Universidade de Aveiro
Ano 2008

Departamento de Matemática

Cecilia Solange Gomes Godinho

Alguma da Matemática do Sudoku

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 científica, apoio e disponibilidade.

À minha amiga e colega de Mestrado, Andreia Morgado, pelo companheirismo e apoio com que ultrapassamos as dificuldades encontradas.

A toda a minha família, pelo apoio e compreensão nos momentos mais difíceis.

À minha grande amiga Ana Pinto, pelo incentivo e ânimo que sempre me transmitiu.

o júri

Presidente

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

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

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

palavras-chave Quadrados Latinos, MOLS, Plano afim, Plano projectivo, Sudoku.

resumo

Neste trabalho o objectivo principal é fazer um estudo de alguma da Matemática presente no conhecido puzzle Sudoku.
Dado que o tema da presente dissertação foi proposto a duas alunas, e como se tratava de um assunto novo para ambas, os dois primeiros capítulos resultam de um trabalho conjunto com a minha colega Andreia Cristina Dias Morgado.
Os conceitos introdutórios serão apresentados no primeiro capítulo, onde se abordarão os Quadrados Latinos e as suas principais características.
No segundo capítulo exibimos as aplicações dos Quadrados Latinos à Teoria de Grupos.
No terceiro capítulo abordamos alguns resultados importantes no estudo das Geometrias finitas, nomeadamente no que diz respeito aos planos afins e projectivos, mostrando-se como se pode obter um deles à custa do outro. Serão abordadas também as principais relações destes planos com os Quadrados Latinos.
Por fim, no quarto capítulo faz-se uma análise da relação entre as propriedades dos Quadrados Latinos e do Sudoku, desenvolvendo-se um pouco da história do aparecimento deste puzzle, o modo como se joga e os níveis de dificuldade. Além disso, serão apresentadas algumas variantes do puzzle, finalizando-se com o problema das possíveis colorações parciais de um Sudoku.

keywords Latin Squares, MOLS, Affine plan, Projective plan, Sudoku.

abstract

In this work, the main aim is to make a study of some Mathematics presents in the Sudoku puzzle we know so well.
Since the theme of this dissertation was purposed to two students, and since this was a new subject for both, the first two chapters resulted from a work, made by me and my colleague Andreia Cristina Dias Morgado.
The introductory concepts will be presented in the first chapter, where we will make reference to the Latin Square and its main features.
In the second chapter we show the applications of Latin Squares to the Theory of Groups.
In the third chapter we will present some important results of the study of finite Geometries, particularly with what is concerned to affine plans and projective plans. We show how to get one from another. It also studies the main relations of these ones with the Latin Squares.
Finally, the fourth chapter is an analysis of the relation between the properties of Latin Squares and Sudoku, developing a bit of history from the beginning of this puzzle and how to play it and its difficulty levels. In addition, we will present some variants of the puzzle, ending with the problem of possible partial colorations of a Sudoku.

ÍNDICE

INTRODUÇÃO

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 respectivamente 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 exactamente 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. Além disso, há ainda resultados sobre Quadrados Latinos que são influenciados por várias áreas, dentro e fora da combinatória, como a Álgebra, a Geometria Finita, a Estatística, e outras, entre as quais a Criptografia.

1. QUADRADOS LATINOS

1.1. CONCEITOS BÁSICOS

Os primeiros registos da utilização de quadrados latinos foram verificados em 1639, num jogo de cartas.

O primeiro matemático que publicou um texto sobre quadrados latinos foi Leonhard Euler em 1783, texto esse que se referia a aplicações da estatística. O nome **quadrados latinos** deve-se ao facto de Euler ter usado letras latinas para os seus quadrados.

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 exactamente uma vez em cada linha e coluna, designam-se por quadrados latinos de ordem n.

Proposição 1.2.: 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 $0,1,...,n-1$. Assim, a linha seguinte será $1,2,...,n-1,0$, continuando-se o processo até à última linha.

Desta forma, obtém-se o seguinte quadrado latino:

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

□

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

Definição 1.3. (*Quadrado latino reduzido ou normalizado*)**:** Um quadrado latino designa-se por reduzido ou normalizado, se a primeira linha e coluna são da forma $0 \quad 1 \quad 2 \quad \cdots \quad n-1$.

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

□

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	75807214831601328114892800
11	$\simeq 5.36\times10^{33}$
12	$\simeq 1.62\times10^{44}$
13	$\simeq 2.51\times10^{56}$
14	$\simeq 2.33\times10^{70}$
15	$\simeq 1.5\times10^{86}$

Até hoje são apenas conhecidos valores exactos 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.

1.2. QUADRADOS LATINOS MUTUAMENTE ORTOGONAIS

Definição 1.5. (*Quadrados latinos ortogonais*)**:** Seja n um inteiro positivo. Dois quadrados latinos dizem-se ortogonais se os pares de números formados pelas entradas de cada quadrado na mesma linha e na mesma coluna aparecem sem repetição. Isto é, L' e L'' são considerados quadrados latinos ortogonais se para qualquer par de símbolos (α,β) existe uma única entrada (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 1.6. (*Matriz Concatenada*)**:** Dadas duas matrizes $n \times n$, $L' = \left(\alpha_{ij}\right)$ e $L'' = \left(\beta_{ij}\right)$, a matriz concatenada é a matriz $n \times n$, $C = \left(\alpha_{ij}, \beta_{ij}\right)$, 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 representados pelas 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 $n \equiv 2 (\mathrm{mod} 4)$, 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 excepção de $n = 2$ e $n = 6$.

Definição 1.7. (*Conjunto mutuamente ortogonal de quadrados latinos*)**:** Seja $A = \{L_1, ..., L_k\}$ 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).

Agora pretende-se 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 1.8.: 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 $(0,1,\ldots,n-1)$. Suponha-se que,

$$L_1 = \begin{matrix} 0 & 1 & \cdots & n-1 \\ x & - & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \cdots & - \end{matrix} \qquad \text{e} \qquad L_2 = \begin{matrix} 0 & 1 & \cdots & n-1 \\ y & - & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \cdots & - \end{matrix}$$

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, $N(n) \leq n-1$.

□

Definição 1.9. (*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 1.10.: 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 $N(4)=3$.

1.3. CONSTRUÇÃO DE CONJUNTOS COMPLETOS DE MOLS

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

- **Interpretação Geométrica**

Os exemplos já falados anteriormente (o exemplo das três variedades de plantas e o exemplo dos trinta e seis oficiais) são simples casos onde os quadrados latinos têm uma aplicação natural, mas existem ainda muitos outros exemplos no contexto da matemática pura.

Como se verá mais à frente, no capítulo dos Planos Afins e Projectivos, a existência de um plano afim de ordem n é equivalente à existência de um conjunto completo de $n-1$ quadrados latinos de ordem n ortogonais dois a dois.

Existe um plano afim de ordem n se n é uma potência de um número primo.

Veremos como construir um conjunto completo de MOLS associado a um plano afim de ordem n, em que n é potência de um primo.

Considere-se o exemplo seguinte, que usa conceitos básicos de álgebra linear. Suponha-se que se tem um vector do espaço a duas dimensões F_q^2 no corpo finito F_q, de q elementos, onde q é potência de um primo. Existem q^2 pontos neste espaço, identificados pelos pares ordenados (x, y), onde $x, y \in F_q$. Um subespaço de dimensão 1 de F_q^2 consistirá em q pontos que satisfazem uma equação linear da forma, $ax + y = 0$ ou $x = 0$, onde $a \in F_q$.

Porque estes subespaços são de dimensão 1 e são dados algebricamente por equações lineares, é natural que se pense neles como rectas, em particular rectas que passam pela origem. Suponha-se que é adicionada uma constante diferente de zero ao 2º membro da equação de um desses subespaços. A nova equação especifica q pontos que constituem uma recta paralela à recta correspondente ao subespaço.

Então, dada uma família de rectas paralelas da forma $ax + y = s$, onde $a \neq 0$ podemos associar-lhe um quadrado latino em que o símbolo s aparece nas posições (x, y) que verificam a equação para cada s. Além disso, quaisquer dois quadrados latinos serão ortogonais, porque para $a_1 \neq a_2$, o sistema de equações,

$$\begin{cases} a_1 x + y = s \\ a_2 x + y = t \end{cases}$$

tem exactamente uma solução. Isto implica que o par ordenado (s, t) ocorrerá exactamente uma vez na concatenação do quadrado latino derivado da família de rectas com declive a_1 com o quadrado obtido das rectas com declive a_2.

Uma vez que se constroem quadrados latinos ortogonais a partir de famílias de rectas paralelas, e se pode obter uma tal família para cada elemento de F_q diferente de zero, é razoável concluir que um conjunto de quadrados latinos mutuamente ortogonais nesta situação incluirá $q - 1$ membros.

Para $q = 5$ ver exemplo nas páginas 34 e 35 (Capítulo 3).

Vimos assim uma forma de construir um conjunto completo de MOLS de ordem q quando q é potência de um primo.

- **Interpretação Algébrica**

Aqui far-se-á uma interpretação algébrica do que foi feito anteriormente.

Considere-se então a construção de conjuntos de MOLS de ordem n tal que $n = p^m$, com p primo. Estas construções estão intimamente ligadas à teoria de 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 atribuam-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. Não é condição necessária, mas convém assumir que os q elementos serão listados na mesma ordem tanto para linhas como para colunas. 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.

Segue-se o teorema fundamental deste capítulo:

Teorema 1.11.: 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 $ax_1 + y_1 = ax_1 + y_2$, 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 $q-1$.

□

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 correspondente 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:

$$L_1 = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix} \qquad \text{e} \qquad L_2 = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

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.

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

Exemplo 1.13.: 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 irredutível 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	$\alpha+1$
1	0	$\alpha+1$	α
α	$\alpha+1$	0	1
$\alpha+1$	α	1	0

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

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

que são representados, respectivamente, 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..

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

Tendo efectivamente 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 que se q não é primo, F_q é apenas um anel com unidade e não um corpo, não herdando as importantes propriedades da teoria de 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!

Agora, para números que não são potências de primos como $n=10,12,15,20,...$ 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 1.14. (*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:

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

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

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

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

$$A=\begin{matrix}0 & 1\\ 1 & 0\end{matrix} \qquad B=\begin{matrix}0 & 1 & 2\\ 1 & 2 & 0\\ 2 & 0 & 1\end{matrix}$$

O produto de Kronecker requer a construção de um quadrado de ordem 6 cujos elementos são pares ordenados[(i)]:

00	01	02	10	11	12
01	02	00	11	12	10
02	00	01	12	10	11
10	11	12	00	01	02
11	12	10	01	02	00
12	10	11	02	00	01

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 1.15.: 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 $A_2 \otimes B_2$.

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 $\left(\left(a_{ij}, b_{kl}\right),\left(a_{pq}, b_{rt}\right)\right)$ da respectiva matriz concatenada $\left(A_1 \otimes B_1\right) \odot \left(A_2 \otimes B_2\right)$, e suponha-se que este par está repetido em $\left(A_1 \otimes B_1\right) \odot \left(A_2 \otimes B_2\right)$. Porém os pares $\left(a_{ij}, a_{pq}\right)$ e

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

(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.

□

Exemplo 1.16.: 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, respectivamente:

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

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

$C_1 =$

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				
10	11	12	13	20				00			
11	10	13	12								
12	13	10	11								
13	12	11	10								
20				00				10			
21											
22											
23											

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

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

Proposição 1.17.: Se $n \equiv 0,1,3 \pmod 4$, tem-se que $N(n) \geq 2$.

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

Aplicando o Teorema 1.11. e o Teorema 1.15., podem construir-se pelo menos dois MOLS de ordem n.

□

Resta analisar-se o caso $n \equiv 2 \pmod 4$ (conjectura de Euler). Assim para $n = 2(2k+1)$, a menor potência de um número primo na factorização 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 qual está enunciado abaixo:

Teorema 1.18.: Para todo n, excepto 2 e 6, existe pelo menos um par de MOLS de ordem n, isto é, para todo n, excepto 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 1.15..

Teorema 1.19.: Seja $q_1 \times ... \times q_r$ a factorização de n em potências de números primos distintas com $q_1 < ... < q_r$. Então, $N(n) \geq q_1 - 1$.

Demonstração: Para cada potência prima q_i na factorização de n, pode-se construir, um conjunto de $q_i - 1$ MOLS de ordem q_i, pelo Teorema 1.11.. 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.

□

Motivado pela conjectura de Euler, MacNeish conjecturou em 1922 o seguinte resultado:

Conjectura 1.20.: Se $q_1 \times ... \times q_r$ é a factorização de n em potências de números primos distintos com $q_1 < ... < q_r$, então $N(n) = q_1 - 1$.

Porém, sabe-se hoje que esta conjectura 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 factorização de n. Por exemplo, para $n \leq 100$, a conjectura 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 (por exemplo, para $n=91$ e $n=96$) onde o número de MOLS ultrapassou o valor dado pelo produto de Kronecker e pelo Teorema 1.11..

1.4. 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:

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

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 $L_1 \odot L_2$, o que contradiz a ortogonalidade. Logo, $p = 2$ e consequentemente, $q = 1$ ($q = 0$ faria ocorrer $(0,0)$ em duas posições de $L_1 \odot L_2$) 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 exactamente 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 1.21.: Um quadrado latino de ordem n tem companheiro ortogonal se e só se contém n transversais disjuntos.

Exemplo 1.22.: Considerem-se os quadrados latinos L e M ortogonais:

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

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 disjuntos. E reciprocamente, a cada símbolo/cor do quadrado M corresponde um transversal do quadrado L, que tem também 3 transversais disjuntos.

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 1.23.: 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 1.24.: Considere-se o seguinte quadrado latino L e o seu transposto L^T :

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

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 ao seu transposto L^T .

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. (*Grupóide*)**:** Um grupóide 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 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;
- $(Z_n,+)$, onde Z_n denota o conjunto dos inteiros $\{0,1,\ldots,n-1\}$ 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).
- $(R^*,\times)$, 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 Z_n denota o conjunto dos inteiros $\{0,1,\ldots,n-1\}$ e $+$ denota a adição módulo n.

Se M é um conjunto com n elementos distintos, a função $f: M \to M$ é uma permutação de M se f é bijectiva (injectiva e sobrejectiva). A função f diz-se injectiva se para $a, b \in M$, $f(a) = f(b)$ implica que $a = b$. Por outro lado, f diz-se sobrejectiva se para todo o $d \in M$, existir um $c \in M$ tal que $f(c) = d$.

Finalmente, se f e g são ambas permutações de um conjunto M, pode-se definir uma terceira permutação h, chamada de composição 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 ($i = 1, 2, \ldots n$) 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.

Exemplo 2.7.: Se $M = \{1, 2, 3, 4\}$, considere-se a permutação $f: M \to M$ 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 $(3 \quad 2 \quad 4 \quad 1)$.

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.

*	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

Na tabela, $a*b \equiv (a+b) \bmod 5$. 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.

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

Demonstração: Suponha-se que na linha a [iii] 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, por isso, o quadrado é latino sobre essa linha. Analogamente, todos os elementos de cada coluna são distintos, logo o quadrado é também latino sobre as colunas.

□

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,

[ii] Ou tabela da operação.

[iii] Designamos por linha a a linha correspondente aos produtos da forma $a*i$, onde $i \in G$.

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 monóide (grupóide com elemento neutro).

