Tópicos Recentes Envolvendo Polinômios de Permutação sobre Corpos Finitos

de

José Alves Oliveira

Departamento de Matemática
Universidade Federal de Minas Gerais

Março de 2019

José Alves Oliveira

Tópicos Recentes Envolvendo Polinômios de Permutação sobre Corpos Finitos

Dissertação apresentada ao corpo docente de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

Orientador: Fabio Enrique Brochero Martínez

Universidade Federal de Minas Gerais

Março de 2019

Ficha catalográfica elaborada pela bibliotecária Irénquer Vismeg Lucas - CRB 6ª Reg. nº 819

Oliveira, José Alves.

O48t Tópicos recentes envolvendo polinômios de permutação sobre corpos finitos / José Alves Oliveira — Belo Horizonte, 2019.
70 f. il.; 29 cm.

Dissertação (mestrado) - Universidade Federal de Minas Gerais – Departamento de Matemática.

Orientador: Fabio Enrique Brochero Martínez

1. Matemática – Teses. 2. Corpos finitos (Álgebra). 3. Polinômios. I. Orientador. II. Título

CDU 51(043)

Universidade Federal de Minas Gerais
Departamento de Matemática
Programa de Pós-Graduação em Matemática

FOLHA DE APROVAÇÃO

Tópicos Recentes Envolvendo Polinômios de Permutação sobre Corpos Finitos

JOSÉ ALVES OLIVEIRA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Fabio Enrique Brochero Martínez
UFMG

Prof. Davi dos Santos Lima
UFAL

Prof. Sávio Ribas
UFOP

Belo Horizonte, 15 de março de 2019.

Av. Antônio Carlos, 6627 – Campus Pampulha - Caixa Postal: 702
CEP-31270-901 - Belo Horizonte – Minas Gerais - Fone (31) 3409-5963
e-mail: pgmat@mat.ufmg.br - home page: http://www.mat.ufmg.br/pgmat

Agradecimentos

Agradeço primeiramente a Deus.

Aos meus pais, Cleber e Magdália, e ao meu irmão, Guilherme, por todo apoio, carinho e incetivo que tem me dado desde que me mudei para Belo Horizonte e me tornei estudante da UFMG.

Ao meu padrinho, César, por toda atenção e conselhos que tem me dado durante toda vida.

À todos meus amigos conterrâneos Claudienses, que estão sempre presentes em diversas situações, mesmo tendo cada um tomado um caminho distinto.

Ao meu orientador e também amigo, Fábio, por toda paciência durante os dois últimos anos e por todos os ensinamentos que tem me passado. Tenho aprendido muito contigo nesses últimos anos.

À todos que moraram comigo durante esses últimos quatro anos, em especial aos grandes amigos que levarei para o resto da vida: Bruno, Ígor, João, Jonas e Lucas.

À todos meus amigos da graduação, mestrado e doutorado em matemática, pela amizade e pelo companheirismo durante todos os momentos de dificuldade.

À toda equipe do PICME, em especial ao Rafael Drumond, André Contiero, e Sylvie, por todo apoio, dicas e por todo suporte que tem me durante os últimos anos.

Ao programa de Pós-Graduação da Matemática, pela oportunidade.

Aos participantes da banca, Sávio Ribas e Davi Lima, por todas as sugestões e dicas apresentadas.

Às secretárias da pós-graduação, Kelli e Andréa, por sempre estarem dispostas a sanar minhas dúvidas e resolver meus contratempos.

À todos os professores com os quais tive aula durante toda a vida, por todos ensinamentos.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

"Importante não é ver o que ninguém nunca viu,
mas sim, pensar o que ninguém nunca pensou
sobre algo que todo mundo vê."

Arthur Schopenhauer

Resumo

Neste trabalho, apresentaremos alguns tópicos atuais envolvendo polinômios de permutação sobre corpos finitos. Em especial, exibiremos a teoria necessária para contar o número de binômios de permutação das formas $x^n(x^{\frac{q-1}{2}}+a)$ e $x^n(x^{\frac{q-1}{3}}+a)$. Apresentaremos também o conceito de posto de Carlitz para polinômios de permutação e uma nova cota inferior para o número de coeficientes não nulos de polinômios de permutação com posto 2.

Palavras-chave: Corpos Finitos, Polinômios de Permutação, Contagem de Binômios, Posto de Carlitz.

Abstract

In this work, we will present some current topics involving permutation polynomials over finite fields. In particular, we will show the necessary theory to count the number of permutation binomials of the forms $x^n(x^{\frac{q-1}{2}}+a)$ and $x^n(x^{\frac{q-1}{3}}+a)$. We will also present the Carlitz rank concept for permutation polynomials and a new lower bound for the number of nonzero coefficients of permutation polynomials with rank 2.

Keywords: Finite Fields, Permutation Polynomials, Binomial Counting, Carlitz Rank.

Sumário

Introdução

O conceito de permutação expressa a ideia de que vários objetos possam ser arranjados de inúmeras formas distintas. Em álgebra e combinatória, esse conceito é bastante estudado. Neste texto, nosso objetivo é estudar os aspectos e as propriedades de polinômios de permutação sobre corpos finitos. Para entendermos melhor esse conceito, segue a definição de polinômio de permutação: Seja q uma potência de um primo p e $\mathbb{F}_q$ um corpo com q elementos. Um polinômio $f(x) \in \mathbb{F}_q[x]$ é chamado de polinômio de permutação de $\mathbb{F}_q$ se a aplicação $a \mapsto f(a)$ permuta os elementos de $\mathbb{F}_q$.

Historicamente, o início do estudo de polinômios de permutação se deu com Hermite, que investigou permutações sobre corpos primos. Dickson [5] foi o primeiro a analisá-los sobre corpos finitos arbitrários. Atualmente, vários resultados envolvendo polinômios de permutação têm sido publicados, grande parte desses apresentando novas famílias de polinômios de permutação, bem como resultados envolvendo aspectos relacionados aos mesmos.

A nossa motivação em estudar polinômios de permutações sobre corpos finitos se deve, principalmente, ao fato de existirem muitos problemas interessantes, tanto teóricos como aplicações práticas, e que foram pouco explorados na área. Um exemplo de polinômio de permutação, com grande aplicação prática, é o polinômio x^n, definido sobre o anel de inteiros $\mathbb{Z}_{p_0 \cdot q_0}$, com p_0 e q_0 primos e $\text{mdc}(n, \varphi(p_0 \cdot q_0)) = 1$, que é uma base da criptografia RSA. Uma quantidade extensa de outros polinômios de permutação são estudados em diversas áreas na matemática. Tais polinômios têm aplicações importantes em Teoria dos Códigos e Corretores de Erros, Criptografia, Curvas Algébricas, entre outros. Atualmente, por existirem noções e propriedades pouco exploradas na área de polinômios de permutação sobre corpos finitos, esta é uma área com grande interesse de pesquisa.

O primeiro capítulo deste trabalho consiste em uma introdução aos corpos finitos, onde são apresentados resultados importantes, que serão utilizados no decorrer do texto. Encontrar polinômios de permutação com estruturas de fácil computabilidade é um problema importante na área de polinômios de permutação. Por esse motivo, a primeira parte do segundo capítulo contém alguns resultados já conhecidos envolvendo polinômios de permutação, bem como teoremas que nos permitem encontrar famílias de polinômios de permutação.

Uma das questões mais importantes no estudo de polinômios de permutação sobre corpos finitos é a contagem desses polinômios com determinada propriedade. Nessa linha, um problema, que está em aberto e com poucos avanços que possam levar a uma solução,

é encontrar o número de polinômios de permutação de determinado grau. Outro problema interessante, e ainda sem resposta, é a contagem binômios de permutação sobre $\mathbb{F}_q$. Esse problema é a motivação para a segunda parte do segundo capítulo, onde começamos enunciando uma cota, já conhecida, apresentada por Masuda e Zieve [15] e seguimos apresentando resultados que possibilitam realizar a contagem do número de binômios de permutação das formas $x^n(x^{\frac{q-1}{2}}+a)$ e $x^n(x^{\frac{q-1}{3}}+a)$, resultados esses que nós conjecturamos e provamos.

No Capítulo 3, apresentamos o conceito de posto de Carlitz, que é a constante numérica relacionada com a "complexidade" de polinômios de permutação, cuja definição e propriedades têm sido bastante estudadas na última década. Especificamente, enunciaremos o resultado de Gómez, Ostafe e Topuzoğlu [6], que apresenta uma cota relacionando o posto de Carlitz ao número de coeficientes não nulos do polinômio. Em seguida, apresentaremos um trabalho original com objetivo de melhorar essa cota para o caso em que o posto de Carlitz é 2.

CAPÍTULO 1

Conceitos Básicos

1.1 Corpos Finitos

Nesta seção, apresentaremos algumas definições e teoremas importantes em corpos finitos e que serão úteis nos próximos capítulos.

Definição 1.1. *Um grupo é um conjunto* $\mathbb{G}$ *munido de uma operação binária* $+ : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ *que satisfaz os seguintes axiomas:*

1. *Associatividade:* $(x + y) + z = x + (y + z)$*, para todos* $x, y, z \in \mathbb{G}$*;*
2. *Elemento Neutro: Existe a identidade* $\mathbb{0} \in \mathbb{G}$ *tal que* $\mathbb{0} + x = x$*, para todos* $x \in \mathbb{G}$*;*
3. *Inversa: Se* $x \in \mathbb{G}$*, existe o elemento inverso de* x *em* $\mathbb{G}$*, denotado por* $-x \in \mathbb{G}$*, tal que* $x + (-x) = \mathbb{0}$*.*

Definição 1.2. *Dizemos que um grupo* $\mathbb{G}$ *é abeliano se* $x + y = y + x$*, para todo* $x, y \in \mathbb{G}$*.*

Definição 1.3. *Um anel é um conjunto* R *munido de duas operações binárias* $+, * : R \times R \to R$*, nomeadamente soma e multiplicação, que é grupo abeliano para operação soma e cuja multiplicação satisfaz o axioma de associatividade e de distributividade, dada por*

- *Distributividade:* $x * (y + z) = x * y + x * z$ *para todos* $x, y, z \in R$*;*
  $(y + z) * x = y * x + z * x$ *para todos* $x, y, z \in R$*.*

Definição 1.4. *Dizemos que um anel* R *é comutativo se* $x * y = y * x$*, para todos* $x, y \in R$*.*

Definição 1.5. *Um conjunto* $\mathbb{F}$ *é chamado de corpo se for um anel comutativo com elemento neutro multiplicativo* $\mathbb{1} \neq \mathbb{0}$ *e tal que todo elemento* $x \in \mathbb{F} \backslash \{\mathbb{0}\}$ *possui inverso multiplicativo. Denotaremos por* x^{-1} *o inverso multiplicativo de um elemento* $x \neq \mathbb{0}$*.*

Muitas vezes, denotamos a operação $a * b$ apenas por ab (justaposição de a e b). Se $\mathbb{F}$ é um corpo, denotamos por $\mathbb{F}^*$ o conjunto dos elementos de $\mathbb{F}$ que possuem inverso multiplicativo, isto é, $\mathbb{F}^* := \mathbb{F}\backslash\{\mathbb{0}\}$.

Exemplo 1.6. Os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, munidos de soma e multiplicação usual, são exemplos de corpos com infinitos elementos.

Exemplo 1.7. Seja $p \in \mathbb{Z}$ um primo e

$$\mathbb{Z}_p := \frac{\mathbb{Z}}{(p)} = \{\overline{0}, \overline{1}, \ldots \overline{p-1}\},$$

o conjunto dos restos módulo p. É fácil verificar que $\mathbb{Z}/(n)$, munido de soma e multiplicação usuais, é um anel comutativo com unidade, para qualquer $n \in \mathbb{N}$, com $n > 1$. Então, para concluir que $\mathbb{Z}_p$ é um corpo, basta verificar a existência de um inverso multiplicativo para todo elemento não nulo. Para isso, tome $\overline{x} \in \mathbb{Z}_p\backslash\{\overline{0}\}$. Sabemos que $\text{mdc}(x, p) = 1$, então, pelo Teorema de Bézout, existem $m, n \in \mathbb{N}$ tais que $xn + pm = 1$. Logo, $\overline{xn + pm} = \overline{x}\,\overline{n} = \overline{1}$. Assim, $\overline{n} = \overline{x}^{\,-1}$. Com isso, concluímos que $\mathbb{Z}_p$ é um corpo.

Definição 1.8. *A característica char(R) de um anel R é menor (caso exista) $n \in \mathbb{N}$ tal que*

$$n \times x := \overbrace{x + \cdots + x}^{n \text{ vezes}} = \mathbb{0}, \text{ para todo } x \in R.$$

Se não existe n com tal propriedade, dizemos que char$(R) = 0$.

Observe que, em um corpo $\mathbb{F}$, as propriedades de associatividade multiplicativa e inversa multiplicativa fazem com essa definição seja equivalente à seguinte: a característica $\text{char}(\mathbb{F})$ de um corpo $\mathbb{F}$ é menor (caso exista) $n \in \mathbb{N}$ tal que $n \times \mathbb{1} = 0$.

Lema 1.9. *Seja $\mathbb{F}$ um corpo finito. Então char$(\mathbb{F}) = p$ primo.*

Demonstração. Suponha que $\text{char}(\mathbb{F}) = nm \in \mathbb{N}$, com $n \neq 1 \neq m$. Então

$$(n \times \mathbb{1}) * (m \times \mathbb{1}) = \overbrace{(\mathbb{1} + \ldots + \mathbb{1})}^{n \text{ vezes}} * \overbrace{(\mathbb{1} + \ldots + \mathbb{1})}^{m \text{ vezes}} = \overbrace{(\mathbb{1} + \ldots + \mathbb{1})}^{nm \text{ vezes}} = \mathbb{0}.$$

Multiplicando ambos os lados por $(m \times \mathbb{1})^{-1}$, temos:

$$n \times \mathbb{1} = \mathbb{0} * (m \times \mathbb{1})^{-1} = \mathbb{0}.$$

Mas $n < nm$, o que é absurdo, já que $\text{char}(\mathbb{F})$ é o menor inteiro com tal propriedade. Concluímos que $\text{char}(\mathbb{F}) = p$ primo. □

Teorema 1.10. *Se $\mathbb{F}$ é um corpo finito, então $|\mathbb{F}| = p^n$, para algum p primo e n um inteiro positivo.*

Demonstração. Sejam $\mathbb{0}, \mathbb{1} \in \mathbb{F}$ as identidades para soma e multiplicação de $\mathbb{F}$, respectivamente. Pelo Lema 1.9, sabemos que $\text{char}(\mathbb{F}) = p$ primo. Sendo assim, o conjunto $\mathbb{K} := \{\mathbb{0}, \mathbb{1}, 2 \times \mathbb{1}, 3 \times \mathbb{1}, \ldots, (p-1) \times \mathbb{1}\} \subset \mathbb{F}$ é um subcorpo de $\mathbb{F}$ com p elementos e é fácil verificar que $\mathbb{F}$ é um espaço vetorial sobre $\mathbb{K}$. Sendo assim, se $\dim_{\mathbb{K}}(\mathbb{F}) = n$, existem vetores $v_1, \ldots, v_n \in \mathbb{F}$ linearmente independentes que formam uma base de $\mathbb{F}$. Logo, um elemento qualquer de $\mathbb{F}$ é da forma $a_1 v_1 + \ldots + a_n v_n$, com $a_i \in \mathbb{K}$. Como são p escolhas para cada a_i, segue que existem p^n elementos distintos em $\mathbb{F}$. □

Até aqui, utilizamos a notação $n \times a$ para representar $\overbrace{a + \cdots + a}^{n \text{ vezes}}$, com $a \in \mathbb{F}$ um corpo e $n \in \mathbb{N}$. Entretanto, podemos usar a justaposição na e esta será condizente com a justaposição já introduzida como sendo a operação multiplicação do corpo, uma vez que que, no decorrer do texto, também abusaremos da notação dizendo que $\mathbb{1} = 1$, $\mathbb{0} = 0$ e que a operação de um corpo $*$ é o mesmo que a multiplicação nos inteiros $\times$.

Observação 1.11. O corpo $\mathbb{K}$ que aparece na prova do Teorema 1.10 é isomorfo ao corpo $\mathbb{Z}_p$ apresentado no exemplo 1.7.

Quando falamos em isomorfismo entre dois conjuntos, estamos nos referindo à existência de uma função bijetiva que preserva a estrutura existente nos mesmos. No caso de isomorfismo entre corpos, daremos, abaixo, a definição formal para tal conceito.

Definição 1.12. *Dizemos que dois corpos* $(\mathbb{F}, +_{\mathbb{F}}, *_{\mathbb{F}})$ *e* $(\mathbb{K}, +_{\mathbb{K}}, *_{\mathbb{K}})$ *são isomorfos se existe uma função* $\varphi : \mathbb{F} \to \mathbb{K}$ *bijetiva tal que*

- $\varphi(x +_{\mathbb{F}} y) = \varphi(x) +_{\mathbb{K}} \varphi(y)$ *para todos* $x, y \in \mathbb{F}$*;*
- $\varphi(x *_{\mathbb{F}} y) = \varphi(x) *_{\mathbb{K}} \varphi(y)$ *para todos* $x, y \in \mathbb{F}$*.*

Teorema 1.13 ([13], Teorema 2.5)**.** *Para todo primo* p *e todo inteiro positivo* n*, existe um corpo com* p^n *elementos. Além disso, todos os corpos com* p^n *elementos são isomorfos.*

A partir de agora, denotaremos por $\mathbb{F}_q$ um corpo qualquer que contenha $q = p^n$ elementos. Com isso, podemos denotar $\mathbb{Z}_p$ por $\mathbb{F}_p$.

Exemplo 1.14. Seja $p \in \mathbb{N}$ um número primo ímpar. Construiremos, a seguir, um corpo com p^2 elementos. Para isso, tome $a \in \mathbb{F}_p^*$ um elemento não quadrado, isto é, um elemento para o qual a equação $x^2 = a$ não possua solução em $\mathbb{F}_p$. É um fato conhecido, de Teoria dos Números, que metade dos elementos de $\mathbb{Z}_p^*$ não são quadrados. Sendo assim, $x^2 - a$ será irredutível em $\mathbb{F}_p[x]$, uma vez que sua fatoração seria $(x + \sqrt{a})(x - \sqrt{a})$, mas $\sqrt{a} \notin \mathbb{F}_p$. Faremos algo análogo ao Exemplo 1.7, tomando

$$\mathbb{F}_{p^2} := \frac{\mathbb{F}_p[x]}{(x^2 - a)}. \tag{1.1.1}$$

É fácil verificar que $\mathbb{F}_{p^2}$ é um anel comutativo com unidade. Note que, de fato, temos $|\mathbb{F}_{p^2}| = p^2$, uma vez que $\mathbb{F}_{p^2} = \{\overline{b + cx} : b, c \in \mathbb{F}_p\}$. Para concluir que $\mathbb{F}_{p^2}$, como definido na igualdade (1.1.1), é um corpo, basta mostrar que todo elemento não nulo possui

inverso multiplicativo. Para isso, tome $\overline{f(x)} \in \mathbb{F}_{p^2} \backslash \{\overline{0}\}$. Sabemos que $\mathbb{F}_p[x]$ é um domínio euclidiano. Como $x^2 - a$ é irredutível, temos $\text{mdc}(f(x), x^2 - a) = 1$ e, assim, pelo Teorema de Bézout, existem $g(x), h(x) \in \mathbb{F}_p[x]$ tais que $f(x)g(x) + (x^2 - a)h(x) = 1$. Logo, $\overline{f(x)g(x) + (x^2 - a)h(x)} = \overline{f(x)g(x)} = \overline{1}$ em $\mathbb{F}_{p^2}$. Assim, $\overline{g(x)} = \overline{f(x)}^{-1}$. Por isso, concluímos que $\mathbb{F}_{p^2}$ é um corpo finito com p^2 elementos.

Observe que esse exemplo apresenta um caminho para a prova da primeira parte do Teorema 1.13, sendo suficiente mostrar a existência de polinômios irredutíveis de grau arbitrário em $\mathbb{F}_p[x]$, para todo primo $p \in \mathbb{N}$.

Teorema 1.15. *Seja $\mathbb{F}_q$ um corpo, então $(\mathbb{F}_q^*, \times)$ é cíclico.*

Demonstração. Em toda prova, usaremos o fato de $(\mathbb{F}_q^*, *)$ ser um grupo e resultados básicos de álgebra, como Teorema de Lagrange e propriedades da ordem de um elemento. Primeiramente, observe que a ordem de $\mathbb{F}_q^*$ é $q - 1 = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ (fatoração em primos distintos). Como estamos trabalhando em um corpo, $x^{\frac{q-1}{p_i}} - 1$ tem no máximo $\frac{q-1}{p_i}$ raízes em $\mathbb{F}_q$. Sabendo disso, podemos escolher um elemento $a_i \in \mathbb{F}_q^*$ que não é raiz de $x^{\frac{q-1}{p_i}} - 1$. Definimos $b_i = a_i^{(q-1)/p_i^{\alpha_i}}$. Como $b_i^{p_i^{\alpha_i}} = 1$, a ordem de b_i é p_i^l, com $1 \leq l \leq \alpha_i$. Mas

$$b_i^{p_i^l} = a_i^{(q-1)/p_i^{\alpha_i - l}} = 1,$$

que é válido apenas se $l = \alpha_i$, uma vez que $a_i^{\frac{q-1}{p_i}} \neq 1$. Definimos $b := b_1 \cdots b_m$ e t a ordem de b. Suponhamos que t seja um divisor próprio de $q - 1$, então t divide $\frac{q-1}{p_j}$ para algum $1 \leq j \leq m$. Dessa forma,

$$b^{\frac{q-1}{p_j}} = b_1^{\frac{q-1}{p_j}} \cdots b_m^{\frac{q-1}{p_j}} = 1 \cdots b_j^{\frac{q-1}{p_j}} \cdots 1 = b_j^{\frac{q-1}{p_j}} \neq 1,$$

o que é absurdo. Então $ord_{\mathbb{F}_q^*}(b) = q - 1$ e, portanto, $\langle b \rangle = \mathbb{F}_q^*$. □

Definição 1.16. *Se $a \in \mathbb{F}_q$ é um gerador de $(\mathbb{F}_q^*, \times)$, dizemos que a é um elemento primitivo de $\mathbb{F}_q$.*

1.1.1 Teorema de Lucas

Como vimos no Lema 1.9, a característica de um corpo finito é sempre um primo. Podemos explorar esse fato para conseguir os seguintes resultados, que serão importantes nos próximos capítulos.

Lema 1.17. *Sejam $a, b \in \mathbb{F}_q$ e $char(\mathbb{F}) = p$. Então $(a + b)^p = a^p + b^p$.*

Demonstração. Basta expandir o binômio de Newton e considerar $(\text{mod } p)$:

$$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \equiv a^p + b^p \pmod{p}.$$

□

No Teorema apresentado abaixo, convencionaremos $\binom{x}{y} = 0$ para $y > x$.

Teorema 1.18 ([14], Teorema de Lucas)**.** *Seja p um primo e $n \geq m \in \mathbb{N}$, que se escrevem na base p como $n = n_0 + n_1 p + \ldots + n_k p^k$ e $m = m_0 + m_1 p + \ldots + m_k p^k$. Então:*

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\ldots\binom{n_k}{m_k} \pmod{p}.$$

Demonstração. Existem várias formas de mostrar tal resultado. Optamos por apresentar essa utilizando congruência polinomial. Observe que

$$\sum_{m=0}^{n}\binom{n}{m}x^m = (1+x)^n = (1+x)^{\sum_{i=0}^{k} n_i p^i} = \prod_{i=0}^{k}(1+x)^{n_i p^i}. \tag{1.1.2}$$

Pelo Lema 1.17, temos

$$\prod_{i=0}^{k}(1+x)^{n_i p^i} \equiv \prod_{i=0}^{k}(1+x^{p^i})^{n_i} \equiv \prod_{i=0}^{k}\sum_{m_i=0}^{n_i}\binom{n_i}{m_i}x^{m_i p^i} \pmod{p}. \tag{1.1.3}$$

Como estamos assumindo $\binom{x}{y} = 0$ para $y > x$, temos

$$\prod_{i=0}^{k}\sum_{m_i=0}^{n_i}\binom{n_i}{m_i}x^{m_i p^i} = \prod_{i=0}^{k}\sum_{m_i=0}^{p-1}\binom{n_i}{m_i}x^{m_i p^i} = \sum_{m=0}^{n}\left[\prod_{i=0}^{k}\binom{n_i}{m_i}\right]x^m. \tag{1.1.4}$$

Com isso, temos o resultado, já que

$$\sum_{m=0}^{n}\binom{n}{m}x^m \equiv \sum_{m=0}^{n}\left[\prod_{i=0}^{k}\binom{n_i}{m_i}\right]x^m \pmod{p}. \tag{1.1.5}$$

□

Corolário 1.19. *Seja p um primo e $m, n \in \mathbb{N}$. Então*

$$\binom{p^n - 1}{m} \equiv (-1)^m \pmod{p}, \text{ para } m \leq p^n - 1$$

e

$$\binom{p^n - 2}{m} \equiv (m+1)(-1)^m \pmod{p}, \text{ para } m \leq p^n - 2.$$

Demonstração. Seja $m = \sum_{i=0}^{n-1} m_i p^i$. Pelo Teorema anterior temos, para a primeira

parte:

$$\begin{aligned}
\binom{p^n-1}{m} &\equiv \binom{p-1}{m_0}\binom{p-1}{m_1}\dots\binom{p-1}{m_{n-1}} \pmod p \\
&\equiv \left(\frac{(p-1)\dots(p-m_0)}{m_0!}\right)\dots\left(\frac{(p-1)\dots(p-m_{n-1})}{m_{n-1}!}\right) \pmod p \\
&\equiv \left(\frac{(-1)^{m_0}m_0!}{m_0!}\right)\dots\left(\frac{(-1)^{m_{n-1}}m_{n-1}!}{m_{n-1}!}\right) \pmod p \\
&\equiv (-1)^{m_0}(-1)^{m_1}\dots(-1)^{m_{n-1}} \pmod p \\
&\equiv (-1)^{m_0}(-1)^{pm_1}\dots(-1)^{p^{n-1}m_{n-1}} \pmod p \\
&\equiv (-1)^{\sum_{i=0}^{n-1} m_i p^i} = (-1)^m \pmod p
\end{aligned}$$

Analogamente para a segunda parte:

$$\begin{aligned}
\binom{p^n-2}{m} &\equiv \binom{p-2}{m_0}\binom{p-1}{m_1}\dots\binom{p-1}{m_{n-1}} \pmod p \\
&\equiv \left(\frac{(p-2)\dots(p-m_0-1)}{m_0!}\right)(-1)^{\sum_{i=1}^{n-1} m_i p^i} \pmod p \\
&\equiv (-1)^{m_0}\frac{(m_0+1)!}{m_0!}(-1)^{\sum_{i=1}^{n-1} m_i p^i} \pmod p \\
&\equiv (m_0+1)(-1)^{\sum_{i=0}^{n-1} m_i p^i} \pmod p \\
&\equiv (m+1)(-1)^m \pmod p.
\end{aligned}$$

□

1.1.2 Função Traço

A aplicação traço é extensivamente utilizada na solução de problemas em corpos finitos. Apresentaremos, abaixo, os resultados principais envolvendo traço.

Definição 1.20. *Sejam $\mathbb{F}_q$ um corpo finito, $\mathbb{K} := \mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ e $\alpha \in \mathbb{K}$. O traço de α sobre $\mathbb{F}_q$ é definido por*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{F}_q}(\alpha) := \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}}.$$

Diretamente da definição, seguem as propriedades enunciadas na proposição abaixo.

Proposição 1.21. *A função traço satisfaz as seguintes propriedades:*

(a) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$, *para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$;

(b) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda\alpha) = \lambda\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, *para todo* $\lambda \in \mathbb{F}_q$ *e* $\alpha \in \mathbb{F}_{q^n}$;

(c) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = n\alpha$, *para todo* $\alpha \in \mathbb{F}_q$;

(d) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q)$, *para todo* $\alpha \in \mathbb{F}_{q^n}$.

Dessas propriedades, segue o seguinte teorema.

Teorema 1.22. *Seja* $\alpha \in \mathbb{F}_{q^n}$. $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ *se, e somente se,* $\beta - \beta^q = \alpha$, *para algum* $\beta \in \mathbb{F}_{q^n}$.

Demonstração. Se existe $\beta \in \mathbb{F}_{q^n}$ tal que $\beta - \beta^q = \alpha$, então $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) - \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta^q) = 0$, pelo item *(d)* da Proposição 1.21. Por outro lado, suponha $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ e tome β, em alguma extensão de $\mathbb{F}_{q^n}$, uma solução de $x - x^q = \alpha$. Então, $\beta - \beta^q = \alpha$ e

$$\begin{aligned} 0 &= \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}} \\ &= \beta - \beta^q + (\beta - \beta^q)^q + \ldots + (\beta - \beta^q)^{q^{n-1}} \\ &= \beta - \beta^q + \beta^q - \beta^{q^2} + \ldots + \beta^{q^{n-1}} - \beta^{q^n} \\ &= \beta - \beta^{q^n}, \end{aligned}$$

isso implica em $\beta \in \mathbb{F}_{q^n}$. □

1.1.3 Caracteres

Um conceito importante em teoria de grupos, que possui muitas aplicações em corpos finitos, será introduzido aqui. Além da definição de caráter, serão apresentados vários resultados acerca do mesmo.

