemplo 4.33.: Para $2m = 4$ as primeiras duas linhas de

$$L'' = \begin{matrix} 0 & 1 & 3 & 2 & 4 \\ 1 & 2 & 0 & 3 & 4 \\ 2 & 3 & 1 & 0 & 4 \\ 3 & 0 & 2 & 1 & 4 \end{matrix} \quad \text{são} \quad \begin{pmatrix} 0 & 1 & 3 & 2 & 4 \\ 1 & 2 & 0 & 3 & 4 \end{pmatrix}$$

A ordem linear das duas linhas dá a seguinte sequência de vértices: 0,1,3,2,4,1,2,0,3,4.

Assumindo que a segunda paragem no vértice 4 é seguida pela volta ao vértice 0 inicial, a sequência 0,1,3,2,4,1,2,0,3,4,0 origina um *circuito Euleriano* de K_5 , como se pode verificar na figura seguinte.

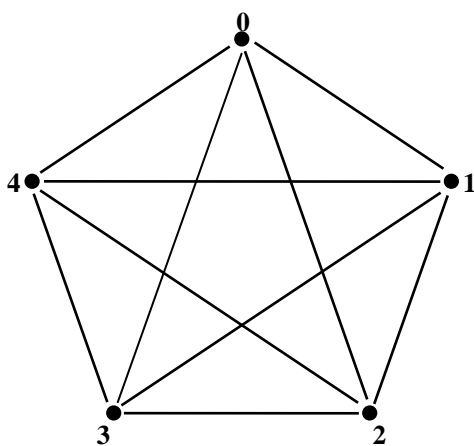


Figura 35 – Circuito Euleriano de K_5 .

Observação: Se estamos a estudar *caminhos Hamiltonianos*, podemos trocar linhas.

Se estivermos a estudar *1-fatorizações*, será que também podemos?

Observemos:

Se $M_1 = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}$ for a matriz de adjacência de um grafo \vec{K}_4 , o que significa trocar linhas?

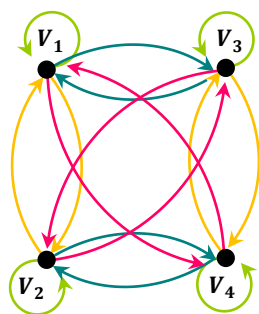


Figura 36 – Grafo dirigido completo com lacetes, correspondente a M_1 .

onde cada número corresponderá à respetiva cor: 1 – verde, 2 – amarelo, 3 – azul e 4 – rosa.

Cada cor é um *1-fator* de \vec{K}_4 , portanto, M_1 traduz a seguinte *1-fatorização* de \vec{K}_4 :

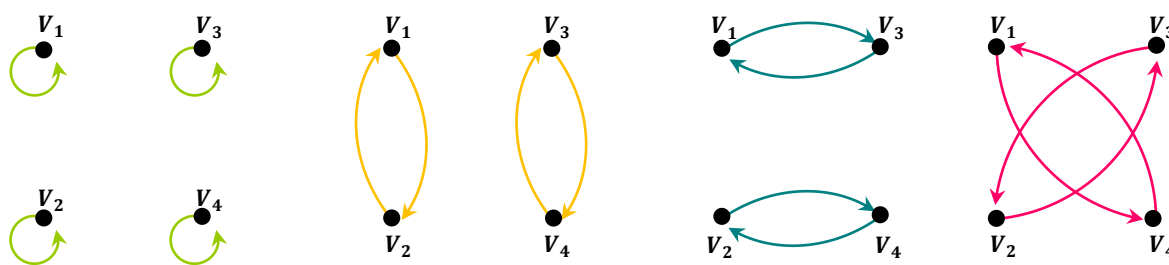


Figura 37 – *1-fatorização* de um grafo dirigido completo, correspondente a M_1 .

Se trocarmos a segunda e a terceira linhas em M_1 obtemos o seguinte *quadrado latino*:

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \end{matrix}$$

Que traduz, no grafo \vec{K}_4 a seguinte *1-fatorização*:

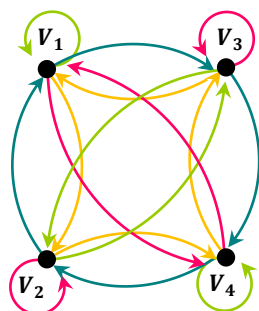


Figura 38 – Grafo dirigido completo com lacetes, correspondente ao quadrado latino anterior.

onde cada número corresponderá à respectiva cor: 1 – verde, 2 – amarelo, 3 – azul e 4 – rosa.

