UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM MATEMÁTICA

Milena Arantes Rocha Maciel

Planos projetivos finitos e aplicações em jogos, grafos, designs e códigos

Juiz de Fora
2023

Milena Arantes Rocha Maciel

Planos projetivos finitos e aplicações em jogos, grafos, designs e códigos

Trabalho de Conclusão de Curso apresentada ao Bacharelado em Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de bacharel em Matemática.

Orientadora: Profa. Dra. Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2023

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Maciel, Milena Arantes Rocha.
Planos projetivos finitos e aplicações em jogos, grafos, designs e códigos / Milena Arantes Rocha Maciel. – 2023.
72 f. : il.

Orientadora: Beatriz Casulari da Motta Ribeiro
Trabalho de Conclusão de Curso – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Bacharelado em Matemática, 2023.

1. Plano Projetivo Finito. 2. Grafos. 3. Designs. 4. Códigos Corretores de Erros. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

Milena Arantes Rocha Maciel

Planos projetivos finitos e aplicações em jogos, grafos, designs e códigos

Trabalho de Conclusão de Curso apresentada ao Bacharelado em Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de bacharel em Matemática.

Aprovada em 12 de dezembro de 2023

BANCA EXAMINADORA

Profa. Dra. Beatriz Casulari da Motta Ribeiro
Orientadora
Universidade Federal de Juiz de Fora

Prof. Dr. Frederico Sercio Feitosa
Universidade Federal de Juiz de Fora

Prof. Dr. Reginaldo Braz Batista
Universidade Federal de Juiz de Fora

Dedico este trabalho à minha rede de apoio.

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais, Maria da Glória e Francisco, por todo amor, carinho, compreensão e incentivo, sem vocês eu nada seria. Agradeço aos meus irmãos, Maíza e Michel, por todo amor e por estarem sempre na minha torcida. E também agradeço à Deus, por me abençoar e iluminar.

Agradeço ao meu namorado, Pedro, por ser um companheiro de vida incrível e deixar meus dias mais leves, sempre ao meu lado nos bons e maus momentos. Sua ajuda tem sido imprescindível para a concretização do meu futuro.

Agradeço à minha orientadora, Beatriz, pela sua sabedoria, paciência, aconselhamento e acolhimento. Você não apenas me inspira como profissional, mas também como a mulher excepcional que é. Aproveito para agradecer à todos os professores que participaram da minha vida acadêmica de alguma forma. Em particular, agradeço à professora Flaviana por me orientar no Programa de Iniciação Científica e Mestrado (PICME), sempre atenciosa e disposta a me ajudar.

Agradeço aos membros da banca examinadora, professores Frederico e Reginaldo, por terem gentilmente aceitado o convite para avaliar e enriquecer este trabalho com suas valiosas considerações.

Agradeço aos amigos presentes na minha vida, por deixarem a caminhada mais leve e alegre, sendo um apoio fundamental para não desistir. Agradeço à equipe de limpeza do espaço universitário, não apenas pelos serviços excepcionais que prestam, mas também pelos cumprimentos calorosos e sorrisos sinceros que compartilham diariamente.

Agradeço à minha professora de matemática do ensino fundamental, Rosani, pelo grande esforço e incentivo aos alunos para se dedicarem nas provas da OBMEP. Graças a esse apoio valioso, portas promissoras se abriram para mim. Aproveito para agradecer ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio financeiro durante minha formação.

Ademais, agradeço à todos os meus familiares que de alguma forma contribuíram para minha formação e à Universidade Federal de Juiz de Fora pelo ensino público, gratuito e de qualidade.

RESUMO

Neste trabalho, estamos interessados em conhecer os planos projetivos finitos e sua relação com diferentes áreas da matemática. Apresentamos uma aplicação em um jogo de cartas, na demonstração de um teorema sobre grafos, na existência de conjunto de quadrados latinos mutuamente ortogonais e, por fim, na construção de códigos corretores de erros sobre corpos finitos.

Palavras-chave: Plano Projetivo Finito. Grafos. Designs. Códigos Corretores de Erros.

ABSTRACT

In this work, we are interested in understanding finite projective planes and their relationship with different areas of mathematics. We present an application in a card game, in the demonstration of a theorem about graphs, in the existence of sets of mutually orthogonal Latin squares, and finally, in the construction of error correcting codes over finite fields.

Keywords: Finite Projective Planes. Graphs. Designs. Error Correcting Codes.

LISTA DE FIGURAS

Figura 1 – Toda reta contém pelo menos 3 pontos. 12
Figura 2 – Toda reta em um plano projetivo finito tem a mesma quantidade de pontos. 13
Figura 3 – Total de pontos em um plano projetivo de ordem n. 14
Figura 4 – Total de retas em um plano projetivo de ordem n. 15
Figura 5 – Plano de Fano. 16
Figura 6 – Plano Jogo da Velha. 17
Figura 7 – Malha 3×3. 17
Figura 8 – Plano de Fano $PG(2, q)$. 21
Figura 9 – O jogo *Dobble* em sua versão original. 22
Figura 10 – Duas cartas do *Dobble* original. 22
Figura 11 – The Lady's and Gentleman's Diary 23
Figura 12 – *Dobble* com temas distintos. 24
Figura 13 – *Dobble* versão animais. 25
Figura 14 – Cartas faltantes no *Dobble* animais. 25
Figura 15 – O *Dobble* Pixar Júnior representando o plano projetivo de ordem 5. . . 26
Figura 16 – *Dobble* de Fano (ordem 2). 27
Figura 17 – *Dobble* Jogo da Velha (ordem 3). 27
Figura 18 – Um grafo qualquer. 28
Figura 19 – Grafos do Teorema da Amizade com $n = 5$, $n = 7$ e $n = 9$. 32
Figura 20 – a tem 3 amigos. 34
Figura 21 – b não conhece a. 34
Figura 22 – $F(a, F(a, b))$ é um amigo comum de a e $F(a, b)$. 35
Figura 23 – Se z conhecesse $F(a, F(a, b))$, então $F(a, F(a, b))$ e a teriam 2 amigos em comum. 35
Figura 24 – $F(a, b), a$ e z não são colineares. 36
Figura 25 – $F(a, b), a$ e b não são colineares. 36
Figura 26 – $F(a, b), b$ e z não são colineares. 37
Figura 27 – a, b e z não são colineares. 37
Figura 28 – Quadrados latinos de ordens 3 e 4, respectivamente. 41
Figura 29 – Quadrados latinos de ordem 4. 41
Figura 30 – Dois quadrados latinos ortogonais de ordem 4. 41
Figura 31 – Conjunto completo de quadrados latinos ortogonais de ordem 5. 42
Figura 32 – Quadrados latinos ortogonais de ordem 9 como aparecem em "Gusuryak". 43
Figura 33 – Os mesmos quadrados latinos de ordem 9 em notação moderna. 43
Figura 34 – Equivalência entre 2 quadrados latinos ortogonais de ordem 3 e o plano projetivo de ordem 3. 48

Figura 35 – Mapa do caminho que A indica para B. 49
Figura 36 – Exemplo de cartão perfurado. 51
Figura 37 – O plano de Fano com coordenadas. 63
Figura 38 – O plano jogo da velha com coordenadas. 66

SUMÁRIO

1 INTRODUÇÃO 10
2 O PLANO PROJETIVO FINITO 12
2.1 DEFINIÇÕES PRELIMINARES 12
2.2 EXEMPLOS 15
2.3 CONSTRUÇÃO DE UM PLANO PROJETIVO 17
2.3.1 Corpos finitos 18
2.3.2 Planos projetivos sobre corpos finitos 19
3 APLICAÇÃO EM UM JOGO NÃO-MATEMÁTICO 22
3.1 O JOGO DOBBLE 22
3.2 RELAÇÃO ENTRE PLANO PROJETIVO FINITO E O DOBBLE . . 24
4 APLICAÇÃO EM GRAFOS 28
4.1 DEFINIÇÕES PRELIMINARES 28
4.1.1 Um pouco de álgebra linear 29
4.2 TEOREMA DA AMIZADE 31
4.2.1 Prova do Teorema da Amizade 32
5 APLICAÇÃO EM DESIGNS 41
5.1 DEFINIÇÕES PRELIMINARES 41
5.2 QUADRADOS LATINOS × PLANOS PROJETIVOS 43
6 APLICAÇÃO EM CÓDIGOS CORRETORES DE ERROS . . 49
6.1 MOTIVAÇÃO 49
6.2 CÓDIGOS LINEARES 50
6.2.1 Distância de Hamming e parâmetros de um código 51
6.2.2 Matrizes geradora e teste de paridade 58
6.2.3 Código de Hamming 61
6.3 CÓDIGO DE FANO 62
6.4 CÓDIGO JOGO DA VELHA 66
7 CONCLUSÃO 70
REFERÊNCIAS 71

1 INTRODUÇÃO

Na matemática, o conceito de um espaço projetivo originou-se do efeito visual da perspectiva, onde linhas paralelas parecem se encontrar no infinito. Um espaço projetivo pode, portanto, ser visto como a extensão de um espaço euclidiano, de forma que haja um ponto no infinito para cada direção de linhas paralelas. Neste trabalho estamos interessados somente em planos projetivos finitos. Por simplicidade, sempre que falarmos de plano projetivo estaremos nos referindo à plano projetivo finito.

Começaremos, no capítulo 2, apresentando a noção de plano projetivo a partir de uma definição axiomática e sua construção sobre corpos finitos. Neste capítulo, veremos ainda que planos projetivos finitos tem uma ordem n, que basicamente, determina o "tamanho" do plano, isto é, sua quantidade de pontos e retas. Até o momento, a ordem é sempre um número primo ou potência de primo. Para os números a que não são primos e nem potências de primos, não se tem um resultado geral sobre existência ou inexistência de planos projetivos de ordem a.

Os menores planos projetivos finitos são os de ordens 2 e 3. No capítulo 2, conheceremos o plano de Fano, construído por Gino Fano (1871 - 1952), que é de ordem 2 e o plano Jogo da Velha, que as primeiras referências aparecem em [15], o qual é de ordem 3, que voltarão a aparecer em capítulos subsequentes.

No início do século XX, Veblen [15], Bussey [16] e Wedderburn [17] provaram a existência de planos projetivos de ordens 4, 5, 7, 8 e 9. Uma observação interessante é que a existência não implica unicidade: em ordem 9, são conhecidos pelo menos 4 planos não isomorfos.

A inexistência de um plano projetivo finito de ordem 6 pode ser obtida de um resultado de Bose [1] em 1938 que diz que existe um plano projetivo de ordem n se, e somente se, existe um conjunto de $n-1$ quadrados latinos $n \times n$ mutuamente ortogonais, como veremos no capítulo 5. A existência ou não de um conjunto de quadrados latinos dessa forma é um problema muito mais antigo, tendo sido proposto por Euler em 1782, como também veremos no capítulo 5. Para $n = 6$, em 1901, Tarry [14] mostrou por enumeração sistemática, que é impossível encontrar um conjunto de 5 quadrados latinos 6×6 mutuamente ortogonais, o que implica, pelo trabalho de Bose, na inexistência do plano projetivo de ordem 6.

Porém, uma demonstração mais algébrica da inexistência de planos projetivos finitos de ordem 6 é como consequência do Teorema de Bruck-Ryser, publicado em 1949 [3], que diz: "Se $n \equiv 1$ ou $2 \pmod 4$, então uma condição necessária para a existência de um plano projetivo finito de ordem n é que existam $x, y \in \mathbb{Z}$ tais que $n = x^2 + y^2$." Como $6 \equiv 2 \pmod 4$ e não pode ser escrito como a soma dos quadrados de dois inteiros, o teorema de Bruck-Ryser implica na inexistência de plano projetivo de ordem 6.

Ainda, o teorema não só confirma essa inexistência, como prova a inexistência de vários outros, como os de ordens 14, 21 e 22. O menor número que não é potência de um número primo que o teorema não se aplica é 10, mas, em 1989 foi provado, depois de centenas de horas de cálculos computacionais [5], que não existe plano projetivo de ordem 10.

O objetivo principal deste trabalho é relacionar planos projetivos finitos com outras áreas da matemática. Assim, começaremos no capítulo 3 com uma forma concreta de ver esse objeto a partir de um jogo não-matemático chamado *Dobble*. Neste capítulo, apresentaremos esse jogo, como ele surgiu e uma das maneiras de jogar, depois faremos a relação dele com planos projetivos.

No capítulo 4, utilizaremos a ideia de plano projetivo finito para demonstrar um teorema da teoria de grafos, conhecido como "Teorema da Amizade". Neste capítulo, introduziremos algumas definições que nos serão necessárias da teoria de grafos e depois apresentaremos a demonstração do Teorema da Amizade usando planos projetivos.

No capítulo 5, apresentaremos o surpreendente Teorema de Bose sobre equivalência entre conjuntos completos de quadrados latinos mutuamente ortogonais e planos projetivos finitos. Para isso, iniciaremos o capítulo com algumas definições e resultados necessários para depois apresentarmos a demonstração do Teorema citado.

Por fim, no capítulo 6 destinaremos nosso estudo à Teoria de Códigos Corretores de Erros. Em particular, estamos interessados em códigos lineares, que serão definidos neste capítulo, assim como alguns resultados importantes. Depois, apresentaremos códigos lineares construídos a partir de planos projetivos conhecidos, que foram apresentados no capítulo 2.

2 O PLANO PROJETIVO FINITO

2.1 DEFINIÇÕES PRELIMINARES

Definição 2.1.1. *Seja V um conjunto finito cujos elementos são chamados pontos e alguns de seus subconjuntos são chamados retas tal que as seguintes propriedades são satisfeitas:*

(i) duas retas distintas se encontram precisamente em um único ponto;

(ii) dois pontos distintos definem uma única reta;

(iii) existem pelo menos 4 pontos dos quais não há 3 em uma mesma reta.

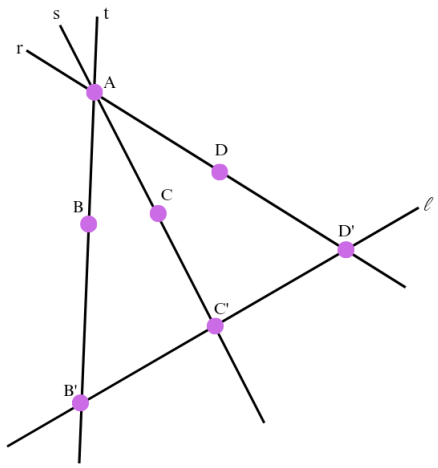
Então, V é chamado de ***plano projetivo finito****.*

Um plano projetivo pode ser considerado um plano euclidiano com "pontos no infinito" adicionais onde retas paralelas se cruzam e esses pontos formam o que chamamos de "reta no infinito".

Lema 2.1.2. *Toda reta em um plano projetivo finito contém pelo menos três pontos.*

Demonstração. Para mostrar este resultado usaremos as propriedades da Definição 2.1.1. Sejam A, B, C e D pontos que satisfazem a propriedade (iii) e ℓ uma reta arbitrária que não contém nenhum desses pontos. Por (ii) temos que A e D definem uma única reta r, A e C definem uma única reta s, e A e B definem uma única reta t. Por (i) cada uma dessas retas intersectam ℓ em um único ponto, sendo eles D', C' e B', respectivamente. Por construção, ℓ contém pelo menos esses três pontos.

Figura 1 – Toda reta contém pelo menos 3 pontos.



Fonte: Elaborada pela autora (2023).

Caso contrário, por exemplo, se as retas s e t intersectassem a reta ℓ no mesmo ponto D', teríamos A, C e D colineares, uma vez que os pontos A e D' pela propriedade (ii) definem uma única reta.

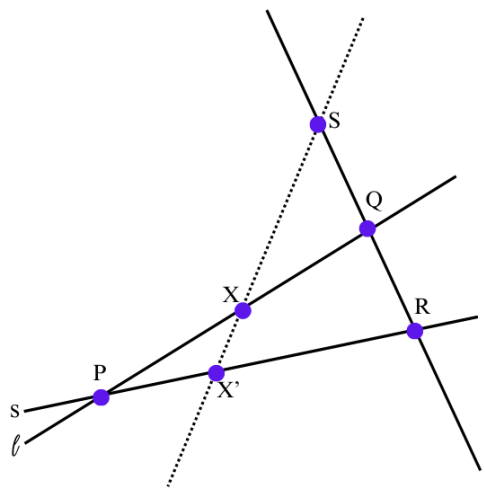
□

Proposição 2.1.3. *Toda reta em um plano projetivo finito tem o mesmo número de pontos.*

Demonstração. Sejam ℓ e s duas retas distintas. Pelo item (i) da Definição 2.1.1, existe um único ponto P na interseção de ℓ e s, e pelo Lema 2.1.2 temos que cada uma dessas retas tem pelo menos mais 2 pontos além de P que não estão na outra reta.

Sejam $Q \in \ell$ e $R \in s$ pontos distintos entre si e distintos do ponto P. Pelo item (ii) da Definição 2.1.1, Q e R definem uma única reta r, que tem pelo menos mais um ponto S (pelo Lema 2.1.2). Agora, conectando um ponto X qualquer de ℓ ao ponto S, temos uma reta que intersecta s em X'. Fazendo o mesmo partindo de X' em s, conectando-o ao ponto S, temos o ponto X em ℓ.

Figura 2 – Toda reta em um plano projetivo finito tem a mesma quantidade de pontos.



Fonte: Elaborada pela autora (2023).

Assim, há uma bijeção entre os pontos de ℓ e s, logo, as retas têm o mesmo número de pontos. É usual chamar essa quantidade de $n + 1$. □

Ainda, pelo mesmo raciocínio, todo ponto está em exatamente $n + 1$ retas.

Definição 2.1.4. *Um plano projetivo que contém $n+1$ pontos sobre cada reta é dito plano projetivo de* ***ordem*** *n.*

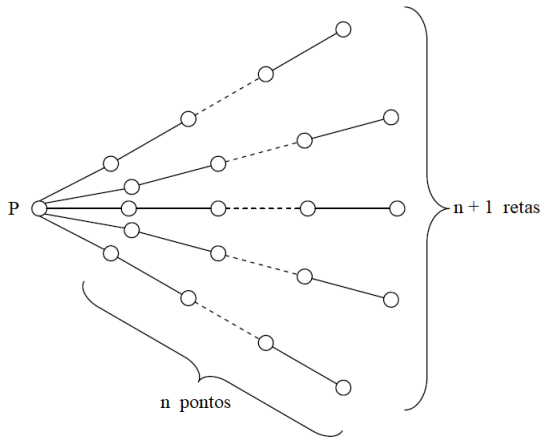
Até o momento, essa ordem n é sempre um número primo ou potência de primo. Para os números compostos x que não são potências de primos, não se tem um resultado geral sobre existência ou inexistência de planos projetivos de ordem x.

Ainda, temos que $n \geq 2$, uma vez que se $n = 1$, então $n^2 + n + 1 = 3$ e daí não satisfaria a propriedade (iii) da Definição 2.1.1.

Proposição 2.1.5. *Todo plano projetivo de ordem n contém exatamente n^2+n+1 pontos e $n^2 + n + 1$ retas.*

Demonstração. Seja P um ponto do plano. Sabemos que P está em $n + 1$ retas e, pelo item (i) da Definição 2.1.1, essas retas não têm mais nenhum ponto em comum. Mas cada uma dessas retas tem outros n pontos, o que implica que o plano tem, além de P, outros $n(n + 1) = n^2 + n$ pontos.