Definição 1.23. *Sejam* $(\mathbb{G}, +_{\mathbb{G}}), (\mathbb{H}, +_{\mathbb{H}})$ *grupos. Uma função* $\varphi : (\mathbb{G}, +_{\mathbb{G}}) \to (\mathbb{H}, +_{\mathbb{H}})$ *é chamada de homomorfismo de grupos se*

$$\varphi(a +_{\mathbb{G}} b) = \varphi(a) +_{\mathbb{H}} \varphi(b).$$

Definição 1.24. *Seja* $\mathbb{G}$ *um grupo abeliano finito e* $U := \{w \in \mathbb{C} : |w| = 1\}$, *visto como um grupo multiplicativo. Uma função* $\chi : \mathbb{G} \to U$ *é chamada de caráter se for um homomorfismo de grupos.*

Exemplo 1.25. Se $\mathbb{G}$ é um grupo abeliano finito, a função $\mathbb{1} : G \to \mathbb{C}$, definida por $\mathbb{1}(x) = 1$, para todo $x \in \mathbb{G}$, é um caráter. A função $\mathbb{1}(x)$ é chamada de caráter trivial.

Se o grupo $\mathbb{G}$ apresentado na Definição 1.24 for $(\mathbb{F}_q, +)$, dizemos que χ é um caráter aditivo e se for $(\mathbb{F}_q^*, \times)$, dizemos que χ é um caráter multiplicativo. Note que o conjunto formado pelos caracteres de um grupo $\mathbb{G}$, o qual denotamos por $\widehat{\mathbb{G}}$, é um grupo (munido da operação multiplicação de caracteres). Com objetivo de apresentar um exemplo de caráter, definiremos o símbolo de Legendre generalizado para corpos finitos.

Definição 1.26. *Seja $q = p^n$, com p primo ímpar. Chamaremos de generalização do Símbolo de Legendre em $\mathbb{F}_q$ a função $\left(\frac{x}{\mathbb{F}_q}\right) : \mathbb{F}_q \to \{-1, 1, 0\} \subset \mathbb{F}_q$ definida por*

$$\left(\frac{a}{\mathbb{F}_q}\right) := \begin{cases} 1, & \text{se } a \text{ é um quadrado em } \mathbb{F}_q^*; \\ -1, & \text{se } a \text{ não é um quadrado em } \mathbb{F}_q^*; \\ 0, & \text{se } a = 0. \end{cases} \tag{1.1.6}$$

Exemplo 1.27. Associaremos à generalização do Símbolo de Legendre, apresentada na definição anterior, a seguinte função $\chi_q : (\mathbb{F}_q^*, \times) \to \{-1, 1\} \subset \{w \in \mathbb{C} : |w| = 1\}$, dada por

$$\chi_q(a) := \begin{cases} 1_{\mathbb{C}}, & \text{se } \left(\frac{a}{\mathbb{F}_q}\right) = 1_{\mathbb{F}_q}; \\ -1_{\mathbb{C}}, & \text{se } \left(\frac{a}{\mathbb{F}_q}\right) = -1_{\mathbb{F}_q}. \end{cases} \tag{1.1.7}$$

Definido dessa forma, χ_q é um caráter multiplicativo, a prova dessa afirmação é uma aplicação direta da seguinte proposição.

Proposição 1.28. *Sejam $a \in \mathbb{F}_q$ e $\left(\frac{x}{\mathbb{F}_q}\right)$ o símbolo de Legendre generalizado. Então*

$$\left(\frac{a}{\mathbb{F}_q}\right) = a^{\frac{q-1}{2}}.$$

Demonstração. Para $a = 0$, temos $\left(\frac{0}{\mathbb{F}_q}\right) := 0 = 0^{\frac{q-1}{2}}$. Agora considere $a \in \mathbb{F}_q^*$ e observe que $a^{\frac{q-1}{2}}$ é raiz da equação $x^2 - 1 = 0$, logo $a^{\frac{q-1}{2}} \in \{\pm 1\}$. Então, para chegar ao resultado, basta provar que $a^{\frac{q-1}{2}} = 1$ se, e somente se, a é um quadrado em $\mathbb{F}_q^*$. Assuma que a é um quadrado, isto é, $a = b^2$. Então $a^{\frac{q-1}{2}} = (b^2)^{\frac{q-1}{2}} = b^{q-1} = 1$.

Por outro lado, se $a^{\frac{q-1}{2}} = 1$ e $\alpha \in \mathbb{F}_q$ é um elemento primitivo, isto é, $\mathbb{F}_q^* = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$, existe $0 \leq i \leq q-2$ tal que $a = \alpha^i$. Notemos também que $\alpha^{\frac{q-1}{2}} = -1$, já que $ord_{\mathbb{F}_q^*}(\alpha) = q - 1$. Com isso,

$$a^{\frac{q-1}{2}} = \alpha^{\frac{i(q-1)}{2}} = (-1)^i = \begin{cases} 1, \text{ se } i \text{ é par;} \\ -1, \text{ se } i \text{ é ímpar.} \end{cases}$$

Como assumimos $a^{\frac{q-1}{2}} = 1$, i tem que ser par. Assim, $a = \alpha^i = \alpha^{2k} = (\alpha^k)^2$. □

No que segue, os grupos apresentados serão munidos de multiplicação, que iremos denotar apenas pela justaposição.

Teorema 1.29 ([13], Corolário 5.3)**.** *Seja $\mathbb{G}$ um grupo abeliano finito e $g_1, g_2 \in \mathbb{G}$ dois elementos distintos. Então existe um caráter $\chi \in \widehat{\mathbb{G}}$ tal que $\chi(g_1) \neq \chi(g_2)$.*

Teorema 1.30. *Se $\chi : \mathbb{G} \to U$ é um caráter não trivial, então*

$$\sum_{g \in \mathbb{G}} \chi(g) = 0.$$

Demonstração. Como χ é não trivial, existe $h \in \mathbb{G}$ tal que $\chi(h) \neq 1$, daí

$$\chi(h)\sum_{g\in\mathbb{G}}\chi(g)=\sum_{g\in\mathbb{G}}\chi(h)\chi(g)=\sum_{g\in\mathbb{G}}\chi(hg)=\sum_{g\in\mathbb{G}}\chi(g).$$

Assim,

$$(\chi(h)-1)\sum_{g\in\mathbb{G}}\chi(g)=0,$$

o que implica em

$$\sum_{g\in\mathbb{G}}\chi(g)=0.$$

□

Corolário 1.31. *Sejam $\chi,\psi:\mathbb{G}\to U$ caracteres não triviais. Então*

$$\sum_{g\in\mathbb{G}}\chi(g)\overline{\psi(g)}=\begin{cases}0, & \text{se } \chi\neq\psi;\\ |\mathbb{G}|, & \text{se } \chi=\psi.\end{cases}$$

Demonstração. Primeiramente notemos que $\chi(x)\overline{\chi(x)}=\|\chi(x)\|=1$. Então $\chi^{-1}=\overline{\chi}$ no grupo dos caracteres $\widehat{\mathbb{G}}$. Sendo assim, se $\chi\neq\psi$, $\chi\overline{\psi}$ será um caráter não trivial. Com isso, do Teorema 1.30, segue que

$$\sum_{g\in\mathbb{G}}\chi(g)\overline{\psi(g)}=0.$$

Para o caso em que $\chi=\psi$, teremos

$$\sum_{g\in\mathbb{G}}\chi(g)\overline{\psi(g)}=\sum_{g\in\mathbb{G}}\chi(g)\overline{\chi(g)}=\sum_{g\in\mathbb{G}}\|\chi(x)\|=\sum_{g\in\mathbb{G}}1=|\mathbb{G}|.$$

□

Teorema 1.32. *Seja $\mathbb{G}$ um grupo abeliano finito e $g\in\mathbb{G}\backslash\{1\}$. Então*

$$\sum_{\chi\in\widehat{\mathbb{G}}}\chi(g)=0.$$

Demonstração. Definimos $\Phi:\widehat{\mathbb{G}}\to U$ um caráter do grupo $\widehat{\mathbb{G}}$, com $\Phi(\chi):=\chi(g)$. Pelo Teorema 1.29, existe $\psi\in\widehat{\mathbb{G}}$ tal que $\psi(g)\neq\psi(1)=1$, logo $\Phi(\psi)\neq 1$, isto é, Φ é não trivial e vale o Teorema 1.30, isto é,

$$\sum_{\chi\in\widehat{\mathbb{G}}}\chi(g)=\sum_{\chi\in\widehat{\mathbb{G}}}\Phi(\chi)=0.$$

□

Teorema 1.33. *Seja $\mathbb{G}$ um grupo abeliano finito. Então $|\widehat{\mathbb{G}}|=|\mathbb{G}|$.*

Demonstração. Pelos Teoremas 1.30 e 1.32, temos

$$|\widehat{\mathbb{G}}|=\sum_{g\in\mathbb{G}}\sum_{\chi\in\widehat{\mathbb{G}}}\chi(g)=\sum_{\chi\in\widehat{\mathbb{G}}}\sum_{g\in\mathbb{G}}\chi(g)=|\mathbb{G}|.$$

□

Teorema 1.34. *Seja $\mathbb{G}$ um grupo abeliano finito e $g, h \in \mathbb{G}$. Então*

$$\sum_{\chi \in \widehat{\mathbb{G}}} \chi(g)\overline{\chi(h)} = \begin{cases} 0, & \text{se } g \neq h; \\ |\mathbb{G}|, & \text{se } g = h. \end{cases}$$

Demonstração. Primeiramente observemos um fato geral sobre caracteres: $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_{\mathbb{G}}) = 1 = \chi(g)\overline{\chi(g)}$, logo $\chi(g^{-1}) = \overline{\chi(g)}$. Sendo assim, se $g \neq h$, basta utilizarmos o resultado do Teorema 1.32 no elemento gh^{-1} para obtermos

$$\sum_{\chi \in \widehat{\mathbb{G}}} \chi(g)\overline{\chi(h)} = \sum_{\chi \in \widehat{\mathbb{G}}} \chi(g)\chi(h^{-1}) = \sum_{\chi \in \widehat{\mathbb{G}}} \chi(gh^{-1}) = 0.$$

Para $g = h$, segue do Teorema 1.33 que

$$\sum_{\chi \in \widehat{\mathbb{G}}} \chi(g)\overline{\chi(g)} = \sum_{\chi \in \widehat{\mathbb{G}}} 1 = |\widehat{\mathbb{G}}| = |\mathbb{G}|.$$

□

Corolário 1.35. *Seja $f : \mathbb{F}_q \to \mathbb{F}_q$ e $N_a := |\{x \in \mathbb{F}_q : f(x) = a\}|$. Então*

$$N_a = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \sum_{\chi \in \widehat{\mathbb{F}_q}} \chi(f(x))\overline{\chi(a)}.$$

Demonstração. Pelo Teorema 1.34, temos:

$$\frac{1}{q} \sum_{x \in \mathbb{F}_q} \sum_{\chi \in \widehat{\mathbb{F}_q}} \chi(f(x))\overline{\chi(a)} = \frac{1}{q} \sum_{\substack{x \in \mathbb{F}_q \\ f(x)=a}} |\mathbb{F}_q| + \frac{1}{q} \sum_{\substack{x \in \mathbb{F}_q \\ f(x)\neq a}} 0 = \sum_{\substack{x \in \mathbb{F}_q \\ f(x)=a}} 1 = |\{x \in \mathbb{F}_q : f(x) = a\}| = N_a.$$

□

Visando facilitar o entendimento sobre os resultados apresentados até aqui sobre caracteres, apresentaremos uma aplicação.

Aplicação 1.36. Para toda função $f : \mathbb{F}_q^n \to \mathbb{F}_q$, definimos

$$N(f(x_1, \ldots, x_n) = 0) := |\{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : f(a_1, \ldots, a_n) = 0\}|, \tag{1.1.8}$$

isto é, $N(f(x_1, \ldots, x_n) = 0)$ é o número de soluções de $f(x_1, \ldots, x_n) = 0$ em $\mathbb{F}_q^n$. Podemos perguntar, por exemplo, qual o valor de $N(x^2 + y^2 = 1)$. A resposta para essa pergunta pode ser encontrada usando o caráter multiplicativo χ_q, apresentado no Exemplo 1.27, e os teoremas apresentados até aqui. Antes, observamos que contar as soluções de $x^2 + y^2 = 1$ é o mesmo que contar:

- quatro vezes as soluções de $a + b = 1$, considerando apenas os elementos $a, b \in \mathbb{F}_q^*$ que são quadrados, uma vez que teremos as soluções $(\pm\sqrt{a}, \pm\sqrt{b})$;
- mais as soluções $(x, y) = (\pm 1, 0)$ e $(0, \pm 1)$.

Usando o fato que

$$1+\chi_q(a)=\begin{cases} 1, \text{ se } a=0; \\ 2, \text{ se } a\in\mathbb{F}_q^* \text{ é um quadrado}; \\ 0, \text{ se } a\in\mathbb{F}_q^* \text{ não é um quadrado}, \end{cases}$$

podemos escrever

$$N(x^2+y^2=1)=\sum_{\substack{a,b\in\mathbb{F}_q\\ a+b=1}}\big(1+\chi_q(a)\big)\big(1+\chi_q(b)\big)=\sum_{\substack{a,b\in\mathbb{F}_q\\ a+b=1}}1+\sum_{\substack{a,b\in\mathbb{F}_q\\ a+b=1}}\chi_q(a)+\sum_{\substack{a,b\in\mathbb{F}_q\\ a+b=1}}\chi_q(b)+\sum_{\substack{a,b\in\mathbb{F}_q\\ a+b=1}}\chi_q(ab).$$

Donde o primeiro somatório vale q, o segundo e o terceiro, pelo Teorema 1.30, valem zero e para o último temos:

$$\sum_{\substack{a,b\in\mathbb{F}_q\\ a+b=1}}\chi_q(ab)=\sum_{a\in\mathbb{F}_q}\chi_q\big(a(1-a)\big)=\sum_{\substack{a\in\mathbb{F}_q\\ a\notin\{0,1\}}}\chi_q(a^2)\chi_q(a^{-1}-1)=\sum_{\substack{x\in\mathbb{F}_q\\ x\neq -1}}\chi_q(x).$$

Usando os Teorema 1.30 e Proposição 1.28, juntamente com a definição de χ_q apresentada no Exemplo 1.27, temos

$$\sum_{\substack{x\in\mathbb{F}_q\\ x\neq -1}}\chi_q(x)=-\chi_q(-1)=(-1)^{\frac{q-1}{2}}.$$

Daí segue que

$$N(x^2+y^2=1)=q-(-1)^{\frac{q-1}{2}}.$$

1.1.4 Curvas Elípticas

Assim como em corpos infinitos, o estudo de soluções de curvas em corpos finitos é importante e aparece em diversos problemas. Os teoremas que apresentaremos nesta seção serão utilizados na contagem de binômios de permutação, que será feita no Capítulo 2. Para isso, precisaremos do conceito de curva elíptica.

Definição 1.37. *Se $f(x_1,\ldots,x_n)\in\mathbb{F}_q[x_1,\ldots,x_n]$ e definimos $E: f(x_1,\ldots,x_n)=0$, o conjunto de pontos em $\mathbb{F}_q^n$ que são raízes de f. Chamamos E de hipersuperfície.*

Para $n=2$ e $n=3$, uma hipersuperfície é chamada de curva e superfície, respectivamente.

Definição 1.38. *Sejam $f(x_1,\ldots,x_n)\in\mathbb{F}_q[x_1,\ldots,x_n]$ e $E: f(x_1,\ldots,x_n)=0$ uma hipersuperfície sobre $\mathbb{F}_q$. Definimos*

$$E(\mathbb{F}_q):=\{(a_1\ldots,a_n)\in\mathbb{F}_q^n : f(a_1\ldots,a_n)=0\}\cup\{\infty\},$$

o conjunto de pontos que estão na hipersuperfície.

Definição 1.39. *Seja $f(x,y) \in \mathbb{F}_q[x,y]$. Consideremos a curva*

$$E : f(x,y) = 0$$

com $a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_q$. Um ponto $p \in E(\mathbb{F}_q)$ é um ponto de singularidade se $\frac{\partial f}{\partial x}(p) = 0$ e $\frac{\partial f}{\partial y}(p) = 0$.

Se uma curva não possui pontos de singularidade, dizemos que a curva é não singular.

Definição 1.40. *Se $a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_q$, a curva*

$$E : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5,$$

é chamada de curva elíptica se for não singular.

Em corpos com característica diferente de 2 e 3, podemos fazer uma mudança de variáveis afim para transformar $E : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$ em $E' : y^2 = x^3 + Ax + B$, com $A, B \in \mathbb{F}_q$. Com essa mudança, as condições necessárias para que E seja uma curva elíptica se resumem em $char(\mathbb{F}_q) \nmid 16(4A^3 + 27B^2)$. Essa nova forma nos permite enunciar um teorema importante envolvendo o número de pontos em curvas elípticas sobre $\mathbb{F}_q$. Para provarmos tal resultado, precisaremos do seguinte lema.

Lema 1.41. *Se $k \in \mathbb{Z}^+$, então vale*

$$\sum_{a \in \mathbb{F}_q} a^k = \begin{cases} 0, \ \textit{se } q-1 \nmid k \ \textit{ou } k = 0; \\ -1 \ \textit{se } q-1 \mid k \ \textit{e } k \neq 0, \end{cases}$$

onde $0^0 := 1$.

Demonstração. Seja $S_k := \sum_{a \in \mathbb{F}_q} a^k$. Temos

$$S_0 = \sum_{a \in \mathbb{F}_q} a^0 = \sum_{a \in \mathbb{F}_q} 1 = q = 0.$$

Se $(q-1) \mid k$, então $k = l(q-1)$ e assim

$$S_k = \sum_{a \in \mathbb{F}_q} a^{l(q-1)} = \sum_{a \in \mathbb{F}_q} (a^l)^{q-1} = 0 + \sum_{a \in \mathbb{F}_q^*} (a^l)^{q-1} = \sum_{a \in \mathbb{F}_q^*} 1 = q - 1 = -1.$$

E por fim, se $q-1 \nmid k$, tomamos $g \in \mathbb{F}_q^*$ um elemento primitivo e assim

$$g^k S_k = g^k \sum_{a \in \mathbb{F}_q} a^k = \sum_{a \in \mathbb{F}_q} (ga)^k = \sum_{a \in \mathbb{F}_q} a^k = S_k.$$

Daí segue que

$$S_k(g^k - 1) = 0,$$

e como g é um elemento primitivo, $g^k \neq 1$, que implica em $S_k = 0$. □

Ainda utilizando os caracteres, podemos provar o seguinte resultado envolvendo o número de pontos de curvas elípticas sobre corpos finitos de tamanho p primo.

Teorema 1.42. *Seja $E : y^2 = x^3 + Ax + B$ uma curva elíptica sobre $\mathbb{F}_p$. O número de pontos de E sobre $\mathbb{F}_p$ satisfaz*

$$|E(\mathbb{F}_p)| - p - 1 \equiv - \sum_{l=\lceil \frac{p-1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} \binom{\frac{p-1}{2}}{2l} \binom{2l}{\frac{p-1-2l}{2}} B^{\frac{p-1}{2}-2l} A^{3l-\frac{p-1}{2}} \pmod{p}$$

Demonstração. Utilizando a Definição 1.26 e o caráter χ_p apresentado no exemplo 1.27, temos

$$|E(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_p} [1 + \chi_p(x^3 + Ax + B)] = p + 1 + \sum_{x \in \mathbb{F}_p} \chi_p(x^3 + Ax + B).$$

Pela Proposição 1.28, temos

$$\begin{aligned}
\sum_{x \in \mathbb{F}_p} \chi_p(x^3 + Ax + B) &\equiv \sum_{x \in \mathbb{F}_p} (x^3 + Ax + B)^{\frac{p-1}{2}} \\
&\equiv \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} x^i (x^2 + A)^i B^{\frac{p-1}{2}-i} \\
&\equiv \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} B^{\frac{p-1}{2}-i} x^i \sum_{j=0}^{i} \binom{i}{j} x^{2j} A^{i-j} \\
&\equiv \sum_{i=0}^{\frac{p-1}{2}} \sum_{j=0}^{i} \binom{\frac{p-1}{2}}{i} \binom{i}{j} A^{i-j} B^{\frac{p-1}{2}-i} \sum_{x \in \mathbb{F}_p} x^{2j+i} \pmod{p}.
\end{aligned}$$

Pelo Lema 1.41, o último somatório é diferente de zero apenas se $2j + i \equiv 0 \pmod{p-1}$ e $2j + i \neq 0$, e nestes casos o valor da soma é -1. Observe que o maior valor que $2j + i$ assume é $2 \cdot \frac{p-1}{2} + \frac{p-1}{2} = \frac{3(p-1)}{2} < 2(p-1)$. Logo, apenas nos interessam os valores em que $2j + i = p - 1$, isto é

$$\begin{aligned}
\sum_{i=0}^{\frac{p-1}{2}} \sum_{j=0}^{i} \binom{\frac{p-1}{2}}{i} \binom{i}{j} A^{i-j} B^{\frac{p-1}{2}-i} \sum_{x \in \mathbb{F}_p} x^{2j+i} &\equiv - \sum_{l=\lceil \frac{p-1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} \binom{\frac{p-1}{2}}{2l} \binom{2l}{\frac{p-1-2l}{2}} B^{\frac{p-1}{2}-2l} A^{2i-\frac{p-1-2l}{2}} \\
&\equiv - \sum_{l=\lceil \frac{p-1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} \binom{\frac{p-1}{2}}{2l} \binom{2l}{\frac{p-1-2l}{2}} B^{\frac{p-1}{2}-2l} A^{3l-\frac{p-1}{2}} \pmod{p}.
\end{aligned}$$

Isso prova o enunciado. □

Associado a esse teorema, utilizaremos o resultado abaixo. Este teorema é equivalente à Hipótese de Riemann para curvas elípticas sobre corpos finitos. Sua demonstração é não trivial e pode ser encontrada em [19].

Teorema 1.43 ([19], Capítulo V)**.** *Se $E : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$ é uma curva elíptica sobre $\mathbb{F}_q$, então existe $\omega \in \mathbb{C}$, com $|\omega| = \sqrt{q}$, tal que*

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \omega^n - \overline{\omega}^n,$$

para todo $n \in \mathbb{N}$.

Os dois últimos teoremas nos permitem calcular o número de pontos de curvas elípticas sobre $\mathbb{F}_q$, como veremos na aplicação abaixo.

Aplicação 1.44. Seja $E : y^2 = x^3 + 1$ uma curva sobre $\mathbb{F}_{283^n}$. Pelo Teorema 1.42, temos

$$|E(\mathbb{F}_{283})| \equiv 1 - \binom{\frac{283-1}{2}}{\frac{283-1}{3}} \equiv 1 - \binom{141}{94} \equiv 252 \equiv -31 \pmod{283}.$$

Por outro lado, pelo Teorema 1.43, temos que $||E(\mathbb{F}_{283})| - 283 - 1| = |-\omega - \overline{\omega}| \leq \lfloor 2\sqrt{283} \rfloor = 33$. Sendo assim, $|E(\mathbb{F}_{283})| = 283 + 1 - 32 = 283 + 1 - 2\Re(\omega)$, e obtemos $\Re(\omega) = 16$. Como $|\omega| = \sqrt{283}$, segue que $\Im(\omega) = \sqrt{283 - 16^2} = 3\sqrt{3}$. Assim, novamente utilizando o Teorema 1.43, obtemos o número de pontos de E sobre qualquer extensão de $\mathbb{F}_{283}$, que é dado por

$$|E(\mathbb{F}_{283^n})| = 283^n + 1 - (16 + 3\sqrt{3}i)^n - (16 - 3\sqrt{3}i)^n.$$

Utilizaremos a ideia desta aplicação na contagem de binômios de permutação, que será feita na Seção 2.4.2.

1.1.5 Polinômios

Começaremos a apresentar os principais resultados envolvendo polinômios. Iniciaremos com Teorema de Interpolação de Lagrange.

Teorema 1.45. *(Polinômio de Interpolação de Lagrange para Corpos Finitos) Seja $\mathbb{F}_q$ um corpo e sejam $a_0, \ldots, a_n$ elementos distintos de $\mathbb{F}_q$ e $b_0, \ldots, b_n \in \mathbb{F}_q$ elementos quaisquer. Existe um único polinômio $f(x) \in \mathbb{F}_q[x]$ com grau $\leq n$ tal que $f(a_i) = b_i$, para todo $i = 0, \ldots, n$. Esse polinômio é dado por:*

$$f(x) = \sum_{i=0}^{n} b_i \prod_{j=0, j\neq i}^{n} \frac{x - a_j}{a_i - a_j}.$$

Demonstração. Note que

$$f(a_k) = \sum_{i=0}^{n} b_i \prod_{j=0, j\neq i}^{n} \frac{a_k - a_j}{a_i - a_j} = b_k \prod_{j=0, j\neq k}^{n} \frac{a_k - a_j}{a_k - a_j} = b_k, \text{ para todo } k = 0, \ldots n.$$

Agora mostraremos a unicidade. Para isso, devemos observar que fixados $a_0, \ldots, a_n$, existem q^{n+1} formas possíveis de escolher os valores dos b_i's, e para cada uma dessas escolhas existe um polinômio de interpolação de Lagrange equivalente. Mas existem apenas q^{n+1} polinômios com grau $\leq n$, daí segue a unicidade. □

Corolário 1.46. *Seja $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ uma função qualquer. Existe um único $f(x) \in \mathbb{F}_q[x]$ de grau $\leq q-1$ tal que $f(a) = \varphi(a)$, para todo $a \in \mathbb{F}_q$.*

Usualmente, utilizamos outra fórmula para esse polinômio, dada por:

$$f(x) = \sum_{a \in \mathbb{F}_q} \varphi(a)(1 - (x-a)^{q-1}). \tag{1.1.9}$$

A interpolação de Lagrange, apesar de modesta, é muito utilizada na matemática em geral, principalmente em matemática aplicada. Mas em corpos finitos a interpolação tem aplicações mais robustas, já que é possível descrever com precisão qualquer função que se deseje. Neste texto, a interpolação de Lagrange será largamente usada, em especial no Capítulo 3, onde usaremos tal técnica para descrever o número de coeficientes não nulos de determinados polinômios.

Com essa introdução sobre corpos finitos é possível perceber que, pela forma simples que apresentam, a maior parte das perguntas que são pertinentes em corpos infinitos se resolvem facilmente em corpos finitos. Quando se trata de polinômios de permutação, surgem muitas perguntas que não tem relevância em corpos infinitos, mas que aqui se mostram bastante interessantes. Parte dessas perguntas, acompanhadas de suas respostas, serão apresentadas na próxima seção. No decorrer de todo esse texto, serão apresentadas várias outras perguntas, não todas com respostas conhecidas, que instigaram e instigam os matemáticos, e que estão sendo alvo de atenção atualmente na área de Polinômios de Permutação sobre Corpos Finitos.

1.2 Polinômios de Permutação

Nesta seção, daremos algumas definições e resultados importantes sobre o tema principal deste texto. No decorrer do texto, se tornará evidente que uma das dificuldades enfrentadas por quem estuda polinômios de permutações sobre corpos finitos é encontrar famílias explícitas. Inicialmente daremos algumas condições necessárias e suficientes para que um polinômio seja uma permutação e, em seguida, apresentaremos alguns exemplos de permutações. Começaremos essa jornada definindo formalmente o que é uma permutação:

Definição 1.47. *Dizemos que um polinômio $f(x) \in \mathbb{F}_q[x]$ é de permutação sobre $\mathbb{F}_q$ se a função avaliação $val_{\mathbb{F}_q}(f) : \mathbb{F}_q \to \mathbb{F}_q$, definida como $val_{\mathbb{F}_q}(f) : x \mapsto f(x)$, permuta os elementos de $\mathbb{F}_q$.*

Teorema 1.48 ([13], Lema 7.1)**.** *Seja $f(x) \in \mathbb{F}_q[x]$ e $val_{\mathbb{F}_q}(f) : \mathbb{F}_q \to \mathbb{F}_q$ sua função avaliação. As seguintes afirmações são equivalentes:*

(i) $f(x)$ é um polinômio de permutação sobre $\mathbb{F}_q$;

(ii) A função $val_{\mathbb{F}_q}(f) : x \mapsto f(x)$ é sobrejetiva;

(iii) A função $val_{\mathbb{F}_q}(f) : x \mapsto f(x)$ é injetiva;

(iv) Para todo $a \in \mathbb{F}_q$, a equação $f(x) = a$ tem uma única solução em $\mathbb{F}_q$.

E com isso, temos de imediato o seguinte corolário.

Corolário 1.49. *Seja $f(x) \in \mathbb{F}_q[x]$ é um polinômio de permutação. Então existe $g(x) \in \mathbb{F}_q[x]$ tal que $g(f(x)) \equiv x \pmod{x^q - x}$ para todo $x \in \mathbb{F}_q$.*

Com os seguintes lemas, provaremos um resultado clássico que nos permite decidir se um polinômio é uma permutação.

