



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

DEPARTAMENTO DE MATEMÁTICA

Torneios de Paley

Ícaro Souza Silva Lins

Orientador: Prof. Me. Wanderson Aleksander da Silva Oliveira

RECIFE

2026



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

DEPARTAMENTO DE MATEMÁTICA

Ícaro Souza Silva Lins

Torneios de Paley

Trabalho apresentado ao Programa de Licenciatura em Matemática do Departamento de Matemática da Universidade Federal Rural De Pernambuco - UFRPE, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Orientador: Prof. Me. Wanderson Aleksander da Silva
Oliveira

RECIFE

2026

Ícaro Souza Silva Lins Torneios de Paley/ Ícaro Souza Silva Lins. – Recife,
2026- 32 p. : il.(alguma color.); 30 cm.

Orientador:Prof. Me. Wanderson Aleksander da Silva Oliveira

Monografia – Universidade Federal Rural de Pernambuco

Departamento de MATEMÁTICA, 2026.

1. Torneios de Paley. 2. Grafos. 3. Corpos finitos. 4. Resíduos quadráticos.

I. Wanderson Aleksander da Silva Oliveira. II. Universidade Federal Rural de
Pernambuco. III. Licenciatura em Matemática. IV. Torneios de Paley

CDU 02:141:005.7

Ícaro Souza Silva Lins

Torneios de Paley

Trabalho apresentado ao Programa de Licenciatura em Matemática do Departamento de Matemática da Universidade Federal Rural De Pernambuco - UFRPE, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Trabalho aprovado. Recife, 20 de fevereiro de 2026:

**Prof. Me. Wanderson Aleksander da
Silva Oliveira**

Orientador - Universidade Federal Rural de
Pernambuco

Profa. Ma. Itacira Ataíde Silva
Universidade de Pernambuco

Prof. Dr. Filipe Andrade da Costa
Universidade Federal Rural de Pernambuco

Recife
2026

Dedico este trabalho à minha mãe e a todos os meus amigos que acreditaram em meu potencial.

Agradecimentos

Não podia deixar de agradecer, primeiramente, a Deus, que tornou tudo isso possível. Ele foi meu refúgio nos momentos de desespero, minha força nos momentos de fraqueza e meu maior incentivador.

Agradeço à minha mãe Maria de Jesus, que, desde que chegou em Olinda, não viveu com outro objetivo a não ser dar o melhor para que seus filhos pudessem ter. Por sua força e garra em ser uma mãe que protege, cuida e faz questão de mostrar que está sempre ali. Porque ela não mediu esforços quando o assunto era dar educação de qualidade para seus filhos e derramou suor todos os dias para que a gente pudesse alcançar os nossos sonhos.

Agradeço à minha irmã Íneg Cecília, que sempre se destacou muito nos estudos e serviu como exemplo para mim, sendo, desde que eu era pequeno, uma das minhas referências para os estudos!

Agradeço à minha ex-chefe, amiga e mãe, nas horas vagas, Micheline, que sempre foi tão cuidadosa comigo, dona de grandes conselhos, uma das minhas maiores incentivadoras para terminar meu curso e que ajudou em tudo o que pôde. Sem ela, tudo seria mais difícil.

Agradeço aos meus amigos de graduação, em especial, Alessandra, Allan, Ana Cristina, Dayza, Elaine, Fernando, Henrique, Leonardo, Thalia, Victória, Vitória e Yuri, que tornaram o processo muito mais prazeroso, que me davam ânimo para continuar e que acreditaram em mim mesmo quando nem eu acreditava. Vocês foram um presente de Deus em minha vida, e eu sempre vou lembrar com carinho de todos vocês!

Agradeço ao meu orientador Wanderson por ter sido um grande motivador para a conclusão do meu curso. Apesar de ter acompanhado apenas o final da minha graduação, sua orientação teve grande significado e serviu como inspiração para que eu seguisse essa carreira tão nobre. Agradeço, ainda, por ter me acolhido em um momento tão necessário.

Por fim, agradeço à professora Anna Paula, que apareceu em minha jornada acadêmica no meu segundo período, com grande impacto em minha vida não só profissional, mas pessoal, e que, com suas palavras tão acolhedoras, conseguiu me mostrar locais seguros

que eu poderia alcançar.