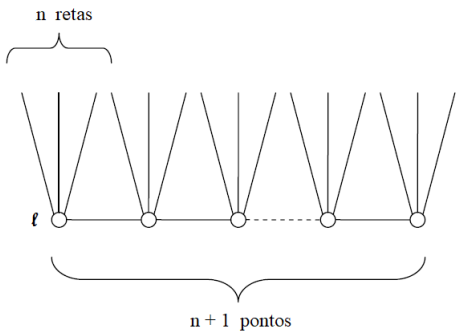
Figura 3 – Total de pontos em um plano projetivo de ordem n.



Fonte: Elaborada pela autora (2023).

Agora, considere uma reta ℓ. Sabemos que ℓ tem $n + 1$ pontos, e pelo item (ii) da Definição 2.1.1, cada ponto de ℓ está ainda em outras n retas distintas. Assim, existem, além de ℓ, $n(n + 1) = n^2 + n$ retas no plano.

Figura 4 – Total de retas em um plano projetivo de ordem n.



Fonte: Elaborada pela autora (2023).

□

Definição 2.1.6. *A* ***matriz de incidência*** $A = [a_{ij}]$ *de um plano projetivo* V *de ordem* n *é uma matriz* $n^2 + n + 1$ *por* $n^2 + n + 1$ *onde as linhas representam os pontos e as colunas representam as retas. A entrada* a_{ij} *é 1 se o ponto* i *está na reta* j*; caso contrário, é 0. Essa é uma representação matricial de quais pontos estão em quais retas.*

As propriedades de ser um plano projetivo são traduzidas em:

1. a soma de cada linha de A é constante igual a n+1;
2. a soma de cada coluna de A é constante igual a n+1;
3. o produto interno entre duas linhas distintas de A é igual a 1;
4. o produto interno entre duas colunas distintas de A é igual a 1.

Note que as propriedades 1 e 2 correspondem aos fatos duais de que cada ponto está em exatamente $n+1$ retas e cada reta contém exatamente $n+1$ pontos. Ainda, a propriedade 3 corresponde ao fato de que dois pontos distintos definem uma única reta e a propriedade 4 corresponde ao fato de que duas retas distintas se encontram em um único ponto.

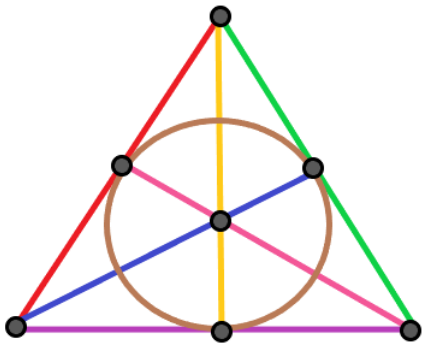
2.2 EXEMPLOS

Nessa seção, fazemos um passeio pelas ordens em que são conhecidos planos projetivos, dando atenção principal aos dois exemplos que usaremos em capítulos futuros.

Exemplo 2.2.1. *O menor plano projetivo não trivial é o de ordem 2, chamado de "Plano de Fano". Construído por Gino Fano (1871 - 1952), ele contém 3 pontos sobre cada reta, 7 retas, 7 pontos e todo ponto está contido em 3 retas distintas, como podemos verificar*

em sua representação mais famosa, a da figura 5. Também é simples verificar que existem 4 pontos dos quais 3 não são colineares. Em um artigo de 1904 [15], Veblen prova que é impossível desenhar o plano de Fano apenas com linhas retas.

Figura 5 – Plano de Fano.



Fonte: Elaborada pela autora (2023).

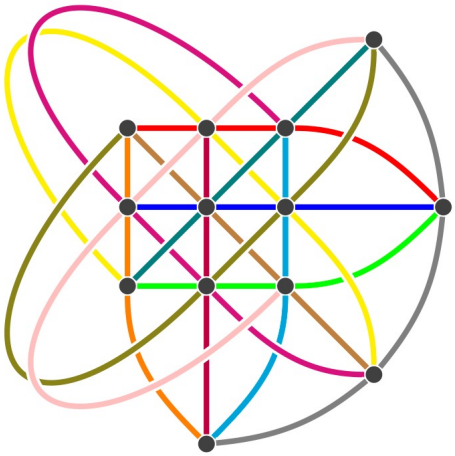
A matriz de incidência do plano de Fano é dada por

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Observe que cada linha e coluna tem três 1's, correspondendo aos fatos duais de que cada ponto está em exatamente três retas e cada reta contém exatamente três pontos. Observe também que qualquer par de linhas ou colunas tem um único 1 em comum, correspondendo aos fatos, respectivamente, de que há uma única reta incidente com dois pontos distintos e duas retas distintas incidentes a um único ponto. Por fim, a soma de cada linha e cada coluna é constante igual a 3. Ainda, o produto interno entre duas linhas distintas ou duas colunas distintas é igual a 1.

Exemplo 2.2.2. *Outro exemplo de plano projetivo é o de ordem 3, conhecido como "Plano Jogo da Velha". Ele contém 4 pontos sobre cada reta, 13 retas, 13 pontos e todo ponto está contido em 4 retas distintas, como podemos ver na figura 6.*

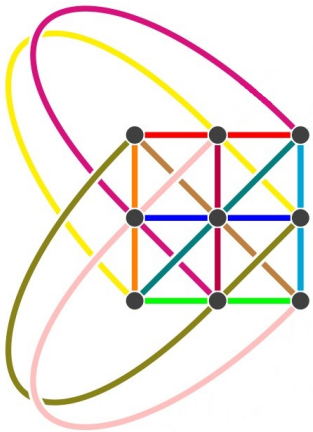
Figura 6 – Plano Jogo da Velha.



Fonte: `http://thewessens.net/ClassroomApps/Main/finitegeometry.html`

Observe que se não existisse a reta de cor cinza, teríamos retas paralelas numa malha 3×3 *como na figura 7. Para corrigir este problema, estendemos as retas que são paralelas entre si e fazemos com que elas se encontrem num único ponto, em seguida esses pontos "criados" formam uma única reta. Esta reta é o que chamamos de "reta no infinito" e os 4 pontos que estão contidos nela são os "pontos no infinito".*

Figura 7 – Malha 3×3.



Fonte: Elaborada pela autora (2023).

2.3 CONSTRUÇÃO DE UM PLANO PROJETIVO

A fim de ter uma estrutura algébrica importante para a utilização de planos projetivos finitos em capítulos subsequentes, vamos apresentar nessa seção a construção

de um plano projetivo sobre um corpo finito $\mathbb{F}_q$. Mas, antes, vamos fazer uma breve introdução aos corpos finitos.

2.3.1 Corpos finitos

Um anel comutativo A é um conjunto com duas operações binárias (usualmente chamadas adição e multiplicação) que é um grupo abeliano com respeito à adição com elemento neutro 0 e tal que a multiplicação é comutativa, associativa, distributiva e tem elemento neutro 1. Um corpo K é um anel comutativo em que todo elemento não-nulo tem inverso. Em particular, isso implica que, em K, se $ab = 0$ então $a = 0$ ou $b = 0$. São exemplos de corpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $\mathbb{Z}_p$ com p primo. Já $\mathbb{Z}_n$ com n composto não é um corpo, pois existem elementos não-nulos que não possuem inverso.

A característica c de um corpo é o menor inteiro positivo tal que $c \cdot 1 = 0$. Se não existe tal c, então dizemos que a característica do corpo é 0. É possível provar se um corpo tem característica positiva, então essa característica é um número primo. Em particular, se o corpo tem um número finito de elementos, sua característica é prima.

Seja K um corpo. O conjunto $K[x]$ dos polinômios em uma variável x com coeficientes em K é um anel comutativo com unidade sem divisores de zero, ou seja, um domínio de integridade. Dado um anel comutativo A, definimos um ideal I de A como um subconjunto de A fechado para a adição e tal que $r \cdot i \in I$ para todo $r \in A$ e $i \in I$. Em $K[x]$, escolhido um polinômio $p(x)$, o conjunto dos múltiplos de $p(x)$ em $K[x]$, isto é $\{g(x)p(x) | g(x) \in K[x]\}$, denotado por $\langle p(x) \rangle$, é um ideal dito gerado por $p(x)$. Mais ainda, todo ideal de $K[x]$ pode ser obtido dessa forma.

Dado um ideal I de A, podemos definir uma relação de equivalência entre elementos de A: $a \equiv b \pmod{I}$ se, e somente se, $a - b \in I$. As classes de equivalência formam o anel comutativo A/I com adição e multiplicação induzidos por A. Ainda, esse anel A/I é um corpo caso I seja maximal (sempre que exista J ideal de A com $I \subset J \subset A$, então $I = J$ ou $J = A$). Em $K[x]$, um polinômio $p(x)$ é dito irredutível se $p(x) = a(x)b(x)$ implica $a(x)$ ou $b(x)$ ser constante. Os ideais maximais de $K[x]$ são justamente os gerados por polinômios irredutíveis $p(x)$. Nesse caso, o anel $K[x]/\langle p(x) \rangle$ é um corpo. Essa é a chave para a construção de corpos finitos.

Em $K[x]$, temos um algoritmo de divisão análogo ao existente em $\mathbb{Z}$. Dados $f(x)$ e $g(x)$ em $K[x]$, existem únicos $q(x)$ e $r(x) \in K[x]$ tais que

$$f(x) = g(x)q(x) + r(x),$$

onde $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$ e $\partial(p(x))$ representa o grau de $p(x)$. Usando isso, podemos provar que se p é um primo e $p(x) \in \mathbb{Z}_p[x]$ é irredutível, então o corpo $\mathbb{Z}_p[x]/\langle p(x) \rangle$ é finito. De fato, dado $f(x) \in \mathbb{Z}_p[x]$, temos que existem únicos $q(x), r(x) \in \mathbb{Z}_p[x]$ tais que $f(x) = p(x)q(x) + r(x)$ e $r(x) = 0$ ou $\partial(r(x)) < \partial(p(x))$. Assim, em $\mathbb{Z}_p[x]/\langle p(x) \rangle$,

$\overline{f(x)} = \overline{r(x)}$. Como $\mathbb{Z}_p$ é finito, existe uma quantidade finita de possíveis polinômios $r(x)$ de grau menor que $p(x)$, donde existe uma quantidade finita de elementos em $\mathbb{Z}_p[x]/\langle p(x)\rangle$. Essa quantidade é justamente $p^{\partial(p(x))}$. Assim, concluímos que:

Proposição 2.3.1. *Seja p primo. Se $p(x) \in \mathbb{Z}_p[x]$ é irredutível sobre $\mathbb{Z}_p$ de grau n, então $\mathbb{Z}_p[x]/\langle p(x)\rangle$ é um corpo finito de característica p com p^n elementos.*

Dessa forma, existem corpos que vamos denotar por $\mathbb{F}_q$ com $q = p^n$ elementos para quaisquer p primo e n inteiro positivo, caso em $\mathbb{Z}_p[x]$ sempre exista pelo menos um polinômio irredutível de grau n. Como isso ocorre (veja o Teorema 2 do Capítulo 4 de [4]), podemos concluir que existem tais corpos. Ainda, esses corpos são únicos a menos de isomorfismo (veja o Teorema 4 do Capítulo 4 de [4]).

Exemplo 2.3.2. *O corpo $\mathbb{F}_{2^2}$ pode ser construído como $\mathbb{F}_2/\langle x^2+x+1\rangle$, já que x^2+x+1 é irredutível em $\mathbb{F}_2[x]$. Nesse caso:*

$$\mathbb{F}_4 = \mathbb{F}_2/\langle x^2+x+1\rangle = \{a\alpha+b\,;\, a,b \in \mathbb{F}_2 \text{ e } \alpha^2+\alpha+1 = 0\} = \{0,1,\alpha,\alpha+1\,;\, \alpha^2+\alpha+1 = 0\}$$

2.3.2 Planos projetivos sobre corpos finitos

Em geral, o plano projetivo $PG(2,q)$ é a geometria cujos subespaços de dimensão i para $i = 0,1,2$ são os subespaços de dimensão $i+1$ do espaço vetorial

$$V(3,q) = \mathbb{F}_q^3 = \{(x,y,z); x,y,z \in \mathbb{F}_q\}\,.$$

Assim, um ponto e uma reta de $PG(2,q)$ são, respectivamente, uma reta e um plano em $V(3,q)$. Essa ideia pode ser estendida para espaços projetivos de dimensão maior: $PG(k-1,q)$ é a geometria cujos subespaços de dimensão i são os subespaços de dimensão $i+1$ de $V(k,q) = \mathbb{F}_q^k$.

Uma forma de construir $PG(2,q)$ é a seguinte.

Em $V(3,q)\setminus\{(0,0,0)\}$ consideramos a relação de equivalência em que $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$ se, e somente se, existe $\lambda \in \mathbb{F}_q$ tal que $(x_1,y_1,z_1) = \lambda(x_2,y_2,z_2)$. O plano projetivo $PG(2,q)$ é, então, o conjunto das classes de equivalência e cada ponto é representado pela classe $(x:y:z)$. Notamos que se $z \neq 0$, então podemos representar o ponto $(x:y:z)$ por $(xz^{-1}:yz^{-1}:1)$, ou simplesmente por $(x:y:1)$ já considerando o produto por z^{-1}. Tais pontos são chamados os "pontos afins" de $PG(2,q)$, enquanto os pontos $(x:y:0)$ são os "pontos no infinito". Como há q elementos em $\mathbb{F}_q$, os pontos afins são exatamente q^2. Já os pontos no infinito são $(1:0:0)$ e q pontos do tipo $(x:1:0)$. Logo, $PG(2,q)$ tem q^2+q+1 pontos.

Uma reta em $PG(2,q)$ é o conjunto de soluções $(x:y:z)$ de uma equação do tipo $ax+by+cz = 0$, com $a,b,c \in \mathbb{F}_q$, sendo pelo menos um deles não nulo. Notamos que, então, há $q^2+q+1 = \dfrac{q^3-1}{q-1}$ retas em $PG(2,q)$, pois $ax+by+cz = 0$ e $\lambda ax+\lambda by+\lambda cz = 0$

representam a mesma reta, qualquer que seja $\lambda \neq 0$. A reta $z = 0$ é chamada "reta no infinito"; as demais retas são chamadas "retas afins".

Vamos ver que o plano $PG(2, q)$ satisfaz, de fato, os axiomas da Definição 2.1.1.

Para começar notamos que os pontos $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$ e $(1 : 1 : 1)$ satisfazem (iii) da Definição 2.1.1.

Agora, sejam $P = (x_1 : y_1 : z_1)$ e $Q = (x_2 : y_2 : z_2)$ pontos distintos em $PG(2, q)$. Para a propriedade (ii) da Definição 2.1.1, devemos mostrar que existem únicos $a, b, c \in \mathbb{F}_q$ tais que

$$\begin{cases} ax_1 + by_1 + cz_1 = 0 \\ ax_2 + by_2 + cz_2 = 0 \end{cases} . \tag{2.1}$$

Tratando (2.1) como um sistema em a, b, c, observamos que sua matriz completa tem posto 2, já que $P \neq Q$ significa que $(x_1, y_1, z_1) \neq \lambda(x_2, y_2, z_2)$ para todo $\lambda \in \mathbb{F}_q$. Se, sem perda de generalidade, $\det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \neq 0$, obtemos a e b como múltiplos de c, o que significa que $c \neq 0$ e a solução é $(a, b, c) = c(ac^{-1}, bc^{-1}, 1)$. Assim, em $PG(2, q)$ há apenas uma reta por P e Q.

Por último, sejam duas retas distintas em $PG(2, q)$. Para a propriedade (i) da Definição 2.1.1, devemos mostrar que existe um único ponto $(x : y : z)$ tal que

$$\begin{cases} a_1x + b_1y + c_1z = 0 \\ a_2x + b_2y + c_2z = 0 \end{cases} . \tag{2.2}$$

Resolvendo (2.2) como um sistema em x, y, z, vemos que sua matriz completa também tem posto 2, já que duas retas serem distintas significa que

$$a_1x + b_1y + c_1z \neq \lambda a_2x + \lambda b_2y + \lambda c_2z \,,$$

qualquer que seja $\lambda \neq 0$. Se, sem perda de generalidade, $\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \neq 0$, obtemos x e y como múltiplos de z, o que implica em $z \neq 0$ e a solução é $(x : y : z) = z(xz^{-1} : yz^{-1} : 1)$. Portanto, em $PG(2, q)$ existe apenas um ponto em comum entre duas retas distintas.

Exemplo 2.3.3. *Os pontos do plano de Fano $PG(2, 2)$, são as classes $(x : y : z)$ com $(x, y, z) \in \mathbb{F}_2^3 \setminus \{(0, 0, 0)\}$. Assim, se $z \neq 0$, temos $z = 1$ e os pontos*

$$(1 : 1 : 1)\,, (1 : 0 : 1)\,, (0 : 1 : 1)\,, (0 : 0 : 1)\,.$$

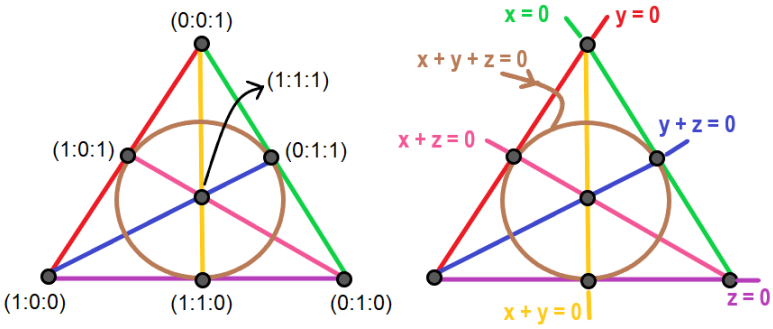
Já se $z = 0$, temos

$$(1 : 1 : 0)\,, (1 : 0 : 0)\,, (0 : 1 : 0)\,.$$

Os pontos com $z = 1$ são ditos pontos afins e os com $z = 0$ são chamados pontos no infinito.

Vemos, por exemplo, que os pontos $(1:1:1)$, $(1:0:1)$, $(0:1:0)$ *estão todos na reta* $x+z=0$. *O ponto* $(1:1:1)$ *está ainda nas retas* $x+y=0$ *e* $y+z=0$. *Veja a figura 8.*

Figura 8 – Plano de Fano $PG(2,q)$.



Fonte: Elaborada pela autora (2023).

3 APLICAÇÃO EM UM JOGO NÃO-MATEMÁTICO

Neste capítulo vamos apresentar um jogo, a princípio, não-matemático, chamado *Dobble* e, em seguida, veremos como sua estrutura de funcionamento depende da noção de plano projetivo finito.

3.1 O JOGO DOBBLE

Figura 9 – O jogo *Dobble* em sua versão original.

Fonte: `www.metropolybar.com.br/dobble-os-segredos-de-um-dos-jogos-mais-populares-da-atualidade/`

Dobble (ou *Spot It*), em sua versão original, é um jogo que contém 57 símbolos distintos distribuídos em 55 cartas, cada uma com 8 símbolos, de maneira que quaisquer duas cartas sempre têm exatamente um símbolo em comum. O jogo oferece 5 maneiras distintas de ser jogado, mas todas se resumem em ser o mais rápido a encontrar qual o símbolo em comum entre um par de cartas (figura 10).