Lema 1.50. *Sejam $f(x), g(x) \in \mathbb{F}_q[x]$ tais que $f(a) = g(a)$, para todo $a \in \mathbb{F}_q$. Então $f(x) \equiv g(x) \pmod{x^q - x}$.*

Demonstração. Notemos que todo $a \in \mathbb{F}_q$ é raiz do polinômio $f(x) - g(x)$. Observe também que $x^q - x$ é o polinômio de grau mínimo que tem todos os elementos de $\mathbb{F}_q$ como raízes. Com isso, concluímos que $(x^q - x)$ divide $(f(x) - g(x))$. Logo, $f(x) \equiv g(x) \pmod{x^q - x}$. □

Lema 1.51 ([13], Lema 7.3)**.** *Sejam $a_0, \dots a_{q-1} \in \mathbb{F}_q$. As seguintes afirmações são equivalentes:*

(a) $a_0, \dots a_{q-1}$ são distintos;

(b) $\displaystyle\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, \text{ para } t = 1, \dots\ q-2; \\ -1, \text{ para } t = q-1. \end{cases}$

Demonstração. Fixado $i \in \{0, \dots, q-1\}$, definimos

$$f_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j.$$

Notemos que se $a_i \neq 0$,

$$f_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} a_i^j = 1 - \sum_{j=0}^{q-1} 1 = 1 - q = 1,$$

e no caso em que $a_i = 0$, $f(0) = 1$. Observamos também que

$$f_i(b) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} b^j \text{ para todo } b \neq a_i.$$

Temos ainda:

- Se $a_i = 0$ e $b \neq 0$, então $\displaystyle\sum_{j=0}^{q-1} a_i^{q-1-j} b^j = 1$.
- Se $a_i \neq 0$ e $b = 0$, $\displaystyle\sum_{j=0}^{q-1} a_i^{q-1-j} b^j = 1$.

- Se $a_i \neq 0$, $b \neq 0$ e $a \neq b$,

$$\sum_{j=0}^{q-1} a_i^{q-1-j} b^j = \sum_{j=0}^{q-1} (a^{-1}b)^j = \sum_{j=1}^{q} (a^{-1}b)^j - (a^{-1}b)^q + (a^{-1}b)^0 = 1 - a^{-1}b + (a^{-1}b) \sum_{j=0}^{q-1} (a^{-1}b)^j,$$

e assim,

$$\sum_{j=0}^{q-1} a_i^{q-1-j} b^j = \frac{1 - a^{-1}b}{1 - a^{-1}b} = 1.$$

Com isso, $f_i(b) = 0$ para todo $b \neq a_i$. Seja

$$f(x) := \sum_{i=0}^{q-1} f_i(x) = q - \sum_{j=0}^{q-1} \left[\sum_{i=0}^{q-1} a_i^{q-1-j} \right] x^j = \sum_{j=0}^{q-1} \left[\sum_{i=0}^{q-1} a_i^{q-1-j} \right] x^j. \tag{1.2.1}$$

Notemos que $f(a) \equiv |\{0 \leq i \leq -1 : a = a_i\}| \pmod{p}$, onde p é a característica de $\mathbb{F}_q$. Sendo assim, $f(a) = 1$ para todo $a \in \mathbb{F}_q$ se, e somente se, todos $a_0, \ldots, a_{q-1}$ forem distintos. Além disso, pelo Lema 1.50 e analisando a equação (1.2.1), $f(a) = 1$ para todo $a \in \mathbb{F}_q$ se, e somente se, a condição (b) segue. Portanto, o resultado está provado. □

Teorema 1.52. *(Critério de Hermite) Seja $\mathbb{F}_q$ um corpo finito de característica p. Um polinômio $f(x) \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, os seguintes itens são verdadeiros:*

(i) $f(x) = 0$ tem apenas uma solução em $\mathbb{F}_q$;

(ii) A redução $f(x)^t \pmod{x^q - x}$ tem grau $\leq q - 2$, para todo $1 \leq t \leq q - 2$, com $t \not\equiv 0 \pmod{p}$.

Demonstração. Assumimos que $f(x)$ é um polinômio de permutação. (i) segue trivialmente. Pelo Lema 1.50, podemos assumir que $f(x)^t \equiv \sum_{i=0}^{q-1} b_i^{(t)} x^i \pmod{x^q - x}$. Para (ii), usaremos o polinômio de interpolação de Lagrange, dado por

$$f(x)^t \equiv \sum_{a \in \mathbb{F}_q} f(a)^t (1 - (x - a)^{q-1}) \pmod{x^q - x}.$$

Igualando os coeficientes de grau $q - 1$ temos que $b_{q-1}^{(t)} = -\sum_{a \in \mathbb{F}_q} f(a)^t$. Como $f(x)$ permuta os elementos de $\mathbb{F}_q$, pelo Lema 1.51,

$$\sum_{a \in \mathbb{F}_q} f(a)^t = 0, \text{ para todo } t = 1, \ldots, q - 2,$$

que implica na condição (ii).

Por outro lado, Suponha que valem (i) e (ii). De novo, pelo Lema 1.51 e a interpolação de Lagrange para $f(x)^t$, que nos mostra a igualdade $b_{q-1}^{(t)} = -\sum_{a \in \mathbb{F}_q} f(a)^t$. Notemos que (i) implica em

$$\sum_{a \in \mathbb{F}_q} f(a)^{q-1} = -1.$$

Assumindo (ii), dado $t \in \{1, \ldots, q-2\}$, com $t = mp^k$ e $\mathrm{mdc}(p, m) = 1$, teremos:

$$\sum_{a \in \mathbb{F}_q} f(a)^t = \sum_{a \in \mathbb{F}_q} f(a)^{mp^k} = \Big(\sum_{a \in \mathbb{F}_q} f(a)^m \Big)^{p^k} = \Big(- b_{q-1}^{(m)} \Big)^{p^k} = 0.$$

Logo, pelo Lema 1.51, o resultado segue. □

Corolário 1.53. *Se $d > 1$ é um divisor de $q-1$, então não existe polinômio de permutação de grau d.*

Demonstração. Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio qualquer de grau d, isto é, $f(x) = \sum_{i=0}^{d} a_i x^i$, com $a_d \neq 0$. Então $f^{\frac{q-1}{d}}(x) = a_d^{\frac{q-1}{d}} x^{q-1} + g(x)$, com $grau(g) \leq q-2$. Pelo critério de Hermite, segue que $f(x)$ não é um polinômio de permutação. Como $f(x)$ era arbitrário de grau d, concluímos que não existe polinômio de permutação de tal grau. □

Outro resultado importante dá condições necessárias e suficiente para que um polinômio seja uma permutação.

Teorema 1.54. *Um polinômio $f(x) \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se,*

$$\sum_{a \in \mathbb{F}_q} \chi(f(a)) = 0$$

para todo caráter aditivo não trivial χ de $\mathbb{F}_q$.

Demonstração. Se $f(x)$ é um polinômio de permutação, então pelo Teorema 1.30,

$$\sum_{a \in \mathbb{F}_q} \chi(f(a)) = \sum_{a \in \mathbb{F}_q} \chi(a) = 0.$$

Por outro lado, suponhamos que $\sum_{a \in \mathbb{F}_q} \chi(f(a)) = 0 = \sum_{a \in \mathbb{F}_q} \chi(a)$, para todo caráter aditivo não trivial $\chi \in \widehat{\mathbb{F}_q}$. Se $a \in \mathbb{F}_q$, definimos $N_a = |\{x \in \mathbb{F}_q : f(x) = a\}|$. Pelo Corolário 1.35,

$$\begin{aligned}
N_a &= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \Big(\sum_{\chi \in \widehat{\mathbb{F}_q}} \chi(f(x)) \overline{\chi(a)} \Big) \\
&= \frac{1}{q} \sum_{\chi \in \widehat{\mathbb{F}_q}} \overline{\chi(a)} \sum_{x \in \mathbb{F}_q} \chi(f(x)) \\
&= \frac{1}{q} \Big(\overline{\mathbb{1}_{\widehat{\mathbb{F}_q}}(a)} \sum_{x \in \mathbb{F}_q} \mathbb{1}_{\widehat{\mathbb{F}_q}}(f(x)) + \sum_{\chi \neq \mathbb{1}_{\widehat{\mathbb{F}_q}}} \overline{\chi(a)} \sum_{x \in \mathbb{F}_q} \chi(f(x)) \Big) \\
&= \frac{1}{q} \sum_{x \in \mathbb{F}_q} 1 \\
&= 1.
\end{aligned}$$

Como a foi tomado arbitrariamente, concluímos que $f(x)$ representa uma função injetiva. Segue do Teorema 1.48 que $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$. □

Tendo apresentados essas formas de distinguir polinômios que são permutações em $\mathbb{F}_q$, seguiremos apresentando exemplos simples de polinômios de permutações que são obtidos com conceitos e resultados elementares.

Teorema 1.55. *Seja $\mathbb{F}_q$ um corpo finito. As seguinte afirmações são verdadeiras:*

(i) $f(x) = ax + b \in \mathbb{F}_q[x]$ *é um polinômio de permutação para todos* $a, b \in \mathbb{F}_q$*, com* $a \neq 0$*;*

(ii) $f(x) = x^n \in \mathbb{F}_q[x]$ *é um polinômio de permutação se, e somente se,* $\text{mdc}(n, q-1) = 1$.

Demonstração. (i) $ax + b$ é invertível, com inversa $\frac{x-b}{a}$, logo é uma permutação.
(ii) Note que o 0 é deixado fixo, uma vez que $f(0) = 0^n = 0$. Para os elementos de $\mathbb{F}_q^*$ utilizaremos o fato deste ser cíclico gerado por algum elemento $g \in \mathbb{F}_q^*$. Sejam $i, j \in \{1, \ldots, q-1\}$, então as seguintes implicações são verdadeiras:

$$\begin{aligned} x^n \text{ é Polinômio de Permutação } &\Leftrightarrow g^{in} \neq g^{jn}, \text{ para todo } i \neq j \\ &\Leftrightarrow g^{n(i-j)} \neq 1, \text{ para todo } i \neq j \\ &\Leftrightarrow n(i-j) \not\equiv 0 \pmod{q-1}, \text{ para todo } i \neq j \\ &\Leftrightarrow \text{mdc}(n, q-1) = 1. \end{aligned}$$

□

1.3 Grupos de Polinômios de Permutação

Nesta seção estaremos interessados em discutir as propriedades do conjunto de polinômios de permutação de $\mathbb{F}_q$, que denotaremos por $S(\mathbb{F}_q)$.

Teorema 1.56. *O conjunto $S(\mathbb{F}_q)$, munido de composição de polinômios, seguida de redução* $\pmod{x^q - x}$*, é um grupo.*

Demonstração. Utilizando o Teorema 1.48 e Lema 1.50, concluímos que $S(\mathbb{F}_q)$ é fechado para composição. Associatividade segue trivialmente. O elemento neutro da composição é $f(x) = x$. Por fim, se $f(x) \in S(\mathbb{F}_q)$, pelo Corolário 1.49, existe $g(x) \in S(\mathbb{F}_q)$ tal que $g(f(x)) \equiv x \pmod{x^q - x}$. □

Pelo Corolário 1.46, existe polinômio para representar qualquer permutação que se deseje em $\mathbb{F}_q$. Sendo assim, $S(\mathbb{F}_q)$ é isomorfo ao grupo de permutação de q elementos S_q. Isso é animador, uma vez que as propriedades de S_q são amplamente conhecidas. Uma das propriedades mais importantes, e que será útil, é o seguinte resultado.

Teorema 1.57 ([7], Lema 2.10.2)**.** *Toda permutação é produto de 2-ciclos.*

De fato, é possível reduzir ainda mais o número de geradores, observando que $(ab) = (1a)(1b)(1a)$. Traduzindo esse resultado para $S(\mathbb{F}_q)$, temos que qualquer polinômio de

permutação pode ser escrito como composição de polinômios de permutação que trocam apenas 0 e $a \in \mathbb{F}_q^*$.

Motivado a estudar propriedades do grupo de polinômios de permutações $S(\mathbb{F}_q)$, no ano de 1953, L. Carlitz [4] provou o seguinte resultado.

Teorema 1.58. *Se $f(x) \in S(\mathbb{F}_q)$, com $q \geq 3$, então $f(x)$ pode ser expresso como composições de polinômios lineares $ax + b$, $a, b \in \mathbb{F}_q$, com $a \neq 0$, e inversões x^{q-2}.*

Demonstração. Primeiramente, definimos

$$f_a(x) := -a^2\left[\left((x-a)^{q-2} + a^{-1}\right)^{q-2} - a\right]^{q-2},$$

e observamos que $f_a(a) = 0$ e $f_a(0) = a$. E também, para todo $x \in \mathbb{F}_q \backslash \{0, a\}$, temos

$$\begin{aligned} f_a(x) &= -a^2\left[\left((x-a)^{q-2} + a^{-1}\right)^{q-2} - a\right]^{q-2} \\ &= -a^2\left[\left((x-a)^{-1} + a^{-1}\right)^{q-2} - a\right]^{q-2} \\ &= -a^2\left[\left(\frac{x}{(x-a)a}\right)^{-1} - a\right]^{q-2} \\ &= -a^2\left[\frac{(x-a)a - ax}{x}\right]^{q-2} \\ &= x. \end{aligned}$$

Com isso, basta utilizar o Teorema 1.57 para obtermos o resultado desejado. □

Corolário 1.59. *Se $q \geq 3$ e α é um elemento primitivo de $\mathbb{F}_q$, então $S(\mathbb{F}_q)$ é gerado por $f(x) := \alpha x$, $x + 1$ e x^{q-2}.*

Demonstração. Pelo teorema anterior, basta mostrar que $ax + b$, com $a, b \in \mathbb{F}_q$, pode ser escrito como composição de funções da forma αx, $x + 1$ e x^{q-2}. Sabemos que existem $t_a, t_b \in \mathbb{N}$ tais que $a = \alpha^{t_a}$, $b = \alpha^{t_b}$ e $t_a \geq t_b \geq 1$. Denotaremos a composição de $f(x)$, com ele mesmo, s vezes por $f^{(s)}(x)$. Assim, se $b \neq 0$,

$$ax + b = f^{(t_b)}\big(f^{(t_a - t_b)}(x) + 1\big).$$

Para $b = 0$, basta observar que

$$ax = f^{(t_a)}(x).$$

Com isso, o resultado segue do Teorema 1.58. □

Exemplo 1.60. Tome o polinômio $f(x) = x^7 + 2x^6 + 2x^4 + 2x^2 \in \mathbb{F}_9[x]$. Para verificar se $f(x)$ é um polonômio de permutação sobre $\mathbb{F}_9$ poderíamos usar o Critério de Hermite 1.52

ou o Teorema 1.54 ou simplesmente calcular o valor de $f(a)$ para todo $a \in \mathbb{F}_9$. Mas, se observamos que

$$\begin{aligned} f(x) &\equiv x^7 + 2x^6 + 2x^4 + 2x^2 \\ &\equiv (x^7 + 2x^6 + 2x^5 + x^4 + x + 3)^7 \\ &\equiv ((x^7 + 2x^6 + x^4 + 2x^3 + x + 4)^7 + 2)^7 \\ &\equiv (((x+2)^7 + 2)^7 + 2)^7 \pmod{x^9 - x}, \end{aligned}$$

segue imediatamente, do Teorema 1.58, que $f(x)$ é um polinômio de permutação de $\mathbb{F}_9$.

CAPÍTULO 2

Classes de Polinômios de Permutação

No primeiro capítulo, mostramos formas de decidir se um polinômio é uma permutação sobre $\mathbb{F}_q$. Mas, computacionalmente, seria interessante conhecer classes de polinômios que sempre fossem permutações se o corpo finito satisfizesse hipóteses de fácil verificação, de forma que não se faça necessário checar se todas as hipóteses apresentadas no Teorema 1.52 (Critério de Hermite) são satisfeitas. Com essa preocupação, surgem diversas conjecturas (por exemplo, ver [11] e [10]), algumas das quais já foram comprovadas, e serão apresentadas neste capítulo, juntamente com referências onde poderão ser encontrados diversos outros resultados.

2.1 Polinômios de Permutação Clássicos

Nesta seção, apresentaremos os primeiros resultados importantes envolvendo polinômios de permutações sobre corpos finitos e que também serão utilizados nas próximas seções. Como já havíamos observado no Teorema 1.10, se $q = p^n$, então $\mathbb{F}_q$ é um espaço vetorial sobre $\mathbb{F}_p$. E quando se fala em espaços vetoriais, muito se sabe. Exploraremos então um fato conhecido de álgebra linear sobre transformações lineares: uma transformação linear é injetiva se, e somente se, o seu núcleo é trivial. Sabendo disso, vamos ao enunciado. De fato, esse resultado é consequência imediata do Teorema do Núcleo e Imagem.

Teorema 2.1. *Seja $\mathbb{F}_q$ um corpo finito de característica p. O polinômio*

$$f(x) = \sum_{i=0}^{m} a_i x^{p^i},\ a_i \in \mathbb{F}_q,$$

chamado de polinômio linearizado, é um polinômio de permutação sobre $\mathbb{F}_q$ se, e somente se, $f(x)$ não possui raízes não nulas.

Demonstração. Como já observamos no Teorema 1.10, $\mathbb{F}_q$ é um espaço vetorial sobre $\mathbb{F}_p$. Então, se mostrarmos que $f(x)$ é uma transformação $\mathbb{F}_p$-linear, o resultado seguirá do Teorema do Núcleo e Imagem para transformações lineares. Observamos, pelo Lema 1.17, que

$$f(x+y) = \sum_{i=0}^{m} a_i(x+y)^{p^i} = \sum_{i=0}^{m} a_i(x^{p^i}+y^{p^i}) = \sum_{i=0}^{m} a_i x^{p^i} + \sum_{i=0}^{m} a_i y^{p^i} = f(x)+f(y), \forall x, y \in \mathbb{F}_q.$$

Além disso, para todo $\lambda \in \mathbb{F}_p$ e $j \in \mathbb{N}$, $\lambda^{p^j} = \lambda$, assim

$$f(\lambda x) = \sum_{i=0}^{m} a_i(\lambda x)^{p^i} = \sum_{i=0}^{m} a_i \lambda x^{p^i} = \lambda \sum_{i=0}^{m} a_i x^{p^i} = \lambda f(x), \text{ para todo } x \in \mathbb{F}_q, \ \lambda \in \mathbb{F}_p.$$

Concluímos que $f(x)$ é uma transformação $\mathbb{F}_p$-linear. Como uma transformação linear é injetiva se, e somente se, o seu núcleo é trivial, pelo Teorema 1.48, concluímos que $f(x)$ será uma permutação se, e somente se, zero for a única raiz de $f(x)$ em $\mathbb{F}_q$. □

Como vimos nesse teorema, todo polinômio $f(x) = \sum_{i=0}^{m} a_i x^{p^i}$, com $a_i \in \mathbb{F}_q$ é uma transformação $\mathbb{F}_p$-linear em $\mathbb{F}_q$. De fato, polinômios dessa forma representam todas as transformações $\mathbb{F}_p$-lineares em $\mathbb{F}_q$, como veremos no Teorema 2.6. Com o propósito de provar tal teorema, apresentaremos alguns resultados envolvendo bases de $\mathbb{F}_q$ como $\mathbb{F}_p$-espaço vetorial. Começaremos pela seguinte definição.

Definição 2.2. *Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_{q^n}$ qualquer extensão. Uma base da forma $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para algum $\alpha \in \mathbb{F}_{q^n}$ adequado, é dita base normal e α é chamado de elemento normal.*

Associada a essa definição é comum encontrar o seguinte resultado, cuja demonstração pode ser consultada na referência.

Teorema 2.3 ([13], Teorema da Base Normal)**.** *Para qualquer corpo finito $\mathbb{F}_q$ e qualquer extensão $\mathbb{F}_{q^n}$, existe uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Esse teorema mostra que sempre existe uma base normal. Mas, como saber se um elemento é normal? A resposta para essa pergunta é uma aplicação do seguinte teorema, cuja demostração também pode ser encontrada em [13].

Teorema 2.4 ([13], Corolário 2.38)**.** *Sejam $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^n}$. Então $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se,*

$$\det \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \alpha_3^q & \ldots & \alpha_n^q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \alpha_3^{q^{n-1}} & \ldots & \alpha_n^{q^{n-1}} \end{bmatrix} \neq 0.$$

Observação 2.5. Pelo Teorema 2.4, uma condição necessária e suficiente para um elemento $\alpha \in \mathbb{F}_{q^n}$ ser normal é que

$$\det \begin{bmatrix} \alpha & \alpha^q & \alpha^{q^2} & \dots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \dots & \alpha^{q^{n-2}} \end{bmatrix} \neq 0.$$

Teorema 2.6. *Seja $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ uma transformação $\mathbb{F}_q$-linear. Então existem únicos $a_1, \dots, a_n \in \mathbb{F}_{q^n}$ tais que*

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i},\ a_i \in \mathbb{F}_{q^n}.$$

Demonstração. Sabemos que uma transformação linear é unicamente determinada pela imagem dos elementos da base. Sendo assim, o primeiro passo é fixar uma base. Pelo Teorema 2.3, existe um elemento normal $\alpha \in \mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ (isto é, $\{\alpha, \dots \alpha^{q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$). Se definirmos $b_j := f(\alpha^{q^j})$, para provar esse teorema basta encontrar $a_0, \dots, a_n \in \mathbb{F}_{q^n}$ tais que

$$f(\alpha^{q^j}) = \sum_{i=0}^{n-1} a_i (\alpha^{q^j})^{q^i} = \sum_{i=0}^{n-1} a_i \alpha^{q^{j+i}} = b_j,$$

que pode ser reescrito como

$$\begin{bmatrix} \alpha & \alpha^q & \alpha^{q^2} & \dots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \dots & \alpha^{q^{n-2}} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}. \tag{2.1.1}$$

Pelo Teorema 2.4, como α é um elemento normal, temos

$$\det \begin{bmatrix} \alpha & \alpha^q & \alpha^{q^2} & \dots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \dots & \alpha^{q^{n-2}} \end{bmatrix} \neq 0.$$

Logo, o sistema linear de equações (2.1.1) tem exatamente uma solução $[a_0, \dots, a_{n-1}]^T$. □

Depois de termos discutido os resultados básicos envolvendo os polinômios que são transformações lineares, passaremos aos resultados envolvendo polinômios gerais. Contudo, para entender a motivação dos próximos resultados, começaremos pela seguinte proposição.

Proposição 2.7. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio qualquer com grau $n \leq q-1$. Então $f(x)$ pode ser escrito na forma $ax^r h(x^{\frac{q-1}{m}}) + b$, com $h(x) \in \mathbb{F}_q[x]$ mônico, com $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, $r, m \in \mathbb{N}$ e $m|(q-1)$. Além disso, $h(x)$ satisfaz a seguinte propriedade: se $h(x) = g(x^k)$ para algum $g(x) \in \mathbb{F}_q[x]$ e $k \geq 1$, então* $\mathrm{mdc}(k, m) = 1$.

Demonstração. Sabemos que

$$f(x) = a_n(x^n + a_{n-n_1}x^{n-n_1} + \ldots + a_{n-n_k}x^{n-n_k}) + b, \tag{2.1.2}$$

onde $a_n, a_{n-n_j} \neq 0$ e $n_j \leq n\,, j = 1, \ldots k$. Agora, façamos $r := n - n_k$ e definamos

$$d := \mathrm{mdc}(n-r, n-n_1-r, \ldots, n-n_{k-1}-r, q-1), \tag{2.1.3}$$

e $m := \frac{q-1}{d}$. Assim,

$$f(x) = ax^r h(x^{\frac{q-1}{m}}) + b. \tag{2.1.4}$$

Onde $h(x) = x^{e_0} + a_{n-n_1}x^{e_1} + \ldots + a_{n-n_{k-1}}x^{e_{k-1}} + a_{n-n_k}$, $e_0 = \frac{n-r}{d}$ e $e_j = \frac{n-n_j-r}{d}$, com $j = 1, \ldots k$. Além disso, $\mathrm{mdc}(e_0, \ldots, e_{k-1}, \frac{q-1}{d}) = 1$. □

Notemos que, pelos Teoremas 1.55 e 1.56, $f(x) = ax^r h(x^{\frac{q-1}{m}}) + b$ é um polinômio de permutação se, e somente se, $x^r h(x^{\frac{q-1}{m}})$ é um polinômio de permutação. Tendo isso em mente, fica claro que basta considerar os polinômios dessa forma. Sabendo disso, alguns autores começaram a explorar os polinômios de permutações para encontrar condições necessárias e suficientes para dizer se um polinômio é uma permutação de $\mathbb{F}_q$. Dentre esses resultados encontra-se o que apresentaremos a seguir, apresentado originalmente por Daqing Wan e Rudolf Lidl [21] e reescrito, da forma como enunciaremos aqui, por Yann Laigle-Chapuy [9]. Para a prova do resultado, precisaremos da seguinte definição.

Definição 2.8. *Seja α um elemento primitivo de $\mathbb{F}_q$ e $w \in \mathbb{F}_q^*$, o logaritmo discreto de w na base α, escrito como* $\log_\alpha(w)$*, é o menor inteiro não-negativo n tal que $w = \alpha^n$.*

Teorema 2.9 ([21], Teorema 1.2, [9], Teorema 2.2)**.** *Sejam α um elemento primitivo de $\mathbb{F}_q$, $m, r \in \mathbb{Z}^+$ tais que $m|(q-1)$ e $h(x) \in \mathbb{F}_q[x]$. Então, $f(x) := x^r h(x^{\frac{q-1}{m}})$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, as seguintes condições são satisfeitas:*

(i) $\mathrm{mdc}\left(r, \frac{q-1}{m}\right) = 1$*;*

(ii) $h(\alpha^{i\frac{q-1}{m}}) \neq 0$*, para todo i;* $0 \leq i < m$*;*

(iii) $f(\alpha^i)^{\frac{q-1}{m}} \neq f(\alpha^j)^{\frac{q-1}{m}}$*, para todo i, j;* $0 \leq i < j < m$.

Demonstração. Primeiramente, observamos que se $f(x)$ é um polinômio de permutação, então 0 deve ser a sua única raiz e, com isso, concluímos que (ii) é necessário. Sendo assim, podemos assumir que (ii) é verdade, de forma que $f(x)$ será uma permutação se, e somente se, (i) e (iii) forem satisfeitas. Tendo adicionado essa hipótese, resta mostrar que $f(x)$

permuta os elementos de $\mathbb{F}_q^*$. E isso equivale a dizer que $f(\alpha^k) = \alpha^{kr+\log_\alpha(h(\alpha^k\frac{q-1}{m}))}$ gera valores distintos para $0 \leq k < q-1$. Note que k tem uma única representação da forma

$$k = i + mj, \text{ com } 0 \leq i \leq m-1 \text{ e } 0 \leq j \leq \tfrac{q-1}{m} - 1. \tag{2.1.5}$$

Sendo assim, para que $f(x)$ seja um polinômio de permutação é necessário (e suficiente) que $l_{i,j} := (i+mj)r + \log_\alpha(h(\alpha^{(i+mj)\frac{q-1}{m}})) = mjr + ir + \log_\alpha(h(\alpha^{i\frac{q-1}{m}}))$ assuma todos os restos módulo $q-1$. De fato, fixando i, mjr assume valores distintos módulo $q-1$ se, e somente se, $\text{mdc}(r, \frac{q-1}{m}) = 1$. Logo, $l_{i,j}$ assume todos os valores módulo $q-1$ se, e somente se, $\text{mdc}\left(r, \frac{q-1}{m}\right) = 1$ e $ir + \log_\alpha(h(\alpha^{i\frac{q-1}{m}}))(0 \leq i \leq m-1)$ percorre todos os restos módulo m. O primeiro equivale ao item (i) e o segundo é o mesmo que dizer que:

$$\log_\alpha\left(\frac{h(\alpha^{i\frac{q-1}{m}})}{h(\alpha^{j\frac{q-1}{m}})}\right) \not\equiv r(j-i) \pmod m \ \forall\ 0 \leq i < j < m, \tag{2.1.6}$$

ou ainda,

$$\left(\frac{h(\alpha^{i\frac{q-1}{m}})}{h(\alpha^{j\frac{q-1}{m}})}\right)^{\frac{q-1}{m}} \neq \alpha^{r(j-i)\frac{q-1}{m}} \ \forall\ 0 \leq i < j < m. \tag{2.1.7}$$

Que é o mesmo que

$$f(\alpha^i)^{\frac{q-1}{m}} \neq f(\alpha^j)^{\frac{q-1}{m}}, \forall\ i, j;\ 0 \leq i < j < m. \tag{2.1.8}$$

Assim, o teorema está provado. □

Como caso particular do teorema anterior, mostraremos o seguinte resultado, que pode ser encontrado em [13].

Corolário 2.10 ([13], Teorema 7.10, [21], Corolário 1.4)**.** *Sejam α um elemento primitivo de $\mathbb{F}_q$, $m, r \in \mathbb{Z}^+$, tais que $m|(q-1)$ e $\text{mdc}(r, q-1) = 1$ e $h(x) \in \mathbb{F}_q[x]$. Então, $f(x) := x^r h(x^{\frac{q-1}{m}})^m$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $h(x^{\frac{q-1}{m}})$ não tem raízes em $\mathbb{F}_q^*$.*

Demonstração. Assumindo que $f(x)$ é um polinômio de permutação, segue do Teorema 2.9 que $h(x^{\frac{q-1}{m}})$ não poderá se anular em $\mathbb{F}_q^*$.