Não que eu tenha alcançado ou esteja perfeito, mas algo eu faço, esqueço aquilo que para trás ficou e avanço para o que está diante de mim.
Efésios 3:12-14

Resumo

O presente trabalho tem como objetivo estudar a estrutura algébrica e as propriedades combinatórias dos Torneios de Paley, uma classe específica de grafos orientados definidos sobre corpos finitos. Inicialmente, são estabelecidos os conceitos preliminares fundamentais, partindo das estruturas de anéis comutativos até a definição formal e classificação dos corpos finitos de ordem $q = p^n$. O estudo aborda a caracterização aritmética dos resíduos quadráticos (quadrados perfeitos), distinguindo o comportamento em corpos de característica 2 e de característica ímpar. A partir dessa base, define-se a família geral dos Grafos de Paley, diferenciando o caso não direcionado ($q \equiv 1 \pmod{4}$) do caso direcionado. O foco central recai sobre os Torneios de Paley, que ocorrem quando a ordem do corpo satisfaz a congruência $q \equiv 3 \pmod{4}$. Por fim, é apresentada a construção detalhada e a representação visual do Torneio de Paley de ordem 7 (P_7), ilustrando a propriedade de antissimetria garantida pelo fato de -1 não ser um resíduo quadrático nesses corpos.

Palavras-chaves: Torneios de Paley. Corpos Finitos. Grafos Dirigidos. Resíduos Quadráticos.

Abstract

This work aims to study the algebraic structure and combinatorial properties of Paley Tournaments, a specific class of oriented graphs defined over finite fields. Initially, fundamental preliminary concepts are established, starting from commutative ring structures to the formal definition and classification of finite fields of order $q = p^n$. The study addresses the arithmetic characterization of quadratic residues (perfect squares), distinguishing the behavior in fields of characteristic 2 and odd characteristic. Based on this foundation, the general family of Paley Graphs is defined, differentiating the undirected case ($q \equiv 1 \pmod{4}$) from the oriented case. The central focus lies on Paley Tournaments, which occur when the order of the field satisfies the congruence $q \equiv 3 \pmod{4}$. Finally, the detailed construction and visual representation of the Paley Tournament of order 7 (P_7) is presented, illustrating the antisymmetry property guaranteed by the fact that -1 is not a quadratic residue in these fields.

Keywords: Paley Tournaments. Finite Fields. Oriented Graphs. Quadratic Residues.

Lista de ilustrações

Figura 1 – Representação do grafo não orientado G	23
Figura 2 – Representação do grafo orientado D	23
Figura 3 – Grafo de Paley $P(5)$, isomorfo ao ciclo C_5	26
Figura 4 – Grafo do Torneio de Paley P_3	28
Figura 5 – Grafo do Torneio de Paley P_7	29
Figura 6 – Grafo do Torneio de Paley P_{11}	30

Sumário

1	INTRODUÇÃO	19
2	CONCEITOS PRELIMINARES	21
2.1	Estruturas Algébricas: De Anéis a Corpos Finitos	21
2.1.1	Definição de Corpo	21
2.1.2	Corpos Finitos	22
2.2	Grafos	22
2.3	Quadrados perfeitos	23
2.3.1	Caso 1: Corpos de ordem $q = 2^n$	24
2.3.2	Caso 2: Corpos de ordem $q = p^n$ (com p primo ímpar)	24
2.4	Grafo de Paley	25
3	TORNEIOS DE PALEY	27
3.1	Torneios de Paley	27
3.1.1	Exemplos de Construção	28
4	CONSIDERAÇÕES FINAIS	31
	REFERÊNCIAS	32

1 Introdução

A interação entre a Álgebra e a Combinatória tem se mostrado uma das áreas mais frutíferas da matemática moderna, permitindo a construção de estruturas discretas com propriedades altamente simétricas e regulares. Dentro da Teoria Algébrica dos Grafos, uma classe que se destaca é a dos Grafos de Paley, definidos a partir de operações aritméticas em corpos finitos.

Estes grafos, introduzidos por Raymond Paley em 1933, são construídos conectando-se vértices com base no caráter quadrático de suas diferenças, ou seja, se a diferença entre dois elementos do corpo é ou não um quadrado perfeito. Dependendo da ordem do corpo finito escolhido, essa construção pode resultar em grafos não orientados ou em grafos orientados.