Figura 10 – Duas cartas do *Dobble* original.

Fonte: `https://boardgamereview.co.uk/game-reviews/dobble-review/`

Por exemplo, uma forma simples de jogar é:

1. Preparação: Distribua as cartas igualmente pelos jogadores, com exceção de uma. Coloque essa carta restante no centro da área de jogo com a face virada para cima. Cada jogador embaralha suas próprias cartas, forma uma pilha de compras e a coloca à sua frente com a face virada para baixo.

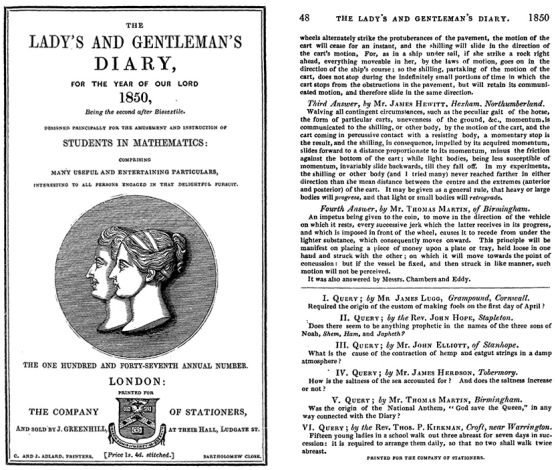
2. Objetivo: Ser o primeiro a livrar-se de todas as suas cartas.

3. Como jogar? O jogo começa com os jogadores virando sua pilha de compras para ficar com a face para cima. Cada jogador deve descartar as cartas de sua pilha de compras o mais rápido possível, colocando-as sobre a carta que está no centro da área de jogo. Para isso, eles precisam dizer o nome do símbolo em comum entre a carta do topo de sua pilha de compras e a carta que está no centro. Os jogadores precisam ser rápidos, pois a carta que está no centro muda assim que um jogador coloca uma de suas cartas sobre ela.

4. O perdedor: O último jogador a livrar-se de suas cartas perde o jogo.

A história por trás do jogo é antiga: em 1850, na Inglaterra, o problema conhecido como *"Kirkman's Schoolgirl Problem"* foi proposto pelo reverendo Thomas Penyngton Kirkman (1806 - 1895) em uma revista anual de matemática recreativa chamada *"The Lady's and Gentleman's Diary"* (figura 11) como Questão VI. O problema era o seguinte: *"Quinze moças em uma escola saem três lado a lado por sete dias consecutivos: é necessário organizá-las diariamente de modo que duas não caminhem duas vezes lado a lado."*

Figura 11 – The Lady's and Gentleman's Diary


THE
LADY'S AND GENTLEMAN'S
DIARY,
FOR THE YEAR OF OUR LORD
1850,
Being the second after Bissextile.
DESIGNED PRINCIPALLY FOR THE AMUSEMENT AND INSTRUCTION OF
STUDENTS IN MATHEMATICS:
COMPRISING
MANY USEFUL AND ENTERTAINING PARTICULARS,
INTERESTING TO ALL PERSONS ENGAGED IN THAT DELIGHTFUL PURSUIT.
THE ONE HUNDRED AND FORTY-SEVENTH ANNUAL NUMBER.
LONDON:
PRINTED FOR
THE COMPANY OF STATIONERS,
AND SOLD BY J. GREENHILL, AT THEIR HALL, LUDGATE ST.
C. AND J. ADLARD, PRINTERS. [*Price* 1*s.* 4*d. stitched.*] BARTHOLOMEW CLOSE.

48 THE LADY'S AND GENTLEMAN'S DIARY. 1850

wheels alternately strike the protuberances of the pavement, the motion of the cart will cease for an instant, and the shilling will slide in the direction of the cart's motion. For, as in a ship under sail, if she strike a rock right ahead, everything moveable in her, by the laws of motion, goes on in the direction of the ship's course; so the shilling, partaking of the motion of the cart, does not stop during the indefinitely small portions of time in which the cart stops from the obstructions in the pavement, but will retain its communicated motion, and therefore slide in the same direction.

Third Answer, by Mr. James Hewitt, *Hexham, Northumberland.*
Waiving all contingent circumstances, such as the peculiar gait of the horse, the form of particular carts, unevenness of the ground, &c., momentum is communicated to the shilling, or other body, by the motion of the cart, and the cart coming in percussive contact with a resisting body, a momentary stop is the result, and the shilling, in consequence, impelled by its acquired momentum, slides forward to a distance proportionate to its momentum, minus the friction against the bottom of the cart; while light bodies, being less susceptible of momentum, invariably slide backwards, till they fall off. In my experiments, the shilling or other body (and I tried many) never reached farther in either direction than the mean distance between the centre and the extremes (anterior and posterior) of the cart. It may be given as a general rule, that heavy or large bodies will *progress*, and that light or small bodies will *retrograde*.

Fourth Answer, by Mr. Thomas Martin, *of Birmingham.*
An impetus being given to the coin, to move in the direction of the vehicle on which it rests, every successive jerk which the latter receives in its progress, and which is imposed in front of the wheel, causes it to recede from under the lighter substance, which consequently moves onward. This principle will be manifest on placing a piece of money upon a plate or tray, held loose in one hand and struck with the other; on which it will move towards the point of concussion: but if the vessel be fixed, and then struck in like manner, such motion will not be perceived.
It was also answered by Messrs. Chambers and Eddy.

I. Query; *by* Mr James Lugg, *Grampound, Cornwall.*
Required the origin of the custom of making fools on the first day of April?

II. Query; *by the* Rev. John Hope, *Stapleton.*
Does there seem to be anything prophetic in the names of the three sons of Noah, *Shem, Ham,* and *Japheth?*

III. Query; *by* Mr. John Elliott, *of Stanhope.*
What is the cause of the contraction of hemp and catgut strings in a damp atmosphere?

IV. Query; *by* Mr. James Herdson, *Tobermory.*
How is the saltness of the sea accounted for? And does the saltness increase or not?

V. Query; *by* Mr. Thomas Martin, *Birmingham.*
Was the origin of the National Anthem, "God save the Queen," in any way connected with the Diary?

VI. Query; *by the* Rev. Thos. P. Kirkman, *Croft, near Warrington.*
Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily, so that no two shall walk twice abreast.

PRINTED FOR THE COMPANY OF STATIONERS.

Fonte: Wikipedia.

Em 1976, um jovem entusiasta da matemática chamado Jacques Cottereau, inspirado pelo problema, decidiu criar um modelo para fazer o "quebra-cabeça" funcionar em qualquer combinação e ser divertido. Assim, surgiu o *"jogo dos insetos"*: conjunto de 31

cartas com 6 imagens de insetos cada e exatamente uma imagem compartilhada entre 2 cartas aleatórias. Entretanto, esse jogo nunca foi divulgado e passou os próximos 30 anos desconhecido, até que em 2008 Denis Blanchot encontrou algumas cartas do *"jogo dos insetos"* - Cottereau é o pai da cunhada de Blanchot - e viu que aquilo poderia se tornar um jogo divertido.

Então, Blanchot trabalhou em símbolos diversos e depois de muitos testes eles descobriram várias abordagens de jogabilidade, assim, foi lançado o *Dobble* na França, em 2009. Segundo dados de 2018, o jogo esteve entre os 10 primeiros da lista de jogos de cartas mais vendidos da Amazon, com mais de 12 milhões de cópias vendidas desde seu lançamento e mais de 500 mil vendidos a cada ano somente nos EUA. Existem várias versões com tipos de símbolos diferentes, como futebol, desenhos animados, filmes famosos, entre outros. Nem todos tem 55 cartas e 57 símbolos, sendo 8 em cada carta. Versões chamadas "júnior" apresentam menos cartas, símbolos e símbolos por cartas, a fim de serem jogadas por crianças mais novas.

Figura 12 – *Dobble* com temas distintos.

Fonte: `www.alquimistasdosjogos.com.br/dobble`

3.2 RELAÇÃO ENTRE PLANO PROJETIVO FINITO E O DOBBLE

Uma pergunta que surge naturalmente ao jogar *Dobble* é: como é garantido que duas cartas distintas têm apenas um símbolo em comum se no total temos apenas 57 símbolos distintos? Chegamos então ao papel da noção de plano projetivo finito no jogo.

Podemos associar o *Dobble* a um plano projetivo de ordem 7. De fato, substituindo na definição 2.1.1 "ponto" por "carta" e "reta" por "símbolo", temos:

(i) Dois símbolos distintos "se encontram" exatamente em uma única carta;

(ii) Duas cartas distintas têm apenas um símbolo em comum;

(iii) Existem pelo menos 4 cartas entre as quais não há 3 com o mesmo símbolo comum.

Assim, o *Dobble* nada mais é do que um modelo de plano projetivo finito em que as cartas são pontos e os símbolos representam as retas. A não ser por uma questão: deveríamos ter $57 = 7^2 + 7 + 1$ cartas no total para satisfazer completamente a ideia de plano projetivo finito. Dessa forma, embora não seja exatamente um modelo completo, é a estrutura de plano projetivo finito que faz com que o jogo funcione perfeitamente. O fato de faltarem duas cartas (pontos) não interfere no fato das demais terem apenas um símbolo (reta) em comum, interfere somente no fato de que alguns símbolos estão presentes em menos de 8 cartas. Embora todos fiquem curiosos, ninguém sabe porque o jogo é produzido com 55 em vez de 57 cartas.

Figura 13 – *Dobble* versão animais.

Fonte: `www.mundogalapagos.com.br/dobble-animais/produto/DOB005`

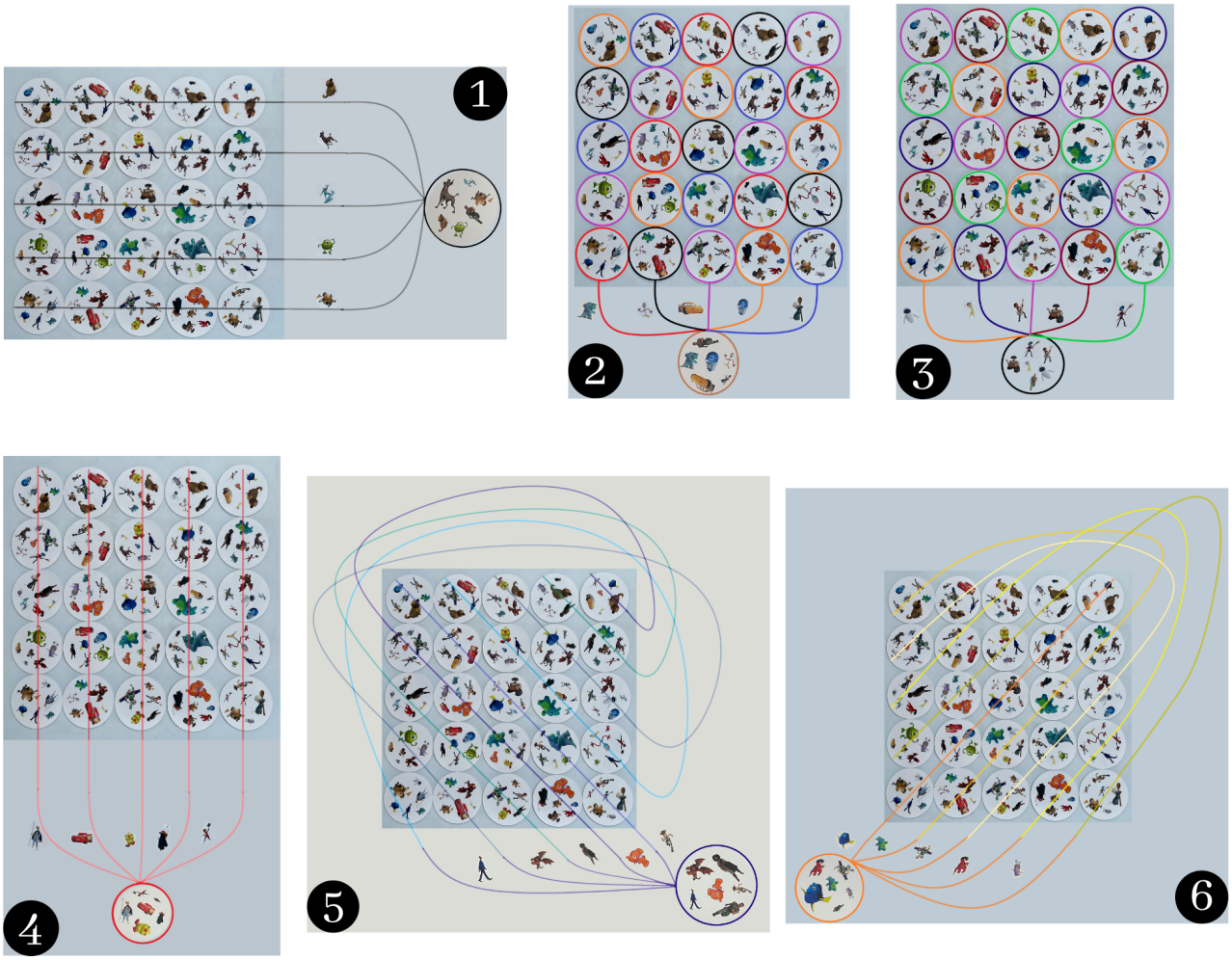
Observando o *Dobble* com tema animais (figura 13), que também tem 55 cartas, cada uma com 8 símbolos dentre os 57 existentes, como a versão original, notamos que a zebra aparece em 6 cartas distintas, 14 animais aparecem em 7 cartas distintas e o restante aparece exatamente em 8 cartas distintas. Assim, na figura 14, construímos as cartas que faltam pro jogo em sua versão animais representar de fato um plano projetivo.

Figura 14 – Cartas faltantes no *Dobble* animais.

Fonte: Elaborada pela autora (2022).

A fim de "enxergar" o plano projetivo finito utilizando o *Dobble*, por simplicidadade, utilizamos a edição Pixar Júnior, que contém 30 cartas, cada carta com 6 símbolos distintos e 31 símbolos diferentes no total. Na figura 15, organizamos as cartas do jogo e a carta faltante de forma a representar um plano projetivo finito de ordem 5 com suas $31 = 5^2+5+1$ retas. Cada um dos 6 desenhos apresenta 5 retas em que os pontos no infinito são as cartas destacadas, todos pertencem à mesma reta, aquela formada pela figura do personagem Combat Carl.

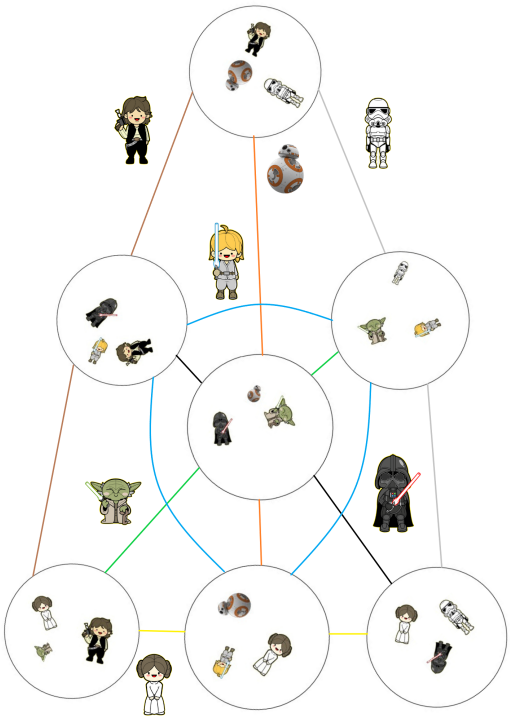
Figura 15 – O *Dobble* Pixar Júnior representando o plano projetivo de ordem 5.



Fonte: Elaborada pela autora (2022).

Essa apresentação visual do plano projetivo finito é bastante interessante para introduzir o conceito mais concretamente a quem esteja interessado. Com o intuito de facilitar essa ideia, podemos usar jogos construídos com menos cartas a partir dos planos de Fano e Jogo da Velha, como apresentados nas figuras 16 e 17 a seguir.

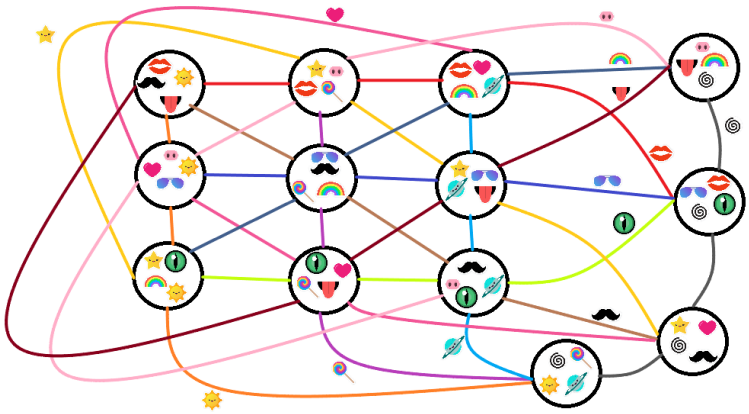
Figura 16 – *Dobble* de Fano (ordem 2).



Fonte: Elaborada pela autora (2022).

Por exemplo, poderíamos mostrar as cartas da figura 16 em que há 7 personagens diferentes de “Star Wars”, cada um representando uma reta em que os pontos são as cartas em que essa figura aparece. Por exemplo, a reta definida pelo Darth Vader é incidente a exatamente 3 pontos. Já o ponto mais ao alto está em 3 retas distintas, a do BB8, a do Stormtrooper e a do Han Solo. Ainda, 2 retas distintas se encontram em exatamente uma carta, ou seja, um par de personagens distintos está em exatamente uma carta.

Figura 17 – *Dobble* Jogo da Velha (ordem 3).



Fonte: Elaborada pela autora (2022).

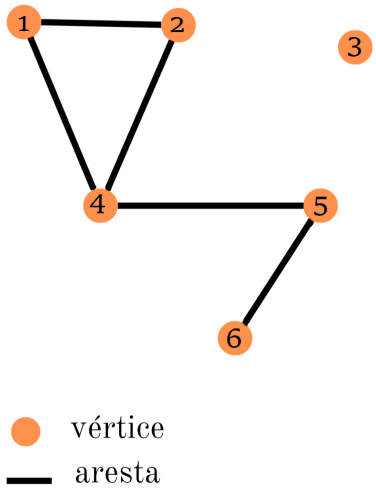
4 APLICAÇÃO EM GRAFOS

Neste capítulo vamos apresentar uma demostração do "Teorema da Amizade" usando planos projetivos finitos.

4.1 DEFINIÇÕES PRELIMINARES

Definição 4.1.1. *Um **grafo** é um par $G = (V, A)$ onde V é um conjunto finito e A é um conjunto de subconjuntos de 2 elementos de V. Os elementos de V são chamados **vértices** e os de A são ditos **arestas**.*

Figura 18 – Um grafo qualquer.



Fonte: Elaborada pela autora (2023).