Ideia da demonstração:

Por exemplo, o seguinte quadrado latino pode ser encarado como a tabela da operação $*$ de um grupóide $G=\{a,b,c,d\}$, 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

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 $\{1,2,\ldots,N\}$. 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 $i \in \{1,2,\ldots,N\}$. 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.

Resta então provar que a lei associativa é válida no conjunto $G = \{1,2,\ldots,N\}$ com a operação binária $*$ definida pelo quadrado latino.

Defina-se φ em $A(G)$, que é o conjunto de todas as permutações em G, por:

$$\begin{aligned} \varphi : G &\to A(G) \\ a \mapsto \varphi_a : G &\to G \\ x &\mapsto a * x, \quad \forall x \in G \end{aligned}$$

Ou seja, φ é a função que a cada elemento $a \in G$ faz corresponder a permutação evidenciada na linha a do quadrado latino, que denotamos por φ_a.

Obviamente, φ_a é uma permutação de G por definição de quadrado latino. Em cada linha, estão representados todos os elementos de G, sem repetição.

Note-se que, φ_1 é a permutação identidade:

$$\begin{aligned} \varphi_1 : G &\to G \\ x &\mapsto 1 * x, \quad \forall x \in G \end{aligned}$$

Sabe-se que $A(G)$ é um grupo para a composição.

Para provar que $(G,*)$ é um grupo, falta provar a associatividade da lei $*$:

Como,

$$\begin{aligned} \varphi_{a*b} : G &\to G \\ c &\to (a*b)*c \end{aligned} \quad \text{e} \quad \begin{aligned} \varphi_a : G &\to G \\ b*c &\to a*(b*c) \end{aligned},$$

a associatividade de $*$, $(a*b)*c = a*(b*c)$, $\forall a,b,c \in \{1,\ldots,N\}$, pode traduzir-se da seguinte forma: $\varphi_{a*b}(c) = \varphi_a(b*c), \forall a,b,c \in \{1,\ldots,N\}$ ou ainda, $\varphi_{a*b}(c) = \varphi_a(\varphi_b(c)), \forall a,b,c \in \{1,\ldots,N\}$ ou $\varphi_{a*b} = \varphi_a \circ \varphi_b, \forall a,b \in \{1,\ldots,N\}$.

Provar a lei associativa em G, $(a*b)*c = a*(b*c)$, $\forall a,b,c \in \{1,\ldots,N\}$, é portanto, equivalente a provar que $\varphi_a \circ \varphi_b = \varphi_{a*b}$, $\forall a,b \in G$.

Se isto for verdade, então $\varphi(G)$ será um subgrupo de $A(G)$, porque o produto de dois elementos de $\varphi(G)$ é um elemento de $\varphi(G)$ e o elemento neutro (a identidade, φ_1) pertence a $\varphi(G)$.

Inversamente, se $\varphi(G)$ é um subgrupo de $A(G)$, a lei associativa verifica-se, pois $\varphi_a \circ \varphi_b = \varphi_c$, para algum c em G.

Para isso, considere-se $c = a*b$, então:

$$\varphi_a \circ \varphi_b(1) = \varphi_a(b*1) = \varphi_a(b) = a*b = c \quad \text{e} \quad \varphi_c(1) = c*1 = c.$$

Logo, $\varphi_a \circ \varphi_b = \varphi_{a*b}$.

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.

□

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

$$\begin{array}{lcccccc} \varphi_1 & \to & 1 & 2 & 3 & 4 & 5 \\ \varphi_2 & \to & 2 & 5 & 4 & 1 & 3 \\ \varphi_3 & \to & 3 & 1 & 2 & 5 & 4 \\ \varphi_4 & \to & 4 & 3 & 5 & 2 & 1 \\ \varphi_5 & \to & 5 & 4 & 1 & 3 & 2 \end{array}$$

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

De facto, $\varphi_3 \circ \varphi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \bullet \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$. 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 composições 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 $M=\{1,2,\ldots,n\}$ e define-se a operação $\bullet : RL_n \times RL_n \to RL_n$ que, a cada par $(A,B) \in RL_n \times RL_n$, faz corresponder $AB \in RL_n$ do seguinte modo:

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

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

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

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

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

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

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

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

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

i. A operação é associativa pois,

$$\begin{aligned} A(BC) &= A(g_1h_1, \ldots, g_nh_n) = (f_1(g_1h_1), \ldots, f_n(g_nh_n)) = \\ &= ((f_1g_1)h_1, \ldots, (f_ng_n)h_n) = \\ &= (AB)C \end{aligned} \quad ;$$

ii. Existe $E \in RL_n$ para todo $A \in RL_n$ tal que $AE = EA = A$, basta tomar a matriz $E = (e, e, \ldots, e)$, 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 $B = (f_1^{-1}, \ldots, f_n^{-1})$.

Por i., ii. e iii. tem-se que RL_n é um grupo para a operação $\bullet$ e $|RL_n| = (n!)^n$, pois dado $A = (f_1, \ldots, f_n)$ tem-se $n!$ possibilidades para cada linha e como se tem n linhas, $(RL_n, \bullet)$ 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 $E = (e, \ldots, e)$, onde e denota a permutação identidade. E e R são ortogonais se, e só se, R é um quadrado latino.

Demonstração:

$(\Rightarrow)$ 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, $a_{ij} \neq a_{kj}$.

$(\Leftarrow)$ 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 $\{A_1, \ldots, A_m\}$ um conjunto de quadrados latinos linha mutuamente ortogonais. Assim, para qualquer quadrado latino linha X, o conjunto $\{A_1X, \ldots, A_mX\}$ 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 $u = a(m, x(m, p)) = a(n, x(n, q))$ e $v = b(m, x(m, p)) = b(n, x(n, q))$, 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 Teorema 2.17., LA é ortogonal a EA e assim, B é ortogonal a C.

□

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

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

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

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

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

Verificação:

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

3. PLANOS AFINS E PROJECTIVOS

3.1. PROPRIEDADES BÁSICAS

Considere-se um sistema geométrico de pontos e rectas que satisfazem os seguintes três axiomas:

A_1) Por quaisquer dois pontos passa uma única recta;

A_2) Dado um ponto P e a recta l que não contém P, existe uma única recta que contém P e que não intersecta l.

A_3) Existem 4 pontos de tal forma que quaisquer três deles não são colineares.

O axioma A_1 simplesmente especifica que quaisquer dois pontos definem uma única recta, o axioma A_2 introduz a noção de paralelismo e o axioma A_3 elimina o caso trivial de uma dimensão onde todos os pontos são colineares. O plano que satisfaz estes três axiomas designa-se por **Plano afim.** O plano euclideano é um exemplo desta estrutura geométrica.

Falar-se-á de planos afins finitos, que são planos em que o número de pontos e rectas é finito. Em contraste à "continuidade" da versão euclideana de uma recta, as rectas agora estudadas consistirão numa colecção finita de pontos. Similarmente, qualquer ponto encontrar-se-á num só número finito de rectas. Para um plano afim finito existir terão de ser satisfeitas simples relações que envolvem um número finito de pontos e rectas.

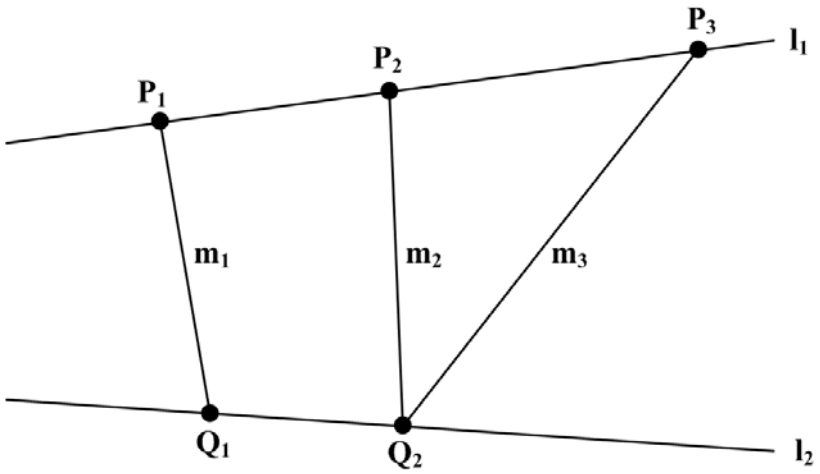
Lema 3.1.: Num qualquer plano afim finito, existe um inteiro positivo n tal que toda a recta contém exactamente n pontos e todo o ponto pertence a exactamente $n+1$ rectas.

Demonstração: Seleccionem-se quaisquer duas rectas l_1 e l_2. Suponha-se que todos os pontos se situam numa ou noutra. Então, por **A_3**, existem 4 pontos P_1, P_2, Q_1, Q_2, dois deles em cada recta. Suponha-se agora que l_1 contém um terceiro ponto sendo $\{P_1, P_2, P_3, ...\}$ o conjunto de pontos de l_1 e $\{Q_1, Q_2, ...\}$ é o conjunto de pontos em l_2.

Considerem-se agora as rectas m_1, m_2 e m_3, onde:

- m_1 une P_1 e Q_1;
- m_2 une P_2 e Q_2;

- m_3 une P_3 e Q_2.



Se m_1 e m_3 se intersectam, o ponto de intersecção será de l_1 ou l_2. Se fosse P_1, m_3 coincidiria com l_1. Se fosse P_3, m_1 coincidiria com l_1. Se fosse Q_1, m_3 coincidiria com l_2. Se fosse Q_2, m_1 coincidiria com l_2. Se fosse P_2, m_2 coincidiria com m_3. Então, m_1 e m_3 não se podem intersectar, pelo Axioma **A₁**. Mas se m_1 e m_3 não se intersectam, existem duas rectas que passam por Q_2 e são paralelas a m_1, o que contradiz **A₂**. Suponha-se que esse ponto é P_2. Isto significa que l_1 e l_2, ambas contém exactamente dois pontos, tal como as outras rectas.

Porque existem seis modos de escolher um subconjunto de duas rectas a partir de um conjunto de 4 pontos dados ($C_2^4 = 6$), e porque exactamente três dessas escolhas contém um ponto específico, o sistema geométrico que satisfaz **A₁**, **A₂** e **A₃** conterá seis rectas, 3 delas que passam por um ponto específico. Por isso, $n = 2$ no caso onde 2 rectas contém todos os pontos.

Se l_1 e l_2 não contém todos os pontos, então existe algum ponto P que não está em qualquer das duas. Por **A₁** existe uma recta que passa por P e por cada ponto de l_1, e por **A₂** exactamente uma recta que passa por P disjunta de l_1 (*). O mesmo é verdade para as rectas que passam por P e pelos pontos de l_2. Se o número de pontos de l_1 for dado por $v_{l_1} = n$, então contando as rectas que passam por P, tem-se, $v_{l_1} + 1 \underset{(*)}{=} v_{l_2} + 1 = n + 1$ e portanto, $v_{l_1} = v_{l_2} = n$.

□

O número de pontos de uma recta é chamado de **ordem de um plano afim finito.** O número total de pontos e rectas do plano são fixos para uma dada ordem.

Lema 3.2.: Um plano afim finito de ordem n contém n^2 pontos.

Demonstração: Qualquer ponto P pertence a $n+1$ rectas, cada uma delas contendo $n-1$ pontos distintos de P.

Por $\mathbf{A_1}$ cada um dos pontos do plano é colinear com P, ou seja, pertence a uma das $n+1$ rectas que passam por P. Assim, existem $(n+1)(n-1)+1=n^2$ pontos no plano.

□

No próximo lema examinar-se-á uma família de rectas paralelas. Para isso, adoptar-se-á a convenção de que qualquer recta é paralela a ela própria. Por isso, estabelece-se que o paralelismo possui a propriedade reflexiva, o que significa que o paralelismo é uma relação de equivalência.

Lema 3.3.: Num plano afim finito de ordem n, existem exactamente n^2+n rectas que são particionadas em $n+1$ classes de rectas paralelas, cada uma contendo n rectas.

Demonstração: Sejam l_1 e l_2 quaisquer duas rectas não-paralelas. Por cada ponto de l_2 passa uma recta paralela a l_1, l_1 incluída. Então, existem n rectas paralelas na classe de equivalência que contém l_1. Cada uma das $n+1$ rectas passa por um ponto pertencente a uma classe de n membros, o que perfaz um total de n^2+n rectas.

□

As configurações dadas na Figura 1 e Figura 2 mostram, respectivamente, planos afins de ordem 2 e 3.

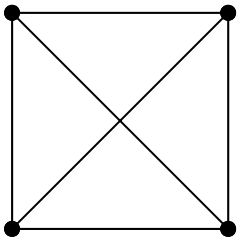


Figura 1 – Plano afim de ordem 2.

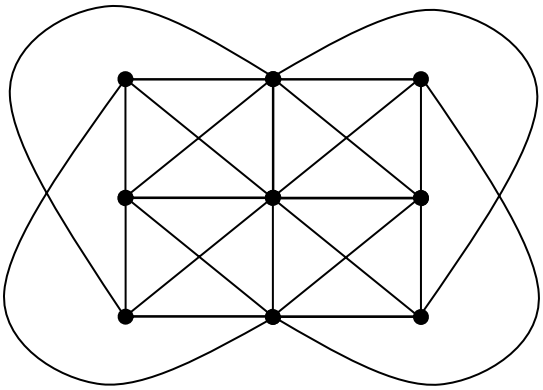


Figura 2 – Plano afim de ordem 3.

3.2. INTERPRETAÇÃO ALGÉBRICA

Comece-se por relembrar a representação algébrica de pontos e rectas no plano euclidiano. Neste caso, existe uma correspondência bi-unívoca entre o conjunto dos pontos de uma recta e o dos números reais. Portanto, cada ponto do plano é representado por um par ordenado (x, y) de reais.

A única recta contendo dois pontos, $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$, com $x_1 \neq x_2$, especificada pelo axioma A_1, é dada por $y = mx + b$ com declive $m = \frac{y_2 - y_1}{x_2 - x_1}$ e intersecta y em $b = y_1 - mx_1$ (se $x_1 = x_2$ a recta é dada por $x = x_1$).

Além disso, a única recta dada pelo axioma A_2, que passa pelo ponto $P_0 = (x_0, y_0)$ e é paralela à recta $y = mx + b$ é dada por $y = mx + y_0 - mx_0$.

Claramente, as propriedades da geometria euclidiana estão interligadas com as dos números reais.

Suponha que decidia fazer os cálculos nas equações anteriores utilizando F_q, o corpo finito de q elementos, em vez do corpo dos números reais.

Como veremos, isto pode ser feito sem violar qualquer dos três axiomas que, colectivamente definem um plano afim.

O plano afim finito construído desta forma, usando equações lineares sobre o corpo finito F_q, será designado por $AG(2,q)$.

Se os elementos do corpo considerado forem identificados com os pontos de uma recta, temos a situação surpreendente de qualquer recta conter apenas q pontos. Isto é, num plano afim finito, uma recta é uma colecção finita de pontos disjuntos.

Isto contrasta radicalmente com a concepção euclidiana de uma recta ser um conjunto infinito contínuo de pontos.

Além disso, existem exactamente q^2 pares ordenados (x,y) distintos, onde $x,y \in F_q$, dando precisamente o número de pontos estipulados pelo Lema 3.2. para um plano finito com q pontos numa recta.

Como exemplo, suponha-se que $q=5$ e que se deseja encontrar uma recta $y=mx+b$ que una os pontos $(1,2)$ e $(3,0)$ no plano $AG(2,5)$.