Reciprocamente, assumindo que $h(x^{\frac{q-1}{m}})$ não tem raízes em $\mathbb{F}_q^*$, que é equivalente à condição (ii) no Teorema 2.9, e teremos ainda, no caso em que α é um elemento primitivo de $\mathbb{F}_q$ que:

$$f(\alpha^i)^{\frac{q-1}{m}} = \alpha^{ir} h(\alpha^{i\frac{q-1}{m}})^m{}^{\frac{q-1}{m}} = \alpha^{ir} \neq \alpha^{jr} = f(\alpha^j)^{\frac{q-1}{m}}, \forall\ i, j;\ 0 \leq i < j < m.$$

Com isso, pelo Teorema 2.9, segue que $f(x)$ é um polinômio de permutação. □

Note que esse enunciado é mais forte que o apresentado em [13], uma vez que a recíproca é verdadeira.

Exemplo 2.11. Seja $\mathbb{F}_q$ um corpo finito com $q \equiv 1 \pmod 3$. Tome $f(x) = x^r h(x^{\frac{q-1}{3}})^3$. Pelo Lema 1.50, basta considerar $h(x)$ da forma $x^2 + ax + b \in \mathbb{F}_q[x]$. Utilizaremos o Corolário 2.10 para verificar quando $f(x)$ é um polinômio de permutação sobre $\mathbb{F}_q$. Pelo resultado apresentado no corolário, basta verificar se as raízes cúbicas da unidade são raízes do polinômio $h(x)$. Suponhamos que as raízes cúbicas da unidade são $1, \lambda_1$ e λ_2. Uma condição necessária para que $f(x)$ seja um polinômio de permutação de $\mathbb{F}_q$ é que $h(1) = 1 + a + b$ seja diferente de zero. Para as raízes restantes, observamos que

$$\lambda_i^2 + \lambda_i + 1 = \tfrac{\lambda_i^3 - 1}{\lambda_i - 1} = 0,$$

isto é, $\lambda_i^2 = -1 - \lambda_i$, para $i \in \{1, 2\}$. Sendo assim,

$$f(\lambda_i) = \lambda_i^2 + a\lambda_i + b = -1 - \lambda_i + a\lambda_i + b = \lambda_i(a-1) + b - 1.$$

Como precisamos que $f(\lambda_i) \neq 1$, outra condição necessária para que $f(x)$ seja um polinômio de permutação é que

$$\frac{1-b}{a-1} \neq \lambda_i, \text{ para } i \in \{1, 2\}.$$

Depois de provar tais resultados, Daquing Wan e Rudolf Lidl perceberam que era possível generalizar o resultado para polinômios da forma $x^r h(x^s)$. Mas antes de apresentar esse resultado, observamos que se $\mathrm{mdc}(r, s, q-1) = d > 1$, então $x^r h(x^s)$ será um polinômio em x^d e, portanto, não será um polinômio de permutação, uma vez que todas raízes d-ésimas da unidade terão a mesma imagem.

Teorema 2.12 ([21], Teorema 1.8)**.** *Seja α um elemento primitivo de $\mathbb{F}_q$ e sejam $r, s, m \in \mathbb{Z}^+$ tais que $\mathrm{mdc}(r, s, q-1) = 1, m|(q-1)$ e $\mathrm{mdc}(s, q-1) = \frac{q-1}{m}$. Se $k \in \mathbb{Z}^+$ primo relativo com $q-1$ é tal que $sk \equiv \frac{q-1}{m} \pmod{q-1}$, então o polinômio $f(x) := x^r h(x^s)$ é um polinômio de permutação se, e somente se, as seguintes condições são satisfeitas:*

i. $h(\alpha^{i\frac{q-1}{m}}) \neq 0$, *para todo* i; $0 \leq i < m$;

ii. $\left(\alpha^{irk} h(\alpha^{i\frac{q-1}{m}})\right)^{\frac{q-1}{m}} \neq \left(\alpha^{jrk} h(\alpha^{j\frac{q-1}{m}})\right)^{\frac{q-1}{m}}$, *para todo* i, j; $0 \leq i < j < m$.

Demonstração. Como $\mathrm{mdc}(k, q-1) = 1$, pelo Teorema 1.55, x^k é um polinômio de permutação e, portanto, pelo Teorema 1.56, $f(x^k) = x^{rk} h(x^{sk})$ também é uma permutação. Notemos também que:

$$f(x^k) = x^{rk} h(x^{sk}) \equiv x^{rk} h(x^{\frac{q-1}{m}}) \pmod{x^q - x}. \tag{2.1.9}$$

E por fim, as hipóteses $\mathrm{mdc}(k, q-1) = 1$, $\mathrm{mdc}(s, q-1) = \frac{q-1}{m}$ e $\mathrm{mdc}(r, s, q-1) = 1$, implicam em $\mathrm{mdc}(rk, \frac{q-1}{m}) = 1$. Com isso, as hipóteses (ii) e (iii) do Teorema 2.9 se traduzem nas hipóteses (i) e (ii) deste teorema. Assim, o resultado está provado. □

Inspirado pelo Teorema 2.9, Michael E. Zieve apresenta o mesmo resultado em [22], mas com condições ligeiramente diferentes. Apesar de o resultado ser semelhante, apresentaremos novamente o resultado, por conter uma prova diferente.

Definição 2.13. *Seja $d \in \mathbb{Z}^+$. Denotamos por μ_d o conjunto de raízes d-ésimas da unidade em $\mathbb{F}_q$.*

Note que se $d|(q-1)$ e α é um elemento primitivo de $\mathbb{F}_q$, $\mu_d = \{\alpha^{i\frac{q-1}{d}} : 0 \leq i < d\}$.

Teorema 2.14 ([22], Lema 2.1)**.** *Sejam α um elemento primitivo de $\mathbb{F}_q$, $m, r \in \mathbb{Z}^+$ tais que $m|(q-1)$ e $h(x) \in \mathbb{F}_q[x]$. Então, $f(x) := x^r h(x^{\frac{q-1}{m}})$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, as seguintes condições são satisfeitas:*

i. $\text{mdc}\left(r, \frac{q-1}{m}\right) = 1$;

ii. $x^r h(x)^{\frac{q-1}{m}}$ *permuta* μ_m.

Demonstração. O primeiro fato que observamos é que se $\xi \in \mu_{\frac{q-1}{m}} = \{\alpha^{im} : 0 \leq i < \frac{q-1}{m}\}$, então

$$f(\xi x) = \xi^r f(x). \tag{2.1.10}$$

Portanto, para que $f(x)$ seja um polinômio de permutação, é necessário que $\xi^r = \alpha^{imr}$ nunca seja 1, quando $0 < i < \frac{q-1}{m}$, e isso acontece justamente quando $\text{mdc}\left(r, \frac{q-1}{m}\right) = 1$. Reciprocamente, se assumimos que $\text{mdc}\left(r, \frac{q-1}{m}\right) = 1$, pelo que já foi observado em (2.1.10), os valores das imagens de f em $\mathbb{F}_q$ são todas as raízes $\frac{q-1}{m}$-ésimas dos valores de

$$f(x)^{\frac{q-1}{m}} = x^{r\frac{q-1}{m}} h(x^{\frac{q-1}{m}})^{\frac{q-1}{m}}. \tag{2.1.11}$$

Mas os valores não nulos de $f(x)^{\frac{q-1}{m}}$ são os valores da forma $\xi^r h(\xi)^{\frac{q-1}{m}}$ para $\xi = \alpha^{i\frac{q-1}{m}}$ e $0 \leq i < q-1$, i.e., $\xi \in \mu_m$. Sendo assim, $f(x)$ será um polinômio de permutação se, e somente se, $x^r h(x)^{\frac{q-1}{m}}$ permuta μ_m. Portanto, o resultado procurado está provado. □

Com um leitura rápida dos enunciados dos teoremas apresentados nessa seção é possível concluir que as condições (ii) e (iii) do Teorema 2.9 devem ser equivalentes à condição (ii) do Teorema 2.14. De fato, não é difícil mostrar essa equivalência, uma vez que todas as implicações são simples, não havendo necessidade de utilizar teoria extra.

Para obter resultados associados aos mostrados até aqui, ver [9, 21, 22].

2.2 Polinômios de Dickson

Nesta seção, introduziremos os polinômios de Dickson, que são amplamente estudados em corpos finitos. Mas antes, é necessário apresentar a fórmula de Waring, que é válida para qualquer anel comutativo com unidade. Esta fórmula nasceu com estudo de sistemas simétricos e pode ser encontrada recursivamente.

$$x_1^n + x_2^n = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-x_1x_2)^i(x_1+x_2)^{n-2i}. \tag{2.2.1}$$

Inspirados por essa fórmula, temos a seguinte definição.

Definição 2.15. *Seja R um anel comutativo com unidade, $a \in R$ e $n \in \mathbb{N}$. Então, o n-ésimo polinômio de Dickson $D_n(x, a)$ é dado por*

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}. \tag{2.2.2}$$

Notemos que, por essa definição e pela fórmula de Waring (2.2.1), a seguinte equação funcional é válida:

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1x_2). \tag{2.2.3}$$

Apesar da definição ser mais geral, trabalharemos apenas sobre corpos finitos.

Lema 2.16. *Os polinômios de Dickson satisfazem a seguinte recursão*

$$D_{n+2}(x,a) = xD_{n+1}(x,a) - aD_n(x,a),$$

para $n \geq 0$, com $D_0(x,a) = 2$ e $D_1(x,a) = x$.

Demonstração. Pela Definição 2.15 e pela fórmula de Waring (2.2.1), temos

$$D_n\left(y + \frac{a}{y}, a\right) = y^n + \left(\frac{a}{y}\right)^n. \tag{2.2.4}$$

Seja y uma variável formal que satisfaz a relação $y + \frac{a}{y} = x \in \mathbb{F}_q$, isto é, y soluciona a equação $y^2 + a - yx = 0$. Portanto, da Equação (2.2.4), segue

$$\begin{aligned} xD_{n+1}(x,a) - aD_n(x,a) &= y^{n+2} + \frac{a^{n+1}}{y^n} + ay^n + \frac{a^{n+2}}{y^{n+2}} - a^n - \frac{a^{n+1}}{y^n} \\ &= y^{n+2} + \left(\frac{a}{y}\right)^{n+2} = D_{n+2}(x,a). \end{aligned}$$

□

E através dessa recursão é possível encontrar uma fórmula fechada para o valor de $D_n(x, a)$, dada por:

$$D_n(x,a) = \left(\frac{x + \sqrt{x^2 - 4a}}{2}\right)^n + \left(\frac{x - \sqrt{x^2 - 4a}}{2}\right)^n. \tag{2.2.5}$$

Até aqui só descrevemos propriedades básicas sobre os polinômios de Dickson, mas o que realmente nos interessa é saber quais são as hipóteses necessárias para que o polinômio de Dickson seja polinômio de permutação de $\mathbb{F}_q$. É exatamente o que veremos a seguir.

Teorema 2.17 ([12], Teorema 3.2)**.** *O polinômio de Dickson $D_n(x, a)$, com $a \in \mathbb{F}_q^*$, é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se,* $\mathrm{mdc}(n, q^2 - 1) = 1$.

Demonstração. Suponhamos $\mathrm{mdc}(n, q^2-1) = 1$ e que $D_n(x_1, a) = D_n(x_2, a)$, para $x_2, x_2 \in \mathbb{F}_q^*$. Então, existem $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$, tais que $\alpha_1 + a\alpha_1^{-1} = x_1$ e $\alpha_2 + a\alpha_2^{-1} = x_2$. Pela equação (2.2.4), na demostração do Lema 2.16, $\alpha_1^n + a^n\alpha_1^{-n} = \alpha_2^n + a^n\alpha_2^{-n}$. Mas isso implica que

$$(\alpha_1^n - \alpha_2^n)(\alpha_1^n\alpha_2^n - a^n) = 0. \tag{2.2.6}$$

Como assumimos $\mathrm{mdc}(n, q^2-1) = 1$, x^n é uma permutação de $\mathbb{F}_{q^2}$. Sendo assim, da equação (2.2.6), teremos $\alpha_1 = \alpha_2$ ou $\alpha_1\alpha_2 = a$. Em ambos os casos, segue que $x_1 = x_2$. Logo, $D_n(x, a)$, como função avaliação em $\mathbb{F}_q$, é injetiva e, pelo Teorema 1.48, concluímos que $D_n(x, a)$ é um polinômio de permutação em $\mathbb{F}_q$.

Resta provar a recíproca. Para isso, provaremos a contra-positiva. Suponhamos que $\mathrm{mdc}(n, q^2-1) = d > 1$. Primeiramente suponhamos que d seja par. Então n é par e q é ímpar. Pela definição dos polinômios de Dickson (2.15), $D_n(x, a)$ só possui potências pares de x e, portanto, $D_n(-x, a) = D_n(x, a)$, para todo $x \in \mathbb{F}_q^*$. Sendo assim, $D_n(x, a)$ não é um polinômio de permutação. Assumiremos, agora, que d seja ímpar. Então existe r um primo ímpar que divide d. Além disso, $r|(q-1)$ ou $r|(q+1)$. Neste ponto, precisamos analisar estes dois casos independentemente:

- Se $r|(q-1)$. Como $x^r = 1$ possui $r \geq 3$ raízes em $\mathbb{F}_q$, é possível escolher uma raiz $\xi \neq 1, a$. Sabemos, também, que $\xi^n = 1$. Para essa raiz, pela equação (2.2.4),

$$D_n(\xi + a\xi^{-1}, a) = \xi^n + a^n\xi^{-n} = 1 + a^n = D_n(1 + a, a). \tag{2.2.7}$$

  Mas $\xi + a\xi^{-1} \neq 1 + a$, uma vez que escolhemos $\xi \neq 1, a$. Sendo assim, $D_n(x, a)$ não é um polinômio de permutação de $\mathbb{F}_q$.

- $r|(q+1)$. Primeiramente tomemos $\gamma \in \mathbb{F}_{q^2}$ tal que $\gamma^{q+1} = a$. Como $x^r = 1$ possui $r \geq 3$ raízes em $\mathbb{F}_{q^2}$, é possível escolher uma raiz $\xi \neq 1, a\gamma^{-2}$. Sabemos também que $\xi^n = 1$. Para essa raiz, pela equação (2.2.4),

$$D_n(\gamma + a\gamma^{-1}, a) = \gamma^n + a^n\gamma^{-n} = D_n(\xi\gamma + a(\xi\gamma)^{-1}, a). \tag{2.2.8}$$

  Notemos que $(\gamma + a\gamma^{-1})^q = \gamma^q + a\gamma^{-q} = a\gamma^{-1} + \gamma$, assim $\gamma + a\gamma^{-1} \in \mathbb{F}_q$. Além disso, $(\xi\gamma + a(\xi\gamma)^{-1})^q = \xi^q\gamma^q + a\xi^{-q}\gamma^{-q} = \xi\gamma + a(\xi\gamma)^{-1}$, que implica em $\xi\gamma + a(\xi\gamma)^{-1} \in \mathbb{F}_q$.

  Mas

$$\gamma + a\gamma^{-1} = \xi\gamma + a(\xi\gamma)^{-1} \tag{2.2.9}$$

  se, e somente se,

$$\xi^2\gamma^2 - \xi(\gamma^2 + a) + a = 0, \tag{2.2.10}$$

  que é equivalente a

$$\xi = 1 \text{ ou } \xi = a\gamma^{-2}. \tag{2.2.11}$$

  Como assumimos $\xi \neq 1, a\gamma^{-2}$, concluímos que $D_n(x, a)$ não é um polinômio de permutação de $\mathbb{F}_q$. Assim, o teorema está provado. □

Uma fonte ampla de resultados sobre polinômios de Dickson é o livro de Lidl, Mullen e Turnwald [12]. Esse livro exibe um estudo sobre os polinômios de Dickson sobre corpos gerais, mas em especial, no Capítulo 5, são apresentados resultados envolvendo o caso em que os corpos são finitos.

2.3 Binômios de Permutação

Uma propriedade importante que buscamos em famílias de polinômios é que o número de coeficientes não nulos seja pequeno. Em geral, isso garante que eles tenham aplicações tecnológicas eficientes. Em particular, precisamos da seguinte definição.

Definição 2.18. *Seja $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_q[x]$. O número de coeficientes a_i diferentes de zero será chamado de peso de f e será denotado por $\omega(f)$. Isto é,*

$$\omega(f) = |\{a_j \neq 0 : 0 \leq j \leq n\}|.$$

Depois de ter estudado resultados gerais sobre polinômios de permutação, nos surgem algumas perguntas: o que podemos dizer de polinômios com peso pequeno? Já vimos, no Teorema 1.55, que um monômio de grau n, isto é, um polinômio com peso um e grau n, é uma permutação se, e somente se, $\text{mdc}(n, q-1) = 1$. O próximo peso para o qual podemos fazer essa pergunta é o dois: como podemos decidir se binômios são permutações? Isto é, se $f(x) = x^m + ax^n$, o que podemos e devemos assumir sobre m, n e q para que $f(x)$ seja um polinômio de permutação de $\mathbb{F}_q$? Essa, inclusive, é uma das perguntas apresentadas em [10].

De fato, essa pergunta é pertinente e difícil de se responder. Em matemática, quando uma pergunta é difícil de se responder, a saída é resolver casos particulares. Na prática, isso é o que acontece em todos os artigos que apresentam resultados envolvendo binômios de permutação. Faremos o mesmo aqui, primeiro tentando reduzir os casos, para depois responder essa pergunta para alguns casos específicos.

Observação 2.19. Nesta seção estamos interessados em estudar propriedades dos polinômios de permutação de $\mathbb{F}_q$ da forma $x^m + ax^n$, com $m, n \in \mathbb{Z}_{\geq 0}$ e $a \in \mathbb{F}_q$. De fato, os polinômios em que $m = n$ ou $m = 0$ ou $n = 0$ ou $a = 0$ são casos particulares do Teorema 1.55. Então consideraremos $m > n > 0$ e $a \neq 0$, escrevendo tais binômios na forma $x^n(n^k + a)$, com $k = m - n$.

Proposição 2.20. *Seja $d|(q-1)$, $a \in \mathbb{F}_q^*$ e $k > 0$ tal que $\text{mdc}(k, q-1) = d$. Existe $m \in \mathbb{N}$ tal que $f(x) := x^m(x^k + a)$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, existe $n \in \mathbb{N}$ tal que $g(x) := x^n(x^d + a)$ é um polinômio de permutação de $\mathbb{F}_q$.*

Demonstração. Pelo Teorema Chinês dos Restos, existe $r \in \mathbb{Z}$ tal que

$$\begin{cases} r\frac{k}{d} \equiv 1 \pmod{\frac{q-1}{d}}; \\ r \equiv 1 \pmod{e}, \end{cases} \tag{2.3.1}$$

onde e é o maior divisor de d que é primo relativo com $\frac{q-1}{d}$. Com isso, da primeira equação, teremos $rk \equiv d \pmod{q-1}$. Como $\text{mdc}(k, q-1) = d$, segue que $\text{mdc}(\frac{k}{d}, \frac{q-1}{d}) = 1$ e, por isso, $\frac{k}{d}$ é invertível em $\mathbb{Z}_{\frac{q-1}{d}}$. Então, da primeira equação temos $r \equiv \left(\frac{k}{d}\right)^{-1} \pmod{\frac{q-1}{d}}$, onde $\text{mdc}\left(\left(\frac{k}{d}\right)^{-1}, \frac{q-1}{d}\right) = 1$, que implica em $r = l\frac{q-1}{d} + \left(\frac{k}{d}\right)^{-1}$. Daí

$$\text{mdc}\left(r, \frac{q-1}{d}\right) = \text{mdc}\left(l\frac{q-1}{d} + \left(\frac{k}{d}\right)^{-1}, \frac{q-1}{d}\right) = \text{mdc}\left(\left(\frac{k}{d}\right)^{-1}, \frac{q-1}{d}\right) = 1. \quad (2.3.2)$$

Além disso, da segunda equivalência na equação (2.3.1) temos que $\text{mdc}\left(r, e\right) = 1$, que juntamente com a equação (2.3.2), implica em $\text{mdc}(r, q-1) = 1$.

Assim, pelo Teorema 1.55, x^r é um polinômio de permutação de $\mathbb{F}_q$. Pelo Teorema 1.56, segue que $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $f(x^r) = x^{rm}(x^{rk} + a) \equiv x^{rm}(x^d + a) = g(x) \pmod{x^q - 1}$, com $n := mr$, é um polinômio de permutação de $\mathbb{F}_q$. □

Por apresentarem estrutura simples, não é difícil imaginar que seja possível contar o número de binômios de permutação. Contar o número de polinômios de permutação com determinada propriedade é um problema recorrente em corpos finitos e quase nunca é solucionado. No caso de binômios de permutação, se nos restringimos aos polinômios das formas $x^n(x^{\frac{q-1}{2}} + a)$ e $x^n(x^{\frac{q-1}{3}} + a)$, é possível contar o número exato de permutações.

2.4 Contagem de Binômios de Permutação

Nesta seção, estaremos interessados em fazer a contagem do número de determinados classes de binômios de permutação sobre um corpo finito $\mathbb{F}_q$. A motivação para enumerar tais classes vem das hipóteses que serão apresentadas no Teorema 2.22. Uma estimativa para binômios de permutação da forma $x^n(x^{\frac{q-1}{k}} + a)$, com $k \in \mathbb{N}$, é apresentada por Zieve e Masuda em [15]. Nós apresentaremos, explicitamente, o número desses binômios para $k = 2$ e $k = 3$. Começaremos apresentado o resultado de Zieve e Masuda.

Teorema 2.21 ([15], Teorema 3.1)**.** *Sejam $q = p^k$, com p um primo ímpar e $r, n \geq 1$, onde $r|(q-1)$. Então o número N de polinômios de permutação da forma $f(x) := x^n(x^{\frac{q-1}{r}} + a) \in \mathbb{F}_q[x]$ satisfaz as seguintes desigualdades*

$$\frac{r!}{r^r}\left(q+1-\sqrt{q}(r^{r+1}-2r^r-r^{r-1}+2)-(r+1)r^{r-1}\right) \leq N \leq \frac{r!}{r^r}\left(q+1+\sqrt{q}(r^{r+1}-2r^r-r^{r-1}+2)\right).$$

2.4.1 Binômios da Forma $x^n(x^{\frac{q-1}{2}} + a)$

Se considerarmos $r = 2$ e fixamos $n \in \mathbb{N}$, o Teorema 2.21 afirma que o número N de polinômios de permutação de $\mathbb{F}_q$ da forma $x^n(x^{\frac{q-1}{2}} + a)$ satisfaz

$$\frac{q-5}{2} \leq N \leq \frac{q+1}{2}.$$

Nos próximos resultados, faremos uso do caráter multiplicativo quadrático, apresentado no Exemplo 1.27, para encontrar explicitamente o valor de N para $r = 2$.

Teorema 2.22. *Sejam $q = p^k$, com p um primo ímpar e $f(x) := x^n(x^{\frac{q-1}{2}} + a) \in \mathbb{F}_q[x]$, com $a \neq 0$ e $n \geq 1$. Então $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se,*

(a) $\operatorname{mdc}\left(n, \frac{q-1}{2}\right) = 1$;

(b) $\chi_q(a^2 - 1) = (-1)^{n+1}$.

Demonstração. Primeiramente, mostraremos a necessidade da condição (a). Suponhamos que $\operatorname{mdc}\left(n, \frac{q-1}{2}\right) = d > 1$. Então, para $\alpha \in \mathbb{F}_q^*$ um elemento primitivo de $\mathbb{F}_q$,

$$f\left(\alpha^{\frac{q-1}{d}}\right) = \alpha^{n\frac{q-1}{d}}\left(\alpha^{\frac{q-1}{d}\frac{q-1}{2}} + a\right) = \left(\alpha^{\frac{n}{d}}\right)^{q-1}\left(\left(\alpha^{\frac{q-1}{2d}}\right)^{q-1} + a\right) = 1\left(1 + a\right) = f(1).$$

Como α é um elemento primitivo, temos $\alpha^{\frac{q-1}{d}} \neq 1$. Logo, $f(x)$ não é um polinômio de permutação de $\mathbb{F}_q$.

Agora seguiremos para prova completa do enunciado. Para isso, utilizaremos o Critério de Hermite (Teorema 1.52). Notemos que o item (i) do critério é equivalente a verificar se $x^{\frac{q-1}{2}} = -a$ tem alguma solução. Como $x^{\frac{q-1}{2}} \in \{\pm 1\}$ para todo $x \in \mathbb{F}_q^*$, para que $f(x) = 0$ tenha solução única basta que $a \neq \pm 1$. Mas $a \in \{\pm 1\}$ se, e somente se, $\left(\frac{a^2-1}{\mathbb{F}_q}\right) = 0$. Assumiremos $a \neq \pm 1$ para verificar as condições necessárias para o item (ii). Se $t \in \{0, \ldots, q-2\}$, então

$$f(x)^t = x^{tn}(x^{\frac{q-1}{2}} + a)^t = \sum_{i=0}^{t} \binom{t}{i} a^{t-i} x^{i(\frac{q-1}{2})+tn}. \tag{2.4.1}$$

Da equação acima, estamos interessados em saber qual o coeficiente do termo x^{q-1} depois de ter realizado a redução $(\text{mod } x^q - x)$. Isto é, queremos saber qual a soma dos coeficientes dos termos tais que $i(\frac{q-1}{2}) + tn \equiv 0 \pmod{q-1}$, quando $0 \leq i \leq t$. No caso em que t não é múltiplo de $\frac{q-1}{2}$, teremos $i(\frac{q-1}{2}) + tn \not\equiv 0 \pmod{q-1}$, para todo $0 \leq i \leq t$. Com isso, basta calcular o caso $t = \frac{q-1}{2}$. Da equação (2.4.1),

$$f(x)^{\frac{q-1}{2}} = \sum_{i=0}^{\frac{q-1}{2}} \binom{\frac{q-1}{2}}{i} a^{(\frac{q-1}{2})-i} x^{(i+n)(\frac{q-1}{2})} \equiv Ax^{\frac{q-1}{2}} + Bx^{q-1} \pmod{x^q - x}. \tag{2.4.2}$$

Onde o coeficiente do termo x^{q-1} é dado por

$$B = \begin{cases} \sum_{i=0}^{\lfloor \frac{q-1}{4} \rfloor} \binom{\frac{q-1}{2}}{2i} a^{(\frac{q-1}{2})-2i} = a^{\frac{q-1}{2}} \left[\frac{(1+a^{-1})^{\frac{q-1}{2}} + (1-a^{-1})^{\frac{q-1}{2}}}{2}\right], \text{ se } n \text{ é par;} \\ \sum_{i=0}^{\lfloor \frac{q-3}{4} \rfloor} \binom{\frac{q-1}{2}}{2i+1} a^{(\frac{q-1}{2})-2i-1} = a^{\frac{q-1}{2}} \left[\frac{(1+a^{-1})^{\frac{q-1}{2}} - (1-a^{-1})^{\frac{q-1}{2}}}{2}\right], \text{ se } n \text{ é ímpar.} \end{cases} \tag{2.4.3}$$

Segue do critério de Hermite, que $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $B = 0$. Pelas igualdades apresentadas em (2.4.3), podemos dividir em dois casos:

- Se n é par, $B = 0$ se, e somente se, $(1 + a^{-1})^{\frac{q-1}{2}} = -(1 - a^{-1})^{\frac{q-1}{2}}$. Como estamos considerando $a \neq \pm 1$, então $(1 - a^{-1})^{\frac{q-1}{2}} \in \{\pm 1\}$. Agora, multiplicamos a identidade anterior por $(1 - a^{-1})^{\frac{q-1}{2}}$. Assim, $B = 0$ se, e somente se,

$$-1 = (1 + a^{-1})^{\frac{q-1}{2}}(1 - a^{-1})^{\frac{q-1}{2}} = (a^{-2})^{\frac{q-1}{2}}(a^2 - 1)^{\frac{q-1}{2}} = (a^2 - 1)^{\frac{q-1}{2}} = \chi_q(a^2 - 1).$$

No qual a última igualdade é dada pela Proposição 1.28 e pela definição de χ_q apresentada no Exemplo 1.27.

- Se n é ímpar, $B = 0$ se, e somente se, $(1 + a^{-1})^{\frac{q-1}{2}} = (1 - a^{-1})^{\frac{q-1}{2}}$. Como no caso anterior, temos $(1 - a^{-1})^{\frac{q-1}{2}} \in \{\pm 1\}$. Por isso, $B = 0$ se, e somente se,

$$1 = (1 + a^{-1})^{\frac{q-1}{2}}(1 - a^{-1})^{\frac{q-1}{2}} = (a^{-2})^{\frac{q-1}{2}}(a^2 - 1)^{\frac{q-1}{2}} = (a^2 - 1)^{\frac{q-1}{2}} = \chi_q(a^2 - 1).$$

Do anterior, segue resultado procurado. □

Como caso particular desse teorema, fixando $n = 1$, obtemos o enunciado do Teorema 7.11 em [13]. Motivados pela Aplicação 1.36, fixado o número de elementos do corpo, contaremos quantos polinômios de permutação existem satisfazendo as hipóteses do Teorema 2.22.