Definição 4.1.2. *Sejam $G = (V, A)$ um grafo, e $u, v \in V$ vértices. Se $\{u, v\} \in A$, então dizemos que u e v são **vizinhos** (ou **adjacentes**). Definimos*

$$N(u) = \{vizinhos\ de\ u\} = \{v \in V; \{u, v\} \in A\}$$

*como a **vizinhança** de u e $d(u) = \#N(u)$ como o **grau** de u.*

Na figura 18, temos o vértice 3 que não tem vizinhos. Os demais vértices têm vizinhos e, portanto, têm graus maiores que zero. Por exemplo, o vértice 6 tem grau 1, já o vértice 4 tem grau 3, já que seus vizinhos são os vértices 1, 2 e 5. Estes, por sua vez, têm grau 2.

Definição 4.1.3. *Um grafo G é **simples** se todo par de vértices é conectado por no máximo uma aresta e nenhum vértice é conectado a si próprio, ou seja, não tem arestas múltiplas nem laços.*

Definição 4.1.4. ***Caminho*** *é uma sequência de vértices tal que de cada um dos vértices existe uma aresta para o vértice seguinte. O* ***comprimento do caminho*** *é o número de arestas que o caminho usa, contando-se arestas múltiplas vezes.* ***Ciclo*** *é um caminho que começa e acaba com o mesmo vértice.*

Na figura 18, por exemplo, podemos fazer um caminho de comprimento 3 do vértice 1 ao 6 percorrendo a sequência de vértices 1, 4, 5, 6. Podemos também observar o ciclo 1, 2, 4, 1.

4.1.1 Um pouco de álgebra linear

Sejam I a matriz identidade e J a matriz onde todas as entradas são iguais a 1, ambas $n \times n$. Nos será útil conhecer os autovalores de uma matriz $n \times n$ qualquer da forma $J + mI$.

Os autovalores de uma matriz A são números λ, tais que $Ax = \lambda x$ tem um vetor de solução diferente de zero, e cada uma dessas soluções é um autovetor associado ao autovalor λ correspondente. Lembre-se que as multiplicidades dos autovalores de uma matriz quadrada de ordem n devem somar n. Vamos mostrar que os autovalores procurados são:

(i) $\lambda_1 = m + n$ com multiplicidade 1, associado ao autovetor $x = (x_1, x_2, \cdots, x_n)$, onde $x_1 = x_2 = \cdots = x_n$; e

(ii) $\lambda_2 = m$ com multiplicidade $n - 1$, associado ao autovetor complementar $w = (w_1, w_2, \cdots, w_n)$, onde $w_1 + w_2 + \cdots + w_n = 0$.

Ainda, sabemos que se A é uma matriz triangular n-quadrada, então os autovalores de A são as entradas da diagonal principal.

Seja $A = J + mI$, ou seja,

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{n\times n} + \begin{pmatrix} m & 0 & \cdots & 0 \\ 0 & m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m \end{pmatrix}_{n\times n} = \begin{pmatrix} m+1 & 1 & \cdots & 1 \\ 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & m+1 \end{pmatrix}_{n\times n}.$$

Considere a equação $Ax = \lambda_1 x$, e seja $x = (x_1, x_2, \cdots, x_n) = (1, 1, \cdots, 1)$, o vetor das unidades. Temos

$$\lambda_1 x = Ax = \begin{pmatrix} m+1 & 1 & \cdots & 1 \\ 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & m+1 \end{pmatrix}_{n\times n} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}_{n\times 1} = \begin{pmatrix} (m+1)+1+\cdots+1 \\ 1+(m+1)+\cdots+1 \\ \vdots \\ 1+1+\cdots+(m+1) \end{pmatrix}_{n\times 1} =$$

$$\begin{pmatrix} m+n \\ m+n \\ \vdots \\ m+n \end{pmatrix}_{n\times 1} = \Big(m+n\Big) \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}_{n\times 1},$$

assim $\lambda_1 = m+n$ é um autovalor de A associado ao autovetor $x = (1, 1, \cdots, 1)$. Como A é simétrica, os autovalores são todos números reais e os autovetores de diferentes autoespaços são ortogonais.

Seja λ_2 outro autovalor de A associado ao autovetor $w = (w_1, w_2, \cdots, w_n)$. Pelo o que foi dito anteriormente, $x \cdot w = (1, 1, \cdots, 1) \cdot (w_1, w_2, \cdots, w_n) = 0$, já que os autovetores são ortogonais, daí

$$\lambda_2 w = Aw = (J + mI)w = Jw + mw = 0 + mw,$$

uma vez que

$$Jw = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{n\times n} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}_{n\times 1} = \begin{pmatrix} 1\cdot w_1 + 1\cdot w_2 + \cdots + 1\cdot w_n \\ 1\cdot w_1 + 1\cdot w_2 + \cdots + 1\cdot w_n \\ \vdots \\ 1\cdot w_1 + 1\cdot w_2 + \cdots + 1\cdot w_n \end{pmatrix}_{n\times 1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{n\times 1} = 0.$$

Então, $\lambda_2 w = Aw = mw$ e $\lambda_2 = m$ é um autovalor de A associado ao w. Como $(1, 1, \cdots, 1) \cdot (w_1, w_2, \cdots, w_n) = 0$, o autovetor w deve satisfazer $w_1 + w_2 + \cdots + w_n = 0$, como desejado.

Para as multiplicidades, usamos propriedades do determinante em operações elementares com linhas.

$$A = \begin{pmatrix} m+1 & 1 & \cdots & 1 \\ 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & m+1 \end{pmatrix}_{n\times n}$$

Some a segunda linha de A com a primeira, a terceira linha com a primeira, e assim por diante até a última linha de A. Chame essa nova matriz de B e observe que $\det B = \det A$:

$$B = \begin{pmatrix} m+n & m+n & \cdots & m+n \\ 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & m+1 \end{pmatrix}_{n\times n}$$

Agora multiplique a primeira linha de B por $\dfrac{1}{m+n}$, e chame essa nova matriz de C. Observe que $\det A = \det B = (m+n)\det C$.

$$C = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & m+1 \end{pmatrix}_{n\times n}$$

Subtraia a primeira linha de C da segunda linha, da terceira linha e de todas as linhas sucessivas e chame essa nova matriz de D.

$$D = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m \end{pmatrix}_{n\times n}$$

Observe que $\det A = (m+n)\det C = (m+n)\det D$. Multiplicando a primeira linha de D por $m+n$, temos uma nova matriz E tal que $\det D = \dfrac{1}{m+n}\det E$, o que implica em $\det A = (m+n)\det D = \det E$.

$$E = \begin{pmatrix} m+n & m+n & \cdots & m+n \\ 0 & m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m \end{pmatrix}_{n\times n}$$

Agora temos uma matriz triangular superior simétrica n-quadrada. O determinante desta nova matriz E é igual ao determinante da nossa matriz original A, então elas têm os mesmos autovalores que são as entradas da diagonal principal. Assim, temos o autovalor $m+n$ com multiplicidade 1 e o autovalor m com multiplicidade $n-1$.

4.2 TEOREMA DA AMIZADE

O Teorema da Amizade é um teorema bem conhecido e de formulação simples da teoria dos grafos, com muitas aplicações fora do campo. Seu enunciado ingênuo é:

Teorema 4.2.1. *Em uma festa de n pessoas, suponha que cada par de pessoas tenha exatamente um amigo em comum. Então, há uma pessoa na festa que conhece todo mundo.*

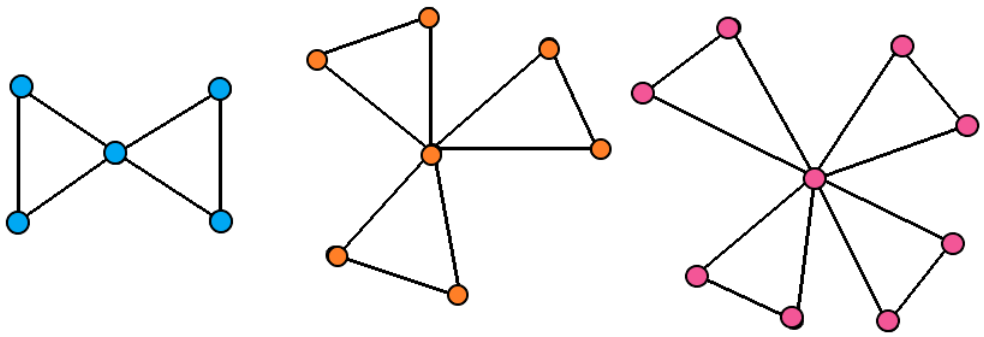
A maioria dos autores reconhece que a primeira prova publicada foi dada por Erdös, Rényi e Sós em 1966, embora apenas como um teorema sem nome. Desde então, muitas provas diferentes foram dadas por outros autores.

Vamos apresentar aqui uma abordagem interessante para o problema: seguindo os passos de um artigo de Herbert Wilf [18] que fornece uma prova geométrica usando planos projetivos finitos. Começamos assumindo que a conclusão do teorema é falsa e usamos essa suposição para construir um plano projetivo a partir da "festa", o que produz uma contradição com a matriz de incidência do plano projetivo e isso então prova que o teorema é verdadeiro.

Originalmente o teorema foi apresentado da seguinte forma:

Teorema 4.2.2 (Erdös)**.** *Seja G_n um grafo com n vértices no qual quaisquer dois pontos são conectados por um caminho de comprimento 2 e que não contém nenhum ciclo de comprimento 4, então $n = 2k + 1$ e G_n consiste em k triângulos que têm um vértice em comum.*

Figura 19 – Grafos do Teorema da Amizade com $n = 5$, $n = 7$ e $n = 9$.



Fonte: Elaborada pela autora (2023).

Podemos ver esse Teorema de uma forma que se assemelha mais ao Teorema ingênuo (Teorema 4.2.1):

Teorema 4.2.3 (Huneke)**.** *Se G é um grafo no qual quaisquer dois vértices distintos têm exatamente um vizinho comum, então G tem um vértice que está ligado a todos os outros.*

4.2.1 Prova do Teorema da Amizade

O teorema diz que em uma festa de n pessoas, se cada par de pessoas têm exatamente um amigo em comum, então há uma pessoa na festa que conhece todo mundo. Suponha que esta conclusão seja falsa, ou seja, não existe pessoa na festa que conheça todos as outras. Assim, em nossa discussão estudaremos as relações entre as pessoas, logo,

precisamos considerá-las como objetos matemáticos. Então, vamos definir que as pessoas são os vértices do grafo e a amizade entre duas pessoas distintas define uma aresta. Ainda, vamos supor que a relação de amizade é irreflexiva (a pessoa não é amiga dela mesma), simétrica (se uma pessoa x é amiga de y, então y é amiga de x) e única entre duas pessoas, ou seja, o grafo formado é simples.

Antes de prosseguirmos, precisamos de duas hipóteses que garantem a existência de amigos e desconhecidos dada uma pessoa arbitrária.

H1: Se x e y são pessoas (vértices) diferentes, eles têm um único amigo em comum $F(x, y)$.

H2: Para toda pessoa x existe uma pessoa $y \neq x$ tal que y não conhece x.

Então, desejamos mostrar que a festa pode ser representada como um plano projetivo V. Para isso, precisamos provar que ela satisfaz as três propriedades da definição de plano projetivo finito:

(i) Duas retas distintas se encontram precisamente em um único ponto.

Sejam $r(x)$ a reta que consiste em todos os amigos de x e $r(y)$ a reta que consiste em todos os amigos de y. Por H1, cada par de retas em V tem exatamente um ponto em comum, ou seja, $r(x) \cap r(y) = \{F(x, y)\}$.

(ii) Dois pontos distintos definem uma única reta.

Também pela suposição H1, se x e y são pontos distintos em V então eles têm um único amigo em comum $F(x, y)$. Assim, podemos dizer que todo par de pontos está em uma única reta e esta é a reta que consiste em todos os amigos de $F(x, y)$, logo, $(x, y) \in r(F(x, y))$.

(iii) Existem pelo menos 4 pontos dos quais não há 3 em uma mesma reta.

A demonstração de (iii) é mais trabalhosa e, portanto, vamos separar essa propriedade como um lema:

Lema 4.2.4. *Existe um conjunto de quatro pontos de V dos quais três não são colineares.*

Demonstração. Primeiro precisamos mostrar que V de fato contém quatro pontos.

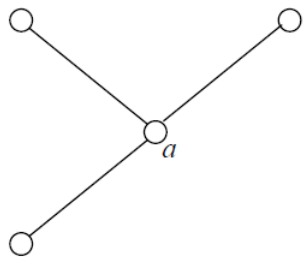
- Suponha que V tenha apenas um ponto x. Então temos uma contradição com H2, pois não há ponto y tal que y não conheça x.
- Suponha que V tenha apenas dois pontos x e y. Então temos uma contradição com H1, pois não há um amigo em comum $F(x, y)$.

- Suponha que V tenha apenas três pontos x, y e z. Por H1, x e y têm um amigo em comum, sendo a única opção z, então $z = F(x, y)$. Por H1, y e z têm um amigo em comum, sendo a única opção x, então $x = F(y, z)$. Por H1, x e z têm um amigo em comum, sendo a única opção y, então $y = F(x, z)$. Mas então todos os três pontos x, y e z são amigos uns dos outros, contradizendo H2.

Assim, V deve conter pelo menos quatro pontos.

Escolha quatro pontos distintos de V. Se não existirem três pontos colineares, terminamos. Caso contrário, existem três pontos que conhecem o mesmo ponto a, como mostrado na figura 20. Aqui, as retas contínuas denotam "conhecer".

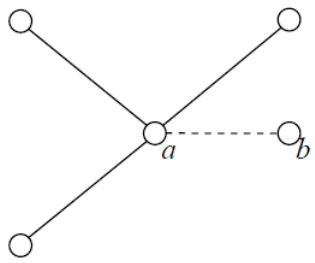
Figura 20 – a tem 3 amigos.



Fonte: [6]

Por H2, existe um b tal que b não conhece a, como mostrado na figura 21. Aqui as retas tracejadas denotam "desconhecer".

Figura 21 – b não conhece a.

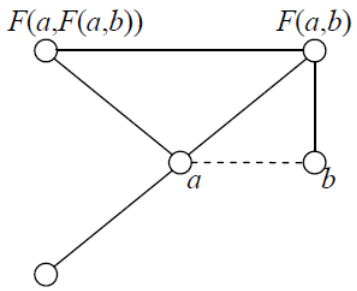


Fonte: [6]

Por H1, a e b devem ter um amigo em comum $F(a, b)$, e também por H1, a e $F(a, b)$ devem ter um amigo em comum $F(a, F(a, b))$, como mostrado na figura 22.

Escolha outro amigo de a diferente de $F(a, b)$ e $F(a, F(a, b))$ e rotule-o como z. Aqui, z não pode conhecer $F(a, F(a, b))$, pois se conhecesse, $F(a, F(a, b))$ e a teriam então

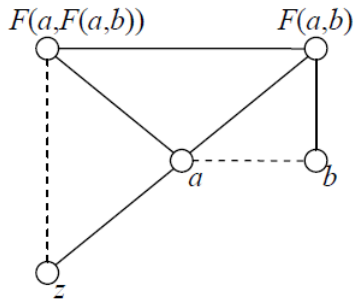
Figura 22 – $F(a, F(a, b))$ é um amigo comum de a e $F(a, b)$.



Fonte: [6]

dois amigos em comum – z e $F(a, b)$ - como podemos ver na figura 23. Afirmamos que os pontos $\{F(a, b), a, b, z\}$ satisfazem o Lema 1, isto é, três deles não são colineares (ou, em nosso contexto, nenhum dos três são amigos).

Figura 23 – Se z conhecesse $F(a, F(a, b))$, então $F(a, F(a, b))$ e a teriam 2 amigos em comum.



Fonte: [6]

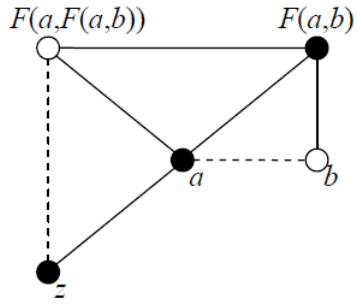
Considere todas as combinações possíveis de três pontos desses quatro.

Suponha que $\{F(a, b), a, z\}$ tenha um amigo em comum. Deve ser $F(a, F(a, b))$, pois já definimos acima que a não conhece b. Mas também definimos que z não conhece $F(a, F(a, b))$, e se isso fosse verdade, z e $F(a, b)$ teriam dois amigos em comum – a e $F(a, F(a, b))$. Isso é uma contradição, então esses três não podem ser amigos. (Veja a figura 24.)

Suponha que $\{F(a, b), a, b\}$ tenha um amigo em comum. Uma escolha lógica seria $F(a, b)$, pois este já é o único amigo em comum de a e b. No entanto, a não conhece b, então esses três não podem ser amigos. (Veja a figura 25.)

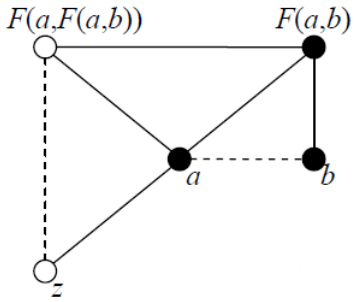
Suponha que $\{F(a, b), b, z\}$ tenha um amigo em comum. Como a já é o amigo em

Figura 24 – $F(a,b), a$ e z não são colineares.



Fonte: [6]

Figura 25 – $F(a,b), a$ e b não são colineares.



Fonte: [6]

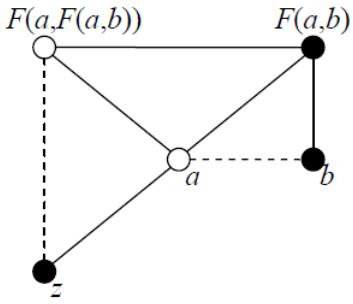
comum de z e $F(a,b)$, e a não conhece b, temos uma contradição, então esses três não podem ser amigos. (Veja a figura 26.)

Suponha que $\{a,b,z\}$ tenha um amigo em comum. Deve ser $F(a,b)$, pois este já é o único amigo em comum de a e b. Mas z não pode conhecer $F(a,b)$, pois caso contrário $F(a,b)$ e a teriam dois amigos em comum - z e $F(a,F(a,b))$. Uma contradição, então esses três não podem ser amigos. (Veja a figura 27.)

Como 3 pontos não podem ser amigos, temos que 3 deles não são colineares, e provamos P3. □

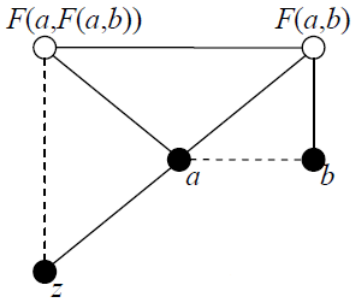
Concluímos então que V tem estrutura de plano projetivo. Seja A a matriz de incidência de V. Pelas definições feitas e pelo conhecimento de matrizes de incidência, sabemos que A deve ser (m^2+m+1)-quadrada, pois existem m^2+m+1 pontos e retas (correspondendo a "pessoas" e "amizades" neste problema). Também sabemos que, como cada reta contém $m+1$ pontos e cada ponto está em $m+1$ retas, cada linha e coluna de

Figura 26 – $F(a,b), b$ e z não são colineares.