O presente trabalho tem como foco o estudo da classe orientada, conhecida como Torneios de Paley. Essas estruturas emergem naturalmente quando a ordem do corpo finito, denotada por q , satisfaz a congruência $q \equiv 3 \pmod{4}$. Sob essa condição, a assimetria na distribuição dos resíduos quadráticos garante que, para qualquer par de vértices distintos, exista exatamente uma aresta orientada entre eles, caracterizando um torneio.

O objetivo geral desta monografia é apresentar a construção algébrica rigorosa necessária para a definição dos Torneios de Paley. Para isso, o trabalho está estruturado da seguinte forma:

No Capítulo 2, estabelecemos os conceitos preliminares. Iniciamos com uma revisão das estruturas algébricas fundamentais, partindo de anéis até a definição e classificação dos corpos finitos. Em seguida, abordamos as definições básicas de grafos e aprofundamos o estudo dos resíduos quadráticos (quadrados perfeitos), cuja compreensão é vital para a regra de adjacência dos grafos de Paley.

No Capítulo 3, definimos formalmente os Torneios de Paley. Discutimos a condição necessária sobre a ordem do corpo ($q \equiv 3 \pmod{4}$) e como ela implica a propriedade de antissimetria do grafo. Apresentamos também um exemplo prático de construção sobre o corpo $\mathbb{F}_7$, ilustrando visualmente as propriedades discutidas.

Por fim, no Capítulo 4, apresentamos as considerações finais, sintetizando os resultados obtidos e a importância da conexão entre a teoria dos números e a teoria dos grafos.

2 Conceitos Preliminares

Neste capítulo, apresentaremos os fundamentos matemáticos essenciais para a compreensão dos Torneios de Paley. Inicialmente, revisaremos as estruturas algébricas de anéis e corpos, com foco especial na classificação e aritmética dos corpos finitos. Em seguida, introduziremos a terminologia básica da Teoria dos Grafos, destacando as propriedades dos grafos orientados. Por fim, exploraremos o conceito de resíduos quadráticos, cuja distribuição aritmética em corpos finitos será a chave para definir as arestas dos torneios que estudaremos posteriormente.

2.1 Estruturas Algébricas: De Anéis a Corpos Finitos

Para definirmos formalmente o conceito de corpos finitos, primeiramente estabelecemos a estrutura de anel e, em seguida, restringimos essa definição para o caso em que a divisão é sempre possível (corpo).

2.1.1 Definição de Corpo

A construção de um corpo pode ser entendida como uma evolução da estrutura de anel comutativo com unidade.

Definição 2.1.1. Seja A um conjunto não vazio equipado com duas operações binárias: adição $(+)$ e multiplicação $(\cdot)$. Dizemos que $(A, +, \cdot)$ é um **anel comutativo com unidade** se satisfaz as seguintes condições:

1. $(A, +)$ é um grupo abeliano (associativo, comutativo, possui elemento neutro 0 e inverso aditivo);
2. A multiplicação é associativa e distributiva em relação à adição;
3. A multiplicação é comutativa $(a \cdot b = b \cdot a)$;
4. Existe um elemento neutro multiplicativo 1 (onde $1 \neq 0$).

A partir dessa base, podemos definir um corpo exigindo apenas uma propriedade adicional: a existência de inversos multiplicativos para todos os elementos não nulos.

Definição 2.1.2. Um corpo $\mathbb{F}$ é um anel comutativo com unidade no qual todo elemento diferente de zero possui um inverso multiplicativo. Ou seja, para todo $a \in \mathbb{F}$ tal que $a \neq 0$, existe um elemento $a^{-1} \in \mathbb{F}$ tal que:

$$a \cdot a^{-1} = 1$$

Dessa forma, em um corpo, as quatro operações básicas (soma, subtração, multiplicação e divisão por não-nulo) estão bem definidas.

2.1.2 Corpos Finitos

Com a estrutura de corpo definida, a distinção para corpos finitos se dá pela cardinalidade do conjunto.

Definição 2.1.3. Diz-se que um corpo $\mathbb{F}$ é um corpo finito se o conjunto $\mathbb{F}$ possui um número finito de elementos. A quantidade de elementos é chamada de ordem do corpo.

