UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
RENAN CARVALHO DE SOUZA

CONSTRUÇÃO DE SEQUÊNCIAS DE POLINÔMIOS AUTORRECÍPROCOS IRREDUTÍVEIS SOBRE CORPOS FINITOS VIA TRANSFORMAÇÕES QUADRÁTICAS

RIO DE JANEIRO
2022

Construção de sequências de polinômios autorrecíprocos irredutíveis sobre corpos finitos via transformações quadráticas

por

Renan Carvalho de Souza

IM-UFRJ

Dissertação de Mestrado apresentada ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Luciane Quoos Conte

Rio de Janeiro

2022

CIP - Catalogação na Publicação

Souza, Renan Carvalho de
SS729c Construção de sequências de polinômios autorrecíprocos irredutíveis sobre corpos finitos via transformações quadráticas / Renan Carvalho de Souza. -- Rio de Janeiro, 2022.
66 f.

Orientadora: Luciane Quoos Conte.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-Graduação em Matemática, 2022.

1. Álgebra. 2. Corpos finitos. I. Conte, Luciane Quoos, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

Construção de sequências de polinômios autorrecíprocos irredutíveis sobre corpos finitos via transformações quadráticas

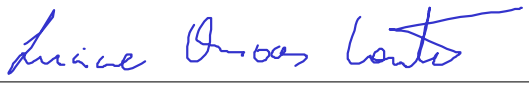
por

Renan Carvalho de Souza

Dissertação submetida ao Corpo Docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do grau de Mestre em Matemática.

Área de concentração: Matemática

Aprovada por:



Profa. Dra. Luciane Quoos Conte - IM-UFRJ
(Orientadora)

Prof. Dr. Luca Scala - IM-UFRJ

Prof. Dr. Fabio Enrique Brochero Martinez - UFMG

Profa. Dra. Lays Grazielle Cardoso Silva de Jesus - UFRR

Rio de Janeiro

Janeiro de 2022

Resumo

Dado um corpo finito $\mathbb{F}_q$ com q elementos, estudamos as propriedades de polinômios autorrecíprocos e de duas transformações quadráticas $Q, R : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$ definidas por $f^Q(x) = x^{\deg(f)} f(x + 1/x)$ e $f^R(x) = (2x)^{\deg(f)} f(2^{-1}(x + 1/x))$, introduzidas por Meyn em 1990 e Cohen em 1992, respectivamente. Estas transformações levam polinômios de grau n sobre $\mathbb{F}_q$ em polinômios autorrecíprocos de grau $2n$. Apresentamos dois métodos para construir sequências de polinômios autorrecíprocos irredutíveis. No primeiro caso, aplicamos a Q-transformação sucessivas vezes a um polinômio irredutível sobre um corpo finito de característica par, e no segundo caso aplicamos a R-transformação sucessivas vezes a um polinômio irredutível sobre um corpo finito de característica ímpar, sendo que, em ambos os casos, supomos algumas hipóteses sobre o polinômio inicial. Posteriormente, baseados nos trabalhos de Ugolini em 2015 e 2016, mostramos como construir sequências de polinômios autorrecíprocos irredutíveis usando as mesmas transformações sobre corpos finitos supondo apenas que o polinômio inicial f é irredutível.

Abstract

Given a finite field $\mathbb{F}_q$ with q elements, we study the properties of self-reciprocal polynomials and two quadratic transformations $Q, R : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$ defined by $f^Q(x) = x^{\deg(f)} f(x + 1/x)$ and $f^R(x) = (2x)^{\deg(f)} f(2^{-1}(x + 1/x))$, introduced by Meyn in 1990 and Cohen in 1992, respectively. These transformations take n degree polynomials over $\mathbb{F}_q$ to $2n$ degree self-reciprocal polynomials. We present two methods to construct sequences of irreducible self-reciprocal polynomials. In the first case, we apply the Q-transformation successive times on an irreducible polynomial over a finite field of even characteristic, and in the second case we apply the R-transformation successive times on an irreducible polynomial over a finite field of odd characteristic, but in both cases, we suppose some hypotheses on the first polynomial. After, based on the works of Ugolini in 2015 and 2016, we show how to construct sequences of irreducible self-reciprocal polynomials using the same transformations over finite fields supposing only that the first polynomial f is irreducible.

Agradecimentos

Agradeço a Deus por me permitir viver e escrever este trabalho.

Agradeço aos meus pais, que sempre me apoiaram e me incentivaram em minhas escolhas.

Agradeço a todos os professores que tive, pois sem eles teria sido muito mais difícil (talvez até impossível) aprender grande parte do que eu sei hoje. Em especial, agradeço à minha orientadora por ter me guiado durante a feitura deste trabalho e por nossos encontros, que sempre foram muito produtivos.

Agradeço a todos os amigos que contribuíram com ideias, sugestões e incentivos.

Agradeço a CAPES e a FAPERJ, que me apoiaram financeiramente durante o meu Mestrado.

Sumário

Introdução

O estudo de polinômios irredutíveis sobre corpos finitos é fundamental para a construção de extensões finitas de corpos finitos e para a determinação de uma aritmética nestas extensões. O conhecimento da aritmética de corpos finitos, por sua vez, é importante em diversos tópicos relacionados a criptografia que têm sido estudados nas últimas décadas (veja, por exemplo, [4], [13], [26]).

Além do interesse intríseco no estudo de polinômios autorrecíprocos sobre corpos finitos, estes também possuem aplicações em teoria de códigos (ver [6] e [25]) e em combinatória (ver [14]). Uma forma de construir polinômios autorrecíprocos irredutíveis de grau arbitrariamente grande pode ser realizado via sequência de polinômios autorrecíprocos irredutíveis. Neste trabalho, apresentamos a construção de duas sequências de polinômios autorrecíprocos irredutíveis definidas pela aplicação de transformações quadráticas sucessivas vezes a um polinômio irredutível inicial sobre $\mathbb{F}_q$ de modo que, após cada transformação, o grau do polinômio aumente e ele se mantenha irredutível sobre o corpo de base $\mathbb{F}_q$. Mais especificamente, sobre um corpo de característica par, utilizamos a transformação

$$Q : f(x) \mapsto f^Q(x) = x^{\deg(f)} f(x + 1/x)$$

e, sobre um corpo de característica ímpar, a transformação

$$R : f(x) \mapsto f^R(x) = (2x)^{\deg(f)} f(2^{-1}(x + 1/x)).$$

Em 1969, Varshamov e Garakov [23] provaram que, sobre o corpo com dois elementos, a transformação quadrática Q preserva a irredutibilidade se, e somente se, os coeficientes do termos de grau 0 e 1 do polinômio original forem 1. Esse resultado foi generalizado para corpos finitos de característica par em 1990, por Meyn [12]. Neste mesmo artigo, Meyn

determinou condições sobre os coeficientes de um polinômio irredutível em característica par de modo que, após cada aplicação da Q-transformação, o polinômio permanecesse irredutível. Em 1992, Cohen [8] provou um resultado semelhante para corpos finitos de característica ímpar, desta vez utilizando a transformação quadrática R.

Posteriormente, sequências de polinômios irredutíveis, não necessariamente autorrecíprocos, definidas por outros tipos de transformações foram descobertas: Chu em 1996 [7] através de transformações cúbicas, Kyuregyan em 2003 [9] e em 2006 [10] através de transformações quadráticas, entre outros. Veja, por exemplo, as citações nos artigos [7], [9] e [10].

Em 2015, Ugolini [21] desenvolveu um método, usando a R-transformação, para criar uma sequência de polinômios irredutíveis sobre um corpo de característica ímpar a partir de um polinômio irredutível qualquer. Todos os termos desta sequência são polinômios autorrecíprocos, exceto um número finito de termos iniciais. Em 2016, o mesmo autor [22] utilizou um método para construir uma sequência de polinômios irredutíveis sobre um corpo finito de característica par a partir da (Q, α)-transformação definida por

$$f^{(Q,\alpha)}(x) = x^n f(x + \alpha/x),$$

onde $\alpha \neq 0$ é um elemento do corpo base e f possui grau n, a partir de um polinômio irredutível qualquer. O caso particular $\alpha = 1$ gera uma sequência onde todos os termos são polinômios autorrecíprocos, exceto um número finito de termos iniciais.

Esta dissertação se baseia na teoria desenvolvida nos artigos Meyn [12], Cohen [8], Ugolini [21] e Ugolini [22].

No primeiro capítulo, apresentamos resultados básicos sobre corpos finitos e fazemos uma breve introdução à teoria de grafos. No segundo capítulo estudamos algumas propriedades de polinômios mônicos autorrecíprocos irredutíveis sobre corpos finitos, tais como a quantidade de polinômios mônicos autorrecíprocos irredutíveis de grau fixado, bem como

o produto de todos os polinômios deste tipo de mesmo grau. Definimos a Q-transformação e a R-transformação e, por fim, construímos as sequências de polinômios autorrecíprocos irredutíveis desenvolvidas por Meyn e Cohen. No terceiro capítulo, definimos a (Q, α)-transformação de polinômios sobre um corpo finito de característica par e definimos um grafo associado a essa transformação. Por fim, construímos a sequência de polinômios irredutíveis sobre este corpo desenvolvida por Ugolini. No quarto capítulo, apresentamos algumas propriedades da R-transformação em polinômios sobre um corpo de característica ímpar e definimos um grafo associado a essa transformação. Por fim, construímos a sequência de polinômios irredutíveis sobre este corpo desenvolvida por Ugolini.

Capítulo 1

Preliminares

Neste capítulo, apresentamos algumas definições e resultados básicos sobre corpos finitos e grafos que serão úteis ao longo dos próximos capítulos.

Na primeira seção, caracterizamos a estrutura de corpos finitos, definimos polinômios irredutíveis e apresentamos uma propriedade do conjunto de raízes de um polinômio irredutível. A segunda seção é dedicada ao estudo de propriedades das funções traço e norma. Na terceira seção, definimos a função de Möbius e calculamos o número de polinômios mônicos irredutíveis de cada grau sobre $\mathbb{F}_q$. Na quarta seção, determinamos todos os polinômios f de grau 2 que são irredutíveis sobre $\mathbb{F}_q$ a partir do número de soluções em $\mathbb{F}_q$ da equação $f(x) = 0$. Na última seção, introduzimos alguns conceitos relacionados à teoria de grafos.

As demonstrações de todos os resultados apresentados nas quatro primeiras seções podem ser encontrados em [11] e [15]. A última seção é baseada em [5].

1.1 Corpos finitos

Dado um anel R, definimos a característica de R como sendo o menor inteiro $n > 0$ tal que $nr = 0$ para todo $r \in R$. Caso não exista um inteiro $n > 0$ satisfazendo esta propriedade, dizemos que R possui característica 0.

Se F é um corpo finito e 1 é o elemento neutro multiplicativo de F, então existem inteiros $m > k$ tais que $m \cdot 1 = k \cdot 1$, ou seja, $(m-k) \cdot 1 = 0$, logo $(m-k) \cdot r = r \cdot (m-k) \cdot 1 = 0$ para todo $r \in R$, portanto a característica de F é positiva. Se $n > 0$ é a característica de F, então n deve ser um primo. Caso contrário, se $n = st$, onde $1 < s, t < n$, então $0 = n \cdot 1 = (s \cdot 1)(t \cdot 1)$, logo $s \cdot 1 = 0$ ou $t \cdot 1 = 0$, portanto $sr = 0$ para todo $r \in R$ ou $tr = 0$ para todo $r \in R$, contrariando o fato de n ser a característica de R.

Seja p um primo. Denotamos por $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ o corpo finito contendo p elementos. Se F é um corpo finito de característica p, então F é uma extensão de $\mathbb{F}_p$ e, consequentemente, um espaço vetorial de dimensão finita sobre $\mathbb{F}_p$. Se $n = [F : \mathbb{F}_p]$, então F possui uma base $\{a_1, ..., a_n\}$ sobre $\mathbb{F}_p$. Desta forma, todo elemento $a \in F$ pode ser escrito da forma $a = b_1a_1 + ... + b_na_n$, onde $b_1, ..., b_n \in \mathbb{F}_p$. Como $\mathbb{F}_p$ possui p elementos, segue que F possui p^n elementos.

Por outro lado, dados p primo e $n \geq 1$ inteiro, pode-se provar que as p^n raízes distintas de $x^{p^n} - x \in \mathbb{F}_p[x]$ no fecho algébrico de $\mathbb{F}_p$ formam de fato um corpo F, e que todo corpo com p^n elementos é isomorfo a F. Assim, dado $q = p^n$, denotamos por $\mathbb{F}_q$ o único (a menos de isomorfismo) corpo com q elementos.

Por definição, todos os elementos de $\mathbb{F}_q$ satisfazem $\alpha^q = \alpha$, enquanto todos os elementos do grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ satisfazem $\alpha^{q-1} = 1$. O resultado a seguir caracteriza a estrutura do grupo $\mathbb{F}_q^*$.

Teorema 1.1.1. ([11], Teorema 2.8) *Seja $\mathbb{F}_q$ um corpo finito. Então o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

Se α é um gerador do grupo $\mathbb{F}_q^*$, então α é dito um elemento primitivo de $\mathbb{F}_q$.

Vimos acima que se $q = p^n$, p primo, então $\mathbb{F}_p$ é um subcorpo de $\mathbb{F}_q$. O teorema a seguir determina todos os subcorpos de $\mathbb{F}_q$.

Teorema 1.1.2. ([11], Teorema 2.6) *Seja $\mathbb{F}_q$ o corpo com $q = p^n$ elementos. Todo subcorpo de $\mathbb{F}_q$ é da forma $\mathbb{F}_{p^m}$, onde $m \geq 1$ divide n. Reciprocamente, para todo $m \geq 1$ tal que $m \mid n$, $\mathbb{F}_{p^m}$ é um subcorpo de $\mathbb{F}_q$.*

A seguir, definimos polinômios irredutíveis sobre corpos finitos e determinamos todas as raízes de um polinômio irredutível a partir de uma raiz qualquer.

Definição 1.1.3. Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau $n \geq 1$. Se $f(x) = g(x)h(x)$, $g, h \in \mathbb{F}_q[x]$, implica que g ou h é constante, então f é dito irredutível sobre $\mathbb{F}_q$.

Teorema 1.1.4. ([11], Teorema 2.14) *Seja f um polinômio irredutível de grau n sobre $\mathbb{F}_q$. Então f possui uma raiz α em $\mathbb{F}_{q^n}$ e todas as n raízes distintas de f são dadas por $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}} \in \mathbb{F}_{q^n}$.*

Se $\alpha \in \mathbb{F}_{q^n}$ e f é um polinômio mônico irredutível de grau d sobre $\mathbb{F}_q$ tal que $f(\alpha) = 0$, dizemos que f é o polinômio mínimo de α sobre $\mathbb{F}_q$. Pelo Teorema 1.1.4, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$ e, como $\alpha \in \mathbb{F}_{q^n}$, segue que $\mathbb{F}_{q^d}$ é um subcorpo de $\mathbb{F}_{q^n}$. Pelo Teorema 1.1.2, temos $d \mid n$. Se $g \in \mathbb{F}_q[x]$ é outro polinômio satisfazendo $g(\alpha) = 0$, então $f(x) \mid g(x)$.

Dado um polinômio f mônico irredutível de grau n sobre $\mathbb{F}_q$, dizemos que f é um polinômio primitivo sobre $\mathbb{F}_q$ se f é o polinômio mínimo de um elemento primitivo de $\mathbb{F}_{q^n}$. Se f é um polinômio primitivo de grau n sobre $\mathbb{F}_q$, pode-se verificar que todas as raízes de f são elementos primitivos de $\mathbb{F}_{q^n}$.

1.2 Traços e normas

Nesta seção, definimos as funções traço e norma sobre corpos finitos e enunciamos algumas propriedades destas funções.

Definição 1.2.1. Para cada $\alpha \in \mathbb{F}_{q^n}$, definimos o traço $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ de α sobre $\mathbb{F}_q$ e a norma $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ de α sobre $\mathbb{F}_q$ por

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

Se f possui grau d e é o polinômio mínimo de $\alpha \in \mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, então as raízes de f são dadas por $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$, e $\alpha^{q^{kd}} = \alpha$ para todo inteiro $k \geq 0$. Logo, as raízes do polinômio $g(x) = f(x)^{n/d}$ são $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}}$. Seja

$$g(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{n-1}}) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{F}_q[x].$$

Então

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -a_{n-1} \quad \text{e} \quad \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = (-1)^n a_0.$$

Em particular, se $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, temos $g(x) = f(x)$. Observamos também que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ e $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ são elementos de $\mathbb{F}_q$, visto que $g \in \mathbb{F}_q[x]$.

As proposições a seguir apresentam outras propriedades básicas de $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ e $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Proposição 1.2.2. ([11], Teorema 2.33) *Sejam $\alpha, \beta \in \mathbb{F}_{q^n}$ e $c \in \mathbb{F}_q$. A função $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ possui as seguintes propriedades:*

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

(ii) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = c\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

(iii) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *é uma função sobrejetiva.*

(iv) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c) = nc$.

(v) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

Proposição 1.2.3. ([11], Teorema 2.28) *Sejam $\alpha, \beta \in \mathbb{F}_{q^n}$ e $c \in \mathbb{F}_q$. A função $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ possui as seguintes propriedades:*

(i) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha\beta) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$.

(ii) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *é uma função sobrejetiva e* $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ *se, e somente se,* $\alpha = 0$.

(iii) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c) = c^n$.

(v) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

Proposição 1.2.4. ([11], Teorema 2.26 e Teorema 2.29) *Sejam K, F, L corpos finitos tais que $K \subseteq F \subseteq L$ e $\alpha \in L$. Então*

(i) $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\alpha))$ *(Transitividade do Traço)*

(ii) $\mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{F/K}(\mathrm{N}_{L/F}(\alpha))$ *(Transitividade da Norma)*

1.3 Polinômios irredutíveis e a função de Möbius

A seguir, apresentamos a definição da função de Möbius e uma propriedade desta função.

Definição 1.3.1. Definimos a função de Möbius como sendo a função $\mu : \mathbb{N}^* \to \mathbb{Z}$ tal que

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1, \\ (-1)^k, & \text{se } n \text{ é o produto de } k \text{ primos distintos}, \\ 0, & \text{se } n \text{ é múltiplo do quadrado de um primo.} \end{cases}$$

Lema 1.3.2. ([11], Teorema 3.23) *Para todo $n \in \mathbb{N}^*$, a função de Möbius satisfaz*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{se } n = 1, \\ 0, & \textit{se } n > 1 \end{cases}$$

O resultado enunciado a seguir também é conhecido como a fórmula de inversão de Möbius.

