JOÃO PAULO GUARDIEIRO SOUSA

Polinômios de permutação e q-polinômios

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2021

JOÃO PAULO GUARDIEIRO SOUSA

Polinômios de permutação e q-polinômios

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Corpos Finitos.

Orientador: Prof. Dr. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG
2021

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

S725 Sousa, João Paulo Guardieiro, 1998-
2021 Polinômios de permutação e q-polinômios [recurso eletrônico] / João Paulo Guardieiro Sousa. - 2021.

Orientador: Guilherme Chaud Tizziotti.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2021.55
Inclui bibliografia.

1. Matemática. I. Tizziotti, Guilherme Chaud,1980-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, nº 94, PPGMAT				
Data:	24 de fevereiro de 2021	Hora de início:	09:00	Hora de encerramento:	10:30
Matrícula do Discente:	11912MAT006				
Nome do Discente:	João Paulo Guardieiro Sousa				
Título do Trabalho:	Polinômios de permutação e q-polinômios				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:					

Reuniu-se em web conferência pela plataforma Mconf-RNP, em conformidade com a PORTARIA Nº 36, DE 19 DE MARÇO DE 2020 da COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, pela Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Fabio Enrique Brochero Martínez - ICEx/UFMG; Victor Gonzalo Lopez Neumann - FAMAT/UFU e Guilherme Chaud Tizziotti - FAMAT/UFU orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Guilherme Chaud Tizziotti, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Fabio Enrique Brochero Martinez**, **Usuário Externo**, em 24/02/2021, às 10:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 24/02/2021, às 10:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 24/02/2021, às 14:14, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2507711** e o código CRC **6FC64794**.

Referência: Processo nº 23117.002292/2021-46 SEI nº 2507711

Dedicatória

A meus pais Cláudia e Valtuir e meu irmão Vinícius, responsáveis por me tornarem quem sou hoje.

A meus avós Dercílio Francisco de Souza e Lina da Silva e Souza, que estiveram comigo no primeiro dia de mestrado, mas não puderam estar presentes no último.

A todos com quem tive oportunidade de conviver nesses dois anos de mestrado.

Agradecimentos

Agradeço primeiramente a Deus por ter me dado forças para chegar até esse momento, superar os obstáculos e alcançar tantas graças. Por ter me dado a vida, minha família e meus amigos.

Agradeço também à Universidade Federal de Uberlândia e a todos os professores que dela fazem parte, que contribuíram diretamente para minha formação acadêmica, me ensinando novas formas de enxergar a matemática e sendo exemplo para o profissional o qual quero me tornar.

Em especial, agradeço a meu orientador Guilherme Chaud Tizziotti pelos ensinamentos ao longo de tantos anos de trabalho. Fico profundamente grato aos desafios de cada seminário, que me fizeram repensar meu modo de estudo. Obrigado pelo apoio e incentivo, principalmente por ter me dado um direcionamento.

Agradeço também aos professores Alonso Sepúlveda Castellanos, Cícero Fernandes de Carvalho e Victor Gonzalo Lopez Neumann, que contribuíram diretamente para esse trabalho, fazendo devidas revisões, auxiliando nos estudos das referências bibliográficas e nos seminários.

Não poderia deixar de agradecer à minha família, minha mãe Cláudia, meu pai Valtuir e meu irmão Vinícius com os quais aprendi a ser mais humano e ajudaram a moldar a pessoa que sou hoje. Agradeço ainda a todos os meus tios, primos e avós os quais sempre me acolheram nas dificuldades e me mostraram a beleza de se viver em família.

Aos meus amigos de mestrado, em especial Arthur, Elis, Fernando, Matheus, Paulo Victor e Walteir, por nunca me deixarem desanimar com os estudos, e também os da São Judas, Arnaldo, Benildo, Gabriel, Isabela, Lucas e Mary por serem meu apoio fora da faculdade.

Também agradeço à CAPES pelo aporte financeiro nesses dois anos de mestrado, proporcionado pelo programa PICME.

Por fim, a todos que, direta ou indiretamente, contribuíram de alguma forma para me tornar quem sou hoje, viabilizando chegar até aqui.

SOUSA, João Paulo Guardieiro. *Polinômios de permutação e q-polinômios.* 2021. (65 pág) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, discutimos alguns resultados envolvendo polinômios de permutação e q-polinômios, ambos definidos sobre corpos finitos. Introduziremos conceitos e teoremas básicos envolvendo cada uma dessas classes polinomiais para, enfim, relacioná-las, encontrando critérios para determinar se um q-polinômio dado é de permutação e estudando dois métodos para se obter q-polinômios que já tenham essa propriedade. Ao final dessa dissertação, aplicaremos os conhecimentos obtidos previamente para encontrar condições para que uma classe específica de polinômios seja planar.

Palavras-chave: Corpos finitos, polinômios de permutação, q-polinômios, polinômios planares.

SOUSA, João Paulo Guardieiro. *Permutation polynomials and q-polynomials.* 2021. (65 pages) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we discuss some results involving permutation polynomials and q-polynomials, both defined over finite fields. Firstly we introduce basic concepts and theorems concerning each one of those polynomials classes. Then, we find criteria to determinate if a given q-polynomial is a permutation one and study two methods in order to obtain q-polynomials which already have this property. At the end of this dissertation, we will apply the results obtained previously in order to find conditions under which a specific polynomial class can be planar.

Keywords: Finite fields, permutations polynomials, q-polynomials, planar polynomials.

Lista de Símbolos

$\mathbb{F}_q$: corpo finito com q elementos.
$\mathbb{F}_q^*$: grupo multiplicativo associado ao corpo finito $\mathbb{F}_q$ ($\mathbb{F}_q \backslash \{0\}$).
$\mathbb{F}_q[X]$: anel de polinômios na variável X com coeficientes no corpo $\mathbb{F}_q$.
$\mathcal{L}_n(\mathbb{F}_{q^n})$: álgebra dos q-polinômios sobre $\mathbb{F}_{q^n}$ módulo $X^{q^n} - X$.
$\mathcal{D}_n(\mathbb{F}_{q^n})$: álgebra das matrizes de Dickson sobre $\mathbb{F}_{q^n}$ de ordem n.
μ_n: grupo das raízes n-ésimas da unidade.
P_q: grupo dos polinômios de permutação sobre $\mathbb{F}_q$ de grau menor que q.

Sumário

Introdução

É difícil determinar quando os matemáticos da antiguidade começaram a estudar polinômios. O problema de se encontrar raízes para uma equação linear, assim como muitos tópicos matemáticos, provavelmente surgiu da necessidade cotidiana dos povos antigos e foi se desenvolvendo até a teoria que temos hoje. Al-Khwarizmi (780-850), considerado um dos pais da álgebra, foi talvez o primeiro matemático a formalizar o processo de resolução de equações de grau um e dois, justificando a famosa "operação"de "passar para o outro lado da igualdade", enquanto Omar Khayyam (1048-1131) foi um dos pioneiros do estudo de equações cúbicas, utiliando-se fortemente de modelagens geométricas e seu estudo sobre razões.

Uma das grandes dificuldades desses autores era a escrita das equações. A expressão $ax^2 + bx = c$, por exemplo, era chamada por Al-Khwarizmi de "quadrado e raiz igual a um número", enquanto Khayyam chamava a expressão $x^3 + bx^2 = ax + c$ de "cubo da coisa mais quadrado da coisa igual a coisa mais número". A notação atual com os símbolos de igualdade, soma, subtração e a representação da variável como uma letra data de meados do século XVI e esse pode ter sido o ponto de partida para que os matemáticos tratassem polinômios como "entes algébricos"ao invés de equações.

Devido ao grande número de aplicações e à dimensão que o estudo desses objetos tomou, é comum autores e pesquisadores focarem seus trabalhos em polinômios com algumas características específicas. Seguindo esse pensamento, também focamos nossos estudos em duas classes polinomiais definidas sobre corpos finitos: os polinômios de permutação, que induzem uma bijeção no corpo de coeficientes, e os q-polinômios, em cujas expressões a variável só admite expoentes que sejam potências da característica do corpo. Os fundamentos para este trabalho podem ser encontrados nos capítulos 2, 3 e 7 de [15] e os principais artigos complementares são [20], [21], [7] e [3].

A dissertação está organizada como se segue. No primeiro capítulo, apresentamos resultados básicos sobre corpos finitos, para familiarizar leitores que não tenham tanto contato com esse assunto ou com as notações e teoremas essenciais para o desenvolvimento da teoria. No segundo capítulo, apresentamos a álgebra dos q-polinômios, bem como a sua identificação com a álgebra de matrizes de Dickson. O terceiro capítulo trata do grupo de polinômios de permutação, e nele destacamos a Proposição 3.22, que é nossa generalização da Proposição 3 de [21]. Em seguida, nós relacionamos essas duas classes polinomiais: no quarto capítulo, estudamos a bijetividade de alguns polinômios e apresentamos dois métodos para se construir q-polinômios de permutação, enquanto que no quinto capítulo estudamos polinômios planares, baseados em [3], mas com uma abordagem diferente: ao invés de usarmos curvas algébricas, usamos o Teorema 4.13, que é definido para q-polinômios.

João Paulo Guardieiro Sousa
Uberlândia-MG, 24 de fevereiro de 2021.

Capítulo 1

Corpos Finitos

A teoria de corpos finitos desenvolveu-se de forma considerável no século XIX, porém a sua origem data dos séculos XVII e XVIII. Grandes matemáticos como Pierre de Fermat, Leonhard Euler, Joseph-Louis Lagrange e Carl Gauss foram os primeiros a trabalharem com corpos finitos. Algumas áreas de suas aplicações são criptografia e teoria de códigos. Assim, com o surgimento dos computadores, o estudo e o uso de corpos finitos foram muito difundidos no século XX. Outras áreas importantes em que corpos finitos aparecem são geometria algébrica, geometria aritmética, geometria finita, combinatória e teoria dos números. A grande diferença dessas estruturas para o corpo dos números reais ou complexos por exemplo, é a característica positiva, o que acaba em alguns casos simplificando vários resultados (ou deixando eles mais interessantes). Este capítulo é baseado nas referências [12] e [15], mas muitos outros resultados podem ser encontrados em livros básicos de Estruturas Algébricas.

Definição 1.1. Um **corpo** é um conjunto F munido de uma operação aditiva $+$ e uma multiplicativa $*$ satisfazendo:

1. $+$ e $*$ são associativas, isto é, para quaisquer $a, b, c \in F$,

$$a + (b + c) = (a + b) + c \text{ e } a * (b * c) = (a * b) * c.$$

2. Existe um elemento nulo 0 e um identidade (ou unidade) 1 em F tais que, para todo $a \in F$,

$$a + 0 = 0 + a = a \text{ e } a * 1 = 1 * a = a.$$

3. Para cada $a \in F$ e $b \in F\backslash\{0\}$, existe um elemento oposto $-a$ e um inverso b^{-1} em F tais que

$$a + (-a) = (-a) + a = 0 \text{ e } b * b^{-1} = b^{-1} * b = 1.$$

4. $+$ e $*$ são comutativas, isto é, para quaisquer $a, b \in F$,

$$a + b = b + a \text{ e } a * b = b * a.$$

5. $*$ é distributiva com relação a $+$, isto é, para quaisquer $a, b, c \in F$,

$$a * (b + c) = a * b + a * c.$$

Se o conjunto F for finito, o corpo será dito **finito** e o número de elementos de F é chamado de ordem de F.

Se $G \subset F$ for um subconjunto de F que também seja um corpo com as mesmas operações de F, diremos que G é um subcorpo de F.

Os exemplos mais conhecidos de corpos são os conjuntos dos números racionais, reais e complexos com as operações usuais. Já para corpos finitos, merecem destaque os conjuntos quociente $\mathbb{Z}_p$, em que p é um número primo, formado pelas classes de equivalência da relação "congruência módulo p" (dizemos que a e b são equivalente segundo essa relação quando p dividir $a-b$). Essa relação está melhor explicada em [12, p.16].

Em $\mathbb{R}$ os elementos $1, 1+1, 1+1+1, ...$ são todos distintos. Isso não ocorre num corpo finito! Mais ainda, existe um menor natural positivo p tal que $\underbrace{1+\cdots+1}_{p \text{ vezes}} = 0$. Esse número é chamado de **característica** de F.

Lema 1.2. *A característica de um corpo finito F é sempre um número primo.*

Demonstração. Consideremos os elementos $1, 1+1, 1+1+1, ...$ Uma vez que F contém apenas uma quantidade finita de tais elementos que sejam distintos, existem inteiros k e m com $1 \leq k < m$ tal que $\underbrace{1+\cdots+1}_{k \text{ vezes}} = \underbrace{1+\cdots+1}_{m \text{ vezes}}$ ou, $\underbrace{1+\cdots+1}_{(m-k) \text{ vezes}} = 0$, então existe um natural positivo p tal que $\underbrace{1+\cdots+1}_{p \text{ vezes}} = 0$ e pelo Princípio da Boa Ordem, podemos supor que p é o menor natural com essa propriedade. Falta provar que p é primo.

Se p não fosse primo, poderíamos escrever $p = km$ com $k, m \in \mathbb{N}$, $1 < k$, $m < n$. Então, $0 = \underbrace{1+\cdots+1}_{p \text{ vezes}} = \underbrace{1+\cdots+1}_{km \text{ vezes}} = \underbrace{(1+\cdots+1)}_{k \text{ vezes}}\underbrace{(1+\cdots+1)}_{m \text{ vezes}}$, e isso implica $\underbrace{1+\cdots+1}_{k \text{ vezes}} = 0$ ou $\underbrace{1+\cdots+1}_{m \text{ vezes}} = 0$, já que F não tem divisores de zero. Isso contradiz a minimalidade de p. ■

É possível verificar que o corpo $\mathbb{Z}_p$ tem característica p, mas também é interessante observar que todo corpo de característica p contém uma cópia isomorfa de $\mathbb{Z}_p$. De fato, existe um único homomorfismo $f : \mathbb{Z} \to F$, definido por $f(1) = 1_F$ ([12, p. 133]), em que 1 é a unidade dos inteiros e 1_F a unidade de F, e seu núcleo é um ideal de $\mathbb{Z}$ ([12, p. 127]), sendo, portanto, da forma $d\mathbb{Z}$ para algum inteiro d ([12, p. 8]). Como a imagem de f é finita, temos $d \neq 0$. Das definições de núcleo e característica, vemos que $d = p$. Assim, existe um isomorfismo entre $\mathbb{Z}_p$ e sua imagem segundo f ([12, p. 131]): um subcorpo de F denotado por $\mathbb{F}_p$.

Encontrar a característica de um corpo finito F pode parecer, a princípio, algo complicado. Mas essa informação pode ser obtida a partir de sua ordem.

Lema 1.3. *Seja F um corpo finito de característica p. Então F contém p^n elementos para algum natural n.*

Demonstração. Podemos enxergar F como um $\mathbb{F}_p$-espaço vetorial, e uma vez que F é finito, ele é um espaço de dimensão finita sobre $\mathbb{F}_p$, digamos n. Então F tem uma base sobre $\mathbb{F}_p$ consistindo de n elementos, digamos $b_1, b_2, ..., b_n$. Logo, cada elemento de F pode ser representado de forma única como $a_1b_1 + \cdots + a_nb_n$, em que $a_1, ..., a_n \in \mathbb{F}_p$. Como cada a_i pode assumir p valores, F tem exatamente p^n elementos. ■

Assim, sabendo-se a ordem de F, que será obrigatoriamente a potência de algum primo, sabemos sua característica.

Como, para qualquer $a \in F$, vale $a = \underbrace{1+\cdots+1}_{a \text{ vezes}}$, temos

$$\underbrace{a+\cdots+a}_{p \text{ vezes}} = \underbrace{\underbrace{(1+\cdots+1)}_{a \text{ vezes}}+\cdots+\underbrace{(1+\cdots+1)}_{a \text{ vezes}}}_{p \text{ vezes}} = \underbrace{\underbrace{(1+\cdots+1)}_{p \text{ vezes}}+\cdots+\underbrace{(1+\cdots+1)}_{p \text{ vezes}}}_{a \text{ vezes}} = 0,$$

isto é, qualquer elemento de um corpo finito multiplicado pela característica é o elemento nulo. Além de simplificar muitos resultados, esse fato também implica no seguinte.

Teorema 1.4. *Seja F um corpo de característica prima p. Então,*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n},$$

para todos $a, b \in F$ e $n \in \mathbb{N}$.

Demonstração. Usamos o fato de que

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i} \equiv 0 (\text{mod } p)$$

para todo $i \in \mathbb{Z}$ com $0 < i < p$, o que segue do fato de $\binom{p}{i}$ ser um inteiro e da observação de que o fator p do numerador não poder ser cancelado. Então, pelo Teorema do Binômio de Newton,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p = a^p + b^p,$$

e usando indução sobre n, completamos a prova. ■

1.1 Extensão de Corpos

Já usamos o conceito de subcorpos. Por exemplo, vimos que todo corpo finito de característica p tem um subcorpo isomorfo a $\mathbb{Z}_p$. Mas também podemos fazer o "contrário", buscar um corpo K que contenha (uma cópia isomorfa, se necessário) um corpo F dado: a isso chamamos **extensão de corpos**. Traremos apenas as definições e teoremas que utilizaremos adiante, mas vários resultados sobre esse assunto podem ser encontrados em ([5, Cap. 14, 15]).

Definição 1.5. Um **polinômio** sobre um corpo F é uma expressão da forma

$$f(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n,$$

em que n é um inteiro não negativo e os **coeficientes** a_i, $0 \leq i \leq n$, são elementos de F. Se $f(X)$ for um polinômio com, pelo menos, um coeficiente não nulo, seja n o maior índice tal que $a_n \neq 0$. Então, a_n é chamado de **coeficiente líder** e a_0 é chamado **termo constante**, enquanto n é chamado **grau** e denotado por $n = \text{gr}(f(X))$. Polinômios com grau 0 são chamados de **polinômios constantes**. Se o coeficiente líder do polinômio for 1, diremos que o polinômio é **mônico**. O conjunto dos polinômios com coeficientes em F forma um anel ([12, p. 117]), que será denotado por $F[X]$.

Frequentemente, quando estiver claro que estamos trabalhando com um polinômio ao invés de um elemento do corpo dos escalares, vamos denotar um polinômio $f(X)$ simplesmente por f. Um polinômio $f \in F[X]$ é dito **irredutível** em F quando seus únicos divisores em $F[X]$ são $c, \pm f$, em que c é um polinômio constante não nulo.

Definição 1.6. Dado um polinômio $f = a_0 + a_1 X + \cdots + a_n X^n \in F[X]$, dizemos que $\alpha \in F$ é uma **raiz** de f se tivermos $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

É possível mostrar que o número máximo de raízes de um polinômio é igual ao seu grau e que qualquer polinômio $f \in F[X]$ pode ser escrito da forma $f(X) = (X-\alpha_1)^{n_1} \cdots (X-\alpha_s)^{n_s} g(X)$, em que $\alpha_1, ..., \alpha_s \in F$ são as únicas raízes de f, $n_1, ..., n_s$ são inteiros positivos e $g(X)$ é um polinômio irredutível em $F[X]$ ([10, p. 104]). O inteiro n_i é chamado de **multiplicidade** da raiz α_i. Se tivermos $n_i = 1$, α_i será chamada de **raiz simples** de f. Caso contrário, α_i será chamada de **raiz múltipla** de f.

Definição 1.7. Dado um polinômio $f(X) = \sum_{i=0}^{n} a_i X^i$, definimos sua **derivada** como sendo o polinômio $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1} = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$.

A multiplicidade de uma raiz de um polinômio f pode ser observada a partir das derivadas de f. Por se tratar de um resultado que envolve muitos cálculos, vamos assumi-lo sem demonstração.

Teorema 1.8. *[15, Teorema 1.68] Sejam $f \in F[X]$ e $\alpha \in F$. α é uma raiz múltipla de $f(X)$ se, e somente se, α for raiz de $f(X)$ e de $f'(X)$.*

De modo similar à construção dos corpos $\mathbb{Z}_p$, podemos encontrar uma extensão para um corpo F de ordem q. Para isso, considere $f \in F[X]$ um polinômio irredutível e suponha que $\text{gr}(f) = n$. Definimos em $F[X]$ a relação de equivalência dada por "$a \sim b$ quando f dividir $a - b$".

Cada possível resto da divisão por f está em uma classe diferente, e qualquer polinômio pertence à classe do seu respectivo resto. Então o conjunto $K = \{\overline{a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}} : a_i \in F, i = 0, ..., n-1\}$, formado pelas classes de equivalência, possui q^n elementos e, usando-se as operações usuais para classes, vemos que K é um corpo (aqui usamos o fato de f ser irredutível para garantir que todos os elementos não nulos tenham um inverso multiplicativo). Além disso, a aplicação $h : F \to K, h(c) = \overline{c}$ é um homomorfismo injetor. Desse modo, K contém uma cópia isomorfa de F. Em outras palavras, K é uma extensão de F.

Suponha que F tenha p^n elementos. Usando uma demonstração completamente análoga ao Lema 1.3, podemos mostrar que qualquer extensão de F terá p^{nm} elementos para algum inteiro positivo m. Além disso, é possível mostrar que existe pelo menos um polinômio irredutível sobre F de grau k para qualquer inteiro positivo k ([15, Teorema 3.25]) e, tomando esse polinômio no procedimento acima, o corpo K encontrado terá p^{nk} elementos. Assim, podemos sempre encontrar uma extensão de F com p^t elementos, para qualquer t múltiplo de n. Isso pode nos incentivar a procurar um subcorpo de F com p^r elementos para qualquer divisor r de n. Isso é sempre possível, mas para demonstrarmos esse fato, precisaremos definir corpos de decomposição e, antes disso, precisamos estudar um pouco mais das extensões.

Definição 1.9. Um elemento α em alguma extensão K de F é dito **algébrico** sobre F se existir um polinômio não nulo $f(X) \in F[X]$ que tenha α como raiz. Se todos os elementos de K forem algébricos sobre F, diremos que K é uma **extensão algébrica** de F.

Podemos enxergar K como um F-espaço vetorial. Se tivermos $\dim K$ finita, diremos que K é uma **extensão finita** de F e a dimensão será chamada **grau** da extensão e denotada por $[K : F]$. Extensões finitas e algébricas se relacionam da seguinte forma.

Teorema 1.10. *Se K for uma extensão finita de F, então K será uma extensão algébrica de F.*

Demonstração. Para qualquer elemento $\alpha \in K$, suas potências $1, \alpha, \alpha^2, ..., \alpha^n$ não podem ser linearmente independentes se $n > \dim K$. Então, existem elementos $a_0, ..., a_n \in F$ não todos nulos tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, isto é, α é raiz do polinômio $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ e temos α algébrico sobre F. ∎

Proposição 1.11. *Seja α um elemento algébrico sobre F. O conjunto dos polinômios de $F[X]$ que se anulam em α é um ideal de $F[X]$, gerado por um único elemento: o polinômio mônico de menor grau que tem α como raiz. Além disso, esse gerador é irredutível.*

Demonstração. Seja

$$I = \{f : f \in F[X], f(\alpha) = 0\}.$$

Vamos mostrar que I é um ideal. Primeiramente, é claro que $0 \in I$ e $I \neq \emptyset$. Agora, dados $f, g \in I$, temos

$$(f+g)(\alpha) = f(\alpha) + g(\alpha) = 0 + 0 = 0$$

e $f + g \in I$. Por fim, para todos $f \in I$ e $h \in F[X]$, temos

$$(f \cdot h)(\alpha) = f(\alpha) \cdot h(\alpha) = 0 \cdot h(\alpha) = 0,$$

o que mostra que $f \cdot h \in I$ e I é um ideal.

Agora, seja $m(X)$ o polinômio de menor grau em I. É claro que $\langle m(X)\rangle \subseteq I$, então precisamos mostrar que $I \subseteq \langle m(X)\rangle$. Para isso, seja $f(X) \in I$. Existem $a(X), b(X) \in F[X]$ tais que

$$f(X) = a(X)m(X) + b(X),$$

com $b(X) = 0$ ou $\text{gr}(b) < \text{gr}(m)$. Mas, por propriedades de ideais, temos

$$b(X) = f(X) - a(X)m(X) \in I$$

e, pela minimalidade do grau de m, devemos ter $b(X) = 0$ e $I = \langle m(X)\rangle$.

Por fim, suponha, por contradição, que possamos escrever $m(X) = g(X)h(X)$ com $1 < \text{gr}(g)$,$\text{gr}(h) < \text{gr}(m)$. Então, como $m(\alpha) = 0$, temos $g(\alpha) = 0$ ou $h(\alpha) = 0$, o que é uma contradição com a minimalidade do grau de m. ■

O polinômio gerador desse ideal será chamado de **polinômio minimal** de α sobre F. Podemos nos questionar se ele possui outras raízes e, em caso afirmativo, se elas se relacionam com α. Se F for um corpo finito, a resposta é muito simples.

Definição 1.12. Sejam F um corpo finito com q elementos e α um elemento em alguma extensão K de F. Os elementos $\alpha^q, \alpha^{q^2}, \alpha^{q^3}, ...$ são chamados **conjugados** de α com respeito a F.

Lema 1.13. *Sejam F um corpo finito com q elementos e α um elemento algébrico sobre F. Então, seus conjugados com relação a F também são raízes do seu polinômio minimal.*

Demonstração. Seja $m(X) = \sum_{i=0}^{n} a_i X^i$ o polinômio minimal de α sobre F. Os conjugados de α são da forma α^{q^j}, com j um número inteiro não negativo. Então, para todo j, vale

$$m(\alpha^{q^j}) = \sum_{i=0}^{n} a_i (\alpha^{q^j})^i = \sum_{i=0}^{n} a_i (\alpha^i)^{q^j} = \left(\sum_{i=0}^{n} a_i \alpha^i\right)^{q^j} = m(\alpha)^{q^j} = 0$$

e o resultado segue. ■

Inspirados por esse lema, já temos um método para determinar o polinômio minimal de um elemento α sobre F, um corpo finito com q elementos. Basta calcularmos as potências $\alpha, \alpha^q, \alpha^{q^2}, ...$ até encontrarmos o menor natural positivo d tal que $\alpha^{q^d} = \alpha$, isto é, precisamos determinar os conjugados distintos de α. O natural d será o grau do polinômio minimal $m(X)$ de α e temos

$$m(X) = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{d-1}}).$$

Exemplo 1.14. Considere $F = \{0, 1\}$, β um elemento em uma extensão de F cujo polinômio minimal sobre F seja $X^5 + X^2 + 1$ e $\alpha = \beta^3 + \beta^2$. Temos

$$\begin{aligned} \alpha^2 &= \beta^4 + \beta^3 + \beta \\ \alpha^4 &= \beta + 1 \\ \alpha^8 &= \beta^2 + 1 \\ \alpha^{16} &= \beta^4 + 1 \\ \alpha^{32} &= \alpha \end{aligned}$$

Dessa forma, temos $d = 5$ e

$$m(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)(X - \alpha^{16}) = X^5 + X^4 + X^2 + X + 1$$

é o polinômio minimal de α sobre F.