Fonte: [6]

Figura 27 – a, b e z não são colineares.



Fonte: [6]

A deve ter $m+1$ entradas rotuladas com "1".

Lema 4.2.5. *A tem as seguintes propriedades:*

(A1) A é simétrica.

(A2) O traço de A é zero ($tr(A) = 0$).

(A3) $A^2 = Q = [q_{ij}]$, *onde* $q_{ij} = \begin{cases} m+1 & se \quad i = j \\ 1 & se \quad i \neq j \end{cases}$

Demonstração. Veja que a matriz de incidência é simétrica, pois se um ponto i está na reta j (ou seja, há "1" na ij-ésima posição de A), então o ponto j está na reta i (ou seja, há "1" na ji-ésima posição de A). Em notação de "pessoas" e "amizades", isto corresponde à "se uma pessoa i está no grupo de amigos da pessoa j, então a pessoa j está no grupo de amigos da pessoa i". Logo, temos a propriedade A1.

Agora, a matriz de incidência tem traço zero, pois todas entradas da diagonal são zero. De fato, o ii-ésimo elemento de A corresponde a perguntar "a pessoa i é amiga da pessoa i?" Como definimos amizade como irreflexiva, a resposta é não, exigindo um zero em todas as entradas da diagonal.

Por fim, quando elevamos A ao quadrado para obter Q, a ij-ésima entrada é encontrada tomando o produto escalar da i-ésima linha de A e a j-ésima coluna de A. Ou, como A é simétrica, a i-ésima linha de A e a j-ésima linha de A. Isso é equivalente ao número de pontos que quaisquer duas linhas i e j têm em comum, que é $m+1$ se $i=j$ (a mesma linha tem $m+1$ pontos nela e, portanto, $m+1$ pontos em comum consigo mesmo), e 1 se $i \neq j$ (pela definição de plano projetivo, duas retas se encontram em um único ponto).

Observe que A^2 também é (m^2+m+1)-quadrada, e

$$A^2 = \begin{pmatrix} m+1 & 1 & \cdots & 1 \\ 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & m+1 \end{pmatrix} = J + mI\,,$$

onde I é a matriz identidade e J é a matriz que todas as entradas são iguais a 1. □

Vamos deduzir uma contradição partindo dessas três propriedades de A do Lema 4.2.5 no seguinte resultado:

Lema 4.2.6. *Não existe plano projetivo de ordem $m > 1$ cuja matriz de incidência seja simétrica com traço zero.*

Demonstração. Com base na propriedade $(A3)$ do Lema 4.2.5, podemos calcular os autovalores de A^2, sabendo que A^2 é uma matriz (m^2+m+1)-quadrada da forma $J+mI$. Mostramos anteriormente que os autovalores de uma matriz n-quadrada desta forma são:

- $m+n$ com multiplicidade 1, e
- m com multiplicidade $n-1$.

Então, para A^2 os autovalores são:

- $m+(m^2+m+1) = m^2+2m+1$ com multiplicidade 1, e
- m com multiplicidade $(m^2+m+1)-1 = m^2+m$.

Ainda, todas as multiplicidades devem somar m^2+m+1. Observe que elas de fato obedecem a essa regra.

Agora, sabemos que se um autovalor de A^2 é λ, um autovalor correspondente de A é $\sqrt{\lambda}$. Portanto, os autovalores de A são:

- $\sqrt{m^2+2m+1} = \sqrt{(m+1)^2} = m+1$ com multiplicidade 1;
- $+\sqrt{m}$ com multiplicidade μ_1, e
- $-\sqrt{m}$ com multiplicidade μ_2.

Como todas as multiplicidades devem somar m^2+m+1 e o autovalor $m+1$ tem multiplicidade 1, então devemos ter

$$\mu_1 + \mu_2 = m^2 + m. \tag{4.1}$$

Também notamos que todas as multiplicidades (incluindo μ_1 e μ_2) devem ser inteiros, pois a multiplicidade de um autovalor representa o número de vezes que ele aparece como zero do polinômio característico.

Anteriormente, fomos capazes de encontrar os autovalores de uma matriz manipulando-a para produzir uma matriz triangular superior com os autovalores desejados ao longo da diagonal principal e o número de vezes que eles aparecem na diagonal principal iguala-se a sua multiplicidade. Também mostramos que $tr(A) = 0$. Combinando esses dois fatos, obtemos

$$\mu_1(\sqrt{m}) + \mu_2(-\sqrt{m}) + 1(m+1) = 0 \quad \Longrightarrow \quad (\mu_1 - \mu_2)\sqrt{m} + m + 1 = 0 \tag{4.2}$$

Pela equação 4.1 temos $\mu_1 = m^2 + m - \mu_2$, e substituindo na equação 4.2 obtemos

$$\begin{aligned}
((m^2+m-\mu_2)-\mu_2)\sqrt{m} + m + 1 &= 0 \\
(m^2+m-2\mu_2)\sqrt{m} + m + 1 &= 0 \\
m^2 + m - 2\mu_2 + \frac{m}{\sqrt{m}} + \frac{1}{\sqrt{m}} &= 0 \\
m^2 + m + \sqrt{m} + \frac{1}{\sqrt{m}} &= 2\mu_2 \\
\frac{1}{2}\left(m^2 + m + \sqrt{m} + \frac{1}{\sqrt{m}}\right) &= \mu_2.
\end{aligned}$$

Mostraremos que a expressão à esquerda não pode ser um inteiro.

Sabemos que tanto m quanto μ_2 são inteiros, pois m é a ordem do nosso plano projetivo e μ_2 é a multiplicidade de um de seus autovalores. Seja $t = \sqrt{m} + \dfrac{1}{\sqrt{m}}$ na equação acima, substituindo e resolvendo para t, obtemos

$$\begin{aligned}
\frac{1}{2}\left(m^2 + m + t\right) &= \mu_2 \\
t &= 2\mu_2 - m^2 - m,
\end{aligned}$$

então t deve ser um inteiro, já que m e μ_2 são inteiros. Se t é um inteiro, claramente t^2 também é um inteiro. No entanto,

$$\begin{aligned} t^2 &= \left(\sqrt{m} + \frac{1}{\sqrt{m}}\right)\left(\sqrt{m} + \frac{1}{\sqrt{m}}\right) \\ &= m + 1 + 1 + \frac{1}{m} \\ &= m + 2 + \frac{1}{m}, \end{aligned}$$

e como estamos considerando apenas $m > 1$, o termo $\frac{1}{m}$ implica que t^2 não pode ser um inteiro, e assim, t também não é um inteiro. Como μ_2 é definido em termos de t, logo, μ_2 não pode ser um inteiro. Esta é uma contradição, o que prova o lema. $\square$

Como provamos o lema, isso contradiz nossa suposição original de que a segunda metade do teorema da amizade é falsa, e portanto, o teorema deve ser verdadeiro.

5 APLICAÇÃO EM DESIGNS

5.1 DEFINIÇÕES PRELIMINARES

Definição 5.1.1. *Um* ***quadrado latino*** *de ordem n é uma matriz $n \times n$ com entradas de $\mathbb{Z}_n = \{1, 2, \cdots n\}$, onde cada número aparece exatamente uma vez em cada linha e cada coluna.*

Figura 28 – Quadrados latinos de ordens 3 e 4, respectivamente.

1	**2**	**3**
2	**3**	**1**
3	**1**	**2**

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

Fonte: Elaborada pela autora (2023).

Definição 5.1.2. *Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$ quadrados latinos. Dizemos que A e B são* ***ortogonais*** *se, e somente se, $C = [c_{ij}]$ contém todos os n^2 pares ordenados possíveis de $\mathbb{Z}_n \times \mathbb{Z}_n$, onde $c_{ij} = (a_{ij}, b_{ij})$.*

Os dois quadrados latinos na figura 29 são de ordem 4 e são ortogonais, como podemos ver na figura 30.

Figura 29 – Quadrados latinos de ordem 4.

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

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

Fonte: Elaborada pela autora (2023).

Figura 30 – Dois quadrados latinos ortogonais de ordem 4.

1,1	**2,2**	**3,3**	**4,4**
2,4	**1,3**	**4,2**	**3,1**
3,2	**4,1**	**1,4**	**2,3**
4,3	**3,4**	**2,1**	**1,2**

Fonte: Elaborada pela autora (2023).

Teorema 5.1.3. *Seja $\{S_1, S_2, \cdots, S_t\}$ um conjunto de t quadrados latinos mutuamente ortogonais de ordem $n \geq 3$. Então, $t \leq n-1$. Se a igualdade for válida, então o conjunto ortogonal é dito* ***completo****.*

Demonstração. Suponhamos, sem perda de generalidade, que na primeira linha de cada quadrado latino os elementos estão ordenados de 1 a n, e consideremos as t entradas que aparecem na posição (2, 1). Essas t entradas são distintas, caso contrário contradiz a ortogonalidade do conjunto. Nenhuma dessas entradas pode ser igual a 1, pois 1 é o elemento da posição (1, 1). Então, para as t entradas que se encontram na posição (2, 1) só existem no máximo $n-1$ possibilidades, e portanto, $t \leq n-1$. □

Figura 31 – Conjunto completo de quadrados latinos ortogonais de ordem 5.

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

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

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

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

Fonte: Elaborada pela autora (2023).

A matriz $C = [c_{ij}]$, $n \times n$, resultante também recebe o nome de quadrado greco-latino ou quadrado de Euler. Isto se deve pois em um artigo de 1782, Euler começou por expor o problema dos 36 oficiais. Este problema exige um arranjo de 36 oficiais de 6 patentes e de 6 regimentos em uma formação quadrada de tamanho 6 por 6. Cada linha vertical e cada linha horizontal desta formação deverá conter um, e apenas um, oficial de cada patente e um, e apenas um, oficial de cada regimento. Euler denotou os 6 regimentos pelas letras latinas a, b, c, d, e, f e as 6 patentes pelas letras gregas $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$. Observou ainda que a característica de um oficial era determinada pelas duas letras, uma latina e outra grega, e que o problema consistia em organizar as 36 combinações de duas letras num quadrado de tal maneira que cada linha e cada coluna contenham as seis letras latinas, bem como as seis letras gregas. Esta foi a origem do termo "quadrado greco-latino". Euler

observou que o primeiro passo era organizar as letras latinas em um quadrado de modo que nenhuma letra faltasse em qualquer linha ou coluna. Ele chamou esse quadrado de quadrado latino. Se ele tivesse escolhido organizar as letras gregas primeiro, provavelmente teríamos quadrados gregos em vez de quadrados latinos. Em qualquer caso, se rotularmos tanto as patentes quanto os regimentos de 1 a 6, então o problema de Euler reduz-se à construção de um par de quadrados latinos ortogonais de ordem 6.

Euler não encontrou solução para este problema específico. Então, ele conjecturou que não existe solução se a ordem do quadrado for da forma $n \equiv 2 \pmod 4$. O primeiro caso, $n = 2$, é trivialmente impossível.

Entretanto, há registros de que o coreano Choi Seok-jeong foi o primeiro a publicar um exemplo de dois quadrados latinos ortogonais de ordem 9 no livro "Gusuryak" (veja as figuras 32 e 33), a fim de construir um quadrado mágico[1] em 1700, antecedendo Leonhard Euler em 67 anos.

Figura 32 – Quadrados latinos ortogonais de ordem 9 como aparecem em "Gusuryak".

Fonte: `https://mathshistory.st-andrews.ac.uk/Biographies/Choi_Seok-jeong`

Figura 33 – Os mesmos quadrados latinos de ordem 9 em notação moderna.

(5,1)	(6,3)	(4,2)	(8,7)	(9,9)	(7,8)	(2,4)	(3,6)	(1,5)
(4,3)	(5,2)	(6,1)	(7,9)	(8,8)	(9,7)	(1,6)	(2,5)	(3,4)
(6,2)	(4,1)	(5,3)	(9,8)	(7,7)	(8,9)	(3,5)	(1,4)	(2,6)
(2,7)	(3,9)	(1,8)	(5,4)	(6,6)	(4,5)	(8,1)	(9,3)	(7,2)
(1,9)	(2,8)	(3,7)	(4,6)	(5,5)	(6,4)	(7,3)	(8,2)	(9,1)
(3,8)	(1,7)	(2,9)	(6,5)	(4,4)	(5,6)	(9,2)	(7,1)	(8,3)
(8,4)	(9,6)	(7,5)	(2,1)	(3,3)	(1,2)	(5,7)	(6,9)	(4,8)
(7,6)	(8,5)	(9,4)	(1,3)	(2,2)	(3,1)	(4,9)	(5,8)	(6,7)
(9,5)	(7,4)	(8,6)	(3,2)	(1,1)	(2,3)	(6,8)	(4,7)	(5,9)

Fonte: `https://mathshistory.st-andrews.ac.uk/Biographies/Choi_Seok-jeong`

5.2 QUADRADOS LATINOS × PLANOS PROJETIVOS

Teorema 5.2.1. *Sejam $n \geq 3$ e $t \geq 2$. Um conjunto de t quadrados latinos mutuamente ortogonais de ordem n é equivalente a uma matriz $n^2 \times (t+2)$ dada por $A = [a_{ij}]$, com $i \in \{1, \cdots, n^2\}$ e $j \in \{1, \cdots, t+2\}$, onde cada entrada a_{ij} varia entre $1, 2, \cdots, n$ e as linhas de cada submatriz n^2 por 2 de A formam os n^2 pares distintos onde cada entrada varia entre $1, 2, \cdots, n$.*

[1] Um quadrado mágico consiste de uma matriz $n \times n$ com entradas $1, 2, \cdots, n^2$ em que as somas dos números em cada linha, cada coluna e ambas as diagonais principais são as mesmas.

Demonstração. Vamos mostrar que uma matriz A dada desta forma de fato equivale a um conjunto de t quadrados latinos mutuamente ortogonais de ordem n. Primeiro, vamos permutar as linhas de A de maneira que as entradas das duas primeiras colunas estejam ordenadas de maneira "natural", ou seja, da seguinte maneira:

$$A = \begin{pmatrix} 1 & 1 & \cdots \\ 1 & 2 & \cdots \\ \vdots & \vdots & \ddots \\ 1 & n & \cdots \\ 2 & 1 & \cdots \\ 2 & 2 & \cdots \\ \vdots & \vdots & \ddots \\ 2 & n & \cdots \\ \vdots & \vdots & \ddots \\ n & 1 & \cdots \\ n & 2 & \cdots \\ \vdots & \vdots & \ddots \\ n & n & \cdots \end{pmatrix}_{n^2 \times (t+2)} .$$

Agora, para cada $k \in \{3, 4, \cdots, t+2\}$ vamos definir as matrizes A_k n por n de forma que a primeira linha de A_k consista das n primeiras entradas da coluna k de A, a segunda linha de A_k consista das próximas n entradas da coluna k de A, assim por diante até que a n-ésima linha de A_k consista das n últimas entradas da coluna k de A. Assim, formamos um conjunto de t matrizes n por n, sendo elas $A_3, A_4, \cdots, A_{t+2}$. Essas matrizes formam um conjunto de t quadrados latinos mutuamente ortogonais de ordem n. De fato, isso ocorre pelo formato da matriz A; a primeira coluna de A implica em A_k não ter duas entradas iguais em uma mesma linha e a segunda coluna de A implica em A_k não ter duas entradas iguais em uma mesma coluna. Ainda, se $l \neq m$ então A_l e A_m são ortogonais por conta da estrutura das colunas l e m de A, $l, m \in \{3, 4, \cdots, t+2\}$. Portanto, a matriz A dada é equivalente a um conjunto de t quadrados latinos mutuamente ortogonais de ordem n. □

Vamos fazer um exemplo para ilustrar o teorema 5.2.1.

Exemplo 5.2.2. *Sejam $n = 3$, $t = 2$ e*

$$A = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 1 & 3 & 2 & 2 \\ 1 & 1 & 1 & 3 \\ 2 & 3 & 3 & 3 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 2 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 2 & 3 \\ 3 & 3 & 1 & 1 \end{pmatrix}_{9\times 4}.$$

Observe que A é da forma descrita no teorema. Seguindo o processo da demonstração, vamos permutar as linhas de A de modo que as entradas das duas primeiras colunas estejam ordenadas de forma "natural". Temos:

$$A = \begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 2 & 2 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 2 \\ 2 & 3 & 3 & 3 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 2 & 3 \\ 3 & 3 & 1 & 1 \end{pmatrix}_{9\times 4}.$$

Agora, para cada $k \in \{3, 4\}$ vamos definir as matrizes A_3 e A_4, onde a primeira linha de de A_3 consiste das 3 primeiras entradas da terceira coluna de A, a segunda linha de A_3 consiste das próximas 3 entradas da terceira coluna de A e a terceira linha de A_3 consiste das 3 últimas entradas da terceira coluna de A. Fazemos de modo análogo para A_4 e obtemos

$$A_3 = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}_{3\times 3} \quad e \quad A_4 = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}_{3\times 3}.$$

Note que essas duas matrizes de fato formam um conjunto de 2 quadrados latinos mutuamente ortogonais de ordem 3. Ainda, este conjunto é completo pelo teorema 5.1.3.

Teorema 5.2.3. *Seja $n \geq 3$. Podemos construir um plano projetivo de ordem n se, e somente se, pudermos construir um conjunto completo de $n - 1$ quadrados latinos mutuamente ortogonais de ordem n.*

Demonstração. ($\Rightarrow$) Sejam V o plano projetivo de ordem n dado, l uma reta de V, $p_1, p_2, \cdots, p_{n+1}$ os $n + 1$ pontos incidentes à l e $q_1, q_2, \cdots, q_{n^2}$ os n^2 pontos que não são

incidentes à l. Para cada $j \in \{1, 2, \cdots, n+1\}$ vamos nomear as n retas que passam por p_j e que são diferentes de l com os números $1, 2, \cdots, n$ de maneira arbitrária.

Em particular, seja $q_i p_j$ a reta que é incidente aos pontos q_i e p_j, vamos chamá-la de a_{ij}. Então, $A = [a_{ij}]$ com $i \in \{1, 2, \cdots, n^2\}$ e $j \in \{1, 2, \cdots, n+1\}$ é uma matriz n^2 por $n+1$ onde cada entrada varia entre $1, 2, \cdots, n$. As linhas de cada submatriz n^2 por 2 de A são os n^2 pares onde cada entrada varia entre $1, 2, \cdots, n$. De fato, suponha que $a_{ij} = a_{i'j}$ e $a_{ik} = a_{i'k}$, onde $i \neq i'$ e $j \neq k$. Isso significa que $q_i p_j = q_{i'} p_j$ e $q_i p_k = q_{i'} p_k$, logo, a reta $q_i q_{i'}$ é incidente aos pontos p_j e p_k, mas como dois pontos distintos definem uma única reta, então $q_i q_{i'} = l$. Mas isto contradiz o fato de que q_i e $q_{i'}$ não são incidentes à l.

Portanto, a matriz A é da forma descrita no teorema 5.2.1 e produz um conjunto completo de $n-1$ quadrados latinos mutuamente ortogonais de ordem n.

($\Leftarrow$) Seja $A = [a_{ij}]$ com $i \in \{1, 2, \cdots, n^2\}$ e $j \in \{1, 2, \cdots, n+1\}$ uma matriz da forma descrita no teorema 5.2.1.