Teorema 1.3.3. ([11], Teorema 3.24)

(i) Sejam G um grupo aditivo abeliano e duas funções $h, H : \mathbb{N}^* \to G$. Então

$$H(n) = \sum_{d|n} h(d)$$

para todo $n \in \mathbb{N}^*$ se, e somente se,

$$h(n) = \sum_{d|n} \mu(n/d)H(d) = \sum_{d|n} \mu(d)H(n/d)$$

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

(ii) Sejam G um grupo multiplicativo abeliano e duas funções $h, H : \mathbb{N}^* \to G$. Então

$$H(n) = \prod_{d|n} h(d)$$

para todo $n \in \mathbb{N}^*$ se, e somente se,

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H(n/d)^{\mu(d)}$$

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

Com o auxílio da função de Möbius e da fórmula de inversão de Möbius, podemos calcular o produto $I_{q,n}$ de todos os polinômios mônicos irredutíveis de grau $n \geq 1$ sobre $\mathbb{F}_q$ e o número $N_q(n)$ de polinômios mônicos irredutíveis de grau $n \geq 1$ sobre $\mathbb{F}_q$.

Teorema 1.3.4. ([11], Teorema 3.25 e Teorema 3.29) *Para todo $n \geq 1$, o polinômio $I_{q,n}$ e o número $N_q(n)$ são dados por*

$$I_{q,n}(x) = \prod_{d|n} (x^{q^d} - x)^{\mu(n/d)} = \prod_{d|n} (x^{q^{n/d}} - x)^{\mu(d)}$$

e

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Utilizando o resultado do Teorema 1.3.4 e o fato de que $\mu(1) = 1$ e $\mu(d) \geq -1$ para todo $d > 1$, concluímos que

$$N_q(n) \geq \frac{1}{n} \left(q^n - \sum_{\substack{d|n \\ d>1}} q^{n/d} \right) \geq \frac{1}{n} \left(q^n - q^{n-1} - ... - q^2 - q \right) = \frac{1}{n} \left(q^n - \frac{q^n - q}{q-1} \right) > 0.$$

Portanto, para todo q e todo $n \geq 1$, existe um polinômio irredutível de grau n sobre $\mathbb{F}_q$.

1.4 Irredutibilidade de polinômios de grau 2

Nesta seção, calculamos o número de soluções de equações quadráticas sobre $\mathbb{F}_q$. Como um polinômio de grau 2 é irredutível sobre $\mathbb{F}_q$ se, e somente se, não possui raízes em $\mathbb{F}_q$, então os resultados a seguir caracterizam os polinômios irredutíveis de grau 2 sobre corpos finitos.

Proposição 1.4.1. *Sejam q ímpar e $f(x) = ax^2 + bx + c \in \mathbb{F}_q[x]$ um polinômio de grau 2. Então a equação $f(x) = 0$*

(i) possui exatamente uma solução em $\mathbb{F}_q$ se $b^2 - 4ac = 0$.

(ii) possui duas soluções distintas em $\mathbb{F}_q$ se $b^2 - 4ac$ é um quadrado em $\mathbb{F}_q^*$.

(iii) não possui soluções em $\mathbb{F}_q$ se $b^2 - 4ac$ não é um quadrado em $\mathbb{F}_q^*$.

Demonstração. Por hipótese, $2a \neq 0$. Seja

$$g(x) = f\left(x - \frac{b}{2a}\right) = ax^2 - \frac{b^2}{4a} + c.$$

Pela definição de g, o número de soluções de $g(x) = 0$ sobre $\mathbb{F}_q$ é o mesmo de $f(x) = 0$ sobre $\mathbb{F}_q$. Como $g(x) = 0$ é equivalente a

$$x^2 = \frac{1}{4a^2}\left(b^2 - 4ac\right)$$

e $4a^2$ é um quadrado em $\mathbb{F}_q$, então $g(x) = 0$ possui pelo menos 1 solução em $\mathbb{F}_q$ se, e somente se, $b^2 - 4ac$ é um quadrado em $\mathbb{F}_q$. Se $b^2 - 4ac = 0$, então a única solução de $g(x) = 0$ é $x = 0$. Se $b^2 - 4ac \in \mathbb{F}_q^*$ é um quadrado e $\alpha \in \mathbb{F}_q^*$ satisfaz $g(\alpha) = 0$, então $-\alpha \neq \alpha$ e $g(-\alpha) = g(\alpha) = 0$. □

Proposição 1.4.2. *Sejam $m \geq 1$ e $f(x) = ax^2 + bx + c \in \mathbb{F}_{2^m}[x]$ um polinômio de grau 2. Então a equação $f(x) = 0$*

(i) possui exatamente uma solução em $\mathbb{F}_{2^m}$ *se* $b = 0$.

(ii) possui duas soluções distintas em $\mathbb{F}_{2^m}$ *se* $b \neq 0$ *e* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(ac/b^2) = 0$.

(iii) não possui soluções em $\mathbb{F}_{2^m}$ *se* $b \neq 0$ *e* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(ac/b^2) = 1$.

Demonstração. Suponha $b = 0$. Então $f(x) = 0$ é equivalente a $x^2 = c/a$. Como

$$c/a = (c/a)^{2^m} = \left((c/a)^{2^{m-1}}\right)^2,$$

temos

$$0 = x^2 + \left((c/a)^{2^{m-1}}\right)^2 = \left(x + (c/a)^{2^{m-1}}\right)^2,$$

o que implica que $f(x) = 0$ possui uma única solução em $\mathbb{F}_{2^m}$.

Suponha $b \neq 0$. Sejam $d = ac/b^2$ e $g(x) = x^2 + x + d$. Então

$$g\left(\frac{a}{b}x\right) = \left(\frac{a}{b}x\right)^2 + \frac{a}{b}x + \frac{ac}{b^2} = \frac{a}{b^2}f(x),$$

o que implica que o número de soluções de $g(x) = 0$ sobre $\mathbb{F}_{2^m}$ é o mesmo de $f(x) = 0$ sobre $\mathbb{F}_{2^m}$. A seguir, mostramos que existe um elemento $\alpha \in \mathbb{F}_{2^m}$ satisfazendo $g(\alpha) = 0$ se, e somente se, $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(d) = 0$. Se $g(\alpha) = 0$ onde $\alpha \in \mathbb{F}_{2^m}$, então

$$\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(d) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\alpha^2) + \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\alpha) = 0.$$

Por outro lado, se $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(d) = 0$ e $\alpha \in \mathbb{F}_{2^{2m}}$ satisfaz $g(\alpha) = 0$, então

$$\begin{aligned} 0 = &\ \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(d) = d + d^2 + d^4 + ... + d^{2^{m-1}} \\ = &\ (\alpha^2 + \alpha) + (\alpha^4 + \alpha^2) + ... + (\alpha^{2^m} + \alpha^{2^{m-1}}) \\ = &\ \alpha + \alpha^{2^m}, \end{aligned}$$

o que implica $\alpha = \alpha^{2^m}$, ou seja, $\alpha \in \mathbb{F}_{2^m}$. Por fim, observamos que se $\alpha \in \mathbb{F}_{2^m}$ é uma raiz de g, então $\alpha + 1$ também é, visto que

$$g(\alpha + 1) = (\alpha + 1)^2 + (\alpha + 1) + d = \alpha^2 + \alpha + d = g(\alpha) = 0.$$

□

1.5 Grafos

Nesta seção, definimos alguns conceitos relacionados a grafos que serão utilizados nos capítulos 3 e 4. Ao leitor interessado em se aprofundar no estudo sobre teoria de grafos, recomendamos o livro [5].

Definimos um *grafo direcionado* (finito) G como sendo um par (V, E), onde V é um conjunto finito de objetos denominados *vértices* e E é um conjunto de pares ordenados de vértices denominados *arestas direcionadas*. Dizemos que dois vértices v_1, v_2 são *adjacentes* se (v_1, v_2) ou (v_2, v_1) é uma aresta direcionada de G. Ao descrever um grafo G por meio de um diagrama, geralmente representamos cada vértice por um ponto ou um círculo e cada aresta direcionada $e = (v_1, v_2)$ por uma seta ligando v_1 a v_2.

Dado um grafo direcionado G, definimos o *grafo invertido* de G como sendo o grafo G' tal que G e G' possuem o mesmo conjunto de vértices V, e cada aresta direcionada de G' é da forma $e' = (v_2, v_1)$, onde $e = (v_1, v_2)$ é uma aresta direcionada de G.

Dizemos que dois grafos direcionados $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ são *isomorfos* se existe uma bijeção $\psi : V_1 \to V_2$ tal que $(u, v) \in E_1$ se, e somente se, $(\psi(u), \psi(v)) \in E_2$. Se G_1 e G_2 são isomorfos, então $\#V_1 = \#V_2$, $\#E_1 = \#E_2$ e, para cada $v \in V_1$, temos

$$\#\{x \in V_1 \mid (v, x) \in E_1\} = \#\{x \in V_2 \mid (\psi(v), x) \in E_2\}$$

e

$$\#\{x \in V_1 \mid (x, v) \in E_1\} = \#\{x \in V_2 \mid (x, \psi(v)) \in E_2\}.$$

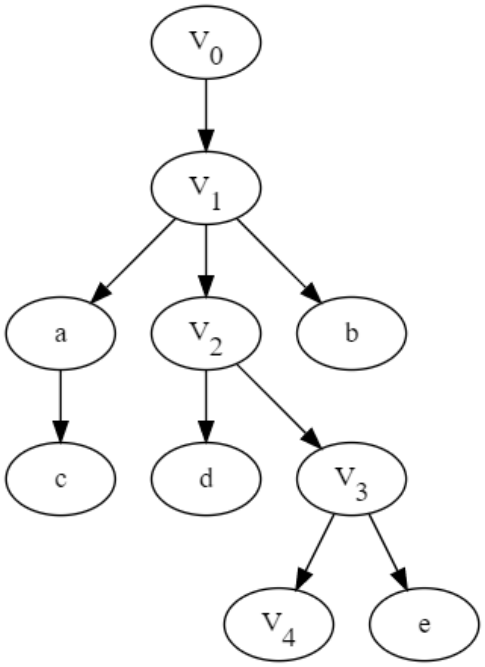
Se $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ são grafos direcionados tais que $V_2 \subseteq V_1$ e $E_2 \subseteq E_1$, dizemos que G_2 é um *subgrafo* de G_1. Se $G_1 \neq G_2$ e G_2 é um subgrafo de G_1, dizemos que G_2 é um *subgrafo próprio* de G_1.

Um grafo $G = (V, E)$ é dito *conexo* se, para todos $v_0, v \in V$ tais que $v_0 \neq v$, existem $v_1, ..., v_n \in V$ tais que v_i e v_{i+1} são adjacentes para todo $0 \leq i \leq n-1$, e v_n e v são adjacentes. Se H é um subgrafo conexo de G tal que H não é um subgrafo próprio de nenhum subgrafo conexo de G, dizemos que H é uma *componente conexa* de G.

Sejam $V = \{v_1, ..., v_n\}$, $n \geq 2$, o conjunto de vértices de um grafo direcionado G. Dizemos que G é um *ciclo de comprimento* n se o seu conjunto de arestas direcionadas é dado por $E = \{(v_1, v_2), (v_2, v_3), ..., (v_{n-1}, v_n), (v_n, v_1)\}$. Se um grafo G possui um subgrafo que é um ciclo, dizemos que G contém um ciclo.

Se $G = (V, E)$ é um grafo direcionado conexo, dizemos que G é uma *árvore* se G não contém ciclos e, para cada $v \in V$, $(u, v) \in E$ e $(w, v) \in E$ implica $u = w$. Seja $G = (V, E)$ uma árvore e $v_0 \in V$ tal que $(v, v_0) \notin E$ para todo $v \in V$. Então dizemos que v_0 é a *raiz* de G e que G é uma *árvore enraizada* em v_0. Se $v_1, ..., v_n \in V$ são tais que $(v_i, v_{i+1}) \in E$ para todo $0 \leq i \leq n-1$, dizemos que v_{i+1} é um *filho* de v_i e que cada v_i pertence ao *nível* i de G. Se v_n não possui filhos, v_n é dito uma *folha* de G. Por fim, definimos a *altura* de G como sendo o maior nível de um vértice de G.

Exemplo 1.5.1. O grafo direcionado $G = (V, E)$ representado a seguir é uma árvore enraizada em v_0.



Neste grafo, v_0 possui apenas v_1 como filho, enquanto v_1 possui três filhos v_2, a, b; v_2 possui dois filhos v_3, d; v_3 possui dois filhos v_4, e; a possui apenas c como filho. Assim, as folhas de G são v_4, b, c, d, e. O vértice v_0 pertence ao nível 0, o vértice v_1 pertence ao nível 1, os filhos de v_1 pertencem ao nível 2, os filhos de v_2 e de a pertencem ao nível 3, e os filhos de v_3 pertencem ao nível 4. Desta forma, G possui altura 4.

Capítulo 2

Construção de polinômios autorrecíprocos irredutíveis sobre corpos finitos

Neste capítulo, demonstramos algumas propriedades de polinômios mônicos irredutíveis autorrecíprocos (abreviados por *miar*) definidos sobre corpos finitos, calculamos o produto de todos os polinômios *miar* de grau $2n$ sobre $\mathbb{F}_q$ e, consequentemente, a quantidade desses polinômios. Introduzimos a Q-transformação e a R-transformação de um polinômio e determinamos condições necessárias e suficientes nos coeficientes de um polinômio f para que os polinômios f^Q e f^R sejam irredutíveis. Ao final do capítulo, apresentamos dois métodos − um em característica par e um em característica ímpar − para construir uma sequência $f_0, f_1, f_2, ...$ de polinômios *miar* (exceto, possivelmente, f_0) sobre um corpo finito, onde $\deg(f_i) = 2\deg(f_{i-1})$, considerando algumas condições sobre f_0.

A teoria abordada neste capítulo se baseia nos trabalhos de Meyn [12] e Cohen [8].

2.1 Polinômios *miar* sobre $\mathbb{F}_q$

Iniciamos esta seção definindo polinômios recíprocos e autorrecíprocos.

Definição 2.1.1. Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ um polinômio de grau n sobre $\mathbb{F}_q$. Definimos por

$$f^*(x) = x^n f(1/x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n$$

o polinômio recíproco de f. Um polinômio é dito autorrecíproco se coincide com o seu recíproco.

Uma consequência imediata da Definição 2.1.1 é que se 0 é uma raiz de f então f^* possui grau menor que o de f e, portanto, f não é autorrecíproco.

Proposição 2.1.2. *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau n.*

(i) Se $g \in \mathbb{F}_q[x]$, então $(fg)^* = f^*g^*$.

(ii) Se f é autorrecíproco, então o conjunto de raízes de f é fechado pela aplicação inversão $\alpha \mapsto 1/\alpha$.

(iii) Se f é autorrecíproco e $f(-1) \neq 0$, então n é par.

(iv) Se f é mônico, irredutível e o conjunto de raízes de f é fechado pela inversão, então

$$f^*(x) = \begin{cases} -f(x), & \text{se } f(x) = x - 1 \text{ e } q \neq 2^s, \\ f(x), & \text{caso contrário.} \end{cases}$$

Demonstração. (i) Seja m o grau de g. Então fg possui grau $n + m$ e

$$(fg)^*(x) = x^{n+m} f(1/x)g(1/x) = x^n f(1/x) \cdot x^m g(1/x) = f^*(x)g^*(x).$$

(ii) Como $f(x) = x^n f(1/x)$, dado α em alguma extensão de $\mathbb{F}_q$ tal que $f(\alpha) = 0$ temos $\alpha^n f(1/\alpha) = 0$, o que implica que $1/\alpha$ é raiz de f.

(iii) Suponha que $f(x) = a_0x^n + a_1x^{n-1} + ... + a_1x + a_0$ é um polinômio autorrecíproco e $n = 2k + 1$ é ímpar. Podemos escrever

$$f(x) = \sum_{i=0}^{k} a_i(x^{n-i} + x^i).$$

Então

$$f(-1) = \sum_{i=0}^{k} a_i((-1)^{n-i} + (-1)^i) = 0.$$

(iv) Se $f(x) = x - 1$ e $q \neq 2^s$, então $f^*(x) = -x + 1 = -f(x)$. Se $f(x) = x - 1$ e $q = 2^s$, então $f^*(x) = -x + 1 = x + 1 = f(x)$. Suponha $n > 1$ e sejam $\alpha, \alpha^q, ..., \alpha^{q^{n-1}} \in \mathbb{F}_{q^n}$ as raízes distintas de f. Por hipótese, $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\} = \{1/\alpha, 1/\alpha^q, ..., 1/\alpha^{q^{n-1}}\}$, logo f e f^* possuem as mesmas raízes, portanto $f(x) = \gamma f^*(x)$, onde $\gamma \in \mathbb{F}_q$. Como 1 e -1 não são raízes de f e o conjunto de raízes de f é fechado pela inversão, então n é par e o produto das raízes de f é 1, logo f^* é mônico e $\gamma = 1$.

□

Como consequência da Proposição 2.1.2 (iii), concluímos que todos os polinômios *miar* sobre $\mathbb{F}_q$ possuem grau par, exceto o polinômio $x + 1$.

Teorema 2.1.3. *(i) Todo polinômio* miar *de grau* $2n$*,* $n \geq 1$*, sobre* $\mathbb{F}_q$ *é um fator do polinômio*

$$H_{q,n}(x) = x^{q^n+1} - 1.$$

(ii) Todo fator mônico irredutível de grau maior que 1 *do polinômio* $H_{q,n}$ *é um polinômio* miar *de grau* $2d$*, onde* $d \mid n$ *e* n/d *é ímpar.*

(iii) Se $d \mid n$ *e* n/d *é ímpar, então* $H_{q,d} \mid H_{q,n}$*.*

Demonstração. (i) Se $f \in \mathbb{F}_q[x]$ é um polinômio miar de grau $2n$, $n \geq 1$, então as suas raízes podem ser descritas como $\alpha, \alpha^q, ..., \alpha^{q^{2n-1}}$, onde $\alpha \in \mathbb{F}_{q^{2n}} \backslash \mathbb{F}_{q^k}$ para todo $k < 2n$. Pela Proposição 2.1.2 (ii), o conjunto das raízes de f é fechado pela inversão, logo existe $1 \leq j \leq 2n - 1$ tal que $\alpha^{q^j} = \alpha^{-1}$. Portanto, α é uma raiz de $H_{q,j}(x) = x^{q^j+1} - 1$. Como $q^{2j} - 1 = (q^j + 1)(q^j - 1)$, concluímos que $H_{q,j}(x) \mid x^{q^{2j}-1} - 1$, o que nos dá $\alpha = \alpha^{q^{2j}}$. Portanto $2n \mid 2j$. Isso significa que $j = n$, logo α é uma raiz de $H_{q,n}$.