Teorema 1.15. *Sejam α um elemento algébrico sobre F, n o grau de seu polinômio minimal p e E o F-espaço vetorial que tem como base $\{1, \alpha, ..., \alpha^{n-1}\}$. Então E é um corpo e sua dimensão é n.*

Demonstração. Seja $f \in F[X]$. Existem $q, r \in F[X]$ tais que $f = pq + r$ e $\text{gr}(r) < \text{gr}(p)$. Então,

$$f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Desse modo, $f(\alpha)$ pertence a E, e é fácil ver que o produto de dois elementos de E também está em E. Suponha que $f(\alpha) \neq 0$. Daí, f não é divisível por p, e como p é irredutível, temos $\text{mdc}(f, p) = 1$. Assim, existem $g, h \in F[X]$ tais que $fg + ph = 1$ ([12, p. 167,168]), donde

$$f(\alpha)g(\alpha) = 1$$

e temos $f(\alpha)$ invertível em E. ■

Denotaremos por $F(\alpha)$ o F-espaço vetorial (que sabemos ser um corpo) que tem como base as potências de α.

Podemos ainda tomar extensões de uma extensão, e é de se esperar que se ambas forem finitas, a extensão final também o seja.

Teorema 1.16. *Se K for uma extensão finita de F e M for uma extensão finita de K, então M é uma extensão finita de F e satisfaz a relação*

$$[M : F] = [M : K][K : F].$$

Demonstração. Sejam $\{v_1, ..., v_r\}$ uma base de M sobre K e $\{u_1, ..., u_s\}$ uma base de K sobre F. Vamos provar que

$$B = \{v_i u_j : i = 1, ..., r, j = 1, ...s\}$$

é uma base de M sobre F. Primeiramente, vejamos que B é L.I. sobre F. De fato, sejam $a_{ij} \in F$, $1 \leq i \leq r$, $1 \leq j \leq s$ e suponha

$$(a_{11}u_1 + \cdots + a_{1s}u_s)v_1 + \cdots + (a_{r1}u_1 + \cdots + a_{rs}u_s)v_r = 0.$$

Como cada $a_{ij}u_i$ está em K, segue, pela independência linear dos v_j's que

$$\begin{aligned} a_{11}u_1 + \cdots + a_{1s}u_s &= 0 \\ &\vdots \\ a_{r1}u_1 + \cdots + a_{rs}u_s &= 0. \end{aligned}$$

Mas, como os a_{ij} estão em F, segue, pela independência linear dos u_i's que $a_{ij} = 0$ para todos $i = 1, ..., r, j = 1, ...s$. Logo, B é L.I. sobre F.

Resta ver que B gera M a partir de F. De fato, seja $\gamma \in M$. Sendo $\{v_1, ..., v_r\}$ uma base de M sobre K, existem $b_1, ..., b_r \in K$ tais que

$$\gamma = b_1 v_1 + \cdots + b_r v_r.$$

Como $b_i \in K$, para todo $i = 1, ..., r$, e $\{u_1, ..., u_s\}$ é uma base de K sobre F, existem $a_{ij} \in F$, $1 \leq i \leq r, 1 \leq j \leq s$, tais que

$$b_i = a_{i1} u_1 + \cdots + a_{is} u_s.$$

Daí, segue que

$$\gamma = \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} a_{ij} v_i u_j,$$

e B é um conjunto gerador de M sobre F. ■

Desse modo, se tivermos α, β algébricos sobre F, claramente temos β algébrico sobre $F(\alpha)$ e podemos considerar o corpo $F(\alpha)(\beta)$. Veja que qualquer corpo que contenha F, α e β conterá $F(\alpha)(\beta)$. Por isso, frequentemente, diremos que $F(\alpha)(\beta)$ é o menor corpo contendo F, α e β.

Pelo Teorema 1.16, temos $F(\alpha)(\beta)$ uma extensão finita, e portanto algébrica, sobre F. Além disso, os corpos $F(\alpha)(\beta)$ e $F(\beta)(\alpha)$ são iguais. Por isso, denotaremos $F(\alpha)(\beta)$ por $F(\alpha, \beta)$ e, de modo indutivo, dados $\alpha_1, ..., \alpha_n$ algébricos sobre F, $F(\alpha_1, ..., \alpha_n)$ denotará o menor corpo contendo F e $\alpha_1, ..., \alpha_n$.

Agora podemos definir os corpos de decomposição.

Definição 1.17. Seja $f \in F[X]$ um polinômio de grau $n \geq 1$. O **corpo de decomposição** de f é a menor extensão finita K de F em que é possível escrever $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$, com $\alpha_1, ..., \alpha_n \in K$, e $K = F(\alpha_1, ..., \alpha_n)$.

É possível mostrar que todo polinômio admite um único (a menos de isomorfismo) corpo de decomposição ([12, p. 359]).

O conjunto dos elementos não nulos de um corpo finito F com $q = p^n$ elementos forma um grupo multiplicativo F^* de ordem $q - 1$ ([12, p. 23]) e, portanto, $a^{q-1} = 1$ para todo $a \in F^*$ ([12, p. 59]). Assim, $a^q = a$ para todo $a \in F$ (esse resultado é óbvio para $a = 0$). Isso nos diz que o polinômio $X^q - X$ se fatora em F como $f(X) = \prod_{a \in F}(X - a)$. Além disso, como F tem p^n elementos, F contém $\mathbb{Z}_p$ como subcorpo. Então, F é o (único) corpo de decomposição de $X^q - X \in \mathbb{Z}_p[X]$.

Essa observação é muito importante, ela nos diz que quaisquer dois corpos finitos de mesma ordem q são isomorfos, uma vez que são corpos de decomposição do polinômio $X^q - X$ sobre $\mathbb{Z}_p$, em que p é a característica desses corpos (que está unicamente determinada por q). Por isso, um corpo finito de ordem q será denotado por $\mathbb{F}_q$.

Agora podemos buscar os subcorpos de $\mathbb{F}_{p^n}$ a partir dos divisores de n: se r dividir n, então o polinômio $X^{p^r} - X$ dividirá $X^{p^n} - X$ em $\mathbb{F}_p[X]$, donde toda raiz de $X^{p^r} - X$ é uma raiz de $X^{p^n} - X$ e, portanto, pertence a $\mathbb{F}_{p^n}$. Em particular, $\mathbb{F}_{p^r}$ é um subcorpo de $\mathbb{F}_{p^n}$. Assim, temos o seguinte.

Teorema 1.18. *Dados um número primo p e naturais não nulos a, b, $\mathbb{F}_{p^a}$ é subcorpo de $\mathbb{F}_{p^b}$ (equivalentemente, $\mathbb{F}_{p^b}$ é extensão de $\mathbb{F}_{p^a}$) se, e somente se, a dividir b.*

Já vimos que o conjunto dos restos da divisão por um polinômio irredutível forma um corpo finito, no entanto essa estrutura pode parecer um pouco complicada para se trabalhar. Podemos então enxergar o corpo como sendo o conjunto das potências de um certo elemento, e esse problema será facilmente resolvido.

Teorema 1.19. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico, isto é, $\mathbb{F}_q^* = \{\alpha, \alpha^2, ..., \alpha^{q-1}\}$ para algum elemento α conveniente.*

Demonstração. Podemos assumir $q > 3$. Seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para cada $i, 1 \leq i \leq m$, o polinômio $x^{\frac{h}{p_i}} - 1$ tem, no máximo, $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Uma vez que $\frac{h}{p_i} < h$, segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um tal elemento e definimos $b_i = a_i^{\frac{h}{p_i^{r_i}}}$. Então $b_i^{p_i^{r_i}} = 1$, logo a ordem de b_i é um divisor de $p_i^{r_i}$ e é, com isso, da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Por outro lado,

$$b_i^{p_i^{r_i - 1}} = a_i^{\frac{h}{p_i}} \neq 1,$$

e, assim, a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h. Suponha, do contrário, que a ordem de b seja um divisor próprio de h e seja, portanto, um divisor de, no mínimo, um dos m inteiros $\frac{h}{p_i}, 1 \leq i \leq m$, digamos de $\frac{h}{p_1}$. Então, temos

$$1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} b_2^{\frac{h}{p_1}} \cdots b_m^{\frac{h}{p_1}}.$$

Agora, para $2 \leq i \leq m$, $p_i^{r_i}$ divide $\frac{h}{p_1}$, e, assim obtemos $b_1^{\frac{h}{p_1}} = 1$. Isso implica que a ordem de b_1 deve dividir $\frac{h}{p_1}$, o que é impossível, já que a ordem de b_1 é $p_1^{r_1}$. Logo, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. ■

Definição 1.20. Um gerador para o grupo cíclico $\mathbb{F}_q^*$ é chamado um **elemento primitivo** de $\mathbb{F}_q$.

Assim como acontece em qualquer grupo, dado um gerador α para $\mathbb{F}_q^*$, α^n é também um elemento primitivo se, e somente se, n for coprimo com $q - 1$, logo existem $\varphi(q-1)$ elementos primitivos em $\mathbb{F}_q$, em que φ é a função de Euler.

Já sabemos escrever todos os elementos não nulos de um corpo finito $\mathbb{F}_q$ como potências de um elemento primitivo, mas quando trabalhamos com uma extensão $\mathbb{F}_{q^n}$ desse corpo, também podemos tomar uma base para esse $\mathbb{F}_q$-espaço vetorial formada por potências de um elemento específico.

Definição 1.21. Uma base para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ da forma $\{\beta, \beta^q, ..., \beta^{q^{n-1}}\}$, consistindo de um elemento $\beta \in \mathbb{F}_{q^n}$ conveniente e seus conjugados é chamada uma **base normal**.

O Teorema da Base Normal (Teorema 2.26) garante que qualquer extensão finita $\mathbb{F}_{q^n}$ admite uma base normal sobre $\mathbb{F}_q$. Apresentaremos uma demonstração alternativa para esse teorema, proposta em [15, Teorema 3.72] usando uma classe especial de polinômios.

1.2 Funções traço e norma

Qualquer extensão $\mathbb{F}_{q^n}$ do corpo $\mathbb{F}_q$ pode ser vista como um $\mathbb{F}_q$-espaço vetorial. Desse modo, podemos estudar os **funcionais lineares**: as transformações lineares de $\mathbb{F}_{q^n}$ em $\mathbb{F}_q$. Uma vez que o corpo de escalares é finito, seremos capazes de caracterizar todos esses funcionais usando um específico.

Definição 1.22. Dado um elemento $\alpha \in \mathbb{F}_{q^n}$, definimos o **traço** de α sobre $\mathbb{F}_q$ como sendo

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

Se tivermos $q = p$ (ou seja, se $\mathbb{F}_q$ for o subcorpo primo de $\mathbb{F}_{q^n}$), $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ será chamado de **traço absoluto** de α e denotado simplesmente por $\mathrm{Tr}_{\mathbb{F}_{q^n}}(\alpha)$.

Podemos enxergar o traço de um elemento sobre $\mathbb{F}_q$ como sendo a soma de seus conjugados com respeito a $\mathbb{F}_q$. Essa função traço nos permitirá caracterizar todos os funcionais lineares de $\mathbb{F}_{q^n}$ em $\mathbb{F}_q$. Para isso, vale destacar as seguintes propriedades.

Teorema 1.23. *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^n}$. A função $Tr_{F/K}$ satisfaz as propriedades:*

(i) $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$, *para todos* $\alpha, \beta \in F$.

(ii) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$, *para todos* $c \in K, \alpha \in F$.

(iii) $Tr_{F/K}$ *é uma transformação linear sobrejetora de* F *em* K.

(iv) $Tr_{F/K}(a) = na$, *para todo* $a \in K$.

(v) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$, *para todo* $\alpha \in F$.

Demonstração. (i) Para todos $\alpha, \beta \in F$, temos

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \cdots (\alpha+\beta)^{q^{n-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta). \end{aligned}$$

(ii) Como $c \in K$, temos $c^{q^i} = c$, para todo $i \geq 0$. Assim,

$$\begin{aligned} \mathrm{Tr}_{F/K}(c\alpha) &= (c\alpha) + (c\alpha)^q + \cdots + (c\alpha)^{q^{n-1}} = c\alpha + c^q\alpha^q + \cdots + c^{q^{n-1}}\alpha^{q^{n-1}} \\ &= c\alpha + c\alpha^q + \cdots + c\alpha^{q^{n-1}} = c\mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

(iii) Observemos que

$$(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha))^q = (\alpha+\alpha^q+\cdots+\alpha^{q^{n-1}})^q = \alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^n} = \alpha^q+\alpha^{q^2}+\cdots+\alpha = \mathrm{Tr}_{F/K}(\alpha).$$

Isso prova que a imagem de $\mathrm{Tr}_{F/K}$ está realmente em K. Os itens (i) e (ii) garantem a linearidade de $\mathrm{Tr}_{F/K}$.

É um resultado conhecido que a imagem de uma transformação linear é um subespaço vetorial do contradomínio. Uma vez que K tem dimensão 1 quando visto como K-espaço vetorial, precisamos apenas mostrar que existe $\alpha \in F$ com $\mathrm{Tr}_{F/K}(\alpha) \neq 0$ e teremos $\mathrm{Tr}_{F/K}$ uma aplicação sobrejetora. De fato, $\mathrm{Tr}_{F/K}(\alpha) = 0$ é equivalente a termos α uma raiz de $X^{q^{n-1}} + \cdots + X^q + X$ em F. Mas, esse polinômio pode ter, no máximo, q^{n-1} raízes e F tem q^n elementos.

(iv) Para $a \in K$,

$$\mathrm{Tr}_{F/K}(a) = a + a^q + \cdots + a^{q^{n-1}} = \underbrace{a + a + \cdots + a}_{n \text{ vezes}} = na.$$

(v) $\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q+(\alpha^q)^q+\cdots+(\alpha^q)^{q^{n-1}} = \alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^n} = \alpha^q+\alpha^{q^2}+\cdots+\alpha = \mathrm{Tr}_{F/K}(\alpha)$. ■

Agora podemos caracterizar os funcionais lineares usando a função traço.

Teorema 1.24. *Sejam $F = \mathbb{F}_{q^n}$ e $K = \mathbb{F}_q$. Os funcionais lineares de F em K são exatamente as aplicações $L_\beta, \beta \in F$, definidas pela relação $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$, para todo $\alpha \in F$. Além disso, $L_\beta \neq L_\gamma$ para todo $\beta \neq \gamma$.*

Demonstração. Repetindo as demonstrações dos itens $(i), (ii)$ e (iii) do teorema acima, é possível verificar que L_β é um funcional linear para cada $\beta \in F$. Agora, dados $\beta, \gamma \in F$, $\beta \neq \gamma$, temos

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta-\gamma)\alpha) \neq 0$$

para um elemento α conveniente (já que a função traço é sobrejetora). Então, $L_\beta \neq L_\gamma$.

Por fim, os funcionais L_β nos fornecem q^n funcionais distintos (já que F tem q^n elementos). Um funcional genérico de F em K pode ser obtido escolhendo a imagem dos elementos de uma base de F como K-espaço vetorial. Como uma tal base tem n elementos e K tem q elementos, podemos fazer q^n escolhas distintas para o funcional, isto é, não existe um funcional de F em K fora do conjunto $\{L_\beta : \beta \in F\}$. ■

O item (iii) do Teorema 1.23 nos disse que a função traço é sobrejetora, isto é, $Im(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}) = \mathbb{F}_q$. O Teorema do Núcleo e da Imagem nos mostra que ela não é injetora quando $n > 1$, então podemos nos perguntar qual é seu núcleo.

Teorema 1.25. *Sejam $F = \mathbb{F}_{q^n}$ e $K = \mathbb{F}_q$. Então $\alpha \in F$ está no núcleo de $Tr_{F/K}$, isto é, $Tr_{F/K}(\alpha) = 0$ se, e somente se, $\alpha = \beta^q - \beta$ para algum elemento $\beta \in F$.*

Demonstração. Usando a linearidade da função traço e o item (v) do Teorema 1.23, a suficiência é clara. Para provar a necessidade, sejam $\alpha \in F$ tal que $\mathrm{Tr}_{F/K}(\alpha) = 0$ e β uma raiz de $X^q - X - \alpha$ em alguma extensão de F. Isto é, $\alpha = \beta^q - \beta$. Mas,

$$\begin{aligned} 0 &= \mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{n-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^n} - \beta^{q^{n-1}}) = \beta^{q^n} - \beta. \end{aligned}$$

Isso prova que $\beta \in F$. ■

O último resultado envolvendo a função traço é a sua transitividade: se tivermos F uma extensão de K e E uma extensão de F, como podemos relacionar o traço de um elemento de E sobre K usando o traço sobre F?

Teorema 1.26. *Sejam K um corpo finito com q elementos, F uma extensão finita de K e E uma extensão finita de F. Então*

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha)), \text{ para todo } \alpha \in E.$$

Demonstração. Escrevendo $[F : K] = m$ e $[E : F] = n$, temos $[E : K] = mn$ e

$$\begin{aligned} \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) &= \textstyle\sum_{i=0}^{m-1} \mathrm{Tr}_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}}\right)^{q^i} \\ &= \textstyle\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha). \end{aligned}$$

■

A função traço foi obtida somando os conjugados de um elemento, podemos obter uma função parecida tomando-se o produto desses conjugados.

Definição 1.27. Para um elemento $\alpha \in \mathbb{F}_{q^n}$, definimos a **norma** de α sobre $\mathbb{F}_q$ como sendo

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}.$$

A imagem da função norma está em $\mathbb{F}_q$. De fato,

$$(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha))^q = (\alpha \cdot \alpha^q \cdots \alpha^{q^{n-1}})^q = \alpha^q \cdot \alpha^{q^2} \cdots \alpha^{q^n} = \alpha^q \cdot \alpha^{q^2} \cdots \alpha = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha).$$

A função norma possui propriedades similares às da função traço, e também é transitiva.

Teorema 1.28. *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^n}$. A função $N_{F/K}$ satisfaz as propriedades:*

(i) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$.

(ii) $N_{F/K}$ *aplica sobrejetivamente* F *em* K *e* F^* *em* K^*.

(iii) $N_{F/K}(a) = a^n$, *para todo* $a \in K$.

(iv) $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$, *para todo* $\alpha \in F$.

Demonstração. (i) $$\begin{aligned} N_{F/K}(\alpha\beta) &= (\alpha\beta)\cdot(\alpha\beta)^q\cdots(\alpha\beta)^{q^{n-1}} \\ &= \alpha\beta\cdot\alpha^q\beta^q\cdots\alpha^{q^{n-1}}\beta^{q^{n-1}} = N_{F/K}(\alpha)N_{F/K}(\beta). \end{aligned}$$

(ii) Já sabemos que a imagem de $N_{F/K}$ está contida em K. Uma vez que $N_{F/K}(\alpha) = 0$ se, e somente se, $\alpha = 0$, $N_{F/K}$ aplica F^* em K^*. O item (i) nos diz que $N_{F/K}$ é um homomorfismo entre esses dois grupos multiplicativos. Assim, restrita a F^*, o núcleo de $N_{F/K}$ são as raízes de $X^{(q^n-1)/(q-1)}$, logo tem ordem $d \leq \frac{q^n-1}{q-1}$. O Primeiro Teorema do Isomorfismo nos mostra que a imagem de $N_{F/K}$ tem ordem $\frac{q^n-1}{d} \geq q-1$. Dessa forma, $N_{F/K}$ aplica sobrejetivamente F^* em K^* e F em K.

(iii) Para todo elemento $a \in K$, temos $a^{q^i} = a$, para todo $i \geq 0$, então

$$N_{F/K}(a) = a\cdot a^q\cdots a^{q^{n-1}} = \underbrace{a\cdot a\cdots a}_{n \text{ vezes}} = a^n.$$

(iv) $N_{F/K}(\alpha^q) = (\alpha^q)\cdot(\alpha^q)^q\cdots(\alpha^q)^{q^{n-1}} = \alpha^q\cdot\alpha^{q^2}\cdots\alpha^{q^n} = \alpha^q\cdot\alpha^{q^2}\cdots\alpha = N_{F/K}(\alpha)$.

■

Teorema 1.29. *Sejam K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então*

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha)), \text{ para todo } \alpha \in E.$$

Demonstração. Com as mesmas notações do Teorema 1.26, temos

$$\begin{aligned} N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}(\alpha^{(q^{mn}-1)/(q^m-1)}) = (\alpha^{(q^{mn}-1)/(q^m-1)})^{(q^m-1)/(q-1)} \\ &= \alpha^{(q^{mn}-1)/(q-1)} = N_{E/K}(\alpha). \end{aligned}$$

■

As funções traço e norma são usadas com certa frequência em pesquisas envolvendo polinômios sobre corpos finitos, e por isso foram destacadas nessa seção. A função traço também será usada neste trabalho.

1.3 Fecho algébrico de $\mathbb{F}_q$

Essa seção não será utilizada no decorrer do trabalho, ela só serve para mostrar como os corpos finitos facilitam alguns resultados. É fato que todo corpo possui um único (a menos de isomorfismo) fecho algébrico. Por exemplo, o fecho algébrico dos reais é o corpo dos complexos. Mas mostrar isso pode ser bastante trabalhoso e faz uso do Lema de Zorn ([8, seção 31]). No entanto, o fecho algébrico de um corpo finito $\mathbb{F}_q$ pode ser encontrado de maneira simples.

Definição 1.30. Seja K um corpo. Diremos que K é **algebricamente fechado** se todo polinômio não constante possuir uma raiz em K.

Definição 1.31. Seja F um corpo. O **fecho algébrico** de F é uma extensão K de F tal que K é algebricamente fechado e é composto exatamente pelos elementos algébricos sobre F.

O fecho algébrico de F é um corpo, pois dados α, β algébricos sobre F, $\alpha - \beta$ e $\alpha\beta^{-1}$ também são algébricos sobre F, pois estão na extensão $F(\alpha, \beta)$, que é finita sobre F.

Seja $\mathbb{F}_q$ um corpo finito. Vamos mostrar que seu fecho algébrico é $A = \cup_{n\in\mathbb{N}}\mathbb{F}_{q^n}$.

Inicialmente, precisamos definir as operações de A. Sejam $a, b \in A$. Então, existem $i, j \in \mathbb{N}$ tais que $a \in \mathbb{F}_{q^i}$ e $b \in \mathbb{F}_{q^j}$. Pelo Teorema 1.18, temos $a, b \in \mathbb{F}_{q^d}$, em que $d = \text{mdc}(i, j)$. Definimos então a soma e o produto de a com b em A como sendo, respectivamente, a soma e o produto entre a e b vistos como elementos de $\mathbb{F}_{q^d}$. Pode-se mostrar que, com essas operações, A é de fato um corpo.

Agora, $\mathbb{F}_q$ é subcorpo de A e, dado $\alpha \in A$, temos $\alpha \in \mathbb{F}_{q^m}$ para algum inteiro positivo m. Assim, α é raiz de $X^{q^m} - X \in \mathbb{F}_q[X]$ e, portanto, algébrico sobre $\mathbb{F}_q$. Resta provar que A é algebricamente fechado.

Para isso, seja $f = a_sX^s + \cdots + a_0 \in A[X]$ e tome α raiz de f em alguma extensão de A. Vamos mostrar que $\alpha \in A$. Cada coeficiente $a_i, i = 0, ..., s$ de f está em algum $\mathbb{F}_{q^{n_i}}$. Então, pelo Teorema 1.18, $f \in \mathbb{F}_{q^n}[X]$, em que $n = \text{mmc}(n_0, ..., n_s)$. Assim, α é algébrico sobre $\mathbb{F}_{q^n}$, donde $\mathbb{F}_{q^n}(\alpha)$ é uma extensão finita, digamos de grau m, sobre $\mathbb{F}_q$ (Teorema 1.16). Dessa forma, $\mathbb{F}_{q^n}(\alpha)$ é um corpo finito com q^m elementos, ou seja, isomorfo a $\mathbb{F}_{q^m}$, que é subcorpo de A. Com isso, provamos que $\alpha \in A$.

Capítulo 2

q-polinômios

No capítulo anterior, demos uma breve introdução à importância dos polinômios. Por exemplo, os corpos finitos foram definidos como sendo o corpo de decomposição de um certo polinômio e definimos extensões de corpos a partir de polinômios irredutíveis. Estudar polinômios definidos sobre corpos finitos pode parecer, a princípio, um trabalho muito extenso e vago. Então, é comum restringir os estudos para subconjuntos de $\mathbb{F}_q[X]$ com propriedades interessantes. Nesse capítulo, vamos destacar a álgebra $\mathcal{L}_n(\mathbb{F}_{q^n})$ formada pelos q-polinômios módulo $X^{q^n} - X$. Na última seção, vamos usar resultados dessa importante classe para fornecer uma demonstração alternativa para o Teorema da Base Normal.

2.1 q-polinômios

Definição 2.1. Um polinômio da forma

$$L(X) = \sum_{i=0}^{s} a_i X^{q^i},$$

com coeficientes em alguma extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ é chamado um **q-polinômio** (ou **polinômio q-linearizado**) sobre $\mathbb{F}_{q^n}$.

A justificativa para essa nomenclatura alternativa é a seguinte.

Teorema 2.2. *Seja $L \in \mathbb{F}_{q^n}[X]$ um q-polinômio sobre $\mathbb{F}_{q^n}$. Então L induz uma aplicação linear em $\mathbb{F}_{q^n}$ visto como $\mathbb{F}_q$-espaço vetorial.*

Demonstração. Dados $\alpha, \beta \in \mathbb{F}_{q^n}$ e $\gamma \in \mathbb{F}_q$, observemos que

$$L(\alpha + \beta) = \sum_{i=0}^{s} a_i(\alpha + \beta)^{q^i} = \sum_{i=0}^{s} a_i(\alpha^{q^i} + \beta^{q^i}) = L(\alpha) + L(\beta)$$

e

$$L(\gamma\alpha) = \sum_{i=0}^{s} a_i(\gamma\alpha)^{q^i} = \sum_{i=0}^{s} a_i\gamma^{q^i}\alpha^{q^i} = \sum_{i=0}^{s} a_i\gamma\alpha^{q^i} = \gamma L(\alpha).$$

Dessa forma, concluímos que L induz uma aplicação linear em $\mathbb{F}_{q^n}$ (visto como $\mathbb{F}_q$-espaço vetorial). ■

O teorema acima nos mostra que o conjunto de raízes de L é o núcleo da transformação linear induzida por L. Dessa forma, podemos transformar o problema de encontrar raízes do polinômio para o problema mais simples de encontrar um subespaço vetorial, que pode ser resolvido por meio de um sistema linear.