E traduz a seguinte *1-fatorização* de \vec{K}_4 :

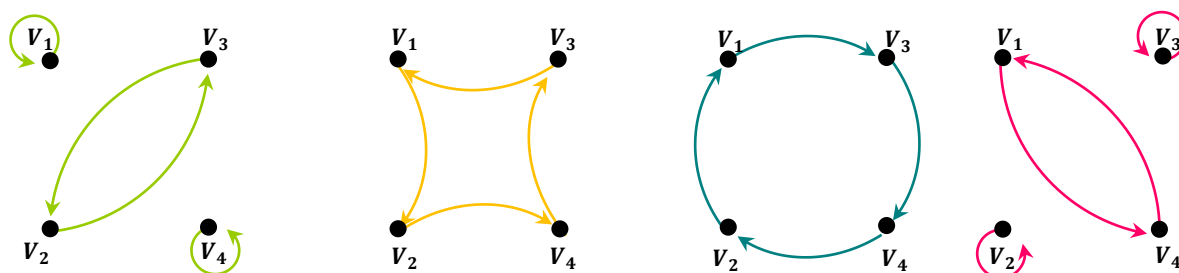


Figura 39 – 1-factorização de um grafo dirigido completo anterior.

Assim, podemos verificar que a dois quadrados latinos de ordem 4 com a primeira linha fixa correspondem duas *1-fatorizações* diferentes de \vec{K}_4 , conforme o corolário 4.16..

Não podemos deixar de questionar, também: O que significará “trocar linhas” quando estudamos as *1-fatorizações* de um \vec{K}_n ?

Consideremos o seguinte quadrado latino:

0	1	2	3
2	0	3	1
1	3	0	2
3	2	1	0

Que traduz a seguinte *1-fatorização* de \overrightarrow{K}_4 :

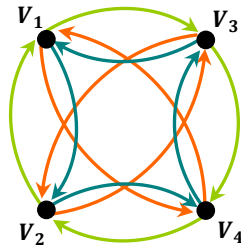


Figura 40 – Grafo dirigido completo sem lacetes, correspondente ao *quadrado latino* anterior.

onde o número 1 toma a cor verde, o 2 a cor laranja, o 3 a cor azul e o 0 a ausência de cor.

Se trocarmos a segunda e a terceira linhas do *quadrado latino* acima obtemos o seguinte *quadrado latino*:

0	1	2	3
1	3	0	2
2	0	3	1
3	2	1	0

que se traduz no seguinte *grafo*:

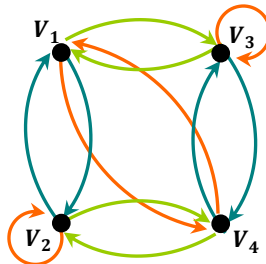


Figura 41 – Grafo correspondente ao *quadrado latino* anterior.

Deixando, assim, de ser \overrightarrow{K}_n ! Podemos, então, concluir que não se podem trocar as linhas do quadrado latino associado a um \overrightarrow{K}_n .

O *quadrado latino* tem de ser *unipotente* e o símbolo na diagonal corresponde à ausência de lacetes.

4.4. Grafos Fortemente Regulares

Atente-se agora num tipo de *grafos* que têm uma estrutura bastante *simétrica* e que possuem características muito fortes.

Recordemos que um *grafo regular* é um *grafo* em que todos os *vértices* têm o mesmo grau, isto é, em todos os *vértices* incide o mesmo número de arestas.

Um *grafo* diz-se *k-regular* se em todos os *vértices* incidem *k* arestas.

E também, que um *grafo fortemente regular* é um *grafo regular* em que para todos os pares de *vértices adjacentes* existe um número λ fixo de *vértices adjacentes a ambos*, e para qualquer par de *vértices não adjacentes* existe um número fixo μ de *vértices adjacentes a ambos*.

Exemplo 4.34: O grafo seguinte diz-se *fortemente regular de ordem 4*, sendo um *2-regular*, onde $\lambda = 0$ e $\mu = 1$.

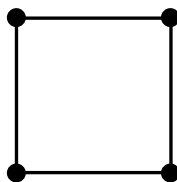


Figura 42 – Grafo fortemente regular de ordem 4.

Considere-se o sistema que consiste nos ternos ordenados (i, j, k) , onde $1 \leq i, j, k \leq n$, tais que cada par de coordenadas toma cada valor possível exatamente uma vez. Observemos que para cada valor \bar{k} de k (por exemplo) existe apenas um par (\bar{i}, \bar{j}) que corresponde a esse valor de $k - (\bar{i}, \bar{j}, \bar{k})$. Portanto haverá tantos ternos (i, j, k) nas condições referidas quantos os pares (i, j) , ou seja, n^2 .