A existência e a unicidade dos corpos finitos são regidas pelo teorema de classificação a seguir:

Teorema 2.1.1. Seja $\mathbb{F}$ um corpo finito. Então:

- A ordem de $\mathbb{F}$ é necessariamente uma potência de um número primo. Isto é, $|\mathbb{F}| = q = p^n$, onde p é um número primo (chamado de característica do corpo) e n é um inteiro positivo.
- Para cada potência de primo $q = p^n$, existe, a menos de isomorfismo, um único corpo finito com q elementos.

Denotamos o corpo finito com q elementos por $\mathbb{F}_q$. Quando $n = 1$, temos os chamados **corpos primos** ($\mathbb{F}_p \cong \mathbb{Z}_p$), onde as operações são realizadas módulo p .

2.2 Grafos

Definição 2.2.1. Um grafo G é um par ordenado (V, E) , onde:

- V é um conjunto não vazio de elementos denominados vértices (ou nós);
- E é um conjunto de elementos denominados arestas.

A cada aresta $e \in E$ estão associados um ou dois vértices distintos de V , chamados de **extremidades**. Diz-se que a aresta conecta suas extremidades.

Em particular, para um **grafo simples** (sem laços ou arestas múltiplas), o conjunto E é composto por pares não ordenados de vértices distintos. Matematicamente: $E \subseteq \{\{u, v\} \mid u, v \in V \text{ e } u \neq v\}$.

Exemplo 2.2.1. Considere o grafo simples $G = (V, E)$, definido pelos seguintes conjuntos de vértices e arestas: $V = \{v_1, v_2, v_3, v_4\}$ e $E = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_1\}, \{v_1, v_3\}\}$

A representação visual deste grafo G é apresentada na Figura 1 abaixo.

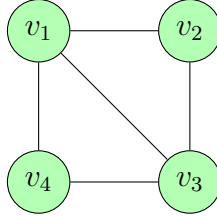


Figura 1 – Representação do grafo não orientado G

Definição 2.2.2. Um grafo orientado D é um par ordenado (V, E) , constituído por:

- V é um conjunto não vazio de vértices;
- E é um conjunto de arestas orientadas (ou arcos).

Cada aresta orientada está associada a um par ordenado de vértices $(u, v) \in V \times V$. Nesta relação, diz-se que a aresta tem origem em u e término em v .

Exemplo 2.2.2. Considere o grafo orientado $D = (V, E)$, onde o conjunto de vértices é $V = \{1, 2, 3\}$ e o conjunto de arestas orientadas é definido por $E = \{(1, 2), (2, 3), (3, 1), (2, 2)\}$

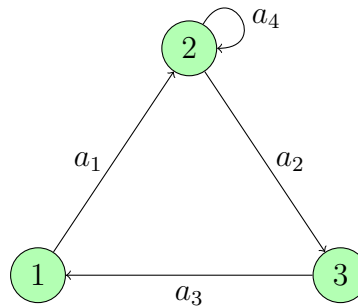


Figura 2 – Representação do grafo orientado D

2.3 Quadrados perfeitos

Para a construção dos Grafos de Paley, é fundamental compreender a estrutura aritmética dos elementos que possuem raiz quadrada no corpo. Iniciamos com a definição geral para anéis.

Definição 2.3.1. Seja A um anel comutativo. Diz-se que um elemento $\alpha \in A$ é um *quadrado perfeito* se existir algum $x \in A$ tal que $x^2 = \alpha$. O conjunto de todos os quadrados perfeitos de A é denotado por $\square_A$.

No contexto de corpos finitos $\mathbb{F}_q$, a notação é simplificada para $\square_q$. A análise deste conjunto depende intrinsecamente da característica do corpo, dividindo-se em dois casos distintos.

2.3.1 Caso 1: Corpos de ordem $q = 2^n$

Neste caso, o corpo possui característica 2, o que implica que $1 = -1$ em $\mathbb{F}_{2^n}$. Esta propriedade simplifica a análise da função quadrática.

Proposição 2.3.1. Para todo $n \in \mathbb{N}$, tem-se que $\mathbb{F}_{2^n} = \square_{2^n}$. Ou seja, todo elemento do corpo é um quadrado perfeito.