Para isso, executar-se-á, simplesmente, o cálculo módulo 5. Então, $m=\frac{0-2}{3-1}=\frac{3}{2}=4$ e $b=y_1-mx_1=2-(4\times 1)=3$, sendo a recta requerida $y=4x+3$.

Esta recta contém 5 pontos correspondentes aos casos $x=0,1,2,3,4$.

Os valores de y para estes casos são:

$$y(0)=4\times 0+3=3$$

$$y(1)=4\times 1+3=2$$

$$y(2)=4\times 2+3=1$$

$$y(3)=4\times 3+3=0$$

$$y(4) = 4 \times 4 + 3 = 4$$

Sendo traçados da seguinte forma:

	$y=0$	$y=1$	$y=2$	$y=3$	$y=4$
$x=0$	$-$	$-$	$-$	$\times$	$-$
$x=1$	$-$	$-$	$\times$	$-$	$-$
$x=2$	$-$	$\times$	$-$	$-$	$-$
$x=3$	$\times$	$-$	$-$	$-$	$-$
$x=4$	$-$	$-$	$-$	$-$	$\times$

No plano euclidiano, dois pontos distintos de uma recta, com declive m não nulo, terão as coordenadas distintas em x e em y. Pela mesma razão, dois dos cinco pontos determinados anteriormente não partilham uma linha ou coluna comum.

Do axioma $\mathbf{A_2}$, infere-se a noção bem conhecida, que rectas paralelas têm o mesmo declive.

Para se encontrar a recta paralela a $y = 4x + 3$ contendo o ponto $(3,3)$, fixa-se $b = 3 - 4(3) = 1$, obtendo-se a recta $y = 4x + 1$.

Analise-se agora a classe de rectas paralelas $y = 4x + b$, onde $b = 0,1,2,3,4$.

Colectivamente, as cinco rectas dividem o plano em cinco conjuntos de cinco pontos.

Individualmente, cada recta identifica cinco pontos, dos quais não há dois que estejam na mesma linha ou coluna.

Se se identificar cada um dos cinco conjuntos por um símbolo, por exemplo o valor de b na equação da recta associada, então é obtido o seguinte quadrado:

$$L_4 = \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{matrix}$$

Claramente cada classe de rectas paralelas com declive $m = 1,2,3,4$ origina quadrados latinos deste tipo. Para os distinguir, identifica-se o quadrado acima por declive comum $m = 4$ da classe das rectas que o gerou.

Por exemplo, a recta $y = 4x\ (b = 0)$ passa pelos pontos $(0,0)$, $(1,4)$, $(2,3)$, $(3,2)$, $(4,1)$, portanto, as células correspondentes de L_4 levam o símbolo 0.

No caso euclidiano, quaisquer duas rectas de classes diferentes partilham exactamente um ponto comum. Também no plano afim isso se verifica, o que se constata no caso em estudo, pois o sistema

$$\begin{cases} y = m_1 x + b_1 \\ y = m_2 x + b_2 \end{cases}$$

tem exactamente uma solução se $m_1 \neq m_2$ independentemente do conjunto no qual os cálculos são executados.

Assim, L_{m_1} e L_{m_2} são quadrados latinos ortogonais, desde que cada par ordenado (b_1, b_2), para $b_1, b_2 \in F_5$ ocorre exactamente uma vez, no ponto de intersecção das rectas dadas por $y = m_1 x + b_1$ e $y = m_2 x + b_2$.

Não somente se obtém quadrados latinos ortogonais a partir das classes das rectas paralelas, como implicitamente construímos um conjunto completo. Isto deve-se ao facto de existirem exactamente quatro dessas classes correspondendo aos declives $m = 1,2,3,4$.

O que se concretizou anteriormente pode, também, ser reproduzido em qualquer corpo finito F_q, onde q é potência de um primo, para se obter um conjunto completo de MOLS de ordem q.

Se $q = p^r$, para todo o inteiro $r \geq 2$, quando p é primo, os elementos de F_q são polinómios (ver Exemplo 1.13. para $q = 4 = 2^2$).

Estes conjuntos completos de MOLS podem ser construídos desta maneira, como é referido no Teorema 1.11., que diz que um conjunto completo de MOLS pode ser construído a de polinómios lineares sobre um conjunto finito. Tais polinómios são exactamente equivalentes às famílias de equações que representam as classes de rectas paralelas num plano afim.

Veremos que é possível relacionar directamente planos afins e MOLS sem ter de passar pelos polinómios lineares num corpo finito, isto é, sem utilizar ferramentas algébricas.

3.3. PLANOS E MOLS

Formalize-se, agora, a equivalência entre planos afins e MOLS. Para isso, trabalhar-se-á directamente com os axiomas definidos de um plano afim e a definição de conjunto completo de MOLS.

Teorema 3.4.: Existe um conjunto completo de MOLS de ordem n se e só se existe um plano afim de ordem n.

Demonstração: Dado um plano afim de ordem n, etiqueta-se arbitrariamente as $n+1$ classes de rectas paralelas como $0,1,2,...,n$ e as rectas de cada classe como $0,1,2,...,n-1$.

Então, atribuem-se as coordenadas (i,j) ao ponto de intersecção da recta i da classe 0 com a recta j da classe n, para $i,j=0,1,2,...,n-1$.

Interpretem-se as rectas das classes 0 e n como sendo, respectivamente, as linhas e colunas do quadrado latino.

Posicione-se o símbolo s na posição (i,j) do quadrado L_α se a recta s, $s=0,1,...,n-1$ da classe α, $\alpha=1,...,n-1$ contém o ponto (i,j). A propriedade do quadrado ser latino é assegurada porque qualquer recta nas classes $1,2,...,n-1$ intersecta qualquer recta de classe 0 ou n exactamente uma vez. Similarmente, qualquer recta de classe α, $\alpha=1,...,n-1$ intersecta qualquer recta de classe β, $\beta\neq\alpha,0,n$ em exactamente um ponto, o que implica a ortogonalidade dos quadrados L_α e L_β.

Reciprocamente, dado um conjunto completo de MOLS de ordem n, as linhas e as colunas fornecem, cada uma delas, uma classe de n rectas paralelas, e cada um dos $n-1$ quadrados latinos origina uma classe de rectas paralelas tomando os pontos contendo o símbolo s, $s=0,1,...,n-1$ como sendo a recta s dessa classe.

Considere-se, agora, um determinado ponto $P_1-(i,j)$. Este encontra-se em $n+1$ rectas que colectivamente contêm $(n+1)(n-1)+1=n^2$ pontos, que são a totalidade dos pontos (cada recta é um transversal que contém (i,j).

Então, qualquer outro ponto P_2 é unido por uma destas rectas a P_1, e o axioma A_1 é satisfeito.

Se l é uma recta (uma linha, uma coluna ou um transversal de um dos quadrados latinos do conjunto completo de MOLS) e $P=(i,j)$ qualquer ponto não contido na mesma, veremos que existirá uma recta contendo P que é paralela a l. Se l é uma linha (coluna), então a recta

requerida é a linha (coluna) que passa por P. Senão, os pontos contendo o mesmo símbolo de P (transversal que contém P), no quadrado latino contendo l, definem a recta referida no axioma A_2.

Por fim, para mostrar que o axioma A_3 também se verifica, basta considerar 4 pontos que correspondam a posições do tipo (i, j), $(i+1, j)$, $(i, j+1)$, $(i+1, j+1)$, em que $i, j < n$. Não há nenhuma recta que passe por quaisquer três destes pontos.

□

Para ilustrar o que se acabou de referir, considerem-se os quadrados:

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

e os quadrados latinos do conjunto completo de MOLS:

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

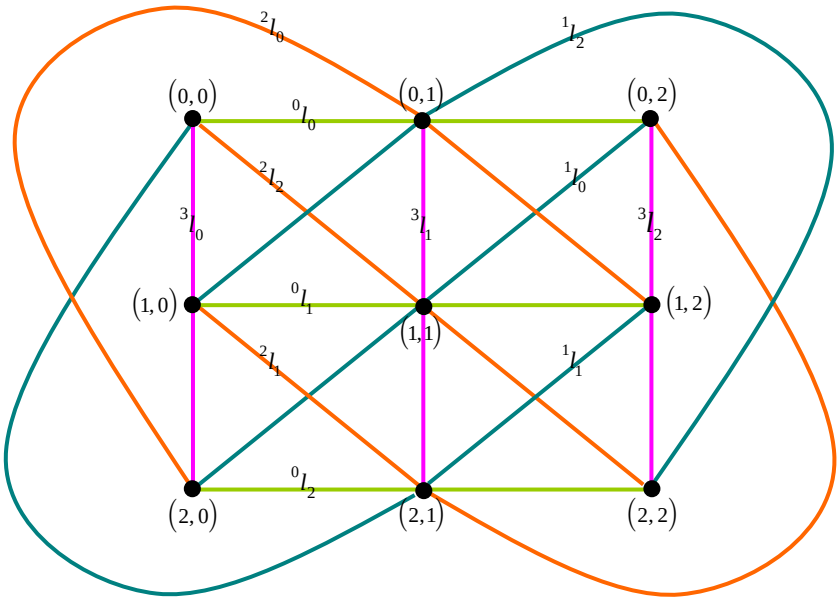
Considere-se, agora, um determinado ponto $P_1 = (2,3)$. Verifica-se que P_1 se encontra numa linha, numa coluna e num transversal de cada um dos quadrados latinos do conjunto completo de MOLS.

Portanto, P_1 encontra-se em $n-1+1+1=n+1$ rectas, representadas nos quadrados anteriores a vermelho.

Este último teorema implica que pode ser construído um plano afim para qualquer ordem q, onde q é potência de um primo.

Exemplo 3.5.: Neste exemplo ilustrar-se-á uma das implicações do Teorema 3.4., ou seja, dado um plano afim de ordem 3 como construir um conjunto completo de MOLS de ordem 3.

Considere-se o seguinte plano afim de ordem 3, no qual existem 4 classes de rectas paralelas. Cada cor representa uma classe, ${}^{\alpha}l_s$ representa a recta s da classe α, com $s=0,1,2$ e $\alpha=0,1,2,3$.



Seja (i,j) o ponto de intersecção da recta i da classe 0 com a recta j da classe n, $i,j=0,1,2$.

O quadrado latino L_1 pertencente ao conjunto completo de MOLS obtém-se da seguinte forma:

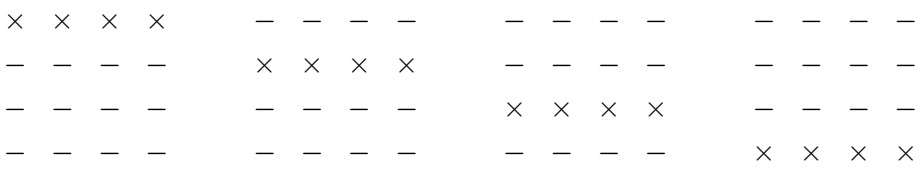
– coloca-se 0 na posição (i,j) de L_1 se a recta ${}^{1}l_0$ passar pelo ponto (i,j);

– coloca-se 1 na posição (i,j) de L_1 se a recta ${}^{1}l_1$ passar pelo ponto (i,j);

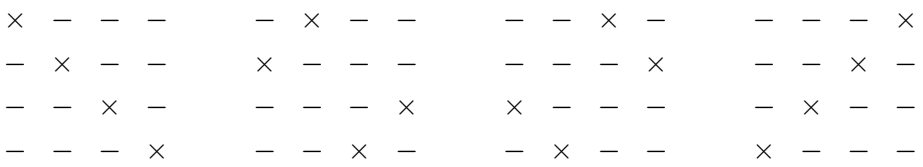
– coloca-se 2 na posição (i,j) de L_1 se a recta ${}^{1}l_2$ passar pelo ponto (i,j).

Então, $L_1=\begin{matrix}1&2&0\\2&0&1\\0&1&2\end{matrix}$ e de forma análoga, $L_2=\begin{matrix}2&0&1\\1&2&0\\0&1&2\end{matrix}$, onde L_1 e L_2 formam o conjunto completo de MOLS de ordem 3.

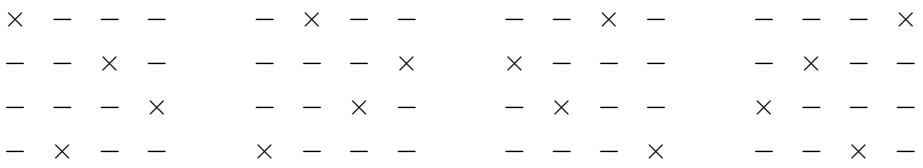
Exemplo 3.6.: Neste outro exemplo são apresentadas as rectas e classes de rectas paralelas de $AG(2,4)$:



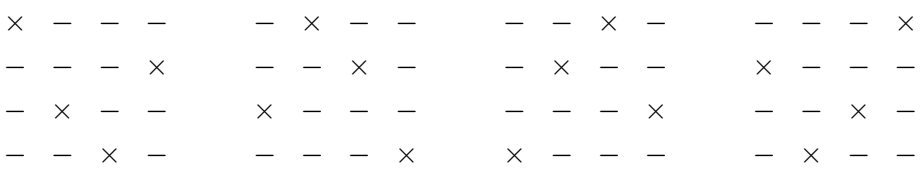
Classe 0



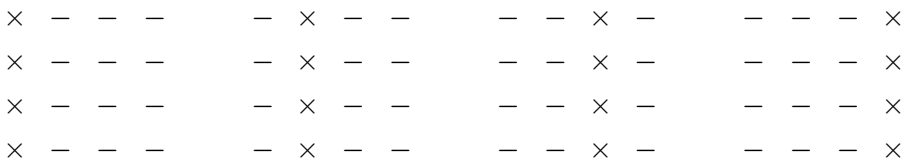
Classe 1



Classe 2



Classe 3



Classe 4

A partir delas podemos construir um conjunto completo de MOLS de ordem 4, conforme o Teorema 3.4..

As classes 0 e 4, respectivamente, fornecem as linhas e colunas dos quadrados latinos. As classes 1,2 e 3 fornecem, respectivamente, os três MOLS:

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

(estes três MOLS, ou alternativamente as rectas no plano afim $AG(2,4)$, podem ser construídas utilizando equações lineares sobre o corpo F_4, de 4 elementos).

3.4. PLANOS PROJECTIVOS

Considere-se agora o sistema geométrico baseado nos seguintes 3 axiomas:

P_1) Por dois quaisquer pontos passa uma única recta;

P_2) Quaisquer duas rectas intersectam-se num único ponto;

P_3) Existem quatro pontos, dos quais quaisquer três não são colineares.

A diferença essencial entre estes axiomas e os axiomas do plano afim, é o axioma do paralelismo, **A_2**, que é substituído por **P_2**, o qual afirma que qualquer par de rectas se intersecta num ponto, ou, de forma equivalente, não existe um par de rectas paralelas.

A estrutura geométrica definida por este sistema de axiomas é conhecida como plano projectivo. Centre-se agora o estudo nestas estruturas, naquelas em que o número de rectas e pontos são finitos. Como no caso afim, iniciar-se-á com as propriedades básicas que dizem respeito a rectas e pontos.

Lema 3.7.: Em qualquer plano projectivo finito existe um inteiro positivo n tal que toda a recta contém $n+1$ pontos e todo o ponto pertence a $n+1$ rectas.