Teorema 2.3. *Sejam L um q-polinômio sobre $\mathbb{F}_q$ e $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ que contenha todas as raízes de L. Então as raízes de L têm a mesma multiplicidade, que pode ser 1 ou uma potência de q.*

Demonstração. Escrevendo

$$L = \sum_{i=0}^{s} a_i X^{q^i},$$

vemos que $L' = a_0$. Assim, L tem apenas raízes simples se, e somente se, $a_0 \neq 0$. Caso contrário, teremos $a_0 = \cdots = a_{k-1} = 0$ e $a_k \neq 0$ para algum $k > 0$. Assim, podemos escrever

$$L = \sum_{i=k}^{s} a_i X^{q^i} = \left(\sum_{i=k}^{s} a_i X^{q^{i-k}} \right)^{q^k},$$

que é a q^k-ésima potência de um q-polinômio que só tem raízes simples, isto é, todas as raízes de L possuem multiplicidade q^k. ■

A recíproca desse teorema não é verdadeira, por exemplo, sobre $\mathbb{F}_3$ o polinômio $X(X-1) = X^2 - X$ só tem raízes simples, mas não é um 3-polinômio. Entretanto, podemos encontrar uma "recíproca parcial"para ele. Antes disso, porém, precisamos do seguinte lema. Uma vez que sua demonstração exige cálculos extensos, vamos apenas referenciá-lo.

Lema 2.4. *[15, Teorema 3.52] Seja U um subespaço de $\mathbb{F}_{q^n}$ visto como $\mathbb{F}_q$-espaço vetorial. Então, para todo inteiro não negativo k, o polinômio*

$$L(X) = \prod_{\beta \in U} (X - \beta)^{q^k}$$

é um q-polinômio sobre $\mathbb{F}_{q^n}$.

Definição 2.5. Seja M um $\mathbb{F}_q$-espaço vetorial de dimensão finita, contido em alguma extensão de corpos de $\mathbb{F}_q$. Se, para todo elemento $\alpha \in M$ tivermos $\alpha^q \in M$, M será chamado de **q-módulo**.

Exemplo 2.6. Já sabemos que as raízes de um q-polinômio $L(X)$ sobre $\mathbb{F}_q$ formam um $\mathbb{F}_q$-espaço vetorial. Denotando $L(X) = \sum_{i=0}^{s} \alpha_i X^{q^i}$, temos, para toda raiz β de L,

$$L(\beta^q) = \sum_{i=0}^{s} \alpha_i (\beta^q)^{q^i} = \left(\sum_{i=0}^{s} \alpha_i \beta^{q^i} \right)^q = L(\beta)^q = 0,$$

isto é, a q-ésima potência de uma raiz de L é também uma raiz de L. Então, as raízes de um q-polinômio com coeficientes em $\mathbb{F}_q$ formam um q-módulo.

Inspirados por esse exemplo e munidos dos resultados anteriores, podemos fornecer a "recíproca parcial"do Teorema 2.3.

Teorema 2.7. *O polinômio mônico $L(X)$ é um q-polinômio sobre $\mathbb{F}_q$ se, e somente se, cada raiz de $L(X)$ tiver a mesma multiplicidade, que pode ser 1 ou uma potência de q, e as raízes formarem um q-módulo.*

Demonstração. Suponha inicialmente que L seja um q-polinômio. Então, basta aplicar o Teorema 2.3 e observar o Exemplo 2.6.

Reciprocamente, suponha que as raízes de L formem um q-módulo. O Lema 2.4 mostra que L é um q-polinômio sobre alguma extensão de $\mathbb{F}_q$. Nosso objetivo agora é provar que essa

extensão é o próprio corpo $\mathbb{F}_q$. Para isso, seja M o q-módulo formado pelas raízes de L. Então, para algum inteiro não negativo k, podemos escrever

$$L(X) = \prod_{\beta \in M} (X - \beta)^{q^k}.$$

Mas, como a q-ésima potência de um elemento de M ainda pertence a M, vale

$$L(X)^q = \prod_{\beta \in M} (X^q - \beta^q)^{q^k} = \prod_{\beta \in M} (X^q - \beta)^{q^k} = L(X^q).$$

Agora, denotando $L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i}$, temos

$$\sum_{i=0}^{n} \alpha_i^q X^{q^{i+1}} = L(X)^q = L(X^q) = \sum_{i=0}^{n} \alpha_i X^{q^{i+1}}.$$

Comparando coeficientes, concluímos que $\alpha_i^q = \alpha_i$, para todo $i = 0, ..., n$, isto é, $L(X)$ é um q-polinômio sobre $\mathbb{F}_q$. ■

Observemos que o produto de dois q-polinômios pode não ser um q-polinômio. Por exemplo, se tivermos $L_1(X) = X^4 + X^2 + X, L_2(X) = X^2 + X$ dois 2-polinômios sobre $\mathbb{F}_2[X]$, teremos

$$L_1(X)L_2(X) = X^6 + X^5 + X^4 + X^2,$$

que não é um 2-polinômio. Entretanto, uma vez que o expoente da variável X é sempre uma potência da característica, a composição de dois q-polinômios ainda é um q-polinômio. No nosso exemplo, temos

$$L_1(L_2(X)) = L_2(L_1(X)) = X^8 + X.$$

Por esse motivo, sobre o conjunto dos q-polinômios vamos introduzir a operação de **multiplicação simbólica** dada pela composição, isto é, $(L_1 \circ L_2)(X) = L_1(L_2(X))$.

É possível mostrar que o conjunto das classes de restos dos q-polinômios sobre $\mathbb{F}_{q^n}$ módulo $X^{q^n} - X$ munidos da multiplicação simbólica, da adição usual e da multiplicação por escalares em $\mathbb{F}_q$ é uma álgebra (um espaço vetorial munido de três operações: adição e multiplicação de vetores e uma multiplicação por um escalar), que será denotada por $\mathcal{L}_n(\mathbb{F}_{q^n})$.

2.2 Caracterizações de $\mathcal{L}_n(\mathbb{F}_{q^n})$

Nessa seção, destacamos o trabalho de Wu e Liu ([20]). Nesse artigo, os autores estabeleceram dois isomorfismos envolvendo $\mathcal{L}_n(\mathbb{F}_{q^n})$: um usando produto tensorial ([20, Teorema 3.1]), que não será abordado, e outro usando matrizes de Dickson, possibilitando assim representações alternativas para q-polinômios. Em particular, esses isomorfismos permitiram aos autores demonstrar uma representação para um q-polinômio a partir da função traço.

Antes de entrar no estudo desse trabalho, vamos fixar algumas notações. Nesta seção, frequentemente vamos denotar uma matriz

$$\begin{pmatrix} a_{0,0} & \cdots & a_{0,n-1} \\ \vdots & \ddots & \vdots \\ a_{n-1,0} & \cdots & a_{n-1,n-1} \end{pmatrix}$$

simplesmente por (a_{ij}). Além disso, dada uma base $\{\beta_0, ..., \beta_{n-1}\}$ para $\mathbb{F}_{q^n}$, o conjunto $\{\beta_0^*, ..., \beta_{n-1}^*\} \subseteq \mathbb{F}_{q^n}$ denotará sua base dual, isto é, $\{\beta_0^*, ..., \beta_{n-1}^*\}$ é também uma base para $\mathbb{F}_{q^n}$ e vale

$$\mathrm{Tr}(\beta_i \beta_j^*) = \begin{cases} 0, & \text{se } i \neq j \\ 1, & \text{se } i = j \end{cases}.$$

Definição 2.8. Uma **matriz de Dickson sobre** $\mathbb{F}_{q^n}$ é uma matriz D da forma

$$D = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}.$$

Se $L = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathcal{L}_n(\mathbb{F}_{q^n})$ for um q-polinômio, a matriz de Dickson D_L de L será aquela que tem em sua primeira linha os coeficientes de L dispostos de forma ordenada.

A matriz de Dickson de um q-polinômio L pode ser usada para se obter a matriz da transformação linear induzida por L do seguinte modo.

Lema 2.9. *Sejam $L = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathcal{L}_n(\mathbb{F}_{q^n})$ e M_L a matriz da transformação linear induzida por L com respeito a uma base genérica $\{\beta_0, ..., \beta_{n-1}\}$. Então,*

$$M_L = (\beta_j^{q^i})^{-1} D_L(\beta_j^{q^i}). \tag{2.1}$$

Demonstração. Por definição de M_L, temos $(L(\beta_0), ..., L(\beta_{n-1})) = (\beta_0, ..., \beta_{n-1})M_L$. Escrevendo $M_L = (m_{ij})$, segue que

$$L(\beta_j) = \sum_{k=0}^{n-1} m_{kj}\beta_k.$$

Da linearidade da função traço, temos

$$\mathrm{Tr}(\beta_i^* L(\beta_j)) = \mathrm{Tr}\left(\beta_i^* \left(\sum_{k=0}^{n-1} m_{kj}\beta_k\right)\right) = \sum_{k=0}^{n-1} m_{kj}\mathrm{Tr}(\beta_i^*\beta_k) = m_{ij}. \tag{2.2}$$

Dessa forma,

$$M_L = (\mathrm{Tr}(\beta_i^* L(\beta_j)) = (\beta_i^{*q^j})(L(\beta_j)^{q^i}). \tag{2.3}$$

Notemos que

$$L(X)^{q^i} = \left(\sum_{j=0}^{n-1} a_j X^{q^j}\right)^{q^i} = \sum_{j=n-i}^{n-1} a_j^{q^i} X^{q^{j+i-n}} + \sum_{j=0}^{n-1-i} a_j^{q^i} X^{q^{j+i}},$$

então, para todo $x \in \mathbb{F}_{q^n}$,

$$\begin{pmatrix} L(x) \\ L(x)^q \\ \vdots \\ L(x)^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix} \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} = D_L \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix}.$$

Portanto, $(L(\beta_j)^{q^i}) = D_L(\beta_j^{q^i})$. Um simples cálculo nos mostra que $(\beta_i^{*q^j})(\beta_j^{q^i}) = (\mathrm{Tr}(\beta_i^*\beta_j))$ $= I_n$, então temos $(\beta_i^{*q^j}) = (\beta_j^{q^i})^{-1}$. Substituindo em (2.3), obtemos

$$M_L = (\beta_j^{q^i})^{-1} D_L(\beta_j^{q^i}).$$

■

Pode-se mostrar que $\mathcal{D}_n(\mathbb{F}_{q^n})$, o conjunto de todas as matrizes de Dickson de ordem n com coeficientes em $\mathbb{F}_{q^n}$, é uma álgebra com as operações usuais de matrizes e enfim podemos provar o isomorfismo entre essa álgebra e $\mathcal{L}_n(\mathbb{F}_{q^n})$.

Teorema 2.10. $\mathcal{L}_n(\mathbb{F}_{q^n}) \cong \mathcal{D}_n(\mathbb{F}_{q^n})$.

Demonstração. Considere a aplicação

$$\begin{array}{rccc} \phi: & \mathcal{L}_n(\mathbb{F}_{q^n}) & \to & \mathcal{D}_n(\mathbb{F}_{q^n}) \\ & L & \mapsto & D_L \end{array}.$$

Primeiro precisamos mostrar que ϕ é de fato um homomorfismo entre álgebras, isto é, $\phi(L_1 + L_2) = \phi(L_1) + \phi(L_2)$, $\phi(L_1 \circ L_2) = \phi(L_1)\phi(L_2)$ e $\phi(\lambda L) = \lambda\phi(L)$, para todos $L_1, L_2 \in \mathcal{L}_n(\mathbb{F}_{q^n})$ e $\lambda \in \mathbb{F}_q$. Para isso, basta usar o fato que $M_{L_1+L_2} = M_{L_1} + M_{L_2}$, $M_{L_1 \circ L_2} = M_{L_1} M_{L_2}$, $M_{\lambda L} = \lambda M_L$ e a caracterização dada em (2.1).

A bijetividade de ϕ segue da definição de D_L. Dada uma matriz $D \in \mathcal{D}_n(\mathbb{F}_{q^n})$, basta tomarmos um q-polinômio L tal que seus coeficientes coincidam com a primeira linha de D e teremos $D = \phi(L)$. Além disso, se L for tal que $0 = \phi(L) = D_L$, devemos ter todos os coeficientes de L nulos, isto é, $L = 0$. ■

Esse isomorfismo nos permite obter informações de L a partir de sua matriz de Dickson D_L.

Teorema 2.11. *Seja $L \in \mathcal{L}_n(\mathbb{F}_{q^n})$. Então, o posto de L (a dimensão do espaço imagem de sua transformação linear induzida) coincide com o posto de D_L e o determinante de L (o determinante da matriz associada à transformação linear com respeito a qualquer base) coincide com o determinante de D_L.*

Demonstração. Do Lema 2.9, obtemos

$$\det(L) := \det(M_L) = \det(D_L),$$

uma vez que o determinante do produto de matrizes é o produto de seus determinantes e $\det(\beta_j^{q^i}) \det(\beta_j^{q^i})^{-1} = 1$. Além disso, devemos ter os postos de D_L e de M_L iguais, afinal, é possível encontrar matrizes invertíveis P, Q tais que

$$M_L = PEQ, \text{ com } E = \begin{pmatrix} 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{2.4}$$

e o número de colunas não nulas de E coincida com posto de M_L ([16, p.137]). Nesse caso,

$$D_L = (\beta_j^{q^i}) PEQ (\beta_j^{q^i})^{-1} = RES,$$

com R, S invertíveis e teremos

$$\text{posto}(D_L) = \text{posto}(E) = \text{posto}(M_L).$$

■

É claro que também podemos obter informações de D_L a partir de L. O próximo teorema é um exemplo disso. Ele não será usado posteriormente, mas merece ser destacado.

Teorema 2.12. *[20, Proposição 4.6] Seja $L \in \mathcal{L}_n(\mathbb{F}_{q^n})$ com posto $0 \leq k \leq n$. Sejam $\{u_0, ..., u_{k-1}\}$ e $\{v_0, ..., v_{n-k-1}\}$ bases da imagem e do núcleo de L respectivamente. Então, $\{\tau(u_0), ..., \tau(u_{k-1})\}$ e $\{\tau(v_0), ..., \tau(v_{n-k-1})\}$ são bases da imagem e do núcleo de D_L respectivamente, em que $\tau(x) = (x, x^q, ..., x^{q^{n-1}})$.*

Pode-se verificar que o posto de $\{a_0, ..., a_{n-1}\}$ e $\{\tau(a_0), ..., \tau(a_{n-1})\}$ coincidem (aqui, o posto de um conjunto denota a maior cardinalidade de subconjuntos formados por elementos linearmente independentes). Então, podemos obter o seguinte corolário, que será usado na demonstração do Teorema 2.16.

Corolário 2.13. *Seja* $\{a_0, ..., a_{n-1}\} \subseteq \mathbb{F}_{q^n}$. *Então,*

$$posto(\{a_0, ..., a_{n-1}\}) = posto(a_j^{q^i}).$$

No caso particular em que trabalharmos com um q-polinômio bijetor, podemos buscar seu inverso com respeito à operação de composição. Uma vez que temos o isomorfismo entre $\mathcal{L}_n(\mathbb{F}_{q^n})$ e $\mathcal{D}_n(\mathbb{F}_{q^n})$ e os postos de um polinômio L e sua matriz associada D_L coincidem, temos L bijetor se, e somente se, D_L for invertível. Uma vez que a composição de dois operadores lineares é dada pelo produto de suas matrizes, temos L^{-1} o q-polinômio associado à matriz D_L^{-1}. Usando um resultado conhecido de álgebra para calcular a inversa de uma matriz ([6, p.212]), temos o seguinte teorema.

Teorema 2.14. *Sejam* $L = \sum_{i=0}^{n-1} a_i X^{q^i}$ *um* q*-polinômio bijetor e* D_L *sua matriz de Dickson associada. Denotando o* $(i, 0)$*-ésimo cofator de* D_L *por* $\overline{a}_i$*, temos*

$$L^{-1}(X) = \frac{1}{\det L} \sum_{i=0}^{n-1} \overline{a}_i X^{q^i}.$$

Observação 2.15. Fixada uma base $\{\beta_0, ..., \beta_{n-1}\}$ para $\mathbb{F}_{q^n}$, toda matriz de Dickson D pode ser escrita sob as formas

$$D = (\beta_j^{q^i})(\alpha_i'^{q^j}) = (\alpha_j^{q^i})(\beta_i^{q^j}), \tag{2.5}$$

com conjuntos $\{\alpha_0', ..., \alpha_{n-1}'\}, \{\alpha_0, ..., \alpha_{n-1}\} \subseteq \mathbb{F}_{q^n}$ convenientes. De fato, tomando L o q-polinômio associado a D e denotando por M_L a matriz da transformação linear induzida por L com respeito à base $\{\beta_0, ..., \beta_{n-1}\}$, o Lema 2.9 nos diz que

$$M_L = (\beta_j^{q^i})^{-1} D (\beta_j^{q^i}).$$

Agora, multiplicando por $(\beta_j^{q^i})$ à esquerda e por $(\beta_j^{q^i})^{-1} = (\beta_i^{*q^j})$ à direita, temos

$$D = (\beta_j^{q^i}) M_L (\beta_i^{*q^j}).$$

Usando $m_{ij} = \mathrm{Tr}(\beta_i^* L(\beta_j))$ (equação (2.2)), pode-se ver que, tomando-se $\alpha_i' = \sum_{k=0}^{n-1} \beta_k^* \mathrm{Tr}(\beta_i^* L(\beta_k))$, a primeira igualdade de (2.5) é obtida. Agora, se repetirmos a demonstração do Lema 2.9 com $\{\beta_0^*, ..., \beta_{n-1}^*\}$ no lugar de $\{\beta_0, ..., \beta_{n-1}\}$ e fizermos essa mesma manipulação, obteremos o conjunto $\{\alpha_0, ..., \alpha_{n-1}\}$.

Saber "enxergar" q-polinômios como uma matriz de Dickson (e vice-versa) pode ser uma ferramenta muito útil, afinal resultados obtidos em um espaço podem ser automaticamente "traduzidos" para o outro, mas essa não é a única finalidade. Wu e Liu usaram os isomorfismos que construíram para demonstrar uma representação alternativa para q-polinômios, proposta por Zhou ([22]): todo q-polinômio pode ser representado a partir da função traço.

Teorema 2.16. *Sejam* $L = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathcal{L}_n(\mathbb{F}_{q^n})$ *um* q*-polinômio de posto* k *e* $\{\beta_0, ..., \beta_{n-1}\}$ *uma base de* $\mathbb{F}_{q^n}$. *Então,*

(i) Existe um único conjunto ordenado $\{\alpha_0', ..., \alpha_{n-1}'\} \subseteq \mathbb{F}_{q^n}$ *de posto* k *tal que* L *pode ser representado sob a forma*

$$L = \sum_{i=0}^{n-1} Tr(\alpha_i' X) \beta_i.$$

(ii) Existe um único conjunto ordenado $\{\alpha_0, ..., \alpha_{n-1}\} \subseteq \mathbb{F}_{q^n}$ *de posto* k *tal que* L *pode ser representado sob a forma*

$$L = \sum_{i=0}^{n-1} Tr(\beta_i X)\alpha_i.$$

(iii) Existem conjuntos ordenados $\{\omega_0, ..., \omega_{k-1}\}, \{\theta_0, ..., \theta_{k-1}\} \subseteq \mathbb{F}_{q^n}$*, ambos de posto* k*, tais que* L *pode ser representado sob a forma*

$$L = \sum_{i=0}^{k-1} Tr(\omega_i X)\theta_i.$$

Demonstração. De acordo com a Observação 2.15, podemos escrever $D_L = (\beta_j^{q^i})(\alpha_i'^{q^j}) = (\alpha_j^{q^i})(\beta_i^{q^j})$ com conjuntos $\{\alpha_0', ..., \alpha_{n-1}'\}, \{\alpha_0, ..., \alpha_{n-1}\} \subseteq \mathbb{F}_{q^n}$ convenientes (e obtidos de forma única). Uma vez que a primeira linha de D_L consiste dos coeficientes de L, temos

$$\begin{aligned} L &= (a_0, ..., a_{n-1}) \begin{pmatrix} X \\ X^q \\ \vdots \\ X^{q^{n-1}} \end{pmatrix} = (\beta_0, \beta_1, ..., \beta_{n-1}) \begin{pmatrix} \alpha_0' & \alpha_0'^q & \cdots & \alpha_0'^{q^{n-1}} \\ \alpha_1' & \alpha_1'^q & \cdots & \alpha_1'^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1}' & \alpha_{n-1}'^q & \cdots & \alpha_{n-1}'^{q^{n-1}} \end{pmatrix} \begin{pmatrix} X \\ X^q \\ \vdots \\ X^{q^{n-1}} \end{pmatrix} \\ &= (\beta_0, \beta_1, ..., \beta_{n-1}) \begin{pmatrix} \mathrm{Tr}(\alpha_0' X) \\ \mathrm{Tr}(\alpha_1' X) \\ \vdots \\ \mathrm{Tr}(\alpha_{n-1}' X) \end{pmatrix} = \textstyle\sum_{i=0}^{n-1} \mathrm{Tr}(\alpha_i' X)\beta_i. \end{aligned}$$

O caso $D_L = (\alpha_j^{q^i})(\beta_i^{q^j})$ é tratado analogamente. Como $\mathrm{posto}(\alpha_j'^{q^i}) = \mathrm{posto}(\alpha_j^{q^i}) = \mathrm{posto}(D_L) = k$, o Corolário 2.13 nos diz que $\mathrm{posto}(\{\alpha_0', ..., \alpha_{n-1}'\}) = \mathrm{posto}(\{\alpha_0, ..., \alpha_{n-1}\}) = k$ e com isso provamos (i) e (ii).

Provaremos (iii) por indução. Se tivermos $k = 1$, existem $c_0, ..., c_{n-1} \in \mathbb{F}_q$ não todos nulos tais que $\{\alpha_0, ..., \alpha_{n-1}\} = \{c_0\theta, ..., c_{n-1}\theta\}$, para algum $\theta \in \mathbb{F}_{q^n}^*$. Então,

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^q & \alpha_1^q & \cdots & \alpha_{n-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{n-1}} & \alpha_1^{q^{n-1}} & \cdots & \alpha_{n-1}^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} \theta \\ \theta^q \\ \vdots \\ \theta^{q^{n-1}} \end{pmatrix} (c_0, c_1, ..., c_{n-1}),$$

donde

$$D_L = \begin{pmatrix} \theta \\ \theta^q \\ \vdots \\ \theta^{q^{n-1}} \end{pmatrix} (c_0, c_1, ..., c_{n-1}) \begin{pmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \cdots & \beta_{n-1}^{q^{n-1}} \end{pmatrix} := \begin{pmatrix} \theta \\ \theta^q \\ \vdots \\ \theta^{q^{n-1}} \end{pmatrix} (\omega, \omega^q, ..., \omega^{q^{n-1}}).$$

Isso implica que $L = \theta\mathrm{Tr}(\omega X)$.

No caso geral, uma matriz de posto k pode ser decomposta como a soma de k matrizes de posto 1 (basta usar a caracterização dada em (2.4) e escrever E como a soma de k matrizes com apenas uma coluna não nula). Aplicando o que acabamos de mostrar, podemos encontrar dois conjuntos $\{\omega_0, ..., \omega_{k-1}\}, \{\theta_0, ..., \theta_{k-1}\} \subseteq \mathbb{F}_{q^n}$ tais que

$$D_L = \sum_{i=0}^{k-1} \begin{pmatrix} \theta_i \\ \theta_i^q \\ \vdots \\ \theta_i^{q^{n-1}} \end{pmatrix} (\omega_i, \omega_i^q, ..., \omega_i^{q^{n-1}}),$$

e concluímos que $L = \sum_{i=0}^{k-1} \mathrm{Tr}(\omega_i X)\theta_i$. Devemos ter $\mathrm{posto}(\{\omega_0, ..., \omega_{k-1}\}) = \mathrm{posto}(\{\theta_0, ..., \theta_{k-1}\}) = k$, pois, caso contrário, D_L poderia ser escrita como a soma de $l < k$ matrizes de posto 1, o que contradiz o fato de D_L ter posto k e o posto da soma de matrizes não exceder a soma dos postos (basta lembrar que o posto é a dimensão do espaço imagem e que a dimensão da soma de espaços vetoriais nunca excede a soma das dimensões). ■

2.3 Teorema da Base Normal

Nessa última seção desse capítulo, traremos uma demonstração alternativa para o Teorema da Base Normal usando apenas os q-polinômios.

Definição 2.17. Os polinômios $l(X) = \sum_{i=0}^{n} \alpha_i X^i$ e $L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i}$ são chamados **q-associados**. De modo mais específico, $l(X)$ é o **q-associado convencional** de $L(X)$ e $L(X)$ é o **q-associado linearizado** de $l(X)$.

Lema 2.18. *Sejam $L_1(X)$ e $L_2(X)$ q-polinômios sobre $\mathbb{F}_q$ com q-associados convencionais $l_1(X)$ e $l_2(X)$ respectivamente. Então, $l(X) = l_1(X)l_2(X)$ e $L(X) = (L_1 \circ L_2)(X)$ são q-associados, e o mesmo ocorre com $s(X) = l_1(X) + l_2(X)$ e $S(X) = L_1(X) + L_2(X)$.*

Demonstração. Sejam $l_1(X) = \sum_i a_i X^i$ e $l_2(X) = \sum_j b_j X^j$. Desse modo, temos $l(X) = \sum_k c_k X^k$, em que $c_k = \sum_{i+j=k} a_i b_j$, e $s(X) = \sum_k (a_k + b_k) X^k$ (se necessário, "completamos"o polinômio l_1 ou l_2 com coeficientes nulos). Além disso, $L_1(X) = \sum_i a_i X^{q^i}$ e $L_2(X) = \sum_j b_j X^{q^j}$. Então,

$$L(X) = (L_1 \circ L_2)(X) = \sum_i a_i \left(\sum_j b_j X^{q^j}\right)^{q^i} = \sum_i a_i \sum_j b_j X^{q^{i+j}} = \sum_k \left(\sum_{i+j=k} a_i b_j\right) X^{q^k} = \sum_k c_k X^{q^k}$$

é o q-associado linearizado de $l(X)$, enquanto que

$$S(X) = L_1(X) + L_2(X) = \sum_k (a_k + b_k) X^{q^k}$$

é o q-associado linearizado de $s(X)$. ■

Podemos "traduzir"alguns conceitos da multiplicação usual para a multiplicação simbólica.