Demonstração. Considere a aplicação $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ definida por $f(x) = x^2$. Sabe-se que $x^2 = y^2$ implica $x^2 - y^2 = 0$. Em característica 2, isso equivale a $(x - y)^2 = 0$, o que implica $x = y$. Portanto, a função é injetora. Como o domínio e o contradomínio são finitos e possuem a mesma cardinalidade, a função é também sobrejetora. Logo, todo elemento de $\mathbb{F}_{2^n}$ é imagem de algum elemento ao quadrado. $\square$

2.3.2 Caso 2: Corpos de ordem $q = p^n$ (com p primo ímpar)

Diferentemente do caso anterior, quando p é ímpar, temos que $1 \neq -1$. Isso altera a caracterização dos quadrados perfeitos, propriedade essencial para a definição dos grafos de Paley.

Proposição 2.3.2. Seja $\mathbb{F}_q$ um corpo finito com q ímpar. O número de quadrados perfeitos não nulos em $\mathbb{F}_q$ é exatamente $\frac{q-1}{2}$.

Demonstração. Considere a equação $x^2 = \alpha$ para $\alpha \in \mathbb{F}_q^*$. Se x é uma solução, então $-x$ (o inverso aditivo de x) também o é, pois $(-x)^2 = (-1)^2 x^2 = x^2 = \alpha$. Como a característica do corpo é ímpar, $x \neq -x$ para todo $x \neq 0$. Assim, os elementos não nulos de $\mathbb{F}_q$ agrupam-se em pares $\{x, -x\}$ que resultam no mesmo quadrado. Consequentemente, a imagem da aplicação $x \mapsto x^2$ (restrita aos não nulos) possui cardinalidade:

$$|\square_q^*| = \frac{|\mathbb{F}_q^*|}{2} = \frac{q-1}{2}.$$

$\square$

Além da contagem, a estrutura algébrica deste conjunto é relevante. Os quadrados não nulos formam um subgrupo do grupo multiplicativo do corpo.

A característica do corpo determina se o elemento -1 comporta-se como um quadrado perfeito. Essa propriedade é fundamental para a natureza das arestas no Grafo de Paley e é regida pelo seguinte critério:

Lema 2.3.1 (Critério de Euler). Seja $\mathbb{F}_q$ um corpo finito de característica ímpar. Um elemento $a \in \mathbb{F}_q^*$ é um quadrado perfeito se, e somente se,

$$a^{\frac{q-1}{2}} = 1$$

Proposição 2.3.3. O elemento -1 é um quadrado perfeito em $\mathbb{F}_q$ se, e somente se, $q \equiv 1 \pmod{4}$.

Demonstração. Pelo Critério de Euler, $-1 \in \square_q$ se, e somente se, $(-1)^{\frac{q-1}{2}} = 1$. Para que essa igualdade seja satisfeita, o expoente $\frac{q-1}{2}$ deve ser par. Logo, $\frac{q-1}{2} = 2k \implies q - 1 = 4k \implies q \equiv 1 \pmod{4}$. $\square$

Proposição 2.3.4. O conjunto dos quadrados perfeitos não nulos, denotado por $\square_q^*$, munido da operação de multiplicação do corpo, constitui um subgrupo de $\mathbb{F}_q^*$.

Demonstração. Como $\square_q^* \subset \mathbb{F}_q$, a associatividade é herdada do corpo. O elemento neutro 1 pertence a $\square_q^*$ pois $1 = 1^2$. O conjunto é fechado sob multiplicação: se $a, b \in \square_q^*$, então existem x, y tais que $x^2 = a$ e $y^2 = b$. Logo, $ab = (xy)^2$, implicando que $ab \in \square_q^*$. Finalmente, o inverso multiplicativo de um quadrado perfeito é um quadrado perfeito, visto que $(x^2)^{-1} = (x^{-1})^2$. $\square$

2.4 Grafo de Paley

Definição 2.4.1. Seja r uma potência de um número primo tal que $r \equiv 1 \pmod{4}$. O Grafo de Paley, denotado frequentemente por $P(r)$, é definido como o grafo não orientado cujos vértices são os elementos do corpo finito $\mathbb{F}_q$.