Demonstração: Sejam l_1 e l_2 duas rectas. Pelo Axioma $\mathbf{P_2}$ as duas rectas encontram-se num ponto, seja I. Pelo Axioma $\mathbf{P_3}$, existe um ponto P que não pertence a nenhuma das rectas.

Pelos Axiomas $\mathbf{P_1}$ e $\mathbf{P_2}$, existe uma recta que une P e cada ponto de l_1, e estas constituem todas as rectas que passam por P. Assim, o número de pontos de l_1 deve ser o mesmo que o número de rectas que passam por P. Seja este número $n+1$. Podemos representar esse número desta forma

porque é superior a 1. Mas, cada recta que passa por P também intersecta l_2, então l_2 também contém $n+1$ pontos.

□

Como no caso afim, o parâmetro n é conhecido como sendo a ordem do plano.

Quando se examina a relação entre os dois tipos de planos (afim e projectivo), torna-se óbvio que, no caso projectivo, a ordem seja definida como o número de pontos por recta menos um.

Lema 3.8.: Num plano projectivo finito de ordem n existem exactamente n^2+n+1 rectas e n^2+n+1 pontos.

Demonstração: Existem $n+1$ rectas que passam por qualquer ponto P. Cada uma contém n pontos além de P, e colectivamente estes constituem todos os pontos do plano. Isto confere um total de $(n+1)n+1=n^2+n+1$ pontos.

Cada um dos n^2+n+1 pontos encontra-se em $n+1$ rectas. Se se contar as rectas, ponto por ponto, serão contabilizadas um total de $(n^2+n+1)(n+1)$ rectas. Mas este processo contabiliza cada recta $n+1$ vezes, daí o número distinto de rectas ser n^2+n+1.

□

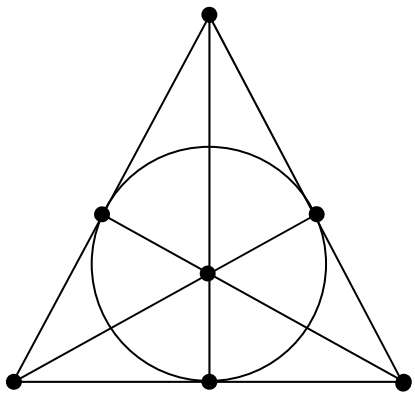


Figura 3 – Plano projectivo de ordem 2

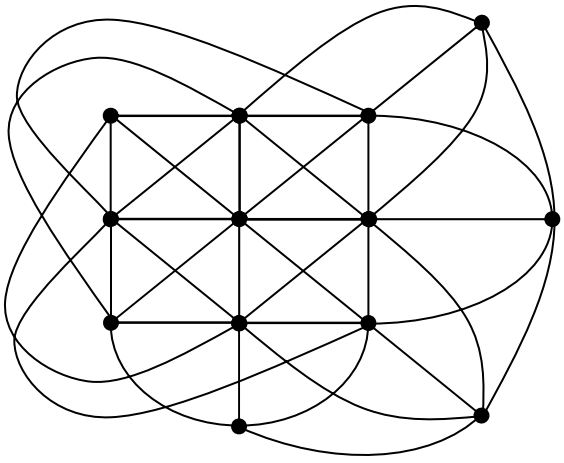


Figura 4 – Plano projectivo de ordem 3

De seguida demonstrar-se-á o processo que permite converter qualquer plano afim finito num plano projectivo, ou invertendo este processo, qualquer plano projectivo finito num plano afim.

Iniciando com um plano afim, por cada classe de rectas paralelas adicione-se um ponto, e estenda-se cada recta da classe para conter esse novo ponto. Estes novos pontos, que representam a intersecção das rectas paralelas anteriores são chamados de **pontos do infinito**. Agora adiciona-se uma recta que passa pelos $n+1$ pontos do infinito a que se chama **recta do infinito**. A estrutura anterior terá agora exactamente n^2+n+1 pontos e rectas. Além disso, facilmente se verifica que $\mathbf{P_1}$, $\mathbf{P_2}$ e $\mathbf{P_3}$ são satisfeitos.

Reciprocamente, se removermos uma recta e os respectivos pontos de um plano projectivo finito de ordem n, a estrutura resultante terá n^2+n rectas e n^2 pontos. O axioma $\mathbf{P_2}$ será violado pela redução na estrutura mas no seu lugar ter-se-á $\mathbf{A_2}$. Os axiomas $\mathbf{A_1}$ e $\mathbf{A_3}$ serão claramente satisfeitos.

Este processo torna-se evidente na relação entre a Figura 1 e Figura 3, e entre a Figura 2 e a Figura 4, tal como se pode verificar de seguida:

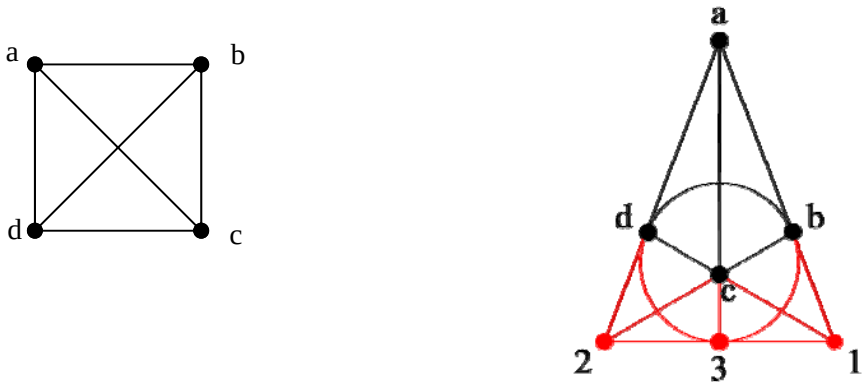


Figura 5 – Análise comparativa entre um Plano afim e um Plano projectivo de ordem 2.

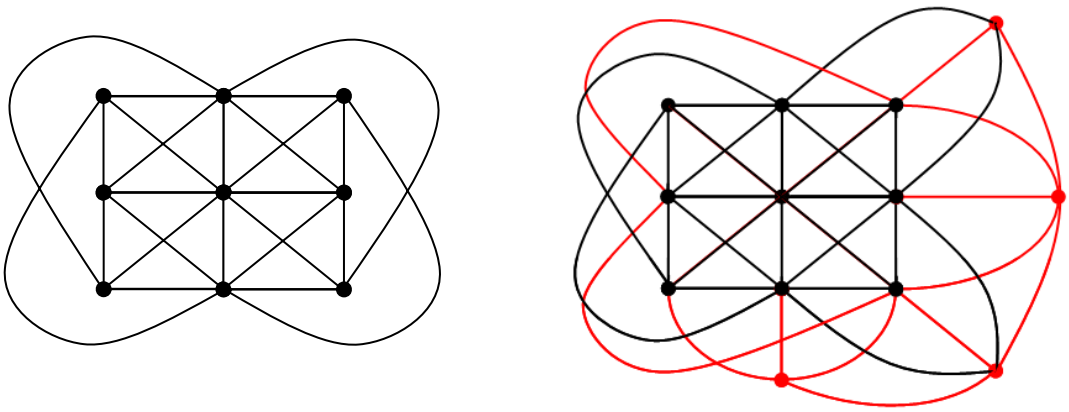


Figura 6 – Análise comparativa entre um Plano afim e um Plano projectivo de ordem 3.

O que se segue é então implícito a partir das construções:

Teorema 3.9.: Existe um plano afim finito de ordem n se e só se existe um plano projectivo finito de ordem n.

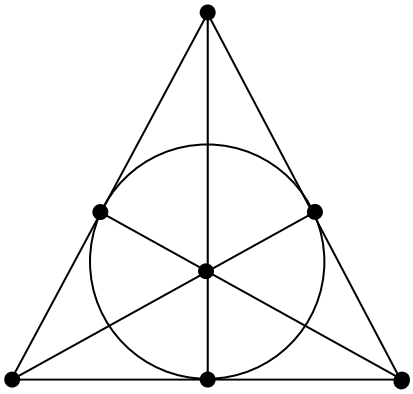


Figura 7 – Plano projectivo de ordem 2

Do Teorema 3.4. e do Teorema 3.9. obtém-se o seguinte corolário:

Corolário 3.10.: Existe um conjunto completo de MOLS de ordem n se e só se existe um plano projectivo finito de ordem n.

Exemplo 3.11.: Suponha que 16 jogadores de golfe combinam fazer um torneio de 5 dias em que cada participante joga uma partida de golfe por dia. O plano é feito de modo que os 16 participantes são divididos cada dia em 4 "foursomes" (partida de golfe entre dois pares), de tal forma que cada par pertence ao mesmo "foursome" uma só vez e quaisquer 2 "foursomes" que não são no mesmo dia têm exactamente um participante comum. Mostre que existe solução e represente-a como um conjunto de quadrados ortogonais.

Solução: As condições requeridas satisfazem exactamente as propriedades do plano afim de ordem 4, $AG(2,4)$, em que os jogadores de golfe representam os pontos, os "foursomes" as rectas e os "foursomes" de cada dia a classe de 4 rectas paralelas.

Considerem-se os jogadores numerados de 1 a 16 e identificados com os correspondentes 16 pontos de $AG(2,4)$ organizados da seguinte forma:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Então, cada um dos 5 quadrados ortogonais representados abaixo fornece a tabela de jogos para cada um dos 5 dias.

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

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

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

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

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

Em cada quadrado, se o símbolo $\alpha = 1,2,3,4$ aparecer na posição $\beta = 1,2,...,16$, então o jogador β joga nesse dia no "foursome" α. O axioma $\mathbf{A_1}$ garante que quaisquer 2 jogadores de golfe jogam juntos exactamente numa única partida, e a ortogonalidade dos quadrados garante que um jogador comum a duas partidas não as joga no mesmo dia.

Por exemplo, o primeiro quadrado indica que os jogadores do "foursome" dois são o 5, 6, 7 e 8, enquanto que, por exemplo, o segundo quadrado indica que os jogadores do "foursome" dois são o 2, 6, 10 e 14.

Exemplo 3.12.: No exemplo anterior dos 16 jogadores de golfe, disponha-se os 5 dias de jogos como sendo as rectas no plano projectivo de ordem 4, $PG(2,4)$ e adicione-se a cada recta um quinto ponto correspondente ao dia do "foursome".

<u>*Solução*</u>*:* Considerem-se as rectas dos quadrados do exemplo anterior e adicione-se o conjunto $\{Seg, Ter, Quar, Quin, Sex\}$ de forma a obter-se a seguinte disposição de jogos:

Seg	1	1	1	1
Seg	2	2	2	2
Seg	3	3	3	3
Seg	4	4	4	4

Ter	1	2	3	4
Ter	1	2	3	4
Ter	1	2	3	4
Ter	1	2	3	4

Quar	1	2	3	4
Quar	2	1	4	3
Quar	3	4	1	2
Quar	4	3	2	1

Quin	1	2	3	4		*Sex*	1	2	3	4
Quin	3	4	1	2		*Sex*	4	3	2	1
Quin	4	3	2	1		*Sex*	2	1	4	3
Quin	2	1	4	3		*Sex*	3	4	1	2

Por exemplo na quarta-feira os jogadores do "foursome" 1 são os que têm os números 1, 6, 11 e 16.

Se a linha *Seg Ter Quar Quin Sex* é adicionada para se obter a vigésima primeira linha do plano de jogos, então as 20 partidas em conjunto com esta linha adicional formam as 21 rectas do plano $PG(2,4)$, em que a última recta representa a recta do infinito.

Cada dia da semana é adicionado a uma classe de rectas paralelas de $AG(2,4)$, sendo assim, considerado o ponto do infinito da respectiva classe. Então, os jogadores em conjunto com os dias da semana fornecem os 21 pontos requeridos.

Além disso, o plano de jogos satisfaz todas as especificações. Qualquer par de "foursomes" tem exactamente um jogador em comum, ou as partidas são jogadas no mesmo dia. Similarmente, quaisquer 2 jogadores encontram-se no mesmo "foursome" uma única vez, e todos os jogadores jogam todos os dias, o que significa que existe uma recta que une cada ponto representado por um jogador a cada ponto representado por um dia da semana.

Por um lado, o plano afim parece mais fundamental que o plano projectivo. Iniciando com um conjunto completo de MOLS, viu-se no Teorema 3.4. como obter um plano afim, e então pelo Corolário 3.10. viu-se como é possível estender o plano afim a um plano projectivo pela adição de pontos do infinito e a recta do infinito.

Por outro lado, existem razões para considerar o plano projectivo mais fundamental. No caso projectivo existe simetria entre as propriedades dos pontos e das rectas.

Especificamente,

1. existem n^2+n+1 pontos e n^2+n+1 rectas;
2. todo o ponto pertence a $n+1$ rectas e toda a recta contém $n+1$ pontos;
3. todo o par de pontos define uma recta e todo par de rectas define um ponto.

De facto, existe uma dualidade entre pontos e rectas.

Consequentemente, qualquer teorema sobre pontos e rectas possui um dual obtido por uma simples substituição de ponto por recta e vice-versa.

4. SUDOKU

4.1. HISTÓRIA DO SUDOKU

O Sudoku é um puzzle baseado na colocação lógica de números e o seu nome provém de uma palavra japonesa que significa “colocando os números” (Figura 8). O Sudoku tem uma história fascinante, "Su" significa número em japonês e "Doku" significa o único lugar onde é possível colocar cada número.

Figura 8 – Palavra Sudoku em Japonês.

O Sudoku é uma espécie de acrónimo da expressão japonesa *Suuji wa dokushin ni kagiru* (栖巾ホ癨銷レ鬍㐂), a qual pode ser traduzida por "Os números devem ser únicos " ou " Os números devem ocorrer apenas uma vez".

Embora seja japonês, as origens do jogo estão na Europa e nos Estados Unidos. Ao contrário de muitos outros jogos, que foram desenvolvidos numa cultura e depois adaptados por outras, o Sudoku tem uma raiz multicultural.

O nome deste puzzle foi proposto por Kaji Maki, o presidente da empresa editora Nikoli, responsável pela introdução deste passatempo no Japão, a qual publicou um Sudoku pela primeira vez no seu jornal Monthly Nikolist em Abril 1984. O termo Sudoku continua a ser uma marca registada da Nikoli.

Contudo, a invenção deste passatempo data de 1979 e deve-se a Howard Garns, um construtor de passatempos independente, baseando-se, provavelmente, no quadrado latino, construção matemática criada pelo suíço Leonhard Euler no século XVIII, tal como já foi referido no início deste trabalho. Garns apresentou a sua nova criação como uma grelha parcialmente preenchida onde o solucionador deveria preencher os restantes quadros vazios.

O primeiro passatempo deste tipo foi publicado em New York nos finais dos anos 70 pela editora Dell Magazines na sua revista Dell Pencil Puzzles and Word Games, sob o título Number Place.

Em Inglaterra, o Times publicou o seu primeiro Sudoku em 12 de Novembro de 2004 sob o título Su Doku. Três dias mais tarde, o Daily Mail iniciou a publicação do passatempo, a que chamou Codenumber. O Daily Telegraph publicou o seu primeiro Sudoku em 19 de Janeiro de 2005. A partir daqui muitos outros jornais e revistas passaram a publicar também este tipo de passatempo.

As primeiras publicações do Sudoku ocorreram nos Estados Unidos no final da década de 70 do século XX na revista americana Math Puzzles and Logic Problems, da editora Dell Magazines, especializada em desafios e quebra-cabeças. A editora deu ao jogo o nome de Number Place, que é usado até hoje nos Estados Unidos. Em 1984, a Nikoli, maior empresa japonesa de quebra-cabeças, descobriu o Number Place e decidiu levá-lo até ao Japão.