Definição 2.19. (*i*) Sejam $L(X)$ e $L_1(X)$ q-polinômios sobre $\mathbb{F}_q$. Dizemos que L é **simbolicamente divisível** por L_1 ou que L_1 **divide simbolicamente** L se existir um q-polinômio $L_2(X)$ sobre $\mathbb{F}_q$ tal que $L(X) = (L_1 \circ L_2)(X)$.

(*ii*) Dizemos que um q-polinômio $L(X)$ é **simbolicamente irredutível** sobre $\mathbb{F}_q$ se toda vez que pudermos escrever $L(X) = (L_1 \circ L_2)(X)$ tivermos que o grau de um desses fatores é 1.

(*iii*) Todo q-polinômio sobre $\mathbb{F}_q$ admite uma única (a menos de reordenação de fatores) **fatoração simbólica** dada pelo produto simbólico de q-polinômios simbolicamente irredutíveis. Usando o lema anterior, é possível mostrar que a fatoração simbólica de um q-polinômio sobre $\mathbb{F}_q$ é composta pelos q-associados linearizados dos fatores irredutíveis de seu q-associado convencional.

(*iv*) O **máximo divisor comum simbólico** dos q-polinômios $L_1(X), ..., L_n(X)$ sobre $\mathbb{F}_q$ é um q-polinômio $D(X)$ tal que D divide simbolicamente cada $L_i(X), i = 1, ..., n$ e, se D_1 for um q-polinômio que divide simbolicamente cada $L_i(X), i = 1, ..., n$, então D_1 dividirá simbolicamente D. Pode-se mostrar que o máximo divisor comum simbólico e o máximo divisor comum usual são iguais ([15, Teorema 3.62]).

Definição 2.20. Seja $L(X)$ um q-polinômio sobre $\mathbb{F}_{q^n}$. Uma raiz ξ de $L(X)$ será chamada uma **q-raiz primitiva** de $L(X)$ sobre $\mathbb{F}_{q^n}$ se ξ não for raiz de nenhum q-polinômio sobre $\mathbb{F}_{q^n}$ de grau menor que o de L.

Dado um elemento ξ em alguma extensão de $\mathbb{F}_{q^n}$, é possível encontrar um q-polinômio sobre $\mathbb{F}_{q^n}$ que tenha ξ como raiz q-primitiva sobre $\mathbb{F}_{q^n}$. Inicialmente, tomamos $m(X)$ o polinômio minimal de ξ sobre $\mathbb{F}_{q^n}$ e vamos denotar por s seu grau. Para cada $i = 0, ..., s$, encontramos o resíduo $r_i(X)$ de X^{q^i} módulo $m(X)$. Como o grau de cada r_i é, no máximo, $s-1$, podemos encontrar elementos $\alpha_0, ..., \alpha_s \in \mathbb{F}_{q^n}$ não todos nulos tais que $\sum_{i=0}^{s} \alpha_i r_i(X) = 0$, já que isso é equivalente a resolver um sistema linear homogêneo de $s+1$ variáveis (os elementos $\alpha_0, ..., \alpha_s$) com s linhas (os coeficientes de X^j para $j = 0, ..., s-1$).

Desse modo, teremos

$$L(X) := \sum_{i=0}^{s} \alpha_i X^{q^i} \equiv \sum_{i=0}^{s} \alpha_i r_i(X) \equiv 0 (\text{mod } m(X)),$$

isto é, L é um q-polinômio não nulo sobre $\mathbb{F}_{q^n}$ divisível por m, em particular, ξ é uma raiz de L. Escolhendo os elementos α_i de forma conveniente, podemos encontrar L mônico e de grau mínimo, e teremos ξ uma raiz q-primitiva sobre $\mathbb{F}_{q^n}$. Toda essa construção nos mostra que o q-polinômio sobre $\mathbb{F}_{q^n}$ mônico, de menor grau e divisível por m é unicamente obtido, e por isso será chamado o **q-polinômio minimal** de ξ sobre $\mathbb{F}_{q^n}$.

Exemplo 2.21. Em geral, o q-polinômio minimal de ξ sobre $\mathbb{F}_{q^n}$ não é o q-associado linearizado de seu polinômio minimal sobre $\mathbb{F}_{q^n}$. Seja $\beta \in \mathbb{F}_{16}$ uma raiz de $X^4 + X + 1$. O q-associado linearizado de seu polinômio minimal é $X^{16} + X^2 + X$. Porém, uma vez que $\beta \in \mathbb{F}_{16}$, temos $\beta^{16} = \beta$, e vemos que β não é uma raiz de $X^{16} + X^2 + X$. Seu q-polinômio minimal sobre $\mathbb{F}_2$ é, na verdade, $M(X) = X^8 + X^4 + X^2 + X$. De fato, nas notações acima, temos

$$r_0(X) = X, r_1(X) = X^2, r_2(X) = X + 1, r_3(X) = X^2 + 1, r_4(X) = X.$$

Queremos $\sum_{i=0}^{4} \alpha_i r_i(X) = 0$, então

$$\alpha_2 + \alpha_3 = 0, \alpha_0 + \alpha_2 + \alpha_4 = 0, \alpha_1 + \alpha_3 = 0.$$

Para que $M(X) = \sum_{i=0}^{4} \alpha_i X^{q^i}$ seja mônico e de menor grau, devemos tomar $\alpha_4 = 0$ e $\alpha_3 = 1$. E isso implica $\alpha_0 = \alpha_1 = \alpha_2 = 1$.

Usando a multiplicação usual, sabemos que um polinômio f admite α como raiz se, e somente se, seu polinômio minimal dividir f. Com a multiplicação simbólica, esse resultado possui uma forma equivalente.

Teorema 2.22. *Sejam ξ um elemento de uma extensão de $\mathbb{F}_{q^n}$ e $M(X)$ seu q-polinômio minimal sobre $\mathbb{F}_{q^n}$. Então, um q-polinômio $K(X)$ sobre $\mathbb{F}_{q^n}$ admite ξ como raiz se, e somente se, existir um q-polinômio $L(X)$ sobre $\mathbb{F}_{q^n}$ tal que $K(X) = (L \circ M)(X)$. Em particular, se tivermos $n = 1$, K admite ξ como raiz se, e somente se, M dividir simbolicamente K.*

Demonstração. Usando o algoritmo da divisão em $\mathbb{F}_{q^n}[X]$ para $k(X)$ e $m(X)$ (os q-associados convencionais de $K(X)$ e $M(X)$), encontraremos $l(X)$ e $r(X)$ tais que

$$k(X) = l(X)m(X) + r(X).$$

Definindo $L(X)$ e $R(X)$ como os q-associados linearizados de l e r, respectivamente, o Lema 2.18 nos garante que

$$K(X) = (L \circ M)(X) + R(X).$$

O teorema segue então dos fatos que $K(\xi) = R(\xi)$ e que o grau de R é menor que o grau de M, logo $R(\xi) = 0$ se, e somente se, R for o polinômio nulo. ∎

Na demonstração do Teorema da Base Normal, precisaremos garantir que um certo q-polinômio tenha uma raiz q-primitiva sobre $\mathbb{F}_q$. Para isso, vamos definir uma função análoga à função φ de Euler. Dado um polinômio $f \in \mathbb{F}_q[X]$ não nulo, $\Phi_q(f)$ denota o número de polinômios em $\mathbb{F}_q[X]$ de grau menor que o grau de f e coprimos com f. Para um polinômio constante e não nulo f, definimos $\Phi_q(f) = 1$.

Lema 2.23. *A função Φ_q possui as seguintes propriedades:*

(i) $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$ *se f e g forem coprimos.*

(ii) Se $gr(f) = n \geq 1$, então

$$\Phi_q(f) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r}),$$

em que os n_i são o grau dos fatores mônicos irredutíveis que aparecem na decomposição de f em $\mathbb{F}_q[X]$.

Demonstração. (i) Sejam $s = \Phi_q(f)$ e $t = \Phi_q(g)$ e $\{f_1, ..., f_s\}$ e $\{g_1, ..., g_t\}$ os polinômios "contados" por $\Phi_q(f)$ e $\Phi_q(g)$. Agora, seja $h \in \mathbb{F}_q[X]$ tal que $\text{gr}(h) < \text{gr}(fg)$ e $\text{mdc}(h, fg) = 1$. Temos $\text{mdc}(h, f) = 1$ e $\text{mdc}(h, g) = 1$, então existe um único par (i, j), com $1 \leq i \leq s, 1 \leq j \leq t$ tal que $h \equiv f_i \pmod f$ e $h \equiv g_j \pmod g$. Por outro lado, dado um par ordenado (i, j), o Teorema Chinês dos Restos ([15, Exercício 1.37]) afirma que existe um único polinômio $h \in \mathbb{F}_q[X]$ tal que $h \equiv f_i \pmod f$, $h \equiv g_j \pmod g$ e $\text{gr}(h) < \text{gr}(fg)$. Tal polinômio h satisfaz $\text{mdc}(h, f) = \text{mdc}(h, g) = 1$, logo $\text{mdc}(h, fg) = 1$. Portanto, existe uma correspondência biunívoca entre os st pares $(i, j), 1 \leq i \leq s, 1 \leq j \leq t$ e polinômios h de grau menor que o grau de fg e $\text{mdc}(h, fg) = 1$. Logo, $\Phi_q(fg) = st = \Phi_q(f)\Phi_q(g)$.

(ii) Falta apenas encontrar o valor de $\Phi_q(f^e)$, em que f é um polinômio irredutível em $\mathbb{F}_q[X]$ e e é um natural positivo. Sejam m o grau de f e h um polinômio de grau menor que o de f^e, isto é, de grau menor que em, e que não seja coprimo com f^e. Então, como f é irredutível, devemos ter $h = fg$ para algum $g \in \mathbb{F}_q[X]$ de grau $\text{gr}(g) < em - m$. Uma vez que temos q^{em-m} opções para o polinômio g, temos $\Phi_q(f^e) = q^{em} - q^{em-m} = q^{em}(1 - q^{-m})$. ■

Agora, vamos encontrar o número N_L de raízes q-primitivas de $L(X)$ sobre $\mathbb{F}_q$. Primeiramente, se $L(X)$ tiver uma (e, portanto, todas) raiz múltipla, podemos escrever $L(X) = L_1(X)^q$, em que $L_1(X)$ é também um q-polinômio sobre $\mathbb{F}_q$ (Teorema 2.3). Como toda raiz de L é também raiz de L_1, temos $N_L = 0$. Então, podemos assumir que $L(X)$ tenha apenas raízes simples. Se L tiver grau 1, claramente $N_L = 1$.

Suponhamos, sem perda de generalidade, que L seja mônico e tenha grau $q^n > 1$. Considere sua fatoração simbólica

$$L(X) = \underbrace{L_1(X) \circ \cdots \circ L_1(X)}_{e_1} \circ \cdots \circ \underbrace{L_r(X) \circ \cdots \circ L_r(X)}_{e_r}.$$

Vamos denotar por $K_i(X), i = 1, ..., r$, o q-polinômio obtido a partir da fatoração simbólica de L, mas omitindo-se um fator $L_i(X)$.

Podemos obter N_L subtraindo de q^n (o número de raízes de L em alguma extensão de $\mathbb{F}_q$) a quantidade de raízes que anulam algum q-polinômio de grau menor que q^n. Se ξ for uma tal raiz, seu q-polinômio minimal M dividirá simbolicamente L pelo Teorema 2.22. Uma vez que o grau de M é menor que q^n, podemos afirmar que M divide simbolicamente algum $K_i(X)$, e novamente o Teorema 2.22 nos garante que $K_i(\xi) = 0$, isto é, se ξ não for uma q-raiz primitiva de L, ξ será uma raiz de algum $K_i(X)$ para $i \in \{1, ..., r\}$.

Se o grau de $L_i(X)$ for q^{n_i}, então o grau de K_i (e, consequentemente, seu número de raízes) será q^{n-n_i}. Agora, o número de raízes comuns a $K_{i_1}, ..., K_{i_s}$ para índices $i_1, ..., i_s$ distintos é igual ao grau do seu máximo divisor comum (que é igual ao máximo divisor simbólico). Da definição de K_i, vemos que esse grau é $q^{n-n_{i_1}-\cdots-n_{i_s}}$. Por fim, usando o princípio da inclusão-exclusão ([17, p.61]), concluímos que

$$N_L = q^n - \sum_{i=1}^{r} q^{n-n_i} + \sum_{1\leq i<j\leq r} q^{n-n_i-n_j} + \cdots + (-1)^r q^{n-n_1-\cdots-n_r} = q^n(1-q^{-n_1})\cdots(1-q^{-n_r}).$$

Teorema 2.24. *Sejam $L(X)$ um q-polinômio não nulo sobre $\mathbb{F}_q$ e $l(X)$ seu q-associado. Então, o número N_L de raízes q-primitivas de L é 0 se L tiver raízes múltiplas ou $\Phi_q(l)$ se L tiver raízes simples.*

Demonstração. O caso em que L possui raízes múltiplas já foi tratado. Falta justificar apenas a segunda igualdade.

Se pudermos escrever $L(X) = L_1(X)^{e_1} \circ \cdots \circ L_r(X)^{e_r}$, teremos $N_L = q^n(1-q^{-n_1})\cdots(1-q^{-n_r})$, em que q^{n_i} é o grau de L_i. Por outro lado, vale $l(X) = l_1(X)^{e_1}\cdots l_r(X)^{e_r}$, em que l_i é o polinômio q-associado de L_i (Lema 2.18). Como o grau de L_i é q^{n_i}, o grau de l_i é n_i. O item (ii) do Lema 2.23 nos mostra que $N_L = \Phi_q(l)$. ■

Corolário 2.25. *Todo q-polinômio não nulo com raízes simples tem, pelo menos, uma raiz q-primitiva.*

Munidos dos resultados acima, podemos apresentar uma demonstração para o Teorema da Base Normal.

Teorema 2.26 (Teorema da Base Normal)**.** *Seja M um q-módulo de dimensão $n \geq 1$ sobre $\mathbb{F}_q$. Então existe um elemento $\xi \in M$ tal que $\{\xi, \xi^q, ..., \xi^{q^{n-1}}\}$ é uma base para M sobre $\mathbb{F}_q$.*

Demonstração. Pelo Teorema 2.7, sabemos que $L(X) = \prod_{\beta\in M}(X-\beta)$ é um q-polinômio sobre $\mathbb{F}_q$. Pelo Corolário 2.25, L admite uma raiz ξ q-primitiva sobre $\mathbb{F}_q$, donde $\xi, \xi^q, ..., \xi^{q^{n-1}}$ são todos elementos de M (afinal, M é um módulo). Se esses elementos fossem linearmente dependentes, existiriam elementos $\alpha_1, \alpha_q, ..., \alpha_{q^{n-1}} \in \mathbb{F}_q$ não todos nulos tais que $\alpha_1\xi + \alpha_q\xi^q + \cdots + \alpha_{q^{n-1}}\xi^{q^{n-1}} = 0$, isto é, ξ seria raiz do q-polinômio

$$L_1(X) = \sum_{i=0}^{n-1} \alpha_{q^i} X^{q^i},$$

que tem grau menor que o grau de L, o que contradiz a definição de raiz q-primitiva. Desse modo, $\{\xi, \xi^q, ..., \xi^{q^{n-1}}\}$ é uma base para M sobre $\mathbb{F}_q$. ■

O teorema acima nos garante que todo corpo finito $\mathbb{F}_{q^n}$ admite uma base normal sobre $\mathbb{F}_q$ (já que o corpo $\mathbb{F}_{q^n}$ é também um q-módulo sobre $\mathbb{F}_q$). Os próximos resultados nos dizem exatamente quantas tais bases existem.

Teorema 2.27. *$\mathbb{F}_{q^n}$ contém $\Phi_q(X^n-1)$ elementos ξ tais que $\{\xi, \xi^q, ..., \xi^{q^{n-1}}\}$ é uma base normal de $\mathbb{F}_{q^n}$.*

Demonstração. Considere

$$L(X) = \prod_{\beta\in\mathbb{F}_{q^n}} (X-\beta) = X^{q^n} - X.$$

Usando o mesmo argumento do teorema anterior, podemos concluir que toda raiz q-primitiva de L nos fornece uma base normal. Por outro lado, se $\xi \in \mathbb{F}_{q^n}$ não for q-primitiva, existirá um q-polinômio não nulo de grau menor que $q^n = \text{gr}(L)$ que admite ξ como raiz, ou seja, $\xi, \xi^q, ..., \xi^{q^{n-1}}$ são linearmente dependentes sobre $\mathbb{F}_q$, e não podem gerar uma base. Assim, concluímos que o número de elementos ξ tais que $\{\xi, \xi^q, ..., \xi^{q^{n-1}}\}$ é uma base normal de $\mathbb{F}_{q^n}$ é igual ao número de raízes q-primitivas de L, que é dado por $\Phi_q(X^n - 1)$ (Teorema 2.24). ■

Corolário 2.28. *$\mathbb{F}_{q^n}$ admite $\frac{\Phi_q(X^n-1)}{n}$ bases normais distintas.*

Demonstração. Esse resultado segue diretamente do teorema anterior observando que os elementos $\xi, \xi^q, ..., \xi^{q^{n-1}}$ geram a mesma base normal. ■

Capítulo 3

Polinômios de permutação

Toda função de $\mathbb{F}_q$ em $\mathbb{F}_q$ admite uma representação polinomial (Equação 3.1) e, no estudo de uma função, é natural nos questionarmos sobre sua bijetividade. Dessa forma, é natural nos interessarmos pelo estudo de polinômios que são também bijeções. Além disso, uma bijeção em um conjunto finito também pode ser interpretada como uma permutação, ou seja, podemos estudar polinômios bijetivos por meio dos grupos de permutação. A maior parte desse capítulo trata dessas duas questões. Começaremos apresentando definições e resultados básicos, e na primeira seção falaremos sobre o grupo dos polinômios de permutação. Na segunda seção, destacamos nossa generalização (Proposição 3.22) de um resultado apresentado em [21]. Através dela, apresentaremos novos exemplos de polinômios de permutação (Teorema 3.27).

Definição 3.1. Um polinômio $f \in \mathbb{F}_q[X]$ será chamado um **polinômio de permutação** se ele induzir uma permutação sobre $\mathbb{F}_q$ (com a associação $a \mapsto f(a)$), isto é, se a função polinomial associada a f for uma bijeção em $\mathbb{F}_q$.

Usando apenas a finitude de $\mathbb{F}_q$, temos ainda algumas definições equivalentes.

Teorema 3.2. *Um polinômio $f \in \mathbb{F}_q[X]$ é de permutação se, e somente se, alguma (e portanto todas) das seguintes condições for válida:*

(i) *A associação $a \mapsto f(a)$ é sobrejetora.*

(ii) *A associação $a \mapsto f(a)$ é injetora.*

(iii) *$f(X) = a$ tem pelo menos uma raiz para cada $a \in \mathbb{F}_q$.*

(iv) *$f(X) = a$ tem no máximo uma raiz para cada $a \in \mathbb{F}_q$.*

(v) *$f(X) = a$ tem exatamente uma raiz para cada $a \in \mathbb{F}_q$.*

Observe que as três últimas condições tratam do número de raízes do polinômio $f(X) - a$ para cada $a \in \mathbb{F}_q$. O seguinte lema é muito útil na determinação da quantidade de raízes de um polinômio em um dado corpo finito.

Lema 3.3. *Seja $f \in \mathbb{F}_q[X]$. As raízes de f em $\mathbb{F}_q$ são precisamente as raízes de $mdc(f, X^q - X)$. Além disso, o número de raízes distintas de f em $\mathbb{F}_q$ é igual ao grau de $mdc(f, X^q - X)$.*

Demonstração. Já sabemos que se as raízes de f forem $\alpha_1, ..., \alpha_s \in \mathbb{F}_q$, podemos escrever $f(X) = (X-\alpha_1)^{n_1} \cdots (X-\alpha_s)^{n_s} g(X)$ com n_i um inteiro positivo para $i = 1, ..., s$ e $g(X) \in \mathbb{F}_q[X]$ irredutível. Então, encontrar as raízes de f em $\mathbb{F}_q$ é equivalente a encontrar seus fatores lineares. Denotemos $d(X) = (X - \alpha_1) \cdots (X - \alpha_s)$. É claro que d divide f.

Dado que o polinômio $X^q - X$ pode ser decomposto em $\mathbb{F}_q[X]$ como $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$, então claramente $d(X)$ divide $X^q - X$. Agora, seja h um polinômio que divida f e $X^q - X$.

Como h divide $X^q - X$, cada fator irredutível de h divide $\prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ e, portanto, divide um dos fatores lineares de $X^q - X$. Dessa forma, cada fator irredutível de h é da forma $X - \alpha$ para algum $\alpha \in \mathbb{F}_q$, isto é, existe um subconjunto $S \subset \mathbb{F}_q$ tal que $h(X) = \prod_{\alpha \in S}(X - \alpha)$.

Agora, como h divide f, cada fator $(X-\alpha)$ de h divide f, donde concluímos que $\alpha = \alpha_i$ para algum $i \in \{1, ..., s\}$ e $|S| \leq s$. Logo, h divide d e, por definição de mdc, $d = \text{mdc}(f, X^q - X)$. ■

Em resumo, para encontrarmos as raízes de f em $\mathbb{F}_q$, podemos nos limitar a encontrar as raízes de $\text{mdc}(f, X^q - X)$. Mais ainda, o grau desse mdc é a quantidade de raízes distintas de f em $\mathbb{F}_q$.

O Teorema 3.2 já nos dá um bom ponto de partida se quisermos determinar se um dado polinômio é de permutação: para cada $a \in \mathbb{F}_q$, precisamos descobrir o número de raízes do polinômio $f(X) - a$ em $\mathbb{F}_q$ que, como visto no Lema 3.3, é igual ao grau do mdc entre f e $X^q - X$. Uma outra possível abordagem para esse problema é usar o Critério de Hermite, mas ainda precisamos de alguns resultados auxiliares para prová-lo.

Primeiramente, o Teorema da Interpolação de Lagrange nos diz que, dada uma função genérica $\Phi : \mathbb{F}_q \to \mathbb{F}_q$, existe um único polinômio $g \in \mathbb{F}_q[X]$ de grau menor que q tal que $\Phi(a) = g(a)$ para todo elemento $a \in \mathbb{F}_q$. Usando o fato que $\alpha^{q-1} = 1$ para todo $\alpha \in \mathbb{F}_q^*$, vemos que

$$g(X) = \sum_{a \in \mathbb{F}_q} \Phi(a)(1 - (X - a)^{q-1}). \tag{3.1}$$

No entanto, se Φ já for um polinômio, o lema a seguir nos diz que basta tomarmos sua redução módulo $X^q - X$.

Lema 3.4. *Sejam $f, g \in \mathbb{F}_q[X]$. Temos $f(a) = g(a)$ para todo $a \in \mathbb{F}_q$ se, e somente se, $f(X) \equiv g(X)$ (mod $X^q - X$).*

Demonstração. Aplicando o algoritmo da divisão para $f - g$, podemos escrever

$$f(X) - g(X) = h(X)(X^q - X) + r(X).$$

Então, temos $f(a) = g(a)$ se, e somente se, $r(a) = 0$, isto é, f e g coincidem em todos os elementos de $\mathbb{F}_q$ se, e somente se, r for o polinômio nulo. ■

Lema 3.5. *Sejam $a_0, ..., a_{q-1}$ elementos de $\mathbb{F}_q$. São equivalentes:*

(i) $a_0, ..., a_{q-1}$ *são distintos.*

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

Demonstração. Nessa demonstração, usaremos um certo abuso de notação: se tivermos $a_k = 0$ para algum k, vamos considerar $a_k^0 = 1$. Para cada $i \in \{0, ..., q-1\}$, considere o polinômio

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

Observe que, se tivermos $a_i = 0$ para algum i, então $g_i(X) = 1 - X^{q-1}$, donde $g_i(a_i) = g_i(0) = 1$. Agora, se $a_i \neq 0$,

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

Para todo $b \in \mathbb{F}_q$ com $b \neq a_i$, podemos escrever

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

Em resumo, para todo $i \in \{0, ..., q-1\}$, vale $g_i(a_i) = 1$ e $g_i(b) = 0$ para todo $b \neq a_i$. Dessa forma, consideremos o polinômio

$$g(X) = \sum_{i=0}^{q-1} g_i(X) = -\sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j} \right) X^j.$$

$((i) \Longrightarrow (ii))$: Se os elementos $a_0, ..., a_{q-1}$ forem dois a dois distintos, teremos $\{a_0, ..., a_{q-1}\} = \mathbb{F}_q$ e vale $g(x) = 1$, para todo $x \in \mathbb{F}_q$. Como o grau de g é menor que q, o Lema 3.4 nos mostra que g é o polinômio constante e igual a 1. Comparando coeficientes, vemos que isso é equivalente a (ii).

$((ii) \Longrightarrow (i))$: Nessa situação, vemos que g é o polinômio constante igual a 1. Então, para todo $j \in \{0, ..., q-1\}$, vale $\sum_{i=0}^{q-1} g_i(a_j) = 1$. Como $g_i(a_j) \in \{0, 1\}$ e $g_j(a_j) = 1$, devemos ter $g_i(a_j) = 0$, para todo $i \neq j$, isto é, devemos ter $a_j \neq a_i$, para todos $i, j \in \{0, ..., q-1\}$ com $i \neq j$. ■

Agora podemos apresentar o Critério de Hermite. Usando os itens (iii), (iv) e (v) do Teorema 3.2, precisaríamos calcular q mdc's. Com o critério de Hermite, podemos calcular um mdc e, no máximo, $q-2$ classes residuais.

Teorema 3.6 (Critério de Hermite)**.** *Seja $\mathbb{F}_q$ um corpo de característica p. Então, $f \in \mathbb{F}_q[X]$ é um polinômio de permutação sobre $\mathbb{F}_q$ se, e somente se, forem satisfeitas as duas condições:*

(i) f tiver exatamente uma raiz em $\mathbb{F}_q$.