Dois vértices distintos x e y são adjacentes se, e somente se, a diferença entre eles for um quadrado não nulo em $\mathbb{F}_q$. Formalmente:

$$V(P(r)) = \mathbb{F}_q$$

$$E(P(r)) = \{\{x, y\} \mid x, y \in V(P(r)) \text{ e } x - y \in \mathcal{Q}\}$$

onde $\mathcal{Q}$ denota o conjunto dos resíduos quadráticos não nulos (quadrados) do corpo $\mathbb{F}_q$.

A condição $r \equiv 1 \pmod{4}$ é necessária para que o Grafo de Paley seja não orientado. Para que a relação de adjacência seja simétrica, se x é adjacente a y ($x - y \in \mathcal{Q}$), então y deve ser adjacente a x ($y - x \in \mathcal{Q}$). Como $y - x = -1(x - y)$ e, sob a condição dada, -1 é um quadrado perfeito, o produto $-1(x - y)$ também será um quadrado perfeito (pois $\square_q^*$ é um subgrupo multiplicativo). Isso garante que a aresta $\{x, y\}$ não possua orientação definida.

Exemplo 2.4.1. Considere o caso onde $r = 5$. Como 5 é um número primo e $5 \equiv 1 \pmod{4}$, podemos construir o Grafo de Paley $P(5)$. O conjunto de Vértices V são os elementos do corpo finito $GF(5)$ (os inteiros módulo 5):

$$V = \{0, 1, 2, 3, 4\}$$

Para definir as arestas, primeiramente identificamos o conjunto $\mathcal{Q}$ dos resíduos quadráticos não nulos em $GF(5)$:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1$$

Portanto, $\mathcal{Q} = \{1, 4\}$.

Dois vértices u, v são adjacentes se a diferença $u - v \pmod{5}$ pertencer a $\mathcal{Q}$.

- 0 é adjacente a 1 e 4 (pois $1 - 0 = 1$ e $4 - 0 = 4$).
- 1 é adjacente a 2 e 0 (pois $2 - 1 = 1$ e $0 - 1 = -1 \equiv 4$).
- 2 é adjacente a 3 e 1 (pois $3 - 2 = 1$ e $1 - 2 = -1 \equiv 4$).
- 3 é adjacente a 4 e 2 (pois $4 - 3 = 1$ e $2 - 3 = -1 \equiv 4$).
- 4 é adjacente a 0 e 3 (pois $0 - 4 = -4 \equiv 1$ e $3 - 4 = -1 \equiv 4$).

A representação visual de $P(5)$, que é isomorfa ao ciclo C_5 , é apresentada na Figura abaixo.

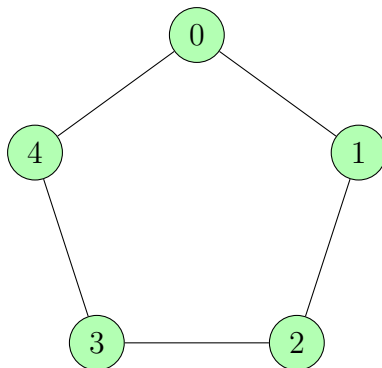


Figura 3 – Grafo de Paley $P(5)$, isomorfo ao ciclo C_5

3 Torneios de Paley

Neste capítulo, consolidaremos os conceitos estudados anteriormente para definir e construir formalmente os Torneios de Paley. Enquanto o capítulo anterior tratou das propriedades gerais dos corpos finitos e grafos, aqui restringiremos nosso foco aos corpos cuja ordem satisfaz a congruência $q \equiv 3 \pmod{4}$. Veremos como essa condição aritmética específica é determinante para garantir a antissimetria das arestas, transformando o Grafo de Paley em um torneio. Além da definição formal, apresentaremos a construção detalhada do torneio de ordem 7 (P_7), ilustrando passo a passo como a teoria dos números dita a estrutura geométrica do grafo.

3.1 Torneios de Paley

Os Grafos de Paley formam uma família infinita de grafos definidos sobre corpos finitos. Dependendo da ordem q do corpo, o grafo resultante pode ser não-orientado ou orientado. O caso orientado é denominado **Torneio de Paley**.

Definição 3.1.1. Seja $q = p^n$ a potência de um número primo tal que $q \equiv 3 \pmod{4}$. O Torneio de Paley, denotado por P_q ou T_q , é um digrafo (grafo orientado) $G = (V, E)$ onde:

- O conjunto de vértices V é o corpo finito $\mathbb{F}_q$.
- O conjunto de arestas E é formado pelos pares ordenados (u, v) tais que a diferença $v - u$ é um resíduo quadrático (quadrado perfeito) não nulo em $\mathbb{F}_q$.