Vamos nomear as n^2 linhas de A como os "pontos afins" $q_1, q_2, \cdots, q_{n^2}$ e sejam $p_1, p_2, \cdots, p_{n+1}$ os $n+1$ "pontos no infinito". Uma "reta afim" l_{kj}, $k \in \{1, 2, \cdots, n\}$, $j \in \{1, 2, \cdots, n+1\}$, é aquela que passa pelo ponto no infinito p_j e pelos pontos afins que possuem k na coluna j de A. A "reta no infinito" l é aquela que passa apenas pelos pontos no infinito $p_1, p_2, \cdots, p_{n+1}$. Assim, definimos uma configuração V com $n^2 + n + 1$ pontos no total onde cada ponto é incidente à $n+1$ retas e cada reta é incidente à $n+1$ pontos.

Vamos mostrar que duas retas distintas têm um único ponto em comum. De fato:

- sejam l_{kj} e $l_{k'm}$ duas retas afins distintas onde $k \neq k'$ e $j \neq m$, essas retas são incidentes à um único ponto que é o ponto afim que tem k na coluna j e k' na coluna m;
- sejam l_{kj} e $l_{k'j}$ duas retas afins distintas onde $k \neq k'$, essas retas são incidentes à um único ponto que é o ponto no infinito p_j;
- a reta afim l_{kj} e a reta no infinito l também têm um único ponto em comum que é o ponto no infinito p_j.

Agora, vamos mostrar que dois pontos distintos definem uma única reta. De fato:

- sejam dois pontos afins q_i e $q_{i'}$, ou seja, estamos olhando para as linhas i e i' da matriz A e essas linhas têm apenas uma entrada com $k \in \{1, 2, \cdots, n\}$ em comum numa mesma coluna j devido à forma de A, logo, esses pontos afins definem uma única reta afim l_{kj};
- sejam dois pontos no infinito p_j e $p_{j'}$, por construção, eles definem uma única reta que é a reta no infinito l;

- o ponto afim q_i e o ponto no infinito p_j também definem uma única reta, pois pelo ponto no infinito sabemos que temos que olhar para a ij-ésima posição da matriz A para determinarmos um valor $k \in \{1, 2, \cdots, n\}$, e teremos somente uma reta afim l_{kj} incidente aos pontos q_i e p_j.

Por último, note que existem pelo menos 4 pontos dos quais não há 3 em uma mesma reta, por exemplo, basta pegarmos os quatro pontos $(1, 1, \cdots), (1, 2, \cdots), (2, 1, \cdots), (2, 2, \cdots)$.

Portanto, essa configuração V é de fato um plano projetivo de ordem n. □

Retornaremos ao exemplo 5.2.2 para podermos visualizar este último teorema feito.

Exemplo 5.2.4. *No exemplo 5.2.2 formamos a matriz*

$$A = \begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 2 & 2 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 2 \\ 2 & 3 & 3 & 3 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 2 & 3 \\ 3 & 3 & 1 & 1 \end{pmatrix}_{9\times 4}.$$

Assim, as linhas $1, 2, 3, 4, 5, 6, 7, 8$ *e* 9 *de* A *formam, respectivamente, os pontos afins* $q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8$ *e* q_9 *e sejam* p_1, p_2, p_3 *e* p_4 *os 4 pontos no infinito. Vamos construir todas as retas afins* l_{kj}, $k \in \{1, 2, 3\}$, $j \in \{1, 2, 3, 4\}$, *que passam pelo ponto no infinito* p_j *e pelos pontos afins que possuem* k *na coluna* j *de* A*:*

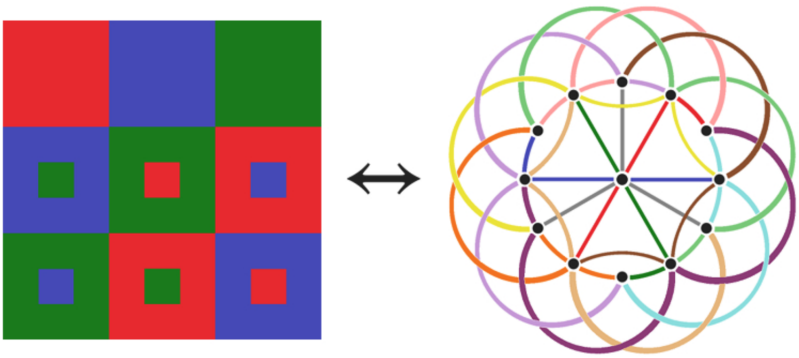
- l_{11} *passa por* p_1 *e pelos pontos afins que possuem 1 na coluna 1 de* A (q_1, q_2, q_3)*;*
- l_{12} *passa por* p_2 *e pelos pontos afins que possuem 1 na coluna 2 de* A (q_1, q_4, q_7)*;*
- l_{13} *passa por* p_3 *e pelos pontos afins que possuem 1 na coluna 3 de* A (q_1, q_5, q_9)*;*
- l_{14} *passa por* p_4 *e pelos pontos afins que possuem 1 na coluna 4 de* A (q_2, q_4, q_4)*;*
- l_{21} *passa por* p_1 *e pelos pontos afins que possuem 2 na coluna 1 de* A (q_4, q_5, q_6)*;*
- l_{22} *passa por* p_2 *e pelos pontos afins que possuem 2 na coluna 2 de* A (q_2, q_5, q_8)*;*
- l_{23} *passa por* p_3 *e pelos pontos afins que possuem 2 na coluna 3 de* A (q_3, q_4, q_8)*;*
- l_{24} *passa por* p_4 *e pelos pontos afins que possuem 2 na coluna 4 de* A (q_3, q_5, q_7)*;*
- l_{31} *passa por* p_1 *e pelos pontos afins que possuem 3 na coluna 1 de* A (q_7, q_8, q_9)*;*

- *l_{32} passa por p_2 e pelos pontos afins que possuem 3 na coluna 2 de A (q_3, q_6, q_9);*
- *l_{33} passa por p_3 e pelos pontos afins que possuem 3 na coluna 3 de A (q_2, q_6, q_7);*
- *l_{34} passa por p_4 e pelos pontos afins que possuem 3 na coluna 4 de A (q_1, q_6, q_8).*

Ainda temos a reta no infinito l que passa por todos os pontos no infinito p_1, p_2, p_3 e p_4. É fácil ver que esta configuração V que foi definida possui 13 pontos no total onde cada ponto é incidente à 4 retas e cada reta é incidente à 4 pontos. Ainda, satisfaz todas as propriedades da definição 2.1.1, e portanto, V é um plano projetivo finito de ordem 3.

Exemplo 5.2.5. *Na figura 34 abaixo, temos um exemplo de equivalência entre dois quadrados latinos ortogonais e o plano projetivo de ordem 3. À esquerda, estão os dois quadrados latinos ortogonais sobrepostos, nos quais, ao invés de números, temos cores. Basta associarmos os números 1, 2 e 3 com as cores vermelho, azul e verde, respectivamente. À direita, está o plano projetivo de ordem 3, onde os pontos e as retas foram reorganizadas para criar um diagrama mais simétrico e atraente em relação ao apresentado na seção 2.2 deste trabalho.*

Figura 34 – Equivalência entre 2 quadrados latinos ortogonais de ordem 3 e o plano projetivo de ordem 3.



Fonte: `https://puzzlewocky.com/math-fun/from-orthogonal-latin-squares-to-finite-projective-planes/`.

6 APLICAÇÃO EM CÓDIGOS CORRETORES DE ERROS

6.1 MOTIVAÇÃO

Suponhamos que uma pessoa A deseja transmitir para outra pessoa B uma mensagem que indica como ir do supermercado (sinalizado por um carrinho de compras) ao restaurante (sinalizado por um garfo e uma faca) a partir das direções Norte (N), Sul (S), Leste (L) e Oeste (O).

Figura 35 – Mapa do caminho que A indica para B.

Fonte: Elaborada pela autora (2023).

O código binário mais curto que poderíamos usar seria

$$C_1 = \begin{cases} N & \mapsto \ 00 \\ L & \mapsto \ 01 \\ S & \mapsto \ 10 \\ O & \mapsto \ 11 \end{cases}$$

Assim, para o mapa da figura 35, bastaria A enviar para B o código

$$0000000101010000000101010110101001010 1.$$

O problema desse código é o seguinte: caso haja uma interferência na transmissão causando um erro, não é possível detectá-lo (muito menos corrigi-lo). Por exemplo: se A envia 00 e B recebe 01, simplesmente irá para leste em vez de norte e provavelmente não chegará ao local correto. Isso acontece porque as palavras do código estão "muito próximas" (a "diferença" entre qualquer uma delas é 1). Podemos adicionar redundâncias

para tentar resolver isso. Por exemplo:

$$C_2 = \begin{cases} N & \mapsto 000 \\ L & \mapsto 011 \\ S & \mapsto 101 \\ O & \mapsto 110 \end{cases}$$

Agora, caso haja erro em um dígito, é possível saber que a informação está errada, pois a palavra recebida não pertencerá ao código. No entanto, não será possível descobrir qual era a mensagem correta. Por exemplo, se B recebe 001, percebe que a mensagem está errada, porém não tem como saber se a correta era 000, 011, 101. Esse código detecta erros, mas não corrige. Isso acontece porque as palavras do código ainda estão muito próximas. Isso pode ser corrigido com mais redundância. Por exemplo:

$$C_3 = \begin{cases} N & \mapsto 000000 \\ L & \mapsto 011011 \\ S & \mapsto 101101 \\ O & \mapsto 110110 \end{cases}$$

Nesse terceiro código, caso haja erro em um dígito, é possível não só detectar, mas também corrigir erros: basta escolher no código a palavra que tem apenas um dígito diferente da recebida. Por exemplo, se B recebe 001101, percebe que a mensagem está errada e consegue corrigi-la para a palavra "mais próxima" que é 101101 (Sul), pois todas as outras tem mais de um algarismos diferentes da recebida. Chamaremos esse código C_3 de *código do mapa*.

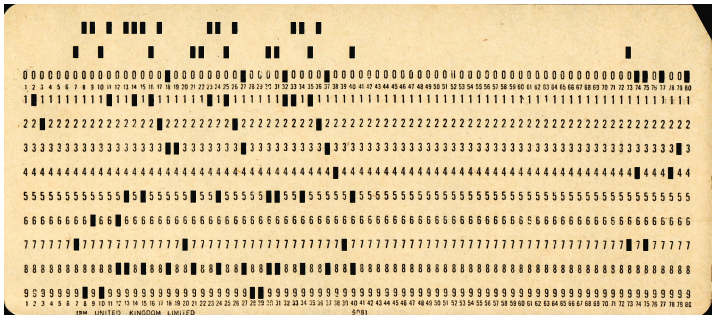
Vamos ver como uma estrutura algébrica vai facilitar a codificação de informações de forma a ser possível detectar e corrigir erros de transmissão.

6.2 CÓDIGOS LINEARES

O nascimento da teoria de Códigos Corretores de Erros foi nos anos 1940. Nessa época, eram utilizados cartões perfurados para programar o computador para fazer as tarefas desejadas. Um furo errado e a tarefa estaria errada. Assim, o "erro na transmissão" era puramente um erro humano. Também nessa época, Richard Hamming trabalhava no Bell Labs (atual Nokia Bell Labs) nos Estados Unidos e não se conformava com a incapacidade do computador de corrigir alguns erros humanos. Segundo o folclore, ele era autorizado a usar o computador para pesquisas nos finais de semana, quando deixava vários cartões "rodando". Quando havia algum erro, o computador pulava esse cartão. Para resolver esse problema do pulo e fazer com que o computador corrigisse um erro ao encontrá-lo, ele criou o primeiro código de correção de erros, o Código de Hamming

(veremos, em breve, esse código na definição 6.2.32 e no exemplo 6.2.33). Esse não era apenas um código corretor de erros qualquer, ele carrega uma estrutura algébrica, como veremos ao longo dessa seção. Surpreendentemente, o código de Hamming pode ser obtido de um plano projetivo finito, como veremos na seção seguinte.

Figura 36 – Exemplo de cartão perfurado.



Fonte: `https://en.wikipedia.org/wiki/Punched_card`

Definição 6.2.1. *Um* ***código linear*** $\mathcal{C}$ *é um subespaço vetorial de* $\mathbb{F}_q^n$ *sobre* $\mathbb{F}_q$*, onde* $\mathbb{F}_q$ *é o corpo finito com* q *elementos e* $n \in \mathbb{N}$*. Nesse caso,* $\mathbb{F}_q^n$ *é dito o* ***alfabeto****, os elementos de* $a_{k_1}a_{k_2}\cdots a_{k_n}$ *ou* $(a_{k_1}, a_{k_2}, \cdots, a_{k_n}) \in \mathcal{C}$ *são chamados* ***palavras-código****, sendo que cada palavra tem comprimento* n*. A dimensão* k *do código é a dimensão de* $\mathcal{C}$ *sobre* $\mathbb{F}_q$ *como espaço vetorial.*

Exemplo 6.2.2. *Para o código do mapa, nosso alfabeto será* $\mathbb{F}_2 = \{0, 1\}$ *que contém 2 elementos. Como o comprimento das palavras é 6, então trabalharemos com* $\mathbb{F}_2^6$*, que é um espaço vetorial sobre* $\mathbb{F}_2$ *de dimensão* 6*.*

6.2.1 Distância de Hamming e parâmetros de um código

Na motivação, vimos que a detecção de erros depende da distância entre as palavras. Então, vamos introduzir matematicamente um modo de medir distâncias entre elas.

Definição 6.2.3. *Seja* A *um conjunto não vazio. Uma* ***métrica*** *(ou* ***distância****) em* A *é uma função*

$$\begin{aligned} d : A \times A &\to \mathbb{R}_+ \\ (x, y) &\mapsto d(x, y) \in \mathbb{R}_+ \end{aligned}$$

que associa a cada par ordenado $(x, y) \in A \times A$ *um número real positivo* $d(x, y)$*, de modo que, dados* $x, y, z \in A$ *as seguintes condições são satisfeitas:*

(i) $d(x, x) = 0$*;*

(ii) se $x \neq y$*, então* $d(x, y) > 0$*;*

(iii) $d(x,y) = d(y,x)$;

(iv) $d(x,z) \leq d(x,y) + d(y,z)$.

Definição 6.2.4. *Dados dois elementos $u, v \in \mathbb{F}_q^n$, a* ***distância de Hamming*** *entre u e v é dada por*

$$d(u,v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|. \tag{6.1}$$

Em outras palavras, a distância de Hamming entre u e v é definida como o número de coordenadas distintas entre u e v.

Mostraremos a seguir que a distância de Hamming realmente pode ser vista como uma distância.

Proposição 6.2.5. *Dados $u, v, w \in \mathbb{F}_q^n$, valem as seguintes propriedades:*

(i) positividade: $d(u,v) \geq 0$, valendo a igualdade se, e somente se, $u = v$;

(ii) simetria: $d(u,v) = d(v,u)$;

(iii) desigualdade triangular: $d(u,v) \leq d(u,w) + d(w,v)$.

Demonstração. (i) Da forma que definimos a distância de Hamming é direto que $d(u,v) \geq 0$. Ainda:

$$\begin{aligned} d(u,v) = 0 \quad &\Leftrightarrow \quad |\{i;\ u_i \neq v_i,\ 1 \leq i \leq n\}| = 0 \\ &\Leftrightarrow \quad \nexists\, i;\ u_i \neq v_i \\ &\Leftrightarrow \quad u_i = v_i, \forall\, i = 1, \ldots, n \\ &\Leftrightarrow \quad u = v. \end{aligned}$$

(ii) Temos:

$$\begin{aligned} d(u,v) &= |\{i;\ u_i \neq v_i,\ 1 \leq i \leq n\}| \\ &= |\{i;\ v_i \neq u_i,\ 1 \leq i \leq n\}| \\ &= d(v,u). \end{aligned}$$

(iii) Agora, temos que a contribuição das i-ésimas coordenadas de u e v para $d(u,v)$ é igual a:

$$\begin{cases} 0, & \text{se } u_i = v_i \\ 1, & \text{se } u_i \neq v_i \end{cases}.$$

Por outro lado, a contribuição das i-ésimas coordenadas para $d(u,w) + d(w,v)$ é

$$\begin{cases} 0, & \text{se } u_i = w_i \text{ e } w_i = v_i \\ 1, & \text{se } u_i = w_i \text{ e } w_i \neq v_i, \text{ ou } u_i \neq w_i \text{ e } w_i = v_i \\ 2, & \text{se } u_i \neq w_i \text{ e } w_i \neq v_i \end{cases}.$$

Temos dois casos:

- Se a contribuição das i-ésimas coordenadas de de u e v para $d(u,v)$ for 0, então segue que a contribuição das i-ésimas coordenadas para $d(u,v)$ será menor ou igual a das i-ésimas coordenadas a $d(u,w)+d(w,v)$.
- Se a contribuição das i-ésimas coordenadas de u e v para $d(u,v)$ for 1, isto é, $u_i \neq v_i$, não teremos $u_i = w_i$ e $w_i = v_i$, simultaneamente. Assim, a contribuição das i-ésimas coordenadas para $d(u,w)+d(w,v)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas para $d(u,v)$.

Então, em ambos os casos teremos $d(u,v) \leq d(u,w)+d(w,v)$, como queríamos. □

As propriedades que provamos na Proposição 6.2.5 estão dentro das condições da Definição 6.2.3. Por conta disso, a distância de Hamming entre elementos de $\mathbb{F}_q^n$ é também chamada de **métrica de Hamming**.

Exemplo 6.2.6. *Vamos calcular todas as distâncias de Hamming do código do mapa. Temos o seguinte código linear*

$$\mathcal{C} = \begin{cases} N & \mapsto 000000 \\ L & \mapsto 011011 \\ S & \mapsto 101101 \\ O & \mapsto 110110 \end{cases},$$

assim:

$$\begin{aligned}
d(000000,000000) &= 0; & d(000000,011011) &= 4;\\
d(000000,101101) &= 4; & d(000000,110110) &= 4;\\
d(011011,000000) &= 4; & d(011011,011011) &= 0;\\
d(011011,101101) &= 4; & d(011011,110110) &= 4;\\
d(101101,000000) &= 4; & d(101101,011011) &= 4;\\
d(101101,101101) &= 0; & d(101101,110110) &= 4;\\
d(110110,000000) &= 4; & d(110110,011011) &= 4;\\
d(110110,101101) &= 4; & d(110110,110110) &= 0.
\end{aligned}$$

Definição 6.2.7. *Dados um elemento $a \in \mathbb{F}_q^n$ e um número real $t \geq 0$, definimos o* ***disco*** *e a* ***esfera*** *de centro a e raio t como sendo, respectivamente, os conjuntos*

$$D(a,t) = \{u \in \mathbb{F}_q^n;\ d(u,a) \leq t\},$$

$$S(a,t) = \{u \in \mathbb{F}_q^n;\ d(u,a) = t\}.$$

Estes conjunto são finitos e o próximo lema nos fornecerá as suas cardinalidades.

A seguir, empregaremos a notação usual para a combinação de elementos dois a dois, ou seja,

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

e denotaremos por $|A|$ o número de elementos de um conjunto finito A.