Identificando i, j e k com as linhas, colunas e símbolos, respetivamente de uma matriz, mostra-se que cada sistema é equivalente a um *quadrado latino de ordem n*.

Existe uma segunda interpretação deste sistema, isto é, suponha-se que se toma os n^2 ternos para vértices de um *grafo* onde dois vértices são adjacentes se e só se uma das coordenadas toma o mesmo valor em ambos os ternos correspondentes.

Assim, relacionando este grafo com o quadrado latino anterior, unem-se vértices por uma aresta se eles correspondem a duas entradas situadas na *mesma linha*, *mesma coluna* ou que tenham o

mesmo símbolo. Representar-se-á o grafo obtido desta forma por $L_1(n)$. Trata-se de um grafo com n^2 vértices que corresponde a um quadrado latino de ordem n .

Tais grafos são frequentemente referidos como grafos quadrados latinos (este termo é também associado ao grafo bipartido $K_{n,n}$ com a coloração de arestas associada aos símbolos de um quadrado latino de ordem n).

Exemplo 4.35.: Considere o seguinte quadrado latino de ordem 3

1	2	3
2	3	1
3	1	2

Baseando-nos no anteriormente referido, podemos representar o quadrado latino anterior pelo grafo seguinte.

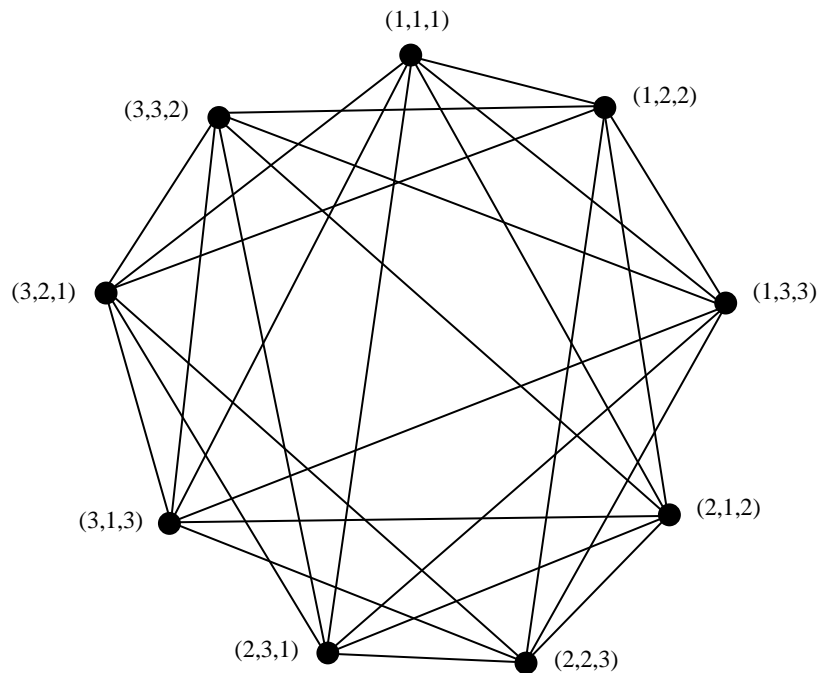


Figura 43 – Grafo fortemente regular de ordem 3^2 , $L_1(3)$.

Note-se que é um grafo de ordem 9, 6-regular e fortemente regular com $\lambda = 3$ e $\mu = 6$.

Teorema 4.36.: $L_1(n)$ é um grafo fortemente regular com grau $3(n - 1)$, $\lambda = n$ e $\mu = 6$.

Demonstração. Qualquer vértice é adjacente aos vértices que correspondem às entradas de um *quadrado latino* na *mesma linha, coluna* ou com o *mesmo símbolo*. Existem $n - 1$ em cada categoria, por isso cada vértice tem grau $3(n - 1)$.

Considere-se duas entradas de um *quadrado latino* na linha i dadas por dois ternos (i, j_1, k_1) e (i, j_2, k_2) . Os vértices associados são adjacentes entre si e ambos adjacentes aos restantes $n - 2$ vértices identificados com as restantes entradas da linha i . Adicionalmente, para algum i' e i'' não necessariamente distintos existem vértices dados por (i', j_1, k_2) e (i'', j_2, k_1) adjacentes a ambos - o que perfaz um total de n vértices adjacentes a (i, j_1, k_1) e (i, j_2, k_2) .