(ii) Seja g um fator mônico irredutível de grau $k > 1$ de $H_{q,n}$. As raízes de g são $\{\alpha, \alpha^q, ..., \alpha^{q^{k-1}}\}$, onde $\alpha^{q^k} = \alpha$. Se $n = sk + i$, onde $0 \leq i < k$, então $\alpha^{q^n} = \alpha^{(q^k)^s \cdot q^i} = (\alpha^{(q^k)^s})^{q^i} = \alpha^{q^i}$ é uma raiz de g. Como α é uma raiz de $H_{q,n}$, temos que $\alpha^{q^n} = \alpha^{-1}$.

Assim, o conjunto das raízes de g é fechado pela inversão e, pela Proposição 2.1.2 (iii) e (iv), g é autorrecíproco de grau par $k = 2d$. Pelo enunciado do item (i), g divide $H_{q,d}$ e, pelo mesmo argumento utilizado na demonstração do item (i), temos que $d \mid n$, ou seja, $n = \ell d$ para algum inteiro ℓ. Suponha que $\ell = 2r$ é par. Como α é uma raiz de g, então $g \mid H_{q,d}$ implica $\alpha^{q^d} = \alpha^{-1}$ e $\alpha^{q^{2d}} = \alpha$. Logo $\alpha^{q^n} = \alpha^{q^{\ell d}} = \alpha^{(q^{2d})^r} = \alpha$, o que contradiz o fato de α ser uma raiz de $H_{q,n}$. Portanto, concluímos que $\ell = n/d$ deve ser ímpar.

(iii) Sejam $\alpha \in \mathbb{F}_{q^{2d}}$ uma raiz de $H_{q,d}$ e $n = \ell d$, onde ℓ é um inteiro ímpar. Então $\alpha^{q^d} = \alpha^{-1}$ implica $\alpha^{q^n} = \alpha^{(q^d)^\ell} = \alpha^{-1}$. Portanto, α é uma raiz de $H_{q,n}$.

□

Definimos o polinômio $R_{q,n}$ como sendo o produto de todos os polinômios *miar* de grau $2n$, $n \geq 1$, sobre $\mathbb{F}_q$. Como toda raiz α do polinômio $H_{q,n}$ satisfaz $\alpha^{q^n} = \alpha^{-1}$ então, se $\alpha \in \mathbb{F}_q$, devemos ter $\alpha = \alpha^{-1}$, ou seja, $\alpha \in \{1, -1\}$. Portanto, pelo Teorema 2.1.3,

$$H_{q,n}(x) = (x^{1+e_q} - 1) \prod_{\substack{d \mid n \\ n/d \text{ ímpar}}} R_{q,d}(x),$$

onde $e_q = 0$ se q for par e $e_q = 1$ se q for ímpar.

O próximo lema nos dá uma fórmula explícita para o cálculo de $R_{q,n}$.

Lema 2.1.4. *Para todo $n \geq 1$, o polinômio $R_{q,n}$ é dado por*

$$R_{q,n}(x) = \begin{cases} \dfrac{H_{q,n}(x)}{x^{1+e_q} - 1}, & \text{se } n = 2^s \text{ para algum } s \geq 0, \\ \displaystyle\prod_{\substack{d \mid n \\ d \text{ ímpar}}} H_{q,n/d}(x)^{\mu(d)}, & \text{se } n \neq 2^s \text{ para todo } s \geq 0. \end{cases}$$

Demonstração. Sejam $n = 2^s r$, onde r é ímpar e

$$H^0_{q,n}(x) = \frac{H_{q,n}(x)}{x^{1+e_q}-1} = \prod_{\substack{d|n \\ n/d \text{ ímpar}}} R_{q,d}(x).$$

Pela fórmula de inversão de Möbius, temos

$$R_{q,n}(x) = \prod_{\substack{d|n \\ d \text{ ímpar}}} H^0_{q,n/d}(x)^{\mu(d)} = \prod_{d|r} H^0_{q,n/d}(x)^{\mu(d)} = \left(\prod_{d|r} H_{q,n/d}(x)^{\mu(d)}\right)\left(\prod_{d|r}(x^{1+e_q}-1)^{-\mu(d)}\right).$$

Como $\sum_{d|r}\mu(d) = 0$ para todo $r > 1$ e $x^{1+e_q}-1$ não depende de d, concluímos que

$$R_{q,n}(x) = \prod_{d|r} H_{q,n/d}(x)^{\mu(d)} = \prod_{\substack{d|n \\ d \text{ ímpar}}} H_{q,n/d}(x)^{\mu(d)}$$

se $n \neq 2^s$. Se $n = 2^s$, então o único fator ímpar de n é 1, logo

$$R_{q,n}(x) = \prod_{\substack{d|n \\ d \text{ ímpar}}} H^0_{q,n/d}(x)^{\mu(d)} = H^0_{q,n}(x) = \frac{H_{q,n}(x)}{x^{1+e_q}-1}.$$

□

Exemplo 2.1.5. O produto de todos os polinômios *miar* de grau 4 sobre $\mathbb{F}_4$ é dado por

$$R_{4,2}(x) = \frac{x^{17}+1}{x+1}.$$

Os 4 fatores irredutíveis de $R_{4,2}(x)$ são exatamente os 4 polinômios *miar* de grau 4 sobre $\mathbb{F}_4$: $x^4+\omega x^3+x^2+\omega x+1$, $x^4+\omega^2 x^3+x^2+\omega^2 x+1$, $x^4+x^3+\omega x^2+x+1$, $x^4+x^3+\omega^2 x^2+x+1$, onde ω satisfaz $\omega = \omega^2+1$.

Uma aplicação do Lema 2.1.4 é o teorema a seguir, que determina o número exato de

polinômios *miar* de grau $2n$ sobre um corpo finito.

Teorema 2.1.6. *Seja $S_q(n)$ o número de polinômios* miar *de grau $2n$ sobre $\mathbb{F}_q$. Então*

$$S_q(n) = \begin{cases} \dfrac{1}{2n}(q^n - 1) & \text{se } q \text{ é ímpar e } n = 2^s \text{ para algum } s \geq 0, \\ \dfrac{1}{2n} \displaystyle\sum_{\substack{d|n \\ d \text{ ímpar}}} \mu(d) q^{n/d} & \text{caso contrário.} \end{cases}$$

Demonstração. Se q é ímpar e $n = 2^s$, então

$$R_{q,n}(x) = \frac{x^{q^n+1} - 1}{x^2 - 1}.$$

Como $R_{q,n}$ possui grau $q^n - 1$, então existem $(q^n - 1)/2n$ polinômios *miar* de grau $2n$ sobre $\mathbb{F}_q$.

Se q é par e $n = 2^s$, então

$$R_{q,n}(x) = \frac{x^{q^n+1} - 1}{x - 1}.$$

Como $R_{q,n}$ possui grau q^n, então o número de polinômios *miar* de grau $2n$ sobre $\mathbb{F}_q$ é dado por

$$\frac{1}{2n} q^n = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ ímpar}}} \mu(d) q^{n/d}.$$

Se $n \neq 2^s$, então

$$\deg(R_{q,n}) = \sum_{\substack{d|n \\ d \text{ ímpar}}} \mu(d) \deg(H_{q,n/d}) = \sum_{\substack{d|n \\ d \text{ ímpar}}} \mu(d)(q^{n/d} + 1) = \sum_{\substack{d|n \\ d \text{ ímpar}}} \mu(d) q^{n/d}.$$

Desta forma, existem

$$\frac{1}{2n}\sum_{\substack{d|n \\ d \text{ ímpar}}} \mu(d)q^{n/d}$$

polinômios *miar* de grau $2n$ sobre $\mathbb{F}_q$. □

Observação 2.1.7. No Teorema 1.3.4, é calculado o número $N_q(n)$ de polinômios mônicos irredutíveis de grau n sobre $\mathbb{F}_q$. A partir do Teorema 2.1.6, podemos calcular o número $N_q(2n) - S_q(n)$ de polinômios mônicos irredutíveis de grau $2n$ sobre $\mathbb{F}_q$ que não são autorrecíprocos.

Exemplo 2.1.8. O número de polinômios mônicos irredutíveis de grau 30 sobre $\mathbb{F}_q$ autorrecíprocos e não autorrecíprocos são dados, respectivamente, por

$$S_q(n) = \frac{1}{30}(q^{15} - q^5 - q^3 + q)$$

e

$$N_q(2n) - S_q(n) = \frac{1}{30}(q^{30} - 2q^{15} - q^{10} - q^6 + 2q^5 + 2q^3 + q^2 - 2q).$$

2.2 O polinômio f^Q

Nesta seção, estudamos uma transformação quadrática que associa um polinômio de grau n a um polinômio autorrecíproco de grau $2n$.

Definição 2.2.1. Se $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{F}_q[x]$ é um polinômio de grau n, definimos a Q-transformação de f por

$$f^Q(x) = x^n f(x + 1/x) = \sum_{i=0}^{n} a_i(1 + x^2)^i x^{n-i}.$$

A proposição a seguir, que apresenta uma propriedade importante da Q-transformação, pode ser encontrada em [1].

Proposição 2.2.2. *Se g é um polinômio autorrecíproco de grau $2n$ sobre $\mathbb{F}_q$, então existe um único polinômio $f \in \mathbb{F}_q[x]$ de grau n tal que $g = f^Q$.*

Demonstração. Seja $g(x) = a_0x^{2n} + ... + a_{n-1}x^{n+1} + a_nx^n + a_{n-1}x^{n-1} + ... + a_0$. Então

$$g(x) = a_nx^n + \sum_{i=0}^{n-1} a_i(x^{2n-i} + x^i) = x^n \left(a_n + \sum_{j=1}^{n} a_{n-j}(x^j + 1/x^j) \right).$$

Definimos $g_0(x) = 1$ e $g_j(x) = x^j + 1/x^j$ para $j \geq 1$. Afirmamos que, para cada $j \geq 0$, existe f_j sobre $\mathbb{F}_q$ tal que $g_j(x) = f_j(x + 1/x)$. Os casos $j = 0$ e $j = 1$ são triviais, basta definir $f_0(x) = 1$ e $f_1(x) = x$. Suponha que para todo $\ell \leq j-1$ existe f_ℓ satisfazendo esta condição. Como

$$(x + 1/x)^j = \begin{cases} x^j + 1/x^j + \displaystyle\sum_{i=1}^{(j-1)/2} \binom{j}{i}(x^{j-2i} + 1/x^{j-2i}), & \text{se } j \text{ é ímpar,} \\ x^j + 1/x^j + \displaystyle\sum_{i=1}^{j/2-1} \binom{j}{i}(x^{j-2i} + 1/x^{j-2i}) + \binom{j}{j/2}, & \text{se } j \text{ é par,} \end{cases}$$

então existem $b_0, ..., b_{j-1} \in \mathbb{F}_q$ tais que

$$x^j + 1/x^j = (x + 1/x)^j + \sum_{\ell=0}^{j-1} b_\ell g_\ell(x) = (x + 1/x)^j + \sum_{\ell=0}^{j-1} b_\ell f_\ell(x + 1/x).$$

Logo, podemos definir

$$f_j(x) = x^j + \sum_{\ell=0}^{j-1} b_\ell f_\ell(x).$$

Portanto, o polinômio

$$f(x) = a_n + \sum_{j=1}^{n} a_{n-j} f_j(x)$$

satisfaz

$$f^Q(x) = x^n \left(a_n + \sum_{j=1}^{n} a_{n-j} f_j(x + 1/x) \right) = g(x).$$

Como os polinômios autorrecíprocos de grau $2n$ são determinados por apenas $n+1$ de seus coeficientes, concluímos que o número de polinômios autorrecíprocos de grau $2n$ sobre $\mathbb{F}_q$ é igual ao número de polinômios de grau n sobre $\mathbb{F}_q$. Portanto, dado g autorrecíproco de grau $2n$, existe um único polinômio f de grau n tal que $f^Q = g$. □

Observamos que se $f(x) = f_1(x)f_2(x)$ é um polinômio redutível sobre $\mathbb{F}_q$, então f^Q também é redutível sobre $\mathbb{F}_q$. De fato, se $\deg(f_1) = n_1$ e $\deg(f_2) = n_2$, então

$$f^Q(x) = x^{n_1+n_2} f_1(x + 1/x) f_2(x + 1/x) = x^{n_1} f_1(x + 1/x) \cdot x^{n_2} f_2(x + 1/x) = f_1^Q(x) f_2^Q(x).$$

O próximo lema estuda a fatoração de f^Q quando f é irredutível.

Lema 2.2.3. *Seja f um polinômio mônico irredutível de grau n diferente de $x+2$ sobre $\mathbb{F}_q$. Então f^Q é um polinômio* miar *de grau $2n$ ou $f^Q(x) = g(x)h(x)$ onde g, h são irredutíveis de grau n sobre $\mathbb{F}_q$ tais que $g^*(x) = \gamma h(x)$ para algum $\gamma \in \mathbb{F}_q^*$ e ambos g, h não são autorrecíprocos.*

Demonstração. Seja $n = 1$. Então $f(x) = x + c$ para algum $c \neq 2$ e $f^Q(x) = x^2 + cx + 1$. Se f^Q não for *miar*, então f^Q possui uma raiz $\alpha \in \mathbb{F}_q$. Como o produto das raízes de f^Q é 1, segue que $1/\alpha$ também é raiz de f^Q, e $f^Q(x) = (x - \alpha)(x - 1/\alpha)$. Por hipótese, $c \neq 2$, logo $\alpha \neq -1$, o que implica que f^Q é o produto de dois polinômios irredutíveis de grau 1 com as propriedades desejadas.

Suponha agora $n > 1$. Se α é uma raiz de f^Q, então $\alpha + 1/\alpha$ é uma raiz de f, pela definição de f^Q. Como f é irredutível, então $\mathbb{F}_q(\alpha + 1/\alpha) = \mathbb{F}_{q^n}$ e n é o menor inteiro

positivo tal que

$$(\alpha + 1/\alpha)^{q^n} = \alpha + 1/\alpha \Leftrightarrow (\alpha^{q^n-1} - 1)(\alpha^{q^n+1} - 1) = 0.$$

Se $\alpha^{q^n+1} - 1 = 0$, então $\alpha^{q^n} = \alpha^{-1}$, o que implica $\alpha \notin \mathbb{F}_{q^n}$ e, também, α é uma raiz de $x^{q^{2n}-1} - 1$, logo $\alpha \in \mathbb{F}_{q^{2n}}$. Portanto $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{2n}}$ e f^Q é *miar*. Se $\alpha^{q^n-1} - 1 = 0$, então $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, logo f^Q é o produto de dois fatores mônicos irredutíveis g, h de grau n. Se um desses fatores, digamos g, fosse *miar*, teríamos n par e $g \mid H_{q,n/2}$, logo $\alpha^{q^{n/2}+1} - 1 = 0$, o que implicaria

$$(\alpha + 1/\alpha)^{q^{n/2}} = \alpha + 1/\alpha,$$

uma contradição com a minimalidade de n. Pelo fato de $f^Q(x) = g(x)h(x)$ ser autorrecíproco, temos $g(x)h(x) = g^*(x)h^*(x)$. Note que $h \nmid h^*$, já que, caso contrário, h seria autorrecíproco pela Proposição 2.1.2 (iv), logo devemos ter $h \mid g^*$, ou seja, $g^*(x) = \gamma h(x)$ para algum $\gamma \in \mathbb{F}_q^*$. □

De acordo com o Lema 2.2.3, uma forma de construir um polinômio *miar* de grau $2n$ sobre $\mathbb{F}_q$ é:

(1) gerar um polinômio irredutível f de grau n,

(2) transformar f em f^Q,

(3) calcular $\text{mdc}(x^{q^n-1} - 1, f^Q(x))$. Se o resultado for 1, então f^Q é um polinômio *miar*, caso contrário recomeçamos em (1).

Um critério mais simples para decidir se f^Q é ou não *miar* é apresentado no lema a seguir.

Lema 2.2.4. *Sejam f um polinômio irredutível de grau n sobre $\mathbb{F}_q$ e $\beta \in \mathbb{F}_{q^n}$ uma raiz de f. Então f^Q é irredutível sobre $\mathbb{F}_q$ se, e somente se, o polinômio*

$$g(x) = x^2 - \beta x + 1 \in \mathbb{F}_{q^n}[x]$$

é irredutível sobre $\mathbb{F}_{q^n}$.

Demonstração. Seja α uma raiz de f^Q. Então $\beta = \alpha + 1/\alpha$ é uma raiz de f e α é uma raiz de g. Suponha g irredutível sobre $\mathbb{F}_{q^n}$. Então $[\mathbb{F}_{q^n}(\alpha) : \mathbb{F}_{q^n}] = 2$, o que implica $\mathbb{F}_{q^n}(\alpha) = \mathbb{F}_{q^{2n}}$, logo f^Q é irredutível sobre $\mathbb{F}_q$. Por outro lado, se f^Q é irredutível sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = 2n$, o que implica $[\mathbb{F}_{q^n}(\alpha) : \mathbb{F}_{q^n}] = 2$, logo g é irredutível sobre $\mathbb{F}_{q^n}$. □

Observação 2.2.5. De acordo com o Lema 2.2.4, podemos determinar a irredutibilidade de f^Q sobre $\mathbb{F}_q$ a partir da irredutibilidade de um polinômio de grau 2 sobre $\mathbb{F}_{q^n}$. Pela Proposição 1.4.1, se q é ímpar, o polinômio $g(x) = x^2 - \beta x + 1$ é irredutível sobre $\mathbb{F}_{q^n}$ se, e somente se, $\beta^2 - 4$ não é um quadrado em $\mathbb{F}_{q^n}$. Pela Proposição 1.4.2, se q é par, então o polinômio $g(x) = x^2 - \beta x + 1$ é irredutível sobre $\mathbb{F}_{q^n}$ se, e somente se, $\beta \neq 0$ e $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(1/\beta^2) = 1$.