A partir de Julho de 2005 o canal de TV Channel 4 publica diariamente um Sudoku no seu serviço de teletexto. O primeiro programa de TV ao vivo dedicado ao Sudoku, chamado Sudoku Live foi transmitido em 1 de Julho de 2005 no canal Sky One.

O Sudoku é publicado pela primeira vez em Portugal, em Maio de 2005 pelo jornal Público. No entanto, actualmente diversas editoras publicam o Sudoku.

O Sudoku tem vindo a ganhar uma enorme popularidade nos últimos tempos. É vulgar nos dias que correm aparecer na secção de passatempos de um jornal ou revista, um ou mais problemas de Sudoku, lado a lado com problemas de Palavras Cruzadas.

Uma grande vantagem do Sudoku é que se trata de um puzzle que não tem de ultrapassar barreiras linguísticas: um problema publicado nos Estados Unidos ou no Japão é igualmente válido em Portugal.

A versão mais comum do problema tem este aspecto:

				8			7	
	2	7	9		5			
6								
						4		7
4	9		2				5	
3		2	8	5				
						6		
	3			7	9			
8			6	4			9	

Figura 9 – Um problema comum de Sudoku.

O jogo é constituído por uma grelha 9×9, constituída por subgrelhas de 3×3, chamadas regiões, que também podem ser designadas caixas, blocos ou quadrantes. Algumas células já contêm números, isto é, contém pistas.

O objectivo é preencher os quadrados com os números de 1 a 9, de tal forma que em cada domínio não haja números repetidos. Um domínio é constituído por uma linha, uma coluna ou um bloco de 3x3. À partida o problema é apresentado com um número variável (normalmente à volta de 30) de quadrículas já preenchidas, as quais condicionam o preenchimento das restantes.

A solução para o problema apresentado acima é:

9	5	3	4	**8**	6	2	**7**	1
1	**2**	**7**	**9**	3	**5**	8	4	6
6	8	4	7	1	2	9	3	5
5	6	8	3	9	1	**4**	2	**7**
4	**9**	1	**2**	6	7	3	**5**	8
3	7	**2**	**8**	**5**	4	1	6	9
7	4	9	5	2	8	**6**	1	3
2	**3**	6	1	**7**	**9**	5	8	4
8	1	5	**6**	**4**	3	7	**9**	2

Figura 10 – Solução do problema de Sudoku apresentado anteriormente.

A atracção do jogo é que as regras são simples, contudo, a linha de raciocínio requerida para alcançar a solução pode ser complexa. O Sudoku é recomendado por alguns educadores como um exercício para o pensamento lógico. O nível de dificuldade pode ser seleccionado de acordo com o público a quem se destina.

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Figura 11 – Um problema de Sudoku difícil.

Não demorou muito para alguns matemáticos começarem a calcular quantos jogos de Sudoku seria possível criar. Existem apenas 12 quadrados latinos de ordem 3 e 576 de ordem 4, mas 5.524.751.496.156.892.842.531.225.600 de ordem 9 (ver tabela da página 3 e Teorema 1.4.). No entanto, a Teoria de Grupos defende que um quadrado que deriva de outro é equivalente ao original, isto é, se se trocarem os números de forma sistemática (por exemplo, o 1 pelo 2, o 2 pelo 7 e assim sucessivamente), ou se se inverter duas linhas ou duas colunas, os resultados finais, serão em essência, os mesmos.
Neste sentido, considerando apenas as formas reduzidas, o número de quadrados latinos de ordem 9 é 337.597.590.964.258.819.

Se pensarmos em quadrados latinos que sejam Sudoku, é possível obter um Sudoku a partir de outro, recorrendo a operações elementares, tais como:

- *Permutações dos 9 algarismos da grelha;*
- *Permutações dos 3 blocos verticais 9x3;*
- *Permutações dos 3 blocos horizontais 3x9;*
- *Permutações das 3 colunas de cada bloco vertical 9x3;*
- *Permutações das 3 linhas de cada bloco horizontal 3x9;*
- *Reflexões e rotações do quadrado.*

Um puzzle Sudoku, tal como um quadrado, tem simetrias. Por exemplo, podemos rodar um quadrado de diferentes maneiras, obtendo sempre o mesmo resultado, isto é, pode-

se fazer uma rotação de centro no centro do quadrado e ângulo de 90º ou 180º, no sentido positivo ou negativo, ou seja, uma rotação cujo ângulo é múltiplo de 90º; uma reflexão em relação a cada uma das mediatrizes dos lados, em relação à diagonal principal e à diagonal não principal. O mesmo se passa num puzzle Sudoku, onde ao aplicar este tipo de operações elementares, resulta sempre numa grelha equivalente à inicial.

Determinar o número exacto de grelhas Sudoku possíveis revelou-se uma tarefa difícil. Em 2005, Bertram Felgenhauer da Universidade Técnica de Dresden na Alemanha estimou que o número de Sudoku válidos para uma grelha padrão de 9×9 era 6.670.903.752.021.072.936.960 = 9! × 72² × 27 × 27.704.267.971. Esse montante inclui as soluções derivadas de qualquer quadrado, por meio de operações elementares. Este resultado foi simplificado consideravelmente por análises fornecidas por Frazer Jarvis, da Universidade de Sheffield de Inglaterra, e confirmado independentemente por Ed Russell. Russel e Jarvis também demonstraram que quando as simetrias são levadas em conta, isto é, quando são contabilizadas apenas as formas reduzidas, o número final será 5.472.730.538 – pouco menor que a população da Terra.

Note-se ainda que uma grelha completa de Sudoku pode dar origem a várias grelhas de enunciados a partir de um dado quadrado inicial (ou seja, um quadrado parcialmente preenchido cuja solução é única). Ninguém ainda conseguiu determinar quantos quadrados iniciais existem. Além disso, um quadrado inicial só tem interesse para matemáticos se for mínimo – ou seja, se a remoção de um elemento implicar que a solução não seja única. O desafio para o futuro é calcular o número de quadrados iniciais mínimos, o que representaria em última instância o número de configurações de Sudoku possíveis.

Outro problema relativo à minimalidade continua sem resolução: **qual deve ser o menor número de elementos do quadrado inicial para que a sua solução seja única?** A resposta parece ser 17. Actualmente conhecem-se dezenas de milhar de quadrados Sudoku, S_3, com 17 entradas inicialmente preenchidas que apresentam solução única. Porém, continua em aberto o problema de saber se existe algum quadrado Sudoku, S_3, com 16 entradas inicialmente preenchidas que tenha uma solução única.

Gordon Royle, da Universidade do Oeste da Austrália, testou mais de 38 mil exemplos de quadrados que satisfazem esse critério e não podem ser transformados noutros por meio de operações elementares.

Gary McGuire, da Universidade Nacional da Irlanda, em Maynooth, coordena estudos em busca de um quadrado inicial com 16 elementos, mas até agora não identificou nenhum. Por outro lado, outros pesquisadores que trabalham independentemente nessa área conseguiram encontrar um que

apresenta apenas duas soluções. Isto significa que um Sudoku válido com 16 casas ainda não foi encontrado.
Se fosse possível analisar um quadrado por segundo, o estudo de todos os quadrados possíveis demoraria 173 anos.
O que os matemáticos já conhecem é a resposta para o problema oposto: **qual é o número máximo de elementos do quadrado inicial para o qual não há garantia de solução única?** É 77. É fácil observar que com 80, 79 ou 78 elementos, se houver solução, ela é única. Mas o mesmo não pode ser dito para 77.

4.2. COMO JOGAR

O Sudoku não requer cálculo ou aptidões aritméticas. É essencialmente um jogo de colocação de números em células, usando regras muito simples de lógica e dedução.
O objectivo do jogo é preencher todas as casas vazias com números. Existem três regras simples a seguir num jogo Sudoku 9 por 9, isto é, cada linha de 9 casas, cada coluna de 9 casas e cada bloco 3x3 tem de incluir todos os algarismos de 1 a 9 independentemente da sua ordem.

Em cada jogo já são fornecidos, à partida, alguns números. A dificuldade do jogo depende, quer do número de casas que se encontram preenchidas no início, quer das posições que estas ocupam. Completar as casas correctamente torna a determinação dos restantes números cada vez mais fácil, uma vez que o número de possibilidades vai decrescendo.
Quem gosta de resolver Sudoku manualmente conta com muitas tácticas à disposição. Inicialmente, identificam-se as casas vazias que pertencem a linhas, colunas ou blocos que já estejam bem preenchidos. Eliminar as opções impossíveis (números que já ocupam casas na mesma linha, coluna ou bloco) diminui consideravelmente as alternativas e às vezes resulta na descoberta de que apenas um algarismo cabe naquela casa.
Em segundo lugar, procuram-se buracos em que um dado elemento se possa se encaixar em determinada coluna, linha ou bloco. Às vezes, a busca leva a uma única possibilidade de resposta. Noutros momentos, apenas o facto de saber que, por exemplo, o 3 pode ser colocado em dois ou três quadrados pode ajudar.
Para resolver um Sudoku é necessário, antes de mais, definir um método de identificar quais os números válidos para cada posição. Todas as restantes operações se baseiam neste tipo de informação. Diversos programas disponíveis na internet (como por exemplo, o programa NovCruz) geram vários tipos de Sudoku com o nível de dificuldade desejado. Alguns permitem que o

utilizador coloque marcas ou pontos temporários nas casas, o que torna desnecessário o uso de lápis e borracha e estimulam o uso da subtileza e habilidade.

Uma forma expedita de atingir este objectivo é o sistema de pontos, o qual consiste em colocar um ponto numa dada posição da quadrícula para cada algarismo que não pode ser colocado nessa quadrícula, seguindo o esquema:

1	**2**	**3**
4	**5**	**6**
7	**8**	**9**

Seguindo este método, a janela de um Sudoku em fase de resolução aparece no programa NovCruz com este aspecto:

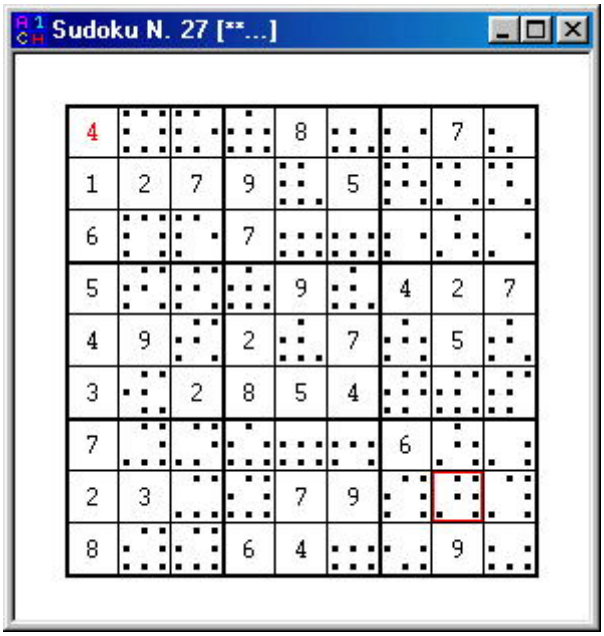


Figura 12 – Sudoku em fase de resolução.

Olhando para a figura anterior e tomando como exemplo a terceira posição da primeira linha, torna-se imediatamente aparente que nesta posição apenas podem aparecer os algarismos 3, 5 e 9. A grande vantagem de usar o programa é que este automaticamente actualiza os pontos referentes a cada quadrícula quando se coloca um número. Na resolução em papel é necessário proceder a essa operação manualmente, o que se torna, por vezes, fastidioso e sujeito a enganos.

Uma vez encontrada uma forma expedita de identificar os números que podem ser colocados numa dada posição podemos avançar para os métodos de solução propriamente ditos, os quais irão determinar qual o número a colocar numa dada posição, respeitando os condicionalismos derivados das regras básicas do problema.

Apresentam-se, de seguida, alguns métodos de dificuldade progressivamente crescente para se solucionar um Sudoku. Os Métodos 1 e 2 são os mais simples e, geralmente, são usados em conjunto.

Infelizmente, essas técnicas não levam o jogador muito longe e, por isso, deve-se acrescentar o Método 3 e, caso também este se revele insuficiente, o Método 4 – que funciona sempre, mas por vezes, implica alguma dificuldade.

4.2.1. MÉTODO 1 – CASA FORÇADA

Esta é a operação mais simples de todas. Consiste em varrer a grelha à procura de quadrículas que apenas possam conter um número.

A varredura das linhas ou colunas serve para identificar que linha de uma região particular pode conter um determinado número por um processo de eliminação. Este processo é repetido então com as colunas ou linhas. É importante executar sistematicamente este processo, verificando todos os dígitos de 1 a 9.

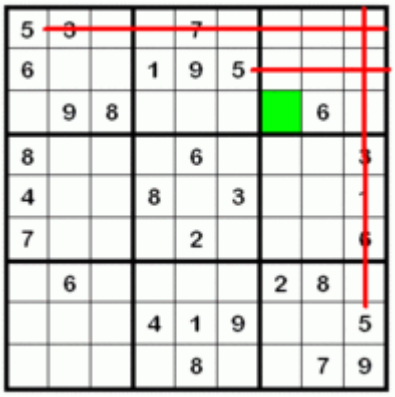


Figura 13 – O jogador pode eliminar todas as células vazias no canto superior direito que contenham um 5 nas mesmas colunas ou linhas, deixando apenas uma célula possível (destacada a verde).

Considere o seguinte Sudoku, ao qual chamamos Grelha A.

5		1					9	6
				9			5	
					5	2		7
4	9		1				7	
					7			
1	3						2	
3		4		5	9			
	2	8		7	1		4	
7	6	5	8	2				

Figura 14 – Grelha A.

Considere agora uma casa fixa. Ao eliminar os outros algarismos que aparecem na mesma coluna, na mesma linha ou na mesma subgrelha, é possível que sobre uma única possibilidade, com a qual a casa deve ser preenchida.

Tal análise da grelha A revela que existem "casas forçadas", as quais estão representadas com algarismos a verde na Grelha B.

5		1					9	6
				9			5	
					5	2		7
4	9		1				7	
					7			
1	3						2	
3	1	4	6	5	9			
9	2	8		7	1		4	
7	6	5	8	2				

Figura 15 – Grelha B: "casas forçadas" representadas a verde.

4.2.2. MÉTODO 2 – CASA ÚNICA

No Método 2, foca-se um determinado algarismo, por exemplo, o 5. Nas colunas 1 e 3 da grelha A já existe um 5, mas na coluna 2 ainda não. Onde deve este algarismo ficar? Nas três primeiras casas da coluna 2 não pode ser, pois a primeira subgrelha já contém um 5. Na sétima casa da coluna 2 também não, pois a subgrelha respectiva também já contém um 5. Assim, o 5 da coluna 2 só poderá entrar na quarta, na quinta ou na sexta casas dessa coluna. Como a quinta é a única disponível, o número vai para lá. As casas marcadas com números em azul são, então, as "casas únicas".

5		1					9	6
				9			5	
				1	5	2		7
4	9		1				7	
	5				7			
1	3	7					2	
3	1	4	6	5	9	7		2
9	2	8		7	1		4	
7	6	5	8	2				

Figura 16 – Grelha C: "casas únicas" representadas a azul.