(ii) para cada inteiro $t \in \{1, ..., q-2\}$ tal que $t \not\equiv 0 \pmod p$, a classe residual de $f(X)^t$ módulo $X^q - X$ tiver grau menor que $q-1$.

Demonstração. Se f for um polinômio de permutação, é claro que (i) é satisfeita. Agora, para cada inteiro $t \in \{1, ..., q-2\}$, a redução de $f(X)^t$ módulo $X^q - X$ é um polinômio da forma $g(X) = \sum_{j=0}^{q-1} b_j^{(t)} X^j$. Se usarmos a equação (3.1) para g, veremos que $b_{q-1}^{(t)} = -\sum_{a \in \mathbb{F}_q} f(a)^t$. Como f é de permutação, $\{f(a) : a \in \mathbb{F}_q\} = \mathbb{F}_q$ e o Lema 3.5 nos mostra que (ii) é satisfeita.

Inversamente, suponha que (i) e (ii) sejam satisfeitas. Como f tem exatamente uma raiz, $\sum_{a \in \mathbb{F}_q} f(a)^{q-1} = -1$ e, usando os mesmos cálculos que acabamos de fazer, (ii) nos mostra que $\sum_{a \in \mathbb{F}_q} f(a)^t = 0$ para todo $1 \leq t \leq q-2$ com $t \not\equiv 0 \pmod p$. Agora, se tivermos $t \equiv 0 \pmod p$, $t \neq 0$, podemos escrever $t = rp^j$, com $r \not\equiv 0 \pmod p$. Daí,

$$\sum_{a \in \mathbb{F}_q} f(a)^t = \sum_{a \in \mathbb{F}_q} f(a)^{rp^j} = \left(\sum_{a \in \mathbb{F}_q} f(a)^r \right)^{p^j} = 0.$$

Portanto, temos $\sum_{a \in \mathbb{F}_q} f(a)^t = 0$ para $1 \leq t \leq q-2$, e essa igualdade é trivial para $t = 0$ (usando novamente o abuso de notação $0^0 = 1$). Desse modo, temos f um polinômio de permutação pelo Lema 3.5. ■

Corolário 3.7. *Se $d > 1$ for um divisor de $q-1$, então não existe polinômio de permutação de grau d sobre $\mathbb{F}_q$.*

Demonstração. Se $f \in \mathbb{F}_q[X]$ for um polinômio de grau d, então o grau de $f^{(q-1)/d}$ é $q-1$. Como a característica p de $\mathbb{F}_q$ divide q, então $p \nmid q-1$ e, consequentemente, $\frac{q-1}{d} \not\equiv 0 \pmod p$. Assim, a condição (ii) do Critério de Hermite não é satisfeita para $t = \frac{q-1}{d}$. ■

3.1 Grupo dos polinômios de permutação

É um resultado conhecido que a composição de duas funções bijetoras é ainda uma função bijetora, e o mesmo ocorre com polinômios de permutação (Lema 3.8). Dessa forma, a composição é uma operação no conjunto dos polinômios de permutação. Se tomarmos a redução módulo $X^q - X$, veremos que esse conjunto forma um grupo munido com essa operação (Teorema 3.9). Essa seção é dedicada a provar esse resultado e apresentar algumas de suas consequências.

Primeiramente, precisamos provar que a composição é de fato uma operação no conjunto dos polinômios de permutação, isto é, que a composição de dois elementos desse conjunto também pertence ao conjunto. A demonstração desse fato é ainda mais fácil que quando trabalhamos com funções genéricas, mesmo assim será descrita abaixo.

Lema 3.8. *A composição de dois polinômios de permutação sobre $\mathbb{F}_q$ é ainda um polinômio de permutação sobre $\mathbb{F}_q$.*

Demonstração. Sejam $f, g \in \mathbb{F}_q[X]$ polinômios de permutação. Vamos provar que $f \circ g$ é também um polinômio de permutação. Para isso, sejam $\alpha, \beta \in \mathbb{F}_q$ com $\alpha \neq \beta$. Como g é de permutação, $g(\alpha) \neq g(\beta)$, e como f é de permutação, $f(g(\alpha)) \neq f(g(\beta))$. Com isso, temos provado que $f \circ g$ é injetor em $\mathbb{F}_q$. Pelo Teorema 3.2(ii), temos $f \circ g$ uma permutação. ■

Na introdução dessa seção, dissemos que precisamos tomar a redução módulo $X^q - X$. Isso é justificado pelo Lema 3.4: dois polinômios que, a princípio são diferentes, podem induzir a mesma bijeção em $\mathbb{F}_q$. Na prática, isso vai garantir a unicidade dos elementos identidade e inverso.

Teorema 3.9. *O conjunto dos polinômios de permutação sobre $\mathbb{F}_q$ de grau menor que q munido da operação de composição seguida da redução módulo $X^q - X$, isto é,*

$$f * g = f \circ g (mod\ X^q - X),$$

é um grupo, que denotaremos por P_q, que é isomorfo a S_q, o grupo de permutação de q elementos.

Demonstração. Para provarmos a associatividade dessa operação, isto é, para provarmos que $f * (g * h) = (f * g) * h$, basta usarmos a equação (3.1) e o fato que $f \circ (g \circ h) = (f \circ g) \circ h$. Temos:

$$f*(g*h)(X) = \sum_{a\in\mathbb{F}_q} (f\circ(g\circ h))(a)(1-(X-a)^{q-1}) = \sum_{a\in\mathbb{F}_q} ((f\circ g)\circ h)(a)(1-(X-a)^{q-1}) = (f*g)*h(X).$$

Provar a existência dos elementos neutro e inverso de um elemento é algo muito simples. O elemento neutro é claramente o polinômio identidade $f(X) = X$. Agora, dado um elemento f no conjunto, seu inverso é um polinômio g que induz a aplicação $f(a) \mapsto a$, para todo $a \in \mathbb{F}_q$. A equação (3.1) nos diz que

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

Tudo que resta provar é o isomorfismo desse conjunto com S_q. Primeiramente, tomando uma bijeção entre $\mathbb{F}_q$ e $\{1, 2, ..., q\}$ (que existe pois esses dois conjuntos têm a mesma quantidade de elementos), podemos pensar que S_q é um conjunto composto por permutações que agem sobre $\mathbb{F}_q$. A equação (3.1) nos dará o isomorfismo T entre S_q e P_q do seguinte modo:

$$\begin{array}{rccc} T: & S_q & \to & P_q \\ & \sigma & \mapsto & \sum_{a\in\mathbb{F}_q} \sigma(a)(1-(X-a)^{q-1}) \end{array}.$$

Em particular, $T(\sigma)(a) = \sigma(a)$, para todos $\sigma \in S_q$ e $a \in \mathbb{F}_q$. Vamos primeiro mostrar que T é um homomorfismo. Sejam $\sigma, \psi \in S_q$. $T(\sigma \circ \psi)$ é um polinômio de grau menor que q tal que

$$T(\sigma \circ \psi)(a) = (\sigma \circ \psi)(a), \forall a \in \mathbb{F}_q.$$

Por outro lado, $T(\sigma) * T(\psi)$ é também um polinômio de grau menor que q (pela definição da operação) e

$$(T(\sigma) * T(\psi))(a) = (T(\sigma) \circ T(\psi)(a) = T(\sigma)(\psi(a)) = \sigma(\psi(a)) = (\sigma \circ \psi)(a) = T(\sigma \circ \psi)(a).$$

O Lema 3.4 nos diz que $T(\sigma \circ \psi) \equiv T(\sigma) * T(\psi) \pmod{X^q - X}$. A igualdade dos dois (e por consequência o homomorfismo de T) segue do fato que seus graus são menores que q.

Uma vez que o polinômio identidade de P_q é obtido unicamente pela fórmula $\sum_{a \in \mathbb{F}_q} a(1 - (X-a)^{q-1})$, o núcleo desse homomorfismo é composto somente pela aplicação identidade, logo T é injetor. Para a sobrejetividade, basta notar que, por definição, um polinômio de permutação $f \in P_q$ induz uma permutação em $\mathbb{F}_q$ pela relação $a \mapsto f(a)$. Basta então tomar a permutação σ_f tal que $\sigma_f(a) = f(a)$. Como f e $T(\sigma_f)$ têm graus menores do que q e $f(a) = T(\sigma_f)(a)$ para todo $a \in \mathbb{F}_q$, temos $f = T(\sigma_f)$ (Lema 3.4), donde T é sobrejetor. ■

Tendo em vista o teorema anterior, podemos identificar P_q com S_q. Assim, todos os resultados válidos para S_q são "transferidos"para P_q. Vamos então citar algumas definições e resultados envolvendo S_q, que serão úteis nas demonstrações de propriedades de P_q.

Definição 3.10. Uma **transposição** $\sigma = (ab)$ é uma permutação tal que $\sigma(a) = b, \sigma(b) = a$ e $\sigma(c) = c$, para todo $c \notin \{a, b\}$, isto é, ela permuta os elementos a e b e mantém fixos os demais.

Definição 3.11. Um **ciclo de comprimento** n $\sigma = (a_1 a_2 \cdots a_n)$ é uma permutação tal que $\sigma(a_i) = a_{i+1}, i = 1, ..., n-1$, $\sigma(a_n) = a_1$ e $\sigma(b) = b$ para todo $b \notin \{a_1, ..., a_n\}$.

Lema 3.12. *Toda permutação pode ser escrita como produto (composição) de transposições. Em particular, um ciclo de comprimento n pode ser escrito como o produto de $n-1$ transposições.*

Embora o número de "fatores"possa diferir de uma representação para outra, sua paridade é sempre constante ([6, p.199]).

Definição 3.13. Uma permutação será chamada **par** se for escrita como o produto de uma quantidade par de transposições, e é chamada de **ímpar** caso contrário.

Uma vez que P_q é um grupo finito, podemos nos questionar quais são seus geradores. No próximo resultado, responderemos a essa pergunta.

Teorema 3.14. *Sejam $q > 2$ e ξ um elemento primitivo sobre $\mathbb{F}_q$. Então, P_q é gerado por X^{q-2} e todos os polinômios lineares $aX + b$ sobre $\mathbb{F}_q$, com $a \neq 0$, ou ainda, gerado por $\xi X, X + 1$ e X^{q-2}.*

Demonstração. Primeiro, precisamos provar que esses polinômios estão, de fato, em P_q. Sejam $a, b \in \mathbb{F}_q$, $a \neq 0$. Suponha que existam elementos $x, y \in \mathbb{F}_q$ tais que

$$ax + b = ay + b.$$

Se somarmos o oposto de b e multiplicarmos pelo inverso de a em ambos os lados da igualdade, veremos que $x = y$, isto é, $aX + b$ é injetor (logo, de permutação). Isso mostra que polinômios lineares realmente pertencem a P_q.

No caso do monômio X^{q-2}, podemos generalizar um pouco: o monômio X^r é de permutação se, e somente se, $\text{mdc}(r, q-1) = 1$. Para demonstrar esse fato, seja ξ um elemento primitivo de

$\mathbb{F}_q$ e suponha que existam elementos $\xi^a, \xi^b \in \mathbb{F}_q$, com $0 \leq a, b < q-1$, tais que $(\xi^r)^a = (\xi^a)^r = (\xi^b)^r = (\xi^r)^b$. Uma vez que ξ^r é também um elemento primitivo, devemos ter $a - b \equiv 0 \pmod{q-1}$, o que implica $a = b$ e X^r uma injeção (logo bijeção) em $\mathbb{F}_q$.

Vamos agora provar que toda transposição pode ser gerada por esses elementos. Como P_q é isomorfo a S_q, o resultado desse teorema seguirá do fato que toda permutação pode ser escrita como o produto de transposições. Observe que, para $a \neq 0$,

$$f_a(X) = -a^2[((x-a)^{q-2} + a^{-1})^{q-2} - a]^{q-2} \tag{3.2}$$

representa a transposição $(0a)$, e é uma composição de polinômios lineares com o monômio X^{q-2}. Uma transposição (bc) pode ser escrita como $(0b)(0c)(0b)$, logo a transposição (bc) é representada por $f_b \circ f_c \circ f_b$ e o primeiro resultado segue.

Para usarmos a caracterização com o elemento primitivo ξ, basta mostrar que um polinômio linear $aX + b$ pode ser escrito como a composição de ξX e $X + 1$. Uma vez que ξ é primitivo, existe um inteiro $s > q - 1$ tal que $a = \xi^s$. Se tivermos $b = 0$, então vale $aX = (\xi X)^s$. Caso contrário, vai existir um inteiro $t \in \{1, ..., q-1\}$ tal que $b = \xi^t$, daí

$$aX + b = \xi^s X + \xi^t = (\xi X)^t \circ (X+1) \circ (\xi X)^{s-t}.$$

■

Uma vez que P_q e S_q são isomorfos, podemos relacionar seus subgrupos. O subgrupo de S_q mais conhecido é o subgrupo alternado, formado por permutações pares. De modo análogo, diremos que $f \in P_q$ é um **polinômio de permutação par** se a permutação por ele induzida for par.

Lema 3.15. *Sejam $q > 2$ e $a \in \mathbb{F}_q$. Então $X + a$ e $(X^{q-2} + a)^{q-2}$ são polinômios de permutação pares. aX é um polinômio de permutação par se, e somente se, a for o quadrado de um elemento em $\mathbb{F}_q^*$. Além disso, X^{q-2} é um polinômio de permutação par se, e somente se, $q \equiv 3 \pmod 4$.*

Demonstração. Seja $q = p^n$. Para um elemento $a \in \mathbb{F}_q$ dado, denotemos por σ a permutação induzida por $X + a$. Observe que, para um elemento $b \in \mathbb{F}_q$, temos

$$\sigma(b) = b + a, \sigma(b + a) = b + 2a, ..., \sigma(b + (p-1)a) = b + pa = b.$$

Dessa forma, é possível ver que σ pode ser escrita como o produto de p^{n-1} ciclos de comprimento p.

Assim, se p for ímpar, esses ciclos serão pares, e se p for 2, mas $n > 1$ teremos uma quantidade par de cíclos ímpares. De qualquer modo, teremos provado que, para $q > 2$, $X + a$ induz uma permutação par e é, portanto, um polinômio de permutação par.

Agora, reparemos que

$$(X^{q-2} + a)^{q-2} = (X^{q-2}) \circ (X + a) \circ (X^{q-2}).$$

Independentemente da paridade de X^{q-2}, como ele corresponde a dois "fatores", a paridade de $(X^{q-2} + a)^{q-2}$ é igual à paridade de $X + a$, ou seja, é par.

aX é um polinômio de permutação se, e somente se, $a \neq 0$. Nesse caso, tomando ξ um elemento primitivo de $\mathbb{F}_q$, podemos escrever $a = \xi^s$, para algum inteiro s. Desse modo,

$$aX = \underbrace{(\xi X) \circ (\xi X) \circ \cdots \circ (\xi X)}_{s \text{ vezes}}.$$

A permutação induzida por ξX é o ciclo $(1\xi\xi^2 \cdots \xi^{q-2})$. Portanto, se tivermos q ímpar, esse ciclo será ímpar, e temos aX par se, e somente se, s for par, ou seja, se a for o quadrado de

um elemento em $\mathbb{F}_q$. Se q for par, o ciclo será par, e como a é sempre um quadrado (uma vez que $\text{mdc}(2, q-1) = 1$, temos X^2 uma bijeção, conforme notado na demonstração do Teorema 3.14), o resultado vale.

Por fim, note que, para um elemento $a \in \mathbb{F}_q^*$, $a^{q-2} = a^{-1}$ (já que $a^{q-1} = 1$). Então, a permutação induzida por X^{q-2} fixa o elemento 0 e leva todo elemento não nulo em seu inverso. Se q for ímpar, $0, \pm 1$ serão os únicos elementos fixados por X^{q-2}. Assim sendo, a permutação induzida por X^{q-2} é o produto de $\frac{q-3}{2}$ transposições. No caso q par, temos $1 = -1$, e a permutação é o produto de $\frac{q-2}{2}$ transposições. ■

Podemos definir os seguintes subconjuntos de P_q (para $q > 2$):

$$A_q = \{f : f \text{ é polinômio de permutação par}\},$$

$$L_q = \{aX + b : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\},$$
$$AL_q = \{a^2X + b : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\},$$
$$Q_q = \{(X^{q-2} + a)^{q-2} : a \in \mathbb{F}_q\}.$$

Teorema 3.16. *Sejam $q > 2$ e ξ um elemento primitivo de $\mathbb{F}_q$. Os conjuntos acima são subgrupos de P_q e possuem as seguintes propriedades:*

(i) $|L_q| = q(q-1)$ *e* L_q *é gerado por* ξX *e* $X + 1$*;*

(ii) $|AL_q| = \frac{q(q-1)}{2}$ *se* q *for ímpar e* $|AL_q| = q(q-1)$ *se* q *for par. Além disso,* AL_q *é gerado por* $\xi^2 X$ *e* $X + 1$*;*

(iii) $|Q_q| = q$ *e* Q_q *é isomorfo ao grupo aditivo de* $\mathbb{F}_q$*;*

(iv) A_q *é gerado por* $\xi^2 X, X + 1$ *e* $(X^{q-2} + 1)^{q-2}$*;*

(v) A_q *é gerado por seus subgrupos* AL_q *e* Q_q*.*

Demonstração. (i) Observe que temos q opções para b e $q-1$ opções para a, logo $|L_q| = q(q-1)$. Podemos ver que os geradores de L_q são ξX e $X + 1$ na demonstração do Teorema 3.14.

(ii) Novamente temos q opções para b. Agora, se q for ímpar, teremos $a \neq -a$ (uma vez que $a \neq 0$), mas $a^2 = (-a)^2$, isto é, existem apenas $\frac{q-1}{2}$ quadrados não nulos em $\mathbb{F}_q$, donde concluímos que $|AL_q| = \frac{q(q-1)}{2}$. Por outro lado, se q for par, todo elemento de $\mathbb{F}_q$ será um quadrado e temos $q-1$ opções para a. Assim, $|AL_q| = q(q-1)$. Podemos ver que os geradores de L_q são $\xi^2 X$ e $X + 1$ repetindo a demonstração do Teorema 3.14.

(iii) Basta mostrar que

$$\begin{array}{rccc} \sigma : & \mathbb{F}_q & \longrightarrow & Q_q \\ & a & \mapsto & (X^{q-2} + a)^{q-2} \end{array}$$

é um isomorfismo. Temos

$$\sigma(a) \circ \sigma(b) = (((X^{q-2} + b)^{q-2})^{q-2} + a)^{q-2}.$$

Agora, seja $c \in \mathbb{F}_q$. Se tivermos $c^{q-2} + b = 0$, então $(\sigma(a) \circ \sigma(b))(c) = a^{q-2}$. Por outro lado,

$$\sigma(a + b)(c) = (c^{q-2} + a + b)^{q-2} = a^{q-2}.$$

Agora, se $c^{q-2} + b \neq 0$, então

$$(\sigma(a) \circ \sigma(b))(c) = (((c^{q-2} + b)^{q-2})^{q-2} + a)^{q-2} = (c^{q-2} + b + a)^{q-2} = \sigma(a + b)(c).$$

(Aqui, usamos o fato que, se $\alpha \neq 0$, então $\alpha^{q-2} = \alpha^{-1}$). Desse modo, temos $(\sigma(a) \circ \sigma(b)) = \sigma(a+b)$ e σ é um homomorfismo.

A sobrejetividade de σ é trivial, restando mostrar apenas a injetividade. Para isso, sejam $a, b \in \mathbb{F}_q$ tais que

$$\sigma(a) = (X^{q-2} + a)^{q-2} = (X^{q-2} + b)^{q-2} = \sigma(b).$$

Tomando $x = 0$, vemos que $a = b$ e σ é uma bijeção.

(iv) Para provar esse item, vamos usar a caracterização da transposição $(0a)$ dada em (3.2). Já usamos o fato que uma qualquer transposição (bc) pode ser escrita como $(0b)(0c)(0b)$, então uma permutação par (e, portanto, um elemento de A_q) é escrito a partir de uma quantidade par de transposições do tipo $(0a)$. O que faremos agora é mostrar que o produto de duas tais composições pode ser gerada pelos elementos $\xi^2 X, X+1$ e $(X^{q-2}+1)^{q-2}$. Temos

$$(0a)(0b) = -a^2[((-b^2[((X-b)^{q-2} + b^{-1})^{q-2} - b]^{q-2} - a)^{q-2} + a^{-1})^{q-2} - a]^{q-2}.$$

Observe que $(-1)^{q-2} = -1$ (em característica par, $1 = -1$), então podemos reescrever essa equação na forma

$$a^2[((b^2[((X-b)^{q-2} + b^{-1})^{q-2} - b]^{q-2} + a)^{q-2} - a^{-1})^{q-2} + a]^{q-2}.$$

É fácil ver que essa expressão é uma composição dos polinômios $\xi^2 X, X+1$ e $(X^{q-2}+1)^{q-2}$, observando-se que $X + \alpha$ pode ser escrito como composições de $X+1$, $\alpha^2 X$ é composição de uma quantidade adequada de fatores $\xi^2 X$ e $(X^{q-2} + \alpha)^{q-2}$ é decomposto apenas nos fatores $(X^{q-2}+1)^{q-2}$.

(v) Como foi mencionado no item anterior, Q_q é gerado por $(X^{q-2}+1)^{q-2}$ e AL_q é gerado por $\xi^2 X$ e $X+1$.

■

Encerraremos esta seção relacionando a bijetivade de um polinômio sobre $\mathbb{F}_q$ com sua bijetividade em extensões de $\mathbb{F}_q$.

Teorema 3.17. *Um polinômio $f \in \mathbb{F}_q[X]$ é de permutação sobre todas as extensões finitas de $\mathbb{F}_q$ se, e somente se, for da forma $f(X) = aX^{p^h} + b$, em que $a \neq 0$, p é a característica de $\mathbb{F}_q$ e h é um inteiro não negativo.*

Demonstração. A suficiência é trivial: uma vez que $\text{mdc}(p^h, q^r - 1) = 1$ para todo $r > 1$, o monômio X^{p^h} é de permutação sobre toda extensão finita de $\mathbb{F}_q$. O resultado segue observando-se que $aX^{p^h} + b$ é a composição de $aX + b$ com X^{p^h}.

Para a necessidade, precisaremos de um lema, que referenciaremos para assumir sem demonstração.

Lema 3.18. *([15, Lema 6.39]) Para um primo p fixado, denotemos por s_m a soma dos dígitos da representação de m na base p e $E_p(m)$ o maior expoente de p que divide m. Se m for não negativo, então*

$$E_p(m) = \frac{m - s_m}{p-1}.$$

Agora, note que, se f for de permutação sobre $\mathbb{F}_q$, então, para todo $c \in \mathbb{F}_q$, a equação $f(X) = c$ terá exatamente uma solução $\alpha_c \in \mathbb{F}_q$. Dessa forma, devemos ter

$$f(X) - c = (X - \alpha_c)^{k_c} g_c(X),$$

em que $g_c(X)$ é um fator constante ou o produto de fatores irredutíveis sobre $\mathbb{F}_q$ de graus maiores que 1. Porém, se r_c for múltiplo do grau de algum fator irredutível $g_c(X)$, $f(X) - c$ possuirá uma raiz em $\mathbb{F}_{q^{r_c}}$ diferente de α_c (Teorema 1.15 combinado com Teorema 1.18). Desse modo, f não seria de permutação sobre $\mathbb{F}_{q^{r_c}}$.

Então, concluímos que $g_c(X)$ é uma constante (o coeficiente líder de f) e $k_c = \deg(f) := k$, para todo $c \in \mathbb{F}_q$, então

$$f(X) - c = a(X - \alpha_c)^k, a \neq 0.$$

Fazendo $c = 0$, $c = 1$ e subtraindo as duas equações, obtemos

$$a(X - \alpha_0)^k - a(X - \alpha_1)^k = 1.$$

Por fim, substituindo X por $X + \alpha_1$, temos

$$a(X + \alpha_1 - \alpha_0)^k - aX^k = 1.$$

Se fizermos a expansão binomial e compararmos os dois lados da equação, devemos ter

$$\binom{k}{j} \equiv 0 (\text{mod } p), \text{ para } 0 < j < k.$$

Podemos encontrar um inteiro não negativo h tal que $p^h \leq k < p^{h+1}$. Se tivéssemos $k \neq p^h$, a equação acima nos diria que $\binom{k}{p^h} \equiv 0 \pmod{p}$, mas o lema referenciado nessa demonstração nos diz que

$$E_p\left(\binom{k}{p^h}\right) = \frac{s_{p^h} + s_{k-p^h} - s_k}{p-1} = \frac{1 + (s_k - 1) - s_k}{p-1} = 0,$$

e p não divide $\binom{k}{p^h}$. Essa contradição nos mostra que devemos ter $k = p^h$ e $f(X) = a(X - \alpha_0)^{p^h} = aX^{p^h} + a(-\alpha_0)^{p^h}$. ■

Corolário 3.19. *Se $f \in \mathbb{F}_q[X]$ não for da forma $aX^{p^h} + b$, então existirão infinitas extensões $\mathbb{F}_{q^r}$ de $\mathbb{F}_q$ tais que f não é de permutação sobre $\mathbb{F}_{q^r}$.*

Demonstração. Se f não for de permutação sobre $\mathbb{F}_q$, ele não poderá ser de permutação sobre nenhuma extensão $\mathbb{F}_{q^r}$. Se f for de permutação sobre $\mathbb{F}_q$, nas notações do teorema anterior, deveremos ter $f(X) = (X - \alpha_0)^{k_0} g_0(X)$, em que $g_0(X)$ não é um fator constante. Assim, f possui uma raiz diferente de α_0 (e, portanto, não é de permutação) em cada $\mathbb{F}_{q^r}$ em que r é múltiplo do grau de algum fator irredutível de $g_0(X)$. ■

3.2 PPs gerados a partir de outros PPs

Uma vez que existem $q!$ bijeções em um conjunto com q elementos (assim como $\mathbb{F}_q$), existem $q!$ polinômios de permutação sobre $\mathbb{F}_q$ de grau menor do que q, que podem ser construídos através da equação (3.1). Por isso, um polinômio é de permutação se, e somente se, sua classe residual módulo $X^q - X$ coincidir com algum dos polinômios obtidos dessa forma (Lema 3.4).

Embora seja simples criar um polinômio de permutação usando a fórmula, é ainda melhor tentar obter um tal polinômio a partir de outro. Na seção anterior, vimos que podemos compor dois polinômios de permutação, mas esse não é o único modo. O próximo resultado, por exemplo, é talvez o mais famoso e pode ser aplicado não apenas no estudo da bijeção de polinômios, mas também de funções definidas sobre conjuntos finitos.