2.3 Sequências de polinômios *miar* sobre $\mathbb{F}_{2^m}$ via Q-transformação

O objetivo desta seção é construir, a partir de um polinômio irredutível $f_0 \in \mathbb{F}_{2^m}[x]$, uma sequência de polinômios indutivamente por $f_i = f_{i-1}^Q$, $i \geq 1$, tal que todos os termos sejam *miar* (exceto, possivelmente, o polinômio f_0). Para isso, precisamos supor que o polinômio inicial f_0 seja do tipo A, cuja definição apresentamos a seguir.

Definição 2.3.1. Sejam $m \geq 1$ e $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{F}_{2^m}[x]$ um polinômio irredutível diferente do polinômio x. Dizemos que f é um polinômio do tipo A se $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_1/a_0) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_{n-1}) = 1$.

Teorema 2.3.2. *Sejam* $m \geq 1$ *e* $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{F}_{2^m}[x]$ *um polinômio irredutível diferente do polinômio* x. *Então* f^Q *é irredutível sobre* $\mathbb{F}_{2^m}$ *se, e somente se,* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_1/a_0) = 1$.

Demonstração. Pelo Lema 2.2.4 e pela Observação 2.2.5, f^Q é irredutível se, e somente se, $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta^2) = 1$, onde $\beta \in \mathbb{F}_{2^{mn}}$ é uma raiz qualquer de f. Como

$$\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta^2) = (\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta))^2$$

e $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta) \in \mathbb{F}_2$, então

$$\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta^2) = \mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta).$$

Pela transitividade do traço, temos

$$\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_{2^m}}(1/\beta)).$$

Como β é raiz de f, então $1/\beta$ é raiz de $f^*(x)/a_0 = x^n + (a_1/a_0)x^{n-1} + ... + 1/a_0$, portanto $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_{2^m}}(1/\beta) = a_1/a_0$.
Assim, $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_1/a_0) = 1$ se, e somente se, $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(1/\beta) = 1$. □

Corolário 2.3.3. (Varshamov e Garakov, [23]) *Seja* $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + 1 \in \mathbb{F}_2[x]$ *um polinômio irredutível. Então* f^Q *é irredutível sobre* $\mathbb{F}_2$ *se, e somente se,* $a_1 = 1$.

Demonstração. Segue do Teorema 2.3.2, visto que a função traço, neste caso, é a identidade. □

Corolário 2.3.4. *Seja* $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{F}_4[x]$ *um polinômio irredutível diferente do polinômio* x. *Então* f^Q *é irredutível sobre* $\mathbb{F}_4$ *se, e somente se,* $a_1 \neq 0$ *e* $a_1 \neq a_0$.

Demonstração. Seja $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, onde ω é uma raiz de $x^2 + x + 1 \in \mathbb{F}_2[x]$. Calculando o traço absoluto de cada elemento de $\mathbb{F}_4$, temos

$$\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(0) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(1) = 0;\ \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\omega) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\omega^2) = 1.$$

Logo, o Teorema 2.3.2 nos garante que f^Q é irredutível se, e somente se, $a_1/a_0 \notin \{0,1\}$ ou, equivalentemente, $a_1 \neq 0$ e $a_1 \neq a_0$. □

No Exemplo 2.1.5 encontramos todos os quatro polinômios *miar* de grau 4 sobre $\mathbb{F}_4$. Pelo Corolário 2.3.4, esses mesmos polinômios também poderiam ser encontrados através da transformação $f \mapsto f^Q$ nos polinômios irredutíveis $x^2+\omega x+1$, $x^2+\omega^2 x+1$, $x^2+x+\omega$, $x^2+x+\omega^2$.

Observação 2.3.5. Podemos utilizar um raciocínio semelhante ao feito no Corolário 2.3.4 para encontrar um critério de irredutibilidade em cada corpo finito de característica 2. Entretanto, esse critério dependerá do elemento primitivo escolhido e não pode ser expresso apenas pelos coeficientes de f.

Teorema 2.3.6. (Meyn, [12]) *Sejam $m \geq 1$ e $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{F}_{2^m}[x]$ um polinômio irredutível. Então $f^Q(x) = x^{2n} + a_1' x^{2n-1} + ... + a_1' x + 1$ é um polinômio* miar *do tipo A se, e somente se, f é do tipo A.*

Demonstração. Denotamos por $K = \mathbb{F}_{2^m}$, $F = \mathbb{F}_{2^{mn}}$, $L = \mathbb{F}_{2^{2mn}}$. Suponhamos que f é do tipo A. Pelo Teorema 2.3.2, f^Q é irredutível. Resta mostrar que $\mathrm{Tr}_{K/\mathbb{F}_2}(a_1') = 1$. Se α é uma raiz de f^Q, então $\beta = \alpha + 1/\alpha$ é uma raiz de f e α é uma raiz de $g(x) = x^2 + \beta x + 1 \in F[x]$. Então,

$$\mathrm{Tr}_{L/F}(\alpha) = \beta; \quad \mathrm{Tr}_{L/K}(\alpha) = a_1'; \quad \mathrm{Tr}_{F/K}(\beta) = a_{n-1}.$$

Pela transitividade do traço temos

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{F}_2}(a_1') &= \mathrm{Tr}_{K/\mathbb{F}_2}(\mathrm{Tr}_{L/K}(\alpha)) \\ &= \mathrm{Tr}_{K/\mathbb{F}_2}(\mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\alpha))) \\ &= \mathrm{Tr}_{K/\mathbb{F}_2}(\mathrm{Tr}_{F/K}(\beta)) \\ &= \mathrm{Tr}_{K/\mathbb{F}_2}(a_{n-1}) \\ &= 1. \end{aligned}$$

Suponhamos agora que f não é do tipo A. Então $\mathrm{Tr}_{K/\mathbb{F}_2}(a_1/a_0) = 0$ ou $\mathrm{Tr}_{K/\mathbb{F}_2}(a_{n-1}) = 0$. No primeiro caso, f^Q não é irredutível pelo Teorema 2.3.2. No segundo caso, pelas mesmas contas feitas acima, temos $\mathrm{Tr}_{K/\mathbb{F}_2}(a_1') = \mathrm{Tr}_{K/\mathbb{F}_2}(a_{n-1}) = 0$. Em ambos os casos, f^Q não é *miar* do tipo A. □

Como consequência do Teorema de Meyn, se f_0 é um polinômio do tipo A de grau n, então a sequência dada por $f_i = f_{i-1}^Q$, $i \geq 1$, é formada apenas por polinômios *miar*. Em [3], é provado que existem polinômios do tipo A de grau n sobre $\mathbb{F}_{2^m}$ para todos os valores m, n, exceto $(m, n) = (1, 3)$. Portanto, a Q-transformação nos permite construir polinômios *miar* de grau arbitrariamente grande sobre $\mathbb{F}_{2^m}$ a partir de um polinômio inicial f_0 do tipo A de grau n, para todos m, n tais que $(m, n) \neq (1, 3)$.

2.4 Sequências de polinômios *miar* sobre corpos de característica ímpar via R-transformação

Seja $\mathbb{F}_q$ um corpo de característica ímpar. O teorema a seguir caracteriza os polinômios mônicos irredutíveis $f^Q \in \mathbb{F}_q[x]$.

Teorema 2.4.1. *Seja f um polinômio mônico irredutível sobre um corpo $\mathbb{F}_q$ de característica ímpar. Então f^Q é irredutível sobre $\mathbb{F}_q$ se, e somente se, $f(2)f(-2)$ não é um quadrado em $\mathbb{F}_q$.*

Demonstração. Sejam n o grau de f e $\beta \in \mathbb{F}_{q^n}$ uma raiz de f. Pela Observação 2.2.5, basta mostrar que $\beta^2 - 4$ não ser um quadrado em $\mathbb{F}_{q^n}$ é equivalente a $f(2)f(-2)$ não ser um

quadrado em $\mathbb{F}_q$. Temos que

$$\begin{aligned}
\beta^2-4 \text{ não é um quadrado em } \mathbb{F}_{q^n} &\Leftrightarrow (\beta^2-4)^{(q^n-1)/2}=-1\\
&\Leftrightarrow \{[(2-\beta)(-2-\beta)]^{(q^n-1)/(q-1)}\}^{(q-1)/2}=-1\\
&\Leftrightarrow \{[\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(2-\beta)\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(-2-\beta)]\}^{(q-1)/2}=-1\\
&\Leftrightarrow \{f(2)f(-2)\}^{(q-1)/2}=-1\\
&\Leftrightarrow f(2)f(-2) \text{ não é um quadrado em } \mathbb{F}_q.
\end{aligned}$$

Acima utilizamos que $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\pm 2-\beta)=(-1)^n h(0)$, onde $h(x)=f(\pm 2-x)$ é o polinômio mínimo de $\pm 2-\beta$ sobre $\mathbb{F}_q$. □

Exemplo 2.4.2. Pelo Teorema 2.1.6, existem 6 polinômios *miar* de grau 4 sobre $\mathbb{F}_5$. Dos 10 polinômios mônicos irredutíveis de grau 2 sobre $\mathbb{F}_5$, 6 deles satisfazem $f(2)f(-2)\notin\{\pm 1\}$. São eles: x^2+x+2, x^2+2x+3, x^2+2x+4, x^2+3x+3, x^2+3x+4, x^2+4x+2. Portanto, aplicando a Q-transformação a cada um desses polinômios, obtemos os 6 polinômios *miar* de grau 4 sobre $\mathbb{F}_5$.

Definição 2.4.3. Sejam f um polinômio de grau n sobre $\mathbb{F}_q$, onde q é ímpar, e $g(x)=2^n f(x/2)$. Definimos a R-transformação de f por $f^R(x)=g^Q(x)$.

Segue diretamente da definição que f^R é autorrecíproco de grau $2n$ e que f^R é mônico se, e somente se, f é mônico. Como $g^Q(x)=x^n g(x+1/x)$, uma forma alternativa de calcular f^R é dada por

$$f^R(x)=(2x)^n f(2^{-1}(x+1/x)). \tag{2.1}$$

Na seção anterior, o Teorema de Meyn nos permitiu construir sequências de polinômios *miar* via Q-transformação em corpos finitos de característica par. O próximo teorema, desenvolvido por Cohen, apresenta um resultado semelhante em característica ímpar, desta vez utilizando a R-transformação.

Teorema 2.4.4. (Cohen, [8]) *Sejam q ímpar e f_0 um polinômio mônico irredutível de grau $n \geq 1$ sobre $\mathbb{F}_q$, onde n é par se $q \equiv 3 \pmod 4$. Suponha que $f_0(-1)f_0(1)$ não é um quadrado em $\mathbb{F}_q$. Então todos os polinômios da sequência definida por $f_{i+1} = f_i^R$, $i \geq 0$, são* miar *exceto, possivelmente, f_0.*

Demonstração. Dado $f(x) \in \mathbb{F}_q[x]$, denotamos $\lambda(f) = f(-1)f(1) \in \mathbb{F}_q$. Primeiramente, provamos por indução em i que existe $c_i \in \mathbb{F}_q$ tal que

$$\lambda(f_i) = c_i^2 \lambda(f_0),$$

para todo $i \geq 0$. Suponhamos $i = 1$. Então, pela Equação (2.1),

$$\lambda(f_1) = f_0^R(-1)f_0^R(1) = (-1)^n 4^n \lambda(f_0).$$

Se $q \equiv 1 \pmod 4$, então -1 é um quadrado em $\mathbb{F}_q$. Se $q \equiv 3 \pmod 4$, então, por hipótese, n é par, logo $(-1)^n = 1$. Em ambos os casos, $(-1)^n 4^n$ é um quadrado em $\mathbb{F}_q$, portanto $\lambda(f_1) = c_1^2 \lambda(f_0)$ para algum $c_1 \in \mathbb{F}_q$. Supondo que vale $\lambda(f_i) = c_i^2 \lambda(f_0)$ para algum $i \geq 1$, temos, pela Equação (2.1),

$$\lambda(f_{i+1}) = f_i^R(-1)f_i^R(1) = (-1)^{2^i n} 4^{2^i n} \lambda(f_i) = ((-4)^{2^{i-1} n})^2 \lambda(f_i).$$

Portanto $\lambda(f_{i+1}) = c_{i+1}^2 \lambda(f_i)$ para algum $c_{i+1} \in \mathbb{F}_q$. Por hipótese, $\lambda(f_0)$ não é um quadrado em $\mathbb{F}_q$, logo $\lambda(f_i)$ não é um quadrado em $\mathbb{F}_q$, para todo $i \geq 1$.

Seja $g_i(x) = 2^{2^i n} f_i(x/2)$. Segue que $f_{i+1} = f_i^R = g_i^Q$. Por hipótese, f_0 é irredutível sobre $\mathbb{F}_q$, logo g_0 é irredutível sobre $\mathbb{F}_q$. Suponha, por indução, que f_i, $i \geq 0$, é irredutível sobre $\mathbb{F}_q$. Então g_i é irredutível sobre $\mathbb{F}_q$ e, pelo Teorema 2.4.1, f_{i+1} é irredutível se, e somente se, $g_i(-2)g_i(2)$ não é um quadrado em $\mathbb{F}_q$. Como $g_i(-2)g_i(2) = 4^{2^i n} \lambda(f_i)$, concluímos que f_{i+1} é irredutível sobre $\mathbb{F}_q$. □

Observação 2.4.5. Ressaltamos que, para todo $n \geq 1$, existe um polinômio f_0 sobre $\mathbb{F}_q$ tal que $f_0(-1)f_0(1)$ não é um quadrado em $\mathbb{F}_q$. De fato, pelo Teorema 2.1.6, existe um polinômio *miar* h de grau $2n$, logo $h = g^Q$ para algum polinômio irredutível g de grau n, portanto $f_0(x) = 2^{-n}g(2x)$ é mônico e irredutivel. Pelo Teorema 2.4.1, $g(-2)g(2)$ não é um quadrado em $\mathbb{F}_q$, logo $f_0(-1)f_0(1)$ não é um quadrado em $\mathbb{F}_q$.

Capítulo 3

Uma generalização do Teorema de Meyn em corpos de característica par

O objetivo deste capítulo é desenvolver um algoritmo para construir uma sequência de polinômios *miar* sobre $\mathbb{F}_{2^m}$ semelhante à construída a partir do Teorema de Meyn. Neste caso, a única hipótese que vamos supor sobre o polinômio inicial f_0 é que ele seja irredutível. Para isso, definimos a reta projetiva $\mathbb{P}^1(\mathbb{F}_{2^m}) = \mathbb{F}_{2^m} \cup \{\infty\}$, a aplicação $\theta_\alpha : \mathbb{P}^1(\mathbb{F}_{2^m}) \to \mathbb{P}^1(\mathbb{F}_{2^m})$, onde $\alpha \in \mathbb{F}_{2^m}^*$ é fixo, construímos um grafo associado a essa aplicação cujos vértices são os elementos de $\mathbb{P}^1(\mathbb{F}_{2^m})$, e associamos θ_α a uma transformação quadrática (Q, α). Essas ferramentas nos permitem construir sequências de polinômios irredutíveis a partir de um polinômio irredutível qualquer, e o caso especial $\alpha = 1$ nos permite encontrar um polinômio do tipo A. Os resultados apresentados neste capítulo se baseiam no trabalho de Ugolini [22].

A partir deste capítulo, denotaremos por $\nu_2(n)$ o maior inteiro ℓ tal que 2^ℓ divide n.

3.1 A aplicação θ_α e o grafo $\mathbf{Gr}_m(\alpha)$

Dado $\alpha \in \mathbb{F}_{2^m}^*$, definimos a aplicação $\theta_\alpha : \mathbb{P}^1(\mathbb{F}_{2^m}) \to \mathbb{P}^1(\mathbb{F}_{2^m})$ por

$$\theta_\alpha(x) = \begin{cases} \infty, & \text{se } x \in \{0, \infty\}, \\ x + \alpha/x, & \text{caso contrário.} \end{cases}$$

Podemos construir um grafo direcionado $\mathrm{Gr}_m(\alpha)$ associado à aplicação θ_α. Para isso, basta representar cada elemento de $\mathbb{P}^1(\mathbb{F}_{2^m})$ por um vértice e definir uma aresta direcionada (β_1, β_2) se $\beta_2 = \theta_\alpha(\beta_1)$.

Dizemos que um elemento $\beta \in \mathbb{P}^1(\mathbb{F}_{2^m})$ é θ_α-periódico se $\theta_\alpha^k(\beta) = \beta$ para algum inteiro

positivo k. Se β é θ_α-periódico e k é o menor inteiro positivo tal que $\theta_\alpha^k(\beta) = \beta$, então o vértice β em $\mathrm{Gr}_m(\alpha)$ pertence a um ciclo de comprimento k. Podemos verificar que se β não é periódico, então existe $d > 1$ tal que $\theta_\alpha^d(\beta)$ é periódico. De fato, como $\mathbb{P}^1(\mathbb{F}_{2^m})$ é finito, existem inteiros positivos $d < d + e$ tais que $\theta_\alpha^d(\beta) = \theta_\alpha^{d+e}(\beta)$.

A seguir, mostramos que, para todo $\alpha \in \mathbb{F}_{2^m}^*$, os grafos $\mathrm{Gr}_m(\alpha)$ e $\mathrm{Gr}_m(1)$ são isomorfos. Dado $\gamma \in \mathbb{F}_{2^m}^*$, definimos uma bijeção ψ_γ em $\mathbb{P}^1(\mathbb{F}_{2^m})$ da seguinte forma:

$$\psi_\gamma(x) = \begin{cases} \infty, & \text{se } x = \infty, \\ \gamma x, & \text{caso contrário.} \end{cases}$$

Escolhendo γ como sendo a solução de $x^2 = \alpha$ em $\mathbb{F}_{2^m}^*$, temos que

$$\psi_{\gamma^{-1}} \circ \theta_\alpha \circ \psi_\gamma = \theta_1,$$

logo $\theta_\alpha(\psi_\gamma(x)) = \psi_\gamma(\theta_1(x))$ para todo $x \in \mathbb{P}^1(\mathbb{F}_{2^m})$. Se (δ_1, δ_2) é uma aresta direcionada de $\mathrm{Gr}_m(1)$, então

$$\theta_\alpha(\psi_\gamma(\delta_1)) = \psi_\gamma(\theta_1(\delta_1)) = \psi_\gamma(\delta_2),$$

ou seja, $(\psi_\gamma(\delta_1), \psi_\gamma(\delta_2))$ é uma aresta direcionada de $\mathrm{Gr}_m(\alpha)$.