Teorema 2.23. *Seja $\mathbb{F}_q$ um corpo de característica ímpar e $n \geq 1$ um inteiro tal que* $\mathrm{mdc}(n, \frac{q-1}{2}) = 1$. *Então o número de polinômios de permutação de $\mathbb{F}_q$ da forma $f(x) = x^n(x^{\frac{q-1}{2}} + a)$ é dado por*

$$\begin{cases} \frac{q-1}{2}, & \text{se } n \text{ é par;} \\ \frac{q-3}{2}, & \text{se } n \text{ é ímpar.} \end{cases}$$

Demonstração. Primeiro consideremos n ímpar. Pelo Teorema 2.22, basta calcular a quantidade M de elementos a para os quais $\chi_q(a^2 - 1) = 1$. É claro que não iremos considerar os casos em que $a \in \{\pm 1\}$, uma vez que, como vimos, o polinômio não é uma permutação para esses valores de a. Se denotamos por $b = a^2$, segue que a gera um binômio de permutação se, e somente se, b for um quadrado em $\mathbb{F}_q$ e $b - 1$ for um quadrado em $\mathbb{F}_q$. Logo, fixando b, queremos saber se b e $b + 1$ são quadrados simultaneamente. Além disso, cada elemento b gera dois elementos a, a saber $\sqrt{b}$ e $-\sqrt{b}$. Sendo assim, calculamos a quantidade M de valores de a que geram permutação da seguinte forma.

$$2M = \sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} \big(1 + \chi_q(b)\big)\big(1 + \chi_q(b-1)\big) = \sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} 1 + \sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} \chi_q(b) + \sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} \chi_q(b-1) + \sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} \chi_q(b(b-1)).$$

Donde o primeiro somatório vale $q - 1$. Pelo Teorema 1.30, o segundo somatório vale -1 e o terceiro vale 0 e, para o último somatório, pelo Teorema 1.28, teremos:

$$\sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} \chi_q(b(b-1)) = \sum_{\substack{b \in \mathbb{F}_q \\ b \neq 1}} \chi_q(b^2)\chi_q(1 - b^{-1}) = \sum_{\substack{x \in \mathbb{F}_q \\ x \neq 1}} \chi_q(x) = -\chi_q(1) = -1.$$

Com isso, concluímos que $M = \frac{q-3}{2}$. Todos os elementos $a \in \mathbb{F}_q \backslash \{\pm 1\}$ que não foram contados são tais que $a^2 - 1$ não é um quadrado. Pelo Teorema 2.22, esses são justamente os casos em que $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$, considerando n ímpar. Sendo assim, para n par, o número de polinômios de permutação de $\mathbb{F}_q$ da forma $f(x) = x^n(x^{\frac{q-1}{2}} + a)$ é igual a $q - 2 - M = \frac{q-1}{2}$. □

2.4.2 Binômios da Forma $x^n(x^{\frac{q-1}{3}}+a)$

Tendo feito o caso $r=2$, podemos nos perguntar qual o número N de binômios de permutação da forma $x^n(x^{\frac{q-1}{r}}+a)$, com $r=3$. Pelo Teorema 2.21, N satisfaz

$$\frac{2}{9}\big(q+1-20\sqrt{q}-36\big) \leq N \leq \frac{2}{9}\big(q+1+20\sqrt{q}\big).$$

Nos seguintes resultados, apresentaremos as ferramentas necessárias para calcular explicitamente o valor de N. Para isso, definimos o caráter cúbico, mas antes iremos exibir uma definição que generaliza o Símbolo de Legendre apresentado na Definição 1.26.

Definição 2.24. *Sejam $d \in \mathbb{N}$ um divisor de $q-1$ e $\xi \in \mathbb{F}_q$ uma raiz $d-$ésima primitiva da unidade. Definimos a função $\left(\frac{x}{\mathbb{F}_q}\right)_d : \mathbb{F}_q \to \{0\} \cup \{\xi^i : i=0,\ldots,d-1\} \subset \mathbb{F}_q$ por*

$$\left(\frac{a}{\mathbb{F}_q}\right)_d := a^{\frac{q-1}{d}}. \tag{2.4.4}$$

Note que $\left(\frac{x}{\mathbb{F}_q}\right)_d$ está bem definido, uma vez que $\left(\frac{0}{\mathbb{F}_q}\right)_d = 0$ e pelo fato de $\left(\frac{a}{\mathbb{F}_q}\right)_d^d = (a^{\frac{q-1}{d}})^d = a^{q-1} = 1$ que implica em $\left(\frac{a}{\mathbb{F}_q}\right)_d \in \{\xi^i : i=0,\ldots,d-1\}$.

Da mesma forma que apresentamos o caráter multiplicativo quadrático no Exemplo 1.27, definimos o caráter multiplicativo cúbico.

Definição 2.25. *Sejam $\mathbb{F}_q$ um corpo finito tal que $q = 1 \pmod 3$, $\xi \in \mathbb{F}_q$ uma raiz cúbica primitiva da unidade e $\delta \in \mathbb{C}\backslash\{1\}$ uma raiz cúbica da unidade. Definimos o caráter multiplicativo cúbico $\eta_q : (\mathbb{F}_q^*, \times) \to \{1, \delta, \delta^2\} \subset \{w \in \mathbb{C} : |w| = 1\}$ por*

$$\eta_q(a) := \delta^i \text{ se } \left(\frac{a}{\mathbb{F}_q}\right)_3 = \xi^i. \tag{2.4.5}$$

Definido dessa forma, η_q é um caráter multiplicativo e a prova dessa afirmação é uma aplicação direta da definição de $\left(\frac{x}{\mathbb{F}_q}\right)_3$.

Observemos que na definição anterior, η_q depende da escolha de δ e ξ. De forma análoga ao caráter multiplicativo quadrático, temos a seguinte resultado.

Proposição 2.26. *Sejam $\mathbb{F}_q$ um corpo finito tal que $q = 1 \pmod 3$ e $a \in \mathbb{F}_q[x]^*$. Então, a é um cubo em $\mathbb{F}_q$ se, e somente se $\eta_q(a) = 1$.*

Demonstração. Pela forma que foi definido o caráter multiplicativo cúbico η_q e pela Definição 2.24, resumimos a prova da preposição em mostrar que a é um cubo em $\mathbb{F}_q$ se, e somente se, $a^{\frac{q-1}{3}} = 1$. Para mostrar isso, tomemos $\alpha \in \mathbb{F}_q$ um elemento primitivo.

Primeiramente, assumimos que a é um cubo, isto é, existe $b \in \mathbb{F}_q$ tal que $a = b^3$. Então $a^{\frac{q-1}{3}} = (b^3)^{\frac{q-1}{3}} = b^{q-1} = 1$.

Por outro lado, como $\mathbb{F}_q^* = \langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$, existe $0 \leq i \leq q-2$ tal que $a = \alpha^i$. Notemos também que $\alpha^{\frac{q-1}{3}} \neq 1$ e $\alpha^{\frac{2(q-1)}{3}} \neq 1$, já que $ord_{\mathbb{F}_q^*}(\alpha) = q-1$. Com isso,

teremos

$$a^{\frac{q-1}{3}} = \alpha^{\frac{i(q-1)}{3}} = \begin{cases} 1, \text{ se } i \equiv 0 \pmod 3; \\ \alpha^{\frac{q-1}{3}}, \text{ se } i \equiv 1 \pmod 3; \\ \alpha^{\frac{2(q-1)}{3}}, \text{ se } i \equiv 2 \pmod 3. \end{cases}$$

Assim, se assumimos que $a^{\frac{q-1}{3}} = 1$, existirá um $k \in \mathbb{Z}$ tal que $i = 3k$ e, com isso, $a = \alpha^i = \alpha^{3k} = (\alpha^k)^3$. □

Nos próximos resultados, fixaremos $\delta \in \mathbb{C}$ uma raiz cúbica primitiva da unidade, $\xi \in \mathbb{F}_q$ raiz cúbica primitiva da unidade e η_q o caráter multiplicativo cúbico associado a δ e ξ. Com isso, estamos prontos para apresentar um resultado semelhante ao Teorema 2.22, que será dado no próximo teorema.

Teorema 2.27. *Seja $\mathbb{F}_q$ um corpo finito tal que $q \equiv 1 \pmod 3$ e $f(x) := x^n(x^{\frac{q-1}{3}} + a) \in \mathbb{F}_q[x]$, com $n \geq 1$. Então, $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, todas as seguintes condições são satisfeitas:*

(a) $\operatorname{mdc}\left(n, \frac{q-1}{3}\right) = 1$;

(b) $a \notin \{-1, -\xi, -\xi^2\}$;

(c) $\eta_q\left(\frac{\xi+a}{1+a}\right) \neq \delta^{2n}$;

(d) $\eta_q\left(\frac{1+a}{\xi^2+a}\right) \neq \delta^{2n}$;

(e) $\eta_q\left(\frac{\xi^2+a}{\xi+a}\right) \neq \delta^{2n}$.

Onde η_q é o caráter multiplicativo cúbico relacionado aos elementos δ e ξ.

Demonstração. Os itens (a) e (b) seguem diretamente do Teorema 2.9. Para os itens restantes utilizaremos o item (iii) desse mesmo teorema, obtendo

$$\xi^{ni}(\xi^i + a)^{\frac{q-1}{3}} \neq \xi^{nj}(\xi^j + a)^{\frac{q-1}{3}}, \text{ com } 0 \leq i < j < 3,$$

ou ainda,

$$\frac{\xi^n(\xi + a)^{\frac{q-1}{3}}}{\xi^{0\cdot n}(1 + a)^{\frac{q-1}{3}}} \neq 1, \ \frac{\xi^n(1 + a)^{\frac{q-1}{3}}}{\xi^{2n}(\xi^2 + a)^{\frac{q-1}{3}}} \neq 1 \ \text{ e } \ \frac{\xi^{2n}(\xi^2 + a)^{\frac{q-1}{3}}}{\xi^n(\xi + a)^{\frac{q-1}{3}}} \neq 1.$$

Da Definição 2.25, teremos

$$\eta_q\left(\frac{\xi + a}{1 + a}\right) \neq \delta^{2n}, \ \eta_q\left(\frac{1 + a}{\xi^2 + a}\right) \neq \delta^{2n} \ \text{ e } \ \eta_q\left(\frac{\xi^2 + a}{\xi + a}\right) \neq \delta^{2n}.$$

Com isso, segue o resultado procurado. □

O lema seguinte, juntamente com o Lema 2.33, são parte da teoria necessária para calcular o número de permutações da forma $x^n(x^{\frac{q-1}{3}} + a)$.

Lema 2.28. *Seja $\mathbb{F}_q$ um corpo finito tal que $q \equiv 1 \pmod 3$. Se $\Lambda = \mathbb{F}_q \backslash \{-1, -\xi, -\xi^2\}$, então*

$$\delta^n \sum_{a\in\Lambda} \eta_q\left(\frac{\xi+a}{1+a}\right) + \delta^{2n} \sum_{a\in\Lambda} \eta_q^2\left(\frac{\xi+a}{1+a}\right) = \epsilon_1 + \epsilon_2,$$

onde

$$\epsilon_1 = \begin{cases} -2, \text{ se } q - 3n \equiv 1 \pmod 9; \\ 1, \text{ se } q - 3n \not\equiv 1 \pmod 9. \end{cases} \quad e \quad \epsilon_2 = \begin{cases} -2, \text{ se } n \equiv 0 \pmod 3; \\ 1, \text{ se } n \not\equiv 0 \pmod 3. \end{cases}$$

Demonstração. O primeiro fato que observamos é que a função $f : \Lambda \to \mathbb{F}_q$, definida por $f(x) := \frac{\xi+x}{1+x}$, é uma função injetiva. Para mostrar isso, tomamos um elemento $b \in \Im(\Lambda) = \{f(a) : a \in \Lambda\} = \mathbb{F}_q \backslash \{0, 1, -\xi^2\}$. Então, queremos saber para quais elementos $a \in \mathbb{F}_q$ temos $f(a) = \frac{\xi+a}{1+a} = b$. Isso implica em $a = \frac{b-\xi}{1-b}$, istó é, b tem uma única pré-imagem. Logo, $f(x)$ é injetiva e, assim, podemos reescrever os termos que queremos calcular como

$$\delta^n \sum_{a\in\Lambda} \eta_q\left(\frac{\xi+a}{1+a}\right) + \delta^{2n} \sum_{a\in\Lambda} \eta_q^2\left(\frac{\xi+a}{1+a}\right) = \delta^n \sum_{b\in\Im(\Lambda)} \eta_q(b) + \delta^{2n} \sum_{b\in\Im(\Lambda)} \eta_q^2(b).$$

Sendo assim, pelo Teorema 1.30,

$$\begin{aligned} \delta^n \sum_{b\in\Im(\Lambda)} \eta_q(b) + \delta^{2n} \sum_{b\in\Im(\Lambda)} \eta_q^2(b) &= \delta^n[-\eta_q(1) - \eta_q(-\xi^2)] + \delta^{2n}[-\eta_q^2(1) - \eta_q^2(-\xi^2)] \\ &= -\delta^n - \delta^{2n} - \left(\delta^{-n}\delta^{\frac{q-1}{3}}\right)^2 - \left(\delta^{-n}\delta^{\frac{q-1}{3}}\right) \end{aligned}$$

Com isso, como $1 + \delta + \delta^2 = 0$, definindo $\epsilon_1 := -\delta^n - \delta^{2n}$ e $\epsilon_2 := -\left(\delta^{-n}\delta^{\frac{q-1}{3}}\right)^2 - \left(\delta^{-n}\delta^{\frac{q-1}{3}}\right)$, teremos o resultado desejado. □

2.4.2.1 Característica Ímpar

Os lemas que serão apresentados a partir desse ponto serão utilizados para calcular o número de binômios de permutação da forma $x^n(x^{\frac{q-1}{3}} + a)$ em corpos finitos de característica ímpar. Em seguida, apresentaremos também os respectivos resultados para efetuar o cálculo em característica par. Apresentaremos alguns lemas envolvendo número de soluções sobre curvas elípticas, que serão usados na prova do teorema principal desta seção.

Na próxima definição, introduziremos a constante κ_p, que aparecerá no enunciado dos próximos lemas. Nessa definição, usaremos 4^{-1} para representar o inverso de 4 em $\mathbb{F}_p$.

Definição 2.29. *Seja $p \in \mathbb{Z}^+$ um número primo $p \geq 5$. Se $p \equiv 1 \pmod 3$, definimos κ_p como o inteiro tal que $|\kappa_p| \leq 2\sqrt{p}$ e*

$$\kappa_p \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \cdot 4^{-\frac{p-1}{6}} \pmod p, \text{ para } p \geq 19.$$

Definimos $\kappa_7 = 1$ e $\kappa_{13} = -5$. No caso $p \equiv 2 \pmod 3$, definimos $\kappa_p = 0$.

A motivação para essa definição vem do Lema 1.43 e o número complexo, que será apresentado na próxima definição, aparecerá naturalmente relacionado ao número de pontos de uma curva elíptica que será importante na demonstração do principal resultado dessa seção.

Definição 2.30. *Definimos o número complexo*

$$\pi_p := \frac{-\kappa_p}{2} + i\sqrt{p - \frac{\kappa_p^2}{4}}.$$

Lema 2.31. *Seja $E : y^2 = x^3 + 4^{-1}$ uma curva elíptica sobre $\mathbb{F}_p$. Se $p \notin \{2, 3\}$, então*

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - \pi_p^n - \overline{\pi_p}^n,$$

para todo $n \in \mathbb{N}$.

Demonstração. Pelo Teorema 1.42, apresentado no Capítulo 1, se $p \equiv 1 \pmod 3$, temos

$$|E(\mathbb{F}_p)| - 1 \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{3}} 4^{-\frac{p-1}{6}} \pmod p.$$

Por outro lado, do Lema 1.43, existe $\omega \in \mathbb{C}$, com $|\omega| = \sqrt{p}$ tal que

$$|E(\mathbb{F}_p)| - p - 1 = -\omega - \overline{\omega} = 2\Re(\omega),$$

assim

$$||E(\mathbb{F}_p)| - p - 1| = |2\Re(\omega)| \leq 2\sqrt{p}.$$

Sendo assim, se $p > 4\sqrt{p}$ (isto é, $p > 16$), podemos determinar unicamente o valor de ω, que será π_p. Os valores de π_p para $p = 7$ e $p = 13$ foram escolhidos de tal forma que o resultado fosse válido, então o resultado segue de forma imediata pelo Lema 1.43.

Da mesma forma, se $p \equiv 2 \pmod 3$, usando o Teorema 1.42 e o Lema 1.43, segue que $|E(\mathbb{F}_p)| - p - 1 = 0 = -\pi_p - \overline{\pi_p}$. Assim, pelo Lema 1.43, temos $|E(\mathbb{F}_{p^k})| - p^k - 1 = -\pi_p^k - \overline{\pi_p}^k$. □

Exemplo 2.32. Usando o lema anterior, podemos calcular o número de pontos da curva $E : y^2 = x^3 + 5$ sobre $\mathbb{F}_{19}$, já que $4^{-1} = 5$ em $\mathbb{F}_{19}$. Pela definição, temos $\kappa_{19} \leq \lfloor 2\sqrt{19} \rfloor = 8$ e

$$\kappa_{19} \equiv -\binom{\frac{19-1}{2}}{\frac{19-1}{3}} \cdot 5^{\frac{19-1}{6}} \equiv -\binom{9}{6} \cdot 5^3 \equiv -84 \cdot 125 \equiv 7 \pmod{19}.$$

Portanto, $\kappa_{19} = 7$. Assim,

$$\pi_{19} = -\frac{7}{2} + i\sqrt{19 - \frac{49}{4}} = -\frac{7}{2} + \frac{3\sqrt{3}}{2}i.$$

Pelo lema, segue que

$$|E(\mathbb{F}_{19^n})| = 19^n + 1 - \left(-\frac{7}{2} + \frac{3\sqrt{3}}{2}i\right)^n - \left(-\frac{7}{2} - \frac{3\sqrt{3}}{2}i\right)^n.$$

De fato, se $n = 1$, temos $|E(\mathbb{F}_{19}) = 19+1+7 = 27$, onde as soluções são $\infty, (0, \pm 9), (1, \pm 5), (5, \pm 4), (7, \pm 5), (8, \pm 2), (10, \pm 6), (11, \pm 5), (12, \pm 2), (13, \pm 6), (15, \pm 6), (16, \pm 4), (17, \pm 4)$ e $(18, \pm 2)$.

Para mais exemplos, consultar Apêndice A.

Lema 2.33. *Seja $\mathbb{F}_q$ um corpo de característica p ímpar tal que $q \equiv 1 \pmod 3$, onde $q = p^k$. Se $\Lambda := \mathbb{F}_q \backslash \{-1, -\xi, -\xi^2\}$, então*

$$S := \sum_{a \in \Lambda} \eta_q\left(\frac{a^2-a+1}{a^2+2a+1}\right) + \eta_q^2\left(\frac{a^2-a+1}{a^2+2a+1}\right) = -2 - \pi_p^k - \overline{\pi_p}^k.$$

Demonstração. Primeiramente, definimos $f(x) := \frac{x^2-x+1}{x^2+2x+1}$. Sabemos, pela Definição 2.25 e pela Proposição 2.26, que

$$\eta_q(b) + \eta_q^2(b) = \begin{cases} 1+1=2, \text{ se existe } c \in \mathbb{F}_q^* \text{ tal que } b = c^3; \\ \delta + \delta^2 = -1, \text{ se } b \neq c^3 \text{ para todo } c \in \mathbb{F}_q. \end{cases}$$

Sendo assim,

$$S = 2 \cdot \big|\{a \in \Lambda : f(a) \text{ é um cubo}\}\big| - 1 \cdot \big|\{a \in \Lambda : f(a) \text{ não é um cubo}\}\big|. \tag{2.4.6}$$

Agora, calcularemos o valor de $|\{a \in \Lambda : f(a) \text{ é um cubo}\}|$. Para isso, dado b^3, com $b \in \mathbb{F}_q^*$, estaremos interessados em saber se existem e quantos são os elementos $a \in \{a \in \Lambda : f(a) \text{ é um cubo}\}$ para os quais $f(a) = b^3$. Considerando que $f(a) = b^3$, teremos

$$a^2(1-b^3) - a(1+2b^3) + 1 - b^3 = 0. \tag{2.4.7}$$

Se $b^3 \neq 1$, essa equação possui duas soluções em $\mathbb{F}_{q^2}$, dadas por

$$a = \frac{1+2b^3 \pm \sqrt{\Delta}}{2(1-b^3)}, \tag{2.4.8}$$

onde $\Delta = (1+2b^3)^2 - 4(1-b^3)^2 = (1+2b^3+2-2b^3)(1+2b^3-2+2b^3) = -3+12b^3$. Mas os valores para a dados na Equação (2.4.8) estão em $\mathbb{F}_q$ se, e somente se, $\Delta = -3+12b^3$ for um quadrado em $\mathbb{F}_q$. Isto é, para cada $b^3 \in \mathbb{F}_q$ existe $a \in \Lambda$ tal que $f(a) = b^3$ se, e somente se, existe $x_a \in \mathbb{F}_q$ tal que $x_a^2 = -3+12b^3$. Então o problema se resume em encontrar as soluções de $E : x^2 = -3+12y^3$. Todavia, devemos ignorar as soluções em que $y^3 = f(-\xi) = f(-\xi^2) = 0$, casos elas existam. De fato, elas existem, uma vez que $x^2 = -3$ tem solução em $\mathbb{F}_q$, dadas por $\pm(\xi^2 - \xi)$. Devemos ignorar também as soluções $\{(\pm 3, \xi^j)\}_{j=0}^3$, referentes a $b = 1$, e adicionar a solução $a = 0$ e $b = 1$. Note que não precisamos nos preocupar em evitar o valor $f(-1)$, uma vez que $f(x)$ não está definido para $-\xi$ em $\mathbb{F}_q$.

Sendo assim, o conjunto $\{a \in \Lambda : f(a) \text{ é um cubo}\}$ pode ser visto como

$$\{a \in \Lambda : \text{ existe } (x,y) \in E(\mathbb{F}_q), \text{ com } y \in \mathbb{F}_q^* \backslash \{1\}, \text{ tal que } y^3 = f(a)\} \cup \{0\}.$$

Seja $\mathcal{A} := \{(x,y) \in E(\mathbb{F}_q) : \text{ existe } a \in \Lambda \text{ tal que } y^3 = f(a)\}$. Observamos que se $(x_0, y_0) \in \mathcal{A}$, então $(x_0, \xi y_0)$ e $(x_0, \xi^2 y_0)$ também pertencem a $\mathcal{A}$. Mas esses três pares ordenados representam o elemento

$$a = \frac{1+2y_0^3+x_0}{2(1-y_0^3)} \in \{a \in \Lambda : f(a) \text{ é um cubo}\}.$$

Isto é, estamos interessados em apenas $\frac{1}{3}$ dos valores de $\mathcal{A}$. Notemos que número de pontos de $E : x^2 = -3 + 12y^3$ é igual ao número de soluções de $E' : ((2\xi^2 - 2\xi)x)^2 = -12x^2 = -3 + 12(-y)^3$, que equivale ao número de soluções de $E'' : x^2 = 4^{-1} + y^3$.

Pelo Lema 2.31, o número de soluções de $x^2 = 4^{-1} + y^3$ é dado por $q + 1 - \pi_p^k - \overline{\pi_p}^k$. Nesta enumeração também é contado o ponto no infinito, o qual devemos desconsiderar em nossa contagem. Então, como não estamos considerando as soluções $\pm(\xi^2 - \xi, 0)$ e $\{(\pm 3, \xi^j)\}_{j=0}^3$, adicionando a solução $a = 0$ e $b = 1$, o número de elementos procurado é

$$|\{a \in \Lambda : f(a) \text{ é um cubo}\}| = \frac{q - 8 - \pi_p^k - \overline{\pi_p}^k}{3} + 1.$$

Com isso, também podemos encontrar o valor do outro termo procurado da Equação (2.4.6), da seguinte forma

$$\begin{aligned}\left|\left\{a \in \Lambda : f(a) \text{ não é um cubo}\right\}\right| &= |\Lambda| - |\{a \in \Lambda : f(a) \text{ é um cubo}\}| \\ &= q - 3 - \frac{q - 8 - \pi_p^k - \overline{\pi_p}^k}{3} - 1.\end{aligned}$$

Assim, o valor de S será dada por

$$S = 2 \cdot \left[\frac{q - 8 - \pi_p^k - \overline{\pi_p}^k}{3} + 1\right] - 1 \cdot \left[q - 3 - \frac{q - 8 - \pi_p^k - \overline{\pi_p}^k}{3} - 1\right] = -2 - (\pi_p^k + \overline{\pi_p}^k).$$

□

Com isso, estamos prontos para apresentar o resultado principal dessa seção, onde apresentamos o número exato de binômios de permutação da forma $x^n(x^{\frac{q-1}{3}} + a)$, melhorando o resultado apresentado no Teorema 2.21 para o caso $r = 3$.