Argumentos similares aplicam-se a dois vértices associados a ternos com elementos na mesma coluna ou com o mesmo símbolo.

De seguida, considere-se os vértices p e q associados aos ternos (i_1, j_1, k_1) e (i_2, j_2, k_2) onde $i_1 \neq i_2, j_1 \neq j_2$ e $k_1 \neq k_2$.

Para um vértice ser adjacente a p e q , o terno correspondente deve coincidir numa coordenada com o de p e noutra coordenada com o de q . Existem, portanto $3 \times 2 = 6$ ternos que satisfazem esta condição. ■

Pode-se construir um tipo similar de *grafos*, representado por $L_r(n)$ a partir de um conjunto de r *MOLS* (*quadrados latinos mutuamente ortogonais de ordem n*), com $1 \leq r \leq n - 1$ (como vimos anteriormente, existem no máximo $n - 1$ *MOLS* de ordem n). Como no caso anterior, que só corresponde a $r = 1$, as n^2 posições de qualquer dos *quadrados latinos de ordem n* são tomadas como sendo os vértices. Quaisquer dois deles são adjacentes se estão situados na *mesma linha*, na *mesma coluna* ou contém o *mesmo símbolo* em algum dos *quadrados latinos mutuamente ortogonais*. Associando a cada vértice um $(r + 2)$ -*uplos* $(i, j, k_1, k_2, \dots, k_r)$ onde $k_l, l = 1, \dots, r$ é o símbolo na posição (i, j) do *quadrado latino* l , a propriedade de *latino* garante que os pares ordenados (i, k_l) e (j, k_l) tomam cada valor possível exatamente uma vez.

A *ortogonalidade* de quaisquer dois quadrados s e t garante que o par (k_s, k_t) toma cada valor possível exatamente uma vez. Assim, há tantos $(r + 2)$ -*uplos* nestas condições quantos pares (i, j) , ou seja, n^2 .

Exemplo 4.37.: Considere o seguinte par de *MOLS de ordem 3*:

$$L_1 = \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \quad \text{e} \quad L_2 = \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array}$$

$$\begin{array}{ccc}
 (1,1) & (2,2) & (3,3) \\
 \text{Então } L_1 \odot L_2 = & (2,3) & (3,1) & (1,2) \\
 & (3,2) & (1,3) & (2,1)
 \end{array}$$

que pode ser representado pelo *grafo fortemente regular* seguinte, onde $\lambda = 7$ e não faz sentido pensar em μ , pois não há pares de vértices não adjacentes, o grafo neste caso é completo de grau 9, K_9 .

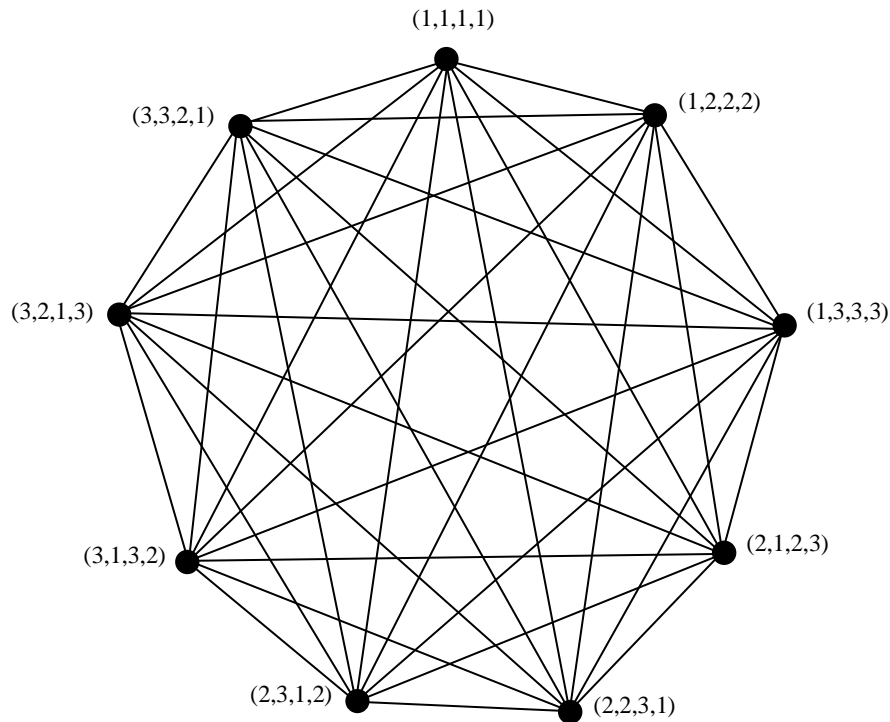


Figura 44 – Grafo fortemente regular $L_2(3)$.