4.2.3. MÉTODO 3 – SIMPLIFICAÇÃO DAS POSSIBILIDADES

Após a varredura e determinação de que mais nenhum número adicional pode ser descoberto, é necessário fazer algumas análises lógicas. Muitos acham útil guiar esta análise através da marcação dos números possíveis (candidatos) nas células em branco. Há duas formas populares: notação subscrita e pontos.

Na notação subscrita os números possíveis são subscritos (escritos em tamanho pequeno). O inconveniente a este é que os puzzles originais impressos num jornal são geralmente demasiado pequenos para acomodar mais do que alguns dígitos da escrita normal. Quando se utiliza a notação subscrita, o jogador geralmente cria uma cópia maior do puzzle e utiliza um lápis ou lapiseira.

A segunda notação usa um padrão de pontos dentro de cada quadrado, onde a posição do ponto representa um número de 1 a 9. A notação do ponto tem a vantagem que pode ser usada no enigma original. É necessária destreza para colocar os pontos, já que os pontos posicionados em lugares

errados ou inadvertidos conduzem inevitavelmente a confusões e podem não ser fáceis de apagar sem gerar mais confusão.

Uma técnica alternativa, que alguns acham mais fácil, é marcar na célula os números que não podem ser lá colocados. Assim, uma célula começará vazia e quanto mais restrições se tornam conhecidas, lentamente vai sendo preenchida. Quando só faltar uma marca ou número, esse número corresponderá ao valor da célula.

Ao usar a marcação, uma análise adicional pode ser executada. Por exemplo, se um dígito aparecer somente uma vez nas marcações escritas dentro de uma célula, então está claro qual o dígito que deve estar lá, mesmo que a célula tenha outros dígitos marcados. Ao usar a marcação (ver figura 18), algumas regras similares aplicadas numa ordem específica podem resolver todo o Sudoku sem necessidade de retornar os passos anteriormente feitos.

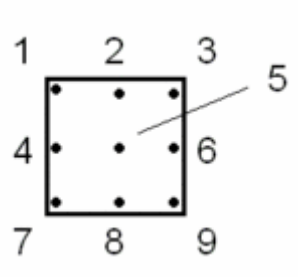


Figura 17 – Um método para marcar números prováveis numa única célula é colocando pontos com lápis.

Para reduzir o número dos pontos usados em cada célula, a marcação deveria ser feita somente depois do número máximo possível ter sido adicionado ao puzzle através da varredura. Os pontos são apagados à medida que os números correspondentes são eliminados como candidatos.

De seguida, apresenta-se um exemplo em que se utiliza a notação subscrita. Tal como já foi referido, esta técnica é extremamente eficiente, mas requer a utilização de um lápis e de uma borracha. Em cada casa, anotam-se os algarismos que ainda são possíveis e aplica-se a lógica para tentar eliminar as alternativas.

A grelha seguinte (Grelha D) mostra como a Grelha C ficaria se fossem assinaladas todas as possibilidades, sem a aplicação prévia do Método 2.

5	4 6 7 8	1	2 3 4 7	3 4 8	2 3 4 8	3 4 8	9	6
2 6 8	4 7 8	2 3 6 7	1 2 3 4 6	9	2 3 4 6 8	1 3 4 8	5	1 3 4 8
6 8 9	4 8	3 6 9	3 4 6	1 3 4 6 8	5	2	1 3 8	7
4	9	2 6	1	3 6 8	2 3 6 8	3 5 6 8	7	3 5 8
2 6 8	5 8	2 6	2 3 5 6 9	3 4 6 8	7	1 3 5 6 8 9	1 3 6 8	1 3 4 5 8 9
1	3	6 7	5 6 9	6 8 9	6 8 9	5 6 8 9	2	4 5 8 9
3	1	4	6	5	9	1 6 7 8	1 6 8	1 2 8
9	2	8	3 6	7	1	3 5 6 9	4	3 5 9
7	6	5	8	2	3 4	1 3 9	1 3	1 3 9

Figura 18 – Grelha D.

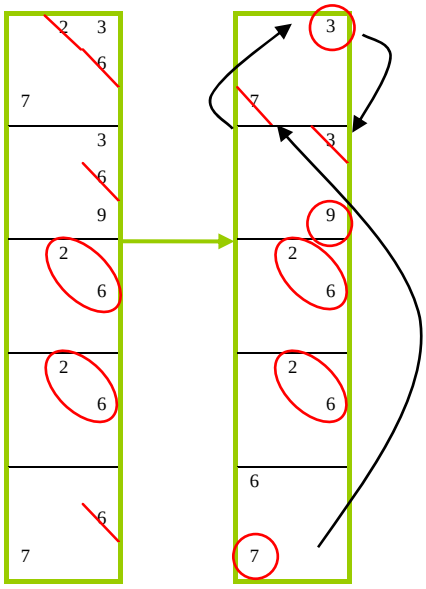


Figura 19 – Zona da Grelha D delineada a verde ampliada.

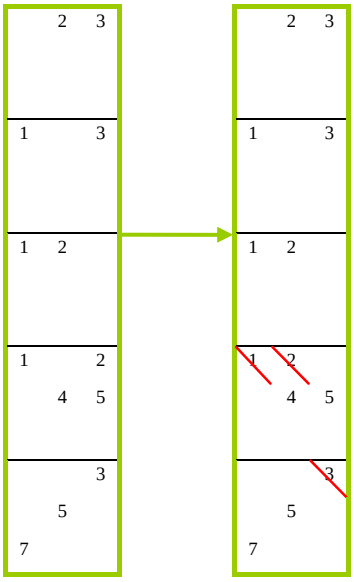


Figura 20 – Resultado final.

Na terceira coluna, a série de possibilidades para as casas 2, 3, 4, 5 e 6 é, respectivamente {2, 3, 6, 7}, {3, 6, 9}, {2, 6}, {2, 6} e {6, 7}. A coluna deve conter um 2 e um 6, portanto esses números devem estar nas duas casas nas quais são as únicas possibilidades (circulados no primeiro destaque). Consequentemente, o 2 e o 6 não podem estar em nenhum outro lugar nesta coluna e podem ser apagados das outras casas (vermelho). A série de possibilidades da coluna simplifica-se, ficando reduzida a: {3, 7}, {3, 9}, {2, 6}. {2, 6}, {7}. Com essa eliminação, descobre-se que o único número possível para a casa 6 é o 7, o que dita as posições do 3 (na casa 2) e do 9 (na casa 3). Assim ficamos com {3}, {9}, {2,6}, {2,6}, {7} (segundo destaque). A única dúvida que persiste é onde colocar o 2 e o 6. A regra geral de simplificação é a seguinte: se, entre uma gama de possibilidades (para uma linha, coluna ou subgrelha) existirem m casas que contêm conjuntos com m algarismos (mas não necessariamente todos em cada casa), os números poderão ser eliminados de acordo com as possibilidades das outras casas. Por exemplo, na Figura 20 {2,3}, {1,3}, {1,2}, {1,2,4,5}, {3,5,7} podem ser simplificados para {2, 3}, {1,3}, {1, 2}, {4, 5}, {5,7}, porque as casas {2, 3}, {1, 3}, {1, 2} vêm do subconjunto {1, 2, 3} e não têm outros números.

4.2.4. MÉTODO 4 – TENTATIVA E ERRO

Com os três métodos anteriores é possível resolver muitos quebra-cabeças. Mas os níveis "diabólicos" frequentemente requerem uma fase de tentativa e erro. Quando a incerteza persiste, é preciso fazer uma escolha e aplicar todas as estratégias para o preenchimento das restantes casas. Se se deparar com uma impossibilidade (como o aparecimento de um número duas vezes numa

coluna), significa que a escolha estava errada. Por exemplo, é possível tentar o 2 na quarta casa da terceira coluna na Grelha C. Se esta tentativa falhar, é preciso recomeçar o jogo daquele ponto, desta vez com o número 6. Infelizmente, algumas vezes é preciso fazer várias rodadas de tentativa e erro e estar preparado para voltar atrás.

A ideia do método, aliás, é a mesma usada pelos algoritmos de retrocesso sistemático (Backtracking), que os programas podem executar facilmente mas para o qual a nossa memória tem dificuldade. É impressionante que o método mais eficiente para as máquinas seja o menos adequado para o ser humano.

4.3. NÍVEIS DE DIFICULDADE

Os autores destes passatempos geralmente classificam-nos por nível de dificuldade. Surpreendentemente o número de pistas dadas pode ter pouca relação com o nível de dificuldade do jogo. Um jogo com um número pequeno de pistas dadas pode ser muito fácil de resolver, enquanto que um jogo com um número maior do que a média de pistas dadas pode ser extremamente difícil de resolver. A dificuldade de um jogo está mais baseada no posicionamento dos números dados do que propriamente na quantidade de números.

A maioria das publicações classifica os seus enigmas do Sudoku em quatro níveis de dificuldade. Tipicamente, alguns jogos são classificados de "fácil", "intermédio", "difícil" e "desafiador".

Nos problemas resolvidos com o programa NovCruz, o grau de dificuldade aparece no título da janela associada, podendo tomar os valores de 1 a 5, correspondendo ao número de asteriscos que aparecem entre parêntesis rectos.

4.4. QUALIDADE

Um problema Sudoku bem construído deve ter apenas uma solução, determinada univocamente a partir do enunciado. Infelizmente, aparecem problemas publicados em jornais e revistas que não respeitam esta regra fundamental, verificando-se, por vezes, que o resultado obtido por um jogador é diferente da solução publicada, podendo este ficar a pensar que a sua solução está errada quando poderá não ser esse o caso.

4.5. CONSTRUÇÃO

É possível criar puzzles com mais do que uma solução possível e criar puzzles que não tenham nenhuma solução, mas tais não são considerados enigmas apropriados para o Sudoku. Assim, como

na maioria dos outros enigmas de lógica pura, deve-se esperar uma única solução para o desafio de Sudoku.

Construir um puzzle Sudoku manualmente pode ser uma tarefa executada eficientemente através da pré-determinação das pistas, as quais constituem os valores necessários para que se consiga resolver o enigma.

Muitos defendem que os jogos Sudoku (Number Place) da Dell Magazines são gerados por computador; eles normalmente possuem mais de 30 pistas espalhadas aparentemente de maneira aleatória, muitas das quais podem possivelmente ser deduzidas a partir de outras pistas.

Os Sudokus da Nikoli são construídos manualmente, com o crédito para o autor e as pistas são geralmente encontradas num padrão simétrico. Os jogos Number Place Challenger da Dell também listam seus autores. Os jogos Sudoku impressos na maioria dos jornais da Grã-Bretanha são aparentemente gerados por computador, mas empregam pistas simétricas.

O desafio para os programadores de Sudoku é criar um programa para construir jogos "inteligentes", de tal maneira que eles se tornem indistinguíveis dos construídos por humanos. Wayne Gould passou seis anos a ajustar o seu popular programa até que acreditou que tinha conseguido atingir este nível.

4.6. VARIANTES

Apesar da grelha 9×9 com subregiões 3×3 ser de longe a mais conhecida, existem diversas variações do Sudoku comum que embora assumam configurações diferentes, seguem as mesmas regras.

Na Figura 21, as letras das palavras MARTIN GARDNER (tem 9 letras diferentes) substituem os números e as formas geométricas tomam o lugar das subregiões do Sudoku.

O inventor deste formato baptizou-o de Du-Sum-Oh.

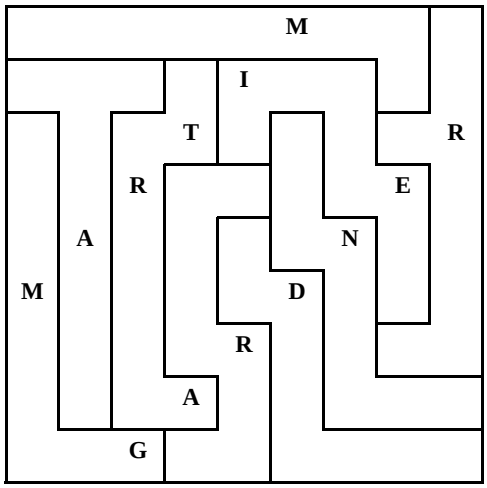


Figura 21 – Du-Sum-Oh.

Existem muitas variantes de Du-Sum-Oh, observe-se por exemplo o seguinte puzzle e a sua respectiva solução:

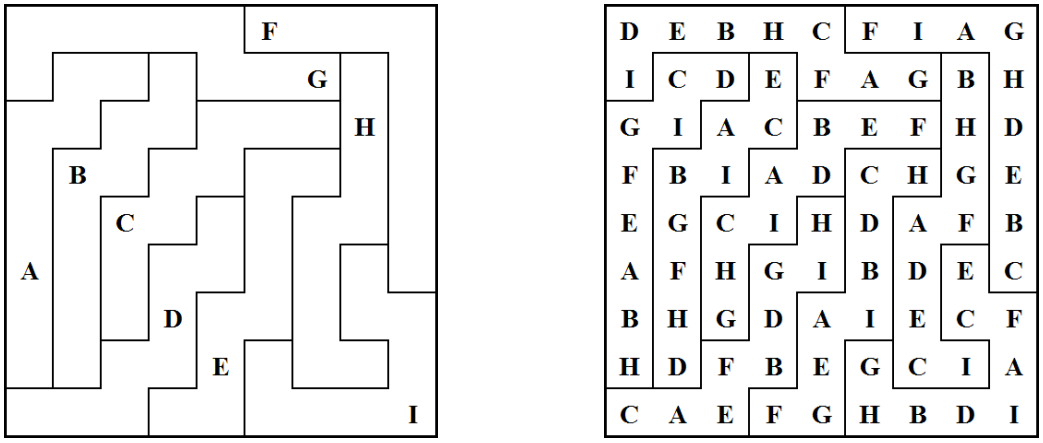


Figura 22 – Outra variante de Du-Sum-Oh e respectiva solução.

Também pode ser encontrado o Sudoku Circular, também conhecido como Target Sudoku, inventado pelo matemático Peter Higgins. Nesta variante, os dez números (de 0 a 9) devem aparecer em cada um dos círculos concêntricos, bem como em todos os pares de fatias "verticalmente opostas" (correspondentes a ângulos verticalmente opostos).

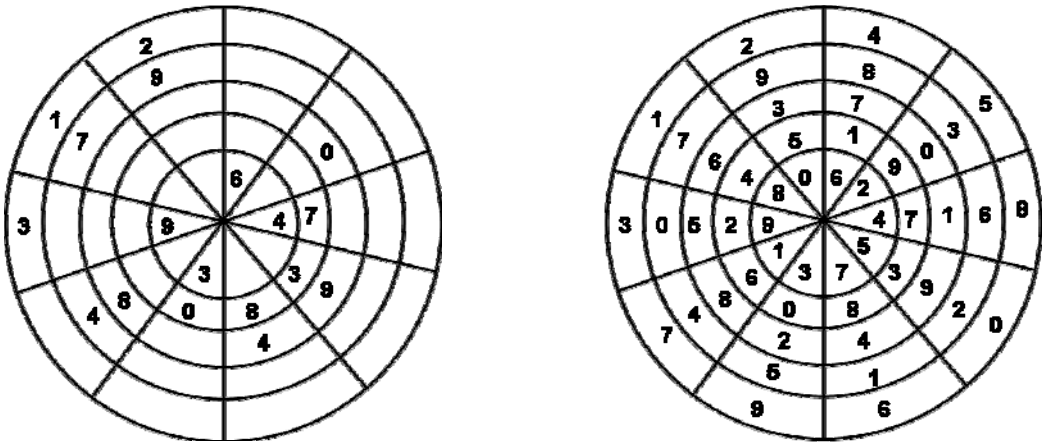


Figura 23 – Target Sudoku e respectiva solução.