Teorema 3.20 (Critério AGW, [2]). *Sejam A, S e $\bar{S}$ conjuntos finitos com $\#S = \#\bar{S}$, e sejam $f : A \to A$, $h : S \to \bar{S}$, $\lambda : A \to S$ e $\bar{\lambda} : A \to \bar{S}$ aplicações tais que $\bar{\lambda} \circ f = h \circ \lambda$, ou seja, o seguinte diagrama é comutativo.*

$$\begin{array}{ccc} A & \xrightarrow{f} & A \\ {\scriptstyle\lambda}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\bar{\lambda}} \\ S & \xrightarrow[h]{} & \bar{S} \end{array}$$

Se ambas λ e $\bar{\lambda}$ forem sobrejetoras, então são equivalentes:
(1) f é uma bijeção;
(2) h é uma bijeção de S em $\bar{S}$ e f é injetora em $\lambda^{-1}(t)$ para cada $t \in S$.

Demonstração. Primeiro, assuma que f seja uma bijeção. Por definição, f será injetora em $\lambda^{-1}(t)$ para cada $t \in S$. Além disso, f e $\bar{\lambda}$ são sobrejetoras, e como $\bar{\lambda} \circ f = h \circ \lambda$, temos h uma sobrejeção de S em $\bar{S}$, logo uma bijeção de S em $\bar{S}$ (pois S e $\bar{S}$ são conjuntos finitos com a mesma quantidade de elementos).

Reciprocamente, suponha que existam $a_1, a_2 \in A$ tais que $f(a_1) = f(a_2)$. Assim,

$$h(\lambda(a_1)) = \bar{\lambda}(f(a_1)) = \bar{\lambda}(f(a_2)) = h(\lambda(a_2)).$$

Como h é uma bijeção, temos $\lambda(a_1) = \lambda(a_2)$, isto é, $a_1, a_2 \in \lambda^{-1}(t)$ para algum $t \in S$. Como f é injetora em cada $\lambda^{-1}(t)$, temos $a_1 = a_2$. Dessa forma, f é uma injeção, e portanto uma bijeção, já que A é um conjunto finito. ■

Em particular, se tomarmos, nas notações do teorema anterior, $A = \mathbb{F}_q$, $S = \bar{S} = \mu_d$ (o conjunto das raízes d-ésimas da unidade em $\mathbb{F}_q^*$ com $d \mid (q-1)$), $f(X) = X^r g(X^{(q-1)/d})$, $\lambda = \bar{\lambda} = X^{(q-1)/d}$ e $h(X) = X^r g(X)^{(q-1)/d}$, obteremos o seguinte resultado, que também é bastante utilizado e nos diz que, sob certas condições, ao invés de estudar a bijeção de um polinômio em todo o corpo $\mathbb{F}_q$, podemos estudá-la apenas em um subconjunto.

Teorema 3.21. *[11, Proposição 2.2] Dados $g(X) \in \mathbb{F}_q[X]$ e $r, d > 0$ com $d \mid (q-1)$, o polinômio $X^r g(X^{(q-1)/d})$ permuta $\mathbb{F}_q$ se, e somente se, as duas seguintes condições forem satisfeitas:*

(i) $mdc(r, (q-1)/d) = 1$;

(ii) $X^r g(X)^{(q-1)/d}$ permuta μ_d.

Talvez inspirados por esses teoremas, diversos autores buscaram equivalências para bijeções entre diferentes classes de polinômios. Nessa seção, destacamos nossa generalização da Proposição 3 de [21]. Sua demonstração é análoga à original e baseia-se apenas no Teorema 3.20, mas merece ser apresentada.

Proposição 3.22. *Sejam $k_1, ..., k_s, n$ inteiros tais que $0 < k_1 < \cdots < k_s < n$, $d = mdc(k_1, ..., k_s, n)$, $c \in \mathbb{F}_{q^d}^*$, $\alpha_0, ..., \alpha_s \in \mathbb{F}_{q^n}$ e $g(X) \in \mathbb{F}_{q^n}[X]$. Então,*

$$f(X) = g(\alpha_0 X + \alpha_1 X^{q^{k_1}} + \cdots + \alpha_s X^{q^{k_s}} + \delta) + cX$$

permuta $\mathbb{F}_{q^n}$ para cada $\delta \in \mathbb{F}_{q^n}$ se, e somente se,

$$h(X) = \alpha_0 g(X) + \alpha_1 g(X)^{q^{k_1}} + \cdots + \alpha_s g(X)^{q^{k_s}} + cX$$

permutar $\mathbb{F}_{q^n}$.

Demonstração. Sejam

$$\varphi(X) = \alpha_0 X + \alpha_1 X^{q^{k_1}} + \cdots + \alpha_s X^{q^{k_s}} + \delta \text{ e } S_\delta = \{\alpha_0 x + \alpha_1 x^{q^{k_1}} + \cdots + \alpha_s x^{q^{k_s}} + \delta : x \in \mathbb{F}_{q^n}\}.$$

Claramente $S_\delta \subseteq \mathbb{F}_{q^n}$ e $\cup_{\delta \in \mathbb{F}_{q^n}} S_\delta = \mathbb{F}_{q^n}$ (tomando $x = 0$, vemos que $\delta \in S_\delta$). Denote por

$$\bar{h}(X) = \alpha_0 g(X) + \alpha_1 g(X)^{q^{k_1}} + \cdots + \alpha_s g(X)^{q^{k_s}} + cX + (1-c)\delta = h(X) + (1-c)\delta.$$

Temos $\bar{h} : S_\delta \to S_\delta$. De fato, seja $y = \alpha_0 x + \alpha_1 x^{q^{k_1}} + \cdots + \alpha_s x^{q^{k_s}} + \delta \in S_\delta$, para algum $x \in \mathbb{F}_{q^n}$. Então,

$$\begin{aligned}
\bar{h}(y) &= \alpha_0 g(y) + \alpha_1 g(y)^{q^{k_1}} + \cdots + \alpha_s g(y)^{q^{k_s}} + c(\alpha_0 x + \alpha_1 x^{q^{k_1}} + \cdots + \alpha_s x^{q^{k_s}} + \delta) + (1-c)\delta \\
&= \alpha_0 \underbrace{(g(y) + cx)}_{z} + \alpha_1 (g(y) + cx)^{q^{k_1}} + \cdots + \alpha_s (g(y) + cx)^{q^{k_s}} + c\delta + (1-c)\delta \\
&= \alpha_0 z + \alpha_1 z^{q^{k_1}} + \cdots + \alpha_s z^{q^{k_s}} + \delta \in S_\delta.
\end{aligned}$$

Além disso,

$$\begin{aligned}
\varphi \circ f &= \alpha_0[g(\varphi(X)) + cX] + \alpha_1[g(\varphi(X)) + cX]^{q^{k_1}} + \cdots + \alpha_s[g(\varphi(X)) + cX]^{q^{k_s}} + \delta \\
&= \alpha_0 g(\varphi(X)) + \alpha_1 g(\varphi(X))^{q^{k_1}} + \cdots + \alpha_s g(\varphi(X))^{q^{k_s}} + c(\alpha_0 X + \alpha_1 X^{q^{k_1}} + \cdots + \alpha_s X^{q^{k_s}}) + \delta
\end{aligned}$$

$$\begin{aligned}
\bar{h} \circ \varphi &= \alpha_0 g(\varphi(X)) + \alpha_1 g(\varphi(X))^{q^{k_1}} + \cdots + \alpha_s g(\varphi(X))^{q^{k_s}} + c(\varphi(X)) + (1-c)\delta \\
&= \alpha_0 g(\varphi(X)) + \alpha_1 g(\varphi(X))^{q^{k_1}} + \cdots + \alpha_s g(\varphi(X))^{q^{k_s}} + c(\alpha_0 X + \alpha_1 X^{q^{k_1}} + \cdots + \alpha_s X^{q^{k_s}}) + \delta
\end{aligned},$$

donde concluímos que $\varphi \circ f = \bar{h} \circ \varphi$.

Para cada $\beta \in S_\delta$, temos $f(X) = g(\beta) + cX$, o que implica que f é injetora em $\varphi^{-1}(\beta)$. O Teorema 3.20 nos diz então que $f(X)$ permuta $\mathbb{F}_{q^n}$ se, e somente se, $\bar{h}(X)$ permutar S_δ para cada $\delta \in \mathbb{F}_{q^n}$. Mas, como $\bar{h} = h + (1-c)\delta$, concluímos que $\bar{h}$ permuta S_δ se, e somente se, h for bijeção entre S_δ e $S_{c\delta}$ para cada $\delta \in \mathbb{F}_{q^n}$.

Por fim, notemos que $\cup_{\delta \in \mathbb{F}_{q^n}} S_\delta = \cup_{\delta \in \mathbb{F}_{q^n}} S_{c\delta} = \mathbb{F}_{q^n}$. Então, se h for bijeção entre S_δ e $S_{c\delta}$ para todo δ, h será uma sobrejeção de $\mathbb{F}_{q^n}$ em si mesmo, e como $\mathbb{F}_{q^n}$ é finito, teremos h uma bijeção. Por outro lado, se h for uma bijeção em $\mathbb{F}_{q^n}$, h será uma bijeção entre S_δ e $S_{c\delta}$. Então, $\bar{h}$ permuta S_δ para cada $\delta \in \mathbb{F}_{q^n}$ se, e somente se, h for uma bijeção em $\mathbb{F}_{q^n}$. ■

Buscando alguns exemplos para aplicar nossa proposição, nos deparamos com o trabalho de Kyureghyan e Zieve ([11]). Nesse artigo, eles também trouxeram algumas equivalências entre bijeções de certas funções, e que merecem ser apresentadas uma vez que tratam do problema central dessa seção.

Proposição 3.23. *Sejam $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, com $n \geq 2$ e $\gamma \in \mathbb{F}_{q^n}^*$. São equivalentes:*

(i) A aplicação $F : x \mapsto x + \gamma f(x)$ é bijetivo em $\mathbb{F}_{q^n}$;

(ii) Para cada $\alpha \in \mathbb{F}_{q^n}$ a aplicação $x \mapsto x + f(\alpha + \gamma x)$ é bijetivo em $\mathbb{F}_q$;

(iii) Para cada $\alpha \in \mathbb{F}_{q^n}$ existe um único $x \in \mathbb{F}_q$ tal que $x + f(\alpha + \gamma x) = 0$.

Demonstração. ($(i) \iff (ii)$): Observe que, fixados $\alpha \in \mathbb{F}_{q^n}$ e $u \in \mathbb{F}_q$, temos

$$F(\alpha + \gamma u) = \alpha + \gamma(u + f(\alpha + \gamma u)), \tag{3.3}$$

donde concluímos que F aplica $\alpha + \gamma\mathbb{F}_q$ em si mesmo. Assim, F é uma bijeção em $\mathbb{F}_{q^n}$ se, e somente se, for uma bijeção em cada conjunto $\alpha + \gamma\mathbb{F}_q$. Além disso, a equação (3.3) nos mostra que F é uma bijeção em $\alpha + \gamma\mathbb{F}_q$ se, e somente se, a aplicação $x \mapsto x + f(\alpha + \gamma x)$ for bijetor em $\mathbb{F}_q$.

$((ii) \iff (iii))$: Usando o Teorema 3.2(v), concluímos que $(ii) \implies (iii)$. Agora, suponha que exista $\alpha' \in \mathbb{F}_{q^n}$ tal que a função $X + f(\alpha' + \gamma X)$ não seja bijetora em $\mathbb{F}_q$. Então, existem $u_1, u_2 \in \mathbb{F}_q$ com mesma imagem y. Assim,

$$y = u_1 + f(\alpha' + \gamma u_1) \iff (u_1 - y) + f(\alpha' + \gamma(u_1 - y) + \gamma y) = 0$$

e $x_1 = u_1 - y$ é um zero de $X + f(\alpha + \gamma X)$, com $\alpha = \alpha' + \gamma y$. É claro que podemos repetir as contas para u_2 e veremos que $x_2 = u_2 - y$ é também um zero de $X + f(\alpha + \gamma X)$, ou seja, (iii) não é válido. ■

Proposição 3.24. *Sejam $\gamma, \omega \in \mathbb{F}_{q^2}$ linearmente independentes sobre $\mathbb{F}_q$ e seja $f : \mathbb{F}_{q^2} \to \mathbb{F}_q$ uma função satisfazendo $f(ux) = uf(x)$, para todos $u \in \mathbb{F}_q, x \in \mathbb{F}_{q^2}$. Então $x \mapsto x + \gamma f(x)$ permuta $\mathbb{F}_{q^2}$ se, e somente se, $f(\gamma) \neq -1$ e $x \mapsto x + f(\omega + \gamma x)$ permutar $\mathbb{F}_q$.*

Demonstração. Pela Proposição 3.23, $X + \gamma f(X)$ permuta $\mathbb{F}_{q^2}$ se, e somente se, $F_\alpha(X) = X + f(\alpha + \gamma X)$ permutar $\mathbb{F}_q$ para cada $\alpha \in \mathbb{F}_{q^2}$. Uma vez que γ e ω são linearmente independentes, todo elemento de $\mathbb{F}_{q^2}$ pode ser escrito sob a forma $\alpha = u\gamma + v\omega$, $u, v \in \mathbb{F}_q$.

Se tivermos $v = 0$, para cada $x \in \mathbb{F}_q$ valerá

$$F_\alpha(x) = x + f((u + x)\gamma) = x + (u + x)f(\gamma) = (1 + f(\gamma))x + uf(\gamma),$$

e temos F_α uma bijeção em $\mathbb{F}_q$ se, e somente se, $f(\gamma) \neq -1$. Se $v \neq 0$, obteremos

$$F_\alpha(x) = x + f(v\omega + (u + x)\gamma) = v\left(\frac{x}{v} + f\left(\omega + \frac{u + x}{v}\gamma\right)\right).$$

Fazendo a mudança de variáveis $X = \frac{x}{v}$, temos F_α uma bijeção em $\mathbb{F}_q$ se, e somente se, $X + f(\omega + (X + \frac{u}{v})\gamma)$ for uma bijeção em $\mathbb{F}_q$, o que é equivalente a $x \mapsto x + f(\omega + \gamma x)$ permutar $\mathbb{F}_q$. ■

A proposição a seguir é um exemplo de como podemos relacionar a bijetividade de um polinômio com uma função racional.

Proposição 3.25. *Sejam $k := (q-1)N+1$ para algum natural N e $\gamma \in \mathbb{F}_{q^2}^*$. Então o polinômio $F(X) := X + \gamma\, Tr_{q^2/q}(X^k)$ permuta $\mathbb{F}_{q^2}$ se, e somente se,*

$$H(X) := \frac{X^N + \gamma^q(1 + X^{2N-1})}{X^{N-1} + \gamma(X^{2N-1} + 1)}$$

permutar o conjunto μ_{q+1} das raízes $(q+1)$-ésimas da unidade em $\mathbb{F}_{q^2}^*$, ou, de modo equivalente, essa função racional for injetiva em μ_{q+1} e seu denominador não tiver nenhuma raiz nesse conjunto.

Demonstração. Observe que

$$F(X) = X + \gamma(X^k + X^{qk}) = X(1 + \gamma(X^{(q-1)N} + X^{(q-1)(qN+1)})).$$

Assim, pelo Teorema 3.21, F permuta $\mathbb{F}_{q^2}$ se, e somente se,

$$G(X) = X(1 + \gamma(X^N + X^{qN+1}))^{q-1}$$

permutar μ_{q+1}. Então, seja $x \in \mu_{q+1}$ tal que $G(x) \neq 0$. Temos $x^q = x^{-1}$ (pois $x \in \mu_{q+1}$), $x^{q^2} = x$ (pois $x \in \mathbb{F}_{q^2}$) e

$$\frac{G(x)}{x} = \frac{(1 + \gamma(x^N + x^{qN+1}))^q}{1 + \gamma(x^N + x^{qN+1})} = \frac{1 + \gamma^q(x^{-N} + x^{N-1})}{1 + \gamma(x^N + x^{-N+1})} = \frac{x^N(1 + \gamma^q(1 + x^{2N-1})x^{-N})}{x \cdot x^{N-1}(1 + \gamma(x^{2N-1} + 1)x^{-N+1})} = \frac{H(x)}{x}.$$

Desse modo, podemos concluir que G permuta μ_{q+1} se, e somente se, H permutar μ_{q+1}.

Além disso, se o denominador de H não se anular em μ_{q+1}, teremos $G(x) = H(x)$, para todo $x \in \mu_{q+1}$, logo $H(\mu_{q+1}) = G(\mu_{q+1}) \subseteq \mu_{q+1}$ e a bijetividade de H em μ_{q+1} será equivalente à sua injetividade. ■

Encerramos esse capítulo apresentando alguns polinômios que encontramos em ([11]) e que podem ser usados na Proposição 3.22. Nas notações dessa proposição, o lema a seguir nos fornece seis exemplos de polinômios h.

Lema 3.26. *[11, Teorema 1.1] O polinômio $F(X) = X + \gamma Tr_{q^n/q}(X^k)$ é um polinômio de permutação sobre $\mathbb{F}_{q^n}$ nos seguintes casos:*
(i) $n = 2$, $q \equiv \pm 1 \pmod 6$, $\gamma = \frac{-1}{3}$, $k = 2q - 1$.
(ii) $n = 2$, $q \equiv 5 \pmod 6$, $\gamma^3 = \frac{-1}{27}$, $k = 2q - 1$.
(iii) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = \frac{q^2+q+1}{3}$.
(iv) $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = \frac{(q+1)^2}{4}$.
(v) $n = 3$, q *ímpar*, $\gamma = 1$, $k = \frac{q^2+1}{2}$.
(vi) $n = 3$, q *ímpar*, $\gamma = \frac{-1}{2}$, $k = q^2 - q + 1$.

Agora, munidos desses vários exemplos, podemos aplicar a Proposição 3.22 e encontrar mais seis exemplos de polinômios de permutação.

Teorema 3.27. *O polinômio $(\gamma Tr_{q^n/q}(X) + \delta)^k + X$, $\gamma \in \mathbb{F}_{q^n}^*$, permuta $\mathbb{F}_{q^n}$ para todo $\delta \in \mathbb{F}_{q^n}$ nos seguintes casos:*
(i) $n = 2$, $q \equiv \pm 1 \pmod 6$, $\gamma = \frac{-1}{3}$, $k = 2q - 1$.
(ii) $n = 2$, $q \equiv 5 \pmod 6$, $\gamma^3 = \frac{-1}{27}$, $k = 2q - 1$.
(iii) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = \frac{q^2+q+1}{3}$.
(iv) $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = \frac{(q+1)^2}{4}$.
(v) $n = 3$, q *ímpar*, $\gamma = 1$, $k = \frac{q^2+1}{2}$.
(vi) $n = 3$, q *ímpar*, $\gamma = \frac{-1}{2}$, $k = q^2 - q + 1$.

Capítulo 4

Polinômios de permutação obtidos a partir de q-polinômios

Nos capítulos anteriores, vimos alguns resultados sobre q-polinômios e polinômios de permutação. É natural agora tentar unir esses dois assuntos e tentar descobrir quando q-polinômios são de permutação ou tentar obter polinômios de permutação usando, de algum modo, os q-polinômios. Uma vez que q-polinômios induzem aplicações lineares em $\mathbb{F}_{q^n}$, o seguinte critério é muito útil para esse fim.

Teorema 4.1. *Seja $\mathbb{F}_q$ um corpo de característica p. O p-polinômio*

$$L(X) = \sum_{i=0}^{n} a_i X^{p^i}$$

é de permutação sobre $\mathbb{F}_q$ se, e somente se, sua única raiz em $\mathbb{F}_q$ for 0.

Demonstração. Como visto no Teorema 2.2, o polinômio L induz uma aplicação linear de $\mathbb{F}_q$ em $\mathbb{F}_q$. Por isso, L é injetor (e portanto, de permutação) se, e somente se seu núcleo (seu conjunto de raízes) for $\{0\}$. ■

Em vista do Lema 3.3, um q-polinômio $L(X)$ é de permutação sobre $\mathbb{F}_q$ se, e somente se, o grau do mdc entre L e $X^q - X$ for 1.

É claro que, impondo mais condições em L, pode-se obter resultados mais específicos para determinadas situações, mas não entraremos nesses detalhes. Nesse capítulo, vamos estudar polinômios de permutação da forma $(X^{p^k} - X + \delta)^s + L(X)$ e dois métodos para construir q-polinômios de permutação.

4.1 Uma classe de polinômios de permutação

A grande maioria dos autores da área de polinômios de permutação foca seus trabalhos em uma determinada classe polinomial, porque precisam de um resultado específico para determinada situação que se depararam ou porque foram inspirados pelo trabalho de outros autores. A classe de polinômios da forma $(X^{p^k} - X + \delta)^s + L(X)$, com $\delta \in \mathbb{F}_{p^n}$ e $L(X)$ um q-polinômio, por exemplo, foi primeiro estudada por Helleseth e Zinoviev que buscavam obter novas identidades para as somas de Kloosterman ([9]). Dando continuidade a esse estudo inicial, Li, Helleseth e Tang obtiveram novas condições sobre n e k para que p seja um polinômio de permutação com valores específicos de s ([14]). Esse trabalho será destacado nessa seção.

4.1.1 Caso $s = \frac{p^n-1}{2} + p^r$

Inicialmente, vamos fixar algumas notações. Nessa seção, sempre trabalharemos sobre $\mathbb{F}_{p^n}$. Seja $\alpha \in \mathbb{F}_{p^n}$ um elemento primitivo e defina $D_0 = \langle \alpha^2 \rangle$ e $D_1 = \alpha D_0$, ou seja, o conjunto formado pelas potências pares e ímpares, respectivamente, de α. Então, $\mathbb{F}_{p^n} = \{0\} \cup D_0 \cup D_1$. Note ainda que, uma vez que a ordem multiplicativa de α é $p^n - 1$, vale $x^{(p^n-1)/2} = 1$ se $x \in D_0$ e $x^{(p^n-1)/2} = -1$ se $x \in D_1$. Com essa restrição de s, os autores forneceram cinco condições para que polinômios da forma $(X^{p^k} - X + \delta)^s + L(X)$ sejam de permutação. Todos os resultados serão citados, mas vamos demonstrar apenas dois deles, uma vez que suas provas são bastante similares.

Teorema 4.2. *Sejam p um primo ímpar e n, k inteiros positivos. Então, o polinômio $(X^{p^k} - X + \delta)^{\frac{p^n+1}{2}} + X^{p^k} + X$ é um polinômio de permutação em $\mathbb{F}_{p^n}$ para todo $\delta \in \mathbb{F}_{p^n}$.*

Demonstração. Pelo Teorema 3.2(iv), precisamos mostrar que, para todo $b \in \mathbb{F}_{p^n}$, a equação

$$(X^{p^k} - X + \delta)^{\frac{p^n-1}{2}+1} + X^{p^k} + X = b \tag{4.1}$$

tem no máximo uma solução em $\mathbb{F}_{p^n}$. Então, suponhamos que exista uma solução x e temos três possíveis casos.

Caso 1) $x^{p^k} - x + \delta = 0$: podemos concluir que $x^{p^k} = x - \delta$. A equação (4.1) nos diz que $x^{p^k} + x = b$, então

$$x^{p^k} + x = b \Longrightarrow x - \delta + x = b \Longrightarrow x = \frac{b+\delta}{2}.$$

Em particular, x está unicamente determinado por b e δ e

$$x^{p^k} + x = b \Longrightarrow \left(\frac{b+\delta}{2}\right)^{p^k} + \frac{b+\delta}{2} = b \Longrightarrow b^{p^k} + \delta^{p^k} - b + \delta = 0.$$

Caso 2) $x^{p^k} - x + \delta \in D_0$: nessa situação, temos $(x^{p^k} - x + \delta)^{\frac{p^n-1}{2}} = 1$ e a equação (4.1) se torna $(x^{p^k} - x + \delta) + x^{p^k} + x = b$, donde obtemos $x^{p^k} = \frac{b-\delta}{2}$. Como $\mathrm{mdc}(p^k, p^n - 1) = 1$, X^{p^k} é uma bijeção em $\mathbb{F}_{p^n}$. Em particular, x é unicamente determinado por

$$x = \frac{b^{p^{n-k}} - \delta^{p^{n-k}}}{2}$$

e vale

$$x^{p^k} - x + \delta = \frac{b + \delta - b^{p^{n-k}} + \delta^{p^{n-k}}}{2}.$$

Caso 3) $x^{p^k} - x + \delta \in D_1$: nesse último caso, a equação (4.1) pode ser reescrita como $-(x^{p^k} - x + \delta) + x^{p^k} + x = b$ e x é unicamente determinado por $\frac{b+\delta}{2}$. Fazendo um cálculo análogo ao que fizemos para o caso 1, temos

$$x^{p^k} - x + \delta = \frac{b^{p^k} + \delta^{p^k} - b + \delta}{2}.$$

Resta mostrar que apenas um dos casos pode acontecer. Para simplificar a notação, denotaremos $\Delta = \frac{b + \delta - b^{p^{n-k}} + \delta^{p^{n-k}}}{2}$ e temos $\frac{b^{p^k} + \delta^{p^k} - b + \delta}{2} = \Delta^{p^k}$. É claro que se (4.1) tiver uma solução x, um dos casos acima deve ocorrer. Observe que, se o caso 1 acontecer, temos $\Delta = 0$ e os casos 2 e 3 (que podem ser reescritos como $\Delta \in D_0$ e $\Delta^{p^k} \in D_1$, respectivamente)

não podem ocorrer. Por outro lado, se, para essa solução x, a condição do caso 1 não for satisfeita, exatamente um dos casos 2 ou 3 deve acontecer, uma vez que, por definição de D_0, $\Delta^{p^k} \in D_0$ se, e somente se, $\Delta \in D_0$.

Uma vez que Δ está unicamente determinado por b e δ e apenas um elemento $x \in \mathbb{F}_{p^n}$ pode satisfazer cada caso dentre (ii) e (iii), que são mutuamente exclusivos, se (4.1) tiver uma solução em $\mathbb{F}_{p^n}$, ela deve ser única. ■

As demonstrações dos próximos dois teoremas seguem a mesma linha de raciocínio, e portanto serão omitidas.