De um modo geral prova-se que:

Teorema 4.38.: Para $1 \leq r \leq n - 1$ o grafo $L_r(n)$ é fortemente regular com:

- I. Todo o vértice é de grau $(r + 2)(n - 1)$;
- II. $\lambda = (n - 2) + r(r + 1)$;
- III. $\mu = (r + 2)(r + 1)$, quando existe.

BIBLIOGRAFIA

- [1] LAYWINE, Charles F.; MULLEN, Gary L. – **Discrete Mathematics Using Latin Squares**. Wiley Inter-Science, 1998.
- [2] CARDOSO, Domingos M.; SZYMANSKI, Jerzy; ROSTAMI, Mohammad – **Matemática Discreta. Combinatória, Teoria dos Grafos e Algoritmos**. Aveiro: Escolar Editora, 2009.
- [3] DENÉS, J. – Latin squares: new developments in the theory and applications. North-Holland. Amsterdam, 1991.
- [4] GILBERT, William J.; NICHOLSON, W. Keith [et al.] – **Modern Algebra with Applications**, Second Edition. Wiley-Interscience, 2000.
- [5] ROSEN, Kenneth H., [et al.] – **Handbook of Discrete and Combinatorial Mathematics**. CCR-Press, 2000.
- [6] SHUMER, Peter D. – **Mathematical Journeys**. Wiley-Interscience, 2004.
- [7] CRILLY, Tony – **50 Ideias de Matemática que precisa mesmo de saber**. D.Quixote, 2011.
- [8] FUTALGO, Novacruz – **Latin Squares** [Em linha]. Disponível na WWW: URL: <http://futalgo.planetaclix.pt/novacruz/hlpsdku.htm>, acessado em 17 Out. 2007.
- [9] IME, Algoritmos – **Grafos** [Em linha]. Disponível na WWW: URL: http://www.ime.usp.br/~pf/algoritmos_em_grafos/aulas/cliques.html, acessado em 22 Out. 2008.
- [10] KNOT, Arithmetic – **Latin Squares** [Em linha]. Disponível na WWW: URL: <http://www.cut-the-knot.org/arithmetic/latin.shtml>, acessado em 7 Jan. 2008.
- [11] WIKIPEDIA, The Free Encyclopedia – **Latin Squares** [Em linha]. Disponível na WWW: URL: http://en.wikipedia.org/wiki/Latin_square, acessado em 10 Out. 2007.

ANEXOS

O presente anexo contém as demonstrações dos resultados dos capítulos 1 e 2, “*Quadrados latinos*” e “*Grupos e quadrados latinos*”, respetivamente.

Proposição 1.3.: Para qualquer $n > 1$, existe um quadrado latino de ordem n .

Demonstração: Considere-se a primeira linha do quadrado $n \times n$ como sendo a dos inteiros $0, 1, \dots, n - 1$. Assim, a linha seguinte será $1, \dots, n - 1, 0$, continuando-se o processo até à última linha.

Desta forma, obtém-se o seguinte quadrado latino:

$$L = \begin{matrix} 0 & 1 & \cdots & n-1 \\ 1 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ n-1 & 0 & \cdots & n-2 \end{matrix}$$

■

Teorema 1.5.: Para $n > 1$, L_n é dado por:

$$L_n = n! (n - 1)! l_n$$

Demonstração: Dado um quadrado latino de ordem n , podemos permutar as suas colunas de $n!$ maneiras, de modo que o quadrado resultante seja ainda um quadrado latino. Analogamente, depois de se permutar as colunas podemos permutar as últimas $n - 1$ linhas de $(n - 1)!$ maneiras, de tal forma que cada um destes quadrados seja ainda um quadrado latino e distinto, o que se verifica desde que na permutação das linhas, a primeira (por exemplo) não seja desarranjada. Então, começando com um quadrado latino reduzido de ordem n podemos fazer $n!$ permutações nas colunas e $(n - 1)!$ nas linhas, que resultariam em $n! (n - 1)!$ quadrados latinos de ordem n , em que exactamente um deles é quadrado latino reduzido.

Assim, $L_n = n! (n - 1)! l_n$.

■

Proposição 1.9.: Para cada $n \geq 2$, $N(n) \leq n - 1$.

