# Universidade Estadual de Campinas

FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

Departamento de Telemática


## Códigos Cíclicos sobre Anéis Locais e suas Relações com a Transformada Discreta de Fourier


**Ingrid Araújo Sampaio**

**Orientador: Prof. Dr. Reginaldo Palazzo Júnior**


Dissertação apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para obtenção do título de **Mestre em Engenharia Elétrica**.

**Banca Examinadora:**

| | |
|---|---|
| Prof. Dr. Reginaldo Palazzo Júnior | DT/FEEC / UNICAMP |
| Prof. Dr. Yuzo Iano | DECOM/FEEC/UNICAMP |
| Prof. Dr. Carlos Eduardo Câmara | FCC/USF |


Campinas, SP

26 de Julho de 2007

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

Sa47c

Sampaio, Ingrid Araújo
Códigos cíclicos sobre anéis locais e suas relações com a transformada discreta de Fourier / Ingrid Araújo Sampaio. -- Campinas, SP: [s.n.], 2007.

Orientador: Reginaldo Palazzo Júnior
Dissertação (Mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Anéis locais. 2. Galois, Teoria de. 3. Teoria da codificação. 4. Fourier, Transformações de. I. Palazzo Júnior, Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: Cyclics codes on local rings and its relations with the discrete transformed of Fourier.
Palavras-chave em Inglês: Local rings, Extension Galois, Theory of codification, Discrete Transformed of Fourier.
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Carlos Eduardo Câmara e Yuzo Iano.
Data da defesa: 26/07/2007
Programa de Pós-Graduação: Engenharia Elétrica

## COMISSÃO JULGADORA - TESE DE MESTRADO

**Candidata:** Ingrid Araújo Sampaio

**Data da Defesa:** 26 de julho de 2007

**Título da Tese:** "Códigos Cíclicos sobre Anéis Locais e suas Relações com a Transformada Discreta de Fourier"

Prof. Dr. Reginaldo Palazzo Júnior (Presidente): _____

Prof. Dr. Carlos Eduardo Câmara: _____

Prof. Dr. Yuzo Iano: _____

# AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, pela permissão da conclusão deste trabalho, e por ter me abençoado a todo momento.

Gostaria de agradecer em especial ao meu orientador, Prof. Reginaldo Palazzo Júnior, pela atenção, incentivo, paciência e amizade.

Aos professores da Banca Examinadora: Prof.Carlos Eduardo Camara e o Prof. Yuzo Iano, pelas sugestões e leitura que leveram ao enriquecimento deste trabalho.

A toda minha família, em especial a meus pais, mainha Zelina, painho Vavá, vó Maçú, meu avô Sampaio, Kika, Allan, Tia Telma, Tio Waltinho, Tia Vanusa, Lando, Tia Vilmara, Linho, Gliciane, Larissa, Jaciara, Márcio, Airam.

A meu esposo Rinaldo pelo incentivo, carinho e paciência.

A todos os meus amigos que direta ou indiretamente contribuíram para que esta oportunidade fosse concedida, em especial a Antonio Hudson, Dona Graça, Alana Paula, Elayne, Alana Seibert, Tia Rita, Orlandinho, Thaís Barreto, Dayanne, Polyane, Márcia Braga, Lúcio, Neto, Josimar, Renata Marcuz, Tia Gloria, Viviane, Jaqueline, Márcio, Gilmara, Patrícia Mendonça, Íris, Fabiana, Valtemir, Nolmar, Liliane e Gilhiarde.

Ao Programa de Moradia Estudantil-PME da Unicamp, em particular as assistentes sociais Patrícia, Cibele, Sônia, Mara e a Profa. Maria Tereza.

Aos amigos e professores da graduação João Paulo, Afonso, Flávio, Jaime, Valter, Eurivalda, Humberto, Eduardo e Chagas.

Ao CNPq, pelo apoio financeiro durante um ano e três meses.

# DEDICATÓRIA

*À meu esposo, Rinaldo Vieira da Silva Júnior,*
*à meus pais, Wilian Araújo de Castro e Washington José F. Sampaio e a meus avós, Zelina Araújo de Castro(in memorian), Valdimiro Matias de Castro e Maximiana Maria de Jesus.*

# SUMÁRIO

# RESUMO

Neste trabalho apresentamos algumas relações existentes entre códigos cíclicos e a transformada discreta de Fourier ambos sobre anéis locais. Para isso, é necessário a identificação do grupo das unidades associado a cada um dos anéis considerados. Como conseqüência, códigos cíclicos sobre tais anéis podem ser construídos. Em seguida, construímos geradores de seqüências através dos registros de deslocamento com realimentação linear (LFSR), a partir dos polinômios geradores, cujos coeficientes pertencem a um corpo finito e a um anel comutativo finito local com identidade. Finalmente, realizamos a transformada discreta de Fourier por meio do polinômio gerador dos códigos cíclicos sobre anéis locais.

# ABSTRACT

In this research we present some existing relationships between cyclic codes and discrete Fourier transform both local rings. For this, it is necessary to identify the groups of unit associated with each corresponding local ring. As a consequence, cyclic codes over these rings may be constructed. Next, we construct sequence generators by use of linear feedback shift register (LFSR), from generator polynomials whose coefficients belong either to finite field or to a local finite commutative ring with identity. Finally, the discrete Fourier transform is realized by use of the generator polynomial of cyclic codes over local rings.

# Lista de Símbolos

| | | |
|---|---|---|
| $*$ | - | Operação binária sobre um conjunto |
| $\|.\|$ | - | Ordem de um conjunto |
| $\times$ | - | Produto direto de grupos |
| $\langle a \rangle$ | - | Subgrupo gerado por $a$ |
| $\bar{a}$ | - | Classe de equivalência |
| $\langle p(x) \rangle$ | - | Anel gerado pelo polinômio $p(x)$ |
| $\bar{x}$ | - | Classe lateral |
| $a \sim b$ | - | Relação de equivalência entre $a$ e $b$ |
| $G/H$ | - | Grupo quociente de um grupo $G$ por um subgrupo normal $H$ |
| $H \leq G$ | - | $H$ é subgrupo de um grupo $G$ |
| $\alpha$ | - | Raiz de um polinômio |
| $\beta$ | - | Elemento primitivo ou zero de um polinômio pertencente a $\mathbb{F}_q$ |
| $\eta$ | - | Vetor localizador de um código BCH ou alternante |
| $\mathcal{A}$ | - | Alfabeto de um código |
| $a^{-1}$ | - | Elemento inverso de $a$ em um grupo |
| $\mathcal{C}$ | - | Código |
| $d_{mim}$ | - | Distância mínima de um código |
| $e$ | - | Elemento identidade em um grupo |
| $f$ | - | Elemento de $GR^*(p^m, r)$ |

| | | |
|---|---|---|
| $\bar{f}$ | - | Redução de $f$ módulo 2 |
| $\mathbb{F}$ | - | Corpo |
| $G$ | - | Matriz geradora de um código |
| $G$ | - | Grupo |
| $GFq, \mathbb{F}_q$ | - | Corpo algébrico de Galois ou corpo de Galois |
| $GFq[x], \mathbb{F}_q[x]$ | - | Anel de polinômios sobre $GF(q)$ |
| $G_s$ | - | Subgrupo cíclico do grupo multiplicativo $R^*$ |
| $GR(q, r)$ | - | Extensão do anel de Galois de grau $r$ |
| $GR^*(q, r)$ | - | Grupo das unidades de $GR(p^m, r)$ |
| $g(x)$ | - | Polinômio gerador de um código |
| $H$ | - | Subgrupo de um grupo |
| $H$ | - | Matriz verificação de paridade |
| $I$ | - | Matriz identidade |
| $k$ | - | Dimensão de um código |
| mdc(.,.) | - | Maximo divisor comum |
| $m_i(x)$ | - | Polinômio minimal associado ao elemento $\beta^i$ sobre $GF(q)$ |
| mmc(.,.) | - | Mínimo múltiplo comum |
| $M_i(x)$ | - | Polinômio minimal associado ao elemento $\beta^i$ sobre $R^*$ |
| $n$ | - | Comprimento de um código |
| $L$ | - | Subanel de um anel |
| $r$ | - | Taxa de um código |
| $r$ | - | Grau da extensão de Galois |
| $A$ | - | Anel |
| $R_p(f)$ | - | Redução de $f$ módulo $p$ |
| $t$ | - | Capacidade de correção de erros de um código |
| $\underline{v}$ | - | Palavra-código |
| $\mathbb{Z}$ | - | Conjunto dos números inteiros |
| $\mathbb{Z}_n$ | - | Conjunto dos números inteiros módulo $n$ |

# LISTA DE TABELAS

# LISTA DE FIGURAS

# CAPÍTULO 1

# INTRODUÇÃO

## 1.1 Apresentação do Problema

Os códigos cíclicos formam uma ampla classe de códigos corretores de erros de grande importância teórica e prática. A importância teórica vem do fato de que vários resultados da álgebra abstrata, em particular corpos finitos, mostram-se bastante úteis para caracterizar as propriedades algébricas desta classe de códigos. Já a importância na prática vem do fato de que os circuitos que realizam a codificação são menos complexos do que aqueles para códigos lineares em geral. Entretanto, os códigos cíclicos não apresentam, na maioria das vezes, propriedades ótimas com relação à distância mínima e taxa, isto é, valores de distâncias mínimas grandes são obtidas ao custo de "baixas"taxas.

Os códigos BCH formam uma classe importante de códigos cíclicos. Uma característica desta importância está relacionada com a simplicidade de geração de códigos, tornando-os candidatos a serem utilizados em aplicações práticas. Os códigos binários foram descobertos por R. C. Bose e D. K. Chaudhuri em 1960 e independentemente por A. Hocquenghem em 1959 e representam uma generalização dos códigos de Hamming, permitindo múltipla correção de erros. A generalização dos códigos BCH binários, a subclasse mais importante é formada pelos códigos Reed-Solomon, os quais foram introduzidos por Reed e Solomon em 1960, independentemente dos trabalhos de Hocquenghem, Bose e Chaudhuri.

Interlando em [3] descreve sobre as principais classes de códigos corretores de erros definidos sobre anéis de inteiros residuais $\mathbb{Z}_q$, onde $q$ é uma potência de primo. Abordando a importância dos códigos cíclicos, de Hamming, BCH e Reed-Solomon, onde grande parte dos códigos conhecidos na literatura estão definidos sobre corpos, estrutura algébrica mais complexa que anéis. Portanto, códigos sobre anéis podem ser mais apropriado a determinadas aplicações.

Vamos agora descrever mais precisamente o problema que será tratado neste trabalho partindo do trabalho desenvolvido encontrado nas referências [1],[2], [3], [4] e [15].

É sabido que a transformada discreta de Fourier está intimamente ligada a construção de códigos. Então, nosso objetivo, o qual atingimos, é mostrar que é possível desenvolver técnicas por meio da transformada discreta de Fourier sobre anéis locais onde utilizamos o mesmo procedimento que é feito sobre corpos finitos, através do uso dos códigos cíclicos. Sabendo que, a estrutura sobre anéis embute um grau de dificuldade para a determinação do grupo das unidades, por este motivo, podemos dizer que existe uma forte possibilidade de aplicação desta técnica em criptografia.

Portanto, apresentamos duas aplicações das extensões de Galois sobre anéis locais. A partir da cardinalidade do grupo das unidades dos anéis locais, iremos:

- identificar o polinômio gerador para a construção de um circuito linear de deslocamento com realimentação (LFSR), gerando seqüências pseudo-aleatórias;

- mostrar que a transformada discreta de Fourier pode ser obtida através do polinômio gerador dos códigos cíclicos sobre anéis locais;

Os suportes computacionais utilizados foram o Maple, Matlab, X-fig e o Gimp.

## 1.2 Descrição do Trabalho

Esta dissertação está organizada em seis capítulos, sendo que o conteúdo dos próximos cinco capítulos é como se segue:

**Capítulo 2:** Fazemos uma breve revisão dos principais conceitos básicos relacionados a álgebra abstrata e aos códigos corretores de erros, os quais serão primordiais para a fundamentação deste trabalho;

**Capítulo 3:** Apresentamos alguns dos principais conceitos da transformada discreta de Fourier sobre corpos finitos. Em seguida, uma revisão de códigos de bloco lineares sobre corpos finitos, teoria esta necessária para o desenvolvimento deste trabalho, descrevendo espectralmente os códigos cíclicos sobre corpos finitos. Finalmente, apresentamos procedimentos de como são feitas as extensões Galoisianas sobre corpos dos códigos BCH, Reed-Solomon e Alternantes.

**Capítulo 4:** Neste capítulo revisamos a construção de códigos cíclicos sobre anéis locais. De particular interesse, consideramos os códigos BCH e Alternantes provenientes de extensões Galoisianas de dimensão $r$ sobre anéis de inteiros módulo $q = p^m$, $m \geq 2, p$ primo.

**Capítulo 5:** Apresentamos a cardinalidade de alguns dos grupos das unidades sobre anéis locais e, através dos polinômios geradores, construímos geradores de seqüências sobre corpos finitos bem como para o caso em que a seqüência pertence a um anel comutativo finito local com identidade por meio dos registros de deslocamento com realimentação linear (LFSR), gerando códigos cíclicos. E, finalmente, realizamos a transformada discreta de Fourier através do polinômio gerador do código cíclico sobre anéis locais.

**Capítulo 6:** Apresentamos as conclusões do trabalho bem como propomos alguns tópicos para serem abordados em pesquisas futuras.

# CAPÍTULO 2

# CONCEITOS PRELIMINARES

Neste capítulo, apresentamos alguns conceitos preliminares sobre estruturas algébricas e códigos que servirão de base para o desenvolvimento deste trabalho. Estes conceitos podem ser encontrados nas referências [3],[4] e [6].

Na Seção 2.1 apresentamos as principais definições e propriedades das estruturas de grupo, anel, corpo e espaço vetorial, as quais são de fundamental importância na teoria de códigos corretores de erros, pois facilitam o processo de codificação. Na Seção 2.2 apresentamos uma breve introdução dos conceitos de códigos corretores de erros.

## 2.1 Álgebra Abstrata e Álgebra Linear

### 2.1.1 Grupo

**Definição 1** (Operação Binária)**.** *Uma operação binária $*$ sobre um conjunto $S$ é uma regra que associa algum elemento de $S$ a cada par ordenado $(a, b)$ de elementos de $S$ ($a*b$ denotará o elemento associado a $(a, b)$ através de $*$).*

Está implícito na Definição 1 a exigência que $S$ seja fechado sob a operação binária, e que apenas um único elemento é associado a cada par ordenado de $S$.

**Definição 2** (Grupo)**.** *Um grupo $\langle G, * \rangle$ é um conjunto não vazio $G$, com uma operação binária $*$ sobre $G$, tal que as seguintes propriedades são satisfeitas:*

*(i) A operação binária $*$ é associativa, isto é, $(a * b) * c = a * (b * c)$, para todo $a, b, c \in G$;*

*(ii) Existe um elemento $e$ em $G$ tal que $e * x = x * e = x$ para todo $x \in G$.(Este elemento é um elemento identidade para $*$ sobre $G$);*

*(iii) Para cada $a$ em $G$, existe um elemento $a'$ em $G$ com a propriedade de que $a' * a = a * a' = e$. (O elemento $a'$ é um inverso de $a$ com respeito a operação $*$).*

**Definição 3** (Grupo Abeliano)**.** *Um grupo $G$ é abeliano se a sua operação binária $*$ for comutativa, isto é, $a * b = b * a$, para todo $a, b \in G$.*

**Definição 4.** *Seja $n$ um inteiro positivo e sejam $s$ e $t$ inteiros quaisquer. O resto $r$ quando $s + t$ é dividido por $n$ segundo o algoritmo da divisão de Euclides é a soma de $s$ e $t$ módulo $n$. Assim, temos que $\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$.*

**Teorema 1.** *[4] O conjunto $\mathbb{Z}_n$ é um grupo sob a operação de adição módulo $n$.*

**Definição 5.** *Se $G$ é um grupo finito, então a ordem de $G$, $|G|$, é o número de elementos de $G$.*

**Definição 6** (Subgrupo)**.** *Se um subconjunto $H$ de um grupo $G$ é fechado sob a operação binária de $G$ e se $H$ forma um grupo sob esta operação binária, então $H$ é um subgrupo de $G$. Denotamos por $H \leq G$.*

**Teorema 2.** *[3] Seja $G$ um grupo e seja $a \in G$. Então*

$$H = \{a^n \mid n \in \mathbb{Z}\} \tag{2.1}$$

*é um subgrupo de $G$ e é o menor subgrupo de $G$ que contém $a$, isto é, todo subgrupo contendo $a$, contém $H$. Este grupo $H$ é o subgrupo cíclico $\langle a \rangle$ de $G$ gerado por $a$.*

**Definição 7.** *Seja $H$ um subgrupo de um grupo $G$. O subconjunto de $G$*

$$aH = \{ah \mid h \in H\} \tag{2.2}$$

*é a classe lateral à esquerda de $H$ contendo $a$. Analogamente,*

$$Ha = \{ha \mid h \in H\} \tag{2.3}$$

*é a classe lateral à direita de $H$ contendo $a$.*

**Teorema 3** (Teorema de Lagrange)**.** *[4] Seja $H$ um subgrupo de um grupo finito $G$. Então a ordem de $H$ é um divisor da ordem de $G$, ou seja, $|H|\cdot$ (número de classes laterais de $G$ com relação a $H$) $= |G|$.*

**Definição 8** (Grupo Quociente)**.** *Seja $H$ um subgrupo normal de $G$. Então, o conjunto das classes laterais de $H$ formam um grupo, denotado por $G/H$, sob uma operação binária $(aH)(bH) = (ab)H$. O grupo $G/H$ é chamado grupo quociente de $G$ módulo $H$.*

**Corolário 1.** *[4] Todo grupo cuja ordem é um número primo é cíclico.*

**Definição 9.** *A ordem $n$ de um elemento $g$ pertencente a um grupo $G$ é o menor inteiro positivo tal que $g^n = e$, onde $e$ é a identidade do grupo.*

**Teorema 4.** *[4] A ordem de qualquer elemento de um grupo finito divide a ordem do grupo.*

**Definição 10** (Isomorfismo de Grupos)**.** *Seja um homomorfismo onde a função $\phi : G \longrightarrow H$ é bijetora. Dizemos que $G$ e $H$ são isomorfos e denotamos $G \cong H$.*

### 2.1.2 Anel

**Definição 11** (Anel Comutativo com Unidade)**.** *Um anel $(A, +, \cdot)$ é um conjunto $A$ com duas operações binárias, que denotaremos por $+$ e $\cdot$, tais que:*

*(i)* $(A, +)$ *é um grupo abeliano;*

*(ii)* $(A\backslash\{0\}, \cdot)$ *é um grupo abeliano;*

*(iii)* $\cdot$ *é associativa, ou seja,* $(x \cdot y) \cdot z = x \cdot (y \cdot z)\ \forall\ x, y, z \in A$.

*(iv)* $\cdot$ *é distributiva relativamente a* $+$*, ou seja,*

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

*e*

$$(y + z) \cdot x = y \cdot x + z \cdot x\ \forall\ x, y, z \in A.$$

*(v)* $\exists\ 1 \in A;\quad 1 \cdot a = a \cdot 1 = a\ \ \forall\ a \in A$

**Definição 12** (Subanel)**.** *Seja* $(A, +, \cdot)$ *um anel. Dizemos que um subconjunto* $L \subset A,\ L \neq \emptyset$*, é um subanel de* $A$*, se e somente se:*

*(i)* $L$ *é fechado para ambas as operações de* $A$*, isto é,* $\forall\ x, y,\ x, y \in A \Longrightarrow x+y \in L$ *e* $x \cdot y \in L$;

*(ii)* $(L, +, \cdot)$ *também é um anel.*

**Definição 13** (Homomorfismo de Anéis)**.** *Sejam* $A$ *e* $B$ *anéis. Uma função (mapeamento)* $\phi : A \longrightarrow B$ *é um homomorfismo se as condições abaixo são satisfeitas, para* $x, y \in A$ *:*

*(i)* $\phi(x + y) = \phi(x) + \phi(y)$;

*(ii)* $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$;

**Definição 14** (Isomorfismo de Anéis)**.** *Um isomorfismo de* $A$ *e* $B$ *é um homomorfismo* $\phi : A \longrightarrow B$ *bijetor. Dizemos então que* $A$ *e* $B$ *são isomorfos.*

**Proposição 1** (Teorema do Isomorfismo)**.** *[6] Dado um homomorfismo sobrejetor* $h : A \longrightarrow B$*. Existe um isomorfismo* $\widetilde{h} : A/N(h) \longrightarrow B$ *tal que* $h = \widetilde{h} \circ \varphi$

**Teorema 5.** *[4] Se* $A$ *é um anel com unidade, então esta unidade* $1$ *é a única identidade multiplicativa do anel.*

**Definição 15.** *Seja* $A$ *um anel:*

*(i) Um elemento não nulo $x$ de $A$ é chamado um divisor de zero se existe um elemento não nulo $y$ em $A$ tal que $x \cdot y = 0$ ou $y \cdot x = 0$;*

*(ii) Seja $A$ um anel com unidade. Um elemento $x$ de $A$ é chamado invertível em $A$ se existe $x^{-1}$ em $A$ tal que $x \cdot x^{-1} = x^{-1} \cdot x = 1$.*

**Definição 16** (Ideal num Anel Comutativo)**.** *Seja $A$ um anel comutativo. Dizemos que um subconjunto $I \subset A, I \neq \emptyset$, é um ideal em $A$ se, e somente se,:*

$(i)$ $\forall\ x, y \in I \Longrightarrow x - y \in I$

$(ii)$ $\forall\ a \in A$ *e* $x \in I \Longrightarrow ax \in I$

**Proposição 2.** *[6] Seja $I$ um ideal num anel comutativo $A$. Então:*

*(i)* $0 \in I$;

*(ii)* $\forall\ a \in I \Longrightarrow\ -a \in I$;

*(iii)* $\forall\ a, b \in I \Longrightarrow\ a + b \in I$;

*(iv) Se o anel $A$ possui unidade e se existe um elemento inversível $u \in A$ tal que $u \in I$ então $I = A$.*

**Definição 17** (Ideal à direita(à esquerda))**.** *Um subanel $L$ de um anel $A$ é um ideal à direita (à esquerda) em $A$ se $bL \subseteq N (Lb \subseteq N)$ para todo $b \in A$. Se $L$ é simultaneamente um ideal à direita e à esquerda em $A$, dizemos que $L$ é um ideal em $A$.*

Sejam $A$ um anel e $L$ um ideal de $A$. Então, $N$ determina uma relação de equivalência em $A$ dada por:

$$x \sim x' \Longleftrightarrow x \sim x' \in L \tag{2.4}$$

Estas classes de equivalência são os conjuntos

$$\bar{x} = x + L = \{x + l \mid l \in L\} \tag{2.5}$$

com $x \in A$, e são chamadas de classes laterais aditivas de $L$ em $A$. Todo elemento de $A$ está contido em exatamente uma classe lateral $\bar{x}$. Denotaremos por $A/L$ o conjunto dessas classes

laterais. Define-se em $A/L$ duas operações, a partir das operações de adição e multiplicação em $A$, da seguinte forma:

$$\bar{x} + \bar{y} = (x + L) + (y + L) = \overline{x + y} = (x + y) + L \tag{2.6}$$

e

$$\bar{x} \cdot \bar{y} = (x + L) \cdot (y + L) = \overline{x \cdot y} = (x \cdot y) + L \tag{2.7}$$

Pode-se verificar que estas definições das operações não dependem da escolha de representantes em $\bar{x}$ e $\bar{y}$. Mais ainda, mostra-se que $A/L$ é um anel em relação às operações introduzidas, conhecido como anel quociente de $A$ módulo $L$.

**Definição 18** (A-módulo)**.** *Seja $A$ um anel. Um $A$-módulo(à esquerda) consiste de um grupo abeliano $N$ junto com uma operação de multiplicação externa de cada elemento de $N$ por cada elemento de $A$(à esquerda) tal que para todo $\lambda, \beta \in N$ e $k, t \in A$, as seguintes condições são satisfeitas:*

*(i)* $(k \cdot \lambda) \in N$

*(ii)* $k \cdot (\lambda + \beta) = k\lambda + k\beta$

*(iii)* $(k + t) \cdot \lambda = k \cdot \lambda + t \cdot \lambda$

*(iv)* $(k \cdot t)\lambda = k \cdot (t \cdot \lambda)$

Um $A$-módulo assemelha-se com um espaço vetorial exceto que os escalares precisam somente formar um anel. Se $A$ é um anel com unidade e $1 \cdot \lambda = \lambda$ para todo $\lambda \in N$, então $N$ é um $A$-módulo unitário.

**Definição 19** ($A$-módulo Cíclico)**.** *Um $A$-módulo $N$ é cíclico se existe $\lambda \in N$ tal que $N = \{k \cdot \lambda \mid k \in A\}$.*

Portanto, um $A$-módulo cíclico é gerado por um único elemento. A idéia de um conjunto de geradores para um $A$-módulo é a generalização natural da idéia de um conjunto de vetores geradores de um espaço vetorial.

**Definição 20** (Ideal Primo)**.** *Seja $P$ um ideal num anel comutativo $A$. Dizemos que $P$ é um ideal primo se $P \neq A$ e se é verdade a seguinte frase:*

$$\forall\ x, y \in A,\ x \cdot y \in P \Longrightarrow x \in P \text{ ou } y \in P \tag{2.8}$$

**Definição 21** (Ideal Maximal)**.** *Um ideal $M \neq A$ chama-se maximal se, para qualquer ideal $I$ de $A$, a propriedade $M \subseteq I$ implica $I = M$ ou $I = A$.*

**Teorema 6.** *[6] Seja $A$ um anel comutativo com identidade e $I$ um ideal de $A$ com $I \neq A$. Então:*

*(i) $A/I$ é um domínio de integridade se e somente se $I$ é primo;*

*(ii) $A/I$ é um corpo se e somente se $I$ é ideal maximal*

*(iii) todo ideal maximal de $A$ é primo;*

**Definição 22** (Anel Local)**.** *Um anel $R$ é chamado um anel local se $R$ possui somente um ideal maximal.*

### 2.1.3 Corpo

**Definição 23** (Corpo)**.** *Um anel $\mathbb{F}$, comutativo com unidade, recebe o nome de corpo se todo elemento não nulo de $\mathbb{F}$ admite simétrico multiplicativo. Ou seja,*

$$\forall\ a \in \mathbb{F},\ a \neq 0 \Longrightarrow \exists\ b \in \mathbb{F} \mid a \cdot b = 1 \tag{2.9}$$

*Podemos também falar que um corpo $\mathbb{F}$ é um anel de divisão comutativo.*

Portanto, dizemos que $\mathbb{F}$ é um corpo sob as operações binárias $+$ e $\cdot$ se, e somente se, $\mathbb{F}$ constutui um grupo abeliano sob estas operações e, para a operação $\cdot$, é válida a lei distributiva. Assim, podemos dizer que um corpo apresenta no mínimo dois elementos: as identidades das operações $+$ e $\cdot$. O número de elementos num corpo é a ordem do mesmo e um corpo onde este número é finito é chamado corpo finito.

**Exemplo 1.** *São exemplos de corpos: o conjunto dos números racionais e dos números reais sob adição e multiplicação usuais e o conjunto* $\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}$ *para p primo sob adição e multiplicação módulo p.*

**Definição 24** (Subcorpo)**.** *Um subcorpo é um subconjunto de um corpo que tem estrutura de corpo sob as operações herdadas do mesmo.*

Nosso trabalho será desenvolvido assumindo que os corpos são finitos, pois estes são usados na maioria das construções dos códigos conhecidos. Estes corpos são também conhecidos como corpos algébricos de Galois ou corpos de Galois e são denotados por $GF(q)$ ou $\mathbb{F}_q$, onde $q \geq 2$ é o número de elementos do corpo.

**Definição 25** (Polinômio)**.** *Um polinômio de grau* $n-1$ *sobre um corpo* $\mathbb{F}_q$ *é escrito como:*

$$p(x) = p_{n-1}x^{n-1} + p_{n-2}x^{n-2} + ... + p_1x + p_0, \tag{2.10}$$

*onde* $x$ *é uma variável e os coeficientes* $p_i's,\ 0 \leq i \leq n-1,\ i \in \mathbb{Z},$ *são elementos de* $\mathbb{F}_q$*.*

**Definição 26** (Polinômio Mônico)**.** *Um polinômio mônico é aquele cujo coeficiente líder(coeficiente da variável de maior expoente)* $p_{n-1}$ *é igual a* $1$*, a identidade multiplicativa de* $GF(q)$*.*

**Definição 27** (Polinômio Irredutível)**.** *Seja* $\mathbb{F}$ *um corpo. Dizemos que um polinômio* $p \in \mathbb{F}[X]$*(anel de polinômios) é irredutível em* $\mathbb{F}[X]$ *ou irredutível sobre* $\mathbb{F}$ *se:*

*(i)* $p \notin \mathbb{F}$ *(ou seja, p não é polinômio constante);*

*(ii) Dado* $f \in \mathbb{F}[X]$*, se* $f \mid p$ *então ou* $f \in \mathbb{F}^*$ *ou existe* $c \in \mathbb{F}^*$ *tal que* $f = cp$*.*

Sabemos que o conjunto de todos os polinômios sobre $\mathbb{F}_q$ forma um anel sob as operações usuais de soma e multiplicação de polinômios. Este anel é donotado por $GF(q)[x]$ ou $\mathbb{F}_q[x]$.

**Definição 28.** *Um elemento* $\beta \in \mathbb{F}_q$ *é uma raiz ou zero do polinômio* $p(x) \in \mathbb{F}_q[x]$ *se* $p(\beta) = 0$*.*

**Teorema 7.** *[4] Se G é um subgrupo multiplicativo do grupo* $\langle \mathbb{F}^*, \cdot \rangle$ *de elementos não nulos de um corpo* $\mathbb{F}$*, então G é cíclico.*

**Corolário 2.** *[4] O grupo multiplicativo de todos os elementos não nulos de um corpo finito sob a operação multiplicação deste corpo é cíclico.*

**Corolário 3.** *[4] Uma extensão (corpo de extensão) $E$ de grau $r$ de um corpo finito $\mathbb{F}_q$ é o conjunto dos polinômios sobre $\mathbb{F}_q$ módulo um polinômio irredutível de grau $r$.*

**Teorema 8.** *[4] Considere uma extensão finita de grau $r$ sobre o corpo $\mathbb{F}_q$. Então esta extensão tem $q^r$ elementos.*

**Teorema 9.** *[4] Todos os corpos de ordem $p^m$ são isomorfos.*

**Definição 29** (Polinômio Primo)**.** *Dizemos que um polinômio $p(x)$ sobre $\mathbb{F}_q$ é primo se ele for mônico e irredutível sobre $\mathbb{F}_q$.*

**Teorema 10.** *[4] O anel de polinômios módulo um polinômio $p(x)$ sobre $\mathbb{F}_q$ é um corpo se, e somente se, $p(x)$ é um polinômio primo.*

**Definição 30** (Elemento Primitivo)**.** *Um gerador do grupo multiplicativo de $\mathbb{F}_q$ é denominado um elemento primitivo de $\mathbb{F}_q$.*

**Corolário 4.** *[4] Todo corpo finito $\mathbb{F}$ contém um elemento primitivo.*

**Teorema 11.** *[3] Seja $\mathbb{F}^*$ o conjunto dos $q-1$ elementos não-nulos de $GF(q)$, onde $q = p^m$. Então, $\mathbb{F}^*$ é um grupo cíclico multiplicativo de ordem $p^m - 1$.*

**Teorema 12** (Garantia da Unicidade de $GF(p^m)$)**.** *[3] Todos os corpos finitos de ordem $p^m$ são isomorfos (diz-se que dois corpos $\mathbb{F}$ e $G$ são isomorfos se existe uma bijeção de $\mathbb{F}$ em $G$ a qual preserva adição e multiplicação).*

Portanto, todo corpo de Galois contém um elemento $\beta$, tal que todo elemento pertencente ao grupo multiplicativo do corpo finito pode ser expresso como uma potência de $\beta$.

**Definição 31** (Polinômio Minimal)**.** *[3] Seja $GF(q')$ um corpo finito e $GF(q)$ um subcorpo de $GF(q')$. Seja $\beta \in GF(q')$. O polinômio primo $p(x)$ de menor grau sobre $GF(q)$, tal que $p(\beta) = 0$, é chamado polinômio minimal de $\beta$ sobre $GF(q)$.*

**Teorema 13.** *[4] Considere os corpos $GF(q')$ e $GF(q)$ como definidos acima. Cada elemento $\beta$ de $GF(q')$ tem um único polinômio minimal sobre $GF(q)$. Mais do que isso, se $\beta$ tem $p(x)$ como seu polinômio minimal e um polinômio $g(x)$ tem $\beta$ como um zero, então $p(x)$ divide $g(x)$.*

### 2.1.4 Espaço Vetorial

**Definição 32** (Espaço Vetorial)**.** *Seja $\mathbb{F}$ um corpo. Um espaço vetorial sobre $\mathbb{F}$ consiste de um grupo abeliano $V$ sob adição junto com uma operação de multiplicação por escalar de cada elemento de $V$ por cada elemento de $\mathbb{F}$ à esquerda, tal que para todo $a, b \in \mathbb{F}$ e $\lambda, \beta \in V$, valem as seguintes propriedades:*

*(i)* $a \cdot \lambda \in V$;

*(ii)* $a \cdot (b \cdot \lambda) = (a \cdot b) \cdot \lambda$;

*(iii)* $(a + b) \cdot \lambda = (a \cdot \lambda) + (b \cdot \lambda)$;

*(iv)* $a \cdot (\lambda + \beta) = (a \cdot \lambda) + (a \cdot \beta)$;

*(v)* $1 \cdot \lambda = \lambda$, *onde* $1$ *é a unidade multiplicativa d e $K$;*

Os elementos de $V$ são vetores e os elementos de $K$ são escalares.

**Definição 33** (Combinação Linear)**.** *Seja $V$ um espaço vetorial sobre $K$. Os vetores em um subconjunto $S = \{\lambda_i \mid i \in I\}$ (onde $I$ é um conjunto de índices) de $V$ geram $V$ se para todo $\beta \in V$ tem-se que:*

$$\beta = a_1 \cdot \lambda_{i_1} + a_2 \cdot \lambda_{i_2} + ... + a_n \cdot \lambda_{i_n} \tag{2.11}$$

*para algum conjunto de $a_j \in K$ e $\lambda_{i_j} \in S, j = 1, ..., n$. Um vetor*

$$\sum_{j=1}^{n} a_j \cdot \lambda_{i_j} \tag{2.12}$$

*é chamado de combinação linear dos $\lambda_{i_j}$.*

**Definição 34** (Dimensão Finita)**.** *Um espaço vetorial sobre um corpo $K$ tem dimensão finita se existe um subconjunto finito de $V$ cujos vetores geram $V$.*

**Definição 35** (Linearmente Independentes)**.** *Os vetores em um subconjunto $S = \{\lambda_i \mid i \in I\}$ de um espaço vetorial $V$ sobre um corpo $K$ são linearmente independentes sobre $K$ se*

$$\sum_{j=1}^{n} a_j \cdot \lambda_{i_j} = 0 \tag{2.13}$$

*implica que $a_j = 0$ para $j = 1, ..., n$. Se os vetores não são linearmente independentes sobre $K$, dizemos que eles são linearmente dependentes sobre $K$.*

**Definição 36** (Base e Dimensão)**.** *Se $V$ é um espaço vetorial sobre um corpo $\mathbb{F}$, os vetores em um subconjunto $B = \{\beta_i \mid i \in I\}$ de $V$ formam uma base para $V$ sobre $\mathbb{F}$ se eles geram $V$ e são linearmente independentes. O número de elementos de $B$ é conhecido como a dimensão de $V$ sobre $\mathbb{F}$.*

### 2.1.5 Álgebra

**Definição 37** (Álgebra)**.** *Uma álgebra consiste de um espaço vetorial $V$ sobre um corpo $\mathbb{F}$, junto com uma operação binária de multiplicação sobre o conjunto $V$ de vetores, tal que para todo $a \in \mathbb{F}$ e $\lambda, \beta, \varphi \in V$, as seguintes condições são satisfeitas:*

*(i)* $(a \cdot \lambda) \cdot \beta = a \cdot (\lambda \cdot \beta) = \lambda \cdot (a \cdot \beta)$;

*(ii)* $(\lambda + \beta) \cdot \varphi = \lambda \cdot \varphi + \beta \cdot \varphi$;

*(iii)* $\lambda \cdot (\beta + \varphi) = \lambda \cdot \beta + \lambda \cdot \varphi$;

*Dizemos que $V$ é uma álgebra associativa sobre $\mathbb{F}$ se além das três condições acima,*

*(iv)* $(\lambda \cdot \beta) \cdot \varphi = \lambda \cdot (\beta \cdot \varphi)$, *para todo* $\lambda, \beta, \varphi \in V$.