Teorema 4.3. *[14, Teorema 4] Sejam p um primo ímpar, n, k inteiros positivos tais que $n \mid 3k$ e $\delta \in \mathbb{F}_{p^n}$. Então, $(X^{p^k} - X + \delta)^{\frac{p^n-1}{2}+p^k} + X$ é um polinômio de permutação sobre $\mathbb{F}_{p^n}$.*

Teorema 4.4. *[14, Teorema 5] Sejam $n = 3d, k = d$ ou $k = 2d$, em que d é um inteiro positivo e $\delta \in \mathbb{F}_{3^n}$ com $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^d}}(\delta) = 0$. Então, $(X^{3^k} - X + \delta)^{\frac{3^n-1}{2}+3^k} + X^{3k} + X$ é um polinômio de permutação sobre $\mathbb{F}_{3^n}$.*

No próximo teorema, vamos usar um resultado sobre um tipo particular de matriz.

Definição 4.5. Uma matriz quadrada é dita uma **matriz de Hadamard** se seus elementos forem apenas 1 ou -1 e suas linhas forem duas a duas ortogonais.

Teorema 4.6. *Seja H uma matriz de Hadamard de ordem n. Então, H é invertível e vale $H^{-1} = \dfrac{H^T}{n}$.*

Demonstração. Seja $\ell_i = (a_{i,1}, ..., a_{i,n})$ o vetor correspondente à linha i de H. Uma vez que os elementos de uma matriz de Hadamard são sempre 1 ou -1, temos

$$\ell_i \cdot \ell_i = \sum_{j=1}^{n} a_{i,j}^2 = n,$$

em que $\cdot$ denota o produto interno padrão. Além disso, da própria definição, temos $\ell_i \cdot \ell_j = 0$ sempre que $i \neq j$. Assim,

$$HH^T = \begin{pmatrix} \ell_1 \cdot \ell_1 & \cdots & \ell_1 \cdot \ell_n \\ \vdots & \ddots & \vdots \\ \ell_n \cdot \ell_1 & \cdots & \ell_n \cdot \ell_n \end{pmatrix} = nI_n,$$

em que I_n é a matriz identidade de ordem n. ■

Teorema 4.7. *Sejam p um primo ímpar, n, k inteiros positivos tais que $n \mid 4k$ e $\delta \in \mathbb{F}_{p^n}$. Então, $(X^{p^k} - X + \delta)^{\frac{p^n-1}{2}+p^{2k}} + X^{p^k} + X$ é um polinômio de permutação sobre $\mathbb{F}_{p^n}$.*

Demonstração. Novamente, vamos mostrar que, para cada $b \in \mathbb{F}_{p^n}$,

$$(X^{p^k} - X + \delta)^{\frac{p^n-1}{2}+p^{2k}} + X^{p^k} + X = b \tag{4.2}$$

tem no máximo uma solução em $\mathbb{F}_{p^n}$. Suponha que exista uma solução x e temos os mesmos três possíveis casos.

Caso 1) $x^{p^k} - x + \delta = 0$: podemos concluir que $x^{p^k} = x - \delta$. A equação (4.2) nos diz que $x^{p^k} + x = b$, então obtemos $x = \frac{b+\delta}{2}$ e $b^{p^k} + \delta^{p^k} - b + \delta = 0$.

Caso 2) $x^{p^k}-x+\delta \in D_0$: nessa situação, (4.2) pode ser reescrita como $(x^{p^k}-x+\delta)^{p^{2k}}+x^{p^k}+x=b$, donde concluímos que

$$x^{p^{3k}} - x^{p^{2k}} + x^{p^k} + x = b - \delta^{p^{2k}}. \tag{4.3}$$

Defina $\mu = b - \delta^{p^{2k}}$. Uma vez que $n \mid 4k$, temos $x^{p^{4k}} = x$. Então, tomando a p^{ik}-ésima potência de ambos os lados de (4.3), com $i = 0, 1, 2, 3$, obtemos o sistema linear

$$\begin{pmatrix} 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x^{p^{3k}} \\ x^{p^{2k}} \\ x^{p^k} \\ x \end{pmatrix} = \begin{pmatrix} \mu \\ \mu^{p^k} \\ \mu^{p^{2k}} \\ \mu^{p^{3k}} \end{pmatrix}. \tag{4.4}$$

Para simplificar a notação, vamos denotar a matriz de coeficientes do sistema linear por A. Observe que A é uma matriz simétrica de Hadamard de ordem 4 e, portanto, é invertível e vale $A^{-1} = \frac{A}{4}$. Então, esse sistema é possível e determinado, ou seja, (4.4) tem apenas uma solução, bem como (4.3), uma vez que qualquer solução x para (4.3) nos fornece uma solução $(x^{p^{3k}}, x^{p^{2k}}, x^{p^k}, x)$ para (4.4).

Além disso, como $A^{-1} = \frac{A}{4}$, multiplicando A^{-1} à esquerda de ambos os lados de (4.4), encontramos $x = \dfrac{\mu + \mu^{p^k} - \mu^{p^{2k}} + \mu^{p^{3k}}}{4}$. Por fim, obtemos

$$x^{p^k} - x + \delta = \frac{\delta + \delta^{p^k} + b^{p^{2k}} - b^{p^{3k}}}{2}.$$

Caso 3) $x^{p^k} - x + \delta \in D_1$: nesse último caso, (4.2) pode ser reescrita como $-(x^{p^k} - x + \delta)^{p^{2k}} + x^{p^k} + x = b$, donde concluímos que $-x^{p^{3k}} + x^{p^{2k}} + x^{p^k} + x = b + \delta^{p^{2k}}$. Agora, denotando $\nu = b + \delta^{p^{2k}}$ e procedendo de maneira completamente análoga ao caso anterior, vemos que essa equação possui solução única $x = \dfrac{\nu - \nu^{p^k} + \nu^{p^{2k}} + \nu^{p^{3k}}}{4}$, bem como

$$x^{p^k} - x + \delta = \frac{\delta + \delta^{p^{3k}} + b^{p^k} - b^{p^{2k}}}{2}.$$

Resta provar que apenas um dos casos pode ocorrer. Agora, denotaremos

$$\Delta = \frac{\delta + \delta^{p^{3k}} + b^{p^k} - b^{p^{2k}}}{2}$$

e temos $\Delta^{p^k} = \dfrac{\delta + \delta^{p^k} + b^{p^{2k}} - b^{p^{3k}}}{2}$. Se o caso 1 não acontecer, analogamente ao Teorema 4.2, sabemos que um e apenas um dos casos 2 ou 3 acontece. Por outro lado, se 1 acontecer, a igualdade $x - x^{p^k} = \delta$ nos diz que

$$\delta + \delta^{p^k} + \delta^{p^{2k}} + \delta^{p^{3k}} = (x - x^{p^k}) + (x - x^{p^k})^{p^k} + (x - x^{p^k})^{p^{2k}} + (x - x^{p^k})^{p^{3k}} = 0.$$

Também sabemos que $b^{p^k} + \delta^{p^k} - b + \delta = 0$, então

$$\Delta^{p^k} = \frac{\delta + \delta^{p^k} + b^{p^{2k}} - b^{p^{3k}}}{2} = \frac{\delta + \delta^{p^k} + (b - b^{p^k})^{p^{2k}}}{2} = \frac{\delta + \delta^{p^k} + (\delta + \delta^{p^k})^{p^{2k}}}{2} = 0$$

e os casos 2 e 3 não podem acontecer. ■

A última condição proposta pelos autores com essa restrição de s é demonstrada de modo muito similar ao teorema anterior.

Teorema 4.8. *[14, Teorema 7] Sejam p um primo ímpar, n, k inteiros positivos tais que $n \mid 4k$ e $\delta \in \mathbb{F}_{p^n}$. Então, $(X^{p^k} - X + \delta)^{\frac{p^n-1}{2}+p^{2k}} - X^{p^k} - X$ é um polinômio de permutação sobre $\mathbb{F}_{p^n}$.*

4.1.2 Caso $s = \frac{p^n-1}{3} + p^r$

Agora, para um elemento primitivo $\alpha \in \mathbb{F}_{p^n}$, vamos definir $D_0 = \langle \alpha^3 \rangle$ e $D_i = \alpha^i D_0$, para $i = 1, 2$. Assim, $\mathbb{F}_{p^n} = \{0\} \cup D_0 \cup D_1 \cup D_2$. É interessante notar que, para quaisquer $\beta \in D_i$ e $\gamma \in D_j$, temos $\beta\gamma \in D_{i+j}$ e, se $\beta \in D_i$, então $\beta^{-1} \in D_{3-i}$ (os índices são tomado módulo 3). Além disso, denotando $\epsilon = \alpha^{\frac{p^n-1}{3}}$, temos $x^{\frac{p^n-1}{3}} = \alpha^{\frac{(p^n-1)i}{3}} = \epsilon^i$, para todo $x \in D_i$. Mais ainda, como $X^3 - 1 = (X-1)(X^2+X+1)$ e $\epsilon \neq 1$, temos $\epsilon^2 + \epsilon + 1 = 0$.

Com essa restrição de s, os autores forneceram duas condições para que polinômios da forma $(X^{p^k} - X + \delta)^s + L(X)$ sejam de permutação. Embora suas demonstrações sejam parecidas (inclusive parecidas com as provas dos casos anteriores), elas possuem algumas particularidades, e por isso serão apresentadas.

Teorema 4.9. *Sejam p um primo ímpar, n, k inteiros positivos tais que $n = 2k$ e $p^k \equiv 2$ (mod 3) e $\delta \in \mathbb{F}_{p^n}$ tal que $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^k}}(\delta) = 0$. Então, $(X^{p^k} - X + \delta)^{\frac{p^n-1}{3}+1} + X$ é um polinômio de permutação sobre $\mathbb{F}_{p^n}$ se $-\frac{1}{2} \in D_0$.*

Demonstração. Vamos mostrar que, para cada $b \in \mathbb{F}_{p^n}$,

$$(X^{p^k} - X + \delta)^{\frac{p^n-1}{3}+1} + X = b \tag{4.5}$$

tem no máximo uma solução em $\mathbb{F}_{p^n}$. Suponha que exista uma solução x.

Caso 1) $x^{p^k} - x + \delta = 0$: podemos concluir que $x = b$ e $b^{p^k} - b + \delta = 0$.

Caso 2) $x^{p^k} - x + \delta \in D_0$: nessa situação, (4.5) pode ser reescrita como $x^{p^k} - x + \delta + x = b$, ou seja, $x^{p^k} = b - \delta$. Como $\text{mdc}(p^k, p^n - 1) = 1$ e $n = 2k$, podemos concluir que $x = b^{p^k} - \delta^{p^k}$. Além disso,

$$x^{p^k} - x + \delta = b - \delta - b^{p^k} + \delta^{p^k} + \delta = b - b^{p^k} + \delta^{p^k} = b - b^{p^k} - \delta,$$

uma vez que $0 = \text{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^k}}(\delta) = \delta + \delta^{p^k}$.

Caso 3) $x^{p^k} - x + \delta \in D_1$: agora, vamos reescrever (4.5) sob a forma

$$\epsilon(x^{p^k} - x + \delta) + x = b. \tag{4.6}$$

Elevando ambos os lados à p^k-ésima potência, temos $\epsilon^{p^k}(x^{p^{2k}} - x^{p^k} + \delta^{p^k}) + x^{p^k} = b^{p^k}$ e, como, $p^k \equiv 2 \pmod 3$, $n = 2k$ e $\text{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^k}}(\delta) = 0$, segue

$$\epsilon^2(x - x^{p^k} - \delta) + x^{p^k} = b^{p^k}. \tag{4.7}$$

Multiplicando (4.6) por $(1 - \epsilon^2)$, (4.7) por $-\epsilon$, somando as duas e usando os fatos que $\epsilon^3 = 1$ e $\epsilon^2 + \epsilon + 1 = 0$, temos

$$x = \frac{b - b\epsilon^2 - b^{p^k}\epsilon - \delta\epsilon}{2}.$$

Com isso, $x^{p^k} - x + \delta = -\dfrac{b - b^{p^k} - \delta}{2}$.

Caso 4) $x^{p^k} - x + \delta \in D_2$: nesse último caso, (4.5) é reescrita como $\epsilon^2(x^{p^k} - x + \delta) + x = b$. Procedendo de forma análoga ao caso anterior, vamos obter $x = \dfrac{b - b\epsilon - b^{p^k}\epsilon^2 - \delta\epsilon^2}{2}$ e $x^{p^k} - x + \delta = -\dfrac{b - b^{p^k} - \delta}{2}$.

Denote $\Delta = b - b^{p^k} - \delta$. Observe que se o caso 1 acontecer, temos $\Delta = 0$ e nenhum outro pode ocorrer. Agora, se 1 não acontecer, uma vez que $-\frac{1}{2} \in D_0$, temos $\Delta, -\frac{\Delta}{2} \in D_i$, para algum $i = 0, 1, 2$, e exatamente um dos casos 2, 3 ou 4 pode ocorrer. ■

Teorema 4.10. *Sejam $p \neq 7$ um primo, n, k inteiros positivos tais que $n = 2k$ e $p^k \equiv 1 \pmod 3$ e $\delta \in \mathbb{F}_{p^n}$ tal que $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^k}}(\delta) = 0$. Suponha que $2\epsilon - 1 \in D_\lambda$ e $2\epsilon^2 - 1 \in D_\tau$, com $0 \leq \lambda, \tau \leq 2$. Então, $(X^{p^k} - X + \delta)^{\frac{p^n-1}{3}+1} + X$ é um polinômio de permutação sobre $\mathbb{F}_{p^n}$ se $\lambda - 1 \not\equiv \tau \pmod 3$.*

Demonstração. Queremos que, para cada $b \in \mathbb{F}_{p^n}$,

$$(X^{p^k} - X + \delta)^{\frac{p^n-1}{3}+1} + X = b \tag{4.8}$$

tenha no máximo uma solução em $\mathbb{F}_{p^n}$. Suponha que exista uma solução x. Os dois primeiros casos são exatamente iguais aos do teorema anterior.

Caso 1) $x^{p^k} - x + \delta = 0$: podemos concluir que $x = b$ e $b^{p^k} - b + \delta = 0$.

Caso 2) $x^{p^k} - x + \delta \in D_0$: podemos concluir que $x = b^{p^k} - \delta^{p^k}$ e $x^{p^k} - x + \delta = b - b^{p^k} - \delta$.

Caso 3) $x^{p^k} - x + \delta \in D_1$: agora, procedendo de modo similar ao que fizemos no teorema anterior, vamos obter as equações $\epsilon(x^{p^k} - x + \delta) + x = b$ e $\epsilon(x - x^{p^k} - \delta) + x^{p^k} = b^{p^k}$ (notemos que agora usamos $\epsilon^{p^k} = \epsilon$, já que nossa hipótese é $p^k \equiv 1 \pmod 3$). Multiplicando a primeira por $(1 - \epsilon)$, a segunda por $-\epsilon$ e somando, encontramos $(2\epsilon - 1)x = b\epsilon + b^{p^k}\epsilon + \delta\epsilon - b$. Se multiplicarmos a primeira por $-\epsilon$, a segunda por $(1 - \epsilon)$ e somarmos, encontraremos $(2\epsilon - 1)x^{p^k} = b\epsilon + b^{p^k}\epsilon - \delta\epsilon - b^{p^k}$. Uma vez que $\epsilon^3 = 1$ e $\epsilon^2 + \epsilon + 1 = 0$, temos $(2\epsilon - 1)(2\epsilon^2 - 1) = 7$. Já que $p \neq 7$, $(2\epsilon - 1)(2\epsilon^2 - 1) \neq 0$ e podemos escrever $x^{p^k} - x + \delta = \dfrac{b - b^{p^k} - \delta}{2\epsilon - 1}$.

Caso 4) $x^{p^k} - x + \delta \in D_2$: procedendo como no caso anterior, vamos obter $(2\epsilon^2 - 1)x = b\epsilon^2 + b^{p^k}\epsilon^2 + \delta\epsilon^2 - b$, $(2\epsilon^2 - 1)x^{p^k} = b\epsilon^2 + b^{p^k}\epsilon^2 - \delta\epsilon^2 - b^{p^k}$ e $x^{p^k} - x + \delta = \dfrac{b - b^{p^k} - \delta}{2\epsilon^2 - 1}$.

Definamos $\Delta = b - b^{p^k} - \delta$. Se o caso 1 acontecer, temos $\Delta = 0$ e nenhum dos outros pode ocorrer. Se o caso 1 não acontecer, temos três novas situações.

(*i*) Se $\Delta \in D_0$, isto é, se o caso 2 acontecer, precisamos ter $\dfrac{\Delta}{2\epsilon - 1} \notin D_1$ (ou seja, 3 não acontece) e $\dfrac{\Delta}{2\epsilon^2 - 1} \notin D_2$ (4 não acontece). Mas, como $2\epsilon - 1 \in D_\lambda$, $\frac{1}{2\epsilon-1} \in D_{3-\lambda}$ e devemos ter $\lambda \neq 2$. De modo análogo, devemos ter $\tau \neq 1$.

(*ii*) Se $\Delta \in D_1$, o caso 2 não pode acontecer e, para que apenas 3 ocorra, precisamos ter $\dfrac{\Delta}{2\epsilon - 1} \in D_1$ e $\dfrac{\Delta}{2\epsilon^2 - 1} \notin D_2$, ou seja, $\lambda = 0$ e $\tau \neq 2$. Para que apenas 4 aconteça, devemos ter $\dfrac{\Delta}{2\epsilon - 1} \notin D_1$ e $\dfrac{\Delta}{2\epsilon^2 - 1} \in D_2$, ou seja, $\lambda \neq 0$ e $\tau = 2$.

(*iii*) Se $\Delta \in D_2$, fazemos uma análise similar ao caso anterior e obtemos $\lambda = 1$ e $\tau \neq 0$ ou $\lambda \neq 1$ e $\tau = 0$.

■

Vamos finalizar essa seção aplicando nossa Proposição 3.22 juntamente com o Teorema 4.3. Observe que esse é o único caso em que podemos aplicar nosso resultado, uma vez que esse teorema é o único da forma $g(\alpha_0 X + \alpha_1 X^{q^{k_1}} + \cdots + \alpha_s X^{q^{k_s}} + \delta) + cX$ sem restrição de δ.

Teorema 4.11. *Sejam p um primo ímpar, n, k inteiros positivos tais que $n \mid 3k$ e $s = \frac{p^n-1}{2} + p^k$. Então, o polinômio $X^{sp^k} - X^s + X$ é de permutação sobre $\mathbb{F}_{p^n}$.*

4.2 Construindo q-polinômios de permutação

Dado um q-polinômio $L(X)$, é relativamente fácil determinar se ele é ou não de permutação: podemos calcular o núcleo da aplicação linear induzida por ele, por exemplo. Nessa seção, traremos os resultados de Cao e Hu ([7]). Nesse artigo, os autores apresentam métodos para construir q-polinômios que já serão de permutação.

A ideia é trabalhar com um polinômio da forma

$$L_b(X) = \alpha_0(b)X + \alpha_1(b)X^q + \cdots + \alpha_{n-1}(b)X^{q^{n-1}} \in \mathbb{F}_{q^n}[X],$$

em que $b \in \mathbb{F}_{q^n}$ e os $\alpha_i(X)$ são q-polinômios sobre $\mathbb{F}_q$. Para garantir que L_b seja uma permutação, os autores construíram dois processos: o primeiro consiste em tomar uma composição de L_b com outro q-polinômio, enquanto que o segundo consiste na diagonalização de uma matriz associada a L_b.

4.2.1 Método da composição

Para o primeiro método, nas notações acima, podemos escrever

$$\alpha_i(b) = \sum_{j=0}^{n-1} \alpha_{i,j} b^{q^j}$$

e considerar a matriz

$$A = \begin{pmatrix} \alpha_{0,0} & \alpha_{1,0} & \cdots & \alpha_{n-1,0} \\ \alpha_{0,1} & \alpha_{1,1} & \cdots & \alpha_{n-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{0,n-1} & \alpha_{1,n-1} & \cdots & \alpha_{n-1,n-1} \end{pmatrix}.$$

Então, $L_b(X)$ pode ser expresso na forma $L(b, X)$, com

$$L(Y, X) = (Y, Y^q, ..., Y^{q^{n-1}})A(X, X^q, ..., X^{q^{n-1}})^T := \tilde{Y}A\tilde{X}^T. \tag{4.9}$$

Agora, sejam $k = (k_0, k_1, ..., k_{n-1}) \in (\mathbb{F}_{q^n})^n$, $L_k(X) = \sum_{i=0}^{n-1} k_i X^{q^i}$ e

$$P = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Lema 4.12. *$L_k(X) \circ L_b(X) = \sum_{i=0}^{n-1} k_i L_b(X)^{q^i} = \tilde{b}B\tilde{X}^T$, em que*

$$B = k_0 A + k_1 PAP^T + \cdots + k_{n-1}P^{n-1}A(P^{n-1})^T. \tag{4.10}$$

Demonstração. A multiplicação XP, em que X é uma matriz de ordem n qualquer, é responsável por uma permutação cíclica nas colunas de X (em que a n-ésima coluna passa a ser a $n-1$-ésima e assim por diante), enquanto que a multiplicação P^TX é responsável por uma permutação cíclica em suas linhas (novamente, a n-ésima linha passa a ser a $n-1$-ésima). Desse modo, uma vez que podemos escrever $L_b(X) = \tilde{b}A\tilde{X}^T$, um simples cálculo nos mostra que

$$\tilde{b}PAP^T\tilde{X}^T = (\tilde{b}P)A(P^T\tilde{X}^T) = \tilde{b}^q A\tilde{X}^q = L_b(X)^q,$$

em que, por abuso de notação, $\tilde{b}^q = (b^q, b^{q^2}, ..., b)$. Procedendo indutivamente, podemos mostrar que

$$L_b(X)^{q^i} = \tilde{b}P^iA(P^i)^T\tilde{X}^T$$

e o lema está provado. ∎

Em particular, se tomarmos $u, v \in (\mathbb{F}_q)^n$, e considerarmos $B = u^T v$, B será uma matriz sobre $\mathbb{F}_q$ e teremos

$$L_k(X) \circ L_b(X) = \tilde{b} u^T v \tilde{X}^T = L_1(b) L_2(X),$$

em que $L_1(X) = \tilde{X} u^T$ e $L_2(X) = v\tilde{X}^T$. Se L_2 for de permutação, $L_1(b)L_2(X)$ será uma permutação sempre que $L_1(b) \neq 0$. Em particular, se tivermos $L_1(X)$ também uma permutação, $L_1(b)L_2(X)$ será uma permutação para todo $b \neq 0$. Assim, $L_k(X) \circ L_b(X)$ será injetora e, portanto, $L_b(X)$ também (donde concluímos que $L_b(X)$ será uma permutação para todo $b \neq 0$). Uma vez que A e B são matrizes com coeficientes em $\mathbb{F}_q$, também precisamos exigir $k \in (\mathbb{F}_q)^n$.

Precisamos apenas garantir que a equação (4.10) admita uma solução. Isso será feito no Teorema 4.14. Sua demonstração é um pouco extensa e envolve apenas contas diretas. Por isso, será omitida.

Na demonstração desse teorema, os autores usaram um resultado bastante conhecido para se estudar a bijetividade de um q-polinômio a partir do determinante de uma matriz ([15, p.362]). Usando o isomorfismo entre $\mathcal{L}_n(\mathbb{F}_{q^n})$ e $\mathcal{D}_n(\mathbb{F}_{q^n})$, podemos fornecer uma demonstração diferente da original.

Teorema 4.13. *Sejam $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ e $\alpha = (\alpha_0, ..., \alpha_{n-1}) \in (\mathbb{F}_{q^n})^n$. Considere o q-polinômio*

$$L(X) = \sum_{s=0}^{n-1} \alpha_s X^{q^s} \in \mathbb{F}_{q^n}[X].$$

L é um polinômio de permutação sobre $\mathbb{F}_{q^n}$ se, e somente se, o determinante da matriz

$$M_\alpha = \begin{pmatrix} \alpha_0 & \alpha_{n-1}^q & \alpha_{n-2}^{q^2} & \cdots & \alpha_1^{q^{n-1}} \\ \alpha_1 & \alpha_0^q & \alpha_{n-1}^{q^2} & \cdots & \alpha_2^{q^{n-1}} \\ \alpha_2 & \alpha_1^q & \alpha_0^{q^2} & \cdots & \alpha_3^{q^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_{n-2}^q & \alpha_{n-3}^{q^2} & \cdots & \alpha_0^{q^{n-1}} \end{pmatrix}$$

for diferente de zero.

Demonstração. Por definição, um q-polinômio L é uma permutação quando a aplicação linear por ele definida é uma bijeção. É um resultado conhecido de álgebra linear que uma transformação linear é bijetora se, e somente se, sua matriz de transformação linear tiver determinante não nulo. O resultado então segue do Teorema 2.11 e das observações de que M_α é a transposta da matriz D_L e o determinante de uma matriz e sua transposta coincidem. ■

Teorema 4.14. *[7, Proposição 2.3] Seja $k = (k_0, ..., k_{n-1}) \in (\mathbb{F}_q)^n$. Nas notações do teorema anterior, se M_k tiver determinante não nulo, então*

(i) Para toda matriz B, existe uma única matriz A tal que o sistema linear dado em (4.10) seja satisfeito.

(ii) Se B for uma matriz simétrica, a matriz A também será.

Em resumo, o primeiro método para se construir q-polinômios de permutação é o seguinte: escolhemos três vetores $u = (u_0, ..., u_{n-1}), v = (v_0, ..., v_{n-1}), k = (k_0, ..., k_{n-1}) \in (\mathbb{F}_q)^n$ tais que os determinantes de M_u, M_v, M_k sejam todos não nulos, depois, consideramos a matriz $B = u^T v$ e resolvemos o sistema linear dado em (4.10), cuja solução A é garantida pelo Teorema 4.14(i). O polinômio $L_b(X)$ definido em (4.9) é um q-polinômio de permutação.

No caso particular em que tomarmos $u = v$, a matriz $B = u^T u$ será simétrica, bem como a matriz A (Teorema 4.14(ii)). Na prática, isso diminui o número de incógnitas do sistema de n^2 para $\frac{n(n+1)}{2}$.