Demonstração: Considere dois quadrados latinos, L_1 e L_2 pertencentes ao conjunto de MOLS. Os n símbolos de qualquer quadrado latino L_1 podem ser permutados de qualquer maneira sem afectar a sua ortogonalidade com o quadrado L_2 . Assim, pode-se reordenar os símbolos na primeira linha de cada quadrado de forma a obter $(0, 1, \dots, n - 1)$. Suponha-se que,

$$L_1 = \begin{array}{cccc} 0 & 1 & \dots & n-1 \\ x & - & \dots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \dots & - \end{array} \quad \text{e} \quad L_2 = \begin{array}{cccc} 0 & 1 & \dots & n-1 \\ y & - & \dots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \dots & - \end{array}$$

são dois membros do conjunto. Nem o símbolo x , nem o símbolo y podem ser zero, porque L_1 e L_2 são quadrados latinos. Além disso, $x \neq y$, pois se $x = y = i$, o par (i, i) apareceria duas vezes em $L_1 \odot L_2$ uma vez que já existe na primeira linha de $L_1 \odot L_2$. Então, existem no máximo $n - 1$ símbolos que podem aparecer na primeira posição da segunda linha destes quadrados que pertencem a um conjunto ortogonal.

Logo, $N(n) \leq n - 1$. ■

Teorema 1.13.: Para q , potência de um número primo, o conjunto de polinómios da forma $f_a(x, y) = ax + y$ com $a \neq 0 \in F_q$ representa um conjunto completo de $q - 1$ MOLS de ordem q .

Demonstração: Mostre-se primeiramente que se $a \neq 0$, o polinómio $f_a(x, y) = ax + y$ representa um quadrado latino de ordem q . Suponha-se que algum símbolo ocorre duas vezes na coluna y_1 , na posição (x_1, y_1) e (x_2, y_1) . Então, $ax_1 + y_1 = ax_2 + y_1$ e $ax_1 = ax_2$. Sendo $a \neq 0$ e usando o facto de que F_q é corpo vem $x_1 = x_2$ e, portanto, (x_1, y_1) e (x_2, y_1) são o mesmo ponto.

Analogamente, se $ax_1 + y_1 = ax_2 + y_1$, então $y_1 = y_2$. Logo, o polinómio $f_a(x, y)$ representa um quadrado latino de ordem q .

Para mostrar que se $a \neq b$ então f_a e f_b representam quadrados latinos ortogonais, suponha-se que (x_1, y_1) e (x_2, y_2) são duas posições que representam o mesmo par ordenado. Depois de concatenar os quadrados latinos representados respectivamente por f_a e f_b , obtém-se:

$$ax_1 + y_1 = ax_2 + y_2$$

$$bx_1 + y_1 = bx_2 + y_2$$

Assim, tem-se

$$ax_1 - bx_1 = ax_2 - bx_2 \Leftrightarrow (a - b)x_1 = (a - b)x_2$$

e como $a \neq b$, $x_1 = x_2$ o que implica $y_1 = y_2$.

Isto mostra que os quadrados latinos representados por f_a e f_b são ortogonais.

Como para cada $a \neq 0$ existe um quadrado latino, o número de quadrados latinos mutuamente ortogonais que podemos construir é $q - 1$. ■

Teorema 1.16. Se existir um par de MOLS de ordem n e um par de MOLS de ordem m , então existe um par de MOLS de ordem mn .

Demonstração: Sejam A_1, A_2 um par de MOLS de ordem m e B_1, B_2 outro par de MOLS de ordem n . Considerem-se os quadrados $A_1 \otimes B_1$ e $A_2 \otimes B_2$ de ordem mn . Provar-se-á que $A_1 \otimes B_1$ e $A_2 \otimes B_2$ são quadrados latinos. Suponha-se que um elemento de $A_1 \otimes B_1$, (a, b) está repetido na mesma coluna, j . Como A_1 e B_1 são quadrados latinos, isto é impossível.

De forma análoga prova-se o mesmo para $A_1 \otimes B_1$.

Mostre-se agora que $A_1 \otimes B_1$ e $A_2 \otimes B_2$ formam um par de quadrados latinos ortogonais. Considere-se um par $((a_{ij}, b_{kl}), (a_{pq}, b_{rt}))$ da respectiva matriz concatenada $(A_1 \otimes B_1) \odot (A_2 \otimes B_2)$, e suponha-se que este par está repetido em $(A_1 \otimes B_1) \odot (A_2 \otimes B_2)$. Porém os pares (a_{ij}, a_{pq}) e (b_{kl}, b_{rt}) ocorrem apenas uma vez em $A_1 \odot A_2$ e $B_1 \odot B_2$, respectivamente. Logo, conclui-se que isto é impossível. Desta forma, $A_1 \otimes B_1$ e $A_2 \otimes B_2$ formam um conjunto de quadrados latinos ortogonais. ■

Proposição 1.18. Se $n \equiv 0,1,3(mod 4)$, tem-se que $N(n) \geq 2$.