Teorema 2.34. *Seja $\mathbb{F}_q$ um corpo de característica p ímpar, com $q = p^k$. Se $q \equiv 1 \pmod 3$ e $n \geq 1$ é um inteiro tal que $\text{mdc}(n, \frac{q-1}{3}) = 1$, então o número N de polinômios de permutação de $\mathbb{F}_q$ da forma $f(x) = x^n(x^{\frac{q-1}{3}} + a)$ é dado por*

$$N = \frac{2q - 3(\epsilon_1 + \epsilon_2) - 10 - 2(\pi_p^k + \overline{\pi_p}^k)}{9},$$

onde

$$\epsilon_1 = \begin{cases} -2, \text{ se } q - 3n \equiv 1 \pmod 9; \\ 1, \text{ se } q - 3n \not\equiv 1 \pmod 9. \end{cases} \quad e \quad \epsilon_2 = \begin{cases} -2, \text{ se } n \equiv 0 \pmod 3; \\ 1, \text{ se } n \not\equiv 0 \pmod 3. \end{cases}$$

Demonstração. Sejam $\delta \in \mathbb{C}$ uma raiz cúbica primitiva da unidade, $\xi \in \mathbb{F}_q$ raiz cúbica primitiva da unidade em $\mathbb{F}_q$ e η_q o caráter multiplicativo cúbico associado a ξ e δ. Com o intuito de não deixar a notação carregada, utilizaremos apenas η para representar tal caráter. Para a prova do resultado, utilizaremos o Teorema 2.27. Note que para realizar a contagem não precisamos considerar os casos em que $a \in \{-1, -\xi, -\xi^2\}$. Para simplificar a notação, definiremos a função racional $\lambda : \mathbb{F}_q \to \mathbb{F}_q$ por

$$\lambda(a) = \frac{\xi + a}{1 + a}. \tag{2.4.9}$$

Dessa definição para λ, teremos também:

$$\lambda(\xi a) = \frac{1 + a}{\xi^2 + a} \text{ e } \lambda(\xi^2 a) = \frac{\xi^2 + a}{\xi + a}. \tag{2.4.10}$$

Assim, pelo Teorema 2.27, estamos interessados em contar quais elementos $a \in \mathbb{F}_q$ satisfazem $\eta(\lambda(a)) \neq \delta^{2n},\ \eta(\lambda(\xi a)) \neq \delta^{2n}$ e $\eta(\lambda(\xi^2 a)) \neq \delta^{2n}$. Como δ é uma raiz primitiva da unidade, $1 + \delta + \delta^2 = 0$. Dessa igualdade, concluímos que

$$2 - \delta^{-2n}\eta(x) - \delta^{-4n}\eta^2(x) = \begin{cases} 0, \text{ se } \eta(x) = \delta^{2n}; \\ 3, \text{ se } \eta(x) \neq \delta^{2n}. \end{cases}$$

Com isso, assim como fizemos no Teorema 2.23, se definimos $\Lambda := \mathbb{F}_q \backslash \{-1, -\xi, -\xi^2\}$, o número de binômios de permutação N é dado por

$$N = \frac{1}{27} \sum_{a \in \Lambda} \left[2 - \frac{\eta(\lambda(a))}{\delta^{2n}} - \frac{\eta^2(\lambda(a))}{\delta^n}\right] \left[2 - \frac{\eta(\lambda(\xi a))}{\delta^{2n}} - \frac{\eta^2(\lambda(\xi a))}{\delta^n}\right] \left[2 - \frac{\eta(\lambda(\xi^2 a))}{\delta^{2n}} - \frac{\eta^2(\lambda(\xi^2 a))}{\delta^n}\right]$$

Ao todo, teremos vinte e sete termos depois que realizarmos a multiplicação. Para diminuir o volume de notação, utilizaremos

$$\lambda_0 := \lambda(a),\ \lambda_1 := \lambda(\xi a) \text{ e } \lambda_2 := \lambda(\xi^2 a) \tag{2.4.11}$$

deixando implícito o fato de que λ_0, λ_1 e λ_2 dependem de a. Assim,

$$N = \frac{1}{27} \sum_{a \in \Lambda} \left[2 - \frac{\eta(\lambda_0)}{\delta^{2n}} - \frac{\eta^2(\lambda_0)}{\delta^n}\right] \left[2 - \frac{\eta(\lambda_1)}{\delta^{2n}} - \frac{\eta^2(\lambda_1)}{\delta^n}\right] \left[2 - \frac{\eta(\lambda_2)}{\delta^{2n}} - \frac{\eta^2(\lambda_2)}{\delta^n}\right]$$

Nas seguintes manipulações, faremos uso das Equações (2.4.9), (2.4.10) e (2.4.11), utilizaremos λ_i^{-1} para denotar o inverso algébrico $\frac{1}{\lambda_i}$ e o fato de η ser um caráter multiplicativo cúbico. Além disso, da Equação (2.4.10) e da definição de Λ, $\{\eta(\lambda(a))\}_{a \in \Lambda} = \{\eta(\lambda(\xi a))\}_{a \in \Lambda} = \{\eta(\lambda(\xi^2 a))\}_{a \in \Lambda}$, isso também será usado abaixo. Pelo grande número de termos, convém organizá-los da seguinte forma:

$$\begin{aligned} N_1 &= \sum_{a \in \Lambda} 8 - \eta(\lambda_0)\eta(\lambda_1)\eta(\lambda_2) - \eta^2(\lambda_0)\eta^2(\lambda_1)\eta^2(\lambda_2) \\ &= \sum_{a \in \Lambda} 8 - \eta(1) - \eta^2(1) = \sum_{a \in \Lambda} 8 - 1 - 1 = 6|\Lambda| = 6(q - 3). \end{aligned}$$

$$\begin{aligned} N_2 &= -4\delta^n \sum_{a \in \Lambda} \eta(\lambda_0) + \eta(\lambda_1) + \eta(\lambda_2) - 4\delta^{2n} \sum_{a \in \Lambda} \eta^2(\lambda_0) + \eta^2(\lambda_1) + \eta^2(\lambda_2) \\ &= -12\delta^n \sum_{a \in \Lambda} \eta(\lambda_0) - 12\delta^{2n} \sum_{a \in \Lambda} \eta^2(\lambda_0). \end{aligned}$$

$$N_3 = -\delta^n \sum_{a\in\Lambda} \eta^2(\lambda_0)\eta(\lambda_1)\eta(\lambda_2) + \eta^2(\lambda_1)\eta(\lambda_0)\eta(\lambda_2) + \eta^2(\lambda_2)\eta(\lambda_0)\eta(\lambda_1)$$
$$= -\delta^n \sum_{a\in\Lambda} \eta(\lambda_0)\eta(1) + \eta(\lambda_1)\eta(1) + \eta(\lambda_2)\eta(1) = -3\delta^n \sum_{a\in\Lambda} \eta(\lambda_0).$$

$$N_4 = -\delta^{2n} \sum_{a\in\Lambda} \eta(\lambda_0)\eta^2(\lambda_1)\eta^2(\lambda_2) + \eta(\lambda_1)\eta^2(\lambda_0)\eta^2(\lambda_2) + \eta(\lambda_2)\eta^2(\lambda_0)\eta^2(\lambda_1)$$
$$= -\delta^{2n} \sum_{a\in\Lambda} \eta^2(\lambda_0)\eta^2(1) + \eta^2(\lambda_1)\eta^2(1) + \eta^2(\lambda_2)\eta^2(1) = -3\delta^{2n} \sum_{a\in\Lambda} \eta^2(\lambda_0).$$

$$N_5 = 2\delta^{2n} \sum_{a\in\Lambda} \eta(\lambda_1)\eta(\lambda_2) + \eta(\lambda_0)\eta(\lambda_3) + \eta(\lambda_1)\eta(\lambda_3)$$
$$= 2\delta^{2n} \sum_{a\in\Lambda} \eta(\lambda_0^{-1}) + \eta(\lambda_1^{-1}) + \eta(\lambda_2^{-1}) = 6\delta^{2n} \sum_{a\in\Lambda} \eta^2(\lambda_0).$$

$$N_6 = 2\delta^n \sum_{a\in\Lambda} \eta^2(\lambda_1)\eta^2(\lambda_2) + \eta^2(\lambda_0)\eta^2(\lambda_3) + \eta^2(\lambda_1)\eta^2(\lambda_3)$$
$$= 2\delta^n \sum_{a\in\Lambda} \eta^2(\lambda_0^{-1}) + \eta^2(\lambda_1^{-1}) + \eta^2(\lambda_2^{-1}) = 6\delta^n \sum_{a\in\Lambda} \eta(\lambda_0).$$

$$N_7 = 2\sum_{a\in\Lambda} \eta(\lambda_0\lambda_1^{-1}) + \eta(\lambda_0\lambda_2^{-1}) + \eta(\lambda_1\lambda_0^{-1}) + \eta(\lambda_1\lambda_2^{-1}) + \eta(\lambda_2\lambda_0^{-1}) + \eta(\lambda_2\lambda_1^{-1})$$
$$= 6\sum_{a\in\Lambda} \eta(\lambda_0\lambda_1^{-1}) + \eta(\lambda_1\lambda_0^{-1}) = 6\sum_{a\in\Lambda} \eta(\lambda_0\lambda_1^{-1}) + \eta^2(\lambda_0\lambda_1^{-1}).$$

Assim,

$$N = \frac{1}{27}\sum_{j=1}^{7} N_j = \frac{6(q-3)}{27} - \frac{9}{27}\left[\delta^n \sum_{a\in\Lambda} \eta(\lambda_0) + \delta^{2n} \sum_{a\in\Lambda} \eta^2(\lambda_0)\right] + \frac{6}{27}\sum_{a\in\Lambda} \eta(\lambda_0\lambda_1^{-1}) + \eta^2(\lambda_0\lambda_1^{-1}).$$

Utilizando o Lema 2.28 para o segundo termo e o Lema 2.33 para o terceiro, chegamos ao resultado buscado. □

Exemplo 2.35. Como vimos no exemplo 2.32,

$$\pi_{19} = -\frac{7}{2} + \frac{3\sqrt{3}}{2}i.$$

Sendo assim, pelo Teorema 2.34, o número N_k de binômios de permutação da forma $x^5(x^6 + a)$ sobre $\mathbb{F}_{19^k}$ é dado por

$$N_k = \frac{2\cdot 38^k - 3\cdot 2^k\cdot(\epsilon_1+\epsilon_2) - 5\cdot 2^{k+1} - 2\cdot(-7+3\sqrt{3}i)^k - 2\cdot(-7-3\sqrt{3}i)^k}{9\cdot 2^k}.$$

De fato, $N_1 = \frac{44-2\cdot(-7)-2\cdot(-7)}{9\cdot 2} = 4$, onde os binômios de permutação sobre $\mathbb{F}_{19}$ são $x^5(x^6+0)$, $x^5(x^6+4), x^5(x^6+6)$ e $x^5(x^6+9)$.

Exemplo 2.36. Se consideramos $k = 3$ no exemplo anterior, então

$$N_3 = \frac{2^4\cdot 19^2 - 2^3\cdot 16 - 2\cdot(-7+3\sqrt{3}i)^3 - 2\cdot(-7-3\sqrt{3}i)^3}{9\cdot 2^3} = 1510.$$

Para mais exemplos, consultar Apêndice A.

2.4.2.2 Característica Par

Nesta seção, calcularemos o número de binômios da forma $x^n(x^{\frac{q-1}{3}}+a)$ em corpos da forma $\mathbb{F}_{2^k}$. Observe que $2^k \equiv 1 \pmod 3$ se, e somente se, k é par. Sendo assim, nos interessa apenas os corpos da forma $\mathbb{F}_{4^k}$. Começaremos apresentando um resultado conhecido em corpos de característica 2.

Lema 2.37. *Se $v \in \mathbb{F}_{2^k}$, a equação $x^2+x+v=0$ tem soluções em $\mathbb{F}_{2^k}$ se, e somente se,* $\mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(v)=0$.

Demonstração. Segue diretamente do Teorema 1.22. □

Note que se x_0 é solução de $x^2+x+v=0$ em $\mathbb{F}_{2^k}$, $(x_0+1)^2+(x_0+1)+v = x_0^2+1+x_0+1+v = x_0^2+x_0+v=0$. Isto é, se $x^2+x+v=0$ tem soluções, então elas são distintas, da forma x_0 e x_0+1.

Para prosseguirmos, será necessário provar o seguinte lema, que é o equivalente ao Lema 2.33 em característica par.

Lema 2.38. *Se $\Lambda := \mathbb{F}_{4^k}\backslash\{-1,-\xi,-\xi^2\}$, então*

$$S := \sum_{a\in\Lambda} \eta_q\left(\frac{a^2+a+1}{a^2+1}\right) + \eta_q^2\left(\frac{a^2+a+1}{a^2+1}\right) = -2+(-2)^{k+1}.$$

Demonstração. Primeiramente, definimos $f(x) := \frac{x^2+x+1}{x^2+1}$. Pela Definição 2.25 e pela Proposição 2.26, segue que

$$\eta_q(b)+\eta_q^2(b) = \begin{cases} 1+1=2, \text{ se existe } c\in\mathbb{F}_{4^k}^* \text{ tal que } b=c^3; \\ \delta+\delta^2=-1, \text{ se } b\neq c^3 \text{ para todo } c\in\mathbb{F}_{4^k}. \end{cases}$$

Sendo assim,

$$S = 2\cdot\left|\{a\in\Lambda : f(a) \text{ é um cubo}\}\right| - 1\cdot\left|\{a\in\Lambda : f(a) \text{ não é um cubo}\}\right|. \tag{2.4.12}$$

De forma semelhante, calcularemos o valor de $|\{a\in\Lambda : f(a) \text{ é um cubo}\}|$. Para isso, dado b^3, com $b\in\mathbb{F}_{4^k}^*$, estaremos interessados em saber se existem e quantos são os elementos $a\in\{a\in\Lambda : f(a) \text{ é um cubo}\}$ para os quais $f(a)=b^3$. Considerando que $f(a)=b^3$, teremos

$$a^2(1-b^3)-a+1-b^3 = a^2(1+b^3)+a+1+b^3 = 0. \tag{2.4.13}$$

Se $b^3\neq 1$, fazendo a substituição $a\mapsto a(1+b^3)^{-1}$ na equação (1.36) e obteremos a equação $a^2+a+(1+b^3)^2=0$. Observamos que, como estamos desconsiderando o caso $b=1$, estamos perdendo a solução $a=0$, que deverá ser contabilizada separadamente ao final. Sendo assim, nos interessa saber quantos são os valores de b para os quais $a^2+a+(1+b^3)^2=0$ tem solução em $\mathbb{F}_{4^k}$. Pelo Lema 2.37, $a^2+a+(1+b^3)^2=0$ tem solução se, e somente se, $\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}((1+b^3)^2)=0$. Pela Proposição 1.21,

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}((1+b^3)^2) &= \mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(1+b^3) = \mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(1)+\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(b^3) \\ &= 2k+\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(b^3) = \mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(b^3)\end{aligned}$$

Mas $\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}((1+b^3)^2)=0$ é o mesmo que $\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(b^3)=0$. Novamente utilizando o Lema 2.37, $\mathrm{Tr}_{\mathbb{F}_{4^k}/\mathbb{F}_2}(b^3)=0$ se, e somente se, $x^2+x=b^3$ tem solução em $\mathbb{F}_{4^k}$. Se $E: x^2+x=y^3$ é uma curva sobre $\mathbb{F}_{4^k}$, o conjunto $\{a\in\Lambda : f(a) \text{ é um cubo}\}$ pode ser visto como

$$\{a\in\Lambda:\ \text{existe } (x,y)\in E(\mathbb{F}_{4^k}),\ \text{com } y\in\mathbb{F}_q^*\backslash\{1\},\ \text{tal que } y^3=f(a)\}.$$

Como $\frac{\partial(x^2+x-y^3)}{\partial x}(a,b)=1$ para todo $(a,b)\in\mathbb{F}_{4^k}^2$, segue que E é uma curva elíptica sobre $\mathbb{F}_2$. Com isso, podemos utilizar o Teorema 1.43, que afirma que existe $\omega\in\mathbb{C}$, com $|\omega|=\sqrt{2}$, tal que

$$|E(\mathbb{F}_{2^m})|=2^n+1-\omega^m-\overline{\omega}^m,\ \text{para todo } m\in\mathbb{N}.$$

Pelo Teorema 1.55, y^3 permuta $\mathbb{F}_2$ e, com isso, segue que $|E(\mathbb{F}_2)|=2+1=3$. Com isso, podemos obter ω explicitamente, uma vez que $|E(\mathbb{F}_2)|=2+1-\omega-\overline{\omega}=3-2\Re(\omega)=3$. Logo, $\Re(\omega)=0$, e utilizando $|\omega|=\sqrt{2}$, segue que $\omega=\sqrt{2}i$.

Agora, para calcular o número de elementos em $\{a\in\Lambda : f(a) \text{ é um cubo}\}$, desconsideraremos os pontos em E nos quais não estamos interessados. Isto é, os pontos $(\pm\xi,\xi),(\pm\xi,\xi^2),(\pm\xi,1),(0,0)$ e $(1,0)$. Sendo assim, adicionando o caso $a=0$, temos

$$|\{a\in\Lambda : f(a) \text{ é um cubo}\}|=\frac{q-8-(\sqrt{2}i)^{2k}-(-\sqrt{2}i)^{2k}}{3}+1=\frac{q-8+(-2)^{k+1}}{3}+1.$$

Com isso, também podemos encontrar o valor do outro termo procurado da Equação (2.4.6), da seguinte forma

$$\begin{aligned}\left|\{a\in\Lambda : f(a) \text{ não é um cubo}\}\right| &= |\Lambda|-|\{a\in\Lambda : f(a) \text{ é um cubo}\}|\\ &= q-3-\frac{q-8+(-2)^{k+1}}{3}-1.\end{aligned}$$

Assim, o valor de S será dada por

$$S=2\cdot\left[\frac{q-8+(-2)^{k+1}}{3}+1\right]-1\cdot\left[q-3-\frac{q-8+(-2)^{k+1}}{3}-1\right]=-2+(-2)^{k+1}.$$

□

Teorema 2.39. *Se* $\mathrm{mdc}(4^k-1,n)=1$*, então o número* N *de polinômios de permutação de* $\mathbb{F}_{4^k}$ *da forma* $f(x)=x^n(x^{\frac{4^k-1}{3}}+a)$ *é dado por*

$$N=\frac{2q-3(\epsilon_1+\epsilon_2)-10-(-2)^{k+2}}{9},$$

onde

$$\epsilon_1=\begin{cases}-2,\ \textit{se } q-3n\equiv 1 \pmod 9;\\ 1,\ \textit{se } q-3n\not\equiv 1 \pmod 9.\end{cases}\quad e\quad \epsilon_2=\begin{cases}-2,\ \textit{se } n\equiv 0 \pmod 3;\\ 1,\ \textit{se } n\not\equiv 0 \pmod 3.\end{cases}$$

Demonstração. Observe que todos os passos feitos no Teorema 2.34 são válidos para característica 2. Então segue que

$$N = \frac{6(q-3)}{27} - \frac{9}{27}\left[\delta^n \sum_{a\in\Lambda} \eta(\lambda_0) + \delta^{2n} \sum_{a\in\Lambda} \eta^2(\lambda_0)\right] + \frac{6}{27} \sum_{a\in\Lambda} \eta(\lambda_0\lambda_1^{-1}) + \eta^2(\lambda_0\lambda_1^{-1}),$$

onde $\lambda_0 = \frac{\xi+a}{1+a}$ e $\lambda_0\lambda_1^{-1} = \frac{a^2+a+1}{a^2+1}$. Utilizando o Lema 2.28 para o segundo termo e o Lema 2.38 para o terceiro, temos o resultado desejado. □

Exemplo 2.40. Seja $\mathbb{F}_{64} := \frac{\mathbb{F}_2[c]}{(c^6+c^4+c^3+c+1)}$. Pelo Teorema 2.39, se $n \in \mathbb{N}$, o número N de binômios de permutação da forma $x^{2^n}(x^{\frac{4^k-1}{3}} + a)$ sobre $\mathbb{F}_{4^k}$ é dado por

$$N = \frac{2q - 3(\epsilon_1+\epsilon_2) - 10 - (-2)^{k+2}}{9}.$$

Se $n = 1$ e $k = 3$, então o número de binômios de permutação da forma $x^2(x^{21} + a)$ sobre $\mathbb{F}_{64}$ é

$$\frac{2\cdot 64 - 3(1+1) - 10 - (-2)^{3+2}}{9} = \frac{128 - 6 - 10 + 32}{9} = \frac{144}{9} = 16.$$

De fato, calculando computacionalmente podemos encontrar tais polinômios, que são $x^{23}, x^{23}+c^3x^2, x^{23}+(c^4+c^3+c+1)x^{21}, x^{23}+(c^5+c^4+c^2+c)x^{21}, x^{23}+(c^5+c^3+1)x^{21}, x^{23}+(c^4+c)x^{21}, x^{23}+(c^5+c^3+c+1)x^{21}, x^{23}+(c^5+c^4+c^2)x^{21}, x^{23}+(c^5+c^4+c+1)x^{21}, x^{23}+(c^5+c^4+c^3+c^2+c+1)x^{21}, x^{23}+(c^4+1)x^{21}, x^{23}+(c^5+c+1)x^{21}, x^{23}+(c^5+c^3+c^2+c+1)x^{21}, x^{23}+(c^2+1)x^{21}, x^{23}+(c^4+c^2+c)x^{21}$ e $x^{23}+(c+1)x^{21}$.

Como corolário dos Teoremas 2.34 e 2.39, temos o resultado abaixo que melhora a cota de Masuda e Zieve, apresentada no Teorema 2.21.

Corolário 2.41. *Se $q \equiv 1 \pmod 3$ e $n \geq 1$ é um inteiro tal que $\mathrm{mdc}(n, \frac{q-1}{3}) = 1$, então o número N de polinômios de permutação de $\mathbb{F}_q$ da forma $f(x) = x^n(x^{\frac{q-1}{3}} + a)$ satisfaz*

$$\left| N - \frac{2q - 3(\epsilon_1+\epsilon_2) - 10}{9} \right| \leq \frac{4}{9}\sqrt{q},$$

onde

$$\epsilon_1 = \begin{cases} -2, \text{ se } q - 3n \equiv 1 \pmod 9; \\ 1, \text{ se } q - 3n \not\equiv 1 \pmod 9. \end{cases} \quad e \quad \epsilon_2 = \begin{cases} -2, \text{ se } n \equiv 0 \pmod 3; \\ 1, \text{ se } n \not\equiv 0 \pmod 3. \end{cases}$$

Tendo feito a contagem de binômios de permutação das formas $x^n(x^{\frac{q-1}{2}}+a)$ e $x^n(x^{\frac{q-1}{3}}+a)$ sobre $\mathbb{F}_q$, é natural tentar repetir o método para calcular o número de binômios de permutação da forma $x^n(x^{\frac{q-1}{r}} + a)$, com $r > 3$. Entretanto, se tentamos utilizar esse método, nos deparamos com um problema ainda sem solução: encontrar o número de soluções de curvas com grau maior que 3.

Problema 2.42. Dados $r > 3$, com $r|(q-1)$, e $n \in \mathbb{N}$ tais que $\mathrm{mdc}(n, \frac{q-1}{r}) = 1$, calcular o número exato de binômios de permutação da forma $x^n(x^{\frac{q-1}{r}} + a)$ sobre $\mathbb{F}_q$.

2.4.3 Heurística

Fazendo uma análise heurística dos resultados apresentados envolvendo o binômios de permutação $f(x) = x^n(x^{\frac{q-1}{r}} + a)$, observamos que, fixado uma raiz $r-$ésima da unidade $\xi \in \mathbb{F}_q$, se $x \neq y$ são tais que $x^{\frac{q-1}{r}} = y^{\frac{q-1}{r}} = \xi$, então $f(x) \neq f(y)$. Sendo assim, supostamente, para decidirmos se $f(x)$ é um binômio de permutação, basta verificar se as raízes $d-$ésimas da unidade são levadas em elementos distintos. De fato, isso acontece para quaisquer polinômios, como já vimos nos Teoremas 2.9, 2.12, 2.14, 2.22 e 2.27.

Note que, como temos r raízes $r-$ésimas da unidade, existem r^r formas de distribuirmos essas raízes. Agora, se supomos que $f(x)$ distribui uniformemente as $r-$ésimas raízes da unidade, exatamente $r!$ dessas distribuições farão com que $f(x)$ seja uma permutação. Sendo assim, é natural imaginar que o número de valores $a \in \mathbb{F}_q$ para os quais $x^n(x^{\frac{q-1}{r}} + a)$ é um binômio de permutação de $\mathbb{F}_q$ seja próximo de

$$\frac{q \cdot r!}{r^r}.$$

Como vimos nos Teoremas 2.23, 2.34 e 2.39, isso acontece nos casos em que $r = 2$ e $r = 3$. Além disso, o Teorema 2.21, apresentado por Masuda e Zieve [15], também mostra que esses binômios tem comportamento quase uniforme.

Apesar de no momento não ser conhecida uma fórmula explicita para o número de binômios de permutação da forma $x^n(x^{\frac{q-1}{r}} + a)$, podemos utilizar nossos métodos, aliado à desigualdade de Hasse-Weil, para conjecturar uma nova cota para o número de tais binômios. Antes de apresentar a cota de Hasse-Weil, introduziremos uma nova definição.

Definição 2.43. *Um polinômio $f(x, y) \in \mathbb{F}_q[x, y]$ é dito absolutamente irredutível se é irredutível em $\overline{\mathbb{F}_q}[x, y]$.*

Teorema 2.44 ([17], Teorema 3.3)**.** *Sejam $f(x, y) \in \mathbb{F}_q[x, y]$ e $E : f(x, y) = 0$ uma curva sobre $\mathbb{F}_q$. Se E é uma curva não singular e $f(x, y)$ é um polinômio absolutamente irredutível de grau d, vale que*

$$||E(\mathbb{F}_{q^n})| - q^n - 1| \leq (d-1)(d-2)\sqrt{q}.$$

Com essa cota, conjecturamos o resultado abaixo.

Conjectura 2.45. *Seja $r \in \mathbb{N}$ e $\mathbb{F}_q$ um corpo de característica p ímpar, com $q = p^k$ e $q \equiv 1 \pmod{r}$. Se $n \geq 1$ é um inteiro tal que $\text{mdc}(n, \frac{q-1}{r}) = 1$, então o número N de polinômios de permutação de $\mathbb{F}_q$ da forma $f(x) = x^n(x^{\frac{q-1}{r}} + a)$ satisfaz*

$$\left| N - \frac{q \cdot r! + \mu_{n,q}}{r^r} \right| \leq \frac{r!}{r^r} \left[\binom{r}{2} \cdot r - 1 \right] \left[\binom{r}{2} \cdot r - 2 \right] \sqrt{q} < \frac{r!}{r^r} \cdot r^6 \sqrt{q},$$

onde $\mu_{n,q}$ depende de q e n e assume apenas um número finito de valores.

Note que essa cota melhora o Teorema 2.21, uma vez que r^6 cresce mais lentamente do que r^{r+1}. Para um trabalho futuro, tentaremos encontrar uma prova para a validade deste resultado. Para provar tal conjectura, seriam usados os mesmos métodos aplicados

nesta seção, com auxílio da desigualdade de Hasse-Weil, onde é necessário mostrar que suas hipóteses são satisfeitas.

CAPÍTULO 3

Estrutura de Grupo

3.1 Posto de Carlitz

Neste capítulo, abordaremos questões que estão sendo discutidas atualmente acerca do posto de Carlitz. O nosso principal objetivo é apresentar uma cota para o peso de polinômios de permutação específicos. Como vimos no Teorema 1.58, todo polinômio de permutação $f(x)$ em $\mathbb{F}_q[x]$ pode ser representado em $\mathbb{F}_q$ pelo polinômio

$$\mathcal{P}_n(x) = (\dots((a_0x + a_1)^{q-2} + a_2)^{q-2} \dots + a_n)^{q-2} + a_{n+1}, \tag{3.1.1}$$

com $a_1, a_{n+1} \in \mathbb{F}_q$ e $a_0, a_2, \dots, a_n \in \mathbb{F}_q^*$. Um polinômio pode ser representado de várias formas como na equação acima e, com isso, surge a necessidade da seguinte definição.

Definição 3.1. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação. Chamaremos de posto de Carlitz de $f(x)$ o menor $n \in \mathbb{N}$ tal que existe $\mathcal{P}_n(x)$ como em (3.1.1) que satisfaça $f(x) \equiv \mathcal{P}_n(x) \pmod{x^q - x}$. Denotaremos por $Crk(f)$ o posto de Carlitz de $f(x)$.*

Considerando a equação (3.1.1), como $x^{q-2} = x^{-1}$ para todo $x \in \mathbb{F}_q^*$, inspirados pelas frações contínuas estudadas em teoria dos números, podemos considerar a fração contínua de $\mathcal{P}_n(x)$, dada por

$$a_{n+1} + \cfrac{1}{a_n + \ \dots \ \cfrac{1}{a_2 + \cfrac{1}{a_0x + a_1}}}, \tag{3.1.2}$$

e sua respectiva convergente

$$\mathcal{R}_n(x) = \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n}, \tag{3.1.3}$$

onde $\alpha_k := \alpha_{k-1}a_k + \alpha_{k-2}$ e $\beta_k := \beta_{k-1}a_k + \beta_{k-2}$ para $k \geq 2$, onde $\alpha_0 := 0$, $\alpha_1 := a_0$, $\beta_0 := 1$ e $\beta_1 := a_1$.

A partir de agora, dado $f(x)$ um polinômio de permutação, apenas mencionaremos $\mathcal{P}_n(x)$ e $\mathcal{R}_n(x)$ para $n = Crk(f)$. O fato da inversão não poder ser calculada no ponto 0 faz com que $\mathcal{P}_n(x)$ e $\mathcal{R}_n(x)$ não coincidam nos pontos em que os denominadores dos convergentes

$$\frac{\alpha_{k+1}x + \beta_{k+1}}{\alpha_k x + \beta_k}, \text{ com } k = 1, \ldots, n,$$

se anulam. Esta sequência de pontos, que denotaremos por

$$\mathcal{O}_n := \left\{ \frac{-\beta_i}{\alpha_i} : i = 1 \ldots n \right\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}, \tag{3.1.4}$$

será chamado de sequência de polos de $\mathcal{R}_n(x)$. Observamos que os polos podem estar repetidos. Assim, teremos

$$f(a) = \mathcal{R}_n(a) = \frac{\alpha_{n+1}a + \beta_{n+1}}{\alpha_n a + \beta_n}, \text{ para todo } a \in \mathbb{F}_q \backslash \mathcal{O}_n. \tag{3.1.5}$$

De fato, associar um polinômio de permutação $f(x)$ com sua respectiva forma racional (como acima) pode facilitar a procura de respostas para outras perguntas envolvendo polinômios de permutações e, por isso, foram investigados algumas propriedades relacionadas ao posto de Carlitz em [1, 6, 8, 20]. Nesses trabalhos, são apresentados resultados envolvendo órbitas dos polos, relações entre posto de Carlitz e grau de polinômios, relação entre posto de Carlitz e peso de polinômios, entre outros resultados. O seguinte teorema, por exemplo, encontra-se entre os citados.

Proposição 3.2 ([1], Teorema 4)**.** *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação de grau d e com $Crk(f) = n$. Então*

$$n \geq q - 1 - d.$$

Demonstração. Notemos, pela Equação (3.1.5), que $f(x)(\alpha_n x + \beta_n) - (\alpha_{n-1}x + \beta_{n-1}) = 0$, para todo $a \in \mathbb{F}_q \backslash \mathcal{O}_n$. Então o grau de $f(x)(\alpha_n x + \beta_n) - (\alpha_{n-1}x + \beta_{n-1})$, que é $d + 1$ ou d, deve ser maior ou igual à quantidade de raízes em $\mathbb{F}_q$, que é $|\mathbb{F}_q \backslash \mathcal{O}_n| \geq q - n$. Isto é, $d + 1 \geq q - n$, que era o que queríamos. □

Outro resultado importante, apresentado em [6], relaciona o posto de Carlitz ao peso de polinômios de permutação de $\mathbb{F}_q$, como veremos abaixo.

Teorema 3.3 ([6], Teorema 4)**.** *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio com grau ≥ 2,*

$$f(x) = \sum_{i=1}^{w(f)} a_i x^{e_i} \text{ e } f(x) \neq c_1 + c_2 x^{q-2},$$

para $c_1, c_2 \in \mathbb{F}_q, c_2 \neq 0$. Então

$$Crk(f) > \frac{q}{\omega(f) + 2} - 1.$$

Com esse teorema, se fixamos $Crk(f) = n$, temos um limite inferior para o peso do polinômio, dado por

$$\omega(f) > \frac{q}{n+1} - 2$$

.

Essa cota é fraca, principalmente para valores de $Crk(f)$ pequenos. O nosso objetivo na próxima seção é melhorar esse resultado para $Crk(f) = 2$.

3.2 Polinômios de Permutação com Posto 2

Apresentaremos, nesta seção, todas as ferramentas necessárias para estimar o número máximo de coeficientes nulos em polinômios com $Crk(f) = 2$. Para tanto, será necessário apresentar uma sequência de lemas técnicos. O primeiro desses descreve a forma geral de polinômios de posto de Carlitz 2. No que segue, se $f(x), g(x) \in \mathbb{F}_q[x]$, usaremos a notação $f(x) \equiv_q g(x)$ para dizer que $f(x) \equiv g(x) \pmod{x^q - x}$.

