O Plano Projetivo Finito e suas aplicações

Milena Maciel & Beatriz Ribeiro

Universidade Federal de Juiz de Fora
Departamento de Matemática

milena.arantes@ice.ufjf.br & betriz@ice.ufjf.br

Resumo

O plano projetivo finito é um objeto geométrico definido de diversas formas equivalentes. Neste trabalho, começamos com uma definição axiomática e exploramos aplicações diversas: um jogo não-matemático, grafos, designs e códigos.

1 Plano projetivo finito

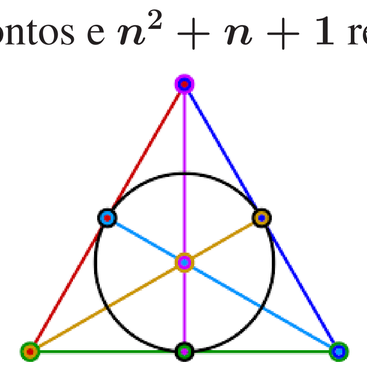
Definição. *Um plano projetivo finito é um conjunto finito V cujos elementos são chamados pontos e alguns subconjuntos são chamados retas de forma que:*

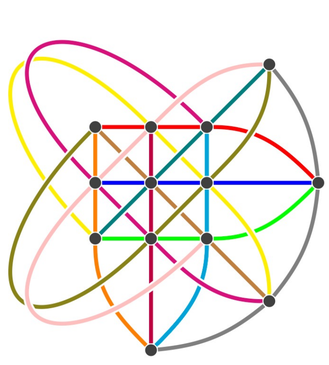
1) Duas retas distintas se encontram em um único ponto;

2) Dois pontos distintos definem uma única reta;

3) Existem pelo menos 4 pontos dos quais não há 3 colineares.

Em um plano projetivo finito, toda reta contém a mesma quantidade de pontos e todo ponto está na mesma quantidade de retas. Um plano projetivo que contém $n+1$ pontos em cada reta é dito de ordem n e tem exatamente n^2+n+1 pontos e n^2+n+1 retas.





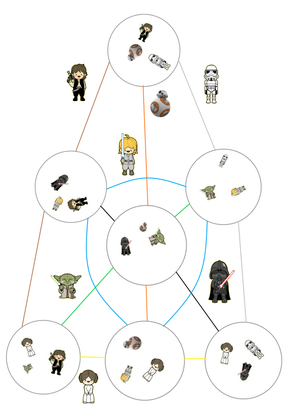
Fixado um corpo finito $\mathbb{F}_q$, o plano projetivo $PG(2,q)$ é a geometria cujos subespaços de dimensão 0 e 1 são os subespaços de dimensão 1 e 2 de $\mathbb{F}_q^3$.
Dados $X, Y \in \mathbb{F}_q^3 \setminus \{0\}$, consideremos a relação:

$$X \sim Y \iff X = \lambda Y \text{ para algum } \lambda \in \mathbb{F}_q^* .$$

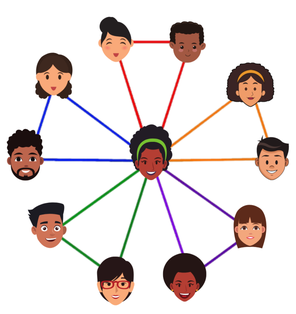
Assim, $PG(2,q)$ é o conjunto das classes de equivalência.

2 O jogo *Dobble*

Dobble é um jogo não-matemático que contém 55 cartas e 57 símbolos, sendo 8 símbolos em cada carta de modo que 2 cartas têm exatamente 1 símbolo em comum. A ideia do jogo é ser o mais rápido a achar o símbolo em comum entre 2 cartas quaisquer. Podemos associar o *Dobble* a um plano projetivo de ordem 7 substituindo, na definição, "ponto" por "carta" e "reta" por "símbolo". Nesse caso, o jogo deveria contar com 57 e não 55 cartas. Assim, embora não seja de fato um plano projetivo, é a estrutura de plano projetivo que faz com que o *Dobble* funcione.