**Teorema 14.** *[3] As classes residuais de polinômios módulo um polinômio $f(x)$ de grau $n$ formam uma álgebra de dimensão $n$ sobre o corpo dos coeficientes.*

**Teorema 15.** *[3] Seja $p(x)$ um polinômio com coeficientes em um corpo $\mathbb{F}$. Se $p(x)$ for irredutível em $\mathbb{F}$, isto é, se $p(x)$ não possuir fatores com coeficientes em $\mathbb{F}$, então a álgebra de polinômios sobre $\mathbb{F}$ módulo $p(x)$ será um corpo.*

O corpo de extensão de grau $m$ sobre $\mathbb{F}$ é formado tomando-se polinômios sobre $\mathbb{F}$, módulo um polinômio irredutível $p(x)$ de grau $m$. As classes residuais módulo um dado inteiro $n$ formam um anel sob adição e multiplicação módulo $n$, denotado por $\mathbb{Z}_n$. Portanto, quando $n$ é um primo $p$, então estas classes residuais formam um corpo de $p$ elementos, chamado corpo de Galois e denotado por $GF(p)$.

Um resultado da álgebra nos diz que o anel de polinômios sobre qualquer corpo finito tem pelo menos um polinômio irredutível de todo grau. O corpo de polinômios sobre $GF(p)$ módulo um polinômio irredutível de grau $m$ é chamado corpo de Galois de ordem $p^m$ e é denotado por $GF(p^m)$. Com isso concluímos que é sempre possível encontrar um corpo de $q = p^m$ elementos, onde $p$ é um primo. Pelo Teorema 14, o corpo $GF(p^m)$ é um espaço vetorial de dimensão $m$ sobre $GF(p)$, logo, tem $p^m$ elementos.

## 2.2 Códigos Corretores de Erros

Estaremos considerando somente alfabetos finitos. Inicialmente, o alfabeto $\mathcal{A}$ pode ser qualquer conjunto de símbolos. Entretanto, muitas vezes é conveniente que o mesmo seja "estruturado"para que a codificação e a decodificação sejam simplificadas. Entendemos por alfabetos "estruturados"aqueles que apresentam alguma estrutura algébrica, tal como grupo, anel ou corpo.

**Definição 38** (Espaço de Sequências)**.** *Um espaço de sequências $\mathcal{A}^I$ é o conjunto de todas as sequências $c = \{c_i \mid i \in I\}$ de elementos $c_i$ sobre algum alfabeto $\mathcal{A}$, onde $I$ é um conjunto de índices.*

**Definição 39** (Código)**.** *Um código $\mathcal{C}$ sobre um conjunto $\mathcal{A}$ é qualquer subconjunto não-vazio do espaço de sequências $\mathcal{A}^I$.*

**Definição 40** (Código de Bloco)**.** *Um código de bloco $\mathcal{C}$ de comprimento $n$(número natural) é qualquer subconjunto não-vazio do conjunto $\mathcal{A}^n$ de todas as sequências $c = \{c_i \mid 1 \leq i \leq n\}$, onde $c_i$ é denominada palavra-código.*

Um código de bloco é caracterizado por três parâmetros principais: seu comprimento, sua dimensão e sua distância mínima.

**Definição 41.** *Seja $\mathcal{C}$ um código sobre um alfabeto $\mathcal{A}$ :*

*(i) As coordenadas de uma palavra-código são chamadas de símbolos;*

*(ii) A cardinalidade de um código finito é chamado tamanho do código;*

*(iii) Quando o conjunto de índices $I$ é finito temos um código de bloco. Neste caso, a cardinalidade de $I$, denotada por $n$, é denominada comprimento do código;*

*(iv) Quando $I$ é infinito temos um código convolucional ou um código de treliça.*

**Definição 42** (Distância de Hamming)**.** *Sejam $u$ e $v$ dois elementos pertencentes a $\mathcal{A}^n$, a distância de Hamming será $d(u, v) = \sharp\{i \mid u_i \neq v_i, 1 \leq i \leq n\}$.*

**Definição 43** (Distância de Hamming Mínima)**.** *Seja $\mathcal{C}$ um código de bloco. A distância de Hamming mínima do código $\mathcal{C}$ é definida como o número $d = min\{d(u, v)| \, u, v \in \mathcal{C} \text{ e } u \neq v\}$.*

Sabendo que a métrica utilizada será a de Hamming, representaremos um código de bloco pela terna ordenada $(n, k, d_{min})$, onde valerá o teorema abaixo:

**Teorema 16.** *[4] Para qualquer código de bloco $(n, k, d_{min})$, vale a seguinte desigualdade:*

$$d \leq n - k + 1 \tag{2.14}$$

Um outro parâmetro primordial na caracterização de um código de bloco, é a taxa do código, definida pela razão entre a dimensão $k$ do código e seu comprimento $n$, ou seja,

$$r = \frac{k}{n}. \tag{2.15}$$

Códigos de bloco podem ser usados como códigos corretores de erros. A capacidade de correção de erros de um código $(n, k, d)$, denotada por $t$, está relacionada à distância mínima deste código da seguinte forma:

$$d_{min} \leq 2t + 1 \tag{2.16}$$

Logo, quanto maior a distância mínima do código, maior é a capacidade deste de corrigir erros.

A maioria dos códigos de interesse prático pertencem à classe dos códigos lineares. Um código $(n, k, d)$ é dito linear se, e somente se, todas as suas palavras códigos formam um subespaço vetorial de dimensão $k$ do espaço vetorial $\mathbb{F}_q^n$, o conjunto das $n-$uplas de $GF(q)$. Portanto, podemos representar este código matricialmente como:

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}, \tag{2.17}$$

conhecida como matriz geradora do código $(n, k, d)$, cujas linhas formam uma base do espaço vetorial. Portanto, combinações lineares das linhas de $G$ são palavras-código de $\mathcal{C}$. Dessa forma, o processo de codificação pode ser escrito como:

$$\underline{v} = \underline{u} \cdot G, \tag{2.18}$$

onde $\underline{u}$ é a seqüência de informação a ser codificada e $\underline{v}$ é a palavra-código correspondente.

Para toda palavra-código $\underline{v}$ vale a relação,

$$\underline{v} H^T = 0, \tag{2.19}$$

onde a matriz $(n - k) \times n$, denotada por $H$, é chamada matriz verificação de paridade e qualquer vetor ortogonal às suas linhas pertence ao espaço vetorial das linhas da matriz geradora $G$ associada e vice-versa. O código gerado pela matriz $H$ é chamado código dual do código $\mathcal{C}$.

# CAPÍTULO 3

# TRANSFORMADA DISCRETA DE FOURIER SOBRE CORPOS FINITOS

Neste capítulo, apresentamos alguns dos principais conceitos da transformada discreta de Fourier sobre corpos finitos que são fundamentais para a compreensão e comparação com o desenvolvimento a ser realizado no Capítulo 4 porém, sobre anéis comutativos finitos com identidade. Estes conceitos, inclusive os Teoremas e suas demonstrações que serviram de base teorica para as aplicações que serão feitas no Capítulo 5, podem ser encontrados nas referências [1] e [2].

Desenvolvemos este capítulo da seguinte maneira. A Seção 3.1, apresenta uma introdução da transformada discreta de Fourier assumindo que o corpo em questão é dos complexos. Na Seção 3.2, apresentamos uma revisão de códigos de bloco lineares sobre corpos finitos, teoria esta necessária para o desenvolvimento deste trabalho. Na Seção 3.3, descrevemos espectralmente os códigos cíclicos sobre corpos finitos. Já na Seção 3.4, veremos o procedimento de como é feita uma extensão Galoisiana sobre corpos. Nas Seções 3.5, 3.6 e 3.7 apresentamos procedimentos para obtermos as extensões dos códigos Reed-Solomon, BCH e Alternantes, respectivamente.

## 3.1 Introdução

Assumiremos que o corpo em questão é o dos complexos. A definição da transformada discreta de Fourier de $\mathbf{p} = (p_0,\ p_1\ , ...,\ p_{N-1})$, um vetor de números complexos, é um vetor $\mathbf{P} = (P_0, P_1, ..., P_{N-1})$ dado por:

$$P_k = \sum_{i=0}^{N-1} e^{-j2\pi N^{-1}ik} p_i, \quad k = 0, ..., N-1. \tag{3.1}$$

onde $j = \sqrt{-1}$. O núcleo da transformada de Fourier, $exp(-j2\pi N^{-1})$, é a raiz $N$-ésima da unidade no corpo de números complexos. No corpo finito $GF(q^m)$, um elemento $\alpha$ de ordem $n$ é uma $n$-ésima raiz da unidade. Da analogia entre $exp(-j2\pi N^{-1})$ e $\alpha$, temos:

**Definição 44.** *Seja* $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ *um vetor sobre* $GF(q)^n$ *onde* $n$ *divide* $q^m - 1$ *para algum* $m$, *e seja* $\alpha$ *um elemento de* $GF(q^m)$ *de ordem* $n$. *A transformada de Fourier do vetor* $\mathbf{v}$ *é o vetor* $\mathbf{V} = \{V_0, V_1, \ldots, V_{n-1}\}$ *dado por:*

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i, \quad j = 0, \ldots, n-1. \tag{3.2}$$

O índice $i$ é definido como o tempo, e $\mathbf{v}$ como uma função no domínio do tempo ou sinal. Também definimos o índice $j$ como a freqüência, e $\mathbf{V}$ como a função no domínio da freqüência ou o espectro e $\alpha$ é o núcleo da transformada.

Qualquer fator de $q^m - 1$ pode ser usado como o comprimento de uma transformada de Fourier, mas o valor mais importante para $n$ é o de comprimento primitivo, $n = q^m - 1$. Com isso, $\alpha$ é um elemento primitivo de $GF(q^m)$. Diferentemente do que ocorre no corpo dos complexos, a transformada de Fourier para qualquer valor do comprimento não existe no corpo de Galois porque não existem elementos com toda e qualquer ordem no corpo de Galois. Se $m$ é o menor inteiro resultante da divisão de $q^m - 1$ por $n$, então existe um corpo de Galois na transformada de Fourier sobre $GF(q)$ de comprimento $n$, e as componentes da transformada de Fourier estão em $GF(q^m)$.

No caso da transformada discreta de Fourier, embora a função no domínio do tempo $\mathbf{p}$ seja real, a transformada $\mathbf{P}$ é complexa. Analogamente, a transformada de Fourier sobre o

corpo de Galois, embora a função no domínio do tempo **v** seja sobre $GF(q)$, o espectro **V** é sobre o corpo de extensão $GF(q^m)$. Em aplicações onde seja exigido o controle de erro, o processo de decodificação é realizado sobre $GF(q^m)$.

**Teorema 17.** *Seja $GF(q)$ um corpo de característica p, então os elementos do par de transformada $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \longleftrightarrow \mathbf{V} = \{V_0, V_1, \ldots, V_{n-1}\}$ são dados por:*

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i \qquad\qquad v_i = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-ij} V_j, \tag{3.3}$$

*onde n é interpretado como um número inteiro do corpo módulo p.*

A transformada de Fourier apresenta algumas propriedades importantes que são facilmente transportadas para o caso do corpo finito. Um exemplo é a propriedade de convolução.

**Teorema 18** (Teorema da Convolução)**.** *Se $e_i = f_i g_i$, para todo $i = 0, 1, ..., n-1$, então*

$$nE_j = \sum \mathbb{F}_{(j-k-1)} G_k \qquad j = 0, 1, ..., n-1, \tag{3.4}$$

*onde $j - k - 1$ é interpretado módulo n e o produto $nE_j$ é interpretado módulo p.*

**Teorema 19** (Propriedade de Translação)**.** *Se $\{v_i\} \leftrightarrow \{V_j\}$ é um par de transformada de Fourier, então os seguintes pares de transformadas de Fourier são obtidos:*

$$\{\alpha^i v_i\} \leftrightarrow \{V_{((j+1))}\} \tag{3.5}$$

$$\{v_{((i-1))}\} \leftrightarrow \{\alpha^j V_j\} \tag{3.6}$$

Podemos representar um vetor **v** por um polinômio $v(x)$. O polinômio

$$v(x) = v_{n-1}x^{n-1} + ... + v_1 x + v_0$$

pode ser transformado em um polinômio,

$$V(x) = V_{n-1}x^{n-1} + ... + V_1 x + V_0 \tag{3.7}$$

por meio da transformada de Fourier sobre o corpo de Galois. Este último polinômio é chamado **polinômio espectral** ou o **polinômio associado** a $v(x)$. Propriedades do espectro estão relacionadas com os zeros do polinômio, como mostrado no teorema a seguir.

**Teorema 20.**

*(i) O polinômio $v(x)$ tem um zero $\alpha^j$ se, e somente se, a $j$-ésima componente da freqüência $V_j$ é igual a zero;*

*(ii) O polinômio $V(x)$ tem um zero $\alpha^{-i}$ se, e somente se, a $i$-ésima componente no tempo $v_i$ é igual a zero.*

Assim, em corpos finitos, quando falamos dos zeros do polinômio ou da componente espectral igual a zero, estamos falando a mesma coisa. Mas na verdade, em relação aos zeros do polinômio nos referimos à fatoração de polinômios, enquanto que em relação à componente espectral estamos relacionando com a transformada de Fourier.

## 3.2 Códigos sobre Corpos Finitos

Nesta seção, faremos uma breve revisão de códigos sobre corpos finitos necessários para o desenvolvimento deste trabalho. A teoria apresentada nesta seção segue de [14].

**Definição 45.** *Se o alfabeto $A$ for um corpo finito $\mathbb{F}_q = GF(q)$, onde $q = p^m$, com $p$ um número primo e $m$ um inteiro positivo, dizemos que um código de bloco $\mathcal{C}$ sobre $\mathbb{F}_q$ é **linear** se for um subespaço vetorial de $\mathbb{F}_q^n$.*

A seguir definiremos dimensão e taxa, sendo estes dois parâmetros importantes para um código de bloco.

**Definição 46.** *Seja $\mathcal{C}$ um código de bloco linear:*

1. *A **dimensão** do código $\mathcal{C}$ é definida como $k = log_{|A|}|\mathcal{C}|$ símbolos por bloco, onde $|\cdot|$ denota a cardinalidade do conjunto.*

2. *A **taxa** do código $\mathcal{C}$ é definida como $R_{\mathcal{C}} = k/n$, onde $k$ é a dimensão do espaço vetorial e $n$ é o comprimento da palavra-código.*

3. *Um código de bloco $\mathcal{C}$ de comprimento $n$, dimensão $k$ e distância mínima de Hamming $d$ é denotado por $(n, k, d)-$ código.*

Quando $k$ é inteiro, dizemos que a palavra-código contém $k$ dígitos de **informação** e $n-k$ dígitos de **redundância**.

Há várias formas de descrever um código. Uma delas é considerar que um código é derivado de uma estrutura de espaço vetorial. Nesta direção, é necessário identificar um conjunto $k$ de vetores em $GF(q)^n$ que sejam linearmente independentes (base do espaço vetorial). Assim, é possível gerar $q^k$ vetores distintos, e que a dimensão do código é dada por $log_{|A|}|\mathcal{C}| = log_q q^k = k$. Consequentemente, $k$ vetores linearmente independentes de $\mathbb{F}_q^n$ geram um $(n,k)-$código de bloco linear sobre $\mathbb{F}_q$, onde $q$ é uma potência de primo.

Se $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_k$ são vetores de $\mathbb{F}_q^n$ que geram um $(n,k)-$código linear $\mathcal{C}$, onde $\mathbf{g}_i = (g_{i1}, g_{i2}, \ldots, g_{in})$, $i = 1, 2, \ldots, k$, então a aplicação $f : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ definida por $f(\mathbf{u}) = f(u_1, u_2, \ldots, u_k) = \sum_{i=1}^{k} u_i \mathbf{g}_i = (\sum_{i=1}^{k} u_i g_{i1}, \ldots, \sum_{i=1}^{k} u_i g_{in})$ é um "codificador", isto é, se $\mathbb{F}_q^k$ for visto como o conjunto das palavras numa linguagem "natural", a função $f$ nos diz como codificá-las. Deste modo, qualquer palavra-código $\mathbf{v} \in \mathcal{C}$ pode ser expressa na forma $\mathbf{v} = \mathbf{u}G$, onde $\mathbf{u} = (u_1, u_2, \ldots, u_k) \in \mathbb{F}_q^k$ e

$$G = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}. \tag{3.8}$$

A matriz $G = [g_{ij}]$, que descreve a aplicação linear $f$, é chamada **matriz geradora** do código $\mathcal{C}$. Dizemos que $G$ está na forma sistemática se $G = [I_k | P_{k \times n-k}]$ para alguma matriz $P$, isto é, $g_{ij} = \delta_{ij}$ para $i, j = 1, 2, \ldots, k$ (onde $\delta_{ij} = 0$ se $i \neq j$ e $\delta_{ij} = 1$ se $i = j$). Neste caso, dizemos que o código é **sistemático,** e que os primeiros $k$ símbolos ou coordenadas de $\mathbf{c} \in \mathcal{C}$ são os símbolos de informação, e os demais símbolos de paridade.

Os símbolos de controle ou de paridade têm a seguinte finalidade. Dado um vetor $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ em $\mathbb{F}_q^n$, para determinar se $\mathbf{x} \in \mathcal{C}$ basta verificar se $\mathbf{x} = f(\mathbf{u})$ para algum $\mathbf{u} \in \mathbb{F}_q^k$. Neste caso (estamos supondo $\mathcal{C}$ na forma sistemática), $x_i = u_j$, para $i \leq k$, e $x_j = \sum_{i=1}^{k} u_i g_{ij} = \sum_{i=1}^{k} x_i g_{ij}$, para $j > k$. Logo, para verificar se $\mathbf{x} \in \mathcal{C}$ basta verificar se $x_j =$

$\sum_{i=1}^{k} x_i g_{ij}$, para $j = k+1, \ldots, n$.

Note que a matriz $G$ não é univocamente determinanada por $\mathcal{C}$, pois ela depende da escolha da base. Duas matrizes geradoras de um mesmo código $\mathcal{C}$ podem ser obtidas uma da outra por uma seqüência de operações elementares do tipo: 1) troca de duas linhas; 2) multiplicação de uma linha por um elemento não nulo do corpo $\mathbb{F}_q$; 3) adição de qualquer múltiplo de uma linha à outra.

Se além disso, efetuarmos seqüências de operações sobre $G$ do tipo: 1) permutações de duas colunas; 2) multiplicação de uma coluna por um escalar não nulo. Então, obteremos uma matriz $G'$ de um código equivalente a $\mathcal{C}$. Reciprocamente, podemos construir códigos a partir de matrizes geradoras $G$. Para isto, basta considerar uma matriz cujas linhas são linearmente independentes.

Note que pelo fato de $G$ ter posto $k$ é sempre possível reduzí-la à forma escalonada através das operações elementares sobre as suas linhas. Dessa forma, dizemos que dois códigos são **equivalentes** se um puder ser obtido do outro através de permutações de suas coordenadas.

De acordo com o que vimos anteriormente, podemos afirmar que a informação contida numa palavra-código $\mathbf{c} \in \mathcal{C}$ depende de $k$ de suas coordenadas e as demais coordenadas representam a redundância usada para a verificação da paridade. A taxa do código $\mathcal{C}$, denotada por $R_{\mathcal{C}} = \dfrac{k}{n}$, é a razão entre o número de coordenadas "informativas"e o número total de coordenadas.

Uma outra maneira de descrever um código é estabelecer uma aplicação linear sobrejetora $h : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^k$ tal que o núcleo de $h$ é o código $\mathcal{C}$. Neste caso, $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathcal{C}$ se, e somente se, $H(x_1, x_2, \ldots, x_n) = \mathbf{0}$. Se temos uma matriz $H$ de posto $k$ e ordem $n-k$ por $n$ dada por $H = [h_{ij}]$, então esta última equação se escreve como $\sum_{i=1}^{n} h_{ij} x_j = 0, \;\; i = 1, 2, \ldots, k$, isto é, $\mathbf{x}H^T = \mathbf{0}$, onde $H^T$ denota a transposta da matriz $H$. A matriz $H$ é chamada **matriz verificação de paridade** do código $\mathcal{C}$ e gera um $(n, n-k)-$ código sobre $\mathbb{F}_q$ chamado código dual de $\mathcal{C}$.

Note que um código $\mathcal{C}$ com matriz geradora $G$, para verificar se um determinado vetor $\mathbf{c} \in \mathbb{F}_q^n$ pertence ou não a $\mathcal{C}$, é preciso verificar se o sistema de equações com $k$ incógnitas

dado por $\mathbf{x}G = \mathbf{c}$, admite solução. Em geral, o custo computacional associado é elevado. No entanto, trabalhando com uma matriz verificação de paridade $H$, a questão pode ser respondida bem mais rapidamente. Basta verificar se é nulo o vetor $\mathbf{c}H^T$, o que é fácil de realizar computacionalmente.

Dados um código $\mathcal{C}$ com matriz verificação de paridade $H$ e um vetor $\mathbf{c} \in \mathbb{F}_q^n$, chamamos o vetor $\mathbf{c}H^T$ de **síndrome** de $\mathbf{c}$.

## 3.3 Descrição Espectral de Códigos Cíclicos sobre Corpos Finitos

Em um código cíclico cada palavra-código $c(x)$ é representada pelo produto do polinômio gerador por um polinômio de grau $k-1$, isto é, $c(x) = g(x)d(x)$, onde $d(x)$ é um polinômio de grau $k-1$. A convolução cíclica no domínio do tempo é definida, para todo $i$, como

$$c_i = \sum_{k=0}^{n-1} g_{((i-k))} d_k. \tag{3.9}$$

Portanto, no domínio da freqüência, a componente $C_j$ é dada por

$$C_j = G_j D_j. \tag{3.10}$$

Qualquer espectro que satisfaça esta expressão é uma palavra-código no domínio da freqüência, se todas as componentes no domínio do tempo estão em $GF(q)$. Como o espectro é arbitrário, o único papel significativo de $G_j$ é especificar as freqüências onde o espectro da palavra-código $C_j$ é zero. Assim, podemos definir um código cíclico como: Dado um conjunto de componentes espectrais $j_1, \ldots, j_{n-k}$ chamado **freqüência de paridade**, o código cíclico $\eta$ é o conjunto de palavras-código em $GF(q)$ cujo espectro é zero nas componentes $j_1, \ldots, j_{n-k}$.

**Teorema 21.** *[2] Seja $\boldsymbol{V}$ um vetor de dimensão $n$ com elementos em $GF(q^m)$, onde $n$ é um divisor de $q^m - 1$. Então, a transformada de Fourier inversa $\mathbf{v}$ é um vetor de elementos sobre $GF(q)$ se, e somente se, as seguintes equações são satisfeitas:*

$$V_j^q = V_{((qj))}, \qquad j = 0, \ldots, n-1. \tag{3.11}$$

DEMONSTRAÇÃO: *Por definição,*

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i \qquad j = 0, \ldots, n-1. \tag{3.12}$$

*Para um corpo de característica p, sabemos que* $(a+b)^r = a^{p^r} + b^{p^r}$ *para qualquer inteiro r. Então, se* $v_i$ *é um elemento de* $GF(q)$*, para todo i, então* $v_i^q = v_i$*. Consequentemente,*

$$V_j^q = (\sum_{i=0}^{n-1} \alpha^{ij} v_i)^q = \sum_{i=0}^{n-1} \alpha^{qji} v_i^q = \sum_{i=0}^{n-1} \alpha^{qji} v_i = V_{((qj))}. \tag{3.13}$$

*Reciprocamente, suponha que para todo* $j$*,* $V_j^q = V_{((qj))}$*. Então*

$$\sum_{i=0}^{n-1} \alpha^{iqj} v_i^q = \sum_{i=0}^{n-1} \alpha^{iqj} v_i \qquad j = 0, \ldots, n-1. \tag{3.14}$$

*Seja* $k = qj$*. Dado que q é relativamente primo a* $n = q^m - 1$*, e como j abrange todos os valores entre* 0 *e* $n-1$*, k também assume todos os valores entre* 0 *e* $n-1$*. Portanto,*

$$\sum_{i=0}^{n-1} \alpha^{ik} v_i^q = \sum_{i=0}^{n-1} \alpha^{ik} v_i \qquad k = 0, \ldots, n-1, \tag{3.15}$$

*e por unicidade da transformada de Fourier,* $v_i^q = v_i$*, para todo i. Assim,* $v_i$ *é um zero de* $x^q - x$ *para todo i, e tais zeros são elementos de* $GF(q)$*.* ■

Para aplicar o Teorema 21, o módulo dos $n$ inteiros é dividido em uma coleção de conjuntos, conhecida como *classes conjugadas*, conforme segue:

$$A_j = \{j, jq, jq^2, \ldots, jq^{m_j - 1}\}, \tag{3.16}$$

onde $m_j$ é o menor inteiro positvo que satisfaz $jq^{m_j-1} = j \bmod n$. Como o corpo é finito, deve existir um $m_j$. Embora cada palavra-código no código cíclico seja um vetor em $GF(q)$, o espectro da palavra-código é um vetor em $GF(q^m)$. Portanto, um código cíclico pode ser descrito como o conjunto de transformadas de Fourier inversa do conjunto de todos os vetores espectrais que são restritos a zero em muitas componentes prescritas, dado que estas transformadas inversas de Fourier estão em $GF(q)$. Não é possível escolher qualquer espectro que seja zero nas componentes prescritas; algumas destas pode ter transformada

inversa com componentes que não estão em $GF(q)$. Para obter palavras-códigos em $GF(q)$ devemos escolher somente espectros que satisfaça as restrições conjugadas do Teorema 21.

Os códigos BCH são códigos cíclicos em que as freqüências de paridade são escolhidas consecutivamente. Um código BCH corrigindo $t$ erros, com comprimento $n = q^m - 1$ é o conjunto de todas as palavras-código em $GF(q)$ cujo espectro é zero em um bloco específico de $2t$ componentes consecutivas. O limitante da distância mínima de um código no domínio da freqüência é estabelecido através do seguinte resultado.

**Teorema 22.** *[2] Seja $n$ um fator de $q^m - 1$ para algum $m$. O único vetor em $GF(q)^n$ com peso menor ou igual a $d-1$, resultando em $d-1$ valores seqüênciais de seu espectro iguais a zero é o vetor todo nulo.*

DEMONSTRAÇÃO: *Sejam $i_1, \ldots, i_\upsilon$ os índices das $\upsilon$ componentes diferentes de zero do vetor $\boldsymbol{c}$, $\upsilon \leq d-1$. Defina um vetor no domínio da freqüência cuja transformada inversa de Fourier é zero quando $c_i \neq 0$. Existem muitos vetores no domínio da freqüência que poderiam ser usados. Uma escolha é baseada no polinômio localizador $\Lambda(x)$ :*

$$\Lambda(x) = \prod_{k=1}^{\upsilon}(1 - x\alpha^{-i_k}) = \Lambda_\upsilon x^\upsilon + \Lambda_{\upsilon-1}x^{\upsilon-1} + \ldots + \Lambda_1 x + \Lambda_0. \tag{3.17}$$

*Como um vetor, $\Lambda$ é um espectro de freqüência arbitrariamente definido, tal que sua transformada inversa $\lambda = \{\lambda_i\}$ é igual a zero para todo $i$ em que $c_i \neq 0$. O produto no domínio do tempo é zero ($\lambda_i c_i = 0$ para $i = 0, \ldots, n-1$); portanto, a convolução cíclica no domínio da freqüência é zero:*

$$\Lambda * \boldsymbol{C} = 0, \tag{3.18}$$

*pois, $\Lambda_0 = 1$ e $\Lambda_k = 0$ se $k > d-1$. Esta convolução pode ser escrita como*

$$C_j = -\sum_{k=1}^{d-1} \Lambda_k C_{((j-k))}. \tag{3.19}$$

*Mas $\boldsymbol{C}$ é zero no comprimento do bloco $d-1$. Conseqüentemente, a recursão implica que $\boldsymbol{C}$ é zero em toda componente e que $\boldsymbol{c}$ deve ser o vetor todo nulo.* ∎

Quando $n = q - 1$, o código BCH é um código Reed-Solomon, a palavra-código e o espectro estão no mesmo corpo. Pode-se codificar diretamente no domínio da freqüência por

estar ultilizando a informação de símbolos para especificar as componentes espectrais. Cada espectro, consistente com as restrições de paridade, produz uma palavra-código. Qualquer conjunto de $2t$ freqüências consecutivas é escolhido como símbolos restritos a zero. As $n-2t$ componentes não restritas do espectro são preeenchidas com símbolos de informação sobre $GF(q)$.

Para códigos BCH mais gerais, a codificação é mais complexa. Existem dois corpos: o corpo de símbolos $GF(q)$ e o corpo localizador $GF(q^m)$ usado para o espectro. Novamente, $2t$ componentes consecutivas do espectro são escolhidas como nulas. Os símbolos restantes devem ser escolhidos de $GF(q^m)$ para representar as $k$ informações de símbolos somente nas $q^k$ possíveis formas que tem a transformada inversa de Fourier sobre valores $q$-*á*rios.

Para o caso geral, os inteiros módulo $n$ são divididos em classes conjugadas:

$$A_j = \{j, jq, jq^2, \ldots, jq^{m_j-1}\}. \tag{3.20}$$

Se a componente espectral $C_j$ é especificada, então cada componente espectral cujo índice está na classe conjugada de $j$, deve ser uma potência de $C_j$ e, portanto, não pode ser especificada separadamente. Além disso, se a classe conjugada tem $r$ membros, então devemos ter

$$C_j^{q^r} = C_j \tag{3.21}$$

e

$$C_j^{q^r-1} = 1. \tag{3.22}$$

Consequentemente, não estamos livres para escolher qualquer elemento de $GF(q^m)$ para $C_j$, porém, somente aqueles cuja ordem divide $q^r - 1$ ou o elemento zero. Cada elemento de $GF(q^m)$ tem ordem que divide $q^m - 1$. Portanto, $q^r - 1$ divide $q^m - 1$, e é claro que a cardinalidade de cada classe conjugada divide $m$.

Para especificar uma codificação, particionamos os $q^m - 1$ primeiros inteiros nas classes conjugadas, e selecionamos um inteiro para representar cada classe. Esta representatividade especifica a unicidade dos símbolos assinaláveis. Para formar um código BCH, um bloco de $2t$ componentes espectrais são escolhidas como freqüências de paridade e igualadas a zero.

Os símbolos restantes são símbolos de informação arbitrários com **exceção** das restrições ocasionais na ordem. Todos os outros símbolos indexados na mesma classe conjugada não são livres, são freqüências obrigatórias.

## 3.4 Extensão Galoisiana sobre Corpos Finitos

A Teoria de Galois é uma forma fascinante de conectar a matemática moderna à clássica. Seu objetivo é estudar as soluções da equação polinomial.

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0, \tag{3.23}$$

considerando o polinômio $f(x)$ com coeficientes em um corpo $k$. Os zeros deste polinômio determinam outro corpo $L$ o qual contém $k$. Se $\alpha_1, \ldots, \alpha_n$ são raízes de $f(x)$, então $L = k(\alpha_1, \ldots, \alpha_n)$, e este corpo é chamado **corpo de decomposição** de $f$ sobre $k$ ou **extensão Galoisiana** de $k$.

Veremos, a seguir, o procedimento geral de como construir um código sobre corpos de Galois. Inicialmente deve-se determinar o polinômio gerador de um código de bloco cíclico $q$-ário. Sabendo que $q = p^m$, o corpo de Galois $GF(p^m)$ é formado pelas classes residuais de polinômios em $GF(p)[x]$ módulo um ideal primitivo de grau $m$, também pertencente a $GF(p)[x]$. Suponha que $\alpha$ seja um elemento primitivo no corpo em questão. Portanto, $\alpha$ é uma raiz do polinômio gerador desse ideal. Consequentemente, é possível expressar uma dada potência de $\alpha$ em função de outras menores, ferramenta essencial para se determinar os elementos do corpo $GF(p^m)$. Ressalta-se que as operações devem ser realizadas em $GF(p)$. Determinados os polinômios minimais associados a cada um dos $p^m - 1$ elementos do grupo multiplicativo de $GF(p^m)$, pode-se definir o polinômio gerador do código de bloco cíclico.

Considere os códigos sobre $GF(q)$ construídos usando o corpo localizador $GF(q^m)$. Uma extensão do código Reed-Solomon sobre $GF(q^m)$ pode ser usado para criar um código sobre $GF(q)$ tomando o subcorpo-subcódigo da extensão do código Reed-Solomon no corpo $GF(q)$.

## 3.5 Códigos Reed-Solomon sobre Corpos Finitos

A classe de códigos Reed-Solomon, um dos casos particulares mais simples de códigos BCH sobre $\mathbb{F}_q$, encontra na prática aplicações bastante importante, isto é, gravação magnética, transmissão via satélite e muitas outras. Uma das características importantes desta classe de códigos é a eficiência na correção de erros que ocorrem em surtos.

É possível, em geral, adicionar duas componentes extras no código Reed-Solomon, sempre colocaremos um novo símbolo no início e um no final do código. Códigos obtidos pela adição de uma ou ambas componentes extras são chamados códigos Reed-Solomon estendidos. Cada uma dessas componentes extras pode ser usada tanto como informação ou como paridade, isto é, expandir o código aumentando a taxa ou alongar o código aumentando a distância mínima. Usamos o termo menos específico, código Reed-Solomon estendido, porque os códigos podem ser considerados como códigos construídos por ser código Reed-Solomon expandido de distância mínima $d^*$ ou pelo código Reed-Solomon alongado de distância mínima $d^* - 2$. O mesmo código Reed-Solomon é obtido no outro caso.

As duas novas localizações devem ser identificadas. Para isso, várias notações podem ser utilizadas. Se as componentes originais são rotuladas por elementos do corpo, então o elemento zero pode ser usado para identificar uma nova componente, e um símbolo adicional é necessário para identificar o outro. Geralmente, utiliza-se o símbolo infinito. Se as componentes originais são rotuladas por representantes de um elemento primitivo, então o zero não está disponível para identificar um novo símbolo, e dois novos símbolos são necessários. Utilizaremos $-$ e $+$ para estes. Assim um código aumentado é

$$(c_-, c_0, c_1, c_2, \ldots, c_{q^m-3}, c_{q^m-2}, c_+) \tag{3.24}$$

e $n = q^m + 1$. O vetor obtido, por exclusão de $c_-$ e $c_+$, será chamado de **interior**. Devemos estudar códigos estendidos por meio de propriedades da transformada de Fourier, junto com propriedades adicionais do espaço vetorial estendido. Quando falamos de espectro de palavras-código, queremos dizer espectro do interior.