Lema 3.4. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação com $Crk(f) = 2$ e q ímpar. Então, existem $a_0, a_1, a_2, a_3 \in \mathbb{F}_q$, com $a_0, a_2 \neq 0$, tais que*

$$f(x) \equiv_q a_2^{-1} \sum_{i=1}^{q-2} x^i (-a_0)^i \left[(a_1 - i a_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}\right] + a_3 + a_2^{-1} \left[\frac{a_1}{a_1 + a_2^{-1}} + 1 - a_1^{q-1}\right]. \tag{3.2.1}$$

Demonstração. Pela definição de posto de Carlitz, existem $a_0, a_1, a_2, a_3 \in \mathbb{F}_q$, com $a_0, a_2 \neq 0$, tais que $f(x) = ((a_0 x + a_1)^{q-2} + a_2)^{q-2} + a_3$. Assim, como observado na equação (3.1.5),

$$f\left(a_0^{-1} x\right) \equiv_q \begin{cases} \mathcal{R}_2(x) = \dfrac{x + a_1}{a_2 x + a_1 a_2 + 1} + a_3, & \text{se } x \notin \{-a_1, -a_1 - a_2^{-1}\}; \\ a_2^{-1} + a_3, & \text{se } x = -a_1; \\ a_3, & \text{se } x = -(a_1 + a_2^{-1}). \end{cases}$$

Notemos que, se $x \neq -(a_1 + a_2^{-1})$, as seguintes igualdades seguem:

$$\begin{aligned} \frac{x + a_1}{a_2 x + a_1 a_2 + 1} + a_3 &\equiv_q a_2^{-1}(x + a_1)\left(x + a_1 + a_2^{-1}\right)^{q-2} + a_3 \\ &= a_2^{-1}(x + a_1) \sum_{i=0}^{q-2} \binom{q-2}{i} x^i \left(a_1 + a_2^{-1}\right)^{q-2-i} + a_3 =: \overline{\mathcal{R}}_2(x). \end{aligned}$$

Sendo assim, o polinômio $f\left(a_0^{-1} x\right) - \overline{\mathcal{R}}_2(x)$ tem como zeros todos os pontos $x \in \mathbb{F}_q \backslash \{-a_1, -a_1 - a_2^{-1}\}$. O polinômio também pode ser construído usando o método de interpolação de Lagrange apresentado na equação (1.1.9) para encontrar uma relação com poucos termos para $f(x)$:

$$f\big(a_0^{-1}x\big) - \overline{\mathcal{R}}_2(x) \equiv_q \sum_{a\in\mathbb{F}_q} \big[f(a_0^{-1}a) - \overline{\mathcal{R}}_2(a)\big](1-(x-a)^{q-1})$$
$$= (1-(x+a_1)^{q-1})a_2^{-1} + (1-(x+a_1+a_2^{-1})^{q-1})\cdot 0$$
$$= (1-(x+a_1)^{q-1})a_2^{-1}.$$

Com isso, podemos recuperar a equação para $f(x)$, como segue:

$$f\big(a_0^{-1}x\big) \equiv_q \overline{\mathcal{R}}_2(x) + (1-(x+a_1)^{q-1})a_2^{-1}$$
$$= a_2^{-1}(x+a_1)\sum_{i=0}^{q-2}\binom{q-2}{i}x^i(a_1+a_2^{-1})^{q-2-i} + a_3 + (1-(x+a_1)^{q-1})a_2^{-1}$$
$$= a_2^{-1}(x+a_1)\sum_{i=0}^{q-2}\binom{q-2}{i}x^i(a_1+a_2^{-1})^{q-2-i} + a_3 + a_2^{-1} - a_2^{-1}\sum_{i=0}^{q-1}\binom{q-1}{i}x^i a_1^{q-1-i}.$$

Pelo Corolário 1.19, temos

$$f\big(a_0^{-1}x\big) \equiv_q a_2^{-1}(x+a_1)\sum_{i=0}^{q-2}(i+1)(-1)^i x^i(a_1+a_2^{-1})^{q-2-i} + a_3 + a_2^{-1} - a_2^{-1}\sum_{i=0}^{q-1}(-1)^i x^i a_1^{q-1-i}$$
$$= a_2^{-1}\sum_{i=1}^{q-2}\frac{x^i}{(-1)^i}\big[(a_1 - ia_2^{-1})(a_1+a_2^{-1})^{q-2-i} - a_1^{q-1-i}\big] + a_3 + a_2^{-1}\left[\frac{a_1}{a_1+a_2^{-1}} + 1 - a_1^{q-1}\right].$$

De onde podemos concluir que

$$f(x) \equiv_q a_2^{-1}\sum_{i=1}^{q-2}(-a_0)^i x^i\big[(a_1 - ia_2^{-1})(a_1+a_2^{-1})^{q-2-i} - a_1^{q-1-i}\big] + a_3 + a_2^{-1}\left[\frac{a_1}{a_1+a_2^{-1}} + 1 - a_1^{q-1}\right],$$

que era a expressão desejada. □

Como nosso propósito é determinar o peso mínimo para polinômios de posto de Carlitz 2, precisamos determinar a_1, a_2 e a_3 tais que $(a_1 - ia_2^{-1})(a_1+a_2^{-1})^{q-2-i} - a_1^{q-1-i}$ se anule o número máximo de vezes. Observemos que no caso em que $a_1 + a_2^{-1} \neq 0$, isto equivale que a equação

$$a_1 + ia_2^{-1} = \left(\frac{a_1+a_2^{-1}}{a_1}\right)^i (a_1+a_2^{-1})$$

tenha o número máximo de soluções. Para estimar este número de soluções, precisaremos dos seguintes lemas.

Lema 3.5. *Sejam Ω um conjunto finito e $f, g : \mathbb{Z} \to \Omega$ funções periódicas de períodos m e n, respectivamente, tais que $f|_{[1,m]}$ e $g|_{[1,n]}$ são injetivas e* $\mathrm{mdc}(m,n) = 1$. *Então*

$$|\{i \in [1, mn] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq m\} \cap \{g(i) : 0 \leq i \leq n\}|.$$

Demonstração. Para facilitar a demostração, observemos o seguinte esquema:

$f(i)$	$f(1)$	$\ldots$		$f(m)$	$\ldots$	$f(1)$		$\ldots$	$f(m)$
i	1				$\ldots$				mn
$g(i)$	$g(1)$	$\ldots$	$g(n)$		$\ldots$		$g(1)$	$\ldots$	$g(n)$

(3.2.2)

Notemos que, fixado $j \in [1, mn]$, para que haja uma igualdade $f(j) = g(j)$ é necessário que $f(j_f) = g(j_g)$ para algum $j_f \in [1, m]$ e $j_g \in [1, n]$. Por outro lado, dados $j_f \in [1, m]$ e $j_g \in [1, n]$ tais que $f(j_f) = g(j_g)$, pelo Teorema Chinês dos Restos, existe um único $j \in [1, mn]$ tal que

$$\begin{cases} j \equiv j_f \pmod{m}; \\ j \equiv j_g \pmod{n}. \end{cases}$$

Assim,

$$|\{i \in [1, mn] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq m\} \cap \{g(i) : 0 \leq i \leq n\}|.$$

□

Corolário 3.6. *Sejam Ω um conjunto finito e $l, k \in \mathbb{Z}$. Sejam $f, g : \mathbb{Z} \to \Omega$ funções periódicas de períodos m e n, respectivamente, tais que $f|_{[1,m]}$ e $g|_{[1,n]}$ são injetivas e* $\text{mdc}(m, n) = 1$. *Então*

$$|\{i \in [k+1, k+lmn] : f(i) = g(i)\}| \leq l \times \textit{mín}\{m, n\}.$$

Demonstração. Usando o Lema 3.5,

$$|\{i \in [1, mn] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq m\} \cap \{g(i) : 0 \leq i \leq n\}| \leq \text{mín}\{m, n\}.$$

Como $f(x)$ e $g(x)$ são periódicas, podemos transladar o intervalo por k e o expandir l vezes, chegando a

$$|\{i \in [k+1, k+lmn] : f(i) = g(i)\}| \leq l \times \text{mín}\{m, n\}.$$

□

Usaremos esse corolário na demonstração do Teorema 3.9. Mas antes, precisamos dos seguintes resultados.

Lema 3.7. *Sejam $\mathbb{F}_q$ um corpo finito com característica p ímpar, $\gamma \in \mathbb{F}_q$ e $c, d \in \mathbb{F}_q$, com $c \neq 0$. Se $3 \leq M \leq p$, a seguinte desigualdade vale*

$$|\{1 \leq i \leq M : \gamma^{i+1} = ic + d\}| \leq \sqrt{\frac{3M}{2} - \frac{39}{16}} + \frac{5}{4}.$$

Demonstração. Se $\gamma \in \{0,1\}$, a desigualdade segue trivialmente, então consideraremos $\gamma \in \mathbb{F}_q \backslash \{0,1\}$. Seja $\mathscr{C}_\gamma := \{1 \leq i \leq M : \ \gamma^{i+1} = ic + d\}$, $t := |\mathscr{C}_\gamma|$ e $l := ord_{\mathbb{F}_q}(\gamma)$. Pegando $i_1, i_2 \in \mathscr{C}_\gamma$, com $i_1 \neq i_2$, das relações $\gamma^{i_1+1} = i_1 c + d$ e $\gamma^{i_2+1} = i_2 c + d$ segue que

$$\gamma^{i_2+1} - \gamma^{i_1+1} = i_2 c - i_1 c$$

$$\gamma^{i_2+1} - \gamma^{i_1+1} = (i_2 - i_1)c$$

$$\gamma^{i_1+1}(\gamma^{i_2-i_1} - 1) = (i_2 - i_1)c.$$

Da relação anterior, observamos que se $i_2 - i_1$ é múltiplo da ordem de γ, isto é $i_2 - i_1 \equiv 0 \pmod{l}$, isso implicaria que $(i_2 - i_1)c = 0$. Como $c \neq 0$, teríamos $i_1 = i_2$. Logo, como assumimos $i_1 \neq i_2$, concluímos que $i_2 - i_1 \not\equiv 0 \pmod{l}$. Assim,

$$\gamma^{i_1+1} = (i_2 - i_1)\frac{c}{\gamma^{i_2-i_1} - 1}.$$

Tomemos agora $j_1, j_2 \in \mathscr{C}_\gamma$, com $j_1 \neq j_2$. Da mesma forma, teremos

$$\gamma^{j_1+1} = (j_2 - j_1)\frac{c}{\gamma^{j_2-j_1} - 1}.$$

Suponhamos que $j_2 - j_1 = i_2 - i_1$, então

$$j_1 c + d = \gamma^{j_1+1} = (j_2 - j_1)\frac{c}{\gamma^{j_2-j_1} - 1} = (i_2 - i_1)\frac{c}{\gamma^{i_2-i_1} - 1} = \gamma^{i_1+1} = i_1 c + d.$$

Como estamos assumindo $c \neq 0$, teremos $j_1 = i_1$ e $j_2 = i_2$. Isto é, a diferença entre dois pares distintos de elementos de $\mathscr{C}_\gamma$ nunca será igual. Com isso, se $i_1 < \cdots < i_t$ são todos os elementos de $\mathscr{C}_\gamma$, os valores

$$(i_2 - i_1), (i_3 - i_2), \ldots, (i_t - i_{t-1}),$$

$$(i_3 - i_1), (i_5 - i_3), \ldots, (i_{2\lfloor \frac{t-1}{2} \rfloor + 1} - i_{2\lfloor \frac{t-1}{2} \rfloor - 1}),$$

$$(i_4 - i_2), (i_6 - i_4), \ldots, (i_{2\lfloor \frac{t}{2} \rfloor} - i_{2\lfloor \frac{t}{2} \rfloor - 2})$$

são todos distintos. A quantidade de valores contados acima é $2t - 3$. Além disso,

$$L_1 := (i_2 - i_1) + (i_3 - i_2) + \cdots + (i_t - i_{t-1}) \leq M - 1,$$

$$L_2 := (i_3 - i_1) + \cdots + (i_{2\lfloor \frac{t-1}{2} \rfloor + 1} - i_{2\lfloor \frac{t-1}{2} \rfloor - 1}) + (i_4 - i_2) + \cdots + (i_{2\lfloor \frac{t}{2} \rfloor} - i_{2\lfloor \frac{t}{2} \rfloor - 2}) \leq 2M - 4$$

Por isso,

$$\frac{(2t-3)(2t-2)}{2} = 1 + 2 + \cdots + (2t-3) \leq L_1 + L_2 \leq 3M - 5.$$

E, por isso,

$$t \leq \sqrt{\frac{3M}{2} - \frac{39}{16}} + \frac{5}{4}.$$

□

Observe que a desigualdade desse lema não é ótima. De fato, desconhecemos uma versão ótima desse resultado, como veremos no decorrer do capítulo.

Lema 3.8. *Seja $\mathbb{F}_q$ um corpo finito de característica p e $\gamma \in \mathbb{F}_q \backslash \mathbb{F}_p$. Então*

$$|\{1 \leq i \leq q-2 : \gamma^{i+1} = i(1-\gamma)+1\}| \leq \frac{q}{p}$$

Demonstração. Sabemos que $q = p^n$, com $n \geq 2$. Definimos $l := ord_{\mathbb{F}_q}(\gamma)$. Note que, como l é um divisor de $q-1$, segue que $l \neq p$. Assim, para provar o enunciado, consideraremos dois casos: $l > p$ e $l < p$.

Primeiramente suponhamos $l > p$. Observemos que γ^{i+1} tem período l e $i(1-\gamma)+1$ tem período p. Assim, pelo Corolário 3.6, o número de igualdades que ocorrem no intervalo $\left[1, lp\left\lfloor \frac{q-2}{lp} \right\rfloor\right]$ é, no máximo, igual a $p\left\lfloor \frac{q-2}{lp} \right\rfloor$, e no intervalo $\left[lp\left\lfloor \frac{q-2}{lp} \right\rfloor, q-2\right]$ ocorrerá no máximo p, uma vez que $q-2-lp\left\lfloor \frac{q-2}{lp} \right\rfloor < lp$. Sabendo disso, basta dividir em alguns subcasos para chegar ao resultado:

Se $n = 2$, como $l > p$, temos

$$\left\lfloor \frac{q-2}{lp} \right\rfloor + p = \left\lfloor \frac{p^2-2}{lp} \right\rfloor + p = p = \frac{q}{p}.$$

Se $n = 3$, como $(p+1) \nmid (p^3-1)$, o menor valor que l poderá assumir é $p+2$. Assim

$$p\left\lfloor \frac{q-2}{lp} \right\rfloor + p = p\left\lfloor \frac{p^3-2}{lp} \right\rfloor + p < p\frac{p^3-2}{lp} + p \leq \frac{p^3-2}{p+2} + p \leq p^2 = \frac{p^3}{p} = \frac{q}{p}.$$

Se $n \geq 4$, como $l \geq p+1$, teremos:

$$p\left\lfloor \frac{q-2}{lp} \right\rfloor + p = p\left\lfloor \frac{p^n-2}{lp} \right\rfloor + p < p\frac{p^n-2}{lp} + p \leq \frac{p^n-2}{p+1} + p \leq p^{n-1} = \frac{p^n}{p} = \frac{q}{p}.$$

Dessa forma, o resultado esta provado para $l > p$. Agora, façamos o caso em que $l < p$. Observe que $\gamma^{i+1} = i(1-\gamma)+1$ é o mesmo que $\gamma^i + \ldots + \gamma + 1 = -i$. A ideia da prova é usar o Lema 3.5 e para isso definiremos $f(i) := \sum_{j=0}^{i} \gamma^j$ e $g(i) = -i$. Assim definida, $f(x)$ é uma função periódica de período l e $g(x)$ é uma função periódica de período p. Utilizando o Lema 3.5, temos

$$\begin{aligned} |\{i \in [1, lp] : f(i) = g(i)\}| &= |\{f(i) : 0 \leq i \leq l\} \cap \{g(i) : 0 \leq i \leq p\}| \\ &= |\{f(i) : 0 \leq i \leq l\} \cap \{i : 0 \leq i \leq p\}| \\ &= |\{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p| \end{aligned}$$

Suponhamos que exista $k \in \mathbb{N}$, com $0 \leq k \leq l-1$, tal que $f(k), f(k+1) \in \{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p$. Então

$$f(k) = \gamma^k + \ldots + \gamma + 1 = c_k \in \mathbb{F}_p; \tag{3.2.3}$$

$$f(k+1) = \gamma^{k+1} + \ldots + \gamma + 1 = c_{k+1} \in \mathbb{F}_p. \tag{3.2.4}$$

Note que $c_k \neq 0$, uma vez que $k < l = ord_{\mathbb{F}_q}(\gamma)$. Das equações (3.2.3) e (3.2.4), concluímos que

$$\gamma = \frac{c_{k+1} - 1}{c_k} \in \mathbb{F}_p,$$

que é absurdo. Sendo assim, não existem dois índices consecutivos k e $k+1$ para os quais $f(k), f(k+1) \in \{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p$. Com isso, temos uma limitação para o número de elementos em $|\{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p|$, dada por

$$|\{i \in [1, lp] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p| \leq \left\lfloor \frac{l}{2} \right\rfloor.$$

Com essa limitação, estamos prontos para fazer o mesmo que fizemos na primeira parte da prova deste lema. O número de igualdades que ocorrem no intervalo $\left[1, lp\left\lfloor \frac{q-2}{lp} \right\rfloor\right]$ é, no máximo, igual a $\left\lfloor \frac{l}{2} \right\rfloor \left\lfloor \frac{q-2}{lp} \right\rfloor$, e no intervalo $[lp\left\lfloor \frac{q-2}{lp} \right\rfloor, q-2]$ ocorrerá no máximo $\left\lfloor \frac{l}{2} \right\rfloor$, uma vez que $q - 2 - lp\left\lfloor \frac{q-2}{lp} \right\rfloor < lp$. Logo,

$$|\{1 \leq i \leq q-2 : \gamma^{i+1} = i(1-\gamma) + 1\}| \leq \left\lfloor \frac{l}{2} \right\rfloor \left\lfloor \frac{q-2}{lp} \right\rfloor + \left\lfloor \frac{l}{2} \right\rfloor < \frac{q}{2p} + \frac{p}{2} \leq \frac{q}{p},$$

e o resultado segue. □

3.2.1 Característica Ímpar

Estamos prontos para enunciar o principal teorema deste capítulo. Como vimos, no caso em que $Crk(f) = 2$, o Teorema 3.3 afirma que

$$\omega(f) > \frac{q}{3} - 2.$$

O resultado abaixo melhora essa cota para o caso em que a característica p de $\mathbb{F}_q$ é ímpar. Em seguida, apresentaremos também o caso $p = 2$.

Teorema 3.9. *Seja $\mathbb{F}_q$ com característica p ímpar e $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação com $Crk(f) = 2$. Então*

$$\omega(f) \geq q - \frac{q}{p} - \sqrt{\frac{3p}{2} - \frac{39}{16}} - \frac{1}{4}.$$

Demonstração. Pelo Lema 3.4, existem $a_0, a_1, a_2, a_3 \in \mathbb{F}_q$, com $a_0, a_2 \neq 0$, tais que

$$f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i (-a_0)^i \left[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}\right] + a_3 + a_2^{-1} \left[\frac{a_1}{a_1 + a_2^{-1}} + 1 - a_1^{q-1}\right].$$

Como estamos interessados apenas no peso mínimo que $f(x)$ pode ter, vamos considerar, sem perda de generalidade, que $a_3 := -\dfrac{a_2^{-1}a_1}{a_1 + a_2^{-1}} - a_2^{-1} + a_2^{-1}a_1^{q-1}$ e $a_0 = -1$. Com isso,

$$f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i \left[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}\right]. \tag{3.2.5}$$

Dada a última equação fica claro o que faremos para calcular o peso mínimo que $f(x)$ pode assumir, que é calcular o máximo de índices $i \in \{1, \ldots, q-2\}$ para os quais a igualdade $(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} = a_1^{q-1-i}$ ocorre. Mas antes, faremos alguns casos isoladamente. Primeiramente consideremos o caso em que $a_1 = 0$ e assim,

$$f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i \big[- i(a_2^{-1})^{q-1-i} \big] = -a_2^{-1} \sum_{i=1}^{q-2} i x^i a_2^i.$$

Note que $i\, a_2^i = 0$ precisamente quando $i \equiv 0 \pmod{p}$. Mas, como $i \in \{1, \ldots, q-2\}$, isso acontece exatamente $\frac{q}{p} - 1$ vezes. Sendo assim, para o caso em que $a_1 = 0$, sabemos que

$$\omega(f) = q - 2 - \left(\frac{q}{p} - 1 \right) = q - \frac{q}{p} - 1,$$

e o resultado segue. Façamos agora outro caso isolado, assumindo que $a_1 + a_2^{-1} = 0$ e daqui

$$f(x) = -a_2^{-1} \sum_{i=1}^{q-2} x^i\, a_1^{q-1-i}.$$

Notemos que, nesse caso, $a_1 \neq 0$, uma vez que $a_2 \neq 0$. Mas se $a_1 \neq 0$, teremos $a_1^{q-1-i} \neq 0$ para todo $i \in \{1, \ldots, q-2\}$. Sendo assim, para este caso, temos $\omega(f) = q - 2$.

Tendo feito esses dois casos particulares, estamos prontos para fazer o caso geral. Assumiremos que $a_1 \neq 0$ e $a_1 + a_2^{-1} \neq 0$. Assim:

$$\begin{aligned} f(x) &= a_2^{-1} \sum_{i=1}^{q-2} x^i \big[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i} \big] \\ &= a_2^{-1} \sum_{i=1}^{q-2} x^i \big[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{-(i+1)} - a_1^{-i} \big] \\ &= a_2^{-1} \sum_{i=1}^{q-2} x^i a_1 (a_1 + a_2^{-1})^{-(i+1)} \left[1 - i \left(\frac{a_1 + a_2^{-1}}{a_1} - 1 \right) - \left(\frac{a_1 + a_2^{-1}}{a_1} \right)^{i+1} \right]. \end{aligned}$$

Seja $\gamma := \dfrac{a_1 + a_2^{-1}}{a_1}$. Notemos que o único valor de $\mathbb{F}_q$ que γ não pode assumir é 1, uma vez que isso implicaria em $a_2 = 0$. Da mesma forma que nos casos particulares, estamos interessados em saber, fixado γ, qual o maior número de índices $i \in \{1, \ldots, q-2\}$ para os quais se obtém

$$\gamma^{i+1} = i(1 - \gamma) + 1. \tag{3.2.6}$$

No caso em que $\gamma \in \mathbb{F}_q \backslash \mathbb{F}_p$, o resultado segue do Lema 3.8. Assim, podemos assumir $\gamma \in \mathbb{F}_p$, isto é, $l := ord_{\mathbb{F}_q}(\gamma) | p - 1$. Notemos que a sequência γ^{i+1} tem período l e sequência $i(1-\gamma)+1$ tem período p, então, pelo Corolário 3.6, a igualdade (3.2.6) ocorrerá exatamente $\frac{q}{p} - 1$ vezes no intervalo $[p-1,\ q-2]$. Por fim, pelo Lema 3.7, a igualdade (3.2.6) ocorrerá no máximo

$$\sqrt{\frac{3p}{2} - \frac{39}{16}} + \frac{5}{4}$$

vezes no intervalo $[1, p-2]$.

Com isso, podemos cotar o peso w do polinômio f inferiormente por

$$\omega(f) \geq q - 2 - \left(\frac{q}{p} - 1\right) - \left(\sqrt{\frac{3p}{2} - \frac{39}{16}} + \frac{5}{4}\right) = q - \frac{q}{p} - \sqrt{\frac{3p}{2} - \frac{39}{16}} - \frac{1}{4}.$$

Portanto, o teorema está provado. □

Note que esse teorema melhora a cota apresentada no Teorema 3.3, que afirma que $\omega(f) > \frac{q}{3} - 2$ quando $Crk(f) = 2$. Apesar disso, a desigualdade apresentada nesse teorema não é ótima. Além disso, da demostração apresentada para o teorema, segue o seguinte corolário.

Corolário 3.10. *Seja $\mathbb{F}_{p^n}$ com característica p ímpar e $f(x) \in \mathbb{F}_{p^n}[x]$ um polinômio de permutação com $Crk(f) = 2$. Então, existe um inteiro $\nu_p \geq 0$ tal que*

$$\omega(f) \geq p^n - \frac{p^n}{p} - \nu_p,$$

onde essa desigualdade é ótima.

Como veremos na próxima seção, o mesmo se repete em característica $p = 2$. Estimativas para a constante ν_p serão apresentadas na tabela do Apêndice B. Estes valores foram calculados por uma rotina implementada em linguagem C. Entretanto, encontrar uma fórmula fechada para v_p ainda é um problema sem solução.

Exemplo 3.11. Calculando computacionalmente o caso em que $char(\mathbb{F}_q) = p = 11$, temos $\nu_{11} = 4$ e o valor de $\gamma = 7$ garante que a equação (3.2.6) atinja o número máximo de igualdades. Sendo assim, escolhendo $a_1 = 2$ e $a_2 = 1$, podemos usar a igualdade (3.2.5) para definir o polinômio

$$f_n(x) = \sum_{i=1}^{11^n-2} \left[4^{i+1}(2-i) - 6^i\right] x^i.$$

Dessa forma, $f_n(x)$ é um polinômio de permutação sobre $\mathbb{F}_{11^n}$, de posto de Carlitz 2, podendo também ser escrito como

$$f_n(x) \equiv ((2-x)^{11^n-2} + 1)^{11^n-2} - 8 \pmod{x^{11^n} - x}.$$

Pelo Corolário 3.10, $f_n(x)$ é tal que $\omega(f_n) = 11^n - 11^{n-1} - 4$.

No Apêndice B, apresentamos os valores de ν_p para vários primos p, a fim de mostrar que ν_p cresce bem lentamente, o que indica que o Lema 3.7 pode ser melhorado. Na tabela abaixo, ao lado do número natural n, aparece o menor primo para o qual $\nu_p = n$.

$n \to$ menor primo p tal que $\nu_p = n$	$n \to$ menor primo p tal que $\nu_p = n$
$1 \to 2$	$7 \to 233$
$2 \to 3$	$8 \to 281$
$3 \to 5$	$9 \to 1987$
$4 \to 11$	$10 \to 2003$
$5 \to 29$	$11 \to 10159$
$6 \to 53$	

3.2.2 Característica Par

No caso em que a característica é par, temos um resultado semelhante ao caso anterior, cuja demonstração não necessita de lemas adicionais.

Teorema 3.12. *Seja $\mathbb{F}_{2^n}$ um corpo finito. Se $f(x) \in \mathbb{F}_{2^n}[x]$ é um polinômio de permutação com $Crk(f) = 2$, então*

$$\omega(f) \geq 2^{n-1} - 1,$$

e essa desigualdade é ótima para $n \geq 2$.

Demonstração. Assim como em característica ímpar, sabemos que $f(x)$ é da forma

$$f(x) = a_2^{-1} \sum_{i=1}^{2^n-2} x^i \big[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{2^n-2-i} - a_1^{2^n-1-i}\big].$$

Assumindo que $a_1 = 0$, obtemos

$$f(x) = a_2^{-1} \sum_{i=1}^{2^n-2} x^i \big[- i(a_2^{-1})^{2^n-1-i}\big] = -a_2^{-1} \sum_{i=1}^{2^n-2} i x^i a_2^i.$$

Notemos que $i\, a_2^i = 0$ precisamente quando $i \equiv 0 \pmod 2$. Mas, como $i \in \{1, \ldots, 2^n - 2\}$, isso acontece exatamente $2^{n-1} - 1$ vezes. Sendo assim, para o caso em que $a_1 = 0$, sabemos que

$$\omega(f) = 2^n - 2 - \left(\frac{2^n}{2} - 1\right) = 2^n - \frac{2^n}{2} - 1 = 2^{n-1} - 1. \tag{3.2.7}$$

Para o outro caso, assumindo que $a_1 + a_2^{-1} = 0$, teremos

$$f(x) = -a_2^{-1} \sum_{i=1}^{2^n-2} x^i\, a_1^{2^n-1-i}.$$

Notemos que, nesse caso, $a_1 \neq 0$, uma vez que $a_2 \neq 0$. Mas se $a_1 \neq 0$, teremos $a_1^{2^n-1-i} \neq 0$ para todo $i \in \{1, \ldots, 2^n - 2\}$. Sendo assim, para este caso, temos $\omega(f) = 2^n - 2$.