As proposições a seguir apresentam algumas propriedades da aplicação θ_α e do grafo $\mathrm{Gr}_m(\alpha)$.

Proposição 3.1.1. *Seja $\beta \in \mathbb{P}^1(\mathbb{F}_{2^m})$. Então*

(i) Se $\beta = 0$, a equação $\theta_\alpha(x) = \beta$ possui 1 solução em $\mathbb{P}^1(\mathbb{F}_{2^m})$. Se $\beta \in \mathbb{P}^1(\mathbb{F}_{2^m})\backslash\{0\}$, a equação $\theta_\alpha(x) = \beta$ possui 0 ou 2 soluções distintas em $\mathbb{P}^1(\mathbb{F}_{2^m})$. Mais especificamente, se $\beta \neq \infty$ e $\gamma \in \mathbb{P}^1(\mathbb{F}_{2^m})$ é uma solução da equação $\theta_\alpha(x) = \beta$, então α/γ também é uma solução de $\theta_\alpha(x) = \beta$.

(ii) Se $\beta \in \mathbb{P}^1(\mathbb{F}_{2^m})$ é um elemento θ_α-periódico, a equação $\theta_\alpha(x) = \beta$ possui como soluções

um elemento θ_α-periódico e um elemento que não é θ_α-periódico.

Demonstração. (i) Se $\beta = \infty$, então as soluções de $\theta_\alpha(x) = \beta$ são 0 e ∞. Se $\beta \neq \infty$, temos que $\theta_\alpha(x) = \beta$ se, e somente se, $x^2 + \beta x + \alpha = 0$. Pela Proposição 1.4.2, a equação $x^2 + \beta x + \alpha = 0$ deve possuir 0 ou 2 soluções em $\mathbb{F}_{2^m}$ se $\beta \neq 0$, ou então 1 solução se $\beta = 0$. Se $\beta \neq \infty$ e $\gamma \in \mathbb{P}^1(\mathbb{F}_{2^m})$ é uma solução de $\theta_\alpha(x) = \beta$, então $\gamma + \alpha/\gamma = \beta$, logo $\theta_\alpha(\alpha/\gamma) = \alpha/\gamma + \gamma = \beta$.

(ii) Se $\beta = \infty$, o resultado segue, visto que ∞ é θ_α-periódico e 0 não é θ_α-periódico. Suponha agora $\beta \in \mathbb{F}_{2^m}$ e seja $k \geq 1$ o menor inteiro tal que $\theta_\alpha^k(\beta) = \beta$. Então $\beta_1 = \theta_\alpha^{k-1}(\beta)$ é uma solução de $\theta_\alpha(x) = \beta$. Como $\theta_\alpha^k(\beta_1) = \theta_\alpha^{k-1}(\beta) = \beta_1$, segue que β_1 é um elemento θ_α-periódico.

Pelo item (i), a equação $\theta_\alpha(x) = \beta$ possui uma outra solução $\beta_2 \neq \beta_1$ em $\mathbb{P}^1(\mathbb{F}_{2^m})$. Então $\theta_\alpha^i(\beta_2) = \theta_\alpha^{i-1}(\beta)$ para todo $i \geq 1$. Suponha por contradição que β_2 é θ_α-periódico. Como β pertence a um ciclo de comprimento k, é necessário que $\beta_2 = \theta_\alpha^j(\beta)$ para algum $1 \leq j \leq k-1$. Entretanto, temos $\theta_\alpha^{k-1}(\beta) = \beta_1 \neq \beta_2$, e $\theta_\alpha(\beta_2) = \theta_\alpha^{j+1}(\beta) \neq \beta$ se $j < k-1$. Portanto, β_2 não é θ_α-periódico.

□

Proposição 3.1.2. *Se* C *uma componente conexa de* $\mathrm{Gr}_m(1)$*, então*

(i) todos os vértices $\beta \in \mathbb{P}^1(\mathbb{F}_{2^m})$ pertencentes a C diferentes de $0, \infty$ devem satisfazer $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) \neq \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$, ou

(ii) todos os vértices $\beta \in \mathbb{P}^1(\mathbb{F}_{2^m})$ pertencentes a C diferentes de $0, \infty$ devem satisfazer $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$.

Demonstração. Primeiramente, mostramos que $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}((\beta + 1/\beta)^{-1}) = 0$ para todo $\beta \in$

$\mathbb{F}_{2^m}^* \backslash \{1\}$. Pela definição de traço, temos

$$\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}((\beta + 1/\beta)^{-1}) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}\left(\frac{\beta}{\beta^2+1}\right) = \sum_{i=0}^{m-1}\left(\frac{\beta}{\beta^2+1}\right)^{2^i}.$$

Como

$$\frac{1}{\beta^{2^{i-1}}+1} + \frac{1}{\beta^{2^i}+1} = \frac{\beta^{2^{i-1}}}{\beta^{2^i}+1} = \left(\frac{\beta}{\beta^2+1}\right)^{2^{i-1}},$$

concluímos que

$$\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}((\beta + 1/\beta)^{-1}) = \sum_{i=1}^{m}\left(\frac{1}{\beta^{2^{i-1}}+1} + \frac{1}{\beta^{2^i}+1}\right) = \frac{1}{\beta+1} + \frac{1}{\beta^{2^m}+1} = 0.$$

Se β satisfaz $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) \neq \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$, então $\theta_1(\beta) = \beta + 1/\beta$ e

$$\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\theta_1(\beta)) = 1 \neq \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\theta_1(\beta)^{-1}).$$

Por outro lado, se $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$, então

$$\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\theta_1(\beta)) = 0 = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\theta_1(\beta)^{-1}).$$

Como $\beta \in \mathbb{F}_{2^m}^* \backslash \{1\}$ foi escolhido arbitrariamente, o resultado vale em todas as componentes C que não possuem o vértice 1.

Suponha que 1 pertence a C e que existe $\beta \in \mathbb{F}_{2^m}^* \backslash \{1\}$ tal que $\theta_1(\beta) = 1$. Como $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\theta_1(\beta)) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\theta_1(\beta)^{-1})$, devemos ter $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$, logo C satisfaz a condição do item (ii). Se 1 pertence a C e a equação $\theta_1(x) = 1$ não possui soluções em $\mathbb{P}^1(\mathbb{F}_{2^m})$, então o conjunto de vértices de C é dado por $\{1, 0, \infty\}$, logo C satisfaz a condição do item (ii). □

Proposição 3.1.3. *Seja $\alpha \in \mathbb{F}_{2^m}^*$. Cada componente conexa* C *de* $\mathrm{Gr}_m(\alpha)$ *deve satisfazer*

uma das condições abaixo.

(i) C *é formada por um ciclo cujos vértices são raízes de árvores invertidas de altura* 1. *Se* $\alpha = 1$, *todo elemento* $\beta \in \mathbb{F}_{2^m}^*$ *pertencente a uma componente desta forma satisfaz* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) \neq \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$.

(ii) C *é formada por um ciclo cujos vértices são raízes de árvores invertidas de altura* $\nu_2(m)+2$. *Em cada uma destas árvores, todas as folhas pertencem ao nível* $\nu_2(m)+2$, *e todos os vértices possuem dois filhos, exceto a raiz, as folhas e o vértice* 0 *(caso este pertença à árvore). Se* $\alpha = 1$, *todo elemento* $\beta \in \mathbb{F}_{2^m}^*$ *pertencente a uma componente desta forma satisfaz* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(1/\beta)$.

Demonstração. Segue dos Lemas 4.3 e 4.4 de [17] e do fato de que os grafos $\mathrm{Gr}_m(\alpha)$ e $\mathrm{Gr}_m(1)$ são isomorfos. □

Mais detalhes sobre a construção do grafo $\mathrm{Gr}_m(\alpha)$ podem ser encontrados em [17]. Na Seção 3.3, apresentamos alguns exemplos de grafos desta forma.

3.2 Um algoritmo para construir polinômios irredutíveis via (Q, α)-transformação a partir de um polinômio irredutível qualquer

Iniciamos esta seção apresentando uma transformação que generaliza a Q-transformação em corpos de característica par.

Definição 3.2.1. Sejam $\alpha \in \mathbb{F}_{2^m}^*$ e f um polinômio de grau n sobre $\mathbb{F}_{2^m}$. Definimos a (Q, α)-transformação de f por

$$f^{(Q,\alpha)}(x) = x^n f(x + \alpha/x).$$

Em geral, o polinômio $f^{(Q,\alpha)}$ não é autorrecíproco se $\alpha \neq 1$. Entretanto, se $\alpha = 1$, a (Q, α)-transformação coincide com a Q-transformação. Observamos que se $\gamma \in \mathbb{F}_{2^m}^*$ e f possui grau n, então podemos escrever $f^{(Q,\alpha)}(\gamma) = \gamma^n f(\theta_\alpha(\gamma))$.

O lema a seguir caracteriza a fatoração de $f^{(Q,\alpha)}$ sobre um corpo finito $\mathbb{F}_{2^m}$ de forma semelhante à feita pelo Lema 2.2.3 com relação ao polinômio f^Q sobre um corpo finito qualquer.

Lema 3.2.2. *Sejam m, n inteiros positivos, $\alpha \in \mathbb{F}_{2^m}^*$ e f um polinômio mônico irredutível de grau n sobre $\mathbb{F}_{2^m}$. Então $f^{(Q,\alpha)}$ é um polinômio mônico irredutível de grau $2n$ sobre $\mathbb{F}_{2^m}$ ou $f^{(Q,\alpha)}$ é o produto de dois polinômios mônicos irredutíveis g_1, g_2 de grau n sobre $\mathbb{F}_{2^m}$. No segundo caso, todas as raízes de pelo menos um dos polinômios g_1 ou g_2 não são θ_α-periódicas.*

Demonstração. Seja $\beta \in \mathbb{F}_{2^{mn}}$ uma raiz de f e $\gamma \in \mathbb{F}_{2^{2mn}}$ uma solução de $\theta_\alpha(x) = \beta$. Então $f^{(Q,\alpha)}(\gamma) = \gamma^n f(\beta) = 0$. Como γ é uma raiz de $x^2 + \beta x + \alpha \in \mathbb{F}_{2^{mn}}[x]$, devemos ter $\gamma \in \mathbb{F}_{2^{2mn}} \backslash \mathbb{F}_{2^{mn}}$ ou $\gamma \in \mathbb{F}_{2^{mn}}$. No primeiro caso, concluímos que $f^{(Q,\alpha)}$ é irredutível sobre $\mathbb{F}_{2^m}$. No segundo caso, temos $\mathbb{F}_{2^m}(\gamma) = \mathbb{F}_{2^m}(\beta) = \mathbb{F}_{2^{mn}}$, o que implica que o polinômio mínimo de γ sobre $\mathbb{F}_{2^m}$ possui grau n e divide $f^{(Q,\alpha)}$, logo $f^{(Q,\alpha)}$ se fatora como produto de dois polinômios mônicos irredutíveis g_1, g_2 de grau n sobre $\mathbb{F}_{2^m}$.

Suponha que $f^{(Q,\alpha)}(x) = g_1(x)g_2(x)$, onde g_1 e g_2 possuem grau n. Pela Proposição 3.1.1 (i), as soluções de $\theta_\alpha(x) = \beta$ em $\mathbb{P}^1(\mathbb{F}_{2^{mn}})$ são γ e α/γ. Se β não for θ_α-periódico, então ambos γ e α/γ não são θ_α-periódicos. Se β for θ_α-periódico, então a Proposição 3.1.1 (ii) garante que um dos elementos γ ou α/γ, digamos γ, não é θ_α-periódico. Como $f^{(Q,\alpha)}(\gamma) = 0$, devemos ter $g_1(\gamma) = 0$ ou $g_2(\gamma) = 0$.

Suponhamos, sem perda de generalidade, que $g_1(\gamma) = 0$ e seja δ uma outra raiz de g_1. Segue do Teorema 1.1.4 que $\gamma = \delta^{2^{mi}}$ para algum inteiro $i \geq 1$ e temos $(\theta_\alpha^j(\delta))^{2^{mi}} = \theta_\alpha^j(\delta^{2^{mi}}) = \theta_\alpha^j(\gamma)$ para todo $j \geq 1$. Se $\theta_\alpha^k(\delta) = \delta$ para algum $k \geq 1$, temos $(\theta_\alpha^k(\delta))^{2^{mi}} = \delta^{2^{mi}} = \gamma$, o que

implica $\theta_\alpha^k(\gamma) = (\theta_\alpha^k(\delta))^{2^{mi}} = \gamma$, uma contradição. Portanto, todas as raízes de g_1 não são θ_α-periódicas. □

Dados $\alpha \in \mathbb{F}_{2^m}^*$ e f_0 um polinômio mônico irredutível de grau n sobre $\mathbb{F}_{2^m}$, construímos uma sequência de polinômios irredutíveis da seguinte maneira: definimos f_1 como sendo um fator irredutível de $f_0^{(Q,\alpha)}$ sobre $\mathbb{F}_{2^m}$ tal que todas as suas raízes não sejam θ_α-periódicas. Para cada $i \geq 1$, definimos o polinômio f_{i+1} como sendo um dos fatores irredutíveis de $f_i^{(Q,\alpha)}$ sobre $\mathbb{F}_{2^m}$. Segue do Lema 3.2.2 que o grau de cada termo desta sequência é igual ou é o dobro do grau do termo anterior. O teorema a seguir determina a existência de um inteiro t tal que $\deg(f_{i+1}) = 2\deg(f_i)$ para todo $i \geq t$.

Teorema 3.2.3. *Sejam $\alpha \in \mathbb{F}_{2^m}^*$, f_0 um polinômio mônico irredutível de grau n sobre $\mathbb{F}_{2^m}$ e a sequência $\{f_i\}_{i\geq 0}$ definida acima. Se $\nu_2(m) = \ell_m$ e $\nu_2(n) = \ell_n$, então existe um inteiro $t \leq \ell_m + \ell_n + 3$ tal que f_t tem grau $2n$ e $f_{t+j+1} = f_{t+j}^{(Q,\alpha)}$ para todo $j \geq 0$.*

Demonstração. Seja $\beta_0 \in \mathbb{F}_{2^{mn}}$ uma raiz de f_0. Pela definição da (Q,α)-transformação, podemos construir uma sequência $\{\beta_i\}_{i\geq 0}$, onde cada elemento β_i é uma raiz de f_i em alguma extensão de $\mathbb{F}_{2^m}$ e $\beta_i = \theta_\alpha(\beta_{i+1})$. Logo, se β_i pertence ao nível k_i de uma árvore invertida em $\mathrm{Gr}_{2^r}(\alpha)$, $r \geq 1$, e não é uma folha, então β_{i+1} pertence ao nível $k_i + 1$ desta mesma árvore.

Como f_1 não possui raízes θ_α-periódicas, $\beta_1 \in \mathbb{F}_{2^{2mn}}$ não é θ_α-periódico, logo β_1 pertence a um nível não menor que 1 de uma árvore invertida T enraizada em um vértice θ_α-periódico de $\mathrm{Gr}_{2mn}(\alpha)$. Afirmamos que a altura de T é maior ou igual a 2. De fato, se $\beta_1 \in \mathbb{F}_{2^{mn}}$, então $\beta_2 \in \mathbb{F}_{2^{2mn}}$, o que implica que β_2 pertence a um nível não menor que 2 de T. Se $\beta_1 \in \mathbb{F}_{2^{2mn}} \backslash \mathbb{F}_{2^{mn}}$, então β_0 é uma folha em $\mathrm{Gr}_{mn}(\alpha)$, o que implica que β_0 pertence a um nível não menor que 1 de T, logo β_1 pertence a um nível não menor que 2 de T. Assim, a afirmação está provada.

Como T possui altura maior que 1, segue da Proposição 3.1.3 que a altura de T é $\nu_2(2mn) + 2 = \ell_m + \ell_n + 3$. Então existe $t \leq \ell_m + \ell_n + 3$ tal que β_t é uma folha de T. Logo,

para todo $j \geq 0$, temos que β_{t+j} é uma folha em $\mathrm{Gr}_{2^{j+1}mn}(\alpha)$, visto que β_{t+j} deve pertencer ao nível $\ell_m+\ell_n+j+3$ de uma árvore de altura $\ell_m+\ell_n+j+3$. Logo, $\beta_{t+j+1} \in \mathbb{F}_{2^{2^{j+2}mn}} \backslash \mathbb{F}_{2^{2^{j+1}mn}}$. Portanto, f_t possui grau $2n$ enquanto f_{t+j} possui grau $2^{j+1}n$, ou seja, $f_{t+j+1} = f_{t+j}^{(Q,\alpha)}$ para todo $j \geq 0$. □

Corolário 3.2.4. *Seja f_0 um polinômio mônico irredutível de grau n sobre $\mathbb{F}_{2^m}$, e considere a sequência $\{f_i\}_{i\geq 0}$ onde f_1 é um fator de f_0^Q que não possui raízes θ_1-periódicas e f_{i+1} é um dos fatores irredutíveis de f_i^Q sobre $\mathbb{F}_{2^m}$. Se $\nu_2(m) = \ell_m$ e $\nu_2(n) = \ell_n$, então existe um inteiro $t \leq \ell_m + \ell_n + 3$ tal que f_t é um polinômio do tipo A de grau $2n$ e f_{t+j} é* miar *de grau $2^{j+1}n$ para todo $j \geq 1$.*

Demonstração. Tomando $\alpha = 1$ no Teorema 3.2.3, existe um inteiro $t \leq \ell_m + \ell_n + 3$ tal que f_t tem grau $2n$ e $f_{i+1} = f_i^Q$ para todo $i \geq t$. Por construção, todos os polinômios da sequência $\{f_i\}_{i\geq 0}$ são irredutíveis logo, para cada $j \geq 1$, o polinômio f_{t+j} é *miar* e $\deg(f_{t+j}) = 2\deg(f_{t+j-1})$.

Como f_{t+1} é *miar*, segue que f_{t+1} é do tipo A. Do contrário, teríamos $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_1) = 0$, onde a_1 é o coeficiente de grau 1 de f_{t+1}, o que implicaria f_{t+2} redutível pelo Teorema 2.3.2. Portanto, o Teorema de Meyn garante que f_t é do tipo A. □

Observação 3.2.5. Ao construir a sequência $\{f_i\}_{i\geq 0}$, supomos que todas as raízes de f_1 não são θ_α-periódicas. Se $f_1 = f_0^{(Q,\alpha)}$, então as raízes de f_0 são folhas em $\mathrm{Gr}_{mn}(\alpha)$, logo as raízes de f_1 não são θ_α-periódicas. Se $f_0^{(Q,\alpha)}(x) = g_1(x)g_2(x)$, ressaltamos que não é necessário saber previamente qual(is) dos polinômios g_1, g_2 não possui(em) raízes θ_α-periódicas. Suponha que g_1 não possui raízes θ_α-periódicas. Então, escolhendo f_1 como sendo g_1, o último polinômio de grau n da sequência deverá ser f_s, onde $s \leq \ell_m + \ell_n + 2$. Se, ao escolher f_1 como sendo g_2, s são satisfaz esta condição, então paramos a iteração e definimos $f_1 = g_1$.