Um outro desafio derivado do Sudoku é constituído por uma estrela com apenas seis subregiões triangulares, em que as linhas e colunas inclinadas podem ser interrompidas no centro, e quando uma linha ou coluna tem apenas oito casas, a célula próxima que forma uma ponta da "estrela" serve como uma nona casa.

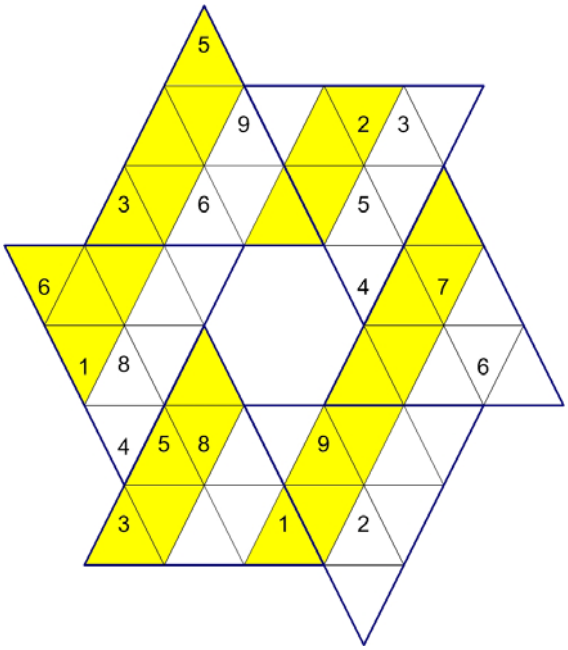


Figura 24 – Estrela com seis subregiões.

Outro tipo de restrições extra podem ser de natureza aritmética, tais como, exigir que os números num delineado segmento da grelha tenham uma soma ou um produto específico.

O quebra-cabeças seguinte consiste em resolver um Sudoku com as regras habituais, com a restrição adicional que nas cinco linhas em que nos aparece o sinal “+” e o símbolo “=”, temos de ter em conta que o número formado pelos três algarismos do primeiro bloco adicionado com o número formado pelos três algarismos do segundo bloco tem de resultar no número formado pelos três algarismos do terceiro bloco.

			+			9	=	6		
6		5			8					2
			+		4		=			9
	6	1		8	5				7	
	5		+				=		8	
	8				1	4		5	6	
5			+		9		=			
8					7			1		6
		7	+	3			=			

Figura 25 – Soma de algarismos.

4	1	8	+	2	3	9	=	6	5	7
6	9	5		7	8	1		3	4	2
2	7	3	+	5	4	6	=	8	1	9
9	6	1		8	5	3		2	7	4
3	5	4	+	6	2	7	=	9	8	1
7	8	2		9	1	4		5	6	3
5	4	6	+	1	9	2	=	7	3	8
8	3	9		4	7	5		1	2	6
1	2	7	+	3	6	8	=	4	9	5

Figura 26 – Solução do puzzle anterior.

O desafio seguinte é constituído por sinais de maior e menor, os quais indicam as casas em que os números devem ser colocados.

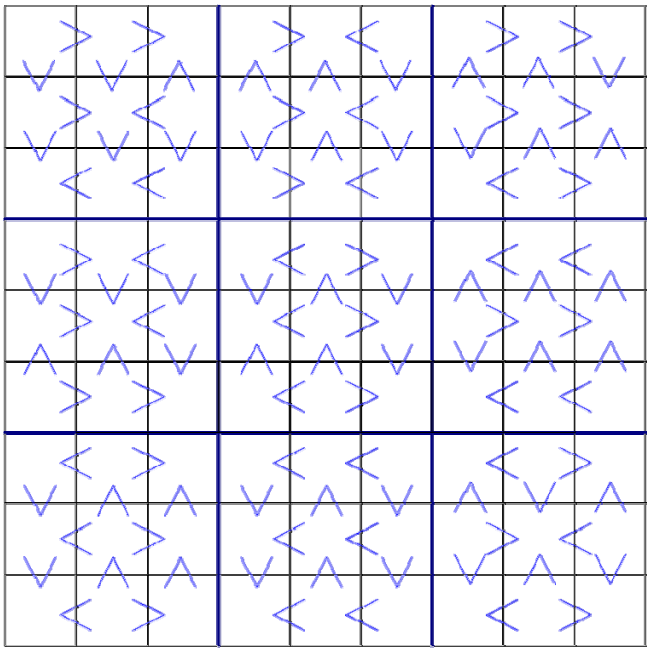


Figura 27 – Utilização dos sinais de maior e menor.

O desafio seguinte é constituído por dominós especiais, em que o número máximo de pintas não é 6, mas sim 9. As peças de dominó que se encontram na figura seguinte podem ser encaixadas nos espaços vazios. Dado que a grelha é constituída por 81 casas, inclui-se à partida, nas casas já fornecidas "meia peça" para que o desafio possa ser completado correctamente sem que fiquem casas em branco. No exemplo da figura seguinte pode verificar-se isso mesmo.

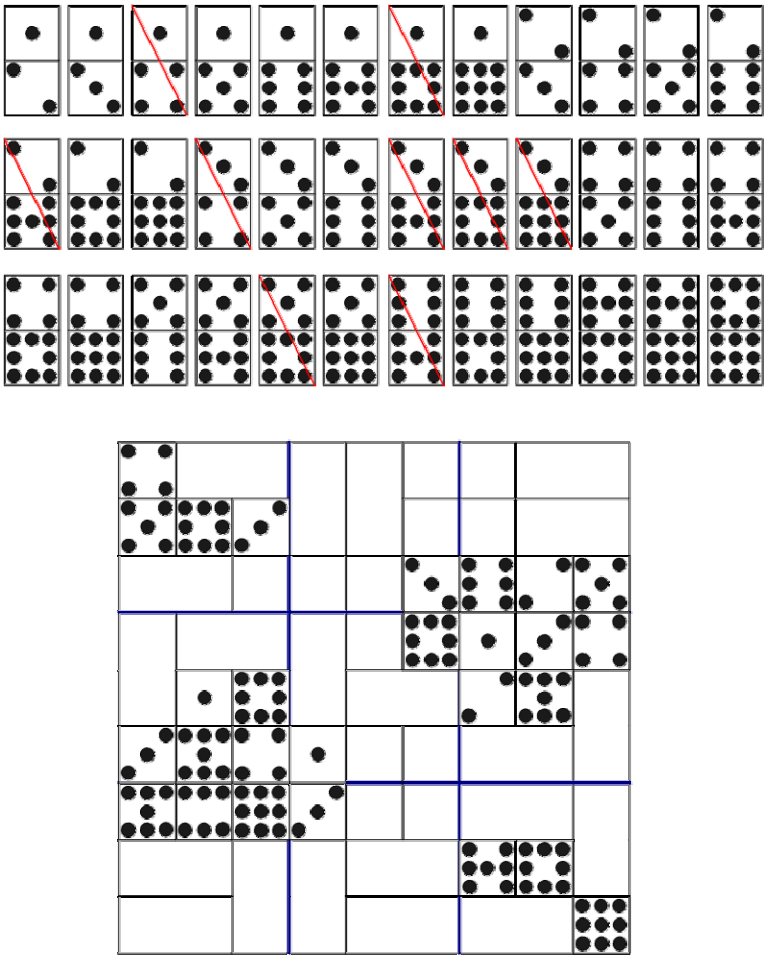


Figura 28 – Dominós.

São ainda comuns passatempos construídos a partir de múltiplas grelhas Sudoku. Cinco grelhas 9×9 as quais se sobrepõem umas às outras nas regiões dos cantos são conhecidas no Japão como Gattai 5 Sudoku. No The Times e no The Sydney Morning Herald esta forma de passatempo é conhecida como Samurai SuDoku.

Os passatempos com vinte ou mais grelhas sobrepostas não são invulgares em algumas publicações japonesas e, geralmente, não é fornecida nenhuma pista nas regiões sobrepostas.

De seguida, apresenta-se um desafio constituído por três grelhas que se sobrepõem.

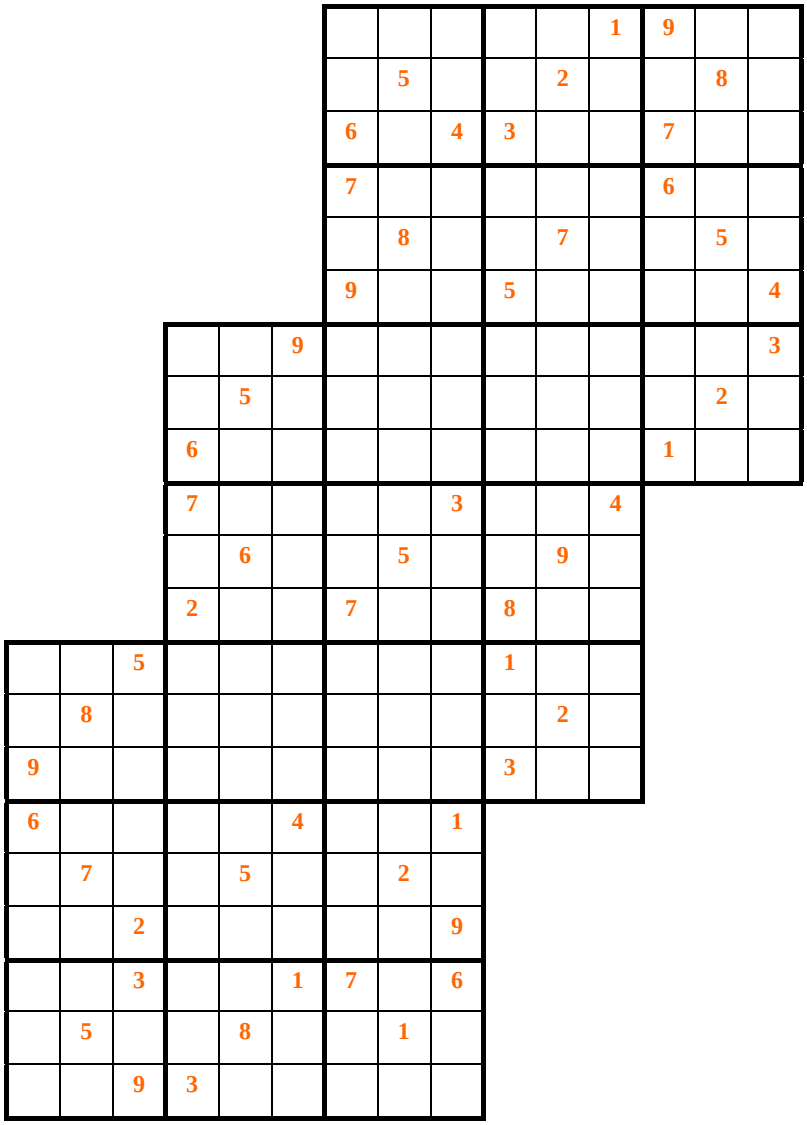


Figura 29 – Quadrados sobrepostos.

Surgiram também variações alfabéticas. Recentes variantes têm esta característica, geralmente em forma de palavra lida ao longo da diagonal principal depois de encontrada a solução. Determinar a palavra antecipadamente pode ser visto como um auxílio para a solução. O Code Doku inventado por Steve Schaefer tem uma palavra completa embutida no passatempo e o Super Wordoku da Top Notch contém duas palavras de nove letras, uma em cada diagonal. É discutível se estas formas são verdadeiros Sudoku, contudo contêm uma solução "linguisticamente" válida e não podem ser resolvidas apenas através da lógica, sendo necessário que o jogador determine a palavra embutida. Seguem alguns exemplares únicos:

- Um passatempo Sudoku tridimensional, inventado por Dion Church e publicado no Daily Telegraph em Maio de 2005.
- Um Sudoku de 100×100, criado por Michael Metcaff, publicado para o grupo do Yahoo! Sudokuworld – de 10x10 blocos de 10x10.

4.7. COLORAÇÕES PARCIAIS E SUDOKU

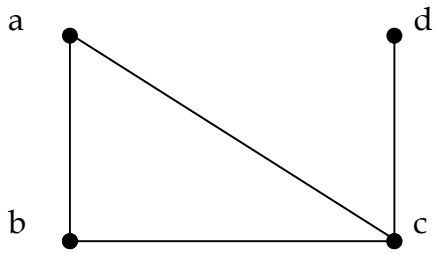
Definição 4.1. (*Grafo*)**:** Um grafo G consiste num conjunto finito de elementos, V, chamados vértices e num conjunto E de pares de vértices relacionados, chamados arestas.

Assim, um grafo G é um par (V,E), tal que $V=V(G)=\{v_1,v_2,\ldots,v_n\}$ é o conjunto dos vértices e $E=E(G)$ é o conjunto das arestas, a cada uma das quais corresponde um subconjunto de $V(G)$ de cardinalidade 2, isto é, $E(G)=\{e_1,e_2,\ldots,e_m\}$, com $e_k=\{v_{k_i},v_{k_j}\}$, para $k\in\{1,\ldots,m\}$.

Dois vértices unidos por uma aresta dizem-se **vértices adjacentes**.

Exemplo 4.2:

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:



Definição 4.3. (*Subgrafo*)**:** Dados dois grafos G e H, diz-se que H é um subgrafo de G, se $V(H)\subseteq V(G)$ e $E(H)$ é constituído por arestas de $E(G)$ que unem vértices de H.

Definição 4.4. (S*ubgrafo induzido*)**:** Dado um grafo G e $\phi\neq\hat{V}\subseteq V(G)$, designa-se por subgrafo de G induzido por $\hat{V}$, o subgrafo cujo conjunto de vértices é $\hat{V}$ e o conjunto de arestas coincide com as arestas de G com extremos em $\hat{V}$. Denota-se por $G[\hat{V}]$.

Definição 4.5. (*$k-$coloração própria*)**:** Uma $k-$coloração própria é uma função $c:V(G)\to\{1,2,3,...,k\}$, tal que $c(i)\neq c(j)$, se ij é aresta do grafo G.

Definição 4.6. (*Número Cromático de G*)**:** O número cromático de G é o menor k para o qual o grafo G admite uma $k-$coloração própria. Representa-se por $\chi(G)$.

Definição 4.7. (*Coloração parcial*)**:** Dado um grafo G, designa-se por coloração parcial de G toda a coloração própria de um subconjunto de vértices $W\subseteq V(G)$, ou seja, toda a função $c:W\mapsto\{1,\ldots,k\}$, tal que $ij\in E(G[W])\Rightarrow c(i)\neq c(j)$.

Dado um grafo G, com uma coloração parcial c, uma questão que se coloca é a de saber se esta coloração pode ser estendida a uma coloração própria de todos os vértices do grafo. Designa-se uma extensão deste tipo por extensão cromática de c.