Agora podemos assumir $a_1 \neq 0$ e $a_1 + a_2^{-1} \neq 0$. Com isso,

$$\begin{aligned} f(x) &= a_2^{-1} \sum_{i=1}^{2^n-2} x^i \left[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{2^n-2-i} - a_1^{2^n-1-i}\right] \\ &= a_2^{-1} \sum_{i=1}^{2^n-2} x^i \left[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{-(i+1)} - a_1^{-i}\right] \\ &= a_2^{-1} \sum_{i=1}^{2^n-2} x^i a_1 (a_1 + a_2^{-1})^{-(i+1)} \left[1 - i\left(\frac{a_1 + a_2^{-1}}{a_1} - 1\right) - \left(\frac{a_1 + a_2^{-1}}{a_1}\right)^{i+1}\right]. \end{aligned}$$

Da mesma forma, definindo $\gamma := \dfrac{a_1 + a_2^{-1}}{a_1}$, notemos que o único valor de $\mathbb{F}_q$ que γ não pode assumir é 1, uma vez que isso implicaria em $a_2 = 0$. Como nos casos anteriores, estamos interessados em saber, fixado γ, qual o maior número de índices $i \in \{1, \ldots, q-2\}$ para os quais se obtém

$$\gamma^{i+1} = i(1-\gamma) + 1. \tag{3.2.8}$$

Mas como estamos em característica 2, isso se traduz em encontrar γ para qual o maior número de valores de $i \in \{1, \ldots, 2^{n-1} - 1\}$ satisfaz $\gamma^{2i+1} = 1$, onde o número de zeros em $\{1, \ldots, 2^n - 1\}$ será exatamente igual a duas vezes esse valor. Isso se dá pois $\gamma^{2i+1} = 2i(1-\gamma) + 1 = 1$ e $\gamma^{2i+2} = (2i+1)(1-\gamma) + 1 = (1-\gamma) + 1 = \gamma$, que é o mesmo que $\gamma^{2i+1} = 1$. O número máximo de valores de i para os quais se tem $\gamma^{2i+1} = 1$ ocorre quando γ tem ordem mínima em $\mathbb{F}_{2^n}$. Sendo assim, se $p_0 > 1$ é o menor divisor de $2^n - 1$, existirá um elemento γ_0 com ordem p_0 e está será a mínima ordem possível para elementos diferentes de 1. Neste caso, teremos $\gamma_0^{2i+1} = 1$ sempre que $i = \frac{k \cdot p_0 - 1}{2}$, com $k \in \mathbb{N}$. Como p_0 é ímpar, isso acontece sempre que k é ímpar. Então, em um intervalo de tamanho $2p_0$, temos exatamente 2 índices para os quais a equação (3.2.8) é satisfeita. Sendo assim, nesse caso temos

$$\omega(f) \geq 2^n - 2 - 2\left\lfloor \frac{2^n - 2}{2p_0} \right\rfloor = 2^n - 2 - 2 \cdot \frac{2^n - 1 - p_0}{2p_0} > 2^n - 2 - \frac{2^n - 4}{3} > 2^{n-1} - 1,$$

e obtemos o que procurávamos. □.

Nesse teorema, a desigualdade apresentada é ótima. No exemplo abaixo, apresentaremos uma família de polinômios para os quais obtemos a igualdade.

Exemplo 3.13. A igualdade ocorre justamente nos casos calculados na equação (3.2.7), referentes ao caso em que $a_1 = 0$. Por isso, se escolhemos $a \in \mathbb{F}_{2^n}^*$, o polinômio

$$f_a(x) = \sum_{i=0}^{2^n-2} i x^i a^i = \sum_{i=1}^{2^{n-1}-1} x^{2i-1} a^{2i-1} = ax + a^3x^3 + \ldots + a^{2^n-3}x^{2^n-3}$$

é um polinômio de permutação sobre $\mathbb{F}_{2^n}$, de posto de Carlitz 2, podendo também ser escrito como

$$f_a(x) \equiv ((ax)^{2^n-2} + 1)^{2^n-2} \pmod{x^{2^n} - x}.$$

Como vimos na demonstração do teorema, $f_a(x)$ é tal que $\omega(f_a) = 2^n - 1$.

Considerações Finais

Tendo feito o caso em que o posto do polinômios é 2, podemos nos perguntar o que acontece para posto maior que 2.

Conjectura 3.14. *Seja $\mathbb{F}_q$ com característica $p \neq 5$ ímpar e $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação com $Crk(f) = 3$. Então*

$$\omega(f) \geq \frac{q-1}{2}.$$

Para $p = 5$, temos uma conjectura semelhante, com $\omega(f) \geq \frac{q-3}{2}$. Afirmamos que a desigualdade é ótima por conhecermos polinômios que atingem a cota. Para construir um polinômio cujo peso seja exatamente $\frac{q-1}{2}$, precisamos apresentar o seguinte lema, que é similar ao Lema 3.4 apresentado para polinômios com posto 2.

Lema 3.15. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação com $Crk(f) = 3$ e q ímpar. Então existem $a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_q$, com $a_0, a_2, a_3 \neq 0$, tais que*

$$f(x) \equiv_q \sum_{i=1}^{q-2} x^i(-a_0)^i \left[\big(i + a_2\beta_1\beta_2\big)\beta_1^{i-1}\beta_3^{q-2-i} - \beta_4 a_1^{q-1-i} - a_3^{-1}\beta_2^{q-1-i} \right] + \beta_5, \qquad (3.2.9)$$

onde

$$\beta_1 = a_2a_3 + 1,\ \beta_2 = a_1 + a_2^{-1},\ \beta_3 = a_1a_2a_3 + a_1 + a_3,\ \beta_4 = (a_2^{-1} + a_3)^{q-2} - a_3^{-1}$$

e

$$\beta_5 = (a_1a_2 + 1)\beta_3^{q-2} + \beta_4(1 - a_1^{q-1}) + a_3^{-1}(1 - \beta_2^{q-1}) + a_4.$$

Não apresentaremos a prova deste lema, uma vez que basta imitar os passos da demostração do Lema 3.4. Com esse lema, construímos um polinômio de posto 3 que atinge a cota da Conjectura 3.14, como veremos no exemplo a seguir.

Exemplo 3.16. Tomando $a_0 = -1, a_1 = -1, a_2 = 2^{-1}, a_3 = -2$ e $a_4 = 4^{-1}$, teremos $\beta_1 = -1, \beta_2 = 0$ e $\beta_3 = 1$. Assim, consideraremos o polinômio de permutação $f(x) \in \mathbb{F}_q[x]$ com posto de Carlitz 3 que satisfaz

$$f(x) \equiv (((-1 - x)^{q-2} + 2^{-1})^{q-2} - 2)^{q-2} + 4^{-1} \pmod{x^q - x},$$

podendo também ser escrito como

$$f(x) = \sum_{i=1}^{q-2} 2^{-1}[(-1)^i - 1]x^i.$$

Dessa forma, $f(x)$ é um polinômio de permutação tal que $\omega(f) = \frac{q-1}{2}$.

Da mesma maneira, podemos encontrar a forma geral de polinômios com posto 4 e propor as seguintes conjecturas.

Conjectura 3.17. *Seja $\mathbb{F}_q$ com característica p ímpar e $f(x) \in \mathbb{F}_q[x]$ um polinômio de permutação com $Crk(f) = 4$. Se $q \equiv 1 \pmod 3$, então*

$$\omega(f) \geq \frac{q-1}{3}.$$

Se $q \not\equiv 1 \pmod 3$, então

$$\omega(f) \geq \frac{q-1}{2}.$$

Em ambos os casos, a desigualdade é ótima.

Para um projeto futuro, seria estudada a validade de tais conjecturas utilizando as ferramentas apresentadas aqui. Entretanto, demonstrar resultados equivalentes aos lemas técnicos 3.7 e 3.8 para estes casos não é trivial.

APÊNDICE A

Alguns Binômios da Forma $x^n(x^{\frac{q-1}{3}} + a)$

Se $n \in \mathbb{N}$ é tal que $\text{mdc}(n, \frac{q-1}{3}) = 1$, então a tabela abaixo apresenta o número $N_{n,q}$ de binômios de permutação da forma $x^n(x^{\frac{q-1}{3}} + a)$ em $\mathbb{F}_q$, para alguns valores de q. Todos esses valores foram obtidos utilizando uma rotina implementada em linguagem C.

p	κ_p	π_p	$N_{n,p}$	N_{n,p^2}	N_{n,p^3}	N_{n,p^4}	N_{n,p^5}	
17	0	$i\sqrt{17}$	–	72	–	18432	–	se $n \equiv 0 \pmod 3$
			–	70	–	18430	–	se $n \equiv 1 \pmod 3$
			–	70	–	18430	–	se $n \equiv 2 \pmod 3$
19	7	$-3.5 + i\sqrt{6.75}$	6	78	1512	29094	549546	se $n \equiv 0 \pmod 3$
			4	76	1510	29092	549544	se $n \equiv 1 \pmod 3$
			4	76	1510	29092	549544	se $n \equiv 2 \pmod 3$
23	0	$i\sqrt{23}$	–	127	–	61951	–	se $n \equiv 0 \pmod 3$
			–	126	–	61951	–	se $n \equiv 1 \pmod 3$
			–	127	–	61950	–	se $n \equiv 2 \pmod 3$
29	0	$i\sqrt{29}$	–	199	–	156799	–	se $n \equiv 0 \pmod 3$
			–	199	–	156798	–	se $n \equiv 1 \pmod 3$
			–	198	–	156799	–	se $n \equiv 2 \pmod 3$
31	4	$-2 + i\sqrt{27}$	7	223	6552	205183	6364327	se $n \equiv 0 \pmod 3$
			7	222	6550	205183	6364326	se $n \equiv 1 \pmod 3$
			6	223	6550	205182	6364327	se $n \equiv 2 \pmod 3$
37	-11	$5.5 + i\sqrt{6.75}$	6	294	11232	416598	15411966	se $n \equiv 0 \pmod 3$
			4	292	11230	416596	15411964	se $n \equiv 1 \pmod 3$
			4	292	11230	416596	15411964	se $n \equiv 2 \pmod 3$

p	κ_p	π_p	$N_{n,p}$	N_{n,p^2}	N_{n,p^3}	N_{n,p^4}	N_{n,p^5}	
41	0	$i\sqrt{41}$	–	391	–	627199	–	se $n \equiv 0 \pmod 3$
			–	390	–	627199	–	se $n \equiv 1 \pmod 3$
			–	391	–	627198	–	se $n \equiv 2 \pmod 3$
43	-8	$4+i\sqrt{27}$	7	415	17784	760447	32669287	se $n \equiv 0 \pmod 3$
			6	415	17782	760446	32669287	se $n \equiv 1 \pmod 3$
			7	414	17782	760447	32669286	se $n \equiv 2 \pmod 3$
47	0	$i\sqrt{47}$	–	511	–	1083391	–	se $n \equiv 0 \pmod 3$
			–	511	–	1083390	–	se $n \equiv 1 \pmod 3$
			–	510	–	1083391	–	se $n \equiv 2 \pmod 3$
53	0	$i\sqrt{53}$	–	648	–	1752192	–	se $n \equiv 0 \pmod 3$
			–	646	–	1752190	–	se $n \equiv 1 \pmod 3$
			–	646	–	1752190	–	se $n \equiv 2 \pmod 3$
59	0	$i\sqrt{59}$	–	798	–	2691199	–	se $n \equiv 1 \pmod 3$
			–	799	–	2691198	–	se $n \equiv 2 \pmod 3$
61	1	$-0.5+i\sqrt{60.75}$	13	853	50400	3075253	187692133	se $n \equiv 0 \pmod 3$
			12	853	50398	3075252	187692133	se $n \equiv 1 \pmod 3$
			13	852	50398	3075253	187692132	se $n \equiv 2 \pmod 3$
67	-5	$2.5+i\sqrt{60.75}$	13	1021	67032	4477381	300011473	se $n \equiv 0 \pmod 3$
			13	1020	67030	4477381	300011472	se $n \equiv 1 \pmod 3$
			12	1021	67030	4477380	300011473	se $n \equiv 2 \pmod 3$
71	0	$i\sqrt{71}$	–	1152	–	5644800	–	se $n \equiv 0 \pmod 3$
			–	1150	–	5644798	–	se $n \equiv 1 \pmod 3$
			–	1150	–	5644798	–	se $n \equiv 2 \pmod 3$
73	7	$-3.5+i\sqrt{60.75}$	18	1206	86184	6310998	460699938	se $n \equiv 0 \pmod 3$
			16	1204	86182	6310996	460699936	se $n \equiv 1 \pmod 3$
			16	1204	86182	6310996	460699936	se $n \equiv 2 \pmod 3$
79	-17	$8.5+i\sqrt{6.75}$	13	1357	109368	8654533	683788153	se $n \equiv 0 \pmod 3$
			12	1357	109366	8654532	683788153	se $n \equiv 1 \pmod 3$
			13	1356	109366	8654533	683788152	se $n \equiv 2 \pmod 3$
83	0	$i\sqrt{83}$	–	1567	–	10543231	–	se $n \equiv 0 \pmod 3$
			–	1567	–	10543230	–	se $n \equiv 1 \pmod 3$
			–	1566	–	10543231	–	se $n \equiv 2 \pmod 3$
89	0	$i\sqrt{89}$	–	1800	–	13939200	–	se $n \equiv 0 \pmod 3$
			–	1798	–	13939198	–	se $n \equiv 1 \pmod 3$
			–	1798	–	13939198	–	se $n \equiv 2 \pmod 3$
97	19	$-9.5+i\sqrt{6.75}$	25	2053	203112	19671157	1908307465	se $n \equiv 0 \pmod 3$
			24	2053	203110	19671156	1908307465	se $n \equiv 1 \pmod 3$
			25	2052	203110	19671157	1908307464	se $n \equiv 2 \pmod 3$

Todos os dados apresentados nessa tabela foram calculados usando o Teorema 2.34. Observe que todos esses valores dependem do resto de n módulo 3, por esse mesmo teorema. Fixamos alguns valores de p e n para verificar quais são os respectivos binômios de permutação. Usando o critério de Hermite, é possível encontrar tais binômios computacionalmente. Utilizamos o software matemático, livre e de código aberto, SageMath para encontrar todos os binômios apresentados abaixo. Na tabela, seguem os valores de p, n e os respectivos binômios de permutação.

p	n	$N_{n,p}$	Binômios da Forma $x^n(x^{\frac{q-1}{3}}+a)$
19	7	4	$x^{13}, x^7(x^6+5), x^7(x^6+16)$ e $x^7(x^6+17)$.
31	17	6	$x^{17}(x^{10}+1), x^{17}(x^{10}+5), x^{17}(x^{10}+17), x^{17}(x^{10}+22), x^{17}(x^{10}+23)$, e $x^{17}(x^{10}+25)$.
37	11	4	$x^{23}, x^{11}(x^{12}+7), x^{11}(x^{12}+33)$ e $x^{11}(x^{12}+33)$,
43	15	7	$x^{29}, x^{15}(x^{14}+1), x^{15}(x^{14}+6), x^{15}(x^{14}+9), x^{15}(x^{14}+11), x^{15}(x^{14}+23)$, e $x^{15}(x^{14}+36)$.
61	43	12	$x^{43}(x^{20}+3), x^{43}(x^{20}+18), x^{43}(x^{20}+19), x^{43}(x^{20}+31), x^{43}(x^{20}+36)$, $x^{43}(x^{20}+37), x^{43}(x^{20}+39), x^{43}(x^{20}+41), x^{43}(x^{20}+45), x^{43}(x^{20}+51)$, $x^{43}(x^{20}+53)$ e $x^{43}(x^{20}+54)$.
67	39	13	$x^{61}, x^{39}(x^{22}+2), x^{39}(x^{22}+5), x^{39}(x^{22}+7), x^{39}(x^{22}+11), x^{39}(x^{22}+25)$, $x^{39}(x^{22}+27), x^{39}(x^{22}+46), x^{39}(x^{22}+51), x^{39}(x^{22}+54)$, $x^{39}(x^{22}+55), x^{39}(x^{22}+58)$ e $x^{39}(x^{22}+61)$.
73	35	16	$x^{59}, x^{35}(x^{24}+2), x^{35}(x^{24}+4), x^{35}(x^{24}+16), x^{35}(x^{24}+18), x^{21}(x^{24}+22)$, $x^{35}(x^{24}+30), x^{35}(x^{24}+21), x^{35}(x^{24}+32), x^{35}(x^{24}+33), x^{35}(x^{24}+37)$, $x^{35}(x^{24}+45), x^{35}(x^{24}+55), x^{35}(x^{24}+57), x^{35}(x^{24}+68)$ e $x^{35}(x^{24}+71)$.
79	3	13	$x^{29}, x^3(x^{26}+4), x^3(x^{26}+13), x^3(x^{26}+15), x^3(x^{26}+20), x^3(x^{26}+29)$, $x^3(x^{26}+35), x^3(x^{26}+37), x^3(x^{26}+60), x^3(x^{26}+61)$, $x^3(x^{26}+62), x^3(x^{26}+65)$ e $x^3(x^{26}+73)$.
97	49	24	$x^{49}(x^{32}+13), x^{49}(x^{32}+17), x^{49}(x^{32}+19), x^{49}(x^{32}+20), x^{49}(x^{32}+21)$, $x^{49}(x^{32}+26), x^{49}(x^{32}+34), x^{49}(x^{32}+37), x^{49}(x^{32}+44), x^{49}(x^{32}+46)$, $x^{49}(x^{32}+47), x^{49}(x^{32}+54), x^{49}(x^{32}+56), x^{49}(x^{32}+58), x^{49}(x^{32}+60)$, $x^{49}(x^{32}+63), x^{49}(x^{32}+65), x^{49}(x^{32}+67), x^{49}(x^{32}+71), x^{49}(x^{32}+83)$, $x^{49}(x^{32}+85), x^{49}(x^{32}+90), x^{49}(x^{32}+92)$ e $x^{49}(x^{32}+93)$.

APÊNDICE B

Uma Análise Assintótica de ν_p

Abaixo, seguem os valores de ν_p para $p \leq 1009$.

$p \to \nu_p$							
$3 \to 1$	$5 \to 3$	$7 \to 2$	$11 \to 4$	$13 \to 3$	$17 \to 0.4$	$19 \to 3$	$23 \to 4$
$29 \to 5$	$31 \to 5$	$37 \to 4$	$41 \to 4$	$43 \to 4$	$47 \to 5$	$53 \to 6$	$59 \to 5$
$61 \to 5$	$67 \to 3$	$71 \to 5$	$73 \to 4$	$79 \to 5$	$83 \to 5$	$89 \to 5$	$97 \to 5$
$101 \to 5$	$103 \to 6$	$107 \to 6$	$109 \to 4$	$113 \to 6$	$127 \to 5$	$131 \to 6$	$137 \to 5$
$139 \to 6$	$149 \to 5$	$151 \to 5$	$157 \to 5$	$163 \to 5$	$167 \to 5$	$173 \to 5$	$179 \to 5$
$181 \to 6$	$191 \to 5$	$193 \to 6$	$197 \to 5$	$199 \to 5$	$211 \to 6$	$223 \to 5$	$227 \to 6$
$229 \to 5$	$233 \to 7$	$239 \to 5$	$241 \to 5$	$251 \to 6$	$257 \to 5$	$263 \to 5$	$269 \to 6$
$271 \to 5$	$277 \to 7$	$281 \to 8$	$283 \to 6$	$293 \to 6$	$307 \to 6$	$311 \to 7$	$313 \to 5$
$317 \to 5$	$331 \to 6$	$337 \to 6$	$347 \to 6$	$349 \to 6$	$353 \to 5$	$359 \to 5$	$367 \to 5$
$373 \to 6$	$379 \to 6$	$383 \to 5$	$389 \to 6$	$397 \to 5$	$401 \to 6$	$409 \to 5$	$419 \to 7$
$421 \to 6$	$431 \to 7$	$433 \to 5$	$439 \to 6$	$443 \to 7$	$449 \to 6$	$457 \to 6$	$461 \to 5$
$463 \to 5$	$467 \to 7$	$479 \to 6$	$487 \to 5$	$491 \to 6$	$499 \to 6$	$503 \to 6$	$509 \to 6$
$521 \to 5$	$523 \to 6$	$541 \to 7$	$547 \to 6$	$557 \to 6$	$563 \to 6$	$569 \to 8$	$571 \to 6$
$577 \to 8$	$587 \to 5$	$593 \to 7$	$599 \to 6$	$601 \to 6$	$607 \to 6$	$613 \to 5$	$617 \to 7$
$619 \to 6$	$631 \to 5$	$641 \to 6$	$643 \to 7$	$647 \to 6$	$653 \to 6$	$659 \to 6$	$661 \to 6$
$673 \to 6$	$677 \to 6$	$683 \to 6$	$691 \to 6$	$701 \to 6$	$709 \to 6$	$719 \to 6$	$727 \to 6$
$733 \to 6$	$739 \to 7$	$743 \to 6$	$751 \to 5$	$757 \to 6$	$761 \to 7$	$769 \to 7$	$773 \to 6$
$787 \to 7$	$797 \to 7$	$809 \to 6$	$811 \to 6$	$821 \to 6$	$823 \to 6$	$827 \to 6$	$829 \to 7$
$839 \to 6$	$853 \to 6$	$857 \to 7$	$859 \to 5$	$863 \to 6$	$877 \to 5$	$881 \to 6$	$883 \to 6$
$887 \to 6$	$907 \to 8$	$911 \to 8$	$919 \to 6$	$929 \to 7$	$937 \to 6$	$941 \to 6$	$947 \to 6$
$953 \to 6$	$967 \to 6$	$971 \to 6$	$977 \to 6$	$983 \to 8$	$991 \to 5$	$997 \to 6$	$1009 \to 6$

Seguem os valores de ν_p para o $i-$ésimo primo ímpar p (com $i \equiv 0 \pmod{10}$).

$p \to \nu_p$						
$31 \to 5$	$73 \to 4$	$127 \to 5$	$179 \to 5$	$233 \to 7$	$283 \to 6$	$353 \to 5$
$419 \to 7$	$467 \to 7$	$547 \to 6$	$607 \to 6$	$661 \to 6$	$739 \to 7$	$811 \to 6$
$877 \to 5$	$947 \to 6$	$1019 \to 6$	$1087 \to 7$	$1153 \to 8$	$1229 \to 8$	$1297 \to 6$
$1381 \to 6$	$1453 \to 7$	$1523 \to 7$	$1597 \to 7$	$1663 \to 6$	$1741 \to 7$	$1823 \to 7$
$1901 \to 6$	$1993 \to 7$	$2063 \to 6$	$2131 \to 7$	$2221 \to 6$	$2293 \to 6$	$2371 \to 7$
$2437 \to 7$	$2539 \to 7$	$2621 \to 7$	$2689 \to 7$	$2749 \to 8$	$2833 \to 6$	$2909 \to 8$
$3001 \to 7$	$3083 \to 7$	$3187 \to 6$	$3259 \to 7$	$3343 \to 6$	$3433 \to 7$	$3517 \to 7$
$3581 \to 9$	$3659 \to 7$	$3733 \to 7$	$3823 \to 7$	$3911 \to 8$	$4001 \to 7$	$4073 \to 8$
$4153 \to 7$	$4241 \to 8$	$4327 \to 8$	$4421 \to 7$	$4507 \to 7$	$4591 \to 7$	$4663 \to 7$
$4759 \to 7$	$4861 \to 8$	$4943 \to 7$	$5009 \to 7$	$5099 \to 8$	$5189 \to 8$	$5281 \to 7$
$5393 \to 8$	$5449 \to 7$	$5527 \to 8$	$5641 \to 7$	$5701 \to 7$	$5801 \to 7$	$5861 \to 8$
$5953 \to 7$	$6067 \to 8$	$6143 \to 8$	$6229 \to 7$	$6311 \to 7$	$6373 \to 7$	$6481 \to 8$
$6577 \to 7$	$6679 \to 8$	$6763 \to 8$	$6841 \to 8$	$6947 \to 7$	$7001 \to 7$	$7109 \to 7$
$7211 \to 8$	$7307 \to 7$	$7417 \to 8$	$7507 \to 8$	$7573 \to 7$	$7649 \to 7$	$7727 \to 8$
$7841 \to 7$	$7927 \to 7$	$8039 \to 9$	$8117 \to 9$	$8221 \to 7$	$8293 \to 7$	$8389 \to 8$
$8513 \to 8$	$8599 \to 7$	$8681 \to 7$	$8747 \to 8$	$8837 \to 7$	$8933 \to 7$	$9013 \to 8$
$9127 \to 9$	$9203 \to 8$	$9293 \to 8$	$9391 \to 7$	$9461 \to 8$	$9539 \to 7$	$9643 \to 7$
$9739 \to 7$	$9817 \to 7$	$9901 \to 8$	$10009 \to 8$	$10103 \to 7$	$10181 \to 7$	$10273 \to 7$
$10357 \to 7$	$10463 \to 8$	$10589 \to 7$	$10663 \to 9$	$10753 \to 7$	$10861 \to 7$	$10957 \to 8$
$11069 \to 10$	$11159 \to 8$	$11257 \to 8$	$11351 \to 7$	$11447 \to 8$	$11549 \to 7$	$11677 \to 8$
$11779 \to 7$	$11839 \to 7$	$11939 \to 8$	$12037 \to 8$	$12113 \to 7$	$12227 \to 8$	$12301 \to 7$
$12409 \to 8$	$12491 \to 9$	$12569 \to 9$	$12647 \to 8$	$12743 \to 8$	$12841 \to 8$	$12941 \to 8$
$13009 \to 8$	$13121 \to 7$	$13217 \to 8$	$13313 \to 8$	$13417 \to 8$	$13513 \to 9$	$13627 \to 8$
$13709 \to 7$	$13789 \to 8$	$13883 \to 7$	$13997 \to 9$	$14083 \to 8$	$14207 \to 8$	$14327 \to 8$
$14423 \to 8$	$14533 \to 7$	$14621 \to 7$	$14713 \to 7$	$14771 \to 8$	$14867 \to 8$	$14951 \to 7$
$15077 \to 8$	$15161 \to 8$	$15263 \to 8$	$15329 \to 9$	$15413 \to 8$	$15511 \to 9$	$15619 \to 8$
$15683 \to 8$	$15787 \to 8$	$15887 \to 8$	$15973 \to 7$	$16073 \to 7$	$16187 \to 8$	$16273 \to 8$
$16411 \to 8$	$16487 \to 8$	$16607 \to 9$	$16693 \to 8$	$16823 \to 8$	$16921 \to 11$	$17011 \to 8$
$17099 \to 8$	$17203 \to 8$	$17321 \to 8$	$17393 \to 7$	$17483 \to 7$	$17579 \to 9$	$17681 \to 8$

Seguem os valores de ν_p para o $i-$ésimo primo ímpar p (com $i \equiv 0 \pmod{1000}$).

$p \to \nu_p$						
$7927 \to 7$	$17393 \to 7$	$27457 \to 9$	$37831 \to 8$	$48619 \to 9$	$59369 \to 9$	$70663 \to 8$
$81817 \to 9$	$93187 \to 8$	$104743 \to 8$	$116461 \to 8$	$128201 \to 9$	$139907 \to 10$	$151717 \to 10$

Analisando as tabelas apresentadas até aqui, observamos que o comportamento de ν_p em função de p é próximo de $\log(p)$, o que nos leva à conjectura abaixo.

Conjectura B.1. *Quando $p \to \infty$, nos temos $\nu_p = \mathcal{O}(\log p)$.*

Referências Bibliográficas

[1] E. Aksoy, A. Çeşmelioğlu, W. Meidl, and A. Topuzoğlu, *On the carlitz rank of permutation polynomials*, Finite Fields and Their Applications, 15 (2009), pp. 428–440.

[2] E. R. Berlekamp, H. Rumsey, and G. Solomon, *On the solution of algebraic equations over finite fields*, Information and control, 10 (1967), pp. 553–564.

[3] F. Brochero Martínez, C. G. Moreira, N. Saldanha, and E. Tengan, *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, Coleção Projeto Euclides, IMPA, 2013.

[4] L. Carlitz, *Permutations in a finite field*, in Proc. Amer. Math. Soc, vol. 4, 1953, p. 194.

[5] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group.*, The Annals of Mathematics, 11 (1896), pp. 65–120.

[6] D. Gómez-Pérez, A. Ostafe, and A. Topuzoğlu, *On the carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences*, Journal of Complexity, 30 (2014), pp. 279–289.

[7] I. N. Herstein, *Topics in Algebra*, John Wiley & Sons, 2006.

[8] L. Işık and A. Winterhof, *Carlitz rank and index of permutation polynomials*, Finite Fields and Their Applications, 49 (2018), pp. 156–165.

[9] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields and Their Applications, 13 (2007), pp. 58–70.

[10] R. Lidi and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?, ii*, The American Mathematical Monthly, 100 (1993), pp. 71–74.

[11] R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, The American Mathematical Monthly, 95 (1988), pp. 243–246.

[12] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, vol. 65, Chapman & Hall/CRC, 1993.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20, Cambridge university press, 1997.

[14] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics, (1878), pp. 289–321.

[15] A. Masuda and M. Zieve, *Permutation binomials over finite fields*, Transactions of the American Mathematical Society, 361 (2009), pp. 4169–4180.

[16] A. M. Masuda and M. E. Zieve, *Nonexistence of permutationbinomials of certain shapes*, the electronic journal of combinatorics, 14 (2007), p. 12.

[17] C. Moreno, *Algebraic Curves over Finite Fields*, no. 97, Cambridge University Press, 1993.

[18] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Chapman and Hall/CRC, 2013.

[19] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106, Springer Science & Business Media, 2009.

[20] A. Topuzoğlu, *The carlitz rank of permutations of finite fields: A survey*, Journal of Symbolic Computation, 64 (2014), pp. 53–66.

[21] D. Wan and R. Lidl, *Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure*, Monatshefte für Mathematik, 112 (1991), pp. 149–163.

[22] M. E. Zieve, *Some families of permutation polynomials over finite fields*, International Journal of Number Theory, 4 (2008), pp. 851–857.