Observação 3.2.6. Seja $\alpha = 1$. Utilizando a notação da observação anterior, devemos ter $s \leq 1$ se as raízes de f_0 satisfazem $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(\beta_0) \neq \mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(\beta_0^{-1})$ ou $s \leq \ell_m + \ell_n + 2$ se as

raízes de f_0 satisfazem $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(\beta_0) = \mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(\beta_0^{-1})$ (Proposição 3.1.3). O segundo caso implica que as raízes de f_s pertencem ao nível $\ell_m + \ell_n + 2$ de árvores invertidas em $\mathrm{Gr}_{mn}(1)$ e em $\mathrm{Gr}_{2mn}(1)$, enquanto as raízes de f_t pertencem ao nível $\ell_m + \ell_n + 3$ de árvores invertidas em $\mathrm{Gr}_{2mn}(1)$. Portanto, se as raízes de f_0 pertencem a uma componente de $\mathrm{Gr}_{mn}(1)$ descrita como na Proposição 3.1.3 (ii), então $f_t = f_s^Q$ é o único polinômio de grau $2n$ da sequência $\{f_i\}_{i\geq 0}$. Neste caso, o polinômio f_s é do tipo A e possui grau n.

Observação 3.2.7. Para determinar os termos da sequência $\{f_i\}_{i\geq 0}$, é necessário saber se um polinômio da forma $f^{(Q,\alpha)}$ é ou não irredutível. Utilizando o mesmo raciocínio empregado na demonstração do Teorema 2.3.2, podemos verificar que, dado $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{F}_{2^m}[x]$ irredutível, então $f^{(Q,\alpha)}$ é irredutível se, e somente se, $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_1\gamma/a_0) = 1$, onde $\gamma^2 = \alpha$.

Para isso, se $\beta \in \mathbb{F}_{2^{mn}}$ é uma raiz de f, basta considerar na demonstração do Teorema 2.3.2 que:

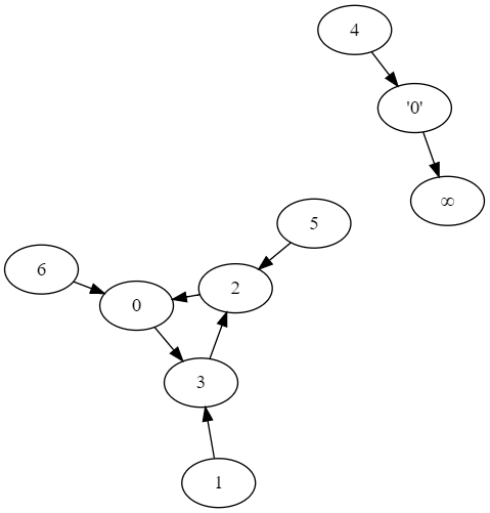
- $f^{(Q,\alpha)}$ é irredutível sobre $\mathbb{F}_{2^m}$ se, e somente se, $x^2 + \beta x + \alpha$ é irredutível sobre $\mathbb{F}_{2^{mn}}$, o que é equivalente a $\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_2}(\alpha/\beta^2) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^{mn}}/\mathbb{F}_{2^m}}(\gamma/\beta)) = 1$;
- γ/β é uma raiz de $(\gamma^n/a_0)f^*(x/\gamma) = x^n + (a_1\gamma/a_0)x^{n-1} + ... + \gamma^n/a_0$.

3.3 Exemplos

Nesta seção, apresentamos alguns exemplos de grafos da forma $\mathrm{Gr}_m(\alpha)$ e alguns exemplos de sequências de polinômios irredutíveis utilizando o Teorema 3.2.3 e o Corolário 3.2.4. Todas as imagens desta seção foram construídas com o auxílio do software Graphviz [2].

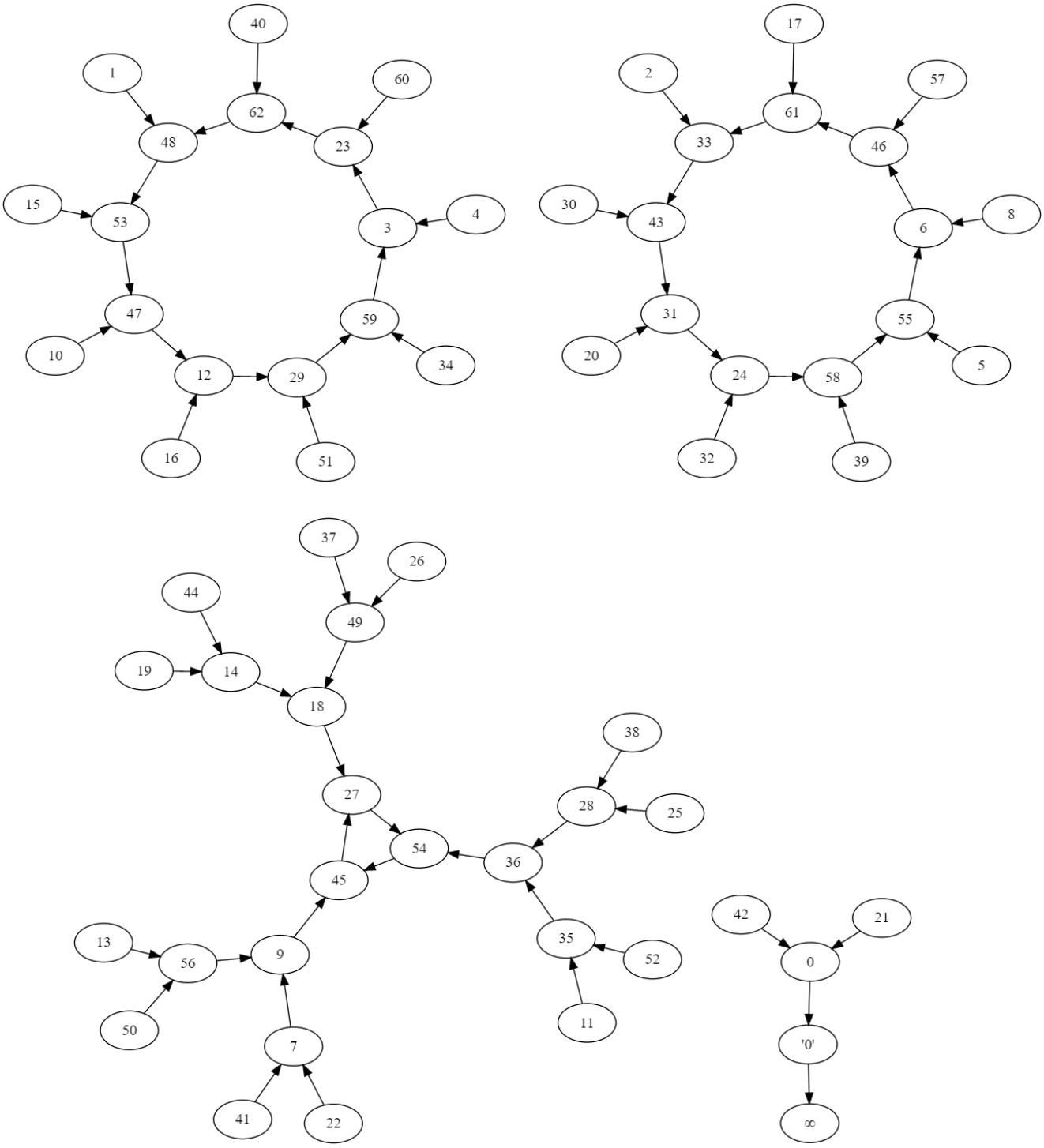
Exemplo 3.3.1. Seja $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, onde α é uma raiz do polinômio primitivo $x^3 + x + 1 \in \mathbb{F}_2[x]$. Então $\mathbb{P}^1(\mathbb{F}_{2^3}) = \{\alpha^i \mid 0 \leq i \leq 6\} \cup \{0, \infty\}$. Como $\nu_2(3) = 0$, todas as árvores de uma mesma componente conexa de $\mathrm{Gr}_3(\alpha)$ devem ter altura 1 ou 2. Aplicando θ_α a cada elemento

de $\mathbb{P}^1(\mathbb{F}_{2^3})$, construímos o grafo $\mathrm{Gr}_3(\alpha)$ a seguir. Um elemento da forma α^i, $0 \leq i \leq 6$, é representado pelo vértice i, enquanto o elemento 0 é representado por '0', e ∞ por ∞.



Exemplo 3.3.2. Seja $\alpha \in \mathbb{F}_{2^6}$ uma raiz do polinômio primitivo $x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$. Então $\mathbb{P}^1(\mathbb{F}_{2^6}) = \{\alpha^i \mid 0 \leq i \leq 62\} \cup \{0, \infty\}$. Como $\nu_2(6) = 1$, todas as árvores de uma mesma componente conexa de $\mathrm{Gr}_6(1)$ devem ter altura 1 ou 3. A seguir, apresentamos o grafo $\mathrm{Gr}_6(1)$. Um elemento da forma α^i, $0 \leq i \leq 62$, é representado pelo vértice i, enquanto o elemento 0 é representado por '0', e ∞ por ∞. Uma representação de $\mathrm{Gr}_6(\alpha)$, que é isomorfo a $\mathrm{Gr}_6(1)$, pode ser encontrada em [22].

Como $\mathbb{P}^1(\mathbb{F}_{2^2}) = \{0, \alpha^0, \alpha^{21}, \alpha^{42}, \infty\}$ e $\mathbb{P}^1(\mathbb{F}_{2^3}) = \{\alpha^{9j} \mid 0 \leq j \leq 6\} \cup \{0, \infty\}$, é interessante ressaltar que os grafos direcionados associados a $\theta_1|_{\mathbb{P}^1(\mathbb{F}_{2^2})}$ e $\theta_1|_{\mathbb{P}^1(\mathbb{F}_{2^3})}$ são isomorfos a $\mathrm{Gr}_2(1)$ e $\mathrm{Gr}_3(1)$, respectivamente.


40
1
60
62
48
23
15
53
3
4
47
59
10
34
12
29
16
51
17
2
57
61
33
46
30
43
6
8
31
55
20
5
24
58
32
39
37
26
44
49
19
14
18
38
27
28
25
54
36
45
42
21
35
13
56
9
52
0
50
11
7
'0'
41
22
∞

Exemplo 3.3.3. Seja $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, onde α é uma raiz de $x^3 + x + 1 \in \mathbb{F}_2[x]$. Construímos uma sequência de polinômios irredutíveis sobre $\mathbb{F}_{2^3}$ a partir de $f_0(x) = x + \alpha^3$ através da (Q, α)-transformação, com o auxílio do Teorema 3.2.3. Utilizando a notação do Teorema 3.2.3, temos $m = 3$, $n = 1$, $\ell_m = \ell_n = 0$, logo $t \leq 3$.

Como

$$f_0^{(Q,\alpha)}(x) = x^2 + \alpha^3 x + \alpha = (x + 1)(x + \alpha),$$

devemos definir $f_1(x) = x+\alpha$, já que α não é θ_α-periódico (vide Exemplo 3.3.1). O polinômio $f_1^{(Q,\alpha)}(x) = x^2 + \alpha x + \alpha$ é irredutível, portanto $f_2(x) = x^2 + \alpha x + \alpha$. Segue que o polinômio f_2 possui suas raízes no nível 2 de uma árvore de $\mathrm{Gr}_6(\alpha)$. Temos

$$f_2^{(Q,\alpha)}(x) = x^4 + \alpha x^3 + \alpha x^2 + \alpha^2 x + \alpha^2 = (x^2 + \alpha^3 x + \alpha^4)(x^2 + x + \alpha^5),$$

logo f_3 deve ser definido como $x^2 + \alpha^3 x + \alpha^4$ ou $x^2 + x + \alpha^5$. Em ambos os casos, f_3 possui grau 2, suas raízes são folhas em $\mathrm{Gr}_6(\alpha)$, e, pelo Teorema 3.2.3, devemos ter $f_{j+4} = f_{j+3}^{(Q,\alpha)}$ para todo $j \geq 0$.

Exemplo 3.3.4. Sejam $\mathbb{F}_{2^2} = \mathbb{F}_2(\omega)$, onde ω é uma raiz de $x^2 + x + 1 \in \mathbb{F}_2[x]$,

$$f_0(x) = x^3 + \omega^2 x^2 + \omega x + \omega \in \mathbb{F}_{2^2}[x]$$

um polinômio irredutível e $\beta_0 \in \mathbb{F}_{2^6}$ uma raiz de f_0. Nosso objetivo é encontrar um polinômio do tipo A de grau 6 através do Corolário 3.2.4. Neste caso, $m = 2$, $n = 3$, $\ell_m = 1$ e $\ell_n = 0$, logo $t \leq 4$.

Como

$$f_0^Q(x) = x^6 + \omega^2 x^5 + \omega^2 x^4 + \omega x^3 + \omega^2 x^2 + \omega^2 x + 1 = (x^3 + \omega^2 x + 1)(x^3 + \omega^2 x^2 + 1),$$

o polinômio f_1 deve ser igual a $x^3 + \omega^2 x + 1$ ou $x^3 + \omega^2 x^2 + 1$.

Pela transitividade do traço, temos $\mathrm{Tr}_{\mathbb{F}_{2^6}/\mathbb{F}_2}(\beta_0) = \mathrm{Tr}_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\omega^2) = 1$ e $\mathrm{Tr}_{\mathbb{F}_{2^6}/\mathbb{F}_2}(1/\beta_0) = \mathrm{Tr}_{\mathbb{F}_{2^2}/\mathbb{F}_2}(1) = 0$, logo β_0 pertence a uma componente conexa de $\mathrm{Gr}_6(1)$ da forma descrita na Proposição 3.1.3 (i). Se escolhêssemos $f_1(x) = x^3 + \omega^2 x^2 + 1$, teríamos f_1^Q redutível (Teorema 2.3.2) e, portanto, f_2 teria grau 3. Logo, a Observação 3.2.6 nos recomenda escolher $f_1(x) = x^3 + \omega^2 x + 1$.

Como $f_1^Q(x) = x^6+\omega x^4+x^3+\omega x^2+1$ é irredutível, definimos $f_2(x) = x^6+\omega x^4+x^3+\omega x^2+1$. Segue que

$$\begin{aligned} f_2^Q(x) = &\ x^{12} + \omega x^{10} + x^9 + \omega^2 x^8 + x^7 + x^6 + x^5 + \omega^2 x^4 + x^3 + \omega x^2 + 1 \\ = &\ (x^6 + \omega^2 x^3 + \omega^2 x^2 + \omega)(x^6 + \omega x^4 + \omega x^3 + \omega^2). \end{aligned}$$

Escolhendo $f_3(x) = x^6 + \omega x^4 + \omega x^3 + \omega^2$, temos

$$\begin{aligned} f_3^Q(x) = &\ x^{12} + \omega x^{10} + \omega x^9 + x^8 + \omega x^7 + \omega^2 x^6 + \omega x^5 + x^4 + \omega x^3 + \omega x^2 + 1 \\ = &\ (x^6 + \omega x^5 + \omega x^4 + x^2 + \omega^2 x + \omega)(x^6 + \omega x^5 + \omega^2 x^4 + x^2 + x + \omega^2). \end{aligned}$$

Assim, f_4 deve ser definido como $x^6+\omega x^5+\omega x^4+x^2+\omega^2 x+\omega$ ou $x^6+\omega x^5+\omega^2 x^4+x^2+x+\omega^2$. Em ambos os casos, f_4 é um polinômio do tipo A de grau 6 e $f_{j+4} = f_{j+3}^Q$ é *miar* para todo $j \geq 1$.

Capítulo 4

Uma generalização do Teorema de Cohen em corpos de característica ímpar

Vimos na Seção 2.4 que, através do Teorema de Cohen, podemos construir uma sequência de polinômios *miar* sobre um corpo de característica ímpar $\mathbb{F}_q$ aplicando a R-transformação sucessivas vezes a um polinômio irredutível f_0 tal que $f_0(-1)f_0(1)$ não é um quadrado em $\mathbb{F}_q$. Entretanto, nem sempre é simples encontrar um polinômio irredutível satisfazendo esta hipótese. Neste capítulo, baseados no trabalho de Ugolini [21], fornecemos um algoritmo para construir uma sequência de polinômios *miar* sobre corpos de característica ímpar a partir de um polinômio irredutível f_0 qualquer.

Ao longo deste capítulo, q representa uma potência de um primo ímpar.

4.1 A aplicação φ e o grafo Gr_q

Seja $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$. Definimos a aplicação $\varphi : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ por

$$\varphi(x) = \begin{cases} \infty, & \text{se } x \in \{0, \infty\}, \\ \frac{1}{2}(x + 1/x), & \text{caso contrário.} \end{cases}$$

Dado um polinômio f de grau n sobre $\mathbb{F}_q$, segue que $f^R(\alpha) = (2\alpha)^n f(\varphi(\alpha))$ para todo $\alpha \in \mathbb{F}_q^*$.

Assim como fizemos na Seção 3.1 com relação à aplicação θ_α em corpos de característica par, construímos um grafo direcionado Gr_q associado à aplicação φ representando cada elemento de $\mathbb{P}^1(\mathbb{F}_q)$ por um vértice e definindo uma aresta direcionada (β_1, β_2) se $\beta_2 = \varphi(\beta_1)$.

Dizemos que um elemento $\beta \in \mathbb{P}^1(\mathbb{F}_q)$ é φ-periódico se $\varphi^k(\beta) = \beta$ para algum inteiro positivo k. O menor inteiro k satisfazendo esta propriedade é dito o período de β. Se β é

φ-periódico de período k, então o vértice β em Gr_q pertence a um ciclo de comprimento k. Segue que se β não é períodico, então existe $d > 1$ tal que $\varphi^d(\beta)$ é periódico.