3 Teorema da Amizade



Teorema 1. *(versão ingênua) Se em uma festa com n pessoas cada par de pessoas tem exatamente um amigo em comum, então existe uma pessoa que conhece todas as outras.*

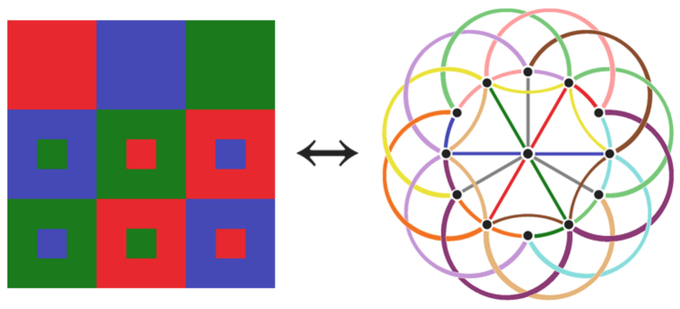
Teorema 2. *Se G é um grafo em que quaisquer dois vértices distintos têm exatamente um vizinho comum, então G tem um vértice que une todos os outros vértices.*

Há muitas demonstrações conhecidas desse teorema, mas nosso interesse está na de Wilf [4]. Sua prova começa assumindo que a conclusão do teorema é falsa e, então, construindo um plano projetivo a partir da "festa", onde pessoas são pontos e a relação "conhecer" representa uma reta, o argumento chega em uma contradição com relação à matriz de incidência do plano projetivo (uma representação matricial de quais pontos estão em quais retas).

4 Quadrados Greco-Latinos

Um quadrado latino é uma tabela $n \times n$ preenchida com $1, \ldots, n$ dispostos cada um n vezes de forma que cada número ocorre exatamente uma vez em cada linha e cada coluna. Para criar um quadrado greco-latino, adicionamos uma "segunda dimensão", sobrepondo um quadrado com outros símbolos sobre um quadrado latino. Os dois quadrados devem ser mutuamente ortogonais, o que significa que cada par número-símbolo ocorre apenas uma vez.

Teorema 3. *Um conjunto completo de quadrados greco-latinos de ordem $n \geq 3$ existe se, e somente se, existe um plano projetivo finito de ordem n.*



Cada cor, em cada "dimensão", aparece uma vez em cada linha e uma vez em cada coluna, e o par de cores internas e externas em cada um dos 9 quadrados é único. À direita, um plano projetivo finito de ordem 3 tem 13 pontos e 13 retas. Cada reta tem 4 pontos e cada ponto está em 4 retas. Os diagramas parecem diferentes, mas um pode ser construído a partir do outro.

5 Códigos corretores de erros

Seja G a matriz geradora de um $[n,k,d]_q-$código C linear e seja S o (multi-)conjunto formado pelas colunas de G. Temos que S é um (multi-)conjunto de n vetores de $PG(k-1,q)$ tal que todo hiperplano de $PG(k-1,q)$ contém no máximo $n-d$ vetores de S e algum hiperplano de $PG(k-1,q)$ contém exatamente $n-d$ vetores de S.

Exemplo. *Sejam $F(X,Y,Z)$ um polinômio homogêneo irredutível sobre $\mathbb{F}_q$ de grau m e a curva*

$$V(F) = \{(x:y:z) \in PG(2,q)\,;\, F(x,y,z) = 0\}\,.$$

Como F é irredutível, cada reta de $PG(2,q)$ intercepta $V(F)$ em no máximo m pontos. A matriz cujas colunas são os vetores de $V(F)$ é uma matriz $3 \times \#V(F)$ que gera um código de distância mínima pelo menos $n - deg(F)$.

Referências

[1] BALL, S., **A Course in Algebraic Error-Correcting Codes**. Suiça: Springer, 2020.

[2] HEFEZ, A,; VILELA, M.L.T. **Códigos Corretores de Erros**. Coleção Matemática e Aplicações. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2017.

[3] LOVÁSZ, L., PELIKÁN, J., VESZTERGOMBI, K. **Matemática Discreta**. Sociedade Brasileira de Matemática, Rio de Janeiro: 2005.

[4] WILF, H. **The Friendship Theorem**. Combinatorial Mathematics and Its Applications, New York; Academic Press, 1971.

Agradecimentos

Agradeço o apoio da FAPEMIG, do IMPA e da UFJF.