**Definição 47.** *Um código cíclico estendido $(n, k)$ sobre $GF(q)$ é um código linear de dimensão $n = q^m + 1$ consistindo do conjunto de palavras com as propriedades que cada*

*palavra-código* $(c_-, c_0, c_1, c_2, \ldots, c_{n-3}, c_+)$ *tem um espectro* $(C_0, C_1, \ldots, C_{n-3})$ *que é igual a zero no conjunto especificado de* $n-k-2$ *componentes com índices* $j_1, \ldots, j_{n-k-2}$, *e que duas outras componentes espectrais satisfazem* $c_{j_0} = c_-, c_{j_n-k-1} = c_+$.

Um código cíclico estendido geralmente não é cíclico.

**Definição 48.** *Sejam* $j_0$ *e* $t$ *inteiros arbitrários. Um código Reed-Solomon estendido é um código linear em* $GF(q)$ *de dimensão* $n = q+1$ *cujas palavras-código* $(c_-, c_0, c_1, c_2, \ldots, c_{q-2}, c_+)$ *têm espectro que satisfazem:*

1. $C_j = 0 \quad j = j_0 + 1, \ldots, j_0 + 2t - 2$
2. $C_{j_0} = c_-$
3. $C_{j_0+2t-1} = c_+$.

O inteiro $2t+1$ é a distância projetada do código Reed-Solomon estendido. A definição restringe a $2t-2$ sucessivas componentes espectrais iguais a zero, e as componentes espectrais em ambos os lados destas $2t-2$ componentes são iguais a $c_-$ e $c_+$, respectivamente. As duas freqüências espectrais são chamadas de freqüências de borda.

Comparados ao código Reed-Solomon obtido por eliminação de $c_-$ e $c_+$ e ajuste $C_{j_0} = C_{j_0+2t-1} = 0$, o código Reed-Solomon estendido sempre resulta em duas componentes extras de informação sem mudar a distância mínima.

Disso segue que:

**Teorema 23.** *[2] Um código Reed-Solomon estendido em* $GF(q)$ *é um código* $(q+1, k)$ *com distância mínima* $2t + 1 = n - k + 1 = q - k + 2$.

## 3.6 Códigos BCH sobre Corpos Finitos

Um código BCH cíclico de comprimento $s$, com $mdc(p, s) = 1$, e distância projetada $d$ sobre corpos finitos é um código cujo polinômio gerador tem como raízes os elementos $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2}$, onde $\alpha \in GF(p^m)$ é uma raiz primitiva de $x^s - 1$, $b$ é um inteiro

não negativo e $m$ é tal que $s$ divide $p^m - 1$. Quando $s = p^m - 1$ o código é chamado BCH primitivo. Agora, considere códigos sobre $GF(q)$ construídos usando o corpo localizador $GF(q^m)$. Um código Reed-Solomon estendido em $GF(q^m)$ pode ser utilizado para gerar um código sobre $GF(q)$ tomando o subcorpo-subcódigo do código Reed-Solomon sobre $GF(q)$. As vezes, devido às restrições no subcorpo $GF(q)$, as componentes estendidas não podem ser utilizadas como locais de informação. Isto é, elas podem conter o mesmo símbolo em cada palavra-código e podem ser omitidas.

Considerando uma aproximação diferente para construir um código sobre $GF(q)$ de um código estendido sobre $GF(q^m)$, esta aproximação é tomada do código estendido Reed-Solomon cujas palavras têm componentes somente em $GF(q)$ nos $q^m - 1$ símbolos interiores. Os dois símbolos estendidos são arbitrários em $GF(q^m)$, porém, são representados na palavra-código por $m$ símbolos $q$-ários.

Por ser um processo um pouco trabalhoso, os códigos resultantes são decodificáveis e muitos podem ser obtidos desta forma, o qual chamamos de códigos BCH estendidos. Pode-se obter códigos originais BCH do código estendido relacionando todos os códigos cujas caudas são iguais a zero.

Um vetor $\mathbf{C}$ sobre $GF(q^m)$ de comprimento $q^m - 1$ é um espectro válido para o interior de uma palavra-código $q$-ária se as restrições conjugadas

$$C_j^q = C_{((qj))}, \tag{3.25}$$

são satisfeitas. Para obter códigos BCH estendidos de distância $d$, procedemos como no caso dos códigos Reed-Solomon estendidos. Escolhemos freqüências contíguas começando em $j_0$ como freqüências de paridade, e fazemos

1. $C_{j_0} = c_-$
2. $C_{j_0} = 0 \quad j = j_0 + 1, \ldots, j_0 + d - 3$
3. $C_{j_0+d-2} = c_+$

onde $c_-$ e $c_+$ são elementos arbitrários de $GF(q^m)$, dado que não violem as restrições conjugadas. As componentes espectrais restantes são escolhidas, de forma arbitrária, porém,

satisfazendo as restrições. O interior é precedido por uma parte final consistindo de no máximo $m$ símbolos $q$-ários representando $c_-$, e é seguido por uma parte semelhante representando $c_+$. Pode ser que as restrições em $C_{j_0}$ ou $C_{j_0+d-2}$ forcem uma ordem menor que $q^m - 1$ em que $c_-$ ou $c_+$ representa menos que $m$ símbolos $q$-ários de informação. Neste caso, o comprimento final é um divisor de $m$.

Quando estudamos códigos BCH, geralmente escolhemos $j_0 = 1$ pois, em geral resulta em códigos melhores.

## 3.7 Códigos Alternantes sobre Corpos Finitos

Um código BCH sobre $GF(q)$ de comprimento $n = q^m - 1$ é um subcorpo-subcódigo de um código Reed-Solomon sobre $GF(q^m)$. Isto é, o código BCH consiste de todas as palavras-código do código Reed-Solomon que são valores de $GF(q)$, tais que o código BCH tem pelo menos uma distância mínima como a do código Reed-Solomon. Infelizmente, os códigos BCH de comprimento grande e distância mínima grande não contêm palavras-código em número suficiente. Mais precisamente, em qualquer seqüência de códigos BCH de comprimento crescente e taxa limite (para algum $R'$ fixado, todos os códigos na sequência satisfazem $k/n \geq R'$) a distância mínima normalizada $d^*/n$ se aproxima de zero com o crescimento de $n$. O código original Reed-Solomon tem muitas palavras-código, porém o subcorpo-subcódigo utiliza poucas delas ou tem estrutura de distância pobre. Nesta seção estudaremos formas de aumentar a distância mínima reduzindo o código Reed-Solomon para um código subcorpo em outra forma.

Códigos alternantes formam uma classe dos códigos lineares que são uma variação dos códigos BCH tais que para taxas fixas, uma maior distância mínima pode ser obtida (pelo menos em princípio). Seja $n = q^m - 1$, escolha $\mathbf{h}$, um vetor $n-$dimensional fixo de componentes diferente de zero sobre $GF(q^m)$, que será chamada de domínio do tempo e escolha um código Reed-Solomon em $GF(q^m)$ com distância projetada $2t + 1$. O código alternante consiste de todos os vetores $\mathbf{c}$ cujos valores estão em $GF(q)$ tal que $c_i^{'} = h_i c_i$, para $i = 0, \ldots, n-1$, é uma palavra-código no código Reed-Solomon.

Equivalentemente, suponha que $h_i$ é sempre diferente de zero e $g_i = h_i^{-1}$. Então, para cada palavra-código $\mathbf{c}'$ no código Reed-Solomon, forme o vetor $c_i = g_i c_i^{'}$, para $i = 0, \ldots, n-1$. Se o vetor $\mathbf{c}$ assume valores em $GF(q)$, então $\mathbf{c}$ está contido no código alternante. O código alternante é o conjunto de todas as palavras-código com valores em $GF(q)$ que podem ser obtidas desta maneira.

Normalmente, selecionamos $\mathbf{h}$ no domínio do tempo com todas as componentes diferentes de zero, porém se no domínio do tempo algum elemento nulo for escolhido, o código deve ser zero naqueles elementos. Os elementos nulos não contêm informação e simplesmente não são transmitidos. O decodificador pode reinserí-los se necessário para ajustar às necessidades de um algoritmo decodificador.

Códigos alternantes atingem grandes distâncias mínimas se os domínios no tempo são selecionados apropriadamente. Para valores grandes do comprimento tais códigos apresentam o mesmo comportamento que quaisquer outros bons códigos conhecidos. Infelizmente, uma regra prática para a escolha de um domínio no tempo de comprimento $n$ não é conhecida, embora bons domínios do tempo existam em abundância.

A definição de código alternante é facilmente traduzida no domínio da freqüência. Suponha que $\mathbf{h}$ é diferente de zero. Seja $\mathbf{H}$ a transformada de $\mathbf{h}$, a qual será chamada de **molde** no domínio da freqüência. Dado $h_i c_i$, para $i = 0, \ldots, n-1$, resulta uma palavra-código Reed-Solomon, a convolução cíclica $\mathbf{H}*\mathbf{C}$ resulta em um espectro da palavra-código Reed-Solomon. Isto é,

$$\sum_{k=0}^{n-1} H_{((j-k))} C_k = 0 \quad j = j_0, \ldots, j_0 + 2t - 1. \tag{3.26}$$

Dado que $\mathbf{h}$ é não nulo, $\mathbf{H}$ é invertível, isto é, existe uma matriz $\mathbf{G}$ (a transformação do vetor $g_i = h_i^{-1}$, para $i = 0, \ldots, n-1$) tal que $\mathbf{H} * \mathbf{G}$ é a função delta de Dirac. (Se $j = 0$, $(\mathbf{H}*\mathbf{G})_j = 1$; caso contrário $(\mathbf{H}*\mathbf{G})_j = 0$.) Em linguagem polinomial, esta convolução se torna

$$H(x)G(x) = 1 \quad (mod\ x^n - 1). \tag{3.27}$$

Se $H(x)$ é um polinômio em $GF(q)$, então $G(x)$ também será um polinômio em $GF(q)$. O argumento é como segue para $n$ primitivo. $H(x)$ não tem nenhum zero em $GF(q^m)$ pois

$H(\alpha^{-i}) = nh_i \neq 0$. Portanto, $H(x)$ é primo relativo a $x^n - 1 = x^{q^m-1} - 1$ e pelo algoritmo de Euclides existem os polinômios $G(x)$ e $F(x)$ em $GF(q)$ tais que

$$H(x)G(x) + (x^n - 1)F(x) = 1. \tag{3.28}$$

Isto é,

$$H(x)G(x) = 1 \pmod{x^n - 1}. \tag{3.29}$$

Os códigos alternantes podem ser definidos no domínio da freqüência como segue:

**Definição 49.** *Seja $\boldsymbol{H}$ um vetor $n-$dimensional fixado no domínio da freqüência e sejam $j_0$ e $t$ inteiros fixos. O código alternante $\varsigma$ é o conjunto que contém todo vetor cuja transformação $\boldsymbol{C}$ satisfaz as duas condições:*

1. $\sum_{k=0}^{n-1} H_{((j-k))}C_k = 0 \quad j = j_0, \ldots, j_0 + 2t - 1;$
2. $C_k^q = C_{((qk))}$.

A primeira destas condições é uma convolução. A segunda condição garante que as palavras-código no domínio do tempo estão em $GF(q)$. O vetor

$$T_j = \sum_{k=0}^{n-1} H_{((j-k))}C_k, \quad j = 0, \ldots, n-1 \tag{3.30}$$

será chamado **espectro filtrado** da palavra-código.

Dado que os códigos alternantes estão relacionados com os códigos Reed-Solomon, é aparente que a distância mínima seja pelo menos tão grande quanto a distância projetada $2t + 1$. O próximo teorema diz que a dimensão também satisfaz $k \geq n - 2tm$.

**Teorema 24.** *[2] Seja $\varsigma$ um código linear $(n, K, D)$ em $GF(q^m)$ e seja $\varsigma'$ um subcorpo-subcódigo $(n, k, d)$ de $\varsigma$ em $GF(q)$. Então*

$$D \leq d \leq n \quad e \quad (n - K) \leq (n - k) \leq m(n - K). \tag{3.31}$$

**Corolário 5.** *[2] Um código alternante de distância projetada* $2t+1$ *tem dimensão* $k$ *satisfazendo*

$$k \geq n - 2tm \tag{3.32}$$

Podemos estender o limitante do código BCH a uma derivação instrutiva no domínio da freqüência de uma estrutura da distância herdada por códigos alternantes de códigos Reed-Solomon.

**Teorema 25.** *[2] Se um vetor* $\boldsymbol{c}$ *tem pelo menos* $d$ *elementos não nulos e, se o espectro filtrado é zero em quaisquer* $d-1$ *elementos sucessivos* $(T_k = 0,\ k = k_0, \ldots, k_0 + d - 2)$, *então* $c_i = 0$ *para todo* $i$, *onde* $\boldsymbol{T} = \boldsymbol{H} * \boldsymbol{C}$ *e* $\boldsymbol{H}$ *é um filtro invertível.*

DEMONSTRAÇÃO: *O polinômio localizador* $\boldsymbol{\Lambda}(\mathbf{x})$ *é definido de tal forma que sua transformada* $\lambda_i$, *é zero quando* $c_i \neq 0$. *Então* $\lambda_i c_i = 0$, *o que implica que* $\boldsymbol{\Lambda} * \mathbf{C} = \mathbf{0}$. *Portanto,* $\boldsymbol{\Lambda} * (\mathbf{H} * \mathbf{C}) = \mathbf{H} * (\boldsymbol{\Lambda} * \mathbf{C}) = \mathbf{0}$. *Porém,* $\boldsymbol{\Lambda}$ *é não nula somente no bloco de comprimento de no máximo* $d$, *e* $\mathbf{H} * \mathbf{C}$ *é nulo em um bloco de comprimento* $d-1$. *Consequentemente,* $\mathbf{H} * \mathbf{C} = \mathbf{0}$ *e* $\mathbf{C} = \mathbf{0}$. *Portanto,* $\mathbf{c}$ *é um vetor nulo.* ■

# CAPÍTULO 4

# TRANSFORMADA DISCRETA DE FOURIER SOBRE ANÉIS LOCAIS

Neste capítulo, apresentamos a importância do grupo das unidades para a realização da transformada discreta de Fourier sobre anéis locais com a utilização de códigos cíclicos BCH, Alternante e Reed-Solomon provenientes de extensões de Galois de dimensão $r$, onde faremos uso desses códigos no Capítulo 5. Dada a similaridade do procedimento de geração tanto via códigos cíclicos BCH quanto os códigos alternantes este trabalho terá como foco a classe dos códigos BCH. Estes conceitos podem ser encontrados nas referências [1],[3],[4] e [10].

Este capítulo está organizado da seguinte forma. A Seção 4.1, apresenta a transformada discreta de Fourier sobre Anéis de Galois mostrando a similaridade com o que foi desenvolvido no Capítulo 3 sobre corpos. Na Seção 4.2, apresentamos códigos cíclicos sobre anéis de inteiros residuais, onde são estabelecidas definições e teoremas que estão relacionados com estes códigos sobre anéis $\mathbb{Z}_q$. Na Seção 4.3, abordamos a extensão galoisiana de anéis sendo esta uma forma de mostrar a sua estrutura e também suas aplicações em códigos. Na Seção 4.4, desenvolvemos os códigos BCH sobre anéis locais comparando-os e mostrando a sua importância por meio de exemplos. Na Seção 4.5, apresentamos propriedades importantes de extensão de Galois sobre anéis, e o processo de construção de códigos alternantes sobre

anéis locais. Finalmente, na Seção 4.6 apresentamos a construção de códigos Reed-Solomon sobre anéis locais, bem como mostramos, através de um exemplo, que em geral os códigos Reed-Solomon sobre anéis **não** são cíclicos.

Dada a similaridade do procedimento de geração da transformada discreta de Fourier sobre anéis locais tanto via códigos cíclicos BCH como os códigos alternantes este trabalho terá como foco a classe dos códigos cíclicos tipo BCH.

## 4.1 Transformada Discreta de Fourier sobre Anéis de Galois

A transformada discreta de Fourier sobre anéis de Galois é muito similar à desenvolvida no Capítulo 3 referente a transformada discreta de Fourier sobre corpos finitos. Iremos assumir que $A$ é um anel comutativo finito com identidade, com ideal maximal $M$ e corpo de resíduo $K = \frac{A}{M} \cong GF(p^m)$, onde $m$ é um inteiro positivo e $p$ primo. Seja $f(x)$ um polinômio mônico de grau $h$ em $A[x]$, tal que $\mu(f(x))$ é irredutível em $K[x]$, onde $\mu$ é a projeção natural. Então $f(x)$ também é irredutível em $A[x]$. Seja $R$ o anel $A[x]/\langle f(x)\rangle$. Então $R$ é um anel local comutativo finito com identidade chamado extensão de Galois de $A$ de grau $h$. Seu corpo de resíduo é $K_1 = \frac{R}{\overline{M_1}} \cong GF(p^{mh})$, onde $\overline{M_1}$ é o ideal maximal de $R$, e $K_1^*$ é o grupo multiplicativo de $K_1$, cuja ordem é $p^{mh} - 1$. Seja $R^*$ o grupo multiplicativo das unidades de $R$. Segue que $R^*$ é um grupo abeliano, e, portanto, pode ser expresso como o produto direto de grupos cíclicos. Estamos interessados no grupo cíclico maximal de $R^*$, denotado por $G_s$, cujos elementos são as raízes de $x^s - 1$ para algum número inteiro positivo $s$ tal que o $mdc(s, p) = 1$. Existe somente um subgrupo cíclico maximal de $R^*$ tendo ordem prima para $p$, este grupo cíclico tem ordem $s = p^{mh} - 1$.

**Definição 50.** *Seja* $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ *um vetor sobre* $A$ *onde* $n$ *divide* $s$, *e seja* $\alpha$ *um elemento de* $G_s$ *de ordem* $n$. *A transformada de Fourier do vetor* $\mathbf{v}$ *é o vetor* $V =$

$\{V_0, V_1, \ldots, V_{n-1}\}$ *definido por:*

$$V_j = \sum_{i=0}^{n-1} \alpha^{i(j+1)} v_i, \quad j = 0, \ldots, n-1. \tag{4.1}$$

O índice $i$ denota tempo-discreto, e $\mathbf{v}$ a função domínio-tempo ou o sinal, o índice $j$ denota freqüência, e $\mathbf{V}$ a função domínio-freqüência ou o espectro.

Decorre da Definição 50 que qualquer fator de $s$ pode ser usado como comprimento do bloco de uma transformada de Fourier. Todavia, a transformada de Fourier pode não existir em um anel de Galois para qualquer valor do comprimento de bloco uma vez que estes devem corresponder à ordem de cada um dos elementos do anel. A transformada de Fourier sobre $A$ com comprimento de bloco $n$ assume valores em um anel de extensão $R$. Podemos representar um vetor $\mathbf{v}$ por um polinômio $v(x)$. O polinômio $v(x) = v_{n-1}x^{n-1} + \ldots + v_1 x + v_0$. O polinômio $\mathbf{v}(x)$ pode ser transformado no seguinte polinômio.

$$V(x) = V_{n-1}x^{n-1} + \ldots + V_1 x + V_0, \tag{4.2}$$

por meio da transformada de Fourier no anel de Galois, $V(x)$ é chamado **polinômio espectral** ou o **polinômio associado** a $v(x)$.

**Lema 1.** *[1] Se $\alpha \in G_s$ é um elemento de ordem $n$, então:*

$$\sum_{i=0}^{n-1} \alpha^i = \begin{cases} 0, & se \quad \alpha \neq 1 \\ n, & se \quad \alpha = 1 \end{cases} \tag{4.3}$$

*onde $n$ é interpretado como um número inteiro módulo $p$.*

**Lema 2.** *[1] Seja $\alpha \in G_s$ um elemento de ordem $n$. Se $v(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1} \in A[x]$, então*

$$nv_i = \sum_{i=0}^{n-1} v(\alpha^{j+1})\alpha^{-i(j+1),} \qquad i = 0, 1, \ldots, n-1 \tag{4.4}$$

*onde o produto $nv_i$, para $i = 0, 1, \ldots, n-1$, é interpretado módulo $p$.*

Relembrando que a partir da Seção 4.2 desenvolveremos códigos cíclicos sobre anéis que vão ser úteis para a transformada Discreta discreta de Fourier sobre anéis.

## 4.2 Códigos Cíclicos sobre Anéis de Inteiros Residuais

Nesta seção apresentaremos definições e teoremas que estão relacionados com os códigos cíclicos sobre anéis $\mathbb{Z}_q$ ($q \geq 4$ e inteiro). Estes conceitos e resultados servirão de suporte para o desenvolvimento dos códigos BCH, que faremos na Seção 4.4.

**Definição 51** (Módulo Livre)**.** *Seja $R$ um anel. Um módulo livre é um $R-$módulo gerado por um conjunto de vetores linearmente independentes.*

**Definição 52** (Código Linear)**.** *Um código linear $(n, k)$ sobre $\mathbb{Z}_q$ é definido como um módulo livre de dimensão $k$ no espaço de todas as n-uplas de $\mathbb{Z}_q^n$.*

**Definição 53.** *Um código linear $\mathcal{C}$ com parâmetros $(n, k)$ sobre $\mathbb{Z}_q$ é cíclico se, para $\underline{v} = (v_0,\ v_1,\ v_2,\ \ldots,\ v_{n-1}) \in \mathcal{C}$, todo deslocamento cíclico $\underline{v}^{(1)} = (v_{n-1},\ \ v_0,\ v_1,\ \ v_2,\ \ \ldots,\ \ v_{n-2}) \in \mathcal{C}$, com $v_i \in \mathbb{Z}_q$ $0 \leq i \leq n-1$.*

**Teorema 26.** *[3] Um conjunto $S$ de elementos em $R_n$ corresponde a um código cíclico se, e somente se, $S$ é um ideal em $R_n$.*

Demonstração*:* Se $S$ corresponde a um código cíclico linear então para $v_1(x)$ e $v_2(x) \in S$, temos que $v_1(x) \pm v_2(x) \in S$. Se $v(x) \in S$, então $x \cdot v(x) \in S$ (de acordo com a Definição 53). Logo, se $w(x) = w_0 + w_1x + w_2x^2 + \ldots + w_{n-1}x^{n-1} \in R_n$ e $v(x) \in S$, então $w(x) \cdot v(x) = w_0v(x) + w_1v(x)x + w_2v(x)x^2 + \ldots + w_{n-1}v(x)x^{n-1} \in S$, sabendo que cada termo pertence a $S$. Estas duas operações caracterizam $S$ como um ideal de $R_n$.

Por outro lado, se $S$ é um ideal em $R_n$, então: 1) A soma de dois elementos em $S$ é um elemento de $S$; 2) Se $v(x) \in S$, então $x \cdot v(x) \in S$. Logo, por 1) e 2) concluímos que $S$ é um código cíclico. ∎

Os códigos cíclicos são, geralmente, representados na forma polinomial. Assim, considere a palavra-código $\mathbf{v} = (v_0,\ v_1,\ v_2, \ldots, v_{n-1})$ de um código cíclico $\mathcal{C}$. Podemos representá-la pelo polinômio:

$$v(x) = v_0 + v_1x + v_2x^2 + \ldots + v_{n-1}x^{n-1}. \tag{4.5}$$

O produto de $x$ por $v(x)$ módulo $x^n - 1$ é dado por:

$$v^1(x) = v_{n-1} + v_0 x + v_1 x^2 + v_2 x^3 + \ldots + v_{n-2} x^{n-1}, \tag{4.6}$$

que corresponde à palavra-código:

$$\mathbf{v}^1 = (v_{n-1},\ v_0,\ v_1,\ v_2, \ldots,\ v_{n-2}), \tag{4.7}$$

a qual é um deslocamento cíclico da palavra-código:

$$\mathbf{v} = (v_0,\ v_1,\ v_2, \ldots,\ v_{n-1}). \tag{4.8}$$

Portanto, $v^1(x)$ é obtido através do produto $x \cdot v(x) \bmod(x^n - 1)$ no anel quociente $R_n = \dfrac{\mathbb{Z}_q[x]}{\langle x^n - 1 \rangle}$, onde $\langle x^n - 1 \rangle$ representa o ideal gerado por $x^n - 1$. A adição de duas palavras-código é feita em $\mathbb{Z}_q[x]$. Observe que o conjunto de todas as palavras pertencentes a um código cíclico $\mathcal{C}$ formam um subconjunto do anel $R_n$, isto é, o conjunto de todos os polinômios cujo grau é menor que $n$.

**Teorema 27.** *[3] Seja $\mathcal{C}$ um ideal em $R_n = \dfrac{\mathbb{Z}_q[x]}{\langle x^n - 1 \rangle}$ e $g(x)$ um polinômio mônico com o menor grau em $\mathcal{C}$. Portanto, $\mathcal{C} = \langle g(x) \rangle$. Logo, o código $\mathcal{C}$ consiste de todos os múltiplos de $g(x)$. Dizemos então que $\mathcal{C}$ é um ideal principal.*

DEMONSTRAÇÃO*:*

Suponha que $g(x)$ seja mônico. Seja $v(x)$ um polinômio em $\mathcal{C}$. Então:

$$v(x) = g(x) \cdot b(x) + r(x), \quad \partial r < \partial g \tag{4.9}$$

onde $\partial p$ denota o grau do polinômio $p(x)$. Pela definição de ideal, $r(x) \in \mathcal{C}$. Isto contradiz a escolha de $g(x)$, a menos que $r(x) \equiv 0$. Portanto, $v(x) = g(x) \cdot b(x)$. Ou seja, todo polinômio em $\mathcal{C}$ é múltiplo de $g(x)$. Provaremos agora a unicidade de $g(x)$. Suponha $h(x)$ um polinômio de menor grau em $\mathcal{C}$ e mônico. Então $k(x) = g(x) - h(x)$ é um polinômio em $\mathcal{C}$ de grau menor que o de $g(x)$ e $h(x)$, o que é um absurdo. Logo, $g(x)$ é único. ∎

**Proposição 3.** *[4] Seja $\mathcal{C}$ um ideal em $R_n = \dfrac{\mathbb{Z}_q[x]}{\langle x^n - 1 \rangle}$, isto é, um código cíclico de comprimento $n$. Se existir um polinômio de grau mínimo em $\mathcal{C}$, cujo coeficiente dominante é um elemento invertível em $\mathbb{Z}_q$, então o polinômio mônico de grau mínimo em $\mathcal{C}$ é único.*

**Teorema 28.** *[4] Seja $\mathcal{C}$ um ideal principal em $R_n$. Se o coeficiente dominante do polinômio de menor grau em $\mathcal{C}$, $g(x)$ é um elemento invertível, então $g(x)$ divide $(x^n-1)$. Observe que se este polinômio for mônico, então $g(x)$ divide $(x^n-1)$.*

DEMONSTRAÇÃO: *Suponha que $g(x)$ seja um polinômio de menor grau em $\mathcal{C}$. Então existem e são únicos os polinômios $a(x)$ e $r(x)$ tais que:*

$$x^n - 1 = g(x) \cdot a(x) + r(x), \quad \partial r < \partial g. \tag{4.10}$$

*Portanto, segue que:*

$$-g(x) \cdot a(x) = -(x^n - 1) + r(x). \tag{4.11}$$

*Logo, $r(x)$ está em $\langle g(x) \rangle$ e tem grau menor do que $g(x)$. Isto é uma contradição (sendo que o polinômio de menor grau em $\mathcal{C}$ é $g(x)$) a menos que $r(x) \equiv 0$. Isto implica que $g(x) \mid (x^n - 1)$.* ■

**Teorema 29.** *[3] Se $g(x) \in \mathcal{C}$ e $g(x)$ divide $(x^n - 1)$, então $g(x)$ tem grau mínimo em $\mathcal{C} = \langle g(x) \rangle$.*

DEMONSTRAÇÃO: *Suponha a existência de um polinômio $b(x)$ pertencente a $\langle g(x) \rangle$ tal que $\partial b < \partial g$. Como $b(x) \in \langle g(x) \rangle$, então:*

$$a(x) \cdot g(x) = (x^n - 1) \cdot d(x) + b(x). \tag{4.12}$$

*Portanto, segue que :*

$$b(x) = a(x) \cdot g(x) - (x^n - 1) \cdot d(x) + b(x). \tag{4.13}$$

*Como $g(x) \mid (x^n - 1)$, então $g(x) \mid (a(x) \cdot g(x) - (x^n - 1) \cdot d(x))$, o que implica que $g(x) \mid b(x)$. Isto é uma contradição, pois assumimos que $\partial b < \partial g$. Logo, se $g(x) \mid (x^n - 1), g(x)$ é o polinômio de menor grau em $\langle g(x) \rangle$.* ■

Os Teoremas 28 e 29 nos fornecem um método de construção de códigos cíclicos sobre anéis de inteiros residuais, que é exatamente análogo ao da construção dos códigos cíclicos sobre corpos finitos, ou seja, por meio da fatoração do polinômio $(x^n - 1)$ sobre o anel de interesse por considerar um fator (ou produto de fatores) como polinômio gerador do código a ser desenvolvido.

**Teorema 30.** *[3] Se $g(x) \mid (x^n - 1)$ e $\partial g = n - k$, então a dimensão de $\mathcal{C} = \langle g(x) \rangle$ é $k$. Se*

$$g(x) = g_0 + g_1 x + ... + x^{n-k}, \tag{4.14}$$

*então uma matriz geradora de $\mathcal{C}$ é dada por:*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{n-k-2} & g_{n-k-1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & 1 \end{bmatrix}. \tag{4.15}$$

DEMONSTRAÇÃO: *Os vetores $g(x)$, $x \cdot g(x)$, $x^2 \cdot g(x)$, ..., $x^{k-1} \cdot g(x)$ são linearmente independentes. Do contrário, existiriam elementos $a_i$, $0 \leq i \leq k-1$, não todos nulos, pertencentes a $\mathbb{Z}_p$ tais que:*

$$\begin{aligned} & a_0 \cdot g(x) \ + \ a_1 \cdot x \cdot g(x) \ + \ a_2 \cdot x^2 \cdot g(x) \ + \ \cdots \ + \ a_{k-1} \cdot x^{k-1} \cdot g(x) = \\ = \ & (a_0 \ + \ a_1 \cdot x \ + \ a_2 \cdot x^2 + \cdots \ + \ a_{k-1} \cdot x^{k-1}) g(x) = 0. \end{aligned}$$

*Como $g(x)$ é mônico e este produto tem grau menor que $n$, esta última igualdade só se verifica se $a_0 = a_1 = a_2 = \cdots = a_{k-1} = 0$. Portanto, estes vetores são linearmente independentes. Vamos agora mostrar que eles geram $\mathcal{C}$. Seja então um polinômio $v(x)$ em $\mathcal{C}$. Sabemos que $v(x) = c(x)g(x)$, onde $\partial c \leq k-1$. Disso segue que:*

$$\begin{aligned} c(x)g(x) \ &= \ (c_0 \ + \ c_1 \cdot x \ + \ c_2 \cdot x^2 \ + \ \cdots \ + \ c_{k-1} \cdot x^{k-1}) g(x) \\ &= \ c_0 \cdot g(x) \ + \ c_1 \cdot g(x) \cdot x \ + \ c_2 \cdot g(x) \cdot x^2 \ + \ \cdots \ + \ c_{k-1} \cdot g(x) \cdot x^{k-1}. \end{aligned}$$

*Logo, as linhas de $G$ geram o $(n, k)$ código cíclico sobre o anel $\mathbb{Z}_q$.* ∎

Uma extensão natural do processo de construção de códigos cíclicos é como estabelecido a seguir:

**Proposição 4.** *[4] Se $\mathcal{C}$ é um código cíclico sobre $\mathbb{Z}_q$ onde $q = p_1^{k_1} p_2^{k_2} \cdots p_q^{k_q}$, então $\mathcal{C} = \bigoplus_{i=1}^{q} \mathcal{C}_i$, onde $\mathcal{C}_i$ é um código cíclico sobre $p_i^{k_i}$, $1 \leq i \leq q$, e $\oplus$ denota sua soma direta.*

## 4.3 Extensão Galoisiana de Anéis

A motivação para utilização do conceito de extensão de Galois em teoria da codificação está diretamente relacionada com a construção de códigos cíclicos sobre anéis locais $\mathbb{Z}_q$, onde $q$ é uma potência de um primo $q = p^m,\ m \geq 2$.

A principal diferença na construção de códigos cíclicos sobre anéis e sobre corpos está no fato de que as raízes do polinômio gerador dos códigos cíclicos sobre anéis encontram-se na extensão do anel $\mathbb{Z}_q$, ao invés de serem encontradas na extensão do corpo $\mathbb{F}_q \cong GF(p^r)$. Neste caso, temos a seguinte definição:

**Definição 54** (Código Cíclico Primitivo)**.** *Um código cíclico sobre $\mathbb{Z}_q$ com comprimento $n = q^r - 1$, onde $q = p^m$ e $r$ é o grau de extensão de Galois, é chamado* ***código cíclico primitivo****.*

**Definição 55** (Comprimento de bloco Primitivo)**.** *Um comprimento de bloco $n$ da forma $n = q^m - 1$ onde $q$ é uma potência de primo é denomianado* ***comprimento de bloco primitivo****.*

Considerando o caso em que $p$ e $n$ são relativamente primos, isto é, que o $\text{mdc}(n, p) = 1$, podemos garantir que $x^n - 1$ não apresenta fatores quadráticos. De acordo com a Seção 4.2 sabemos que um código cíclico de comprimento $n$ sobre $\mathbb{Z}_q$ é o ideal principal no anel de polinômios $\mathbb{Z}_q$ módulo $(x^n - 1)$ e que este ideal é gerado por qualquer polinômio $g(x)$ que divide $(x^n - 1)$.

Seja $\mathbb{Z}_q[x]$ o anel de polinômios na variável $x$ sobre $\mathbb{Z}_q$, e $p(x)$ um polinômio primitivo de grau $r$, irredutível sobre $GF(q)$ e conseqüentemente também sobre $\mathbb{Z}_q$. Representamos por $GR(p^m, r)$, o quociente $\mathbb{Z}_q[x]$ pelo ideal gerado por $p(x)$, ou seja,

$$R \cong GR(p^m, r) \cong \frac{\mathbb{Z}_q}{\langle p(x) \rangle}. \tag{4.16}$$

Além disso, $R$ é um anel comutativo com identidade denominado extensão de Galois de dimensão $r$ de $\mathbb{Z}_q$. Esta extensão é única a menos de isomorfismo. Dizemos que o anel $R \cong GR(p^m, r)$ é um anel local, isto é, seus elementos divisores de zero formam um grupo

abeliano aditivo e consistem dos polinômios de grau menor ou igual a $r-1$ cujos coeficientes são divisores de zero em $\mathbb{Z}_q$. $R^*$ é o grupo dos elementos invertíveis ou grupo das unidades de $R$ e a sua ordem é $p^{(m-1)r}(p^r-1)$. Portanto, um polinômio $p(x) \in R$ com pelo menos um coeficiente invertível em $\mathbb{Z}_q$ não é divisor de zero em $R$ e, logo, pertence a $R^*$, ou seja, é sempre possível encontrar um polinômio $q(x) \in R$, tal que $p(x) \cdot q(x) = 1$. A partir disto, podemos enunciar o seguinte resultado.

**Teorema 31.** *[3] Seja $\beta$ um elemento primitivo de $G_n$ (o subgrupo cíclico de $R^*$ contendo todas as raízes de $x^n-1$), onde $n = p^m - 1$. Então, o elemento $\gamma = \beta^{l_1} - \beta^{l_2}$ é invertível em $R$ se $0 \leq l_1, l_2 \leq s-1$ e $l_1 \neq l_2$.*

Neste sentido, apresentaremos, de forma geral, um procedimento de construção de um código sobre um anel de Galois. Dado um anel $\mathbb{Z}_q$, onde $q = p^m$, inicialmente determinamos o polinômio gerador de um código de bloco cíclico $q^r-$ário. O anel de Galois em $\mathbb{Z}_{p^m}[x]$, consiste do conjunto dos polinômios de grau menor ou igual a $r-1$ pertencentes a $\mathbb{Z}_{p^m}[x]$, cujas operações binárias de adição e multiplicação são tomadas módulo $p(x)$.