Lema 6.2.8. *Para todo $a \in \mathbb{F}_q^n$ e todo número natural $r > 0$, temos que*

$$|D(a,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i. \tag{6.2}$$

Demonstração. Note que $D(a,r) = \bigcup_{i=1}^{n} S(a,i)$ e $S(a,i) \cap S(a,j) = \varnothing$ se $i \neq j$. Então, $|D(a,r)| = \sum_{i=1}^{n} |S(a,i)|$.

Como $S(a,i) = \{u \in \mathbb{F}_q^n;\ d(u,a) = i\}$, $\forall\, i \in (1, \cdots, n)$, é fácil ver que $|S(a,i)| = \binom{n}{i}(q-1)^i$, $\forall\, i \in (1, \cdots, n)$, onde n é o tamanho da maior palavra em $\mathbb{F}_q$, q é o número de elementos de $\mathbb{F}_q$ e r é o raio do disco ou esfera.

Portanto,

$$|D(a,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

□

Definição 6.2.9. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código. A* ***distância mínima*** *de $\mathcal{C}$ é o número*

$$d = \min\{d(u,v);\ u, v \in \mathcal{C} \text{ e } u \neq v\}. \tag{6.3}$$

A princípio, para calcular d é necessário $\binom{M}{2}$ distâncias, onde M é o número de palavras no código, mas isto tem grande custo computacional. Veremos mais adiante como calcular d de modo mais econômico, com alguma estrutura algébrica adicional.

Definição 6.2.10. *Dado um código $\mathcal{C} \subset \mathbb{F}_q^n$ com distância mínima d, define-se*

$$\kappa = \left[\frac{d-1}{2}\right],$$

onde $[t]$ representa a parte inteira de $t \in \mathbb{R}$.

Exemplo 6.2.11. *No exemplo 6.2.6 calculamos todas as distâncias do código do mapa $\mathcal{C}$. Agora vamos calcular a distância mínima e o κ. Sejam $u, v \in \mathcal{C}$, então temos*

$$d = \min\{d(u,v);\ u \neq v\} = \min\{4\} = 4.$$

Ainda,

$$\kappa = \left[\frac{d-1}{2}\right] = \left[\frac{4-1}{2}\right] = \left[\frac{3}{2}\right] = 1.$$

Lema 6.2.12. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código com distância mínima d. Se c e c' são palavras distintas de $\mathcal{C}$, então*

$$D(c,\kappa) \cap D(c',\kappa) = \varnothing. \tag{6.4}$$

Demonstração. Suponhamos, por absurdo , que existe $x \in D(c,\kappa) \cap D(c',\kappa)$. Assim, teríamos $d(x,c) \leq \kappa$ e $d(x,c') \leq \kappa$, donde seguiria

$$\begin{aligned} d(c,c') &\overset{\text{desigualdade triangular}}{\leq} d(c,x) + d(x,c') \\ &\overset{\text{simetria}}{=} \underbrace{d(x,c)}_{\leq\kappa} + \underbrace{d(x,c')}_{\leq\kappa} \\ &\leq 2\kappa \\ &= 2\left[\frac{d-1}{2}\right] \\ &\leq d-1. \end{aligned}$$

Absurdo, pois $d(c,c') \geq d$, já que d é a distância mínima de $\mathcal{C}$.

Portanto,

$$D(c,\kappa) \cap D(c',\kappa) = \varnothing.$$

□

Teorema 6.2.13. *Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $\kappa = \left[\dfrac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Demonstração. Se ao transmitirmos uma palavra c do código cometemos t erros, com $t \leq \kappa$, então recebendo a palavra r, temos $d(r,c) = t \leq \kappa$. Enquanto que, pelo Lema 6.2.12, a distância de r a qualquer outra palavra do código e maior do que κ. Isso determina c univocamente a partir de r.

Por outro lado, dada uma palavra do código, podemos nela introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. □

Exemplo 6.2.14. *Pelo Teorema 6.2.13 acima e pelo o que calculamos no exemplo 6.2.11, temos que o código do mapa $\mathcal{C}$ pode corrigir até 1 erro e detectar até $4-1=3$ erros.*

Observe que pelo Teorema 6.2.13 temos que quanto maior a distância mínima do código, maior será sua capacidade de corrigir erros. Assim, é fundamental para a Teoria de Códigos poder calcular d ou pelo menos determinar uma cota inferior para ele.

Definição 6.2.15. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código com distância mínima d e seja $\kappa = \left[\frac{d-1}{2}\right]$. O código $\mathcal{C}$ será dito **perfeito** se*

$$\bigcup_{c \in \mathcal{C}} D(c,\kappa) = \mathbb{F}_q^n.$$

Todo código linear é por definição um espaço vetorial de dimensão finita. Seja k a dimensão do código $\mathcal{C}$ e seja $v_1, v_2, \cdots, v_k$ uma de suas bases, logo, todo elemento de $\mathcal{C}$ se escreve de maneira única como

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k,$$

onde os $\alpha_i,\ i = 1, 2, \cdots, k$, são elementos de $\mathbb{F}_q$. Assim

$$M = |\mathcal{C}| = q^k,$$

e consequentemente,

$$\dim_{\mathbb{F}_q} \mathcal{C} = k = \log_q q^k = \log_q M.$$

Definição 6.2.16. *Dado $x \in \mathbb{F}_q^n$, define-se o* ***peso*** *de x como sendo o número inteiro*

$$\omega(x) := |\{i;\ x_i \neq 0\}|. \tag{6.5}$$

Em outras palavras, temos que

$$\omega(x) = d(x, 0), \tag{6.6}$$

onde d é a métrica de Hamming.

Definição 6.2.17. *O peso de um código linear $\mathcal{C}$ é o inteiro*

$$\omega(\mathcal{C}) := \min\{\omega(x);\ x \in \mathcal{C} \setminus \{0\}\}. \tag{6.7}$$

Proposição 6.2.18. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Temos que*

(i) para todos $x, y \in \mathbb{F}_q^n$ vale $d(x, y) = \omega(x - y)$;

(ii) $d = \omega(\mathcal{C})$.

Demonstração. (i) Sejam $x, y \in \mathbb{F}_q^n$, dados por $x = (x_1, x_2, \cdots, x_n)$ e $y = (y_1, y_2, \cdots, y_n)$. Pelas Definições 6.2.4 e 6.2.16 temos

$$\begin{aligned}
\omega(x - y) &= d(x - y, 0) \\
&= |\{i;\ x_i - y_i \neq 0,\ 1 \leq i \leq n\}| \\
&= |\{i;\ x_i \neq y_i,\ 1 \leq i \leq n\}| \\
&= d(x, y),
\end{aligned}$$

uma vez que $x - y = (x_1, x_2, \cdots, x_n) - (y_1, y_2, \cdots, y_n) = (x_1 - y_1, x_2 - y_2, \cdots, x_n - y_n)$.

(ii) Para todos $x, y \in \mathcal{C}$ com $x \neq y$, temos $x - y \in \mathcal{C} \setminus \{0\}$. Defina $z = x - y$, pelo item (i) temos que $d(x, y) = \omega(x - y) = \omega(z)$. Assim

$$\begin{aligned} d &= \min\{d(x,y);\ x, y \in \mathcal{C} \text{ e } x \neq y\} \\ &= \min\{d(x,y);\ x, y \in \mathcal{C} \text{ e } x - y \neq 0\} \\ &= \min\{d(x,y);\ x - y \in \mathcal{C} \setminus \{0\}\} \\ &= \min\{\omega(z);\ z \in \mathcal{C} \setminus \{0\}\} \\ &= \omega(\mathcal{C}), \end{aligned}$$

como queríamos. □

Exemplo 6.2.19. *No exemplo 6.2.11 calculamos que a distância mínima do código do mapa $\mathcal{C}$ é 4. Então, pela Proposição 6.2.18 concluímos que $\omega(\mathcal{C}) = 4$ também, já que se trata de um código linear.*

Note que a Proposição **6.2.1** acima nos mostra que, em códigos lineares com M elementos, podemos calcular a distância mínima d a partir de $M - 1$ cálculos de distâncias, em vez dos $\binom{M}{2}$ cálculos requeridos anteriormente. Na prática, em códigos grandes, o custo computacional seria muito elevado para o cálculo de d dessa maneira. Assim, temos que desenvolver outros métodos para determinar a distância mínima de um código.

Devido ao item (ii) da Proposição **6.2.1**, a distância mínima de um código linear $\mathcal{C}$ será também chamada de **peso do código** $\mathcal{C}$.

Sejam $\mathbb{F}_q$ o corpo finito com q elementos e $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear. Chamaremos de **parâmetros** do código linear $\mathcal{C}$ a terna de inteiros $[n, k, d]_q$, onde n é o comprimento do código, k é a dimensão de $\mathcal{C}$ sobre $\mathbb{F}_q$ e d é a distância mínima de $\mathcal{C}$ (que é também igual ao peso $\omega(\mathcal{C})$ do código $\mathcal{C}$). Note que o número de elementos M de $\mathcal{C}$ é igual a q^k.

Exemplo 6.2.20. *Para o código do mapa já temos que $n = 6, d = 4$ e $q = 2$. Falta calcularmos k e para isso precisamos determinar uma base ordenada de $\mathcal{C}$, pois sabemos que k é a dimensão de $\mathcal{C}$ sobre $\mathbb{F}_2$. Temos as seguintes palavras-código:*

$$(0,0,0,0,0,0), (0,1,1,0,1,1), (1,0,1,1,0,1) \text{ e } (1,1,0,1,1,0),$$

que são vetores de $\mathbb{F}_2$. Note que

$$(0,0,0,0,0,0) = (0,1,1,0,1,1) + (0,1,1,0,1,1)$$

e

$$(1,1,0,1,1,0) = (0,1,1,0,1,1) + (1,0,1,1,0,1).$$

Logo, os únicos vetores que são linearmente independentes e que geram todas as palavras de $\mathcal{C}$ são os vetores $(0,1,1,0,1,1)$ e $(1,0,1,1,0,1)$, e portanto, eles formam uma base para $\mathcal{C}$. Sendo assim, temos que $k = 2$ e os parâmetros do código do mapa são $[6, 2, 4]_2$.

6.2.2 Matrizes geradora e teste de paridade

Definição 6.2.21. *Seja $\mathcal{B} = \{v_1, v_2, \cdots, v_k\}$ uma base ordenada de $\mathcal{C}$ e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, $i \in \{1, 2, \ldots, k\}$ da base, isto é,*

$$G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}. \tag{6.8}$$

*A matriz G é chamada de **matriz geradora** de $\mathcal{C}$ associada a base $\mathcal{B}$.*

Considere a transformação linear definida por

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG. \end{array}$$

Se $x = (x_1, x_2, \cdots, x_k)$, temos que

$$T(x) = xG = x_1v_1 + x_2v_2 + \cdots + x_kv_k,$$

logo, $T(\mathbb{F}_q^k) = \mathcal{C}$. Então, podemos considerar $\mathbb{F}_q^k$ como sendo o código da fonte, $\mathcal{C}$ o código de canal e T uma codificação.

Observe que a matriz G não é claramente determinada por $\mathcal{C}$, pois isso depende da escolha da base $\mathcal{B}$. Tenha em mente também que uma base de um espaço vetorial pode ser adquirida de outra qualquer por meio de sequências de operações do tipo:

- permutação de dois elementos da base;
- multiplicação de um elemento da base por um escalar não nulo;
- substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.

Portanto, conclui-se que duas matrizes geradoras de um mesmo código $\mathcal{C}$ podem ser obtidas uma da outra por uma sequência de operações do tipo:

(L1) Permutação de duas linhas.

(L2) Multiplicação de uma linha por um escalar não nulo.

(L3) Adição de um múltiplo escalar de uma linha a outra.

Por outro lado, é possível criar códigos a partir de matrizes geradoras G. Para isso, é suficiente tomar uma matriz com linhas que sejam linearmente independentes e definir um código como sendo a imagem da transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG. \end{array}$$

Definição 6.2.22. *Dizemos que uma matriz geradora G de um código $\mathcal{C}$ está na* ***forma padrão*** *se tivermos*

$$G = (Id_k \mid A),$$

onde Id_k é a matriz identidade $k \times k$ e A é uma matriz $k \times (n-k)$.

Exemplo 6.2.23. *No exemplo 6.2.20 calculamos uma base para o código do mapa $\mathcal{C}$, sendo ela $\mathcal{B} = \{(0,1,1,0,1,1),(1,0,1,1,0,1)\}$. Assim a matriz geradora G associada a base $\mathcal{B}$ é dada por*

$$G = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Permutando suas colunas podemos reescrevê-la na forma padrão e obtemos

$$G = (Id_2 \mid A) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Observação 6.2.24. *Observamos que a matriz geradora na forma padrão, por ter as primeiras k colunas como a identidade $k \times k$, facilita a decodificação pelo receptor. Isso porque ao tomar $u \in \mathbb{F}^k$ e codificar usando G, obtemos $v = uG$ com as k primeiras coordenadas sendo as coordenadas de u e as demais as chamadas redundâncias. Assim, a decodificação, após correção de erros, pode ser feita apenas ignorando as $n-k$ coordenadas finais.*

Definição 6.2.25. *A* ***matriz teste de paridade*** *para um código linear $\mathcal{C} \subset \mathbb{F}_q^n$ é uma matriz H, $m \times n$, com entradas em $\mathbb{F}_q$ tal que*

$$\mathcal{C} \;=\; \{u \in \mathbb{F}_q^n;\; uH^t = 0\}, \tag{6.9}$$

onde H^t é a transposta da matriz H.

Proposição 6.2.26. *Seja $\mathcal{C}$ um código linear com matriz teste de paridade H. Se todo conjunto com $d-1$ colunas de H é linearmente independente e existem d colunas linearmente dependentes, então a distância mínima de $\mathcal{C}$ é d.*

Demonstração. Sejam c uma palavra do código $\mathcal{C}$ e K o conjunto das coordenadas não nulas de c, então $|K| = \omega(c)$. Sejam $h_1, h_2, \cdots, h_n$ as colunas de H. Como H é uma matriz teste de paridade para $\mathcal{C}$, temos:

$$cH^t = 0 \;\Rightarrow\; \sum_{i \in K} c_i h_i = 0.$$

Assim, existe uma combinação linear de $|K|$ colunas de H que são linearmente dependentes. Logo, pela Proposição 6.2.18, existe uma combinação linear de $|K| = d$ colunas de H que são linearmente dependentes. $\square$

Proposição 6.2.27. *Seja G uma matriz geradora de um código linear $\mathcal{C}$ de dimensão k. Uma matriz H, $m \times n$, é uma matriz teste de paridade para $\mathcal{C}$ se, e somente se, $GH^t = 0$ e o posto de H é $n - k$.*

Demonstração. ($\Rightarrow$) Seja H uma matriz teste de paridade $m \times n$ para $\mathcal{C}$. Sendo G uma matriz geradora de $\mathcal{C}$, todas as linhas de G são palavras do código $\mathcal{C}$. Então, se ℓ é uma linha de G, $\ell H^t = 0$, donde $GH^t = 0$. Logo, a dimensão k do código $\mathcal{C}$ é $n - \text{posto}(H)$, ou seja, o posto de H é $n - k$.
($\Leftarrow$) Agora, suponhamos que $GH^t = 0$ e que o posto de H é $n - k$. Sendo G uma matriz geradora, uma palavra do $c \in \mathcal{C}$ se escreve como uma combinação linear das linhas de G, donde $cH^t = 0$. Como o posto de H é $n - k$, a dimensão do núcleo (à esquerda) é k, que é a dimensão de $\mathcal{C}$, logo $\mathcal{C}$ é todo o núcleo. $\square$

Proposição 6.2.28. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = (Id_k|A)$ na forma padrão. Então, $H = (-A^t|Id_{n-k})$ é uma matriz teste de paridade para $\mathcal{C}$.*

Demonstração. Provar que $H = (-A^t|Id_{n-k})$ é uma matriz teste de paridade para $\mathcal{C}$ é provar que e o produto interno da $i-$ésima linha de $G = (g_{ij})$ com a $\ell-$linha de $H = (h_{\ell j})$ é 0. Para $j \leq k$, temos $g_{ij} = 0$, a menos que $i = j$ ($g_{ij} = 0$). Para $j \geq k+1$, temos $h_{\ell j} = 0$, a menos que $\ell = j - k$ ($h_{\ell\ell+k} = 1$). Portanto:

$$\sum_{j=1}^{n} g_{ij}h_{\ell j} = \sum_{j=1}^{k} g_{ij}h_{\ell j} + \sum_{j=k+1}^{n} g_{ij}h_{\ell j} = h_{\ell i} + g_{i,\ell+k} = -a_{i\ell} + a_{i\ell} = 0.$$

$\square$

Exemplo 6.2.29. *No exemplo 6.2.23 obtemos a matriz geradora G para o código do mapa $\mathcal{C}$. Agora, pela Proposição 6.2.28 vamos obter a matriz teste de paridade para $\mathcal{C}$. Temos*

$$G = (Id_2 \mid A) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

onde $A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, *logo,* $-A^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}$ *uma vez que* $-1 \equiv 1$ *em* $\mathbb{F}_2$. *Assim a*

matriz teste de paridade de $\mathcal{C}$ é dada por

$$H = (-A^t|Id_4) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ainda, note que de fato $GH^t = 0$ e que o posto de H é $n - k = 6 - 2 = 4$, pois temos

$$GH^t = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 2 & 2 \\ 0 & 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

uma vez que $2 \equiv 0$ em $\mathbb{F}_2$, e posto$(H) = 4$ pois temos apenas 4 linhas de H que são linearmente independentes.

Finalizamos essa subseção com um comentário sobre correção de erros. Seja $\mathcal{C}$ um código de comprimento n sobre $\mathbb{F}_q$ de matriz geradora G e matriz teste de paridade H. Dado $u \in \mathbb{F}_q^k$, codificamos u fazendo $uG = v$. Ao transmitir v, caso haja exatamente um erro, será recebida a palavra $v_1 = v + r$, onde $r \in \mathbb{F}_q^n$ tem 0 em todas as coordenadas, menos uma delas, por exemplo, digamos que a $i-$ésima coordenada seja $\lambda \in \mathbb{F}_q$. O receptor, para testar se a mensagem recebida tem erros, faz

$$v_1 H^t = (v + r)H^t = vH^t + rH^t = rH^t\,,$$

onde a última igualdade vem do fato que $v \in \mathcal{C}$. Dessa forma, assumimos resultado de $v_1 H^t$ como o indicador de qual coordenada de v_1 deve ser trocada a fim de corrigir o erro e obter v. Esse processo, no entanto, não funciona de forma tão simples se há mais erros. Voltaremos a isso no exemplo 6.3.2.

6.2.3 Código de Hamming

Proposição 6.2.30 (Cota de Singleton)**.** *Os parâmetros $[n, k, d]_q$ de um código linear $\mathcal{C}$ satisfazem a desigualdade*

$$d \leq n - k + 1.$$

Demonstração. Seja H uma matriz teste de paridade, então pela Proposição 6.2.27, H tem posto $n - k$ e pela Proposição 6.2.26, se a distância mínima de $\mathcal{C}$ é d, então quaisquer $d - 1$ colunas de H devem ser linearmente independentes e devem existir d colunas de H linearmente dependentes. Ainda, como posto$(H) = n - k$, existe pelo menos um grupo de $n - k$ colunas de H linearmente independentes e qualquer quantidade maior de colunas é linearmente dependente. Logo, podemos ter:

- $d-1 = n-k$, se quaisquer $n-k$ colunas de H forem linearmente independentes; ou
- $d-1 < n-k$ se existir um grupo de $n-k$ colunas de H linearmente dependentes.