Existem diversos problemas práticos que podem ser modelados como problemas de determinação de uma extensão cromática de uma coloração parcial, como por exemplo, o problema de afectação de frequências de transmissão a novas estações emissoras de rádio, supondo que já existem outras estações com frequências de transmissão atribuídas. Com efeito, a atribuição de frequências de transmissão a estações emissoras deve ser feita de modo que não haja sobreposição, o que, em geral, acontece quando existem postos transmissores que não estando eficientemente afastados, têm a mesma frequência atribuída. Assim, considerando um grafo G cujos vértices são as estações de rádio e onde dois vértices são adjacentes se a distância que separa os correspondentes transmissores é não superior a d (distância mínima exigida para não haver sobreposição), podemos considerar as frequências de transmissão como cores a atribuir aos vértices e as frequências já atribuídas como uma coloração parcial $c:W\subseteq V(G)\mapsto\{1,\ldots,k\}$. Assim, a distribuição de frequências pelas novas estações corresponde à determinação de uma extensão cromática de c.

Teorema 4.8.: Seja G um grafo e $c:W\subseteq V(G)\mapsto\{1,\ldots,k\}$, onde $|W|$[(iv)]$=\chi(G)-2$, é uma coloração parcial. Se existe uma extensão cromática de c, então o número destas extensões é não inferior a 2.

[(iv)] $|W|$ representa o cardinal do conjunto W.

Demonstração: Uma vez que de entre as cores determinadas por uma extensão cromática da coloração parcial c, existem duas que não são utilizadas por c, pode-se trocá-las entre si sem que a coloração dos vértices de G deixe de ser própria e de ser uma extensão cromática de c.

□

Como consequência imediata deste Teorema, pode-se concluir que dado um grafo G, se uma sua coloração parcial, $c:W\subseteq V(G)\mapsto\{1,\ldots,k\}$, admite uma única extensão cromática, então $k\geq\chi(G)-1$.

Uma aplicação muito popular da determinação de extensões cromáticas de colorações parciais está relacionada com a completação de quadrados latinos parcialmente conhecidos, mais particularmente, está relacionada com o Sudoku.

Como já foi referido, inicialmente algumas das entradas deste jogo já estão preenchidas sendo que o objectivo é preencher as restantes, de tal forma que em cada linha, cada coluna e cada bloco, não existam números repetidos. Assim, o objectivo do jogo é a determinação de um quadrado latino com a particularidade de em cada um dos blocos 3×3 também não existirem entradas repetidas. Mais geralmente, estas grelhas com $n^2\times n^2$ entradas (e $n\times n$ blocos, com $n\times n$ entradas cada) designam-se por quadrados Sudoku de característica n e denotam-se por S_n. Com eles, dado um conjunto de entradas inicialmente preenchidas, pretende-se preencher as restantes com inteiros entre 1 e n^2 de modo a obter um quadrado latino com a propriedade adicional de não conter entradas repetidas em cada um dos seus $n\times n$ blocos. Na tabela seguinte apresenta-se um Sudoku de característica 3, S_3, com 17 entradas inicialmente preenchidas.

							1	2
4				9				
							5	
	7		2					
6						4		
			1		8			
	1	8						
				3		7		
5		2						

Figura 30 – Sudoku com 17 entradas inicialmente preenchidas.

Dado um quadrado Sudoku com característica n, S_n, designa-se por grafo Sudoku de S_n e denota-se por $G(S_n)$ o grafo cujos vértices são as entradas (i, j) de S_n, com $1 \le i, j \le n^2$, e onde dois vértices são adjacentes se correspondem a entradas na mesma linha, coluna ou bloco, ou seja, (i_1, j_1) e (i_2, j_2) são adjacentes se $i_1 = i_2$ ou $j_1 = j_2$, ou ainda $\lceil i_1 / n \rceil$ [(v)] $= \lceil i_2 / n \rceil$ e $\lceil j_1 / n \rceil = \lceil j_2 / n \rceil$.

Definição 4.9. (*Clique*)**:** Seja um grafo $G = (V, E)$. Uma clique é um conjunto de vértices adjacentes dois a dois. Por outras palavras, um conjunto C de vértices é uma clique se tiver a seguinte propriedade: para todo par (v, w) de vértices distintos em C, existe uma aresta que une v e w.

Definição 4.10. (*Clique máxima*)**:** Uma clique C diz-se maximal se qualquer que seja $v \in V(G) \setminus C$ o conjunto de vértices $C \cup \{v\}$ não é uma clique. Uma clique de G de cardinalidade máxima designa-se por clique máxima.

Definição 4.11. (*Número de clique*)**:** A cardinalidade de uma clique máxima designa-se por número de clique de G e denota-se por $\omega(G)$.

Teorema 4.12.: Dado um grafo arbitrário G, $\omega(G) \le \chi(G)$.

Demonstração: No grafo G existe um subgrafo induzido por uma clique máxima cuja coloração própria dos vértices exige $\omega(G)$ cores e como os vértices têm de ter todos cores distintas, vem que $\omega(G) \le \chi(G)$.

□

Uma coloração parcial de $G(S_n)$ corresponde a uma grelha de Sudoku S_n parcialmente preenchida.
Completar o Sudoku corresponde a construir uma extensão cromática da coloração parcial dada.

(v) $\lceil i_1 / n \rceil$ representa o menor inteiro não inferior a i_1 / n.

O Teorema seguinte garante que o menor número possível de símbolos para construir um Sudoku S_n é n^2 e fornece ainda uma forma de o fazer, ou seja, uma coloração própria de $G(S_n)$.

Teorema 4.13.: Qualquer que seja $n \in \mathbb{N}$, sendo S_n um quadrado Sudoku de característica n, $\chi(G(S_n)) = n^2$.

Demonstração: Uma vez que cada bloco $n \times n$ de S_n dá origem a uma clique em $G(S_n)$ e quaisquer k vértices, com $k > n^2$, não pertencem a uma mesma linha, coluna ou bloco, podemos concluir que $\omega(G(S_n)) = n^2$, e consequentemente, $\chi(G(S_n)) \geq n^2$. Logo, resta provar que é possível colorir propriamente os vértices de $G(S_n)$, com n^2 cores. Por facilidade de notação, indexa-se os vértices (i, j) do grafo Sudoku $G(S_n)$, com $0 \leq i, j \leq n^2 - 1$. Assim, fazendo $i = nt_i + d_i$, com $0 \leq t_i, d_i \leq n-1$ e $j = nt_j + d_j$, com $0 \leq t_j, d_j \leq n-1$, vamos provar que $\boxed{c(i,j) = nd_i + t_i + nt_j + d_j \pmod{n^2}}$, é uma coloração própria dos vértices de $G(S_n)$, para o que basta provar que vértices adjacentes têm cores distintas.

Sejam (i_1, j_1) e (i_2, j_2) dois vértices tais que $c(i_1, j_1) = c(i_2, j_2)$.

Se $i_1 = i_2 = i$, então,

$$\begin{aligned} c(i, j_1) = c(i, j_2) &\Leftrightarrow nt_{j_1} + d_{j_1} \equiv nt_{j_2} + d_{j_2} \left(mod\ n^2\right) \\ &\Leftrightarrow \left(nt_{j_1} + d_{j_1}\right) - \left(nt_{j_2} + d_{j_2}\right) = kn^2, \textit{ para algum } k \in \mathbb{Z} \\ &\Leftrightarrow n\left(t_{j_1} - t_{j_2}\right) + \left(d_{j_1} - d_{j_2}\right) = kn^2, \textit{ para algum } k \in \mathbb{Z} \\ &\Rightarrow d_{j_1} - d_{j_2} = kn, \textit{ para algum } k \in \mathbb{Z} \end{aligned}.$$

Como $d_{j_1} - d_{j_2}$ está entre $1-n$ e $n-1$, vem $d_{j_1} = d_{j_2}$.

Analogamente se conclui que $t_{j_1} = t_{j_2}$, donde $j_1 = j_2$.

De igual modo se prova que se $j_1 = j_2$, então, $i_1 = i_2$.

Suponhamos agora que (i_1, j_1) e (i_2, j_2) pertencem ao mesmo bloco.

Atendendo a que $0 \leq i, j \leq n^2 - 1$, tem-se que $\lfloor i_1 / n \rfloor = \lfloor i_2 / n \rfloor$ e $\lfloor j_1 / n \rfloor = \lfloor j_2 / n \rfloor$. Como $\lfloor i / n \rfloor = t_i$ e $\lfloor j / n \rfloor = t_j$ vem $t_{i_1} = t_{i_2}$ e $t_{j_1} = t_{j_2}$.

Então $c(i_1, j_1) = c(i_2, j_2)$ é equivalente a

$$nd_{i_1} + \cancel{t_{i_1}} + \cancel{nt_{j_1}} + d_{j_1} = nd_{i_2} + \cancel{t_{i_2}} + \cancel{nt_{j_2}} + d_{j_2} \left(\mathrm{mod}\, n^2\right)$$

que significa que

$$n\left(d_{i_1} - d_{i_2}\right) + \left(d_{j_1} - d_{j_2}\right) = kn^2, \textit{ para algum } k \in \mathbb{Z}$$

que por sua vez implica $d_{j_1} \equiv d_{j_2} \left(mod\, n\right)$ e $d_{j_1} = d_{j_2}$, uma vez que $0 \le d_{j_1}, d_{j_2} \le n-1$.

Então a igualdade $c\left(i_1, j_1\right) = c\left(i_2, j_2\right)$ toma a forma $n\left(d_{i_1} - d_{i_2}\right) = kn^2, \textit{ para a lg um } k \in \mathbb{Z}$, o que implica $d_{i_1} \equiv d_{i_2} \left(\mathrm{mod}\, n\right)$ e $d_{i_1} = d_{i_2}$.

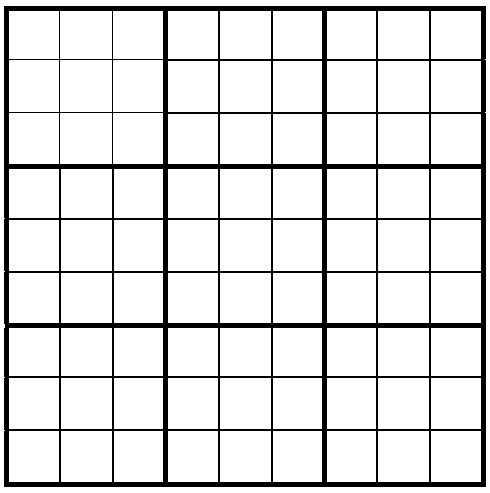
Podemos concluir a igualdade, $\left(i_1, j_1\right) = \left(i_2, j_2\right)$.

□

As entradas de S_n inicialmente preenchidas, correspondem a uma coloração parcial c de $G\left(S_n\right)$, com pelo menos $n^2 - 1$ cores (Teorema 4.8.), e o problema do preenchimento das restantes entradas corresponde ao problema da determinação de uma extensão cromática de c com recurso a n^2 cores.

Exemplo 4.14.: Tendo em conta o que foi abordado anteriormente, pretende-se agora construir um Sudoku utilizando a coloração do Teorema 4.13..

Seja $n = 3$ e $0 \le i, j \le 8$. Como $i = nt_i + d_i$, com $0 \le t_i, d_i \le 2$, $j = nt_j + d_j$, com $0 \le t_j, d_j \le 2$, e $c\left(i, j\right) = 3d_i + t_i + 3t_j + d_j \left(\mathrm{mod}\, 9\right)$ vamos preencher as entradas do seguinte quadrado Sudoku.



Associe-se a cada cor um símbolo (número), tal como se pode ver na seguinte tabela:

Número	**Cor**
0	Azul
1	Vermelho
2	Verde
3	Amarelo
4	Rosa
5	Preto
6	Cinza
7	Laranja
8	Branco

- Para preencher, por exemplo, a entrada $(i,j)=(2,3)$ do Sudoku faz-se, $i \to 2 = 3\times 0+2$ e $j \to 3 = 3\times 1+0$.

Logo,

$$\begin{aligned} c(2,3) &\equiv 3\times 2+0+3\times 1+0 \pmod 9 \\ &\equiv 6+3 \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

Seguindo um raciocínio análogo e tendo em conta a associação estabelecida entre número/cor, poderia preencher-se todas as entradas do Sudoku, obtendo-se o seguinte:

0	1	2	3	4	5	6	7	8
3	4	5	6	7	8	0	1	2
6	7	8	0	1	2	3	4	5
1	2	3	4	5	6	7	8	0
4	5	6	7	8	0	1	2	3
7	8	0	1	2	3	4	5	6
2	3	4	5	6	7	8	0	1
5	6	7	8	0	1	2	3	4
8	0	1	2	3	4	5	6	7

BIBLIOGRAFIA

[1] CARDOSO, Domingos M.; SZYMANSKI, Jerzy; ROSTAMI, Mohammad – **Matemática Discreta. Combinatória, Teoria dos Grafos e Algoritmos**. Aveiro. (2007).

[2] DENÉS, J. – **Latin squares: new developments in the theory and applications**. North-Holland. Amsterdam. (1991).

[3] GILBERT, William J.; NICHOLSON, W. Keith [et al.] – **Modern Algebra with Applications,** Second Edition. Wiley-Interscience. (2000).

[4] LAYWINE, Charles F.; MULLEN, Gary L. – **Discrete Mathematics Using Latin Squares**. Wiley Inter-Science. (1998).

[5] LEE, Wei-Meng – **Programming Sudoku**. Technology in Action. (2006).

[6] ROSEN, Kenneth H., [et al.] – **Handbook of Discrete and Combinatorial Mathematics**. CCR-Press. (2000).

[7] SHUMER, Peter D. – **Mathematical Journeys**. Wiley-Interscience. (2004).

[8] AFJARVIS, Jarvis – **Sudoku** [Em linha]. Disponível na WWW: URL: http://www.afjarvis.staff.shef.ac.uk/sudoku/russell_jarvis_spec2.html, acedido em 17 Out. 2007.

[9] ESDS, Economic and Social Data Service – **Target Sudoku** [Em linha]. Disponível na WWW: URL: http://www.esds.ac.uk/news/newsdetail.asp?ID=1499, acedido em 5 Nov. 2008.

[10] FUTALGO, Novcruz – **Latin Squares** [Em linha]. Disponível na WWW: URL: http://futalgo.planetaclix.pt/novcruz/hlpsdku.htm, acedido em 17 Out. 2007.

[11] IME, Algoritmos – **Grafos** [Em linha]. Disponível na WWW: URL: http://www.ime.usp.br/~pf/algoritmos_em_grafos/aulas/cliques.html, acedido em 22 Out. 2008.

[12] KNOT, Aritmetic – **Latin Squares** [Em linha]. Disponível na WWW: URL: http://www.cut-the-knot.org/arithmetic/latin.shtml, acedido em 7 Jan. 2008.

[13] SCIAM, Reportagens – **A ciência do Sudoku** [Em linha]. Disponível na WWW: URL: http://www2.uol.com.br/sciam/reportagens/a_ciencia_do_sudoku_3.html, acedido em 17 Out. 2007.

[14] SUDOKU, Jorge Buescu – **A Matemática do Sudoku** [Em linha]. Disponível na WWW: URL: https://dspace.ist.utl.pt/bitstream/2295/165442/1/MatSudoku.pdf, acedido em 10 Out. 2007.

[15] WIKIPEDIA, The Free Encyclopedia – **Latin Squares** [Em linha]. Disponível na WWW: URL: http://en.wikipedia.org/wiki/Latin_square, acedido em 10 Out. 2007.

[16] WIKIPEDIA, The Free Encyclopedia – **Sudoku** [Em linha]. Disponível na WWW: URL: http://en.wikipedia.org/wiki/Sudoku, acedido em 10 Out. 2007.