Com o objetivo de determinar um grupo multiplicativo dentro de $GR(p^m, r)$, suponha que $\alpha$ é uma raiz de $p(x)$. Portanto, é possível expressar uma dada potência de $\alpha$ em função de outras menores, ferramenta essencial para se determinar os elementos desse grupo multiplicativo. Ressalta-se que as operações devem ser realizadas em $\mathbb{Z}_{p^m}$. Caso a ordem $\theta$ do grupo multiplicativo seja par, o termo $x^\theta - 1$ não pode ser fatorado de maneira única. Logo, deve-se determinar, nesse grupo multiplicativo, um elemento $\beta$ (potência de $\alpha$), cuja ordem $\delta$ seja uma multiplicidade ímpar da ordem de $\alpha$ no corpo $GF(p^r)$. Desta maneira, o termo $x^\delta - 1$ pode ser fatorado de forma única. Determinados os polinômios minimais associados a cada um dos elementos do grupo multiplicativo gerado por $\beta$, pode-se definir o polinômio gerador do código de bloco cíclico.

**Definição 56.** *Um polinômio $p(x)$ em $\mathbb{Z}_q[x]$ é uma unidade se existe um polinômio $a(x) \in \mathbb{Z}_q[x]$ tal que $a(x)p(x) = 1$.*

**Definição 57** (Polinômio Divisor de Zero)**.** *Um polinômio não nulo $p(x)$ é um divisor de zero em $\mathbb{Z}_q[x]$ se existe um polinômio $q(x) \in \mathbb{Z}_q[x],\ q(x) \neq 0$, tal que $p(x) \cdot q(x) = 0$.*

**Definição 58** (Polinômio Regular)**.** *Um polinômio $p(x)$ é dito regular se ele não é divisor de zero no anel $\mathbb{Z}_q[x]$.*

**Definição 59** (Polinômio Regular Local)**.** *Um polinômio regular $p(x)$ é chamado local se $\frac{\mathbb{Z}_q}{\langle p(x)\rangle}$ é uma extensão **local** de $\mathbb{Z}_q$.*

A garantia da irredutibilidade do polinômio $p(x)$ sobre $\mathbb{Z}_q$ é dada pelo seguinte resultado:

**Teorema 32.** *[4] Seja $p(x)$ um polinômio regular em $\mathbb{Z}_q$. Se existe uma aplicação $\mu$, chamada projeção natural, tal que $\mu(p(x))$ seja diferente de zero e irredutível em $GF(p)$, ent ao $p(x)$ é irredutível em $\mathbb{Z}_q$.*

Nosso interesse reside na classe dos códigos cíclicos, pois temos como objetivo encontrar um procedimento para a construção de tais códigos. O primeiro passo está relacionado com a fatoração de $(x^n - 1)$. Como $R^*$, o grupo das unidades de $R$, é um grupo abeliano multiplicativo, ele pode ser expresso como um produto direto de grupos cíclicos. Uma vez identificado este grupo, o problema da construção de códigos cíclicos se reduz à escolha de determinados elementos deste grupo que sejam raízes do polinômio gerador $g(x)$, que divide $(x^n - 1)$.

A seguir enunciaremos um conjunto de teoremas fornecendo os elementos necessários para a construção do subgrupo cíclico $G_s$, grupo das unidades $R^*$, contendo todas as raízes de $(x^n - 1)$.

**Teorema 33.** *[4] Existe um único subgrupo cíclico de $R^*$ cuja ordem é relativamente prima a $p$. Este subgrupo tem ordem $p^{mh} - 1$.*

O Teorema 33 estabelece que $R^*$ tem um e somente um subgrupo cíclico cuja ordem $p^{mh} - 1$ é relativamente prima a $p$. O teorema a seguir fornece um método de obtenção do subgrupo cíclico.

**Teorema 34.** *[4] Suponha que $f \in R$ gere um subgrupo de ordem $n$ em $R^*$, onde $mdc(n, p) = 1$. Então o polinômio $(x^n - 1)$ pode ser fatorado como $x^n - 1 = (x - f) \cdot (x - f^2) \ldots (x - f^n)$ se, e somente se, $R_p(f)$ tem ordem $n$ em $\mathbb{F}^*$ (grupo multiplicativo de $GF(p^m)$), onde $R_p(f)$ é o resto da divisão de $f$ por $p$ (redução de $f$ módulo $p$).*

**Corolário 6.** *[4] Um polinômio $h(x)$, que divide $(x^n - 1)$ e tem coeficientes em $\mathbb{Z}_q$, pode ser fatorado sobre $G_s$ como:*

$$h(x) = (x - \beta^{e_1})(x - \beta^{e_2}) \dots (x - \beta^{e_j}), \tag{4.17}$$

*se, e somente se, $R_p(h(x))$ pode ser fatorado sobre $GF(p^m)$ como:*

$$R_p(h(x)) = (x - (R_p(\beta))^{e_1})(x - (R_p(\beta))^{e_2}) \dots (x - (R_p(\beta))^{e_j}), \tag{4.18}$$

*onde $\beta$ é um elemento primitivo de $G_s$ e $e_j \in \mathbb{Z}$.*

**Teorema 35.** *[3] Suponha que $\bar{f} = R_p(f)$ gere um subgrupo cíclico de ordem $n$ em $\mathbb{F}^*$. Então $f$ gera um subgrupo cíclico de ordem $nd$ em $R^*$, onde $d$ é um inteiro maior ou igual a um, e $f^d$ gera o subgrupo cíclico $G_s$ de $R^*$.*

O Teorema 35 é útil na determinação do gerador. Do Corolário 6 segue que $M_i(x)$, o polinômio minimal de $\beta^i$ sobre $R^*$ (onde $\beta$ é primitivo em $G_s$), terá como raízes todos os elementos distintos na sequência

$$\beta^i, (\beta^i)^p, (\beta^i)^{p^2} \dots (\beta^i)^{p^m - 1}. \tag{4.19}$$

Portanto, $M_i(x)$ pode ser construído de maneira idêntica à construção de $m_i(x)$, o polinômio minimal de $R_p(\beta^i)$ sobre $GF(p)$.

## 4.4 Códigos BCH sobre Anéis Locais

Nesta seção iremos descrever a construção de códigos BCH sobre anéis comutativos finitos locais $A$ com identidade. Esta construção é bastante semelhante à construção de códigos BCH sobre corpos finitos. A diferença é que os elementos da matriz verificação de paridade estão num anel conveniente.

Os códigos BCH são uma generalização dos códigos de Hamming para múltipla correção de erros e formam a classe dos melhores códigos construtivos para canais em que os erros afetam símbolos de maneira independente.

Os códigos BCH foram descobertos por R. C. Bose e D. K. Ray-Chaudhuri, e independentemente por A. Hocquenghem, os quais levam as iniciais de seus nomes.

Os códigos BCH são definidos a partir da matriz verificação de paridade e projetados para corrigir até $t$ erros, para um $t$ qualquer.

O estudo dos códigos BCH é importante nos seguintes aspectos:

- As taxas dos códigos BCH são assintoticamente ruins, ou seja, quando o comprimento da palavra-código não é grande, existem bons códigos nesta classe, caso contrário, o desempenho destes é prejudicado devido às baixas taxas de transmissão ;

- A real importância dos códigos BCH vem da facilidade de implementação do algoritmo de correção de erros denominado algoritmo de Berlekamp-Massey modificado;

- As técnicas de codificação e decodificação são relativamente simples;

- A subclasse não binária dos códigos Reed-Solomon tem certas propriedades de otimalidade e uma estrutura de distância bem definida;

- O conhecimento destes códigos, é, provavelmente, o ponto inicial para estudar outras classes de códigos cíclicos;

**Definição 60.** *Um código cíclico de comprimento n sobre $GF(p)$ é denominado um código BCH com distância de projeto d se o seu gerador $g(x)$ for o mínimo múltiplo comum dos polinômios minimais de*

$$\beta^r, \beta^{r+1}, \beta^{r+2}, \ldots, \beta^{r+d-2} \tag{4.20}$$

*para algum r inteiro não negativo, onde $\beta$ é uma raiz primitiva (elemento primitivo) de $(x^n - 1)$, em alguma extensão $GF(p^m)$ de $GF(p)$.*

Da Definição 60, temos:

**Definição 61.** *Se $n = p^m - 1$, ou seja, se $\beta$ for um elemento primitivo em $\mathbb{F}_q$, então o código BCH é chamado* ***primitivo****.*

Normalmente, consideramos $r = 1$, o que nos fornece o chamado código BCH no sentido estrito.

Os códigos BCH no sentido estrito definidos sobre anéis de inteiros, com distância de projeto $d$ e comprimento $n$, apresentam $\beta, \beta^2, \beta^3, \ldots, \beta^{2t}$ e seus conjugados como raízes de cada um de seus polinômios. Esta propriedade, juntamente com a Definição 53 de códigos cíclicos sobre anéis $\mathbb{Z}_q$, nos permite especificar a seguinte matriz:

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & (\beta)^2 & (\beta^2)^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\beta)^{2t} & (\beta^{2t})^2 & \cdots & (\beta^{2t})^{n-1} \end{bmatrix}. \tag{4.21}$$

A matriz $H$ é a matriz verificação de paridade para um código BCH. Observe que os elementos $\beta^i,\ 1 \leq i \leq 2t$ de $H$ pertencem a $G_s$, e portanto, os coeficientes de $\beta$ são tomados módulo $s$. Substituindo os elementos $\beta^i$ pelos vetores linha de comprimento $r(r-$uplas) correspondentes, temos a matriz $H$ sobre $\mathbb{Z}_q$.

O nosso interesse é a construção de códigos BCH sobre anéis $\mathbb{Z}_q$, para $q = p^m$ e $m \geq 2$, a qual é análoga à construção de códigos BCH sobre corpos. A diferença entre essas duas construções está no fato de que, na primeira, as raízes do polinômio gerador do código BCH encontram-se na extensão do anel $\mathbb{Z}_q$, ao invés de serem encontradas na extensão do corpo $\mathbb{F}_q$. Vale lembrar também que iremos considerar o caso no qual $mdc(n, p) = 1$.

Vamos agora especificar um código BCH de comprimento $n$ sobre $\mathbb{Z}_q$ (onde $n|p^m - 1$) em termos das raízes do polinômio gerador $g(x)$ em $G_s$. Seja $\beta$ um elemento primitivo de $G_s$. Se $\beta^{e_1}, \beta^{e_2}, \ldots, \beta^{e_j}$ são raízes de $g(x)$, então podemos gerar um código tipo BCH com símbolos de $\mathbb{Z}_q$ se escolhermos $g(x)$ como: polinômios minimais de

$$g(x) = mmc(M_{e_1}(x), M_{e_2}(x), \ldots, M_{e_j}(x)), \tag{4.22}$$

onde $M_{e_i}(x)$ é o polinômio minimal de $\beta^{e_i}$. Além disso,

$$\bar{g}(x) = R_p(g(x)) = mmc(m_{e_1}(x), m_{e_2}(x), \ldots, m_{e_j}(x)), \tag{4.23}$$

onde $m_{e_i}(x)$ é o polinômio minimal de $R_p(\beta^{e_i})$, gera um código BCH com símbolos sobre $GF(p)$.

Logo, a construção de códigos BCH cíclicos sobre o anel $\mathbb{Z}_q$ reduz-se à escolha de elementos do subgrupo cíclico $G_s$ para serem raízes do polinômio gerador $g(x)$.

**Observação 1.** *O método sistemático para o cálculo do mínimo múltiplo comum de um conjunto de polinômios $\{p_1(x), p_2(x), \ldots, p_n(x)\}$ é computar o máximo divisor comum, através do Algoritmo de Euclides e então utilizar a seguinte relação:*

$$mmc(p_1(x), p_2(x), \ldots, p_n(x)) = \frac{\prod_{i=1}^{n} p_1(x)}{mdc(p_1(x), p_2(x), \ldots, p_n(x))} \tag{4.24}$$

Os Teoremas 31 e 32 estabelecem um limitante inferior para a distância de Hamming do código BCH construído:

**Teorema 36.** *[4] Seja $g(x)$ o polinômio gerador de um código cíclico de comprimento $n$ com símbolos sobre $\mathbb{Z}_q$ e sejam também $\beta^{e_1}, \beta^{e_2}, \ldots, \beta^{e_j}$ as raízes de $g(x)$ em $G_s$, onde $\beta$ tem ordem $s$. Então, a distância mínima do código é maior que o número máximo de inteiros consecutivos módulo $n$ no conjunto $E = \{e_1, e_2, \ldots, e_j\}$.*

**Lema 3.** *Seja $\alpha$ um elemento de $G_s$ de ordem $s$. Então as diferenças $\alpha^{l_1} - \alpha^{l_2}$ são unidades em $R$ se $0 \leq l_1 \neq l_2 \leq s - 1$.*

**Teorema 37.** *[4] A distância mínima de Hamming de um código BCH satisfaz a relação:*

$$d \geq 2t + 1, \tag{4.25}$$

*onde $t$ é a capacidade de correção do código.*

Observe que os polinômios geradores dos códigos BCH cíclicos são construídos de acordo com o limitante para a distância mínima indicada nos Teoremas 36 e 37.

### 4.4.1 Exemplos de construção de códigos BCH sobre anéis locais

Nesta subseção, apresentaremos a construção de códigos BCH sobre anéis locais $\mathbb{Z}_q$ de ordem $n = p^r - 1$, onde $q = p^m$, e $r$ é o grau da extensão de Galois.

**Exemplo 2.** *Código BCH sobre* $\mathbb{Z}_4$

Apresenta-se aqui a construção de códigos BCH sobre o anel $\mathbb{Z}_4$ através de extensões de Galois de graus 2 e 3.

Primeiramente, considere o anel $GR(p^m, r) = GR(4, 2)$ dada pela extensão de Galois de grau 2.

$$GR(4,2)[x] \cong \frac{\mathbb{Z}_4[x]}{\langle x^2 + x + 1\rangle} = \{a + bx; a, b \in \mathbb{Z}_4\}. \tag{4.26}$$

Considere, agora, o corpo $GF(p^r) = GF(4)$, onde

$$\begin{aligned} GF(4)[x] \cong \mathbb{F}_4[x] \cong \frac{\mathbb{F}_2[x]}{\langle x^2 + x + 1\rangle} &= \{a' + b'x; a', b' \in \mathbb{F}_2\} \\ &= \{0, 1, x, 1 + x\}. \end{aligned} \tag{4.27}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_4$. Logo, $\alpha$ é uma raiz de $x^2 + x + 1 = 0$, ou seja, $\alpha^2 = -\alpha - 1$ em $\mathbb{Z}_2$ teremos $\alpha^2 = 1 + \alpha$. Assim, o grupo multiplicativo de $\mathbb{F}_4$ apresenta os seguintes elementos:

| | | |
|---|---|---|
| $1 = \alpha^0$ | $\longrightarrow$ | $(1 \ \ 0)$ |
| $\alpha = \alpha^1$ | $\longrightarrow$ | $(0 \ \ 1)$ |
| $\alpha^2 = 1 + \alpha$ | $\longrightarrow$ | $(1 \ \ 1)$ |
| $\alpha^3 = \alpha^0$ | $\longrightarrow$ | $(1 \ \ 0)$ |

Tabela 4.1: Grupo Multiplicativo de $GF(4)$

Seja $f = (0\ 1) \in GR^*(4, 2)$, onde $GR^*(4, 2)$ denota o grupo das unidades de $GR(4, 2)$. Portanto, $\overline{f} = R_2(f) = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 3$ em $\mathbb{F}_4$, lembrando que $R_2(f)$ é a redução módulo 2 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 3d$ em $GR^*(4, 2)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_3$ de $GR^*(4, 2)$.

As operações em $GR^*(4, 2)$ são realizadas módulo $x^2 + x + 1$. Logo, $x^2 = -x - 1$; porém, como os coeficientes de $GR^*(4, 2)$ estão em $\mathbb{Z}_4$, temos que $x^2 = 3x + 3$. Assim, considerando

$(f) = (0\ 1) = x$, a representação dos elementos do grupo das unidades de $GR(4,2)$ é como mostrado abaixo:

| | | |
|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0)$ |
| $x = x^1$ | $\longrightarrow$ | $(0\ \ 1)$ |
| $x^2 = 3 + 3x$ | $\longrightarrow$ | $(3\ \ 3)$ |
| $x^3 = x^0$ | $\longrightarrow$ | $(1\ \ 0)$ |

Tabela 4.2: Grupo das Unidades de $GR(4,2)$

Portanto, $nd = 3$, assim, $d = 1$. Logo, $f = x = (0\ 1)$ gera um grupo de ordem 1 em $GR^*(4,2)$ e também um grupo de ordem 3 em $GR^*(4,2)$. Logo, $\beta = x$ é um elemento primitivo em $G_3$. Podemos agora construir um código BCH de comprimento $n = 3$ sobre $\mathbb{Z}_4$. Considere que a distância mínima de projeto (distância de Hamming) do código seja $d \geq 3$. O polinômio gerador $g(x)$ do código tem como raízes $\beta$ e $\beta^2$. Assim,

$$g(x) = mmc(M_1(x), M_2(x)) = 1 + x + x^2 \tag{4.28}$$

onde $M_i(x)$ é o polinômio minimal de $\beta^i, i = 1, 2$.

O polinômio minimal de $\beta$ é dado por:

$$M_1(x) = M_2(x) = (x - \beta)(x - \beta^2) = 1 + x + x^2. \tag{4.29}$$

Note que os polinômios minimais de $\beta$ e $\beta^2$ são iguais, isto é,

$$M_2(x) = M_1(x). \tag{4.30}$$

Assim, $g(x) = 1+x+x^2$ gera o código BCH desejado. Este polinômio gerador corresponde à seguinte matriz geradora:

$$G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}. \tag{4.31}$$

A matriz verificação de paridade correspondente é dada por:

$$H = \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 3 & 3 \\ 1 & 0 & 3 & 3 & 0 & 1 \end{bmatrix}. \tag{4.32}$$

Considere, agora, o anel $GR(p^m, r) = GR(4, 3)$ dado pela extensão de grau 3, isto é,

$$GR(4,3)[x] \cong \frac{\mathbb{Z}_4[x]}{\langle x^3 + x + 1\rangle} = \{a + bx + cx^2; a, b, c \in \mathbb{Z}_4\}. \tag{4.33}$$

Considere, agora, o corpo $GF(p^r) = GF(8)$, onde

$$\begin{aligned} GF(8)[x] \cong \mathbb{F}_8[x] \cong \frac{\mathbb{F}_2[x]}{\langle x^3 + x + 1\rangle} &= \{a' + b'x + c'x^2; a', b', c', \in \mathbb{F}_2\} \\ &= \{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}. \end{aligned} \tag{4.34}$$

Analogamente à extensão de Galois de grau 2, a Tabela 4.3 apresenta os elementos do grupo multiplicativo de $\mathbb{F}_8$.

| | | | | | |
|---|---|---|---|---|---|
| $1 = \alpha^0$ | $\longrightarrow$ | (1 0 0) | $\alpha = \alpha^1$ | $\longrightarrow$ | (0 1 0) |
| $\alpha^2 = \alpha^2$ | $\longrightarrow$ | (0 0 1) | $\alpha^3 = 1 + \alpha$ | $\longrightarrow$ | (1 1 0) |
| $\alpha^4 = 1 + \alpha^2$ | $\longrightarrow$ | (1 0 1) | $\alpha^5 = \alpha + \alpha^2$ | $\longrightarrow$ | (0 1 1) |
| $\alpha^6 = 1 + \alpha + \alpha^2$ | $\longrightarrow$ | (1 1 1) | $\alpha^7 = \alpha^0$ | $\longrightarrow$ | (1 0 0) |

Tabela 4.3: Grupo Multiplicativo de $GF(8)$

Seja $f = (0\ 1\ 0) \in GR^*(4, 3)$. Então, $\overline{f} = R_2(f) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 7$ em $\mathbb{F}_8$, lembrando que $R_2(f)$ é a redução módulo 2 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 7d$ em $GR^*(4, 3)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_7$ de $GR^*(4, 3)$.

As operações em $GR^*(4, 3)$ são feitas módulo $x^3 + x + 1$. Logo, $x^3 = 3x + 3$, porém, como os coeficientes de $GR^*(4, 3)$ estão em $\mathbb{Z}_4$. Assim, considerando $(f) = (0\ 1\ 0) = x$, a Tabela 4.4 mostra representação dos elementos do grupo das unidades de $GR(4, 3)$.

Portanto, $nd = 14$, implicando que $d = 2$. Logo, $f$ gera um grupo de ordem 14 em $GR^*(4, 3)$. Conseqüentemente, $f^2 = x^2 = (0\ 0\ 1)$ gera também um grupo de ordem 7 em $GR^*(4, 3)$. Logo, $\beta = x^2$ é um elemento primitivo em $G_7$.

Passamos agora à construção de um código BCH de comprimento $n = 7$ sobre $\mathbb{Z}_4$. Considerando que a distância mínima de projeto do código seja $d \geq 3$, o polinômio gerador $g(x)$ do código tem como raízes $\beta$ e $\beta^2$.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ 0\ 0)$ | $x = x^1$ | $\longrightarrow$ | $(0\ 1\ 0)$ |
| $x^2 = x^2$ | $\longrightarrow$ | $(0\ 0\ 1)$ | $x^3 = 3 + 3x$ | $\longrightarrow$ | $(3\ 3\ 0)$ |
| $x^4 = 3x + 3x^2$ | $\longrightarrow$ | $(0\ 3\ 3)$ | $x^5 = 1 + x + 3x^2$ | $\longrightarrow$ | $(1\ 1\ 3)$ |
| $x^6 = 1 + 2x + x^2$ | $\longrightarrow$ | $(1\ 2\ 1)$ | $x^7 = 3 + 2x^2$ | $\longrightarrow$ | $(3\ 0\ 2)$ |
| $x^8 = 2 + x$ | $\longrightarrow$ | $(2\ 1\ 0)$ | $x^9 = 2x + x^2$ | $\longrightarrow$ | $(0\ 2\ 1)$ |
| $x^{10} = 3 + 3x + 2x^2$ | $\longrightarrow$ | $(3\ 3\ 2)$ | $x^{11} = 2 + x + 3x^2$ | $\longrightarrow$ | $(2\ 1\ 3)$ |
| $x^{12} = 1 + 3x + x^2$ | $\longrightarrow$ | $(1\ 3\ 1)$ | $x^{13} = 3 + 3x^2$ | $\longrightarrow$ | $(3\ 0\ 3)$ |
| $x^{14} = x^0$ | $\longrightarrow$ | $(1\ 0\ 0)$ | | | |

Tabela 4.4: Grupo das Unidades de $GR(4, 3)$

Os polinômios minimais de $\beta$ e $\beta^2$ são dados por:

$$M_1(x) = M_2(x) = M_4(x) = (x - \beta)(x - \beta^2)(x - \beta^4) = 3 + x + 2x^2 + x^3. \tag{4.35}$$

O polinômio gerador deste código é dado por $g(x) = mmc(M_1(x), M_2(x))$. Este polinômio gera o código BCH desejado, correspondente à seguinte matriz geradora:

$$G = \begin{bmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{bmatrix}. \tag{4.36}$$

A matriz verificação de paridade correspondente, é dada por:

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 3 & 1 & 2 & 1 & 2 & 1 & 0 & 3 & 3 & 2 & 1 & 3 & 1 \\ 1 & 0 & 0 & 0 & 3 & 3 & 2 & 1 & 0 & 1 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 1 & 3 & 3 & 2 \end{bmatrix}. \tag{4.37}$$

**Exemplo 3.** *Código BCH sobre* $\mathbb{Z}_9$

Apresentamos a seguir construção de códigos BCH sobre o anel $\mathbb{Z}_9$ através da extensão de Galois de graus 2 e 3.

Inicialmente, considere o anel $GR(p^m, r) = GR(9, 2)$ dado pela extensão de Galois de grau 2:

$$GR(9,2)[x] \cong \frac{\mathbb{Z}_9[x]}{\langle x^2 + x + 2\rangle} = \{a + bx; a, b \in \mathbb{Z}_9\}. \tag{4.38}$$

Considere, agora, o corpo $GF(p^r) = GF(9)$, onde

$$\begin{aligned} GF(9)[x] \cong \mathbb{F}_9[x] \cong \frac{\mathbb{F}_3[x]}{\langle x^2 + x + 2\rangle} &= \{a' + b'x; a', b' \in \mathbb{F}_3\} \\ &= \{0, 1, x, 1 + 2x, 2 + 2x, 2, 2x, 2 + x, 1 + x\}. \end{aligned} \tag{4.39}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_9$. Logo, $\alpha$ é uma raiz de $x^2 + x + 2 = 0$, ou seja, $\alpha^2 = -\alpha - 2$. Em $\mathbb{Z}_3$ teremos $\alpha^2 = 2\alpha + 1$. Assim, $\mathbb{F}_9$ apresenta os seguintes elementos do grupo multiplicativo, como mostramos na Tabela 4.5.

| | | | | | |
|---|---|---|---|---|---|
| $1 = \alpha^0$ | $\longrightarrow$ | (1 0) | $\alpha^5 = 2\alpha$ | $\longrightarrow$ | (0 2) |
| $\alpha = \alpha^1$ | $\longrightarrow$ | (0 1) | $\alpha^6 = 2 + \alpha$ | $\longrightarrow$ | (2 1) |
| $\alpha^2 = 1 + 2\alpha$ | $\longrightarrow$ | (1 2) | $\alpha^7 = 1 + \alpha$ | $\longrightarrow$ | (1 1) |
| $\alpha^3 = 2 + 2\alpha$ | $\longrightarrow$ | (2 2) | $\alpha^8 = \alpha^0$ | $\longrightarrow$ | (1 0) |
| $\alpha^4 = 2$ | $\longrightarrow$ | (2 0) | | | |

Tabela 4.5: Grupo Multiplicativo de $GF(9)$

Seja $f = (0\ 1) \in GR^*(9, 2)$, onde $GR^*(9, 2)$ denota o grupo das unidades de $GR(9, 2)$. Portanto, $\overline{f} = R_3(f) = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 8$ em $\mathbb{F}_9$, lembrando que $R_3(f)$ é a redução módulo 3 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 8d$ em $GR^*(9, 2)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_8$ de $GR^*(9, 2)$.

As operações em $GR^*(9, 2)$ são realizadas módulo $(x^2+x+2)$. Logo, $x^2 = -x-2$; porém, como os coeficientes de $GR^*(9, 2)$ estão em $\mathbb{Z}_9$, temos que $x^2 = 8x + 7$. Assim, considerando $(f) = (0\ 1) = x$, a representação dos elementos do grupo das unidades de $GR(9, 2)$ é como mostrado na Tabela 4.6.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | (1 0) | $x^{13} = 8x$ | $\longrightarrow$ | (0 8) |
| $x = x^1$ | $\longrightarrow$ | (0 1) | $x^{14} = 2 + x$ | $\longrightarrow$ | (2 1) |
| $x^2 = 7 + 8x$ | $\longrightarrow$ | (7 8) | $x^{15} = 7 + x$ | $\longrightarrow$ | (7 1) |
| $x^3 = 2 + 8x$ | $\longrightarrow$ | (2 8) | $x^{16} = 7 + 6x$ | $\longrightarrow$ | (7 6) |
| $x^4 = 2 + 3x$ | $\longrightarrow$ | (2 3) | $x^{17} = 6 + x$ | $\longrightarrow$ | (6 1) |
| $x^5 = 3 + 8x$ | $\longrightarrow$ | (3 8) | $x^{18} = 7 + 5x$ | $\longrightarrow$ | (7 5) |
| $x^6 = 2 + 4x$ | $\longrightarrow$ | (2 4) | $x^{19} = 8 + 2x$ | $\longrightarrow$ | (8 2) |
| $x^7 = 1 + 7x$ | $\longrightarrow$ | (1 7) | $x^{20} = 5 + 6x$ | $\longrightarrow$ | (5 6) |
| $x^8 = 4 + 3x$ | $\longrightarrow$ | (4 3) | $x^{21} = 6 + 8x$ | $\longrightarrow$ | (6 8) |
| $x^9 = 3 + x$ | $\longrightarrow$ | (3 1) | $x^{22} = 2 + 7x$ | $\longrightarrow$ | (2 7) |
| $x^{10} = 7 + 2x$ | $\longrightarrow$ | (7 2) | $x^{23} = 4 + 4x$ | $\longrightarrow$ | (4 4) |
| $x^{11} = 5 + 5x$ | $\longrightarrow$ | (5 5) | $x^{24} = x^0$ | $\longrightarrow$ | (1 0) |
| $x^{12} = 8$ | $\longrightarrow$ | (8 0) | | | |

Tabela 4.6: Grupo das Unidades de $GR(9, 2)$

Como o número de elementos desse grupo das unidades é par, a fatoração do termo $x^{24} - 1$ não é única. Neste caso, devemos buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta = \alpha^8$, obtém-se um grupo multiplicativo com 3 elementos, como desejado. Consequentemente, a fatoração do termo $x^3 - 1$ é única.

Analogamente, para o grau 3, teremos:

Considere o anel $GR(p^m, r) = GR(9, 3)$ dado pela extensão de Galois de grau 3:

$$GR(9,3)[x] \cong \frac{\mathbb{Z}_9[x]}{\langle x^3 + 2x + 1\rangle} = \{a + bx + cx^2; a, b, c \in \mathbb{Z}_9\}. \tag{4.40}$$

Considerando, agora, o corpo $GF(p^r) = GF(27)$ :

$$GF(27)[x] \cong \mathbb{F}_{27}[x] \cong \frac{\mathbb{F}_3[x]}{\langle x^3 + 2x + 1\rangle} = \{a' + b'x + c'x^2; a', b', c' \in F_3\}. \tag{4.41}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_{27}$. Logo, $\alpha$ é uma raiz de $x^3 + 2x + 1 = 0$, ou seja, $\alpha^3 = -2\alpha - 1$. Em $\mathbb{Z}_3$ teremos $\alpha^3 = \alpha + 2$. Assim, $\mathbb{F}_{27}$ apresenta os seguintes elementos do

grupo multiplicativo, como na Tabela 4.7.

| | | | | | |
|---|---|---|---|---|---|
| $1=\alpha^0$ | $\longrightarrow$ | $(1\ 0\ 0)$ | $\alpha^{14}=2\alpha$ | $\longrightarrow$ | $(0\ 2\ 0)$ |
| $\alpha=\alpha^1$ | $\longrightarrow$ | $(0\ 1\ 0)$ | $\alpha^{15}=2\alpha^2$ | $\longrightarrow$ | $(0\ 0\ 2)$ |
| $\alpha^2=\alpha^2$ | $\longrightarrow$ | $(0\ 0\ 1)$ | $\alpha^{16}=1+2\alpha$ | $\longrightarrow$ | $(1\ 2\ 0)$ |
| $\alpha^3=2+\alpha$ | $\longrightarrow$ | $(2\ 1\ 0)$ | $\alpha^{17}=\alpha+2\alpha^2$ | $\longrightarrow$ | $(0\ 1\ 2)$ |
| $\alpha^4=2\alpha+\alpha^2$ | $\longrightarrow$ | $(2\ 0\ 1)$ | $\alpha^{18}=1+2\alpha+\alpha^2$ | $\longrightarrow$ | $(1\ 2\ 1)$ |
| $\alpha^5=2+\alpha+2\alpha^2$ | $\longrightarrow$ | $(2\ 1\ 2)$ | $\alpha^{19}=2+2\alpha+2\alpha^2$ | $\longrightarrow$ | $(2\ 2\ 2)$ |
| $\alpha^6=1+\alpha+\alpha^2$ | $\longrightarrow$ | $(1\ 1\ 1)$ | $\alpha^{20}=1+\alpha+2\alpha^2$ | $\longrightarrow$ | $(1\ 1\ 2)$ |
| $\alpha^7=2+2\alpha+\alpha^2$ | $\longrightarrow$ | $(2\ 2\ 1)$ | $\alpha^{21}=1+\alpha^2$ | $\longrightarrow$ | $(1\ 0\ 1)$ |
| $\alpha^8=2+2\alpha^2$ | $\longrightarrow$ | $(2\ 0\ 2)$ | $\alpha^{22}=2+2\alpha$ | $\longrightarrow$ | $(2\ 2\ 0)$ |
| $\alpha^9=1+\alpha$ | $\longrightarrow$ | $(1\ 1\ 0)$ | $\alpha^{23}=2\alpha+2\alpha^2$ | $\longrightarrow$ | $(0\ 2\ 2)$ |
| $\alpha^{10}=\alpha+\alpha^2$ | $\longrightarrow$ | $(0\ 1\ 1)$ | $\alpha^{24}=1+2\alpha+2\alpha^2$ | $\longrightarrow$ | $(1\ 2\ 2)$ |
| $\alpha^{11}=2+\alpha+\alpha^2$ | $\longrightarrow$ | $(2\ 1\ 1)$ | $\alpha^{25}=1+2\alpha^2$ | $\longrightarrow$ | $(1\ 0\ 2)$ |
| $\alpha^{12}=2+\alpha^2$ | $\longrightarrow$ | $(2\ 0\ 1)$ | $\alpha^{26}=\alpha^0$ | $\longrightarrow$ | $(1\ 0\ 0)$ |
| $\alpha^{13}=2$ | $\longrightarrow$ | $(2\ 0\ 0)$ | | | |

Tabela 4.7: Grupo Multiplicativo de $GF(27)$

Seja $f = (0\ 1\ 0) \in GR^*(9,3)$, onde $GR^*(9,3)$ denota o grupo das unidades de $GR(9,3)$. Portanto, $\overline{f} = R_3(f) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 26$ em $\mathbb{F}_9$, lembrando que $R_3(f)$ é a redução módulo 3 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 26d$ em $GR^*(9,3)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_{26}$ de $GR^*(9,3)$.