Portanto, temos que $d-1 \leq n-k$, isto é, $d \leq n-k+1$, como queríamos. □

Note que de fato o código do mapa satisfaz a desigualdade acima, pois pelo exemplo 6.2.20 temos que seus parâmetros são $[6,2,4]_2$ e $d = 4 < 5 = 6-2+1 = n-k+1$.

Definição 6.2.31. *Um código será chamado de* ***MDS (Maximum Distance Separable)*** *se valer a igualdade na cota de Singleton, isto é, se* $d = n-k+1$.

Definição 6.2.32. *Um* ***código de Hamming*** *de ordem* m *sobre* $\mathbb{F}_2$ *é um código com matriz teste de paridade* H_m *de ordem* $m \times n$*, cujas colunas são os elementos de* $\mathbb{F}_2^m \setminus \{0\}$ *numa ordem qualquer.*

Temos que o comprimento de um código de Hamming de ordem m é $n = 2^m - 1$, e portanto, sua dimensão é $k = n - m = 2^m - m - 1$. Podemos verificar facilmente que $d = 3$, pois em H_m é fácil achar três colunas linearmente dependentes.

Exemplo 6.2.33. *Como exemplo numérico, consideremos a matriz*

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Essa é a matriz teste de paridade de um código de Hamming em que $m = 3$.

Proposição 6.2.34. *Todo código de Hamming é perfeito.*

Demonstração. No nosso caso, como $d = 3$, então $\kappa = \left[\frac{d-1}{2}\right] = 1$. Seja x em $\mathbb{F}_2^n$, temos que

$$|D(x,1)| = 1 + n.$$

Logo,

$$|\bigcup_{x \in \mathcal{C}} D(x,1)| = [1+n]2^k = [1+2^m-1]2^{n-m} = 2^n,$$

e consequentemente,

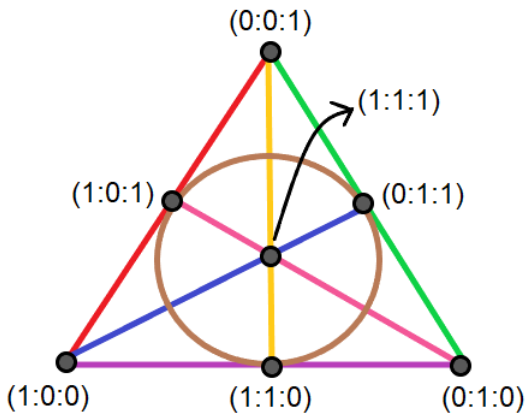
$$\bigcup_{x \in \mathcal{C}} D(x,1) = \mathbb{F}_2^n.$$

□

6.3 CÓDIGO DE FANO

Nessa seção, vamos estudar um código linear perfeito construído a partir do plano de Fano apresentado na seção 2.2. Para isso, vamos dar coordenadas para os pontos, como na figura 37, com coordenadas sobre $\mathbb{F}_2 = \{0,1\}$.

Figura 37 – O plano de Fano com coordenadas.



Fonte: Elaborada pela autora (2023).

Listando os pontos, produzimos uma matriz H com 3 linhas e 7 colunas que será a matriz teste de paridade do código de Fano. Por conveniência, escrevemos a matriz em sua forma padrão $H = (-A^t|Id_3)$ e temos

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Note que essa matriz é igual a do exemplo 6.2.33, ou seja, o código de Fano é um código de Hamming de ordem 3 e, então, é um código linear perfeito.

A partir da matriz H podemos determinar a matriz $G = (Id_4|A)$ geradora do código de Fano, pois temos

$$\begin{aligned} -A^t &= \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \\ -(-A^t) &= A^t \\ &= \begin{pmatrix} -1 & -1 & 0 & -1 \\ -1 & 0 & -1 & -1 \\ 0 & -1 & -1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \end{aligned}$$

uma vez que $-1 \equiv 1$ em $\mathbb{F}_2$, e também

$$\begin{aligned}(A^t)^t &= A \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.\end{aligned}$$

Então,

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Definição 6.3.1. *O código de Fano sobre $\mathbb{F}_2$ é o código gerado por G.*

Como o código de Fano é um código de Hamming de ordem 3, temos que seu comprimento é $2^3 - 1 = 7$, sua dimensão é $2^3 - 3 - 1 = 4$ e sua distância mínima é 3.

Exemplo 6.3.2. *Certo questionário de 4 perguntas só aceita respostas sim ou não, atribuindo às respostas 1 e 0, respectivamente. O conjunto de respostas é, então, organizado como um vetor, por exemplo $u = (1, 1, 0, 0)$ e, em seguida, codificado usando o código de Fano. A palavra*

$$v = uG = \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

obtida é então transmitida para um banco de dados. Veja que, como G está na forma $(Id_4|A)$, a codificação consiste apenas em acrescentar entradas no fim do vetor u, isto é, $v = (u|uA)$. Essas são as chamadas redundâncias. A princípio, a decodificação poderia ser apenas tomar as 4 primeiras coordenadas, ignorando as redundâncias. O problema é se tiver ocorrido algum erro.

Caso, por exemplo, a palavra recebida seja $v_1 = (1, 0, 0, 0, 0, 1, 1)$, calculamos

$$v_1 H^t = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}.$$

Perceba que não obtemos o vetor nulo, isso significa que houve erro. Nesse caso, o vetor obtido de v_1H^t nos diz exatamente a entrada de v_1 com erro. Neste caso, v_1H^t é exatamente a segunda linha de H^t, que corresponde à segunda coluna de H, logo, o erro está na segunda coordenada de v_1, e portanto, corrigimos o erro, obtendo a mensagem correta $(1,1,0,0,0,1,1)$, e podemos decodificar ignorando as 3 últimas coordenadas.

Como a distância mínima do código de Fano é 3, pelo Teorema 6.2.13, seria possível ainda detectar mais um erro, mas não seria possível corrigir dois erros. Por exemplo, se a palavra recebida fosse $v_2 = (0,1,1,0,0,1,1)$, calculamos

$$v_2H^t = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}.$$

Novamente, como o produto não foi o vetor nulo, temos erro. E ainda, obtemos um novo vetor $v_3 = (0,0,1,0,0,1,1)$ com a correção. Note que se fizermos v_3H^t obtemos o vetor nulo, o que indicaria que v_3 não possui erros, entretanto, se ignorarmos as três últimas coordenadas para decodificar obtemos $u_1 = (0,0,1,0)$. Ou seja, não obtemos o vetor correto que é o vetor $u = (1,1,0,0)$ inicial. Isso ocorre porque esse código não corrige 2 erros.

Por fim, veja que se o vetor recebido for $v_4 = (1,1,1,1,1,1,1)$, temos

$$v_4H^t = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix},$$

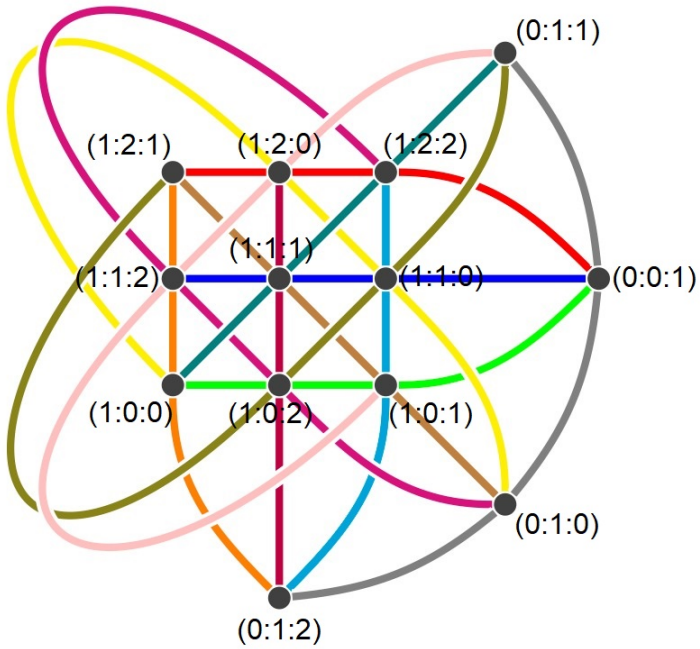
o que nos faria imaginar que não houve erro na transmissão de v. Ou seja, há vetores com 3 erros que podem ser identificados como mensagens corretas. Novamente, isso ocorre porque esse código não tem capacidade de identificar 3 erros.

De qualquer modo, utilizar a codificação em vez de apenas transmitir o vetor u original é mais vantajoso já que alguns casos poderiam ser corrigidos e, sem codificação, não teríamos nem como desconfiar de haver ou não erro.

6.4 CÓDIGO JOGO DA VELHA

O plano jogo da velha (veja seção 2.2) tem 13 pontos e 13 retas. Vamos considerá-lo com coordenadas sobre $\mathbb{F}_3 = \{0, 1, 2\}$.

Figura 38 – O plano jogo da velha com coordenadas.



Fonte: Elaborada pela autora (2023).

Listando os pontos como no código de Fano, produzimos uma matriz H com 3 linhas e 13 colunas que será a matriz teste de paridade do código Jogo da Velha. Por conveniência, escrevemos a matriz em sua forma padrão $H = (-A^t|Id_3)$ e temos

$$H = \begin{pmatrix} 1\,1\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0 \\ 1\,0\,1\,2\,0\,1\,1\,1\,2\,2\,0\,1\,0 \\ 0\,1\,1\,0\,2\,2\,1\,2\,1\,2\,0\,0\,1 \end{pmatrix}.$$

A partir da matriz H podemos determinar a matriz $G = (Id_{10}|A)$ geradora do

código Jogo da Velha, pois temos

$$
\begin{aligned}
-A^t &= \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 0 & 1 & 1 & 1 & 2 & 2 \\ 0 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 1 & 2 \end{pmatrix} \\
-(-A^t) &= A^t \\
&= \begin{pmatrix} -1 & -1 & 0 & -1 & -1 & 0 & -1 & -1 & -1 & -1 \\ -1 & 0 & -1 & -2 & 0 & -1 & -1 & -1 & -2 & -2 \\ 0 & -1 & -1 & 0 & -2 & -2 & -1 & -2 & -1 & -2 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 1 & 0 & 2 & 2 & 2 & 1 & 1 \\ 0 & 2 & 2 & 0 & 1 & 1 & 2 & 1 & 2 & 1 \end{pmatrix},
\end{aligned}
$$

uma vez que $-1 \equiv 2$ e $-2 \equiv 1$ em $\mathbb{F}_3$, e também

$$
\begin{aligned}
(A^t)^t &= A \\
&= \begin{pmatrix} 2 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 2 \\ 2 & 1 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \\ 2 & 1 & 1 \end{pmatrix}.
\end{aligned}
$$

Então,

$$
G = \begin{pmatrix}
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,2\,2\,0 \\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,2\,0\,2 \\
0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,2\,2 \\
0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,2\,1\,0 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,2\,0\,1 \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,2\,1 \\
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,2\,2\,2 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,2\,2\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,2\,1\,2 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,2\,1\,1
\end{pmatrix}.
$$

Definição 6.4.1. *O código Jogo da Velha é o código gerado por G.*

Exemplo 6.4.2. *Uma prova de múltipla escolha com 10 questões só aceita respostas a), b) ou c), atribuindo às respostas 0, 1 e 2, respectivamente. Assim, o conjunto de respostas*

é organizado como um vetor, por exemplo, $u = (1,1,0,1,2,0,0,2,2,1)$ *e, em seguida, codificado usando o código Jogo da Velha. A palavra*

$$v = uG = \begin{pmatrix} 1\,1\,0\,1\,2\,0\,0\,2\,2\,1 \end{pmatrix} \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,2\,2\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,2\,0\,2 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,2\,2 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,2\,1\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,2\,0\,1 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,2\,1 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,2\,2\,2 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,2\,2\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,2\,1\,2 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,2\,1\,1 \end{pmatrix} = \begin{pmatrix} 1\,1\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix}$$

obtida é então transmitida para um banco de dados. Observe que, como G *está na forma padrão, a codificação também consiste apenas em acrescentar redundâncias no fim do vetor* u*, ou seja,* $v = (u|uA)$*, assim como acontece no código de Fano.*

Por exemplo, se a palavra recebida fosse $v_1 = \begin{pmatrix} 1\,2\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix}$*, calculamos*

$$v_1 H^t = \begin{pmatrix} 1\,2\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix} \begin{pmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \\ 1\,2\,0 \\ 1\,0\,2 \\ 0\,1\,2 \\ 1\,1\,1 \\ 1\,1\,2 \\ 1\,2\,1 \\ 1\,2\,2 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{pmatrix} = \begin{pmatrix} 1\,0\,1 \end{pmatrix}.$$

Note que não obtemos o vetor nulo, então houve erro. O vetor obtido $v_1 H^t$ *é exatamente a segunda linha de* H^t*, que corresponde à segunda coluna de* H*, logo, o erro está na segunda coordenada de* v_1*. Agora, como estamos em* $\mathbb{F}_3$ *temos 2 possibilidades de correção, assim, iremos testar cada uma e fazer o produto do novo vetor com* H^t*. O produto que resultar no vetor nulo será aquele em que a correção foi feita corretamente. Temos*

$$v_2 = \begin{pmatrix} 1\,0\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix}, v_3 = \begin{pmatrix} 1\,1\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix}$$

$$v_2H^t = \begin{pmatrix} 1\,0\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix} \begin{pmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \\ 1\,2\,0 \\ 1\,0\,2 \\ 0\,1\,2 \\ 1\,1\,1 \\ 1\,1\,2 \\ 1\,2\,1 \\ 1\,2\,2 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{pmatrix} = \begin{pmatrix} 2\,0\,2 \end{pmatrix}$$

$$v_3H^t = \begin{pmatrix} 1\,1\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix} \begin{pmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \\ 1\,2\,0 \\ 1\,0\,2 \\ 0\,1\,2 \\ 1\,1\,1 \\ 1\,1\,2 \\ 1\,2\,1 \\ 1\,2\,2 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,0\,0 \end{pmatrix}.$$

Portanto, a correção certa foi feita em $v_3 = \begin{pmatrix} 1\,1\,0\,1\,2\,0\,0\,2\,2\,1\,2\,1\,2 \end{pmatrix}$*, e ao ignorarmos as três últimas entradas para decodificar, de fato obtemos a palavra correta inicial* $u = (1, 1, 0, 1, 2, 0, 0, 2, 2, 1)$.

7 CONCLUSÃO

No presente trabalho, através da noção de plano projetivo finito e da construção de corpos finitos, pudemos explorar diferentes áreas da matemática, destacando a surpreendente equivalência entre assuntos que, à primeira vista, parecem completamente distintos. Compreendemos, assim, que a matemática não é formada por áreas de estudo isoladas, já que os assuntos se intersectam e resultados colaboram. Notamos ainda que foram abordados temas clássicos, como o estudo de designs, bem como temas mais modernos, como grafos e códigos corretores de erros, que estão em plena expansão. Sendo assim, há ainda espaço para mais pesquisa na área, o que pretendemos fazer no mestrado.

REFERÊNCIAS

1 BOSE, R. C. On the application of the properties of Galois fields to the problem of constrution of hyper-graeco-latin squares. **Sankhyā: The Indian Journal of Statistics**, v. 3, n. 4, p. 323-338, 1938.

2 BROWN, E. The Many Names of (7, 3, 1). **Mathematics Magazine**, v. 75, n. 2, p. 83-94, 2002.

3 BRUCK, R. H.; RYSER, H. J. The Nonexistence of Certain Finite Projective Planes. **Canadian Journal of Mathematics**, v. 1, n. 1, p. 88-93, 1949.

4 HEFEZ, Abramo; VILELA, Maria Lúcia T. **Códigos Corretores de Erros**. Coleção Matemática e Aplicações. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2017.

5 LAM, C. W. H. The Search for a Finite Projective Plane of Order 10. **The American Mathematical Monthly**, v. 98, n. 4, p. 305-318, 1991.

6 LEONARD, Katie. **The Friendship Theorem and Projective Planes**. 2005. Dissertação (Mestrado em Matemática) - Portland State University, Portland, 2005.

7 LOVÁSZ, László; PELIKÁN, József; VESZTERGOMBI, Katalin. **Matemática Discreta: Elementar e Além**. Coleção Textos Universitários. Sociedade Brasileira de Matemática, 2005.

8 MACIEL, Milena Arantes Rocha. **A Geometria Projetiva do jogo Dobble**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Ciências Exatas) - Instituto de Ciências Exatas, Universidade Federal de Juiz de Fora, Juiz de Fora, 2022.

9 MACIEL, Milena Arantes Rocha; RIBEIRO, Beatriz Casulari da Motta. **A Geometria Projetiva do jogo Dobble**. 2022. Pôster, 27ª Semana da Matemática - Departamento de Matemática, Universidade Federal de Juiz de Fora, Juiz de Fora, 2022.

10 MACIEL, Milena Arantes Rocha; RIBEIRO, Beatriz Casulari da Motta. **A Geometria Projetiva do jogo Dobble**. 2022. Comunicação Oral, VII Workshop de Matemática e Matemática Aplicada - Universidade Federal de São João del-Rei, Evento Online, 2022.

11 MACIEL, Milena Arantes Rocha; RIBEIRO, Beatriz Casulari da Motta. **O Plano Projetivo Finito e suas aplicações**. 2023. Pôster, 34º Colóquio Brasileiro de Matemática - Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2023.

12 MACIEL, Milena Arantes Rocha; RIBEIRO, Beatriz Casulari da Motta. **O Plano Projetivo Finito e suas aplicações**. 2023. Pôster, II Reunião Mineira de Matemática - Instituto de Ciências Exatas, Universidade Federal de Minas Gerais, Belo Horizonte, 2023.

13 MACIEL, Milena Arantes Rocha; RIBEIRO, Beatriz Casulari da Motta. **A relação entre Quadrados Latinos e Planos Projetivos Finitos**. 2023. Comunicação Oral, 28ª Semana da Matemática - Departamento de Matemática, Universidade Federal de Juiz de Fora, Juiz de Fora, 2023.

14 TARRY, G. Le problème des 36 officiers. **Compte Rendu de la Association Française pour l'Avancement des Sciences**, v. 29, p. 122-123., 1900.

15 VEBLEN, O. A system of axioms for geometry. **Transactions of the American Mathematical Society**, v. 5, p. 343-384, 1904.

16 VEBLEN, O.; BUSSEY, W. H. Finite projective geometries. **Transactions of the American Mathematical Society**, v. 7, p. 241-259, 1906.

17 VEBLEN, O.; MACLAGAN-WEDDERBURN, J. H. Non-Desarguesian and non-Pascalian geometries. **Transactions of the American Mathematical Society**, V. 8, p. 379-388, 1907.

18 WILF, H. S. The friendship theorem. **Combinatorial Mathematics and its Applications (Proc. Conf., Oxford, 1969)**, p. 307-309, 1971.