Exemplo 4.15. Considere os vetores em $\mathbb{F}_5$ $u = (1,0,0), v = (1,2,1)$ e $k = (2,0,1)$. Os determinantes de M_u, M_v, M_k são, respectivamente, $1, 4, 4$. A matriz $B = u^T v$ é

$$B = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Dessa forma, o sistema linear dado em (4.10) é

$$\begin{cases} 2a_{1,1} = 1 \\ 2a_{1,2} = 2 \\ 2a_{1,3} = 1 \end{cases} \quad \begin{cases} 2a_{2,1} = 0 \\ 2a_{2,2} = 0 \\ 2a_{2,3} = 0 \end{cases} \quad \begin{cases} 2a_{3,1} + 2 = 0 \\ 2a_{3,2} + 1 = 0 \\ 2a_{3,3} + 1 = 0 \end{cases}$$

Desse modo, concluímos que

$$A = \begin{pmatrix} 3 & 1 & 3 \\ 0 & 0 & 0 \\ 4 & 2 & 2 \end{pmatrix}$$

e

$$L_b(X) = (4b^{25} + 3b)X + (2b^{25} + b)X^5 + (2b^{25} + 3b)X^{25}$$

é um 5-polinômio de permutação sobre $\mathbb{F}_{5^3}$ para todo $b \neq 0$.

Exemplo 4.16. Agora, considere em $\mathbb{F}_9$ os vetores $u = (\alpha, 0, 1), k = (1, 0, 1)$, em que α é uma raiz do polinômio $X^2 + 1$. Os determinantes de M_u e M_k são $2\alpha + 1$ e 2 respectivamente. A matriz $B = u^T u$ é

$$B = \begin{pmatrix} \alpha^2 & 0 & \alpha \\ 0 & 0 & 0 \\ \alpha & 0 & 1 \end{pmatrix}.$$

Dessa forma, o sistema linear dado em 4.10 é

$$\begin{cases} a_{1,1} = \alpha^2 \\ a_{1,2} = 0 \\ a_{1,3} = \alpha \end{cases} \quad \begin{cases} a_{2,2} + 1 = 0 \\ a_{2,3} + \alpha = 0 \\ a_{3,3} + \alpha^2 = 1 \end{cases}$$

Desse modo, concluímos que

$$A = \begin{pmatrix} \alpha^2 & 0 & \alpha \\ 0 & 2 & 2\alpha \\ \alpha & 2\alpha & 2 \end{pmatrix}$$

e

$$L_b(X) = (\alpha b^{81} + 2b)X + (2\alpha b^{81} + 2b^9)X^9 + (2b^{81} + 2\alpha b^9 + \alpha b)X^{81}$$

é um 9-polinômio de permutação sobre $\mathbb{F}_{9^3}$ para todo $b \neq 0$.

4.2.2 Método da diagonalização

O segundo método para se construir q-polinômios de permutação baseia-se na diagonalização de matrizes. Em particular, a matriz A que será usada em (4.9) será simétrica.

Teorema 4.17. *Sejam A uma matriz quadrada de ordem n sobre $\mathbb{F}_{q^n}$, $b \in \mathbb{F}_{q^n}$ e $L_b(X) = \tilde{b}A\tilde{X}^T$. Se existir uma matriz U circulante e invertível sobre $\mathbb{F}_q$ tal que*

$$UAU^T = \begin{pmatrix} \lambda_0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix} =: D$$

e M_λ (nas notações do Teorema 4.13) tiver determinante não nulo, com $\lambda = (\lambda_0, ..., \lambda_{n-1}) \in (\mathbb{F}_q)^n$, então $L_b(X)$ será um q-polinômio de permutação sobre $\mathbb{F}_{q^n}$ para todo $b \neq 0$.

Demonstração. Primeiramente, fixamos uma base normal $\{\beta, \beta^q, ..., \beta^{q^{n-1}}\}$ para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Definimos

$$X = (X_0, X_1, ..., X_{n-1})(\beta, \beta^q, ..., \beta^{q^{n-1}})^T$$

e C_X a matriz circulante cuja primeira linha é $(X_0, X_1, ..., X_{n-1})$. Então,

$$(X, X^q, ..., X^{q^{n-1}})^T = C_X(\beta, \beta^q, ..., \beta^{q^{n-1}})^T.$$

De modo análogo, escrevemos

$$b = (b_0, b_1, ..., b_{n-1})(\beta, \beta^q, ..., \beta^{q^{n-1}})^T$$

e C_b será a matriz circulante cuja primeira linha é $(b_0, b_1, ..., b_{n-1})$. Então,

$$L_b(X) = (\beta, \beta^q, ..., \beta^{q^{n-1}})C_b^T A C_X(\beta, \beta^q, ..., \beta^{q^{n-1}})^T.$$

Se fizermos uma mudança de base de $\{\beta, \beta^q, ..., \beta^{q^{n-1}}\}$ para alguma outra base normal $\{\tau, \tau^q, ..., \tau^{q^{n-1}}\}$, é possível encontrar uma matriz invertível V tal que

$$(\beta, \beta^q, ..., \beta^{q^{n-1}}) = (\tau, \tau^q, ..., \tau^{q^{n-1}})V.$$

Como as duas bases são normais, V será também uma matriz circulante. Reciprocamente, qualquer matriz circulante invertível (em particular, a matriz U dada no enunciado) nos fornecerá uma mudança de bases normais, então podemos escrever

$$L_b(X) = (\tau, \tau^q, ..., \tau^{q^{n-1}})U C_b^T A C_X U^T (\tau, \tau^q, ..., \tau^{q^{n-1}})^T,$$

em que $\{\tau, \tau^q, ..., \tau^{q^{n-1}}\}$ é uma base normal para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Um cálculo simples nos mostra que quaisquer duas matrizes circulantes são comutativas. Então,

$$L_b(X) = (\tau, \tau^q, ..., \tau^{q^{n-1}})C_b^T U A U^T C_X(\tau, \tau^q, ..., \tau^{q^{n-1}})^T.$$

Como, por hipótese, UAU^T é a matriz diagonal D, fazemos uma "mudança de variáveis"

$$(X', X'^q, ..., X'^{q^{n-1}})^T = C_X(\tau, \tau^q, ..., \tau^{q^{n-1}})^T \text{ e } (b', b'^q, ..., b'^{q^{n-1}}) = (\tau, \tau^q, ..., \tau^{q^{n-1}})C_b^T.$$

Desse modo,

$$L_b(X) = \sum_{i=0}^{n-1} \lambda_i (b'X')^{q^i}.$$

Finalmente, pelo Teorema 4.13, esse q-polinômio é de permutação se, e somente se, M_λ tiver determinante não nulo. ■

Portanto, o segundo método consiste em escolher dois vetores $u = (u_0, ..., u_{n-1}), \lambda = (\lambda_0, ..., \lambda_{n-1}) \in (\mathbb{F}_q)^n$ tais que as matrizes M_u e M_λ tenham determinantes não nulos. Definimos U como sendo a matriz circulante cuja primeira linha é o vetor u, D a matriz diagonal formada pelas coordenadas de λ e $A = U^{-1}D(U^{-1})^T$. $L_b(X) = \tilde{b}A\tilde{X}^T$ é então um q-polinômio de permutação para todo $b \neq 0$.

Exemplo 4.18. Considere os vetores $u = (0, 1, 1), \lambda = (1, 2, \alpha) \in \mathbb{F}_{3^3}$, em que α é raiz de $X^3 + X^2 + 2$. Os determinantes de M_u e M_λ são 2 e α^3 respectivamente. Então, temos

$$A = \begin{pmatrix} \alpha & \alpha & 2\alpha+1 \\ \alpha & \alpha & 2\alpha+2 \\ 2\alpha+1 & 2\alpha+2 & \alpha \end{pmatrix}$$

e

$$L_b(X) = (b^9 + 2b^9\alpha + b^3\alpha + b\alpha)X + (2b^9 + 2b^9\alpha + b^3\alpha + b\alpha)X^3 + (2b^3 + b + b^9\alpha + 2b^3\alpha + 2b\alpha)X^9$$

é um 3-polinômio de permutação sobre $\mathbb{F}_{3^3}$ para todo $b \neq 0$.

Capítulo 5

Polinômios planares

Em meados da década de 70, o governo dos Estados Unidos adotou um método de criptografia conhecido como DES (*data encryption stantard*), um sistema de cifra em bloco, ou seja, recebe uma mensagem organizada em palavras de tamanho fixo e retorna uma mensagem criptografada com palavras de mesmo tamanho. O algoritmo do DES utiliza uma chave de 56 *bits* em 16 processos idênticos. Embora esses números possam parecer muito grandes, em janeiro de 1999 duas empresas se uniram e descriptografaram uma mensagem em 22 horas e 15 minutos.

Muitos estudos foram feitos na tentativa de tornar essa criptografia mais segura, mas também vários outros foram desenvolvidos na busca de quebrá-la mais facilmente. A mais eficiente (embora não seja tão viável na prática) é a Criptoanálise Diferencial, que necessita de 2^{47} palavras para encontrar a chave da criptografia DES. Em [18], prova-se que, sob certas condições, a chance de sucesso da criptoanálise é muito baixa, e em [19] prova-se que polinômios planares fornecem essas condições. Este capítulo dá destaque a essa importante classe polinomial definida sobre corpos finitos.

Uma função $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ é chamada planar quando $D_{f,\epsilon}(X) = f(X+\epsilon) - f(X)$ for uma permutação em $\mathbb{F}_{q^n}$ para todo $\epsilon \in \mathbb{F}_{q^n}^*$. É interessante ressaltar que essa definição nunca é satisfeita em corpos de característica 2, já que $D_{f,\epsilon}(x) = D_{f,\epsilon}(x+\epsilon)$. Nesses corpos, pedimos que a função $x \mapsto f(x+\epsilon) + f(x) + \epsilon x$ seja uma permutação para todo $\epsilon \in \mathbb{F}_{q^n}^*$.

Em [3], Bartoli e Bonini deram condições necessárias e suficientes para que um polinômio da forma $f_{A,B}(X) = X(X^{q^2} + AX^q + B) \in \mathbb{F}_{q^3}[X]$, $A, B \in \mathbb{F}_q$, q ímpar seja planar, enquanto que em [4], Bartoli e Timpanella trabalharam com a planaridade de $f_{A,B}(X) = X(AX^{q^2} + BX) \in \mathbb{F}_{2^{3m}}[X]$, $A, B \in \mathbb{F}_{2^{3m}}^*$. Usando resultados de q-polinômios, tentamos estender as contas e estudar quando um polinômio da forma $f_{A,B,C}(X) = X(X^{q^3} + AX^{q^2} + BX^q + C) \in \mathbb{F}_q[X]$ é planar sobre $\mathbb{F}_{q^4}$, mas, quando q é ímpar, só conseguimos resolver o caso em que $\mathbb{F}_q$ é um corpo que contenha uma raiz quadrada de -1.

Para simplificar a notação, vamos denotar $f_{A,B,C}(X)$ apenas por $f(X)$.

Trataremos esse problema primeiramente sobre um corpo de característica 2. Nessa situação, temos

$$D_{f,\epsilon}(X) = \epsilon X^{q^3} + A\epsilon X^{q^2} + B\epsilon X^q + (\epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q + \epsilon)X + (\epsilon^{q^3+1} + A\epsilon^{q^2+1} + B\epsilon^{q+1} + C\epsilon).$$

Note que $D_{f,\epsilon}$ é uma bijeção em $\mathbb{F}_{q^4}$ se, e somente se,

$$g_\epsilon(X) = \epsilon X^{q^3} + A\epsilon X^{q^2} + B\epsilon X^q + (\epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q + \epsilon)X$$

também o for (afinal $\epsilon^{q^3+1} + A\epsilon^{q^2+1} + B\epsilon^{q+1} + C\epsilon$ é uma constante em $\mathbb{F}_{q^4}$).

Usando o Teorema 4.13, g_ϵ é um polinômio de permutação se, e somente se, o determinante

da matriz

$$M_\epsilon = \begin{pmatrix} \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q + \epsilon & \epsilon & A\epsilon & B\epsilon \\ B\epsilon & \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q + \epsilon & \epsilon & A\epsilon \\ A\epsilon & B\epsilon & \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q + \epsilon & \epsilon \\ \epsilon & A\epsilon & B\epsilon & \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q + \epsilon \end{pmatrix}$$

for diferente de zero para todo $\epsilon \in \mathbb{F}_{q^4}^*$.

Com auxílio do programa CoCoA ([1]), obtemos

$$det(M_\epsilon) = (A^4 - B^4)\epsilon^4 + B^4\epsilon^{4q} + A^4\epsilon^{4q^2} + \epsilon^{4q^3} = ((A-B)\epsilon + B\epsilon^q + A\epsilon^{q^2} + \epsilon^{q^3})^4.$$

Isto é, para termos g_ϵ um polinômio de permutação, basta que o q-polinômio $(A-B)X + BX^q + AX^{q^2} + X^{q^3}$ tenha como única raiz o 0 (em particular, esse polinômio deve ser uma bijeção). Novamente pelo Teorema 4.13, isso é equivalente a termos

$$\begin{vmatrix} A-B & 1 & A & B \\ B & A-B & 1 & A \\ A & B & A-B & 1 \\ 1 & A & B & A-B \end{vmatrix} = -1$$

diferente de zero, o que de fato ocorre. Assim, concluímos que $f_{A,B,C}(X) = X(X^{q^3} + AX^{q^2} + BX^q + C)$, com $A, B, C \in \mathbb{F}_q$ e q par, é um polinômio planar sobre $\mathbb{F}_{q^4}$.

Agora, podemos tratar esse problema em corpos de característica ímpar. Nesse caso, temos

$$D_{f,\epsilon}(X) = \epsilon X^{q^3} + A\epsilon X^{q^2} + B\epsilon X^q + (\epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q)X + (\epsilon^{q^3+1} + A\epsilon^{q^2+1} + B\epsilon^{q+1} + C\epsilon).$$

Novamente, podemos "ignorar"o termo independente e $D_{f,\epsilon}(X)$ é bijeção se, e somente se,

$$g_\epsilon(X) = \epsilon X^{q^3} + A\epsilon X^{q^2} + B\epsilon X^q + (\epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q)X$$

for também de permutação. Observe que g_ϵ é novamente um q-polinômio.

Pelo Teorema 4.13, g_ϵ é um polinômio de permutação se, e somente se, o determinante da matriz

$$M_\epsilon = \begin{pmatrix} \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q & \epsilon & A\epsilon & B\epsilon \\ B\epsilon & \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q & \epsilon & A\epsilon \\ A\epsilon & B\epsilon & \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q & \epsilon \\ \epsilon & A\epsilon & B\epsilon & \epsilon^{q^3} + A\epsilon^{q^2} + B\epsilon^q \end{pmatrix}$$

for diferente de zero.

Novamente usando o programa CoCoA, temos

$$\begin{aligned} det(M_\epsilon) = \; & (A^2\epsilon^2 - 2A^2\epsilon^{q^2+1} + A^2\epsilon^{2q^2} - 2AB\epsilon^{q+1} + 2AB\epsilon^{q^2+q} + B^2\epsilon^2 + B^2\epsilon^{2q} - 2A\epsilon^{q^3+1} \\ & + 2A\epsilon^{q^3+q^2} - 2B\epsilon^2 + 2B\epsilon^{q^3+q} + \epsilon^2 + \epsilon^{2q^3}) \cdot (A\epsilon + A\epsilon^{q^2} + B\epsilon + B\epsilon^q + \epsilon + \epsilon^{q^3}) \cdot \\ & (A\epsilon + A\epsilon^{q^2} - B\epsilon + B\epsilon^q - \epsilon + \epsilon^{q^3}). \end{aligned}$$

Reparemos que $det(M_\epsilon)$ é nulo se, e somente se, pelo menos um de seus fatores for zero. Vamos, então, tratar cada um deles separadamente, começando pelos dois últimos.

Podemos pensar que o segundo fator é $h(\epsilon)$, em que $h(X)$ é o q-polinômio

$$h(X) = X^{q^3} + AX^{q^2} + BX^q + (A + B + 1)X.$$

Como queremos $h(\epsilon) \neq 0$ para todo $\epsilon \in \mathbb{F}_{q^4}^*$, queremos que o polinômio h tenha exatamente uma raiz (afinal $x = 0$ é sempre raiz de um q-polinômio). Usando o Teorema 4.1, saberemos que o polinômio $h(X)$ é uma bijeção. Pelo Teorema 4.13, isso é equivalente a termos

$$\begin{vmatrix} A+B+1 & 1 & A & B \\ B & A+B+1 & 1 & A \\ A & B & A+B+1 & 1 \\ 1 & A & B & A+B+1 \end{vmatrix} = 8A[B^3 + (A+1)B^2 + B + (A+1)] \neq 0.$$

Já que estamos em um corpo de característica ímpar, podemos simplificar nossa expressão e teremos $h(X)$ uma bijeção se, e somente se,

$$A(B^2+1)(A+B+1) \neq 0.$$

Procedendo de forma completamente análoga com o terceiro fator, veremos que $A\epsilon + A\epsilon^{q^2} - B\epsilon + B\epsilon^q - \epsilon + \epsilon^{q^3} \neq 0$ para todo $\epsilon \in \mathbb{F}_{q^4}$ se, somente se,

$$A(B^2+1)(A-B-1) \neq 0.$$

Agora, vamos trabalhar com o primeiro fator. Podemos pensar que ele se anula em ϵ se ϵ for raiz do polinômio

$$\begin{aligned} \tilde{h}(X) \; &= (A^2+B^2-2B+1)X^2 - 2ABX^{q+1} - 2A^2X^{q^2+1} - 2AX^{q^3+1} + 2BX^{q^3+q} \\ &\quad + B^2X^{2q} + 2ABX^{q^2+q} + A^2X^{2q^2} + 2AX^{q^3+q^2} + X^{2q^3} \end{aligned}.$$

Infelizmente esse não é um q-polinômio, e não poderemos aplicar o Teorema 4.13. Para contornar essa situação, vamos chamar $X^q = Y$, $X^{q^2} = Z$ e $X^{q^3} = T$. Assim, $\tilde{h}(X)$ tem uma raiz não nula se, e somente se, o polinômio

$$\begin{aligned} h(X,Y,Z,T) = \; &(A^2+B^2-2B+1)X^2 - 2ABXY - 2A^2XZ - 2AXT + B^2Y^2 \\ &+2ABYZ + 2BYT + A^2Z^2 + 2AZT + T^2 \end{aligned}$$

tiver uma raiz da forma $(x, x^q, x^{q^2}, x^{q^3}), x \in \mathbb{F}_{q^4}^*$. Vamos estudar a redutibilidade de h, isto é, vamos tentar escrever

$$h(X,Y,Z,T) = (a_1X + a_2Y + a_3Z + a_4T + a_5)(b_1X + b_2Y + b_3Z + b_4T + b_5).$$

Notemos que h é uma **forma quadrática**, isto é, um polinômio tal que o grau de todos os seus monômios é 2, então usaremos o procedimento descrito em [15, Seção 6.2].

Observemos inicialmente que

$$h(X,Y,Z,T) = (X,Y,Z,T) \underbrace{\begin{pmatrix} A^2+B^2-2B+1 & -AB & -A^2 & -A \\ -AB & B^2 & AB & B \\ -A^2 & AB & A^2 & A \\ -A & B & A & 1 \end{pmatrix}}_{M_1} \underbrace{\begin{pmatrix} X \\ Y \\ Z \\ T \end{pmatrix}}_{u}$$

e, denotando

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ A & -B & -A & 1 \end{pmatrix},$$

vale

$$M_2^T M_1 M_2 = \underbrace{\begin{pmatrix} (B-1)^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{M_3}.$$

Assim, fazendo a mudança de variáveis

$$v = \begin{pmatrix} \tilde{X} \\ \tilde{Y} \\ \tilde{Z} \\ \tilde{T} \end{pmatrix} = (M_2)^{-1}u = (M_2)^{-1}\begin{pmatrix} X \\ Y \\ Z \\ T \end{pmatrix} = \begin{pmatrix} X \\ Y \\ Z \\ -AX + BY + AZ + T \end{pmatrix},$$

temos $u^T M_1 u = h(X, Y, Z, T) = 0$ se, e somente se, $v^T M_3 v = (B-1)^2\tilde{X}^2 + \tilde{T}^2 = 0$, afinal

$$v^T M_3 v = ((M_2)^{-1}u)^T (M_2^T M_1 M_2)((M_2)^{-1}u) = u^T (M_2^T)^{-1} M_2^T M_1 M_2 M_2^{-1} u = u^T M_1 u.$$

Como vale $(B-1)^2\tilde{X}^2 + \tilde{T}^2 = 0$, se o corpo $\mathbb{F}_q$ não contiver uma raiz quadrada de -1, o polinômio $(B-1)^2\tilde{X}^2 + \tilde{T}^2$ (bem como $h(X, Y, Z, T)$) será irredutível em $\mathbb{F}_q[X, Y, Z, T]$ e não conseguimos prosseguir com nossa análise. Por outro lado, se $\mathbb{F}_q$ contiver tal raiz, que denotaremos por ξ, obtemos

$$\pm\xi(B-1)\tilde{X} = \tilde{T} \Longrightarrow \pm\xi(B-1)X = (-AX + BY + AZ + T),$$

isto é, em $\mathbb{F}_{q^4}[X, Y, Z, T]$, podemos escrever

$$h(X, Y, Z, T) = ((-A + \xi(B-1))X + BY + AZ + T)((-A - \xi(B-1))X + BY + AZ + T),$$

o que é equivalente a

$$\tilde{h}(X) = ((-A + \xi(B-1))X + BX^q + AX^{q^2} + X^{q^3})((-A - \xi(B-1))X + BX^q + AX^{q^2} + X^{q^3}).$$

Repare que cada fator de $\tilde{h}$ é novamente um q-polinômio, e mais uma vez precisamos que cada fator seja bijetor para que f seja planar. Aplicando o Teorema 4.13, concluímos que $\tilde{h}(\epsilon) \neq 0$ para todo $\epsilon \neq 0$ se, e somente se,

$$A(B^2 + 1)(A \pm \xi(B-1)) \neq 0.$$

Com isso, temos provado o seguinte teorema.

Teorema 5.1. *Sejam q uma potência de um primo ímpar e $\mathbb{F}_q$ um corpo que contenha uma raiz quadrada de -1, denotada por ξ. Então, $f_{A,B,C}(X) = X(X^{q^3} + AX^{q^2} + BX^q + C) \in \mathbb{F}_{q^4}[X]$ é um polinômio planar sobre $\mathbb{F}_{q^4}$ se, e somente se,*

$$A(B^2 + 1)(A + B + 1)(A - B - 1)(A \pm \xi(B-1)) \neq 0.$$

Referências Bibliográficas

[1] ABBOTT, J., BIGATTI, A. M., ROBBIANO, L. CoCoA: a system for doing Computations in Commutative Algebra. Disponível em http://cocoa.dima.unige.it.

[2] AKBARY, A.; GHIOCA, D.; WANG, Q. On constructing permutations of finite fields. Finite Fields and Their Applications, v. 17, n. 1, p. 51-67, 2011. https://doi.org/10.1016/j.ffa.2010.10.002.

[3] BARTOLI, D.; BONINI, M. Planar Polynomials arising from linearized polynomials. Journal of Algebra and Its Applications (versão online), 2020. https://doi.org/10.1142/S0219498822500025.

[4] BARTOLI, D.; TIMPANELLA, M. A family of planar binomials in characteristic 2. Finite Fields and Their Applications, v. 63, 2020. https://doi.org/10.1016/j.ffa.2020.101651.

[5] BIRKHOFF, G; MACLANE, S. Algebra Moderna. 12ª ed. Teide, 1954. ISBN 9788431612269.

[6] CALLIOLI, C.A.; DOMINGUES, H.H.; COSTA, R.C.F. Álgebra linear e aplicações: 6ª ed. Atual, 1982. ISBN 9788570562975.

[7] CAO, X.; HU, L. New methods for generating permutation polynomials over finite fields. Finite Fields and Their Applications, v. 17, n. 6, p. 493-503, 2011. https://doi.org/10.1016/j.ffa.2011.02.012.

[8] FRALEIGH, J.B. A first course in abstract algebra. Pearson Education India, 2003. ISBN 9780201763904.

[9] HELLESETH, T.; ZINOVIEV V. New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m. Finite Fields and Their Applications, v. 9, p. 187-193, 2003. https://doi.org/10.1016/s1071-5797(02)00028-x.

[10] JACOBSON, N. Lectures in abstract algebra: I. Basic concepts. Springer-Verlag, 1951. ISBN 9781468473018.

[11] KYUREGHYAN, G.; ZIEVE, M. Permutation polynomials of the form X+ γTr(X^k). Contemporary developments in finite fields and applications, p. 178-194, 2016. https://doi.org/10.1142/9789814719261_0011.

[12] LANG, S. Álgebra para graduação: 2ª ed. Ciência Moderna, 2008. ISBN 9788573937466.

[13] LI, K.; QU, L.; ZHOU, Y. A link between two classes of permutation polynomials. Finite Fields and Their Applications, v. 63, 2020. https://doi.org/10.1016/j.ffa.2020.101641.

[14] LI, N.; HELLESETH T.; TANG X. Further results on a class of permutation polynomials over finite fields. Finite Fields and Their Applications, v. 22, p. 16-23, 2013. https://doi.org/10.1016/j.ffa.2013.02.004.

[15] LIDL, R.; NIEDERREITER, H. Finite Fields. Cambridge University Press, 1997. ISBN 9780521392310

[16] MEYER, C. D. Matrix analysis and applied linear algebra. Siam, 2000. ISBN 9780898714548.

[17] MORGADO, A. C. D. O. et al. Análise combinatória e probabilidade. Instituto de Matemática Pura e Aplicada, 1991. ISBN 9788583370833.

[18] NYBERG, K; KNUDSEN, L. R. Provable security against differential cryptanalysis. Annual International Cryptology Conference. Springer, Berlin, Heidelberg, p. 566-574, 1992. https://doi.org/10.1007/3-540-48071-4_41.

[19] NYBERG, K. Differentially uniform mappings for cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, p. 55-64, 1993. https://doi.org/10.1007/3-540-48285-7_6.

[20] WU, B.; LIU, Z. Linearized polynomials over finite fields revisited. Finite Fields and Their Applications, v. 22, p. 79-100, 2013. https://doi.org/10.1016/j.ffa.2013.03.003.

[21] ZHENG, D.; YUAN, M.; YU, L. Two types of permutation polynomials with special forms. Finite Fields and Their Applications, v. 56, p. 1-16, 2019. https://doi.org/10.1016/j.ffa.2018.10.008.

[22] ZHOU, K. A remark on linear permutation polynomials. Finite Fields and Their Applications, v. 14, p. 532–536, 2008. https://doi.org/10.1016/j.ffa.2007.07.002.

[23] ZIEVE, M. E. Some families of permutation polynomials over finite fields. International Journal of Number Theory, v. 4, n. 05, p. 851-857, 2008. https://doi.org/10.1142/s1793042108001717.