As operações em $GR^*(9,3)$ são realizadas módulo $(x^3 + 2x + 1)$. Logo, $x^3 = -2x - 1$. Como os coeficientes de $GR^*(9,3)$ estão em $\mathbb{Z}_9$, temos que $x^3 = 8x + 7$. Assim, considerando $(f) = (0\ 1) = x$, a representação dos elementos do grupo das unidades de $GR(9,3)$ é como mostrado na Tabela 4.8.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0\ \ 0)$ | $x = x^1$ | $\longrightarrow$ | $(0\ \ 1\ \ 0)$ |
| $x^2 = x^2$ | $\longrightarrow$ | $(0\ \ 0\ \ 1)$ | $x^3 = 8 + 7x$ | $\longrightarrow$ | $(8\ \ 7\ \ 0)$ |
| $x^4 = 8x + 7x^2$ | $\longrightarrow$ | $(0\ \ 8\ \ 7)$ | $x^5 = 2 + 4x + 8x^2$ | $\longrightarrow$ | $(2\ \ 4\ \ 8)$ |
| $x^6 = 1 + 4x + 4x^2$ | $\longrightarrow$ | $(1\ \ 4\ \ 4)$ | $x^7 = 5 + 2x + 4x^2$ | $\longrightarrow$ | $(5\ \ 2\ \ 4)$ |
| $x^8 = 5 + 6x + 2x^2$ | $\longrightarrow$ | $(5\ \ 6\ \ 2)$ | $x^9 = 7 + 1x + 6x^2$ | $\longrightarrow$ | $(7\ \ 1\ \ 6)$ |
| $x^{10} = 3 + 4x + x^2$ | $\longrightarrow$ | $(3\ \ 4\ \ 1)$ | $x^{11} = 8 + x + 4x^2$ | $\longrightarrow$ | $(8\ \ 1\ \ 4)$ |
| $x^{12} = 5 + x^2$ | $\longrightarrow$ | $(5\ \ 0\ \ 1)$ | $x^{13} = 8 + 3x$ | $\longrightarrow$ | $(8\ \ 3\ \ 0)$ |
| $x^{14} = 8x + 3x^2$ | $\longrightarrow$ | $(0\ \ 8\ \ 3)$ | $x^{15} = 6 + 3x + 8x^2$ | $\longrightarrow$ | $(6\ \ 3\ \ 8)$ |
| $x^{16} = 1 + 8x + 3x^2$ | $\longrightarrow$ | $(1\ \ 8\ \ 3)$ | $x^{17} = 6 + 4x + 8x^2$ | $\longrightarrow$ | $(6\ \ 4\ \ 8)$ |
| $x^{18} = 1 + 8x + 4x^2$ | $\longrightarrow$ | $(1\ \ 8\ \ 4)$ | $x^{19} = 5 + 2x + 8x^2$ | $\longrightarrow$ | $(5\ \ 2\ \ 8)$ |
| $x^{20} = 1 + 7x + 2x^2$ | $\longrightarrow$ | $(1\ \ 7\ \ 2)$ | $x^{21} = 7 + 6x + 7x^2$ | $\longrightarrow$ | $(7\ \ 6\ \ 7)$ |
| $x^{22} = 2 + 2x + 6x^2$ | $\longrightarrow$ | $(2\ \ 2\ \ 6)$ | $x^{23} = 3 + 8x + 2x^2$ | $\longrightarrow$ | $(3\ \ 8\ \ 2)$ |
| $x^{24} = 7 + 8x + 8x^2$ | $\longrightarrow$ | $(7\ \ 8\ \ 8)$ | $x^{25} = 1 + 8x^2$ | $\longrightarrow$ | $(1\ \ 0\ \ 8)$ |
| $x^{26} = 1 + 3x$ | $\longrightarrow$ | $(1\ \ 3\ \ 0)$ | $x^{27} = x + 3x^2$ | $\longrightarrow$ | $(0\ \ 1\ \ 3)$ |
| $x^{28} = 6 + 3x + x^2$ | $\longrightarrow$ | $(6\ \ 3\ \ 1)$ | $x^{29} = 8 + 4x + 3x^2$ | $\longrightarrow$ | $(8\ \ 4\ \ 3)$ |
| $x^{30} = 6 + 2x + 4x^2$ | $\longrightarrow$ | $(6\ \ 2\ \ 4)$ | $x^{31} = 5 + 7x + 2x^2$ | $\longrightarrow$ | $(5\ \ 7\ \ 2)$ |
| $x^{32} = 7 + x + 7x^2$ | $\longrightarrow$ | $(7\ \ 1\ \ 7)$ | $x^{33} = 2 + 2x + x^2$ | $\longrightarrow$ | $(2\ \ 2\ \ 1)$ |
| $x^{34} = 8 + 2x^2$ | $\longrightarrow$ | $(8\ \ 0\ \ 2)$ | $x^{35} = 7 + 4x$ | $\longrightarrow$ | $(7\ \ 4\ \ 0)$ |
| $x^{36} = 7x + 4x^2$ | $\longrightarrow$ | $(0\ \ 7\ \ 4)$ | $x^{37} = 5 + x + 7x^2$ | $\longrightarrow$ | $(5\ \ 1\ \ 7)$ |
| $x^{38} = 2 + x^2$ | $\longrightarrow$ | $(2\ \ 0\ \ 1)$ | $x^{39} = 8$ | $\longrightarrow$ | $(8\ \ 0\ \ 0)$ |
| $x^{40} = 8x$ | $\longrightarrow$ | $(0\ \ 8\ \ 0)$ | $x^{41} = 8x^2$ | $\longrightarrow$ | $(0\ \ 0\ \ 8)$ |
| $x^{42} = 1 + 2x$ | $\longrightarrow$ | $(1\ \ 2\ \ 0)$ | $x^{43} = x + 2x^2$ | $\longrightarrow$ | $(0\ \ 1\ \ 2)$ |
| $x^{44} = 7 + 5x + x^2$ | $\longrightarrow$ | $(7\ \ 5\ \ 1)$ | $x^{45} = 8 + 5x + 5x^2$ | $\longrightarrow$ | $(8\ \ 5\ \ 5)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{46} = 4 + 7x + 5x^2$ | $\longrightarrow$ | $(4\ \ 7\ \ 5)$ | $x^{47} = 4 + 3x + 7x^2$ | $\longrightarrow$ | $(4\ \ 3\ \ 7)$ |
| $x^{48} = 2 + 8x + 3x^2$ | $\longrightarrow$ | $(2\ \ 8\ \ 3)$ | $x^{49} = 6 + 5x + 8x^2$ | $\longrightarrow$ | $(6\ \ 5\ \ 8)$ |
| $x^{50} = 1 + 8x + 5x^2$ | $\longrightarrow$ | $(1\ \ 8\ \ 5)$ | $x^{51} = 4 + 8x^2$ | $\longrightarrow$ | $(4\ \ 0\ \ 8)$ |
| $x^{52} = 1 + 6x$ | $\longrightarrow$ | $(1\ \ 6\ \ 0)$ | $x^{53} = x + 6x^2$ | $\longrightarrow$ | $(0\ \ 1\ \ 6)$ |
| $x^{54} = 3 + 6x + x^2$ | $\longrightarrow$ | $(3\ \ 6\ \ 1)$ | $x^{55} = 8 + x + 6x^2$ | $\longrightarrow$ | $(8\ \ 1\ \ 6)$ |
| $x^{56} = 3 + 5x + x^2$ | $\longrightarrow$ | $(3\ \ 5\ \ 1)$ | $x^{57} = 8 + x + 5x^2$ | $\longrightarrow$ | $(8\ \ 1\ \ 5)$ |
| $x^{58} = 4 + 7x + x^2$ | $\longrightarrow$ | $(4\ \ 7\ \ 1)$ | $x^{59} = 8 + 2x + 7x^2$ | $\longrightarrow$ | $(8\ \ 2\ \ 7)$ |
| $x^{60} = 2 + 3x + 2x^2$ | $\longrightarrow$ | $(2\ \ 3\ \ 2)$ | $x^{61} = 7 + 7x + 3x^2$ | $\longrightarrow$ | $(7\ \ 7\ \ 3)$ |
| $x^{62} = 6 + x + 7x^2$ | $\longrightarrow$ | $(6\ \ 1\ \ 7)$ | $x^{63} = 2 + x + x^2$ | $\longrightarrow$ | $(2\ \ 1\ \ 1)$ |
| $x^{64} = 8 + x^2$ | $\longrightarrow$ | $(8\ \ 0\ \ 1)$ | $x^{65} = 8 + 6x$ | $\longrightarrow$ | $(8\ \ 6\ \ 0)$ |
| $x^{66} = 8x + 6x^2$ | $\longrightarrow$ | $(0\ \ 8\ \ 6)$ | $x^{67} = 3 + 6x + 8x^2$ | $\longrightarrow$ | $(3\ \ 6\ \ 8)$ |
| $x^{68} = 1 + 5x + 6x^2$ | $\longrightarrow$ | $(1\ \ 5\ \ 6)$ | $x^{69} = 3 + 7x + 5x^2$ | $\longrightarrow$ | $(3\ \ 7\ \ 5)$ |
| $x^{70} = 4 + 2x + 7x^2$ | $\longrightarrow$ | $(4\ \ 2\ \ 7)$ | $x^{71} = 2 + 8x + 2x^2$ | $\longrightarrow$ | $(2\ \ 8\ \ 2)$ |
| $x^{72} = 7 + 7x + 8x^2$ | $\longrightarrow$ | $(7\ \ 7\ \ 8)$ | $x^{73} = 1 + 7x^2$ | $\longrightarrow$ | $(1\ \ 0\ \ 7)$ |
| $x^{74} = 2 + 5x$ | $\longrightarrow$ | $(2\ \ 5\ \ 0)$ | $x^{75} = 2x + 5x^2$ | $\longrightarrow$ | $(0\ \ 2\ \ 5)$ |
| $x^{76} = 4 + 8x + 2x^2$ | $\longrightarrow$ | $(4\ \ 8\ \ 2)$ | $x^{77} = 7 + 8x^2$ | $\longrightarrow$ | $(7\ \ 0\ \ 8)$ |
| $x^{78} = x^0$ | $\longrightarrow$ | $(1\ \ 0\ \ 0)$ | | | |

Tabela 4.8: Grupo das Unidades de $GR(9, 3)$

Sendo o número de elementos do grupo das unidades par, a fatoração do termo $x^{78} - 1$ não é única. Neste caso, existirá outro grupo multiplicativo, cuja ordem será ímpar. Definindo $\beta = \alpha^2$, obtém-se um grupo multiplicativo com 39 elementos, como desejado. Consequentemente, a fatoração do termo $x^{39} - 1$ é única.

## 4.5 Códigos Alternantes sobre Anéis Locais

Nesta seção apresentamos um processo de construção de códigos alternantes sobre anéis comutativos finitos com identidade, classe esta de códigos que pode ser obtida através dos códigos BCH. Nesta direção, precisamos rever algumas propriedades importantes de extensão de Galois sobre anéis, as quais caracterizam os códigos alternantes.

Assumimos que $A$ é um anel comutativo finito com identidade, com ideal maximal $M$ e corpo residual $K = \frac{A}{M} \cong GF(p^m)$, onde $m$ é um inteiro positivo e $p$ primo. Seja $A[x]$ o anel de polinômio na variável $x$ sobre $A$. Denotamos a projeção natural $A[x] \longrightarrow K[x]$ por $\mu$. Seja $f(x)$ um polinômio mônico de grau $h$ sobre o anel $A$, tal que $\mu(f(x))$ seja irredutível em $K[x]$. Então pelo Teorema 4.3.2 temos que $f(x)$ também é irredutível em $A[x]$. Seja $A[x]/\langle f(x)\rangle$ o conjunto das classes residuais de polinômios em $x$ sobre $A$ módulo $f(x)$. Este anel, denotado por $R$, é um anel comutativo finito local com identidade chamado **extensão de Galois** de $A$ de grau $h$. Seu corpo de resíduo é dado por $K_1 = \frac{R}{\overline{M_1}} = \frac{A[x]/\langle f(x)\rangle}{\langle M, f(x)\rangle / \langle f(x)\rangle} = \frac{A[x]}{\langle M, f(x)\rangle} = \frac{(A/M)[x]}{\langle \mu(f(x))\rangle}$, o qual tem ordem $p^{mh}$, onde $\overline{M_1} = \frac{M_1}{\langle f(x)\rangle}$, é o ideal maximal de $R$, sendo que $M_1 = \langle M, f(x)\rangle$. O corpo residual $K_1$ será denotado por $GF(p^{mh})$ e $K_1^*$ o correspondente grupo multiplicativo, cuja ordem é $p^{mh} - 1$. Seja $R^*$ o grupo multiplicativo das unidades de $R$. Segue que $R^*$ é um grupo abeliano e, portanto, pode ser expresso como produto direto de grupos cíclicos. Estamos interessados no grupo cíclico maximal de $R^*$, denotado por $G_s$, cujos elementos são as raízes de $x^s - 1$ para algum número inteiro positivo $s$ tal que o $mdc(s, p) = 1$. Existe somente um subgrupo cíclico maximal de $R^*$ tendo ordem prima para $p$, este grupo ciclico tem ordem $s = p^{mh} - 1$.

**Definição 62** (Código Alternante)**.** *Seja $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ o vetor localizador, consistindo de elementos distintos de $G_s$, e seja $\boldsymbol{w} = (w_1, w_2, \ldots, w_n)$ um vetor que consiste de quaisquer elementos de $G_s$. Seja $H$ a matriz verificação de paridade definida como:*

$$H = \begin{bmatrix} w_1 & w_2 & \cdots & w_n \\ w_1\alpha_1 & w_2\alpha_2 & \cdots & w_n\alpha_n \\ w_1\alpha_1^2 & w_2\alpha_2^2 & \cdots & w_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_1\alpha_1^{r-1} & w_2\alpha_2^{r-1} & \cdots & w_n\alpha_n^{r-1} \end{bmatrix}, \tag{4.42}$$

*para algum $r \geq 1$, onde $r$ é um inteiro positivo. Esta matriz define um código alternante de comprimento $n \leq s$ sobre $A$, e será denotado por $C(n, \eta, \boldsymbol{w})$.*

**Observação 2.** *Os códigos alternantes foram definidos e estudados por Helgert. O nome código alternante está baseado no fato de que a matriz ou determinante da forma*

$$H = \begin{bmatrix} f_0(x_0) & f_1(x_0) & \cdots & f_{n-1}(x_0) \\ f_0(x_1) & f_1(x_1) & \cdots & f_{n-1}(x_1) \\ \vdots & \vdots & \ddots & \vdots \\ f_0(x_{r-1}) & f_1(x_{r-1}) & \cdots & f_{n-1}(x_{r-1}) \end{bmatrix}, \tag{4.43}$$

é chamado alternante.

A matriz $H$ mencionada na Definição 62 pode ser decomposta como produto de duas matrizes, isto é,

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \begin{bmatrix} w_1 & 0 & 0 & \cdots & 0 \\ 0 & w_2 & 0 & \cdots & 0 \\ 0 & 0 & w_3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & w_n \end{bmatrix} = XY. \tag{4.44}$$

Observe que se considerarmos o vetor $\mathbf{w} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, com $\alpha_i \in G_s$, $1 \leq i \leq n$, tomando $\alpha_i = \beta^{i-1}$, $1 \leq i \leq n$, temos:

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \beta^{r-1} & (\beta^{r-1})^2 & \cdots & (\beta^{r-1})^{n-1} \end{bmatrix}. \tag{4.45}$$

Uma palavra $\mathbf{c} = (c_1, c_2, \ldots c_n) \in A^n$ está em $C(n, \eta, \mathbf{w})$ se, e somente se, satisfaz as $2t$ equações de verificação de paridade sobre $R$, ou seja, $\mathbf{c}H^T = 0$. Isto é,

$$\sum_{i=1}^{n} c_i \alpha_i^l = 0, \quad l = 1, 2, \ldots, 2t, \tag{4.46}$$

para $l \geq 1$, cada uma dessas equações de verificação de paridade pode ser reescrita em $h$ equações sobre $A$. O peso de Hamming de uma palavra $\mathbf{c}$ em $A^n$ será donotado por $w_H(\mathbf{c})$. O código $C(n, \eta, \mathbf{w})$ para o qual $n = p^{mh} - 1$ será chamado **primitivo**. Neste caso, $\eta$ é único, a menos de permutação de suas coordenadas.

Uma matriz verificação de paridade $H_1$ com elementos sobre $A$ pode ser obtida substituindo cada elemento em $H$ pelo correspondente vetor coluna de comprimento $h$ sobre $A$. É possível obter uma estimativa da distância de Hamming mínima, d, diretamente da matriz verificação de paridade. Tomando o teorema abaixo como suporte para isto, temos

**Teorema 38.** *[11] $C(n, \eta, \boldsymbol{w})$ tem distância de Hamming mínima $d \geq r + 1$.*

Portanto, é facil notar que $r$ no Teorema 36 é equivalente a $2t$ utilizado no Teorema 32. fazendo esta substituição na matriz em (4.45), obtemos a matriz verificação de paridade de um código BCH como definida em (4.21). Ou seja, através de uma escolha apropriada do vetor localizador e do vetor $w$, a Definição 62 nos fornece a matriz verificação de paridade de um código BCH ou de um código alternante.

### 4.5.1 Exemplo de construção de códigos alternantes sobre anéis locais

**Códigos alternantes sobre $\mathbb{Z}_8$**

Seja $\mathbf{C}$ um código alternante de comprimento 3. Para distância de projeto igual a 3, temos que $r = 2$. Sendo assim, considere $\beta$ um elemento primitivo em $G_3$. Logo, $\eta = (1\ \beta\ \beta^2)$, onde $1 = \beta^3$. Da Tabela 5.1, $\beta = x = f = (0\ 1)$. Fazendo $\mathbf{w} = (1\ 1\ 1)$, temos a seguinte matriz verificação de paridade:

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \beta & \beta^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 7 & 7 \end{bmatrix}. \tag{4.47}$$

Da mesma maneira, podemos construir um código alternante de comprimento 7 e distância 3 considerando os vetores $\eta = (1\ \beta\ \beta^2\ \beta^3\ \beta^4\ \beta^5\ \beta^6)$ e $\mathbf{w} = (1\ 1\ 1\ 1\ 1\ 1\ 1)$, onde $1 = \beta^7$. Pela Tabela 5.2, $\beta = x^4 = f^4 = (0\ 7\ 7)$. Logo, temos a seguinte matriz verificação de paridade:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \end{bmatrix}. \tag{4.48}$$

Fazendo as substituições dos respectivos valores dos elementos de $G_7$, temos:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 7 & 7 & 6 & 5 & 0 & 5 & 7 & 5 & 4 & 4 & 1 & 5 & 2 & 1 & 3 & 7 & 2 \end{bmatrix}. \tag{4.49}$$

Para a distância de projeto 4 ($r = 3$) e comprimento 7, temos a matriz verificação de paridade dada por:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \end{bmatrix}. \tag{4.50}$$

Portanto,

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 7 & 7 & 6 & 5 & 0 & 5 & 7 & 5 & 4 & 4 & 1 & 5 & 2 & 1 & 3 & 7 & 2 \\ 1 & 0 & 0 & 6 & 5 & 0 & 4 & 4 & 1 & 3 & 7 & 2 & 0 & 7 & 7 & 5 & 7 & 5 & 5 & 2 & 1 \end{bmatrix}. \tag{4.51}$$

Finalmente, o código alternante de comprimento 7 e distância 5 ($r = 4$) apresenta a seguinte matriz verificação de paridade

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta & \beta^4 \end{bmatrix}. \tag{4.52}$$

Logo,

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 7 & 7 & 6 & 5 & 0 & 5 & 7 & 5 & 4 & 4 & 1 & 5 & 2 & 1 & 3 & 7 & 2 \\ 1 & 0 & 0 & 6 & 5 & 0 & 4 & 4 & 1 & 3 & 7 & 2 & 0 & 7 & 7 & 5 & 7 & 5 & 5 & 2 & 1 \\ 1 & 0 & 0 & 5 & 7 & 5 & 3 & 7 & 2 & 6 & 5 & 0 & 5 & 2 & 1 & 0 & 7 & 7 & 4 & 4 & 1 \end{bmatrix}. \quad (4.53)$$

## 4.6 Códigos Reed-Solomon sobre Anéis Locais

Neste seção vamos apresentar a construção de códigos Reed-Solomon sobre anéis locais da forma $\mathbb{Z}_q$ onde $q = p^r$, com $p$ um primo ímpar. Esta construção é muito semelhante à dos códigos Reed-Solomon sobre $GF(q)$.

Seja $\alpha \in \mathbb{Z}_q$ um elemento primitivo dos inteiros módulo $p$ tal que $\alpha^{p-1} \cong 1(mod\ p)$ e $\alpha^i \ncong 1(mod\ p)$ se $1 \leqslant i \leqslant p-2$. Sejam $s = p-1$, $G_s = \{1, \alpha, \alpha^2, \ldots, \alpha^{s-1}\}$, o vetor localizador $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ consistindo de elementos distintos de $G_s$ e $m$ um inteiro não negativo. Com isso, a matriz $H$ pode ser definida como:

$$H = \begin{bmatrix} \alpha_1^m & \alpha_2^m & \cdots & \alpha_n^m \\ \alpha_1^{m+1} & \alpha_2^{m+1} & \cdots & \alpha_n^{m+1} \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{m+d-2} & \alpha_2^{m+d-2} & \cdots & \alpha_n^{m+d-2} \end{bmatrix}. \quad (4.54)$$

**Teorema 39.** *[3] O espaço nulo da matriz $H$ sobre $\mathbb{Z}_q$ é um código de comprimento $(p-1)$, distância mínima igual a $d$ e dimensão $(p-d)$.*

### 4.6.1 Exemplo de construção de códigos Reed-Solomon sobre anéis locais

Vamos construir um código Reed-Solomon sobre $\mathbb{Z}_{49}$ com $d_{min} = 5$. Temos: $p = 7,\ r = 2,\ q = p^r = 49, k = p-2 = 5,\ \alpha = 3$ (elemento primitivo de $\mathbb{Z}_q$), $D = p - d = 2$ (dimensão

do código) e supor que $m = 1$. Portanto,

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} \end{bmatrix} = \begin{bmatrix} 1 & 3 & 9 & 27 & 32 & 47 \\ 1 & 9 & 32 & 43 & 44 & 4 \\ 1 & 27 & 43 & 34 & 36 & 41 \\ 1 & 32 & 44 & 36 & 25 & 16 \end{bmatrix}. \tag{4.55}$$

Da teoria apresentada anteriormente, concluímos que $H$ descreve um $(6, 2, 5)-$código linear sobre $\mathbb{Z}_q$ com capacidade de correção de $(d_{min} - 1)/2 = 2$ erros aleatórios.

**Observação 3.** *Esta classe de códigos Reed-Solomon sobre anéis* ***não*** *é formada por códigos cíclicos. Por inspeção direta podemos comprovar que* $\underline{v} = (4\ 44\ 31\ 27\ 1\ 0)$ *é uma palavra-código do exemplo considerado, pois* $\underline{v}.H^T = \underline{0}$*, onde* $H$ *é a matriz verificação de paridade. Entretanto, a palavra* $\underline{v^{(2)}} = (1\ 0\ 4\ 44\ 31\ 27)$ *não pertence a este código, já que* $\underline{v^{(2)}}.H^T \neq \underline{0}$*. Portanto, em geral, os códigos Reed-Solomon sobre anéis* ***não*** *são cíclicos. Entretanto, podemos afirmar que todo polinômio* $v(x)$ *de um código Reed-Solomon é múltiplo de um determinado polinômio mônico* $g(x)$*, também pertencente ao código. Isto é justificado da seguinte maneira: pelo fato de que* $\underline{v}.H^T = \underline{0}$ *(onde* $H$ *é a matriz verificação de paridade), então* $\alpha^m\ \alpha^{m+1}\ \alpha^{m+2}, \ldots, \alpha^{m+d-2}$ *são raízes de* $v(x)$*. Além disso, os coeficientes de* $v(x)$ *pertencem ao anel* $\mathbb{Z}_q$ *(que possui identidade multiplicativa), o que nos leva a concluir que:*

$$f_1(x) = x - \alpha^m,\ f_2(x) = x - \alpha^{m+1},\ f_3(x) = x - \alpha^{m+2}, \ldots, f_{d-1}(x) = x - \alpha^{m+d-2} \tag{4.56}$$

*e*

$$g(x) = mmc\{f_1(x), f_2(x), f_3(x), \ldots, f_{d-1}(x)\}, \tag{4.57}$$

*são fatores de* $v(x)$*. Isto implica que todo polinômio código* $v(x)$ *é múltiplo de* $g(x)$*. Por outro lado, nem todo múltiplo de* $g(x)$ *é um polinômio código.*

# CAPÍTULO 5

# APLICAÇÕES DAS EXTENSÕES GALOISIANAS SOBRE ANÉIS LOCAIS

Neste capítulo, apresentamos duas aplicações das extensões de Galois sobre anéis locais. Estes conceitos podem ser encontrados nas referências [3],[4] e [15].

Este capítulo está organizado da seguinte maneira. Na Seção 5.1, apresentamos a cardinalidade de alguns dos grupos das unidades de anéis locais $\mathbb{Z}_q$, $q = p^m$, através dos conceitos desenvolvidos no Capítulo 4. As Tabelas 5.9 e 5.10 relacionam as cardinalidades do grupo das unidades correspondentes às extensões de graus 2 e 3. Na Seção 5.2, apresentamos os geradores de seqüências sobre corpos finitos bem como para o caso em que a seqüência pertence a um anel comutativo finito local com identidade. Através do polinômio gerador obtido no grupo das unidades, concluímos que a sua cardinalidade está associada ao comprimento da seqüência. Mostramos que os registros de deslocamento com realimentação linear geram os códigos cíclicos. Na Seção 5.3, mostramos que através do polinômio gerador dos códigos cíclicos sobre anéis locais realizamos a transformada discreta de Fourier. Estas aplicações levariam a uma provável aplicação em Criptografia.

## 5.1 Determinação do Grupo das Unidades de certos Anéis Locais

Nesta seção, determinamos o grupo das unidades de alguns anéis locais com graus 2 e 3.

**Exemplo 4.** *Determinação do grupo das unidades de GR(8,2) e GR(8,3)*

Sejam o anel $R$ e o corpo $GF(4)$ gerados pelas seguintes extensões de grau 2:

$$R \cong GR(8,2)[x] \cong \frac{\mathbb{Z}_8[x]}{\langle x^2+x+1\rangle} = \{a+bx; a,b \in \mathbb{Z}_8\}. \tag{5.1}$$

$$\begin{aligned} GF(4)[x] \cong \mathbb{F}_4[x] \cong \frac{\mathbb{F}_2[x]}{\langle x^2+x+1\rangle} &= \{a'+b'x; a',b' \in \mathbb{F}_2\} \\ &= \{0,1,x,1+x\}. \end{aligned} \tag{5.2}$$

Observe que o corpo $GF(4)$ é igual ao estabelecido em (4.27) pois o polinômio utilizado em ambas extensões é o mesmo. Logo, para $\alpha$ primitivo em $GF(4)$, os elementos deste corpo são mostrados na Tabela 4.1.

Seja $f = (0\ 1) \in GR^*(8,2)$. Então, $\overline{f} = R_2(f) = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = 3$. Assim, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 3d$ em $GR^*(8,2)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_3$ de $GR^*(8,2)$.
Em $GR^*(8,2)$, temos $x^2 = 7x + 7$. Logo, considerando $(f) = (0\ 1) = x$, a representação do grupo das unidades dos elementos de $GR(8,2)$ é como mostrada na Tabela 5.1.

| | | |
|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0)$ |
| $x = x^1$ | $\longrightarrow$ | $(0\ \ 1)$ |
| $x^2 = 7 + 7x$ | $\longrightarrow$ | $(7\ \ 7)$ |
| $x^3 = x^0$ | $\longrightarrow$ | $(1\ \ 0)$ |

Tabela 5.1: Grupo das Unidades de $GR(8,2)$

Portanto, $nd = 3$, assim, $d = 1$. Logo, $f = x = (0\ 1)$ gera um grupo de ordem 3 em $GR^*(8,2)$. Logo, $\beta = x$ é um elemento primitivo em $G_3$.

Para a extensão de Galois de grau 3 sobre o anel $\mathbb{Z}_8$, temos:

$$R \cong GR(8,3)[x] \cong \frac{\mathbb{Z}_8[x]}{\langle x^3 + x + 1\rangle} = \{a + bx + cx^2; a, b, c \in \mathbb{Z}_8\}. \tag{5.3}$$

$$\begin{aligned} GF(8)[x] \cong \mathbb{F}_8[x] \cong \frac{\mathbb{F}_2[x]}{\langle x^3 + x + 1\rangle} &= \{a' + b'x + c'x^2; a', b', c' \in \mathbb{F}_2\} \\ &= \{0, 1, x, x^2, 1 + x, 1 + x^2, x^2 + x, 1 + x + x^2\}. \end{aligned} \tag{5.4}$$

O corpo $GF(8)$ apresenta os elementos contidos na Tabela 4.3.

Seja $f = (0\ 1\ 0) \in GR^*(8,3)$. Então, $\overline{f} = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = 7$ em $GF(8)$. Pelo Teorema 35, $f$ deve gerar um grupo de ordem $nd = 7d$ em $GR^*(8,3)$.

Em $GR^*(8,3)$, temos $x^3 = 7x+7$ (coeficientes em $\mathbb{Z}_8$). Logo, considerando $(f) = (0\ 1\ 0) = x$, a representação dos elementos do grupo das unidades de $GR(8,3)$ é como mostrada na Tabela 5.2.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0\ \ 0)$ | $x^{15} = x + 4x^2$ | $\longrightarrow$ | $(0\ \ 1\ \ 4)$ |
| $x = x^1$ | $\longrightarrow$ | $(0\ \ 1\ \ 0)$ | $x^{16} = 4 + 4x + x^2$ | $\longrightarrow$ | $(4\ \ 4\ \ 1)$ |
| $x^2 = x^2$ | $\longrightarrow$ | $(0\ \ 0\ \ 1)$ | $x^{17} = 7 + 3x + 4x^2$ | $\longrightarrow$ | $(7\ \ 3\ \ 4)$ |
| $x^3 = 7 + 7x$ | $\longrightarrow$ | $(7\ \ 7\ \ 0)$ | $x^{18} = 4 + 3x + 3x^2$ | $\longrightarrow$ | $(4\ \ 3\ \ 3)$ |
| $x^4 = 7x + 7x^2$ | $\longrightarrow$ | $(0\ \ 7\ \ 7)$ | $x^{19} = 5 + x + 3x^2$ | $\longrightarrow$ | $(5\ \ 1\ \ 3)$ |
| $x^5 = 1 + x + 7x^2$ | $\longrightarrow$ | $(1\ \ 1\ \ 7)$ | $x^{20} = 5 + 2x + x^2$ | $\longrightarrow$ | $(5\ \ 2\ \ 1)$ |
| $x^6 = 1 + 2x + x^2$ | $\longrightarrow$ | $(1\ \ 2\ \ 1)$ | $x^{21} = 7 + 4x + 2x^2$ | $\longrightarrow$ | $(7\ \ 4\ \ 2)$ |
| $x^7 = 7 + 2x^2$ | $\longrightarrow$ | $(7\ \ 0\ \ 2)$ | $x^{22} = 6 + 5x + 4x^2$ | $\longrightarrow$ | $(6\ \ 5\ \ 4)$ |
| $x^8 = 6 + 5x$ | $\longrightarrow$ | $(6\ \ 5\ \ 0)$ | $x^{23} = 4 + 2x + 5x^2$ | $\longrightarrow$ | $(4\ \ 2\ \ 5)$ |
| $x^9 = 6x + 5x^2$ | $\longrightarrow$ | $(0\ \ 6\ \ 5)$ | $x^{24} = 3 + 7x + 2x^2$ | $\longrightarrow$ | $(3\ \ 7\ \ 2)$ |
| $x^{10} = 3 + 3x + 6x^2$ | $\longrightarrow$ | $(3\ \ 3\ \ 6)$ | $x^{25} = 6 + x + 7x^2$ | $\longrightarrow$ | $(6\ \ 1\ \ 7)$ |
| $x^{11} = 2 + 5x + 3x^2$ | $\longrightarrow$ | $(2\ \ 5\ \ 3)$ | $x^{26} = 1 + 7x + x^2$ | $\longrightarrow$ | $(1\ \ 7\ \ 1)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{13} = 3 + 7x^2$ | $\longrightarrow$ | (3 0 7) | $x^{28} = x^0$ | $\longrightarrow$ | (1 0 0) |
| $x^{14} = 1 + 4x$ | $\longrightarrow$ | (1 4 0) | | | |

Tabela 5.2: Grupo das Unidades de $GR(8, 3)$

Portanto, $nd = 28$, implicando que $d = 4$. Logo, $f$ gera um grupo de ordem 28 em $GR^*(8, 3)$ e, conseqüentemente, $f^4 = x^4 = (0\ 7\ 7)$ gera também um grupo de ordem 7 em $GR^*(8, 3)$. Logo, $\beta = x^4$ é um elemento primitivo em $G_7$.

**Exemplo 5.** *Determinação do grupo das unidades de GR(16,2) e GR(16,3)*

Inicialmente, considere o anel $GR(p^m, r) = GR(16, 2)$ dado pela extensão de Galois de grau 2 :

$$GR(16, 2)[x] \cong \frac{\mathbb{Z}_{16}[x]}{\langle x^2 + x + 1\rangle} = \{a + bx; a, b \in \mathbb{Z}_{16}\}. \tag{5.5}$$

Considere agora o corpo $GF(p^r) = GF(4)$, onde

$$\begin{aligned} GF(4)[x] \cong \mathbb{F}_4[x] \cong \frac{\mathbb{F}_2[x]}{\langle x^2 + x + 1\rangle} &= \{a' + b'x; a', b' \in \mathbb{F}_2\} \\ &= \{0, 1, x, 1 + x\}. \end{aligned} \tag{5.6}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_4$, logo $\alpha$ é uma raiz de $x^2 + x + 1 = 0$, ou seja, $\alpha^2 = -\alpha - 1$ em $\mathbb{F}_2$, teremos $\alpha^2 = 1 + \alpha$. Assim,o grupo multiplicativo de $\mathbb{F}_4$ são os mesmos elementos da Tabela 4.1.

Seja $f = (0\ 1) \in GR^*(16, 2)$, onde $GR^*(16, 2)$ denota o grupo das unidades de $GR(16, 2)$. Portanto, $\overline{f} = R_2(f) = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 3$ em $\mathbb{F}_4$, lembrando que $R_2(f)$ é a redução módulo 2 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 3d$ em $GR^*(16, 2)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_3$ de $GR^*(16, 2)$.

As operações em $GR^*(16, 2)$ são realizadas módulo $x^2 + x + 1$. Logo, $x^2 = -x - 1$; porém, como os coeficientes de $GR^*(16, 2)$ estão em $\mathbb{Z}_{16}$, temos que $x^2 = 15x + 15$. Assim, considerando $(f) = (0\ 1) = x$, a representação dos elementos de $GR^*(16, 2)$, ou seja, os elementos do grupo das unidades é como mostrado abaixo:

| | | |
|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1 \ \ 0)$ |
| $x = x^1$ | $\longrightarrow$ | $(0 \ \ 1)$ |
| $x^2 = 15 + 15x$ | $\longrightarrow$ | $(15 \ \ 15)$ |
| $x^3 = x^0$ | $\longrightarrow$ | $(1 \ \ 0)$ |

Tabela 5.3: Grupo das Unidades de $GR(16, 2)$

Portanto, $nd = 3$, assim, $d = 1$. Logo, $f = x = (0\ 1)$ gera um grupo de ordem 3 em $GR^*(16, 2)$. Logo, $\beta = x$ é um elemento primitivo em $G_3$.

Considere o anel $GR(p^m, r) = GR(16, 3)$ dado pela extensão de Galois de grau 3:

$$GR(16,3)[x] \cong \frac{\mathbb{Z}_{16}[x]}{\langle x^3 + x + 1\rangle} = \{a + bx + cx^2; a, b, c \in \mathbb{Z}_{16}\}. \tag{5.7}$$

Considerando agora o corpo $GF(p^r) = GF(8)$ :

$$\begin{aligned} GF(8)[x] \cong \mathbb{F}_8[x] \cong \frac{\mathbb{F}_2[x]}{\langle x^3 + x + 1\rangle} &= \{a' + b'x + c'x^2; a', b', c', \in \mathbb{F}_2\} \\ &= \{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}. \end{aligned} \tag{5.8}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_8$, logo $\alpha$ é uma raiz de $x^3 + x + 1 = 0$, ou seja, $\alpha^3 = -\alpha - 1$ em $\mathbb{F}_2$ teremos $\alpha^3 = \alpha + 1$. Assim, $\mathbb{F}_8$ apresenta os mesmos elementos do grupo multiplicativo visto na Tabela 4.3.

Seja $f = (0\ 1\ 0) \in GR^*(16, 3)$, onde $GR^*(16, 3)$ denota o grupo das unidades de $GR(16, 3)$. Portanto, $\overline{f} = R_2(f) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 7$ em $\mathbb{F}_8$, lembrando que $R_2(f)$ é a redução módulo 2 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 7d$ em $GR^*(16, 3)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_7$ de $GR^*(16, 3)$.