Podemos mostrar que o grafo Gr_q é isomorfo ao grafo direcionado associado à aplicação quadrática em $\mathbb{P}^1(\mathbb{F}_q)$. Para isso, consideramos as funções $s, \psi : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ definidas por:

$$s(x) = \begin{cases} \infty, & \text{se } x = \infty, \\ x^2, & \text{caso contrário,} \end{cases} \qquad \psi(x) = \begin{cases} \infty, & \text{se } x = 1, \\ 1, & \text{se } x = \infty, \\ \dfrac{x+1}{x-1}, & \text{caso contrário.} \end{cases}$$

Temos que $\psi = \psi^{-1}$ e

$$\psi \circ s \circ \psi = \varphi,$$

logo $s(\psi(x)) = \psi(\varphi(x))$ para todo $x \in \mathbb{P}^1(\mathbb{F}_q)$. Segue que dois vértices δ_1 e δ_2 de Gr_q tais que $\delta_2 = \varphi(\delta_1)$ também satisfazem

$$s(\psi(\delta_1)) = \psi(\varphi(\delta_1)) = \psi(\delta_2),$$

logo $(\psi(\delta_1), \psi(\delta_2))$ é uma aresta direcionada no grafo associado à aplicação quadrática.

A estrutura do grafo associado à transformação quadrática foi estudada em diversos trabalhos, dentre eles destacamos [16] e [24]. Propriedades do grafo Gr_q foram estudadas em [20].

A proposição a seguir caracteriza algumas propriedades da aplicação φ.

Proposição 4.1.1. *Seja $\alpha \in \mathbb{P}^1(\mathbb{F}_q)$. Então*

(i) Se $\alpha = 1$ ou $\alpha = -1$, α é a única solução da equação $\varphi(x) = \alpha$ em $\mathbb{P}^1(\mathbb{F}_q)$. Se $\alpha \in \mathbb{P}^1(\mathbb{F}_q) \backslash \{-1, 1\}$, a equação $\varphi(x) = \alpha$ possui 0 ou 2 soluções distintas em $\mathbb{P}^1(\mathbb{F}_q)$. Mais especificamente, se $\alpha \neq \infty$ e $\gamma \in \mathbb{P}^1(\mathbb{F}_q)$ é uma solução da equação $\varphi(x) = \alpha$, então $1/\gamma$ também é uma solução de $\varphi(x) = \alpha$.

(ii) Se $\alpha \in \mathbb{P}^1(\mathbb{F}_q)\backslash\{-1,1\}$ é um elemento φ-periódico, a equação $\varphi(x) = \alpha$ possui como soluções um elemento φ-periódico e um elemento que não é φ-periódico.

Demonstração. (i) Se $\alpha = \infty$, então as soluções de $\varphi(x) = \alpha$ são 0 e ∞. Se $\alpha \neq \infty$, temos que $\varphi(x) = \alpha$ se, e somente se, $x^2 - 2\alpha x + 1 = 0$. Pela Proposição 1.4.1, a equação $x^2 - 2\alpha x + 1 = 0$ possui exatamente uma solução em $\mathbb{F}_q$ se, e somente se, $(2\alpha)^2 - 4 \cdot 1 = 0$, o que ocorre apenas quando $\alpha \in \{-1, 1\}$. Logo, a equação deve possuir 0 ou 2 soluções em $\mathbb{F}_q$ se $\alpha \notin \{-1, 1\}$. Se $\alpha \in \{-1, 1\}$, é fácil verificar que $\varphi(\alpha) = \alpha$.

Se $\alpha \neq \infty$ e $\gamma \in \mathbb{P}^1(\mathbb{F}_q)$ é uma solução de $\varphi(x) = \alpha$, então $2^{-1}(\gamma + 1/\gamma) = \alpha$, logo $\varphi(1/\gamma) = 2^{-1}(1/\gamma + \gamma) = \alpha$.

(ii) A demonstração é análoga à da Proposição 3.1.1 (ii).

□

Encerramos esta seção com uma proposição que caracteriza as árvores invertidas enraizadas em elementos φ-periódicos de $\mathbb{P}^1(\mathbb{F}_q)$. Para demonstrá-la, faremos uso do seguinte lema.

Lema 4.1.2. *Sejam s e ψ as aplicações definidas no início desta seção, $d \geq 3$, $\mathrm{ord}_d(2)$ a ordem de 2 em $(\mathbb{Z}/d\mathbb{Z})^*$, e $\mathrm{ord}(\delta)$ a ordem multiplicativa de δ em $\mathbb{F}_q^*$. Então*

(i) Um elemento $\alpha \in \mathbb{F}_q\backslash\{-1, 1\}$ é φ-periódico de período k se, e somente se, $\psi(\alpha)$ é s-periódico de período k. Neste caso, $k = \mathrm{ord}_d(2)$, onde $d = \mathrm{ord}(\psi(\alpha))$ é um inteiro ímpar.

(ii) Sejam $e = \nu_2(q-1)$, $\gamma \in \mathbb{F}_q$ um elemento que não é φ-periódico. Se $\mathrm{ord}(\psi(\gamma)) \not\equiv 0 \pmod{2^e}$, então $\varphi(x) = \gamma$ possui 2 soluções em $\mathbb{F}_q$. Se $\mathrm{ord}(\psi(\gamma)) \equiv 0 \pmod{2^e}$, então $\varphi(x) = \gamma$ não possui soluções em $\mathbb{F}_q$.

Demonstração. (i) Por definição, α é φ-periódico se $\varphi^k(\alpha) = \alpha$ para algum k inteiro. Vimos anteriormente que $\varphi = \psi \circ s \circ \psi$ e que $\psi = \psi^{-1}$, logo $\varphi^k(\alpha) = \alpha$ se, e somente se, $(\psi \circ s^k \circ \psi)(\alpha) = \alpha$. Esta última igualdade é equivalente a $s^k(\psi(\alpha)) = \psi(\alpha)$. Portanto, α é φ-periódico de período k se, e somente se, $\psi(\alpha)$ é s-periódico de período k.

Como α é φ-periódico de período k se, e somente se, $s^k(\psi(\alpha)) = \psi(\alpha)^{2^k} = \psi(\alpha)$, segue que $\psi(\alpha)^{2^k-1} = 1$. Isto significa que $d \mid 2^k - 1$, logo $k = \mathrm{ord}_d(2)$ pela minimalidade de k. Como $2^k - 1$ é ímpar, é necessário que d seja ímpar.

(ii) Por hipótese, $\gamma \notin \{-1, 1, \infty\}$. Logo, 0, -1 e 1 não são soluções de $\varphi(x) = \gamma$ em $\mathbb{F}_q$. Então existe $\beta \in \mathbb{F}_q$ tal que $\varphi(\beta) = \gamma$ se, e somente se, $(\psi \circ s \circ \psi)(\beta) = \gamma$. Esta última igualdade é equivalente a $\psi(\beta)^2 = \psi(\gamma)$, ou seja, é equivalente a $\psi(\gamma)$ ser um quadrado em $\mathbb{F}_q^*$. Sabemos que $\psi(\gamma)$ é um quadrado em $\mathbb{F}_q^*$ se, e somente se, $\psi(\gamma)^{(q-1)/2} = 1$, ou seja, se $\mathrm{ord}(\psi(\gamma)) \mid (q-1)/2$. Por fim, $\mathrm{ord}(\psi(\gamma)) \mid (q-1)/2$ é equivalente a $\mathrm{ord}(\psi(\gamma)) \not\equiv 0 \pmod{2^e}$.

□

Proposição 4.1.3. *Seja $\alpha \in \mathbb{P}^1(\mathbb{F}_q)$ um elemento φ-periódico. Se $\alpha \in \{-1, 1\}$, então α não é raiz de uma árvore em Gr_q. Se $\alpha \notin \{-1, 1\}$, então α é raiz de uma árvore invertida de altura $\nu_2(q-1)$ em Gr_q. Nesta árvore, todas as folhas pertencem ao nível $\nu_2(q-1)$, e a raiz possui um filho enquanto todos os outros vértices, exceto as folhas, possuem dois filhos.*

Demonstração. Pela Proposição 4.1.1 (i), a equação $\varphi(x) = \pm 1$ possui apenas uma solução, que é ± 1. Logo $\alpha \in \{-1, 1\}$ não é raiz de uma árvore em Gr_q.

Se $\alpha \notin \{-1, 1\}$, então a Proposição 4.1.1 (ii) afirma que existem β_1, $\gamma_1 \in \mathbb{P}^1(\mathbb{F}_q)$ tais que $\varphi(\beta_1) = \varphi(\gamma_1) = \alpha$, onde β_1 é φ-periódico e γ_1 não é φ-periódico. Assim, γ_1 é o único vértice no nível 1 da árvore invertida enraizada em α. Como $\varphi = \psi \circ s \circ \psi$, temos que $\varphi(\gamma_1) = \alpha$ é equivalente a $\psi(\gamma_1)^2 = \psi(\alpha)$, o que implica $\mathrm{ord}(\psi(\gamma_1)) = 2\mathrm{ord}(\psi(\alpha))$, visto que $\mathrm{ord}(\psi(\alpha))$ é ímpar, pelo Lema 4.1.2 (i).

Por indução, se $j \leq \nu_2(q-1)$ e $\psi(\gamma_1), ..., \psi(\gamma_j) \in \mathbb{P}^1(\mathbb{F}_q)$ não são s-periódicos e satisfazem $s(\psi(\gamma_1)) = \psi(\alpha)$ e $s(\psi(\gamma_{i+1})) = \psi(\gamma_i)$ para todo $1 \leq i \leq j-1$, então

$$\text{ord}(\psi(\gamma_j)) = 2^j \text{ord}(\psi(\alpha)).$$

De fato, se $j = 1$, vimos que $\text{ord}(\psi(\gamma_1)) = 2\text{ord}(\psi(\alpha))$. Supondo que $\text{ord}(\psi(\gamma_{j-1})) = 2^{j-1}\text{ord}(\psi(\alpha))$, temos que $\psi(\gamma_j)^2 = s(\psi(\gamma_j)) = \psi(\gamma_{j-1})$, logo $\text{ord}(\psi(\gamma_j)) = 2\text{ord}(\psi(\gamma_{j-1})) = 2^j\text{ord}(\psi(\alpha))$. Pelo Lema 4.1.2 (i), $\text{ord}(\psi(\alpha))$ é um inteiro ímpar, logo $\nu_2(\text{ord}(\psi(\gamma_j))) = j$.

Seja T a árvore invertida de Gr_q enraizada em α. Queremos mostrar que $e = \nu_2(q-1)$ é a altura de T e que todos os vértices de T pertencentes ao nível $1 \leq j \leq e-1$ possuem dois filhos. Se $e = 1$, então $\text{ord}(\psi(\gamma_1)) \equiv 0 \pmod 2$. Pelo Lema 4.1.2 (ii), γ_1 é uma folha em T, logo T tem altura 1.

Suponha $e > 1$ e sejam $k \geq 1$ a altura de T, γ_j um vértice pertencente ao nível $j \leq k$ de T e $\gamma_1, ..., \gamma_j \in \mathbb{P}^1(\mathbb{F}_q)$ elementos tais que $\varphi^i(\gamma_j) = \gamma_{j-i}$ para $1 \leq i \leq j-1$ e $\varphi^j(\gamma_j) = \alpha$. Por construção, cada γ_i pertence ao nível i de T e $\text{ord}(\psi(\gamma_i)) = 2^i\text{ord}(\psi(\alpha))$ para cada $1 \leq i \leq j$. Se $j = k$, então γ_j não pode ter filhos, enquanto γ_{j-1} possui γ_j como filho. Como $\nu_2(\text{ord}(\psi(\gamma_{j-1}))) = j-1$ e $\nu_2(\text{ord}(\psi(\gamma_j))) = j$, concluímos, pelo Lema 4.1.2 (ii), que $j = k = e$. Se $1 \leq j < k$, então, pelo Lema 4.1.2 (ii), γ_j possui dois filhos e não é uma folha. □

4.2 Um algoritmo para construir polinômios *miar* via R-transformação a partir de um polinômio irredutível qualquer

Nesta seção, apresentamos um procedimento para encontrar um polinômio irredutível sobre $\mathbb{F}_q$ satisfazendo as condições do Teorema de Cohen. Para isto, faremos uso dos lemas a seguir.

Lema 4.2.1. *Seja n um inteiro positivo e suponha que $\nu_2(q^n-1) \geq 2$. Então*

$$\nu_2(q^{2n}-1) = \nu_2(q^n-1) + 1.$$

Demonstração. Por hipótese, temos $q^n - 1 \equiv 0 \pmod 4$. Segue que $q^n + 1 \equiv 2 \pmod 4$, ou seja, $\nu_2(q^n+1) = 1$. Assim,

$$\nu_2(q^{2n}-1) = \nu_2((q^n-1)\cdot(q^n+1)) = \nu_2(q^n-1) + 1.$$

□

Observação 4.2.2. Se $\nu_2(q^n-1) = 1$, então nada podemos concluir sobre $\nu_2(q^{2n}-1)$, além do fato de que $\nu_2(q^{2n}-1) > \nu_2(q^n-1)$. Como exemplos, destacamos: $\nu_2(3^3-1) = 1$ e $\nu_2(3^6-1) = 3$; $\nu_2(7-1) = 1$ e $\nu_2(7^2-1) = 4$; $\nu_2(31-1) = 1$ e $\nu_2(31^2-1) = 6$.

Lema 4.2.3. *Sejam f um polinômio mônico irredutível de grau n sobre $\mathbb{F}_q$ tal que $f(x) \neq x \pm 1$, e α uma raiz de f^R. Valem as seguintes afirmações:*

(i) O polinômio f^R é miar *de grau $2n$ ou $f^R(x) = g_1(x)g_2(x)$, onde g_1 e g_2 são polinômios mônicos irredutíveis de grau n sobre $\mathbb{F}_q$ tais que $g_1(\alpha) = g_2(1/\alpha) = 0$.*

(ii) Se f^R é redutível, então pelo menos um dos elementos α ou $1/\alpha$ não é φ-periódico.

Demonstração. (i) Considere o polinômio mônico irredutível $g(x) = 2^n f(x/2)$. Como $f(x) \neq x \pm 1$, temos $g(x) \neq x \pm 2$. Pela definição da R-transformação, temos $f^R = g^Q$. O resultado segue aplicando o Lema 2.2.3 ao polinômio g.

(ii) Sejam $\gamma = \varphi(\alpha)$ uma raiz de f e $f^R(x) = g_1(x)g_2(x)$, onde g_1 e g_2 satisfazem as condições do enunciado de (i). Primeiramente, mostramos, por contradição, que $\alpha \notin \{-1, 1\}$. Se este fosse o caso, teríamos $n = 1$, visto que g_1 e g_2 são irredutíveis. Então

$\gamma = \varphi(\alpha) = \pm 1$, logo $f(x) = x \pm 1$, uma contradição com a hipótese. Portanto $\alpha \notin \{-1, 1\}$, o que implica $\gamma \notin \{-1, 1\}$.

Se γ não é φ-periódico, então α e $1/\alpha$ não podem ser φ-periódicos, visto que $\varphi(\alpha) = \varphi(1/\alpha) = \gamma$. Se γ é φ-periódico, então o resultado segue da Proposição 4.1.1 (ii).

□

Seja f_0 um polinômio mônico irredutível de grau n diferente de $x \pm 1$ sobre $\mathbb{F}_q$. Se f_0^R for irredutível, definimos f_1 como sendo f_0^R. Se f_0^R for redutível, definimos f_1 como um fator de grau n de f_0^R que possua uma raiz não φ-periódica, de acordo com o Lema 4.2.3. Para cada $i \geq 1$, definimos f_{i+1} como sendo um fator irredutível de f_i^R. Por construção, a sequência $\{f_i\}_{i\geq 0}$ é formada apenas por polinômios irredutíveis e, pelo Lema 4.2.3, cada termo da sequência $\{f_i\}_{i\geq 0}$ possui o mesmo grau ou o dobro do grau em relação ao termo anterior. O Teorema a seguir determina a existência de um inteiro $s_1 + s_2$ tal que $f_{i+1} = f_i^R$ para todo $i \geq s_1 + s_2$.

Teorema 4.2.4. *Seja f_0 um polinômio mônico irredutível de grau n diferente de $x \pm 1$ sobre $\mathbb{F}_q$ e considere a sequência $\{f_i\}_{i\geq 0}$ definida acima. Se $\nu_2(q^n - 1) = e_1$ e $\nu_2(q^{2n} - 1) = e_2$, então existem inteiros $s_1 \leq e_1$, $s_2 = e_2 - e_1$ tais que*

(i) $f_0, ..., f_{s_1}$ são irredutíveis de grau n;

(ii) $f_{s_1+1}, ..., f_{s_1+s_2}$ são irredutíveis de grau $2n$;

(iii) $f_{s_1+s_2+j}$ é miar *de grau $2^{1+j}n$ para todo $j \geq 1$.*

Demonstração. Seja $\beta_0 \in \mathbb{F}_{q^n}$ uma raiz de f_0. Pela definição da R-transformação, podemos construir uma sequência $\{\beta_i\}_{i\geq 0}$, onde cada elemento β_i é uma raiz de f_i em alguma extensão de $\mathbb{F}_q$ e $\beta_i = \varphi(\beta_{i+1})$. Logo, se β_i pertence ao nível k_i de uma árvore invertida em Gr_{q^r}, $r \geq 1$, e não é uma folha, então β_{i+1} pertence ao nível $k_i + 1$ desta mesma árvore.

(i) O vértice β_0 pertence ao nível $k \geq 0$ de uma árvore T de Gr_{q^n} enraizada em um elemento φ-periódico γ. Se f_0^R for irredutível, então $f_1 = f_0^R$ possui grau $2n$, logo $s_1 = 0$. Se f_0^R for redutível, então f_1 é escolhido de forma que β_1 não é φ-periódico, e β_1 pertence ao nível $k+1$ de T. Pela Proposição 4.1.3, a árvore T possui altura e_1. Então, o vértice β_{e_1-k} é uma folha em Gr_{q^n}, logo f_{e_1-k} possui grau n. Como $\deg(f_{i+1}) \geq \deg(f_i)$ para todo $i \geq 0$, segue que $f_0, ..., f_{s_1}$ possuem grau n, onde $s_1 = e_1 - k \leq e_1$.