Em notação matemática:

$$(u, v) \in E \iff v - u \in \square_q$$

onde $\square_q = \{x^2 : x \in \mathbb{F}_q^*\}$ é o conjunto dos quadrados perfeitos de $\mathbb{F}_q$.

A restrição $q \equiv 3 \pmod{4}$ é fundamental para garantir a propriedade de antissimetria necessária para um torneio. Sob essa condição, -1 não é um quadrado perfeito em $\mathbb{F}_q$. Consequentemente, para quaisquer dois vértices distintos u, v , tem-se que se $x = v - u$

é um quadrado, então $-x = u - v$ não é. Isso assegura que existe apenas uma aresta orientada entre qualquer par de vértices distintos.

Diferentemente do caso anterior, nos Torneios de Paley a ordem do corpo satisfaz $q \equiv 3 \pmod{4}$.

Proposição 3.1.1. Se $q \equiv 3 \pmod{4}$, então para qualquer $x \in \mathbb{F}_q^*$, exatamente um entre $\{x, -x\}$ é um quadrado perfeito.

Demonstração. Se $q \equiv 3 \pmod{4}$, o expoente $\frac{q-1}{2}$ no Critério de Euler é ímpar. Assim, $(-1)^{\frac{q-1}{2}} = -1$, o que implica que -1 não é um quadrado perfeito. Se x é um quadrado, então $-x = (-1)x$ é o produto de um não-quadrado por um quadrado, o que resulta em um não-quadrado. Isso garante a antissimetria: se existe a aresta (u, v) , não pode existir a aresta (v, u) , caracterizando a estrutura de torneio. $\square$

3.1.1 Exemplos de Construção

Exemplo 3.1.1. Para ilustrar a base da estrutura cíclica, construímos o menor torneio de Paley possível. Note que $3 \equiv 3 \pmod{4}$.

Considere o corpo primo $\mathbb{F}_3 = \{0, 1, 2\}$.

1. Identificação dos Quadrados ($\square_3$): Elevamos ao quadrado os elementos não nulos (módulo 3):

$$1^2 \equiv 1, \quad 2^2 \equiv 4 \equiv 1$$

Logo, o conjunto dos resíduos quadráticos é $\square_3 = \{1\}$.

2. Construção das Arestas: A aresta (u, v) existe se $v - u \in \{1\}$. As arestas que compõem o torneio são: $(0, 1), (1, 2), (2, 0)$.

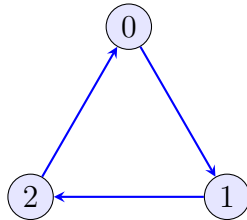


Figura 4 – Grafo do Torneio de Paley P_3 .

$\mathbb{F}_7$. Note que $7 \equiv 3 \pmod{4}$.

Exemplo 3.1.2. Considere o corpo $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

1. Identificação dos Quadrados ($\square_7$): Elevamos ao quadrado os elementos não nulos (módulo 7):

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1$$

Logo, o conjunto dos resíduos quadráticos é $\square_7 = \{1, 2, 4\}$.

2. Construção das Arestas: A aresta (u, v) existe se $v - u \in \{1, 2, 4\}$. Por exemplo, partindo do vértice 0:

- $1 - 0 = 1 \in \square_7 \implies (0, 1) \in E$
- $2 - 0 = 2 \in \square_7 \implies (0, 2) \in E$
- $4 - 0 = 4 \in \square_7 \implies (0, 4) \in E$

O conjunto de arestas que saem de 0 é $N^+(0) = \{1, 2, 4\}$. Devido à simetria rotacional dos grafos de Paley, as arestas dos outros vértices seguem o padrão $u \rightarrow (u + d)$ para todo $d \in \square_7$.

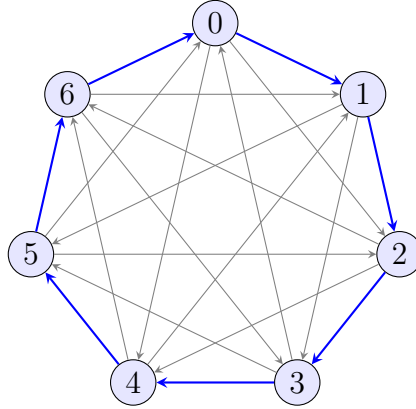


Figura 5 – Grafo do Torneio de Paley P_7 .