Demonstração: Se $n \equiv 0,1,3(mod 4)$, então ou n é ímpar ou n é divisível por 4. Neste caso, se $n = q_1 \dots q_r$ é a fatorização de n em potências de números primos distintas, então, $q_i \geq 3$. Portanto, $q_i - 1 \geq 2$ para cada $i = 1, \dots, r$.

Aplicando o Teorema 1.13. e o Teorema 1.16., podem construir-se pelo menos dois MOLS de ordem n . ■

Teorema 1.20.: Seja $q_1 \times \dots \times q_r$ a fatorização de n em potências de números primos distintas com $q_1 < \dots < q_r$. Então, $N(n) \geq q_1 - 1$.

Demonstração: Para cada potência prima q_i na fatorização de n , pode-se construir, um conjunto de $q_i - 1$ MOLS de ordem q_i , pelo Teorema 1.13.. Então, para cada $i > 1$, tem-se que $q_i - 1 > q_1 - 1$ MOLS de ordem q_i , e aplicando sucessivamente o produto de Kronecker tem-se $q_1 - 1$ MOLS de ordem n . ■

Teorema 2.8.: A tabela de multiplicação de um grupo finito $(G,*)$ de ordem n é um quadrado latino de ordem n .

Demonstração: Suponha-se que na linha a^v se tem $a * b = a * c$. Como a tem inverso, a^{-1} , e a operação é associativa, multiplicando ambos os membros por a^{-1} fica-se com:

$$\begin{aligned} a * b &= a * c \\ \Leftrightarrow a^{-1} * (a * b) &= a^{-1} * (a * c) \\ \Leftrightarrow (a^{-1} * a) * b &= (a^{-1} * a) * c \\ \Leftrightarrow b &= c \end{aligned}$$

Desta forma, os elementos da linha a são distintos e como a é um elemento genérico o quadrado é latino por linhas.

Analogamente, todos os elementos de cada coluna são distintos, logo o quadrado é também latino por colunas, portanto é um quadrado latino. ■

Teorema 2.10.: Um quadrado latino pode sempre ser encarado como a tabela de multiplicação de um monoide (grupoide com elemento neutro).

Ideia da demonstração:

Por exemplo, o seguinte quadrado latino pode ser encarado como a tabela da operação $*$ de um grupoide $G = \{a, b, c, d\}$, em que o elemento neutro é a .

^v Designamos por linha a a linha correspondente aos produtos da forma $a * i$, onde $i \in G$.

	a	c	d	b
a	a	c	d	b
c	c	d	b	a
b	b	a	c	d
d	d	b	a	c

Este quadrado latino pode ser reescrito de modo que a primeira coluna seja igual à primeira linha (basta para isso permutar as linhas). Trocando-se as linhas 3 e 4, obtém-se:

	a	c	d	b
a	a	c	d	b
c	c	d	b	a
d	d	b	a	c
b	b	a	c	d

Suponha-se, sem perda de generalidade, que a primeira linha e a primeira coluna são $\{1, 2, \dots, N\}$. O elemento neutro da operação definida será 1.

Teorema 2.11.: Um quadrado latino é a tabela de Cayley de um grupo se e só se a composta de quaisquer duas linhas do quadrado latino (encaradas como permutações) é ainda uma linha do quadrado latino.

Demonstração: Dado que a operação $*$, representada pelo quadrado latino, tem elemento neutro e que em cada linha não há elementos repetidos, este está presente em todas as linhas.

Pretende-se mostrar que se a operação for associativa, isso implica que cada elemento tem inverso.

Seja $i \in \{1, 2, \dots, N\}$. Existe j tal que $i * j = 1$ (j é a coluna em que aparece 1 na linha i).

Será que $j * i = 1$?

Supondo que $*$ é associativa, $(j * i) * j = j * (i * j) = j * 1 = j = 1 * j$. Se $j * i \neq 1$, na coluna j aparece duas vezes o elemento j , na linha 1 e na linha $j * i$, o que é absurdo. Então, $j * i = 1$.

Então, j é o inverso de i .

Isto reduz o problema de saber se $(G,*)$ é grupo ao de saber se $\varphi(G)$ é um subgrupo de $A(G)$, ou seja, de saber se a composta de quaisquer duas permutações de $\varphi(G)$ é ainda uma permutação em $\varphi(G)$, o que se conclui pela análise das linhas do quadrado latino, pois cada permutação destas é uma linha do quadrado latino. ■

Teorema 2.14.: (RL_n, \cdot) é um grupo de ordem $(n!)^n$.