As operações em $GR^*(16, 3)$ são realizadas módulo $x^3 + x + 1$. Logo, $x^3 = -x - 1$; porém, como os coeficientes de $GR^*(16, 3)$ estão em $\mathbb{Z}_{16}$, temos que $x^2 = 15x + 15$. Assim, considerando $(f) = (0\ 1\ 0) = x$, a representação dos elementos de $GR^*(16, 3)$, ou seja, os elementos do grupo das unidades é como mostrado abaixo:

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0\ \ 0)$ | $x^{29} = x + 8x^2$ | $\longrightarrow$ | $(0\ \ 1\ \ 8)$ |
| $x = x^1$ | $\longrightarrow$ | $(0\ \ 1\ \ 0)$ | $x^{30} = 8 + 8x + x^2$ | $\longrightarrow$ | $(8\ \ 8\ \ 1)$ |
| $x^2 = x^2$ | $\longrightarrow$ | $(0\ \ 0\ \ 1)$ | $x^{31} = 15 + 7x + 8x^2$ | $\longrightarrow$ | $(15\ \ 7\ \ 8)$ |
| $x^3 = 15 + 15x$ | $\longrightarrow$ | $(15\ \ 15\ \ 0)$ | $x^{32} = 8 + 7x + 7x^2$ | $\longrightarrow$ | $(8\ \ 7\ \ 7)$ |
| $x^4 = 15x + 15x^2$ | $\longrightarrow$ | $(0\ \ 15\ \ 15)$ | $x^{33} = 9 + x + 7x^2$ | $\longrightarrow$ | $(9\ \ 1\ \ 7)$ |
| $x^5 = 1 + x + 15x^2$ | $\longrightarrow$ | $(1\ \ 1\ \ 15)$ | $x^{34} = 9 + 2x + x^2$ | $\longrightarrow$ | $(9\ \ 2\ \ 1)$ |
| $x^6 = 1 + 2x + x^2$ | $\longrightarrow$ | $(1\ \ 2\ \ 1)$ | $x^{35} = 15 + 8x + 2x^2$ | $\longrightarrow$ | $(15\ \ 8\ \ 2)$ |
| $x^7 = 15 + 2x^2$ | $\longrightarrow$ | $(15\ \ 0\ \ 2)$ | $x^{36} = 14 + 13x + 8x^2$ | $\longrightarrow$ | $(14\ \ 13\ \ 8)$ |
| $x^8 = 14 + 13x$ | $\longrightarrow$ | $(14\ \ 13\ \ 0)$ | $x^{37} = 8 + 6x + 13x^2$ | $\longrightarrow$ | $(8\ \ 6\ \ 13)$ |
| $x^9 = 14x + 13x^2$ | $\longrightarrow$ | $(0\ \ 14\ \ 13)$ | $x^{38} = 3 + 11x + 6x^2$ | $\longrightarrow$ | $(3\ \ 11\ \ 6)$ |
| $x^{10} = 3 + 3x + 14x^2$ | $\longrightarrow$ | $(3\ \ 3\ \ 14)$ | $x^{39} = 10 + 13x + 11x^2$ | $\longrightarrow$ | $(10\ \ 13\ \ 11)$ |
| $x^{11} = 2 + 5x + 3x^2$ | $\longrightarrow$ | $(2\ \ 5\ \ 3)$ | $x^{40} = 5 + 15x + 13x^2$ | $\longrightarrow$ | $(5\ \ 15\ \ 13)$ |
| $x^{12} = 13 + 15x + 5x^2$ | $\longrightarrow$ | $(13\ \ 15\ \ 5)$ | $x^{41} = 3 + 8x + 15^2$ | $\longrightarrow$ | $(3\ \ 8\ \ 15)$ |
| $x^{13} = 11 + 8x + 15x^2$ | $\longrightarrow$ | $(11\ \ 8\ \ 15)$ | $x^{42} = 1 + 4x + 8x^2$ | $\longrightarrow$ | $(1\ \ 4\ \ 8)$ |
| $x^{14} = 1 + 12x + 8x^2$ | $\longrightarrow$ | $(1\ \ 12\ \ 8)$ | $x^{43} = 8 + 9x + 4x^2$ | $\longrightarrow$ | $(8\ \ 9\ \ 4)$ |
| $x^{15} = 8 + 9x + 12x^2$ | $\longrightarrow$ | $(8\ \ 9\ \ 12)$ | $x^{44} = 12 + 4x + 9x^2$ | $\longrightarrow$ | $(12\ \ 4\ \ 9)$ |
| $x^{16} = 4 + 12x + 9x^2$ | $\longrightarrow$ | $(4\ \ 12\ \ 9)$ | $x^{45} = 7 + 3x + 4x^2$ | $\longrightarrow$ | $(7\ \ 3\ \ 4)$ |
| $x^{17} = 7 + 11x + 12x^2$ | $\longrightarrow$ | $(7\ \ 11\ \ 12)$ | $x^{46} = 12 + 3x + 3x^2$ | $\longrightarrow$ | $(12\ \ 3\ \ 3)$ |
| $x^{18} = 4 + 11x + 11x^2$ | $\longrightarrow$ | $(4\ \ 11\ \ 11)$ | $x^{47} = 13 + 9x + 3x^2$ | $\longrightarrow$ | $(13\ \ 9\ \ 3)$ |
| $x^{19} = 5 + 9x + 11x^2$ | $\longrightarrow$ | $(5\ \ 9\ \ 11)$ | $x^{48} = 13 + 10x + 9x^2$ | $\longrightarrow$ | $(13\ \ 10\ \ 9)$ |
| $x^{20} = 5 + 10x + 9x^2$ | $\longrightarrow$ | $(5\ \ 10\ \ 9)$ | $x^{49} = 7 + 4x + 10x^2$ | $\longrightarrow$ | $(7\ \ 4\ \ 10)$ |
| $x^{21} = 7 + 12x + 10x^2$ | $\longrightarrow$ | $(7\ \ 12\ \ 10)$ | $x^{50} = 6 + 13x + 4x^2$ | $\longrightarrow$ | $(6\ \ 13\ \ 4)$ |
| $x^{22} = 6 + 13x + 12x^2$ | $\longrightarrow$ | $(6\ \ 13\ \ 12)$ | $x^{51} = 12 + 2x + 13x^2$ | $\longrightarrow$ | $(12\ \ 2\ \ 13)$ |
| $x^{23} = 4 + 10x + 13x^2$ | $\longrightarrow$ | $(4\ \ 10\ \ 13)$ | $x^{52} = 3 + 15x + 2x^2$ | $\longrightarrow$ | $(3\ \ 15\ \ 2)$ |
| $x^{24} = 3 + 7x + 10x^2$ | $\longrightarrow$ | $(3\ \ 7\ \ 10)$ | $x^{53} = 14 + x + 15x^2$ | $\longrightarrow$ | $(14\ \ 1\ \ 15)$ |
| $x^{25} = 6 + 9x + 7x^2$ | $\longrightarrow$ | $(6\ \ 9\ \ 7)$ | $x^{54} = 1 + 15x + x^2$ | $\longrightarrow$ | $(1\ \ 15\ \ 1)$ |
| $x^{26} = 9 + 15x + 9x^2$ | $\longrightarrow$ | $(9\ \ 15\ \ 9)$ | $x^{55} = 15 + 15x^2$ | $\longrightarrow$ | $(15\ \ 0\ \ 15)$ |
| $x^{27} = 7 + 15x^2$ | $\longrightarrow$ | $(7\ \ 0\ \ 15)$ | $x^{56} = x^0$ | $\longrightarrow$ | $(1\ \ 0\ \ 0)$ |
| $x^{28} = 1 + 8x$ | $\longrightarrow$ | $(1\ \ 8\ \ 0)$ | | | |

Tabela 5.4: Grupo das Unidades de $GR(16, 3)$

Como o número de elementos desse grupo das unidades é par, a fatoração do termo $x^{56}-1$ não é única. Neste caso, deve-se buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta=\alpha^8$, obtém-se um grupo multiplicativo com 7 elementos, como desejado. Consequentemente, a fatoração do termo $x^7-1$ é única.

**Exemplo 6.** *Determinação do grupo das unidades de GR(27,2) e GR(27,3)*

Inicialmente, considere o anel $GR(p^m,r)=GR(27,2)$ dado pela extensão de Galois de grau 2:

$$GR(27,2)[x]\cong\frac{\mathbb{Z}_{27}[x]}{\langle x^2+x+2\rangle}=\{a+bx;a,b\in\mathbb{Z}_{27}\}. \tag{5.9}$$

Considere agora o corpo $GF(p^r)=GF(9)$, onde

$$\begin{aligned} GF(9)[x]\cong\mathbb{F}_9[x]\cong\frac{\mathbb{F}_3[x]}{\langle x^2+x+2\rangle} &= \{a'+b'x;a',b'\in\mathbb{F}_3\} \\ &= \{0,1,x,1+2x,2+2x,2,2x,2+x,1+x\}. \end{aligned} \tag{5.10}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_{27}$, logo $\alpha$ é uma raiz de $x^2+x+2=0$, ou seja, $\alpha^2=-\alpha-2$ em $\mathbb{Z}_3$ teremos $\alpha^2=2\alpha+1$. Assim, $\mathbb{F}_{27}$ apresenta os mesmos elementos do grupo multiplicativo da Tabela 4.7.

Seja $f=(0\ 1)\in GR^*(27,2)$, onde $GR^*(27,2)$ denota o grupo das unidades de $GR(27,2)$. Portanto, $\overline{f}=R_3(f)=(0\ 1)=f$ gera um subgrupo cíclico de ordem $n=(p^r-1)=8$ em $\mathbb{F}_{27}$, lembrando que $R_3(f)$ é a redução módulo 3 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd=8d$ em $GR^*(27,2)$, onde $d\geq 1\in\mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_8$ de $GR^*(27,2)$.

As operações em $GR^*(27,2)$ são realizadas módulo $(x^2+x+2)$. Logo, $x^2=-x-2$; porém, como os coeficientes de $GR^*(27,2)$ estão em $\mathbb{Z}_{27}$, temos que $x^2=26x+25$. Assim, considerando $(f)=(0\ 1)=x$, a representação dos elementos do grupo das unidades de $GR(27,2)$ é como mostrado abaixo:

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1 \;\; 0)$ | $x^{29} = 12 + 26x$ | $\longrightarrow$ | $(12 \;\; 26)$ |
| $x = x^1$ | $\longrightarrow$ | $(0 \;\; 1)$ | $x^{30} = 2 + 13x$ | $\longrightarrow$ | $(2 \;\; 13)$ |
| $x^2 = 25 + 26x$ | $\longrightarrow$ | $(25 \;\; 26)$ | $x^{31} = 1 + 16x$ | $\longrightarrow$ | $(1 \;\; 16)$ |
| $x^3 = 2 + 26x$ | $\longrightarrow$ | $(2 \;\; 26)$ | $x^{32} = 22 + 12x$ | $\longrightarrow$ | $(22 \;\; 12)$ |
| $x^4 = 2 + 3x$ | $\longrightarrow$ | $(2 \;\; 3)$ | $x^{33} = 3 + 10x$ | $\longrightarrow$ | $(3 \;\; 10)$ |
| $x^5 = 21 + 26x$ | $\longrightarrow$ | $(21 \;\; 26)$ | $x^{34} = 7 + 20x$ | $\longrightarrow$ | $(7 \;\; 20)$ |
| $x^6 = 2 + 22x$ | $\longrightarrow$ | $(2 \;\; 22)$ | $x^{35} = 14 + 14x$ | $\longrightarrow$ | $(14 \;\; 14)$ |
| $x^7 = 10 + 7x$ | $\longrightarrow$ | $(10 \;\; 7)$ | $x^{36} = 26$ | $\longrightarrow$ | $(26 \;\; 0)$ |
| $x^8 = 13 + 3x$ | $\longrightarrow$ | $(13 \;\; 3)$ | $x^{37} = 26x$ | $\longrightarrow$ | $(0 \;\; 26)$ |
| $x^9 = 21 + 10x$ | $\longrightarrow$ | $(21 \;\; 10)$ | $x^{38} = 2 + x$ | $\longrightarrow$ | $(2 \;\; 1)$ |
| $x^{10} = 7 + 11x$ | $\longrightarrow$ | $(7 \;\; 11)$ | $x^{39} = 25 + x$ | $\longrightarrow$ | $(25 \;\; 1)$ |
| $x^{11} = 5 + 23x$ | $\longrightarrow$ | $(5 \;\; 23)$ | $x^{40} = 25 + 24x$ | $\longrightarrow$ | $(25 \;\; 24)$ |
| $x^{12} = 8 + 9x$ | $\longrightarrow$ | $(8 \;\; 9)$ | $x^{41} = 6 + x$ | $\longrightarrow$ | $(6 \;\; 1)$ |
| $x^{13} = 9 + 26x$ | $\longrightarrow$ | $(9 \;\; 26)$ | $x^{42} = 25 + 5x$ | $\longrightarrow$ | $(25 \;\; 5)$ |
| $x^{14} = 2 + 10x$ | $\longrightarrow$ | $(2 \;\; 10)$ | $x^{43} = 17 + 20x$ | $\longrightarrow$ | $(17 \;\; 20)$ |
| $x^{15} = 7 + 19x$ | $\longrightarrow$ | $(7 \;\; 19)$ | $x^{44} = 14 + 24x$ | $\longrightarrow$ | $(14 \;\; 24)$ |
| $x^{16} = 16 + 15x$ | $\longrightarrow$ | $(16 \;\; 15)$ | $x^{45} = 6 + 17x$ | $\longrightarrow$ | $(6 \;\; 17)$ |
| $x^{17} = 24 + x$ | $\longrightarrow$ | $(24 \;\; 1)$ | $x^{46} = 20 + 16x$ | $\longrightarrow$ | $(20 \;\; 16)$ |
| $x^{18} = 25 + 23x$ | $\longrightarrow$ | $(25 \;\; 23)$ | $x^{47} = 22 + 4x$ | $\longrightarrow$ | $(22 \;\; 4)$ |
| $x^{19} = 8 + 2x$ | $\longrightarrow$ | $(8 \;\; 2)$ | $x^{48} = 19 + 18x$ | $\longrightarrow$ | $(19 \;\; 18)$ |
| $x^{20} = 23 + 6x$ | $\longrightarrow$ | $(23 \;\; 6)$ | $x^{49} = 18 + x$ | $\longrightarrow$ | $(18 \;\; 1)$ |
| $x^{21} = 15 + 17x$ | $\longrightarrow$ | $(15 \;\; 17)$ | $x^{50} = 25 + 17x$ | $\longrightarrow$ | $(25 \;\; 17)$ |
| $x^{22} = 20 + 25x$ | $\longrightarrow$ | $(20 \;\; 25)$ | $x^{51} = 20 + 8x$ | $\longrightarrow$ | $(20 \;\; 8)$ |
| $x^{23} = 4 + 22x$ | $\longrightarrow$ | $(4 \;\; 22)$ | $x^{52} = 11 + 12x$ | $\longrightarrow$ | $(11 \;\; 12)$ |
| $x^{24} = 10 + 9x$ | $\longrightarrow$ | $(10 \;\; 9)$ | $x^{53} = 3 + 26x$ | $\longrightarrow$ | $(3 \;\; 26)$ |
| $x^{25} = 9 + x$ | $\longrightarrow$ | $(9 \;\; 1)$ | $x^{54} = 2 + 4x$ | $\longrightarrow$ | $(2 \;\; 4)$ |
| $x^{26} = 25 + 8x$ | $\longrightarrow$ | $(25 \;\; 8)$ | $x^{55} = 19 + 25x$ | $\longrightarrow$ | $(19 \;\; 25)$ |
| $x^{27} = 11 + 17x$ | $\longrightarrow$ | $(11 \;\; 17)$ | $x^{56} = 4 + 21x$ | $\longrightarrow$ | $(4 \;\; 21)$ |
| $x^{28} = 15 + 17x$ | $\longrightarrow$ | $(15 \;\; 17)$ | $x^{57} = 12 + 10x$ | $\longrightarrow$ | $(12 \;\; 10)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{58} = 7 + 2x$ | $\longrightarrow$ | (7 2) | $x^{66} = 25 + 14x$ | $\longrightarrow$ | (25 14) |
| $x^{59} = 23 + 5x$ | $\longrightarrow$ | (23 5) | $x^{67} = 26 + 11x$ | $\longrightarrow$ | (26 11) |
| $x^{60} = 17 + 18x$ | $\longrightarrow$ | (17 18) | $x^{68} = 5 + 15x$ | $\longrightarrow$ | (5 15) |
| $x^{61} = 18 + 26x$ | $\longrightarrow$ | (18 26) | $x^{69} = 24 + 17x$ | $\longrightarrow$ | (24 17) |
| $x^{62} = 2 + 19x$ | $\longrightarrow$ | (2 19) | $x^{70} = 20 + 7x$ | $\longrightarrow$ | (20 7) |
| $x^{63} = 16 + 10x$ | $\longrightarrow$ | (16 10) | $x^{71} = 13 + 13x$ | $\longrightarrow$ | (13 13) |
| $x^{64} = 7 + 6x$ | $\longrightarrow$ | (7 6) | $x^{72} = x^0$ | $\longrightarrow$ | (1 0) |
| $x^{65} = 15 + x$ | $\longrightarrow$ | (15 1) | | | |

Tabela 5.5: Grupo das Unidades de $GR(27, 2)$

Como o número de elementos desse grupo das unidades é par, a fatoração do termo $x^{72} - 1$ não é única. Neste caso, deve-se buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta = \alpha^8$, obtém-se um grupo multiplicativo com 9 elementos, como desejado. Consequentemente, a fatoração do termo $x^9 - 1$ é única. Note que poderíamos definir $\beta = \alpha^{24}$ conduzindo a um grupo multiplicativo com 3 elementos.

Considere o anel $GR(p^m, r) = GR(27, 3)$ dado pela extensão de Galois de grau 3:

$$GR(27,3)[x] \cong \frac{\mathbb{Z}_{27}[x]}{\langle x^3 + 2x + 1\rangle} = \{a + bx + cx^2; a, b, c \in \mathbb{Z}_{27}\}. \tag{5.11}$$

Seja o corpo $GF(p^r) = GF(27)$ :

$$\begin{aligned} GF(27)[x] \cong \mathbb{F}_{27}[x] \cong \frac{\mathbb{F}_3[x]}{\langle x^3 + 2x + 1\rangle} &= \\ &= \{a' + b'x + c'x^2; a', b', c' \in \mathbb{F}_3\}. \end{aligned} \tag{5.12}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_{27}$, logo $\alpha$ é uma raiz de $x^3 + 2x + 1 = 0$, isto é, $\alpha^3 = -2\alpha - 1$ em $\mathbb{F}_3$ temos $\alpha^3 = \alpha + 2$. Assim, $\mathbb{F}_{27}$ apresenta os elementos do grupo multiplicativo da Tabela 4.7.

Seja $f = (0\ 1\ 0) \in GR^*(27,3)$, onde $GR^*(27,3)$ denota o grupo das unidades de $GR(27,3)$. Portanto, $\overline{f} = R_3(f) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 26$ em $\mathbb{F}_{27}$, lembrando que $R_3(f)$ é a redução módulo 3 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 26d$ em $GR^*(27,3)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_{26}$ de $GR^*(27,3)$.

As operações em $GR^*(27,3)$ são realizadas módulo $(x^3 + 2x + 1)$. Logo, $x^3 = -2x - 1$, porém, como os coeficientes de $GR^*(27,3)$ estão em $\mathbb{Z}_{27}$, temos que $x^3 = 25x + 26$. Assim, considerando $(f) = (0\ 1\ 0) = x$, a representação dos elementos do grupo das unidades de $GR(27,3)$ é como mostrado na Tabela C.1 do Apêndice.

Como o número de elementos desse grupo das unidades é par, a fatoração do termo $x^{234} - 1$ não é única. Neste caso, deve-se buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta = \alpha^2$, obtém-se um grupo multiplicativo com 117 elementos, como desejado. Consequentemente, a fatoração do termo $x^{117} - 1$ é única. Note que poderíamos ter escolhido $\beta = \alpha^{18}$, $\beta = \alpha^{26}$ e $\beta = \alpha^{78}$ conduzindo a grupos multiplicativos com ordens $13, 9$ e $3$, respectivamente.

**Exemplo 7.** *Determinação do grupo das unidades de GR(25,2) e GR(25,3)*

Inicialmente, considere o anel $GR(p^m, r) = GR(25,2)$ dado pela extensão de Galois de grau 2:

$$GR(25,2)[x] \cong \frac{\mathbb{Z}_{25}[x]}{\langle x^2 + 4x + 2 \rangle} = \{a + bx; a, b \in \mathbb{Z}_{25}\}. \tag{5.13}$$

Considere agora o corpo $GF(p^r) = GF(25)$, onde

$$GF(25)[x] \cong \mathbb{F}_{25}[x] \cong \frac{\mathbb{F}_5[x]}{\langle x^2 + 4x + 2 \rangle} \quad = \quad \{a' + b'x; a', b' \in \mathbb{F}_5\} \tag{5.14}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_{25}$, logo $\alpha$ é uma raiz de $x^2 + 4x + 2 = 0$, ou seja, $\alpha^2 = -4\alpha - 2$ em $\mathbb{Z}_5$ temos $\alpha^2 = \alpha + 3$. Assim, $\mathbb{F}_{25}$ apresenta seguintes os elementos do grupo multiplicativo como mostrado na Tabela 5.6.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | (1 0) | $x^{13} = 4x$ | $\longrightarrow$ | (0 4) |
| $x = x^1$ | $\longrightarrow$ | (0 1) | $x^{14} = 2 + 4x$ | $\longrightarrow$ | (2 4) |
| $x^2 = 3 + x$ | $\longrightarrow$ | (3 1) | $x^{15} = 2 + x$ | $\longrightarrow$ | (2 1) |
| $x^3 = 3 + 4x$ | $\longrightarrow$ | (3 4) | $x^{16} = 3 + 3x$ | $\longrightarrow$ | (3 3) |
| $x^4 = 2 + 2x$ | $\longrightarrow$ | (2 2) | $x^{17} = 4 + x$ | $\longrightarrow$ | (4 1) |
| $x^5 = 1 + 4x$ | $\longrightarrow$ | (1 4) | $x^{18} = 3$ | $\longrightarrow$ | (3 0) |
| $x^6 = 2$ | $\longrightarrow$ | (2 0) | $x^{19} = 3x$ | $\longrightarrow$ | (0 3) |
| $x^7 = 2x$ | $\longrightarrow$ | (0 2) | $x^{20} = 4 + 3x$ | $\longrightarrow$ | (4 3) |
| $x^8 = 1 + 2x$ | $\longrightarrow$ | (1 2) | $x^{21} = 4 + 2x$ | $\longrightarrow$ | (4 2) |
| $x^9 = 1 + 3x$ | $\longrightarrow$ | (1 3) | $x^{22} = 1 + x$ | $\longrightarrow$ | (1 1) |
| $x^{10} = 4 + 4x$ | $\longrightarrow$ | (4 4) | $x^{23} = 3 + 2x$ | $\longrightarrow$ | (3 2) |
| $x^{11} = 2 + 3x$ | $\longrightarrow$ | (2 3) | $x^{24} = 12 + 26x$ | $\longrightarrow$ | (12 26) |
| $x^{12} = 4$ | $\longrightarrow$ | (4 0) | | | |

Tabela 5.6: Grupo Multiplicativo de GF(25)

Seja $f = (0\ 1) \in GR^*(25, 2)$. Portanto, $f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 24$ em $\mathbb{F}_{25}$, lembrando que $R_5(f)$ é a redução módulo 5 do elemento $f$. Logo, pelo Teorema 35 temos que $f$ deve gerar um grupo de ordem $nd = 24d$ em $GR^*(25, 2)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_{24}$ de $GR^*(25, 2)$. As operações em $GR^*(25, 2)$ são realizadas módulo $(x^2 + 4x + 2)$. Logo, como os coeficientes de $GR^*(25, 2)$ estão em $\mathbb{Z}_{25}$, temos que $x^2 = 21x + 23$. Assim, considerando $(f) = x$, a representação dos elementos do grupo das unidades de $GR(25, 2)$ é como mostrado na Tabela 5.7.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0)$ | $x^{29} = 11 + 9x$ | $\longrightarrow$ | $(11\ \ 9)$ |
| $x = x^1$ | $\longrightarrow$ | $(0\ \ 1)$ | $x^{30} = 7$ | $\longrightarrow$ | $(7\ \ 0)$ |
| $x^2 = 23 + 21x$ | $\longrightarrow$ | $(23\ \ 21)$ | $x^{31} = 7x$ | $\longrightarrow$ | $(0\ \ 7)$ |
| $x^3 = 8 + 14x$ | $\longrightarrow$ | $(8\ \ 14)$ | $x^{32} = 11 + 22x$ | $\longrightarrow$ | $(11\ \ 22)$ |
| $x^4 = 22 + 2x$ | $\longrightarrow$ | $(22\ \ 2)$ | $x^{33} = 6 + 23x$ | $\longrightarrow$ | $(6\ \ 23)$ |
| $x^5 = 21 + 14x$ | $\longrightarrow$ | $(21\ \ 14)$ | $x^{34} = 4 + 14x$ | $\longrightarrow$ | $(4\ \ 14)$ |
| $x^6 = 22 + 15x$ | $\longrightarrow$ | $(22\ \ 15)$ | $x^{35} = 22 + 23x$ | $\longrightarrow$ | $(22\ \ 23)$ |
| $x^7 = 20 + 12x$ | $\longrightarrow$ | $(20\ \ 12)$ | $x^{36} = 4 + 5x$ | $\longrightarrow$ | $(4\ \ 5)$ |
| $x^8 = 1 + 22x$ | $\longrightarrow$ | $(1\ \ 22)$ | $x^{37} = 15 + 9x$ | $\longrightarrow$ | $(15\ \ 9)$ |
| $x^9 = 6 + 13x$ | $\longrightarrow$ | $(6\ \ 13)$ | $x^{38} = 7 + 4x$ | $\longrightarrow$ | $(7\ \ 4)$ |
| $x^{10} = 24 + 4x$ | $\longrightarrow$ | $(24\ \ 4)$ | $x^{39} = 17 + 16x$ | $\longrightarrow$ | $(17\ \ 16)$ |
| $x^{11} = 17 + 8x$ | $\longrightarrow$ | $(17\ \ 8)$ | $x^{40} = 18 + 3x$ | $\longrightarrow$ | $(18\ \ 3)$ |
| $x^{12} = 9 + 10x$ | $\longrightarrow$ | $(9\ \ 10)$ | $x^{41} = 19 + 6x$ | $\longrightarrow$ | $(19\ \ 6)$ |
| $x^{13} = 5 + 19x$ | $\longrightarrow$ | $(5\ \ 19)$ | $x^{42} = 13 + 20x$ | $\longrightarrow$ | $(13\ \ 20)$ |
| $x^{14} = 12 + 4x$ | $\longrightarrow$ | $(12\ \ 4)$ | $x^{43} = 10 + 8x$ | $\longrightarrow$ | $(10\ \ 8)$ |
| $x^{15} = 17 + 21x$ | $\longrightarrow$ | $(17\ \ 21)$ | $x^{44} = 9 + 3x$ | $\longrightarrow$ | $(9\ \ 3)$ |
| $x^{16} = 8 + 8x$ | $\longrightarrow$ | $(8\ \ 8)$ | $x^{45} = 19 + 22x$ | $\longrightarrow$ | $(19\ \ 22)$ |
| $x^{17} = 9 + x$ | $\longrightarrow$ | $(9\ \ 1)$ | $x^{46} = 6 + 6x$ | $\longrightarrow$ | $(6\ \ 6)$ |
| $x^{18} = 23 + 5x$ | $\longrightarrow$ | $(23\ \ 5)$ | $x^{47} = 13 + 7x$ | $\longrightarrow$ | $(13\ \ 7)$ |
| $x^{19} = 15 + 3x$ | $\longrightarrow$ | $(15\ \ 3)$ | $x^{48} = 11 + 10x$ | $\longrightarrow$ | $(11\ \ 10)$ |
| $x^{20} = 19 + 3x$ | $\longrightarrow$ | $(19\ \ 3)$ | $x^{49} = 5 + 21x$ | $\longrightarrow$ | $(5\ \ 21)$ |
| $x^{21} = 19 + 7x$ | $\longrightarrow$ | $(19\ \ 7)$ | $x^{50} = 8 + 21x$ | $\longrightarrow$ | $(8\ \ 21)$ |
| $x^{22} = 11 + 16x$ | $\longrightarrow$ | $(11\ \ 16)$ | $x^{51} = 8 + 24x$ | $\longrightarrow$ | $(8\ \ 24)$ |
| $x^{23} = 18 + 22x$ | $\longrightarrow$ | $(18\ \ 22)$ | $x^{52} = 2 + 12x$ | $\longrightarrow$ | $(2\ \ 12)$ |
| $x^{24} = 6 + 5x$ | $\longrightarrow$ | $(6\ \ 5)$ | $x^{53} = 1 + 4x$ | $\longrightarrow$ | $(1\ \ 4)$ |
| $x^{25} = 15 + 11x$ | $\longrightarrow$ | $(15\ \ 11)$ | $x^{54} = 17 + 10x$ | $\longrightarrow$ | $(17\ \ 10)$ |
| $x^{26} = 3 + 21x$ | $\longrightarrow$ | $(3\ \ 21)$ | $x^{55} = 5 + 2x$ | $\longrightarrow$ | $(5\ \ 2)$ |
| $x^{27} = 8 + 19x$ | $\longrightarrow$ | $(8\ \ 19)$ | $x^{56} = 21 + 22x$ | $\longrightarrow$ | $(21\ \ 22)$ |
| $x^{28} = 12 + 7x$ | $\longrightarrow$ | $(12\ \ 7)$ | $x^{57} = 6 + 8x$ | $\longrightarrow$ | $(6\ \ 8)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{58} = 9 + 24x$ | $\longrightarrow$ | (9 24) | $x^{90} = 18$ | $\longrightarrow$ | (18 0) |
| $x^{59} = 2 + 13x$ | $\longrightarrow$ | (2 13) | $x^{91} = 18x$ | $\longrightarrow$ | (0 18) |
| $x^{60} = 24$ | $\longrightarrow$ | (24 0) | $x^{92} = 14 + 3x$ | $\longrightarrow$ | (14 3) |
| $x^{61} = 24x$ | $\longrightarrow$ | (0 24) | $x^{93} = 19 + 2x$ | $\longrightarrow$ | (19 2) |
| $x^{62} = 2 + 4x$ | $\longrightarrow$ | (2 4) | $x^{94} = 21 + 11x$ | $\longrightarrow$ | (21 11) |
| $x^{63} = 17 + 11x$ | $\longrightarrow$ | (17 11) | $x^{95} = 3 + 2x$ | $\longrightarrow$ | (3 2) |
| $x^{64} = 3 + 23x$ | $\longrightarrow$ | (3 23) | $x^{96} = 21 + 20x$ | $\longrightarrow$ | (21 20) |
| $x^{65} = 4 + 11x$ | $\longrightarrow$ | (4 11) | $x^{97} = 10 + 16x$ | $\longrightarrow$ | (10 16) |
| $x^{66} = 3 + 10x$ | $\longrightarrow$ | (3 10) | $x^{98} = 18 + 21x$ | $\longrightarrow$ | (18 21) |
| $x^{67} = 5 + 13x$ | $\longrightarrow$ | (5 13) | $x^{99} = 8 + 9x$ | $\longrightarrow$ | (8 9) |
| $x^{68} = 24 + 3x$ | $\longrightarrow$ | (24 3) | $x^{100} = 7 + 22x$ | $\longrightarrow$ | (7 22) |
| $x^{69} = 19 + 12x$ | $\longrightarrow$ | (19 12) | $x^{101} = 6 + 19x$ | $\longrightarrow$ | (6 19) |
| $x^{70} = 1 + 21x$ | $\longrightarrow$ | (1 21) | $x^{102} = 12 + 5x$ | $\longrightarrow$ | (12 5) |
| $x^{71} = 8 + 17x$ | $\longrightarrow$ | (8 17) | $x^{103} = 15 + 17x$ | $\longrightarrow$ | (15 17) |
| $x^{72} = 16 + 15x$ | $\longrightarrow$ | (16 15) | $x^{104} = 16 + 22x$ | $\longrightarrow$ | (16 22) |
| $x^{73} = 20 + 6x$ | $\longrightarrow$ | (20 6) | $x^{105} = 6 + 3x$ | $\longrightarrow$ | (6 3) |
| $x^{74} = 13 + 21x$ | $\longrightarrow$ | (13 21) | $x^{106} = 19 + 19x$ | $\longrightarrow$ | (19 19) |
| $x^{75} = 8 + 4x$ | $\longrightarrow$ | (8 4) | $x^{107} = 12 + 18x$ | $\longrightarrow$ | (12 18) |
| $x^{76} = 17 + 17x$ | $\longrightarrow$ | (17 17) | $x^{108} = 14 + 15x$ | $\longrightarrow$ | (14 15) |
| $x^{77} = 16 + 24x$ | $\longrightarrow$ | (16 24) | $x^{109} = 20 + 4x$ | $\longrightarrow$ | (20 4) |
| $x^{78} = 2 + 20x$ | $\longrightarrow$ | (2 20) | $x^{110} = 17 + 4x$ | $\longrightarrow$ | (17 4) |
| $x^{79} = 10 + 22x$ | $\longrightarrow$ | (10 22) | $x^{111} = 17 + x$ | $\longrightarrow$ | (17 1) |
| $x^{80} = 6 + 22x$ | $\longrightarrow$ | (6 22) | $x^{112} = 23 + 13x$ | $\longrightarrow$ | (23 13) |
| $x^{81} = 6 + 18x$ | $\longrightarrow$ | (6 18) | $x^{113} = 24 + 21x$ | $\longrightarrow$ | (24 21) |
| $x^{82} = 14 + 9x$ | $\longrightarrow$ | (14 9) | $x^{114} = 8 + 15x$ | $\longrightarrow$ | (8 15) |
| $x^{83} = 7 + 3x$ | $\longrightarrow$ | (7 3) | $x^{115} = 20 + 23x$ | $\longrightarrow$ | (20 23) |
| $x^{84} = 19 + 20x$ | $\longrightarrow$ | (19 20) | $x^{116} = 4 + 3x$ | $\longrightarrow$ | (4 3) |
| $x^{85} = 10 + 14x$ | $\longrightarrow$ | (10 14) | $x^{117} = 19 + 17x$ | $\longrightarrow$ | (19 17) |
| $x^{86} = 22 + 4x$ | $\longrightarrow$ | (22 4) | $x^{118} = 16 + x$ | $\longrightarrow$ | (16 1) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{87}= 17+6x$ | $\longrightarrow$ | (17 6) | $x^{119} = 23+12x$ | $\longrightarrow$ | (23 12) |
| $x^{88} = 13+18x$ | $\longrightarrow$ | (13 18) | $x^{120} = x^0$ | $\longrightarrow$ | (1 0) |
| $x^{89} = 14+16x$ | $\longrightarrow$ | (14 16) | | | |

Tabela 5.7: Grupo das Unidades de $GR(25,2)$

Como o número de elementos desse grupo das unidades é par, a fatoração do termo $x^{120}-1$ não é única. Neste caso, deve-se buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta = \alpha^8$, obtém-se um grupo multiplicativo com 15 elementos, como desejado. Consequentemente, a fatoração do termo $x^{15}-1$ é única. Note que poderíamos ter escolhido $\beta = \alpha^{24}$ e $\beta = \alpha^{40}$ conduzindo a grupos multiplicativos com ordens 5 e 3, respectivamente.