(ii) Como β_{e_1-k} é uma folha em Gr_{q^n}, temos $\beta_{e_1-k+1} \in \mathbb{F}_{q^{2n}} \backslash \mathbb{F}_{q^n}$, pela definição de β_{e_1-k+1}. Logo, $f_{s+1} = f_{e_1-k+1}$ possui grau $2n$. Observamos que o vértice β_{e_1-k+1} pertence à árvore invertida T' enraizada em γ no grafo $\mathrm{Gr}_{q^{2n}}$. De fato, $\varphi(\beta_{e_1-k+1}) = \beta_{e_1-k}$, onde este último pertence ao nível e_1 de T', visto que $\varphi^{e_1}(\beta_{e_1-k}) = \gamma$ pelo item (i). Logo, β_{e_1-k+1} pertence ao nível e_1+1 de T'. Pela Proposição 4.1.3, a árvore T' possui altura e_2. Como o vértice β_{e_2-k} pertence ao nível e_2 de T', concluímos que β_{e_2-k} é uma folha em $\mathrm{Gr}_{q^{2n}}$, logo f_{e_2-k} possui grau $2n$. Segue que $f_{e_1-k+1}, ..., f_{e_2-k}$ possuem grau $2n$. Como $s_1 = e_1 - k$, temos que $e_2 - k = s_1 + s_2$, onde $s_2 = e_2 - e_1$. Portanto, $f_{s_1+s_2} = f_{e_2-k}$.

(iii) Pelo mesmo raciocínio utilizado no item (ii), $f_{s_1+s_2+1} = f_{e_2-k+1}$ possui grau $4n$ e o vértice β_{e_2-k+j} pertence ao nível $e_2 + j$ de uma árvore invertida enraizada em γ no grafo $\mathrm{Gr}_{q^{2^{1+j}n}}$, $j \geq 1$. Pela Proposição 4.1.3 e pelo Lema 4.2.1, tal árvore possui altura

$$\nu_2(q^{2^{1+j}n} - 1) = \nu_2(q^{2^j n} - 1) + 1.$$

Para $j = 1$, temos

$$\nu_2(q^{2^2 n} - 1) = \nu_2(q^{2n} - 1) + 1 = e_2 + 1,$$

logo, por indução, $\nu_2(q^{2^{1+j}n} - 1) = e_2 + j$. Portanto, o vértice β_{e_2-k+j} é uma folha em $\mathrm{Gr}_{q^{2^{1+j}n}}$. Assim, para cada $j \geq 1$, concluímos que $\beta_{e_2-k+j} \in \mathbb{F}_{q^{2^{1+j}n}} \backslash \mathbb{F}_{q^{2^j n}}$ e $f_{s_1+s_2+j} =$

$f^R_{s_1+s_2+j-1}$.

□

Observação 4.2.5. De acordo com o Lema 4.2.1, temos duas possibilidades para os valores e_1, e_2: $e_1 = 1$, $e_2 \geq 2$ ou $e_1 \geq 2$, $e_2 = e_1 + 1$. No primeiro caso, as raízes de f_0 devem ser todas φ-periódicas ou todas folhas, o que implica que f_1 possui grau n se, e somente se, as raízes de f_0 forem φ-periódicas, enquanto f_2 deve possuir grau maior que n. No segundo caso, apenas o polinômio f_{s_1+1} possui grau $2n$ e $f_{i+1} = f_i^R$ para todo $i \geq s_1$.

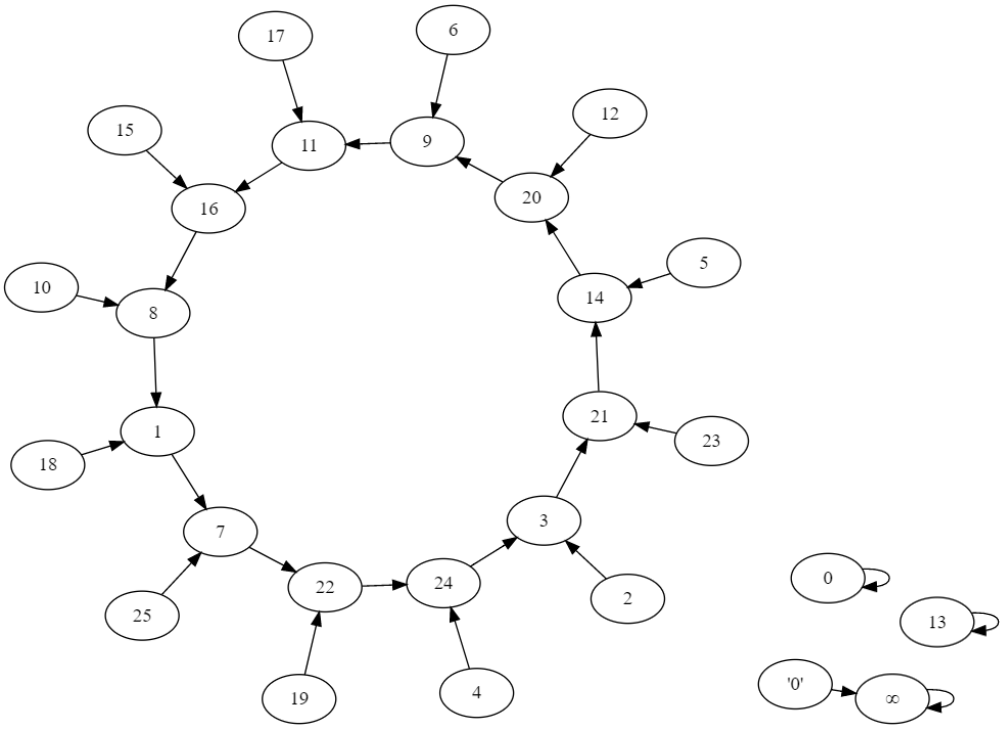
Observação 4.2.6. Se $f_0^R(x) = g_1(x)g_2(x)$ é redutível, então devemos definir f_1 como um polinômio dentre g_1, g_2 que não possui raízes φ-periódicas. A princípio, não precisamos saber qual(is) dos polinômios g_1, g_2 possui(em) esta propriedade. Basta escolher um deles, por exemplo $f_1 = g_2$ e verificar se o polinômio f_{e_1+1} possui grau maior que n. Caso não, concluímos que g_2 possui raízes φ-periódicas, logo devemos definir $f_1 = g_1$.

Observação 4.2.7. O Teorema 4.2.4 nos permite encontrar um inteiro n e um polinômio f satisfazendo todas as hipóteses do Teorema de Cohen. Para isso, considere um polinômio f'_0 mônico, irredutível e de grau n' sobre $\mathbb{F}_q$. Se $q \equiv 3 \pmod 4$ e n' é ímpar, então $e_1 = 1$ e, neste caso, $f = f'_{s_1+s_2}$ é um polinômio mônico irredutível de grau $n = 2n'$ par tal que $f(-1)f(1)$ não é um quadrado em $\mathbb{F}_q$ (caso contrário, $(f'_{s_1+s_2})^R$ seria redutível). Se $q \equiv 1 \pmod 4$ ou n' é par, então $e_1 \geq 2$ e $e_2 = e_1 + 1$, portanto $f = f'_{s_1}$ é um polinômio mônico irredutível de grau $n = n'$ tal que $f(-1)f(1)$ não é um quadrado em $\mathbb{F}_q$.

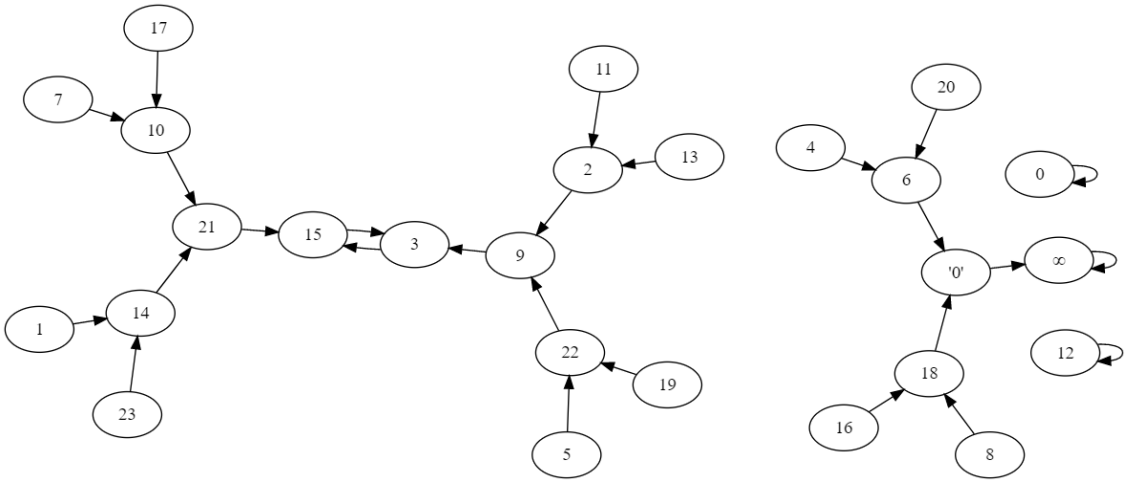
4.3 Exemplos

Nesta seção, apresentamos exemplos de grafos da forma Gr_q e de sequências de polinômios irredutíveis construídas com o auxílio do Teorema 4.2.4. Todas as imagens desta seção foram construídas com o auxílio do software Graphviz [2].

Exemplo 4.3.1. Seja $\mathbb{F}_{3^3} = \mathbb{F}_3(\alpha)$, onde α é uma raiz do polinômio primitivo $x^3 - x + 1 \in \mathbb{F}_3[x]$. Então $\mathbb{P}^1(\mathbb{F}_{3^3}) = \{\alpha^i \mid 0 \leq i \leq 25\} \cup \{0, \infty\}$. Como $\nu_2(3^3 - 1) = 1$, todas as árvores enraizadas em um elemento φ-periódico diferente de ± 1 em Gr_{3^3} possuem altura 1. Apresentamos a seguir o grafo Gr_{3^3}. Um elemento da forma α^i, $0 \leq i \leq 25$, é representado pelo vértice i, enquanto o elemento 0 é representado por '0', e ∞ por ∞.



Exemplo 4.3.2. Seja $\mathbb{F}_{5^2} = \mathbb{F}_5(\alpha)$, onde α é uma raiz do polinômio primitivo $x^2 + 2x + 3 \in \mathbb{F}_5[x]$. Então $\mathbb{P}^1(\mathbb{F}_{5^2}) = \{\alpha^i \mid 0 \leq i \leq 23\} \cup \{0, \infty\}$. Como $\nu_2(5^2 - 1) = 3$, todas as árvores enraizadas em um elemento φ-periódico diferente de ± 1 em Gr_{5^2} possuem altura 3. Apresentamos a seguir o grafo Gr_{5^2}. Um elemento da forma α^i, $0 \leq i \leq 23$, é representado pelo vértice i, enquanto o elemento 0 é representado por '0', e ∞ por ∞.



Exemplo 4.3.3. Seja $\mathbb{F}_{3^3} = \mathbb{F}_3(\alpha)$, onde α é uma raiz de $x^3 - x + 1 \in \mathbb{F}_3[x]$. Neste exemplo, construímos uma sequência de polinômios irredutíveis sobre $\mathbb{F}_{3^3}$ a partir do polinômio inicial $f_0 = x - \alpha^3$. Utilizando a notação do Teorema 4.2.4, $e_1 = \nu_2(3^3 - 1) = 1$, $e_2 = \nu_2(3^6 - 1) = 3$, $s_1 \leq 1$, $s_2 = 2$.

Temos

$$f_0^R(x) = x^2 + \alpha^3 x + 1 = (x - \alpha^2)(x + \alpha^2 + \alpha - 1) = (x - \alpha^2)(x - \alpha^{24}).$$

Como α^2 não é φ-periódico (vide Exemplo 4.3.1), definimos $f_1(x) = x - \alpha^2$. O polinômio $f_1^R(x) = x^2 + \alpha^2 x + 1$ é irredutível, logo devemos definir $f_2 = x^2 + \alpha^2 x + 1$, o que implica $s_1 = 1$ e $s_1 + s_2 = 3$.

Como

$$f_2^R(x) = x^4 - \alpha^2 x^3 - \alpha^2 x + 1 = (x^2 + \alpha x + \alpha^4)(x^2 - \alpha^{10} x - \alpha^9),$$

o polinômio f_3 deve ser escolhido como $x^2 + \alpha x + \alpha^4$ ou $x^2 - \alpha^{10} x - \alpha^9$. Tomamos, por exemplo, $f_3(x) = x^2 + \alpha x + \alpha^4$. Então o Teorema 4.2.4 afirma que $f_{3+j} = f_{2+j}^R$ para todo $j \geq 1$.

Exemplo 4.3.4. Sejam $\mathbb{F}_{5^2} = \mathbb{F}_5(\alpha)$, onde α é uma raiz do polinômio primitivo $x^2+2x+3 \in \mathbb{F}_5[x]$, e $f_0(x) = x^2 - 3 \in \mathbb{F}_5[x]$. Construímos uma sequência de polinômios irredutíveis sobre $\mathbb{F}_5$ a partir do polinômio f_0 através da R-transformação. Neste caso, $e_1 = \nu_2(5^2 - 1) = 3$, $e_2 = \nu_2(5^4 - 1) = 4$, $s_1 \leq 3$, $s_2 = 1$.

Como

$$f_0^R(x) = x^4 + 1 = (x^2 - 2)(x^2 - 3),$$

concluímos que as raízes de f_0 também são raízes de f_0^R, portanto as raízes de f_0 são α^3 e α^{15} (vide Exemplo 4.3.2). Logo, $f_1(x) = x^2 - 2$, cujas raízes são α^9 e α^{21}. Como

$$f_1^R(x) = x^4 + 4x^2 + 1 = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

podemos definir $f_2(x) = x^2 + 2x + 4$, que possui α^2 como raiz. Como

$$f_2^R(x) = x^4 - x^3 - 2x^2 - x + 1 = (x^2 + x + 2)(x^2 + 3x + 3),$$

definimos $f_3(x) = x^2 + x + 2$, que possui α^{11} como raiz.

Portanto, $s_1 = 3$ e $s_1 + s_2 = 4$. Pelo Teorema 4.2.4, $f_4 = f_3^R$ e $f_{4+j} = f_{3+j}^R$ para todo $j \geq 1$.

Referências

[1] Ahmadi, O.; Vega, G.: *On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields.* Finite Fields and Their Applications, 14(1), pp. 124-131, 2008.

[2] AT&T Labs Research and Contributors, Graphviz - Graph Visualization Software, http://graphviz.org

[3] Bassa, A.; Menares, R.: *Enumeration of a special class of irreducible polynomials in characteristic 2.* Acta Arithmetica, vol 194, pp. 51-57, 2020.

[4] Boneh, D.; Franklin, M.: *Identity-based encryption from the Weil pairing.* Annual international cryptology conference, pp. 213-229. Springer, Berlin, Heidelberg. 2001.

[5] Chartrand, G.; Lesniak, L.; Zhang, P.: *Graphs & digraphs.* CRC Press, 5 ed, 2011.

[6] Chen, B.; Ling, S.; Zhang, G.: *Enumeration formulas for self-dual cyclic codes.* Finite Fields and Their Applications 42, pp. 1-22, 2016.

[7] Chu, W.M.: *Construction of irreducible polynomials using cubic transformation.* Appl. Algebra Eng. Commun. Comput. 7(1), pp. 15–19, 1996.

[8] Cohen, S.D.: *The explicit construction of irreducible polynomials over finite fields.* Des. Codes Cryptogr. 2(2), pp. 169–174, 1992.

[9] Kyuregyan, M.K.: *Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics.* Finite Fields and Their Applications 9(1), pp. 39–58, 2003.

[10] Kyuregyan, M.K.: *Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics. II.* Finite Fields and Their Applications 12(3), pp. 357–378, 2006.

[11] Lidl, R.; Niederreiter, H.: *Introduction to finite fields and their applications*, Cambridge University Press, 1 ed, 1986.

[12] Meyn, H.: *On the construction of irreducible self-reciprocal polynomials over finite fields*, Appl. Algebra Eng. Comm. Comp., vol 1, no 1, pp. 43-53, 1990.

[13] Miller, V.S.: *Use of elliptic curves in cryptography.* Conference of the theory and application of cryptographic techniques, pp. 417-426. Springer, Berlin, Heidelberg. 1985.

[14] Pintoptang, U.; Laohakosol, V.; Tadee, S.: *Necklaces, Self-Reciprocal Polynomials, and q-Cycles.* International Journal of Combinatorics, ID 593749, 2014.

[15] Pommerening, K.: *Quadratic Equations in Finite Fields of Characteristic 2*, 2000. Disponível em: https://www.staff.uni-mainz.de/pommeren/MathMisc/QuGlChar2.pdf

[16] Rogers T.D.: *The graph of the square mapping on the prime fields.* Discrete Math. 148(1–3), pp. 317–324, 1996

[17] Ugolini, S.: *Graphs associated with the map $x \mapsto x+x^{-1}$ in finite fields of characteristic two.* Theory and Applications of Finite Fields, 579, pp.187-204, 2012.

[18] Ugolini, S.: *Graphs associated with the map $X \mapsto X+X^{-1}$ in finite fields of characteristic three and five.* Journal of Number Theory, 133(4), pp. 1207-1228. 2013.

[19] Ugolini, S.: *Sequences of binary irreducible polynomials.* Discrete Math. 313, pp. 2656–2662, 2013.

[20] Ugolini, S.: *On the iterations of certain maps $X \mapsto K \cdot (X+X^{-1})$ over finite fields of odd characteristic.* Journal of Number Theory, 142, pp. 274-297, 2014.

[21] Ugolini, S.: *Sequences of irreducible polynomials without prescribed coefficients over odd prime fields.* Designs, Codes and Cryptography, 75(1), pp. 145-155, 2015.

[22] Ugolini, S.: *On an iterated construction of irreducible polynomials over finite fields of even characteristic by Kyuregyan.* Czechoslovak Mathematical Journal, 66(1), pp. 243-250, 2016.

[23] Varshamov, R. R.; Garakov, G. A.: *On the Theory of Selfdual Polynomials over a Galois Field* (Russian). Bull. Math. Soc. Sci. Math. R. S. Roumanie, (N.S.) 13, pp. 403-415, 1969.

[24] Vasiga T., Shallit J.: *On the iteration of certain quadratic maps over GF(p).* Discrete Math. 277(1–3), pp. 219–240, 2004.

[25] Wu, Y.; Yue, Q.; Fan, S.: *Self-reciprocal and self-conjugate-reciprocal irreducible factors of xn-λ and their applications.* Finite Fields and Their Applications 63, 101648, 2020.

[26] Zadeh, A.A.: *Division and inversion over finite fields.* Cryptography and Security in Computing, pp. 117-129, 2012.