Demonstração: Sejam $A = (f_1, \dots, f_n)$, $B = (g_1, \dots, g_n)$ e $C = (h_1, \dots, h_n)$ elementos de RL_n .

i. A operação é associativa pois,

$$\begin{aligned} A(BC) &= A(g_1 h_1, \dots, g_n h_n) \\ &= (f_1(g_1 h_1), \dots, f_n(g_n h_n)) \\ &= ((f_1 g_1) h_1, \dots, (f_n g_n) h_n) \\ &= (AB)C ; \end{aligned}$$

ii. Existe $E \in RL_n$ para todo $A \in RL_n$ tal que $E = AE = A$, basta tomar a matriz $E = (e, e, \dots, e)$, onde e é a permutação identidade.

iii. Para qualquer $A \in RL_n$ existe $B \in RL_n$ tal que $AB = BA = E$, basta tomar $B = (f_1^{-1}, \dots, f_n^{-1})$.

Por i., ii. e iii. tem-se que RL_n é um grupo para a operação \cdot e $|RL_n| = (n!)^n$, pois dado $A = (f_1, \dots, f_n)$ tem-se $n!$ possibilidades para cada linha e como se tem n linhas, (RL_n, \cdot) é um grupo de ordem $(n!)^n$. ■

Lema 2.15.: Sejam $R \in RL_n$ e $E = (e, \dots, e)$, onde e denota a permutação identidade. E e R são ortogonais se, e só se, R é um quadrado latino.

Demonstração:

(\Rightarrow) R e E são ortogonais. Como $R \in RL_n$, é suficiente provar que $a_{ij} \neq a_{kj}$ sempre que $i \neq k$. Na concatenação de R por E temos que o par (a_{ij}, j) aparece na linha i e coluna j , enquanto o par (a_{kj}, j) aparece na linha k e coluna j .

Como R e E são ortogonais e $(i, j) \neq (k, j)$ temos $(a_{ij}, j) = (a_{kj}, j)$ e assim, $a_{ij} \neq a_{kj}$. Então R é um quadrado latino.

(\Leftarrow) Sendo R um quadrado latino, tomando o elemento a_{ij} de R , (a_{ij}, j) só pode ocorrer uma vez, e portanto, R e E são mutuamente ortogonais. ■

Lema 2.16.: Seja $\{A_1, \dots, A_m\}$ um conjunto de quadrados latinos linha mutuamente ortogonais. Assim, para qualquer quadrado latino linha X , o conjunto $\{A_1X, \dots, A_mX\}$ é um conjunto de quadrados latinos linha mutuamente ortogonais.

Demonstração: Basta demonstrar que se A é ortogonal a B , então AX é ortogonal a BX . Desta forma, suponha-se que o par (u, v) ocorre na linha m e na coluna p e também na linha n e coluna q , quando AX é concatenado com BX , com $m \neq n$ ou $p \neq q$.

Seja $x(m, p)$ o elemento que se encontra na linha m e coluna p do quadrado latino linha X .

Assim, se $x(m, p) \in X$, vem

$$u = a(m, x(m, p)) = a(n, x(n, q)) \quad \text{e} \quad v = b(m, x(m, p)) = b(n, x(n, q)),$$

o que significa que o par (u, v) ocorre em duas posições diferentes na concatenação de A com B - linha m e na coluna $x(m, p)$ e também na linha n e coluna $x(n, q)$. Mas isto contradiz o facto de A e B serem ortogonais.

Daqui conclui-se que, AX e BX são ortogonais. ■

Teorema 2.17.: Sejam A e B dois quadrados latinos linha. A e B são ortogonais se e só se existe um quadrado latino L tal que $LA = B$.

Demonstração:

(\Rightarrow) Se A é ortogonal a B , vamos construir um quadrado latino linha L tal que $LA = B$. Seja A^{-1} o quadrado latino linha no qual cada linha é a permutação inversa da correspondente linha de A , tal que $AA^{-1} = E$. Seja $L = BA^{-1}$. Como A e B são ortogonais, do Lema 2.16. tem-se que L é ortogonal a E , e pelo Lema 2.16. L é um quadrado latino.

(\Leftarrow) Reciprocamente, seja L um quadrado latino tal que $LA = B$. Mas L é ortogonal a E . Usando o Lema 2.15., LA é ortogonal a EA e assim, B é ortogonal a C . ■