Considere o anel $GR(p^m, r) = GR(25,3)$ dado pela extensão de Galois de grau 3:

$$GR(25,3)[x] \cong \frac{\mathbb{Z}_{25}[x]}{\langle x^3+3x+2\rangle} = \{a+bx+cx^2; a,b,c \in \mathbb{Z}_{25}\}. \tag{5.15}$$

Seja o corpo $GF(p^r) = GF(125)$ :

$$GF(125)[x] \cong \mathbb{F}_{125}[x] \cong \frac{\mathbb{F}_5[x]}{\langle x^3+3x+2\rangle} = \{a'+b'x+c'x^2; a',b',c' \in \mathbb{F}_5\}. \tag{5.16}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_{25}$, logo $\alpha$ é uma raiz de $x^3+3x+2=0$, ou seja, $\alpha^3 = -3\alpha - 2$. Em $\mathbb{F}_5$ temos $\alpha^3 = 2\alpha + 3$. Assim, $\mathbb{F}_{25}$ apresenta os seguintes elementos do grupo multiplicativo:

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | (1 0 0) | $x^{39} = 3+3x+x^2$ | $\longrightarrow$ | (3 3 1) |
| $x = x^1$ | $\longrightarrow$ | (0 1 0) | $x^{40} = 3+3x^2$ | $\longrightarrow$ | (3 0 3) |
| $x^2 = x^2$ | $\longrightarrow$ | (0 0 1) | $x^{41} = 4+4x$ | $\longrightarrow$ | (4 4 0) |
| $x^3= 3+2x$ | $\longrightarrow$ | (3 2 0) | $x^{42} = 4x+4x^2$ | $\longrightarrow$ | (0 4 4) |
| $x^4 = 3x+2x^2$ | $\longrightarrow$ | (0 3 2) | $x^{43}= 2+3x+4x^2$ | $\longrightarrow$ | (2 3 4) |

| | | | | | |
|---|---|---|---|---|---|
| $x^5 = 1 + 4x + 3x^2$ | $\longrightarrow$ | $(1\ 4\ 3)$ | $x^{44} = 2 + 3x^2$ | $\longrightarrow$ | $(2\ 0\ 3)$ |
| $x^6 = 4 + 2x + 4x^2$ | $\longrightarrow$ | $(4\ 2\ 4)$ | $x^{45} = 4 + 3x$ | $\longrightarrow$ | $(4\ 3\ 0)$ |
| $x^7 = 2 + 2x + 2x^2$ | $\longrightarrow$ | $(2\ 2\ 2)$ | $x^{46} = 4x + 3x^2$ | $\longrightarrow$ | $(0\ 4\ 3)$ |
| $x^8 = 1 + x + 2x^2$ | $\longrightarrow$ | $(1\ 1\ 2)$ | $x^{47} = 4 + x + 4x^2$ | $\longrightarrow$ | $(4\ 1\ 4)$ |
| $x^9 = 1 + x^2$ | $\longrightarrow$ | $(1\ 0\ 1)$ | $x^{48} = 2 + 2x + x^2$ | $\longrightarrow$ | $(2\ 2\ 1)$ |
| $x^{10} = 3 + 3x$ | $\longrightarrow$ | $(3\ 3\ 0)$ | $x^{49} = 3 + 4x + 2x^2$ | $\longrightarrow$ | $(3\ 4\ 2)$ |
| $x^{11} = 3x + 3x^2$ | $\longrightarrow$ | $(0\ 3\ 3)$ | $x^{50} = 1 + 2x + 4x^2$ | $\longrightarrow$ | $(1\ 2\ 4)$ |
| $x^{12} = 4 + x + 3x^2$ | $\longrightarrow$ | $(4\ 1\ 3)$ | $x^{51} = 2 + 4x + 2^2$ | $\longrightarrow$ | $(2\ 4\ 2)$ |
| $x^{13} = 4 + x^2$ | $\longrightarrow$ | $(4\ 0\ 1)$ | $x^{52} = 1 + x + 4x^2$ | $\longrightarrow$ | $(1\ 1\ 4)$ |
| $x^{14} = 3 + x$ | $\longrightarrow$ | $(3\ 1\ 0)$ | $x^{53} = 2 + 4x + x^2$ | $\longrightarrow$ | $(2\ 4\ 1)$ |
| $x^{15} = 3x + x^2$ | $\longrightarrow$ | $(0\ 3\ 1)$ | $x^{54} = 3 + 4x + 4x^2$ | $\longrightarrow$ | $(3\ 4\ 4)$ |
| $x^{16} = 3 + 2x + 3x^2$ | $\longrightarrow$ | $(3\ 2\ 3)$ | $x^{55} = 2 + x + 4x^2$ | $\longrightarrow$ | $(2\ 1\ 4)$ |
| $x^{17} = 4 + 4x + 2x^2$ | $\longrightarrow$ | $(4\ 4\ 2)$ | $x^{56} = 2 + x^2$ | $\longrightarrow$ | $(2\ 0\ 1)$ |
| $x^{18} = 1 + 3x + 4x^2$ | $\longrightarrow$ | $(1\ 3\ 4)$ | $x^{57} = 3 + 4x$ | $\longrightarrow$ | $(3\ 4\ 0)$ |
| $x^{19} = 2 + 4x + 3x^2$ | $\longrightarrow$ | $(2\ 4\ 3)$ | $x^{58} = 3x + 4x^2$ | $\longrightarrow$ | $(0\ 3\ 4)$ |
| $x^{20} = 4 + 3x + 4x^2$ | $\longrightarrow$ | $(4\ 3\ 4)$ | $x^{59} = 2 + 3x + 3x^2$ | $\longrightarrow$ | $(2\ 3\ 3)$ |
| $x^{21} = 2 + 2x + 3x^2$ | $\longrightarrow$ | $(2\ 2\ 3)$ | $x^{60} = 4 + 3x + 3x^2$ | $\longrightarrow$ | $(4\ 3\ 3)$ |
| $x^{22} = 4 + 3x + 2x^2$ | $\longrightarrow$ | $(4\ 3\ 2)$ | $x^{61} = 4 + 3x^2$ | $\longrightarrow$ | $(4\ 0\ 3)$ |
| $x^{23} = 1 + 3x + 3x^2$ | $\longrightarrow$ | $(1\ 3\ 3)$ | $x^{62} = 4$ | $\longrightarrow$ | $(4\ 0\ 0)$ |
| $x^{24} = 4 + 2x + 3x^2$ | $\longrightarrow$ | $(4\ 2\ 3)$ | $x^{63} = 4x$ | $\longrightarrow$ | $(0\ 4\ 0)$ |
| $x^{25} = 4 + 2x^2$ | $\longrightarrow$ | $(4\ 0\ 2)$ | $x^{64} = 4x^2$ | $\longrightarrow$ | $(0\ 0\ 4)$ |
| $x^{26} = 1 + 3x$ | $\longrightarrow$ | $(1\ 3\ 0)$ | $x^{65} = 2 + 3x$ | $\longrightarrow$ | $(2\ 3\ 0)$ |
| $x^{27} = x + 3x^2$ | $\longrightarrow$ | $(0\ 1\ 3)$ | $x^{66} = 2x + 3x^2$ | $\longrightarrow$ | $(0\ 2\ 3)$ |
| $x^{28} = 4 + x + x^2$ | $\longrightarrow$ | $(4\ 1\ 1)$ | $x^{67} = 4 + x + 2x^2$ | $\longrightarrow$ | $(4\ 1\ 2)$ |
| $x^{29} = 3 + x + x^2$ | $\longrightarrow$ | $(3\ 1\ 1)$ | $x^{68} = 1 + 3x + x^2$ | $\longrightarrow$ | $(1\ 3\ 1)$ |
| $x^{30} = 3 + x^2$ | $\longrightarrow$ | $(3\ 0\ 1)$ | $x^{69} = 3 + 3x + 3x^2$ | $\longrightarrow$ | $(3\ 3\ 3)$ |
| $x^{31} = 3$ | $\longrightarrow$ | $(3\ 0\ 0)$ | $x^{70} = 4 + 4x + 3x^2$ | $\longrightarrow$ | $(4\ 4\ 3)$ |
| $x^{32} = 3x$ | $\longrightarrow$ | $(0\ 3\ 0)$ | $x^{71} = 4 + 4x^2$ | $\longrightarrow$ | $(4\ 0\ 4)$ |
| $x^{33} = 3x^2$ | $\longrightarrow$ | $(0\ 0\ 3)$ | $x^{72} = 2 + 2x$ | $\longrightarrow$ | $(2\ 2\ 0)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{34}= 4+x$ | $\longrightarrow$ | $(4\ 1\ 0)$ | $x^{73} = 2x+2x^2$ | $\longrightarrow$ | $(0\ 2\ 2)$ |
| $x^{35} = 4x+x^2$ | $\longrightarrow$ | $(0\ 4\ 1)$ | $x^{74} = 1+4x+2x^2$ | $\longrightarrow$ | $(1\ 4\ 2)$ |
| $x^{36}= 3+2x+4x^2$ | $\longrightarrow$ | $(3\ 2\ 4)$ | $x^{75} = 1+4x^2$ | $\longrightarrow$ | $(1\ 0\ 4)$ |
| $x^{37} = 2+x+2x^2$ | $\longrightarrow$ | $(2\ 1\ 2)$ | $x^{76}= 2+4x$ | $\longrightarrow$ | $(2\ 4\ 0)$ |
| $x^{38} = 1+x+x^2$ | $\longrightarrow$ | $(1\ 1\ 1)$ | $x^{77} = 2x+2x^2$ | $\longrightarrow$ | $(0\ 2\ 2)$ |
| $x^{78} = 2+3x+2x^2$ | $\longrightarrow$ | $(2\ 3\ 2)$ | $x^{102}= 2+2x^2$ | $\longrightarrow$ | $(2\ 0\ 2)$ |
| $x^{79} = 1+x+3x^2$ | $\longrightarrow$ | $(1\ 1\ 3)$ | $x^{103} = 1+x$ | $\longrightarrow$ | $(1\ 1\ 0)$ |
| $x^{80} = 4+2x+x^2$ | $\longrightarrow$ | $(4\ 2\ 1)$ | $x^{104} = x+x^2$ | $\longrightarrow$ | $(0\ 1\ 1)$ |
| $x^{81} = 3+x+2x^2$ | $\longrightarrow$ | $(3\ 1\ 2)$ | $x^{105} = 3+2x+x^2$ | $\longrightarrow$ | $(3\ 2\ 1)$ |
| $x^{82}= 1+2x+x^2$ | $\longrightarrow$ | $(1\ 2\ 1)$ | $x^{106} = 3+2x^2$ | $\longrightarrow$ | $(3\ 0\ 2)$ |
| $x^{83} = 3+3x+2x^2$ | $\longrightarrow$ | $(3\ 3\ 2)$ | $x^{107}= 1+2x$ | $\longrightarrow$ | $(1\ 2\ 0)$ |
| $x^{84}= 1+2x+3x^2$ | $\longrightarrow$ | $(1\ 2\ 3)$ | $x^{108} = x+2x^2$ | $\longrightarrow$ | $(0\ 1\ 2)$ |
| $x^{85} = 4+2x+2x^2$ | $\longrightarrow$ | $(4\ 2\ 2)$ | $x^{109}= 1+4x+x^2$ | $\longrightarrow$ | $(1\ 4\ 1)$ |
| $x^{86} = 1+3x+2x^2$ | $\longrightarrow$ | $(1\ 3\ 2)$ | $x^{110} = 3+3x+4x^2$ | $\longrightarrow$ | $(3\ 3\ 4)$ |
| $x^{87} = 1+3x^2$ | $\longrightarrow$ | $(1\ 0\ 3)$ | $x^{111} = 2+x+3x^2$ | $\longrightarrow$ | $(2\ 1\ 3)$ |
| $x^{88} = 4+2x$ | $\longrightarrow$ | $(4\ 2\ 0)$ | $x^{112} = 4+3x+x^2$ | $\longrightarrow$ | $(4\ 3\ 1)$ |
| $x^{89}= 4x+2x^2$ | $\longrightarrow$ | $(0\ 4\ 2)$ | $x^{113} = 3+x+3x^2$ | $\longrightarrow$ | $(3\ 1\ 3)$ |
| $x^{90} = 1+4x+4x^2$ | $\longrightarrow$ | $(1\ 4\ 4)$ | $x^{114}= 4+4x+x^2$ | $\longrightarrow$ | $(4\ 4\ 1)$ |
| $x^{91}= 2+4x+4x^2$ | $\longrightarrow$ | $(2\ 4\ 4)$ | $x^{115} = 3+x+4x^2$ | $\longrightarrow$ | $(3\ 1\ 4)$ |
| $x^{92} = 2+4x^2$ | $\longrightarrow$ | $(2\ 0\ 4)$ | $x^{116}= 2+x+x^2$ | $\longrightarrow$ | $(2\ 1\ 1)$ |
| $x^{93} = 2$ | $\longrightarrow$ | $(2\ 0\ 0)$ | $x^{117} = 3+4x+x^2$ | $\longrightarrow$ | $(3\ 4\ 1)$ |
| $x^{94} = 2x$ | $\longrightarrow$ | $(0\ 2\ 0)$ | $x^{118} = 3+4x^2$ | $\longrightarrow$ | $(3\ 0\ 4)$ |
| $x^{95} = 2x^2$ | $\longrightarrow$ | $(0\ 0\ 2)$ | $x^{119} = 2+x$ | $\longrightarrow$ | $(2\ 1\ 0)$ |
| $x^{96}= 1+4x$ | $\longrightarrow$ | $(1\ 4\ 0)$ | $x^{120} = 2x+x^2$ | $\longrightarrow$ | $(0\ 2\ 1)$ |
| $x^{97} = x+4x^2$ | $\longrightarrow$ | $(0\ 1\ 4)$ | $x^{121} = 3+2x+2x^2$ | $\longrightarrow$ | $(3\ 2\ 2)$ |
| $x^{98}= 2+3x+x^2$ | $\longrightarrow$ | $(2\ 3\ 1)$ | $x^{122} = 1+2x+2x^2$ | $\longrightarrow$ | $(1\ 2\ 2)$ |
| $x^{99} = 3+4x+3x^2$ | $\longrightarrow$ | $(3\ 4\ 3)$ | $x^{123}= 1+2x^2$ | $\longrightarrow$ | $(1\ 0\ 2)$ |
| $x^{100}= 4+4x+4x^2$ | $\longrightarrow$ | $(4\ 4\ 4)$ | $x^{124} = x^0$ | $\longrightarrow$ | $(1\ 0\ 0)$ |
| $x^{101} = 2+2x+4x^2$ | $\longrightarrow$ | $(2\ 2\ 4)$ | | | |

Tabela 5.8: Grupo Multiplicativo de $GF(125)$

Seja $f = (0\ 1\ 0) \in GR^*(25,3)$, onde $GR^*(25,3)$ denota o grupo das unidades de $GR(25,3)$. Portanto, $\overline{f} = R_5(f) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 124$ em $\mathbb{F}_{25}$, lembrando que $R_5(f)$ é a redução módulo 5 do elemento $f$. Logo, pelo Teorema 35, temos que $f$ deve gerar um grupo de ordem $nd = 124d$ em $GR^*(25,3)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_{26}$ de $GR^*(27,3)$.

As operações em $GR^*(25,3)$ são realizadas módulo $(x^3 + 3x + 2)$. Logo, $x^3 = -3x - 2$; porém, como os coeficientes de $GR^*(25,3)$ estão em $\mathbb{Z}_{25}$, temos que $x^3 = 22x + 23$. Assim, considerando $(f) = (0\ 1\ 0) = x$, a representação dos elementos do grupo das unidades de $GR(25,3)$ é como mostrado na Tabela B.1 do Apêndice.

Como o número de elementos do grupo das unidades de $GR(25,3)$ é de 620 e, portanto, par, a fatoração do termo $x^{620} - 1$ não é única. Neste caso, deve-se buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta = \alpha^4$, obtém-se um grupo multiplicativo com 155 elementos, como desejado. Consequentemente, a fatoração do termo $x^{155} - 1$ é única. Note que poderíamos ter escolhido $\beta = \alpha^{20}$ e $\beta = \alpha^{124}$ conduzindo a grupos multiplicativos com ordens 31 e 5, respectivamente.

Em resumo, por meio dos resultados obtidos nos Capítulos 4 e 5 podemos afirmar que:

| | Cardinalidade do Grupo das Unidades |
|---|---|
| $GR(4,2)$ | 3 |
| $GR(8,2)$ | 3 |
| $GR(16,2)$ | 3 |
| $GR(9,2)$ | 24 |
| $GR(27,2)$ | 72 |
| $GR(25,2)$ | 120 |

Tabela 5.9: Cardinalidade do Grupo das Unidades

| | Cardinalidade do Grupo das Unidades |
|---|---|
| $GR(4,3)$ | 14 |
| $GR(8,3)$ | 28 |
| $GR(16,3)$ | 56 |
| $GR(9,3)$ | 78 |
| $GR(27,3)$ | 234 |
| $GR(25,3)$ | 620 |

Tabela 5.10: Cardinalidade do Grupo das Unidades

Analisando as tabelas observamos que:

- Os anéis de base 2 com grau 2 suas cardinalidades são iguais;
- Os anéis de base 3 com grau 2 a cardinalidade do sucessor é o triplo do antecessor;
- Os anéis de base 2 com grau 3 a cardinalidade do sucessor é o dobro do antecessor;
- Os anéis de base 3 com grau 3 a cardinalidade do sucessor é o triplo do antecessor;
- Utilizando anéis com cardinalidade pequenas, através da extensão podemos conseguir valores de $n$ grandes.

## 5.2 Construção de Geradores de Seqüências através de Polinômios Geradores

O objetivo desta seção é apresentar uma aplicação que é a síntese de circuitos lineares de deslocamentos com realimentação, ou seja, LFSR, que geram uma dada seqüência finita de dígitos pertencentes a um corpo finito $\mathbb{F}$. Consequentemente, através da aplicação estendida em [3] para o caso de anéis locais da forma $\mathbb{Z}_{p^m}$, veremos, na Subseção 5.2.2, uma extensão deste mesmo problema para o caso em que a seqüência pertence a um anel comutativo finito local com identidade.

### 5.2.1 Circuitos lineares com seqüências pertencentes a um corpo finito

Um LFSR de comprimento $L$, mostrado na Figura 5.1, consiste de uma cascata de $L$ atrasadores (registros de deslocamento) e alguns multiplicadores e somadores capazes de gerar uma combinação linear dos conteúdos destes registros.

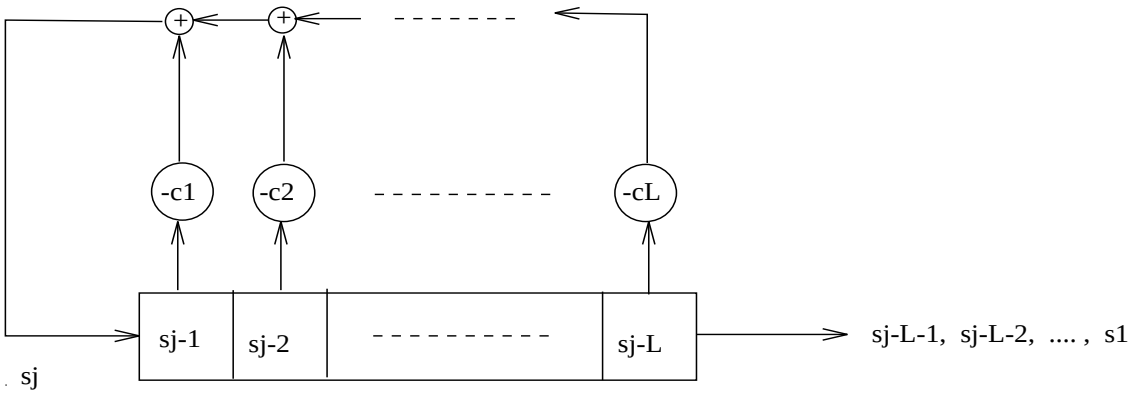


Figura 5.1: LFSR de comprimento $L$.

A saída do LFSR é o conteúdo do último registro. Os conteúdos iniciais $s_0, s_1, s_2, \ldots, s_{L-1}$ dos $L$ atrasadores coincidem com os $L$ primeiros dígitos de saída e os dígitos seguintes de saída são determinados através da relação de recorrência

$$s_j = -\sum_{i=1}^{L} c_i \cdot s_{j-i}, \tag{5.17}$$

para $j = L+1,\ L+2, \ldots$ . Os dígitos de saída e os **coeficientes de realimentação** $c_1, c_2, \ldots, c_L$ pertencem ao mesmo anel $R$. Quando $c_L = 0$, dizemos que o LFSR é **singular**.

Diz-se que um LFSR gera uma seqüência finita de dígitos $s_1, s_2, \ldots, s_N$ quando esta seqüência coincide com os $N$ primeiros dígitos de saída do mesmo, para algum conteúdo inicial. Se $L \geq N$, o LFSR sempre gera a seqüência, e se $L < N$, o LFSR gera a seqüência se, e somente se,

$$s_j + s_{j-1} \cdot c_1 + \ldots + s_{j-L+1} \cdot c_{L-1} + s_{j-L} \cdot c_L = 0, \tag{5.18}$$

para $L+1 \leq j \leq N$. Assim, é óbvio que qualquer LFSR de comprimento $L \geq N$ gera uma seqüência de comprimento $N$. Entretanto, o objetivo maior é encontrar aquele(s) LFSR(s) de mínimo comprimento possível que é (são) capaz(es) de gerar uma dada seqüência de comprimento $N$.

Quando comparamos o sistema linear

$$S_{j+\nu} + S_{j+\nu-1}\sigma_1 + \ldots + S_{j+1}\sigma_{\nu-1} + S_j\sigma_\nu = 0, \tag{5.19}$$

[15] página 96, sobre a decodificação dos códigos BCH, com (5.18), temos que em ambos os casos o objetivo comum é encontrar a menor quantidade de variáveis $(\nu, L)$ que satisfaçam os respectivos conjuntos de equações. Portanto, as equações de (5.18) podem também ser resolvidas pelo algoritmo de Berlekamp-Massey. Neste caso, as entradas para o mesmo deverão ser os elementos $s_1, s_2, \ldots, s_N$ que formam a seqüência dada (a qual se deseja gerar). O algoritmo produz então como saída um polinômio

$$C(X) = 1 + c_1X + \ldots + c_LX^L \tag{5.20}$$

na indeterminada $X$, cujos coeficientes de realimentação do(s) LFSR(s) minimal (minimais) de comprimento $L$ que gera(m) $s_1, s_2, \ldots, s_N$.

**Teorema 40.** *[15] Se um LFSR de comprimento L gera uma seqüência de dígitos* $\{s_1, s_2, \ldots, s_{N-1}\}$, *mas não a seqüência* $\{s_1, s_2, \ldots, s_{N-1}, s_N\}$, *então qualquer LFSR que gera a última seqüência tem comprimento* $L^{'}$ *satisfazendo*

$$L^{'} \geq N + 1 - L. \tag{5.21}$$

Seja $\underline{s} = \{s_1, s_2, \ldots, s_K\}$ uma seqüência finita de dígitos. Definindo $L_N(\underline{s})$ como sendo o mínimo dos comprimentos de todos os LFSR's que geram $\{s_1, s_2, \ldots, s_K\},\ N < K$, temos então do Teorema 40 que

$$L_{N+1}(\underline{s}) \geq \max\{L_{N+1}(\underline{s}), N + 1 - L_N(\underline{s})\}. \tag{5.22}$$

Mais ainda, é possível de se mostrar que

$$L_{N+1}(\underline{s}) = \max\{L_{N+1}(\underline{s}), N + 1 - L_N(\underline{s})\}. \tag{5.23}$$

Assim sendo, quando algum LSFR de comprimento $L_N(\underline{s})$ gera $\{s_1, s_2, \ldots, s_N\}$, mas não gera $\{s_1, s_2, \ldots, s_N, s_{N+1}\}$, isto é, $d_N \neq 0$, então ocorre uma mudança de comprimento (do passo $N$ para o passo $N+1$) se, e somente se, $2L_N(\underline{s}) \leq N$. E, portanto, a conclusão é a de que o LFSR de comprimento mínimo que gera $\underline{s} = \{s_1, s_2, \ldots, s_K\}$ é único se, e somente se, $2L_K(\underline{s}) \leq K$.

### 5.2.2 Circuitos lineares com seqüências pertencentes a um anel comutativo finito local com identidade.

Um circuito linear de deslocamento ou LFSR de comprimento $L$, mostrado na Figura 5.2, consiste de uma cascata de $L$ atrasadores (registros de deslocamento) e alguns multiplicadores e somadores capazes de gerar uma combinação linear dos conteúdos destes registros.

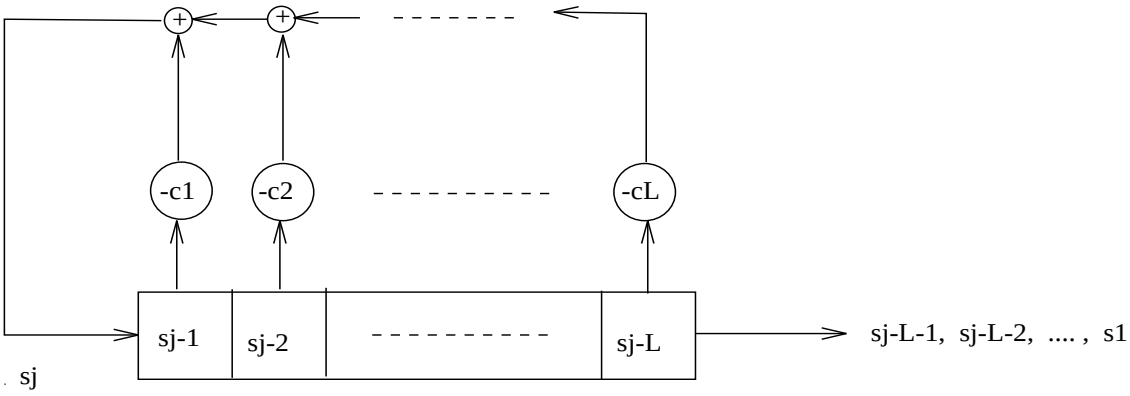


Figura 5.2: LFSR de comprimento L.

A saída do LFSR é o conteúdo do último registro. Os conteúdos iniciais $s_1, s_2, \ldots, s_L$ dos $L$ atrasadores coincidem com os $L$ primeiros dígitos de saída, e os dígitos subsequentes da saída são determinados através da relação de recorrência

$$s_j = -\sum_{i=1}^{L} c_i \cdot s_{j-i}, \tag{5.24}$$

para $j = L+1,\ L+2, \ldots$ . Os dígitos de saída e os **coeficientes de realimentação** $c_1, c_2, \ldots, c_L$ pertencem ao mesmo anel $R$. Quando $c_L = 0$, dizemos que o LFSR é **singular**.

Um LFSR **gera** uma seqüência finita de dígitos $s_1, s_2, \ldots, s_N$ quando esta seqüência coincide com os $N$ primeiros dígitos de saída do mesmo, para algum conteúdo inicial. Se $L \geq N$, o LFSR sempre gera a seqüência e se $L < N$, o LSFR gera a seqüência se, e somente se,

$$s_j + s_{j-1} \cdot c_1 + \ldots + s_{j-L+1} \cdot c_{L-1} + s_{j-L} \cdot c_L = 0, \tag{5.25}$$

para $L + 1 \leq j \leq N$.

Em [15] foi mostrado que o algoritmo usado para a decodificação de códigos BCH também pode ser usado para sintetizar um LFSR de comprimento mínimo $L$ que gera uma seqüência prescrita. Isto é, o problema de geração de um LFSR e a decodificação de um código BCH são equivalentes.

De uma maneira bem semelhante, o algoritmo pode ser aplicado para sintetizar um LFSR de comprimento mínimo que gera uma seqüência $s_1, s_2, \ldots, s_N$ de elementos do anel $R$, em [3] isto foi mostrado para o anel $\mathbb{Z}_{p^m}$.

Deste modo, temos que as entradas do algoritmo serão os elementos $s_1, s_2, \ldots, s_N$ que formam a seqüência dada e a saída do mesmo será o polinômio $c(x) = 1 + c_1 x + \ldots + c_L x^L$ na variável $x$, onde os coeficientes são os coeficientes de realimentação do LFSR mínimo de comprimento $L$ que gera $s_1, s_2, \ldots, s_N$. Este LFSR mínimo será único se, e somente se, $2L \leq N$ e em cada estágio do algoritmo a equação linear $d_n - y d_m = 0$ na variável $y$ tiver solução única, onde $d_n$ e $d_m$ são as $n$-ésima e $m$-ésima discrepâncias, respectivamente. Caso contrário, haverá mais de um LFSR mínimo de comprimento $L$ que gera $s_1, s_2, \ldots, s_N$.

**Exemplo 8.** *Encontrar o LFSR minimal que gere a seqüência* $s_1 = 6, s_2 = 3, s_3 = 1, s_4 = 5,$ *e* $s_5 = 6$ *sobre o anel* $\mathbb{Z}_9$. *Aplicando o algoritmo de Berlekamp Massey modificado, encontramos:*

| n | $\sigma^n(X)$ | $d_n$ | $l_n$ | $n - l_n$ |
|---|---|---|---|---|
| -1 | 1 | 1 | 0 | -1 |
| 0 | 1 | 6 | 0 | 0 |
| 1 | 1 + 3X | 3 | 1 | 0 |
| 2 | 1 + 7X | 4 | 1 | 1 |
| 3 | $1 + 7X + 5X^3$ | 6 | 3 | 0 |
| 4 | $1 + X + 3X^2 + 5X^3$ | 2 | 3 | 1 |
| 5 | $1 + X + 7X^2 + 6X^3$ | - | 3 | 2 |

*Portanto,* $C(X) = 1 + X + 7X^2 + 6X^3$ *e o LFSR minimal (veja Figura 5.3) que gera a seqüência dada tem as suas saídas relacionadas através de:*

$$s_n + s_{n-1} + 7 \cdot s_{n-2} + 6 \cdot s_{n-3} = 0 \quad (mod\ 9), \quad n \geq 4.$$

*Logo, o objetivo é gerar a seqüência* $S = (6,\ 3,\ 1,\ 5,\ 6)$.

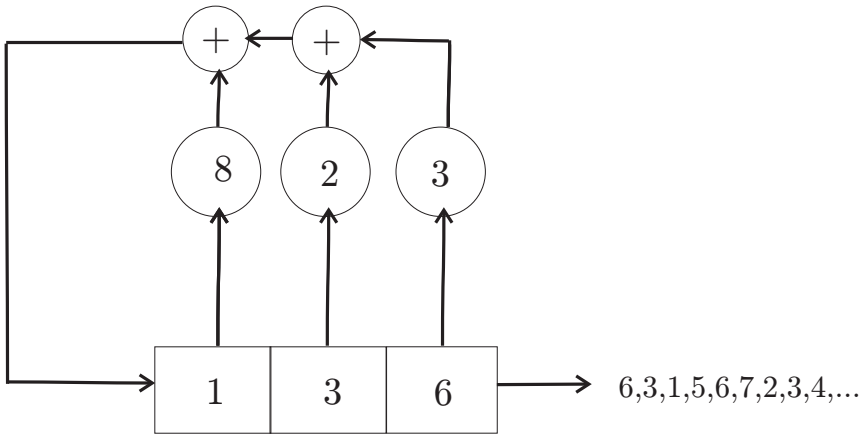


Figura 5.3: Gerador da seqüência S= (6, 3, 1, 5, 6), complexidade linear=3

## 5.3 Transformada Discreta de Fourier

Seja $\{x_n\}$ uma seqüência cujo período é de $N$ amostras, isto é,

$$x(n) = x(n+N). \tag{5.26}$$

Então o $k-$ésimo coeficiente de Fourier $\theta(k)$ é dado por

$$\theta(k) = \sum_{n=0}^{N-1} x(n)\exp\left(-j\frac{2k\pi n}{N}\right),\ k = 0, 1, 2, \ldots, N-1, \tag{5.27}$$

onde $j = \sqrt{-1}$ e a transformada inversa é dada por

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} \theta(k)\exp\left(j\frac{2k\pi n}{N}\right),\ n = 0, 1, 2, \ldots, N-1. \tag{5.28}$$

Note que $|\theta(k)|$ fornece o **espectro de amplitude**, $|\theta(k)|^2$ fornece o **espectro de energia** e $tan^{-1}\left[\frac{Im\{\theta(k)\}}{Re\{\theta(k)\}}\right]$ fornece o **espectro de fase**. Note também que $\theta(k)$ fornece $N$ linhas espectrais periódicas com relação às amostras $\{x(n)\}$.

Uma transformada mais geral, pode ser escrita como

$$\theta(k) = \sum_{n=0}^{N-1} x(n)a(k,n),\ k = 0, 1, 2, \ldots, N-1, \tag{5.29}$$

onde $a(k,n)$ denota o **núcleo da transformada geral**.

De (5.27) notamos que o núcleo $a(k,n)$ é dado por

$$a(k,n) = \exp\left\{-j\frac{2k\pi n}{N}\right\}, \quad k = 0, 1, 2, \ldots, N-1. \tag{5.30}$$

Note que o termo

$$\varepsilon = \exp\left\{-j\frac{2k\pi n}{N}\right\}, \tag{5.31}$$

é um elemento primitivo e uma das $N$ raízes da unidade, isto é, $\varepsilon^N - 1 = 0$. Equivalentemente, $\varepsilon^N = 1$, mas com $\varepsilon^k \neq 1$ para $1 \leq k \leq N$. Com isso, vemos que $\varepsilon = \exp\{-j2\pi n/N\}$ pertence ao corpo dos números complexos.

Como exemplo de um corpo finito, considere o $\mathbb{F}_7$, corpo dos inteiros módulo 7. Seja $\varepsilon = 2$, então $\varepsilon^2 = 4$ e $\varepsilon^3 = 1$, o que implica que $N = 3$, isto é, 2 é a raiz cúbica da unidade, isto é, $\varepsilon^3 = 1$.

Note que os zeros de $x^N - 1$ são dados por $\varepsilon^i$, $0 \leq i \leq N-1$, pois para um $\varepsilon^i$ temos

$$(\varepsilon^i)^N - 1 = (\varepsilon^N)^i - 1 = (1)^i - 1 = 0. \tag{5.32}$$

Logo, $\varepsilon^i$ é um zero de $x^N - 1$. Isto implica que

$$x^N - 1 = (x-1)(x-\varepsilon)(x-\varepsilon^2)\ldots(x-\varepsilon^{N-1}). \tag{5.33}$$

A transformada discreta de Fourier de comprimento $N$ gerada por $\varepsilon$ sobre um corpo $\mathbb{F}$ é o mapeamento

$$TFD_\varepsilon(.) : \mathbb{F}^N \longrightarrow \mathbb{F}^N. \tag{5.34}$$

Sejam $\mathbf{b} = (b(0), b(1), \ldots, b(N-1))$ e $\mathbf{B} = (B(0), B(1), \ldots, B(N-1))$. Então, $\mathbf{B}$ denota a transformada discreta de Fourier de $\mathbf{b}$, isto é, $\mathbf{B} = TFD_\varepsilon(\mathbf{b})$. Com isso, $\mathbf{b}$ representa a seqüência no domínio do tempo e $\mathbf{B}$ a seqüência no domínio da freqüência,

$$B(i) = \sum_{n=0}^{N-1} b(n)\varepsilon^{in}, \tag{5.35}$$

$$b(n) = \frac{1}{N}\sum_{i=0}^{N-1} B(i)\varepsilon^{-in}. \tag{5.36}$$

Agora, iremos identificar $\mathbf{b} = (b(0), b(1), \ldots, b(N-1)) = (b_0, b_1, \ldots, b_{N-1})$ com o polinômio

$$b(x) = b_0 + b_1 x + \ldots + b_{N-1}x^{N-1}. \tag{5.37}$$

Com isso, a equação da transformada discreta de Fourier pode ser escrita como

$$B(i) = b(\varepsilon^i), \quad i = 0, 1, 2, \ldots, N-1. \tag{5.38}$$

Como exemplo, considere o vetor $\mathbf{b} = (1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1)$, como a seqüência no domínio do tempo. A Figura 5.4 ilustra este "sinal."

Através da equação (5.35) notamos que B(0)=10 e B(i)=0, para i=1,2,...,9. Dessa forma, a transformada discreta de Fourier é como mostrada na Figura 5.5.