Exemplo 3.1.3. Considere o corpo primo $\mathbb{F}_{11} = \{0, 1, 2, \dots, 10\}$.

Este exemplo ilustra um torneio com maior densidade de arestas, onde a condição $11 \equiv 3 \pmod{4}$ garante a antissimetria.

1. Identificação dos Quadrados ($\square_{11}$): Calculando os quadrados perfeitos em $\mathbb{F}_{11}$ através da aplicação $x \mapsto x^2$:

$$1^2, 10^2 \equiv 1; \quad 2^2, 9^2 \equiv 4; \quad 3^2, 8^2 \equiv 9; \quad 4^2, 7^2 \equiv 5; \quad 5^2, 6^2 \equiv 3$$

Logo, o conjunto de resíduos quadráticos não nulos é $\square_{11} = \{1, 3, 4, 5, 9\}$.

2. Construção das Arestas: A aresta orientada (u, v) existe se a diferença $v - u$ for um resíduo quadrático. Partindo do vértice 0, as arestas incidem nos vizinhos $N^+(0) = \{1, 3, 4, 5, 9\}$. Pela simetria rotacional, para qualquer vértice u , as arestas são do tipo $(u, u + d)$ para cada $d \in \square_{11}$.

4 Considerações Finais

O presente trabalho dedicou-se ao estudo da construção algébrica e das propriedades combinatórias dos Torneios de Paley, evidenciando a profunda conexão entre a Teoria dos Números e a Teoria Algébrica dos Grafos. Ao longo dos capítulos, demonstramos como estruturas abstratas, como corpos finitos e resíduos quadráticos, fornecem a base rigorosa necessária para definir objetos geométricos complexos e altamente simétricos.

Uma das conclusões centrais desta monografia foi a importância determinante da congruência da ordem do corpo finito. Verificamos que a condição $q \equiv 3 \pmod{4}$ não é meramente uma curiosidade aritmética, mas sim o requisito fundamental que impede a existência de -1 como quadrado perfeito. É essa restrição algébrica que quebra a simetria das arestas, transformando o grafo de Paley em um torneio (grafo orientado), garantindo a propriedade de antissimetria essencial para esta classe.

A construção detalhada do Torneio de Paley de ordem 7 (P_7) serviu como uma ilustração concreta da teoria. Ela permitiu visualizar como a aritmética modular dita a orientação das arestas, gerando uma estrutura que, embora determinística, possui propriedades de quase-aleatoriedade.

Por fim, é importante ressaltar que o estudo dos Torneios de Paley transcende o interesse puramente teórico. Conforme mencionado na literatura consultada, estas estruturas representam instâncias de alta complexidade para problemas de otimização combinatória, como o Problema de Ordenação Linear. Portanto, a compreensão profunda de sua formação algébrica, aqui apresentada, é um passo inicial valioso para investigações futuras em criptografia, teoria de códigos e complexidade de algoritmos.

Esperamos que este trabalho tenha cumprido seu objetivo de desmistificar a construção destes grafos, servindo como uma porta de entrada para o fascinante estudo da interação entre álgebra e combinatória.

Referências

- 1 OLIVEIRA, W. A. da S. *Grafos de Paley*. 32 f. Monografia (Trabalho de Conclusão de Curso (Licenciatura em Matemática)) — Universidade Federal de Pernambuco, Recife, 2009.
- 2 GARCIA, A.; LEQUAIN, Y. *Elementos de Álgebra*. Rio de Janeiro: IMPA, 2002. (Projeto Euclides).
- 3 DAHAB, R. *Corpos Finitos: Parte I*. Campinas: [s.n.], 2006. IC-UNICAMP. Material de aula. Disciplina MO829-MC932: Algoritmos Criptográficos.
- 4 BRGLEZ, F.; HO, Y.; NGUYEN, J. *On Asymptotic Complexity of Linear Ordering the Paley Tournament Graphs: First Prototypes with Self-Avoiding Walks*. Raleigh, USA: [s.n.], 2017. NC State University. A version in progress, January 31, 2017.