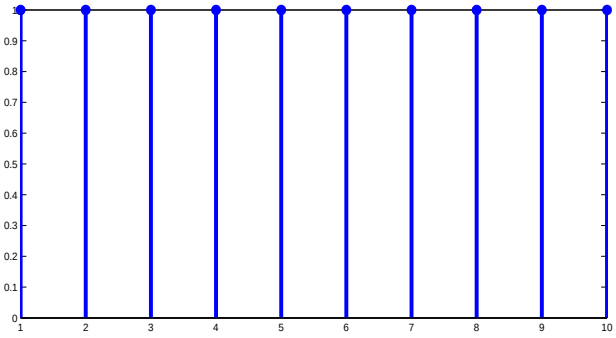


Figura 5.4: Domínio do Tempo (**b**)

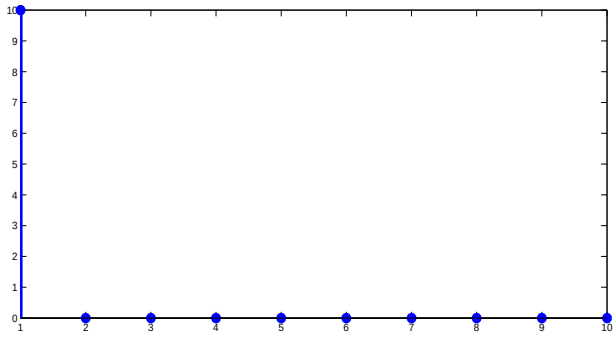


Figura 5.5: Domínio da Freqüência (**B**)

**Exemplo 9.** *Considere* $\varepsilon = 2$ *em* $\mathbb{F}_7$ *tal que* $N = 3$. *Se* $\boldsymbol{b} = (0, 0, 3)$ *então* $b(x) = 3x^2$ *tal que*

$$B_0 = b(\varepsilon^0) = b(1) = 3 \cdot 1 = 3$$

$$B_1 = b(\varepsilon^1) = b(2) = 3 \cdot 4 = 5$$

$$B_2 = b(\varepsilon^2) = b(4) = 3 \cdot 2 = 6$$

*Assim,* $\boldsymbol{B} = (3, 5, 6)$.

As Figuras 5.6 e 5.7 mostram **b** e **B**.

Um código cíclico de comprimento $N$ sobre o corpo finito $\mathbb{F}$, com polinômio gerador $g(x)$, onde $g(x)$ divide $x^N - 1$, é o conjunto de todas as palavras-código **b** tal que $g(x)$ divide $b(x)$.

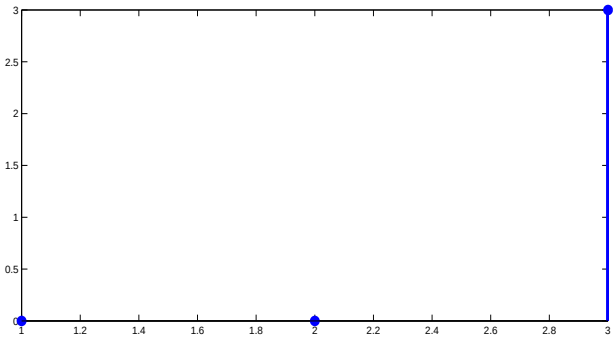


Figura 5.6: Domínio do Tempo (**b**)

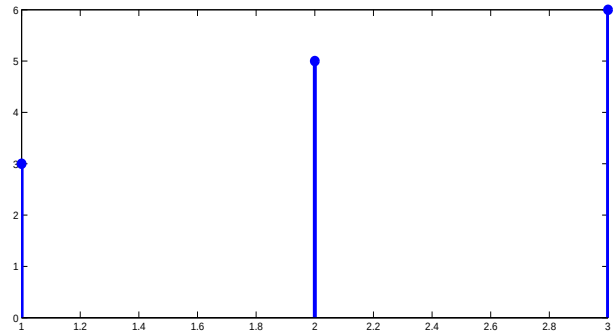


Figura 5.7: Domínio da Freqüência (**B**)

Por outro lado, os zeros de $x^N - 1$ são todos os $\varepsilon^i$ para os quais $0 \leq i \leq N-1$. Assim, $g(x)$ é unicamente caracterizado pelos $i$'s para os quais $\varepsilon^i$ é um zero, digamos $i \in I$, de $g(x)$. Isto implica que $\mathbf{b}$ é uma palavra-código se, e somente se, $B_i = 0$ para $i \in I$.

A complexidade linear de uma seqüência $s_0, s_1, s_2, \ldots, s_{n-1}$ (onde $n$ pode ser infinito) é o menor registro de deslocamento com realimentação linear que quando "carregado" inicialmente com $s_0, s_1, s_2, \ldots, s_{L-1}$ produz a seqüência toda como saída. A Figura 5.2 ilustra um registro de deslocamento com realimentação linear.

**Teorema 41.** *[2] Se $\boldsymbol{B} = TFD_\varepsilon(\boldsymbol{b})$ é a transformada discreta em qualquer corpo $\mathbb{F}$, então o peso de Hamming de $\boldsymbol{b}$ é igual à complexidade linear da seqüência (repetida) periódica $\boldsymbol{B}, \boldsymbol{B}, \ldots, \boldsymbol{B}$.*

A Figura 5.8 ilustra o registro de deslocamento com realimentação linear com $\mathbf{B} = (3, 5, 6)$ em $\mathbb{F}_7$, tal que a complexidade linear vale 1.

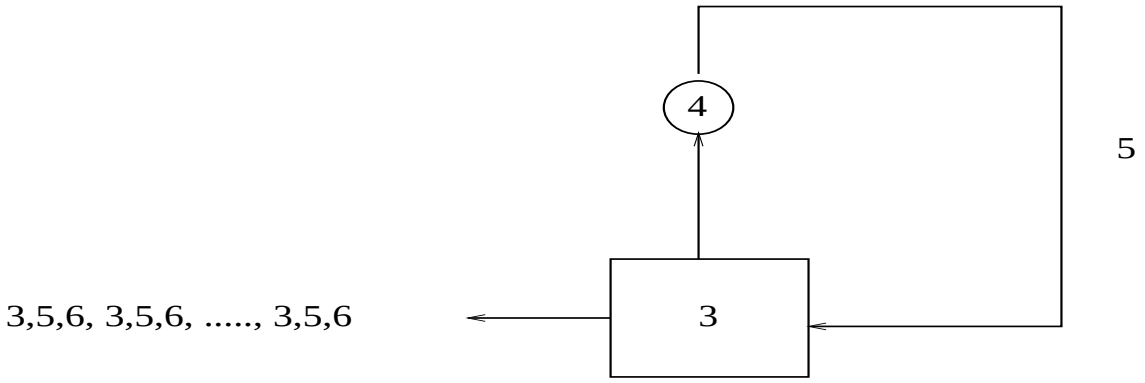


Figura 5.8: LFSR de comprimento 1.

Toda seqüência corrida com $d-1$ zeros consecutivos seguida de um dígito não nulo tem complexidade linear pelo menos $d$.

Note que $g(x)$ tem $d-1$ potências consecutivas de $\varepsilon$ com zero, digamos $\varepsilon^i$ para $i = 0, 1, 2, \ldots, d-1$. Com isso, $B_1 = B_2 = \ldots = B_{d-1} = 0$ para toda palavra-código $\mathbf{b}$. Todavia, toda palavra-código de um código cíclico tem peso de Hamming pelo menos $d$. Com isso, $d_{min} \geq d$, o limitante inferior da distância de projeto do código cíclico BCH.

Iremos agora estabelecer as condições sob as quais a transformada discreta de Fourier e sua inversa podem ser aplicadas às seqüências cujas componentes estão em um anel comutativo $R$ ao invés de estarem em um corpo.

Iremos denotar a $N-$ésima raiz primitiva da unidade por $\varepsilon$ em $R$. Como vimos no Capítulo 2 o anel dos inteiros módulo $m$, $\mathbb{Z}_m$, é um anel comutativo. Este anel é o mais importante dos anéis com interesses em teoria da codificação e criptografia.

Quando $m$ é um número primo, $\mathbb{Z}_m$ é isomorfo ao corpo de Galois $\mathbb{F}_m$. Com isso, o caso de interesse será quando $m$ for composto.

A equação da transformada discreta de Fourier pode ser escrita como

$$\mathbf{B} = M_\varepsilon \mathbf{b}, \tag{5.39}$$

onde $M_\varepsilon$ é uma matriz $N \times N$ dada por

$$M_\varepsilon = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & (\varepsilon) & (\varepsilon^2) & \cdots & (\varepsilon^{N-1}) \\ 1 & (\varepsilon)^2 & (\varepsilon^2)^2 & \cdots & (\varepsilon^{N-1})^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\varepsilon)^{N-1} & (\varepsilon^2)^{N-1} & \cdots & (\varepsilon^{N-1})^{N-1} \end{bmatrix}. \tag{5.40}$$

Como $M_\varepsilon$ é uma matriz do tipo Vandermonde, então o determinante vale

$$\Delta(M_\varepsilon) = \prod_{j=1}^{N-1}\prod_{i=1}^{j-1}(\varepsilon^j - \varepsilon^i) = \prod_{j=1}^{N-1}\prod_{i=1}^{j-1}\varepsilon^i(\varepsilon^{j-i} - 1). \tag{5.41}$$

Mas o produto de elementos em um anel é uma **unidade** se, e somente se, cada elemento é uma unidade. Note que $\varepsilon$ é sempre uma unidade pois $\varepsilon^{N-1} = 1$. Disto segue que $\Delta(M_\varepsilon)$ é uma unidade se, e somente se, $\varepsilon^k - 1$ é uma unidade para $1 \leq k \leq N$.

**Teorema 42.** *[15] Se $\varepsilon$ é uma $N-$ésima raiz primitiva da unidade em um anel comutativo $R$, então $\mathbf{B} = M_\varepsilon \mathbf{b}$ define um mapeamento inversível de $R^N$ em $R^N$ cujo mapeamento inverso é dado pela inversa da transformada discreta de Fourier usual se, e somente se, $\varepsilon^k - 1$ é uma unidade para $1 \leq k \leq N$.*

Um elemento $i$ de $\mathbb{Z}_m$ é uma unidade se, e somente se, $\text{mdc}(i, m) = 1$.

**Observação 4.** *Não existe a transformada discreta de Fourier em $\mathbb{Z}_m$ para qualquer $m \geq 2$ quando $m$ é composto e par. As razões para este resultado são:*

1. *Porque $\varepsilon$ deve ser uma unidade e, portanto ímpar. Com isso, $\varepsilon - 1$ é par, logo não é uma unidade;*

2. *Para todo número composto ímpar mod $m$, $\varepsilon = m - 1$ é uma segunda raiz primitiva da unidade e gera uma transformada discreta de Fourier de comprimento $N = 2$ em $\mathbb{Z}_m$, pois $\varepsilon - 1 = m - 2$ e $mdc(m, m-2) = mdc(m, 2) = 1$ tal que $\varepsilon - 1$ é uma unidade.*

**Exemplo 10.** *Seja $\varepsilon = 2$ uma raiz quadrada primitiva da unidade em $\mathbb{Z}_{15}$, porém não gera uma transformada discreta de Fourier de comprimento $N = 4$ neste anel, embora $\varepsilon - 1 = 1$ seja uma unidade. Isto se deve ao fato de que $\varepsilon^2 - 1 = 3$ não é uma unidade em $\mathbb{Z}_{15}$.*

Neste ponto, faremos a seguinte pergunta: Pode-se encontrar uma transformada discreta de Fourier de comprimento $N > 2$ em qualquer anel $\mathbb{Z}_m$, para um $m$ composto? A resposta é *sim.*

**Exemplo 11.** *Seja* $\varepsilon = 8$ *uma raiz quarta primitiva da unidade em* $\mathbb{Z}_{65}$ *que gera uma transformada discreta de Fourier com comprimento* $N = 4$, *pois* $\varepsilon - 1 = 7$, $\varepsilon^2 - 1 = 63$ *e* $\varepsilon^3 - 1 = 56$ *são unidades em* $\mathbb{Z}_{65}$.

Existem valores de $m$ para os quais $\mathbb{Z}_m$ pode ser considerado de interesse prático? A seguir apresentamos na Tabela 5.3 alguns valores de $m$ ($\mathbb{Z}_m$) para os quais existem a transformada discreta de Fourier.

| m | N |
|---|---|
| 91 | 2, 3, 6 |
| 169 | 2, 3, 4, 6, 12 |
| 121 | 2, 5, 10 |
| 217 | 2, 3, 6 |

Tabela 5.11: Valores de $m$ para os quais existem as correspondentes transformada discreta de Fourier

**Teorema 43.** *[15] Se* $p$ *é um primo (ímpar) e* $\alpha$ *é um elemento primitivo de* $\mathbb{F}_p$, *então com* $\alpha$ *considerado como um elemento de* $\mathbb{Z}_{p^n}$, *para qualquer* $n \geq 2$, $\varepsilon = \alpha^{p^{n-1}}$ *gera uma transformada discreta de Fourier com comprimento* $N = p - 1$ *em* $\mathbb{Z}_{p^n}$.

**Exemplo 12.**

1. *Transformada discreta de Fourier com* $N = 256$ *em* $\mathbb{Z}_{257}$ *tem componentes limitadas a resolução de* 8 *bits;*

2. *Transformada discreta de Fourier com* $N = 256$ *em* $\mathbb{Z}_{257^2}$ *tem componentes limitadas a resolução de* 16 *bits;*

3. *Transformada discreta de Fourier com* $N = 256$ *em* $\mathbb{Z}_{257^3}$ *tem componentes limitadas a resolução de* 24 *bits.*

Agora iremos apresentar um exemplo onde faremos uso do elemento primitivo do grupo multiplicativo de um determinado corpo no processo de geração da transformada discreta de Fourier com o maior comprimento possível, porém sobre o anel $\mathbb{Z}_{p^2}$, com $p$ primo, vide Teorema 43.

Considere o corpo algébrico de Galois com 11 elementos, isto é, $GF(11)$. Seja $\alpha$ o elemento primitivo deste corpo. Então $\alpha$ será considerado um elemento de $\mathbb{Z}_{11^2} = \mathbb{Z}_{121}$. Note que $\varepsilon = \alpha^{11}$ gera um vetor com o maior comprimento possível, isto é, equivalente a dizer que $\varepsilon = \alpha^{11}$ gera uma transformada discreta de Fourier com o maior comprimento possível. Com isso, é possível determinar a matriz $M_\varepsilon$ tal que

$$\mathbf{B} = M_\varepsilon \mathbf{b},$$

onde $\mathbf{B} = (B(0), B(1), \ldots, B(N-1))$ ("domínio da freqüência"), $\mathbf{b} = (b(0), b(1), \ldots, b(N-1))$("domínio do tempo").

$$M_\varepsilon = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & (\varepsilon) & (\varepsilon^2) & \cdots & (\varepsilon^{N-1}) \\ 1 & (\varepsilon)^2 & (\varepsilon^2)^2 & \cdots & (\varepsilon^{N-1})^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\varepsilon)^{N-1} & (\varepsilon^2)^{N-1} & \cdots & (\varepsilon^{N-1})^{N-1} \end{bmatrix}. \tag{5.42}$$

O circuito linear de deslocamento com realimentação (LFSR) que gera a seqüência com o maior comprimento possível é facilmente obtida uma vez que tenhamos o conhecimento do polinômio gerador do código cíclico associado.

De modo a explicitar os procedimentos, considere o corpo de Galois $GF(11)$ dado por

$$GF(11) = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}. \tag{5.43}$$

Tomemos o elemento primitivo $\alpha = 2$ do grupo multiplicativo de $GF(11)$. Este elemento gera todos os elementos não nulos de $GF(11)$, isto é,

Como $\alpha = 2$ é primitivo em $\mathbb{Z}_{11}$, então $\alpha$ também é primitivo em $\mathbb{Z}_{11^2} = \mathbb{Z}_{121}$.

| | |
|---|---|
| $\alpha = 2$ | $\alpha^7 = 7$ |
| $\alpha^2 = 4$ | $\alpha^8 = 3$ |
| $\alpha^3 = 8$ | $\alpha^9 = 6$ |
| $\alpha^4 = 5$ | $\alpha^{10} = 1$ |
| $\alpha^5 = 10$ | $\alpha^{11} = \alpha$ |
| $\alpha^6 = 9$ | |

Tabela 5.12: Elementos do corpo $GF(11)$ gerados por $\alpha = 2$

Consideremos agora, $\varepsilon = \alpha^{11} = 112$ em $\mathbb{Z}_{121}$, a Tabela 5.3 apresenta os elementos do grupo das unidades de $\mathbb{Z}_{121}$, gerados por $\alpha^{11}$.

| |
|---|
| $\varepsilon = \alpha^{11} = 112$ |
| $\varepsilon^2 = (\alpha^{11})^2 = 81$ |
| $\varepsilon^3 = (\alpha^{11})^3 = 118$ |
| $\varepsilon^4 = (\alpha^{11})^4 = 27$ |
| $\varepsilon^5 = (\alpha^{11})^5 = 120$ |
| $\varepsilon^6 = (\alpha^{11})^6 = 9$ |
| $\varepsilon^7 = (\alpha^{11})^7 = 40$ |
| $\varepsilon^8 = (\alpha^{11})^8 = 3$ |
| $\varepsilon^9 = (\alpha^{11})^9 = 94$ |
| $\varepsilon^{10} = (\alpha^{11})^{10} = 1$ |

Tabela 5.13: Elementos do grupo das unidades de $\mathbb{Z}_{121}$

Utilizando o Teorema 43, temos que $\varepsilon = \alpha^{11}$, com $\alpha = 2$, gera uma transformada discreta de Fourier de comprimento $N = 10$ em $\mathbb{Z}_{121}$.

Assim, a matriz $M_\varepsilon$ equação (5.42) com $\varepsilon = 2^{11} = 112$, é dada por

$$M_\varepsilon = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 112 & 81 & 118 & 27 & 120 & 9 & 40 & 3 & 94 \\ 1 & 81 & 27 & 9 & 3 & 1 & 81 & 27 & 9 & 3 \\ 1 & 118 & 9 & 94 & 81 & 120 & 3 & 112 & 27 & 40 \\ 1 & 27 & 3 & 81 & 9 & 1 & 27 & 3 & 81 & 9 \\ 1 & 120 & 1 & 120 & 1 & 120 & 1 & 120 & 1 & 120 \\ 1 & 9 & 81 & 3 & 27 & 1 & 9 & 81 & 3 & 27 \\ 1 & 40 & 27 & 112 & 3 & 120 & 81 & 94 & 9 & 118 \\ 1 & 3 & 9 & 27 & 81 & 1 & 3 & 9 & 27 & 81 \\ 1 & 94 & 3 & 40 & 9 & 120 & 27 & 118 & 81 & 112 \end{bmatrix}. \tag{5.44}$$

Como esta matriz é uma matriz de Vandermonde, seu determinante pode ser calculado da seguinte forma

$$\det(M_\varepsilon) = \prod_{j=1}^{N-1}(\varepsilon^j - \varepsilon^i) = \prod_{j=1}^{9}\prod_{i=1}^{j}(\varepsilon^j - \varepsilon^i) \tag{5.45}$$

$\det(M_\varepsilon) = (\varepsilon^9-\varepsilon^8)\cdot(\varepsilon^9-\varepsilon^7)\cdot(\varepsilon^9-\varepsilon^6)\cdot(\varepsilon^9-\varepsilon^5)\cdot(\varepsilon^9-\varepsilon^4)\cdot(\varepsilon^9-\varepsilon^3)(\varepsilon^9-\varepsilon^2)\cdot(\varepsilon^9-\varepsilon)\cdot(\varepsilon^8-\varepsilon^7)\cdot(\varepsilon^8-\varepsilon^6)\cdot(\varepsilon^8-\varepsilon^5)\cdot(\varepsilon^8-\varepsilon^4)\cdot(\varepsilon^8-\varepsilon^3)\cdot(\varepsilon^8-\varepsilon^2)(\varepsilon^8-\varepsilon)\cdot(\varepsilon^7-\varepsilon^6)\cdot(\varepsilon^7-\varepsilon^5)\cdot(\varepsilon^7-\varepsilon^4)\cdot(\varepsilon^7-\varepsilon^3)\cdot(\varepsilon^7-\varepsilon^2)\cdot(\varepsilon^7-\varepsilon)\cdot(\varepsilon^6-\varepsilon^5)\cdot(\varepsilon^6-\varepsilon^4)\cdot(\varepsilon^6-\varepsilon^3)\cdot(\varepsilon^6-\varepsilon^2)\cdot(\varepsilon^6-\varepsilon)\cdot(\varepsilon^5-\varepsilon^4)\cdot(\varepsilon^5-\varepsilon^3)\cdot(\varepsilon^5-\varepsilon^2)\cdot(\varepsilon^5-\varepsilon)\cdot(\varepsilon^4-\varepsilon^3)\cdot(\varepsilon^4-\varepsilon^2)\cdot(\varepsilon^4-\varepsilon)\cdot(\varepsilon^3-\varepsilon^2)\cdot(\varepsilon^3-\varepsilon)\cdot(\varepsilon^2-\varepsilon).$

$\det(M_\varepsilon) = 91\cdot 54\cdot 85\cdot(-26)\cdot 67\cdot(-24)\cdot 13\cdot(-18)\cdot(-37)\cdot(-6)\cdot(-117)\cdot(-24)(-115)\cdot(-78)\cdot(-109)\cdot 31\cdot(-80)\cdot 13\cdot(-78)\cdot(-41)\cdot(-72)\cdot(-111)\cdot(-18)\cdot(-109)\cdot(-72)\cdot(-103)\cdot 93\cdot 2\cdot 39\cdot 8\cdot(-91)\cdot(-54)\cdot(-85)\cdot 37\cdot 6\cdot(-31) = 78.$

Portanto, como o determinante de $M_\varepsilon \neq 0$, concluímos que a matriz $M_\varepsilon$ é invertível, e isto implica que $M_\varepsilon^{-1}$ realiza a transformada inversa discreta de Fourier.

Como $M_\varepsilon$ é uma matriz simétrica e hermitiana a sua inversa, $M_\varepsilon^{-1}$, é ela mesma.

Por fim, chamamos a atenção ao fato de que se $2^{11}$ é a raiz décima da unidade, então $2^{22}$ é a raiz quinta da unidade e $2^{55}$ é a raiz quadrada da unidade.

Com base no procedimento de decodificação dos códigos Reed-Solomon e BCH, [3], sobre anéis de inteiros residuais $\mathbb{Z}_{p^m}$, para $p$ um primo e $m$ um inteiro maior ou igual a 1, iremos considerar um exemplo que ilustra a aplicação do procedimento de decodificação dos códigos Reed-Solomon e BCH, respectivamente, para a geração do circuito LFSR que realiza a geração de seqüências.

No exemplo a seguir, iremos mostrar que através do segundo passo do algoritmo de Berlekamp-Massey obtemos o polinômio que será utilizado no processo de realimentação e com isso gerar seqüência prescrita.

**Exemplo 13.** *Considere o código do Exemplo 4.6.1, Seção 4.6. Recordando os seus parâmetros temos que* $q = 49$ *(o código é sobre* $\mathbb{Z}_{49}$*),* $p = 7,\ n = 6,\ r = 2,\ k = p - 2 = 5,\ D = 2$ *(dimensão do código) e* $d_{min} = 5$*. A matriz verificação de paridade é dada por:*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} \end{bmatrix} = \begin{bmatrix} 1 & 3 & 9 & 27 & 32 & 47 \\ 1 & 9 & 32 & 43 & 44 & 4 \\ 1 & 27 & 43 & 34 & 36 & 41 \\ 1 & 32 & 44 & 36 & 25 & 16 \end{bmatrix}. \tag{5.46}$$

Suponha agora que a palavra toda nula $\underline{v} = (0\ 0\ 0\ 0\ 0\ 0)$ seja transmitida através do canal e que o mesmo introduza o vetor erro $\underline{e} = (0\ 0\ 7\ 0\ 14\ 0)$. O receptor terá como vetor recebido $\underline{r} = \underline{v} + \underline{e}$, onde $+$ indica a adição módulo 49. Portanto, $\underline{e} = (0\ 0\ 7\ 0\ 14\ 0)$. O procedimento de decodificação é:

1) Cálculo do vetor sindrome:

$\underline{s} = \underline{r}H^t$, onde $H$ é a matriz dada acima. Portanto,

$\underline{s} = (21\ 7\ 21\ 21)$.

2) Cálculo das variáveis $\sigma_1, \sigma_2, \ldots, \sigma_\nu$ que satisfazem o Sistema (5.19). Para tanto, vamos aplicar o algoritmo de Berlekamp-Massey modificado com as entradas $s_1 = 21,\ s_2 = 7,\ s_3 = 21,\ s_4 = 21$.

| n | $\sigma^n(Z)$ | $d_n$ | $l_n$ | $n - l_n$ |
|---|---|---|---|---|
| -1 | 1 | 1 | 0 | -1 |
| 0 | 1 | 21 | 0 | 0 |
| 1 | 1 + 28Z | 7 | 1 | 0 |
| 2 | 1 + 44Z | 35 | 1 | 1 |
| 3 | $1 + 39Z + 7Z^2$ | 7 | 2 | 1 |
| 4 | $1 + 29Z + 8Z^2$ | - | 2 | 2 |

Portanto, o polinômio $C(X) = 1 + c_1X + c_2X^2 = 1 + 29X + 8X^2$ será utilizado para a construção do gerador de seqüências, no caso em particular, da seqüência $S = (21,\ 7,\ 21,\ 21)$.

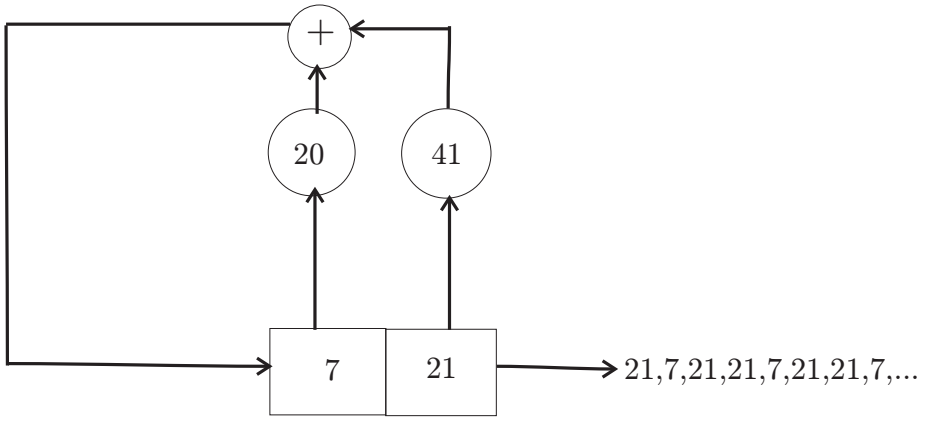


Figura 5.9: Gerador da seqüência $S = (21,\ 7,\ 21,\ 21)$, complexidade linear=2

# CAPÍTULO 6

# CONCLUSÕES

Este trabalho teve como principal motivação a inserção das extensões Galoisianas de anéis locais como sendo uma alternativa de estrutura algébrica na utilização da transformada discreta de Fourier.

Apresentamos, na transformada discreta de Fourier sobre corpos finitos, procedimentos para obtermos as extensões de Galois sobre corpos finitos dos códigos BCH, Alternante e Reed-Solomon. Fizemos da mesma forma para a transformada sobre anéis locais e, através de exemplos, constatamos que em geral os códigos Reed-Solomon não são cíclicos. Contudo, diante da dificuldade para encontrarmos o grupo das unidades dos anéis locais desenvolvemos algoritmos para a determinação do mesmo. Observamos que, conhecida a cardinalidade de um determinado anel $\mathbb{Z}_{p^m}$, consequentemente a base $p$ será conhecida, logo, podemos determinar a cardinalidade dos correspondentes anéis para subsequentes valores de $m$. Através do polinômio gerador obtido no grupo das unidades, concluímos que a sua cardinalidade está associada com o comprimento da palavra-código e que a realização da transformada discreta de Fourier está relacionada com a geração e codificação dos códigos cíclicos sobre anéis locais.

Portanto, para a decodificação dos códigos precisamos da síndrome para utilização do algoritmo de Berlekamp-Massey. Então, em primeiro lugar, é necessário identificar o polinômio gerador para geração da seqüência e por meio dos registros de deslocamento com reali-

mentação linear ou LFSR, obtemos os códigos cíclicos. Finalmente, realizamos a transformada discreta de Fourier através do polinômio gerador dos códigos cíclicos sobre anéis locais, polinômio este que indica quantas módulos terão no circuito.

## 6.1 Contribuições

- Observamos que os conceitos e elementos básicos para realização da transformada discreta de Fourier está relacionado com a geração de códigos cíclicos sobre anéis locais;
- Mostramos que o comprimento da transformada discreta de Fourier depende da ordem do elemento considerado no grupo das unidades;
- Mostramos que os registros de deslocamento com realimentação linear ou LFSR, geram seqüências pré-especificadas;
- Apresentamos a transformada discreta de Fourier através do:

    1. polinômio gerador do código cíclico sobre anéis locais;
    2. polinômio localizador de erros sobre anéis locais;
    3. e na forma matricial(código alternante).

## 6.2 Propostas para Pesquisas Futuras

Como sugestão para futuras pesquisas, propomos os seguintes tópicos:

- Considerando as extensões Galoisianas desenvolvidas nos Capítulos 4 e 5, onde nas tabelas 5.9 e 5.10 fizemos uma análise e comparação da cardinalidade dos anéis de base e grau iguais e também para anéis de base e grau diferentes são dados que servirão de suporte para o desenvolver no caso geral ou a generalização, considerando as extensões;
- Analisar e fazer o estudo da possibilidade de uma provável aplicação em criptografia.

# APÊNDICE A

# ALGORITMOS

Estes foram os algoritmos utilizados para encontrarmos os grupos das unidades desenvolvidos neste trabalho.

**Algoritmo para anéis com grau** 2 :

function[A]=ingrid1(a2,m);

A=[1 0;a2];

a1=a2(1);

a2=a2(2);

i=2;

while(A(i,1) $\neq$ 0 — A(i,2)$\neq$ 1) e i $\leq$ 200

i=i+1;

s=a1;

a1=a1*A(2,1)+a2;

a2=A(2,2)*s;

a1=mod(a1,m);

a2=mod(a2,m);

A=[A;a1 a2];

end;

disp(A);

disp(i);

**Algoritmo para anéis com grau** 3 :

function[A]=ingrid2(a3,m);

A=[1 0 0; 0 1 0; a3];

a=a3(2);

b=a3(3);

b1=a3(1);

b2=a;

b3=b

i=3;

while (A(i,1)≠ 0 — A(i,2)≠ 0 — A(i,3)≠ 1) e i ≤ 5000

i=i+1;

e=b1;

b1=b2;

b2=b3+e*a;

b3=e*b; b1=mod(b1,m);

b2=mod(b2,m);

b3=mod(b3,m);

A=[A;b1  b2  b3];

end;

disp(A);

disp(i);

# APÊNDICE B

# ELEMENTOS DO GRUPO DAS UNIDADES DO ANEL $GR(25,3)$

Apresentamos a Tabela B.1 que corresponde aos elementos do grupo das unidades de GR(25,3). As operações em $GR^*(25,3)$ são realizadas módulo $(x^3+3x+2)$. Logo, $x^3=-3x-2$; porém, como os coeficientes de $GR^*(25,3)$ estão em $\mathbb{Z}_{25}$, temos que $x^3=22x+23$. Portanto, através da última igualdade encontrada, por intermédio do programa Matlab pudemos obter todos os elementos do grupo das unidades.

| | | | | | |
|---|---|---|---|---|---|
| $1=x^0$ | $\longrightarrow$ | (1 0 0) | $x=x^1$ | $\longrightarrow$ | (0 1 0) |
| $x^2=x^2$ | $\longrightarrow$ | (0 0 1) | $x^3=23+22x$ | $\longrightarrow$ | (23 22 0) |
| $x^4=23x+22x^2$ | $\longrightarrow$ | (0 23 22) | $x^5=6+9x+23x^2$ | $\longrightarrow$ | (6 9 23) |
| $x^6=4+12x+9x^2$ | $\longrightarrow$ | (4 12 9) | $x^7=7+2x+12x^2$ | $\longrightarrow$ | (7 2 12) |
| $x^8=1+21x+2x^2$ | $\longrightarrow$ | (1 21 2) | $x^9=21+20x+21x^2$ | $\longrightarrow$ | (21 20 21) |
| $x^{10}=8+8x+20x^2$ | $\longrightarrow$ | (8 8 20) | $x^{11}=10+23x+8x^2$ | $\longrightarrow$ | (10 23 8) |
| $x^{12}=9+11x+23x^2$ | $\longrightarrow$ | (9 11 23) | $x^{13}=4+15x+11x^2$ | $\longrightarrow$ | (4 15 11) |
| $x^{14}=3+21x+15x^2$ | $\longrightarrow$ | (3 21 15) | $x^{15}=20+8x+21x^2$ | $\longrightarrow$ | (20 8 21) |
| $x^{16}=8+7x+8x^2$ | $\longrightarrow$ | (8 7 8) | $x^{17}=9+9x+7x^2$ | $\longrightarrow$ | (9 9 7) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{18} = 11 + 13x + 9x^2$ | $\longrightarrow$ | (11 13 9) | $x^{19} = 7 + 9x + 13x^2$ | $\longrightarrow$ | (7 9 13) |
| $x^{20} = 24 + 18x + 9x^2$ | $\longrightarrow$ | (24 18 9) | $x^{3} = 23 + 22x$ | $\longrightarrow$ | (23 22 0) |
| $x^{21} = 7 + 22x + 18x^2$ | $\longrightarrow$ | (7 22 18) | $x^{22} = 14 + 3x + 22x^2$ | $\longrightarrow$ | (14 3 22) |
| $x^{23} = 6 + 23x + 3x^2$ | $\longrightarrow$ | (6 23 3) | $x^{24} = 19 + 22x + 23x^2$ | $\longrightarrow$ | (4 3 0) |
| $x^{25} = 4 + 22x^2$ | $\longrightarrow$ | (4 0 22) | $x^{26} = 6 + 13x$ | $\longrightarrow$ | (6 13 0) |
| $x^{27} = 6x + 13x^2$ | $\longrightarrow$ | (0 6 13) | $x^{28} = 24 + 11x + 6x^2$ | $\longrightarrow$ | (24 11 6) |
| $x^{29} = 13 + 6x + 11x^2$ | $\longrightarrow$ | (13 6 11) | $x^{30} = 3 + 5x + 6x^2$ | $\longrightarrow$ | (3 5 6) |
| $x^{31} = 13 + 10x + 5x^2$ | $\longrightarrow$ | (13 10 5) | $x^{32} = 15 + 23x + 10x^2$ | $\longrightarrow$ | (15 23 10) |
| $x^{33} = 5 + 10x + 23x^2$ | $\longrightarrow$ | (5 10 23) | $x^{34} = 4 + 11x + 10x^2$ | $\longrightarrow$ | (4 11 10) |
| $x^{35} = 5 + 24x + 11x^2$ | $\longrightarrow$ | (5 24 11) | $x^{36} = 3 + 22x + 24x^2$ | $\longrightarrow$ | (3 22 24) |
| $x^{37} = 2 + 6x + 22x^2$ | $\longrightarrow$ | (2 6 22) | $x^{38} = 6 + 11x + 6x^2$ | $\longrightarrow$ | (6 11 6) |
| $x^{39} = 13 + 13x + 11x^2$ | $\longrightarrow$ | (13 13 11) | $x^{40} = 3 + 5x + 13x^2$ | $\longrightarrow$ | (3 5 13) |
| $x^{41} = 24 + 14x + 5x^2$ | $\longrightarrow$ | (24 14 5) | $x^{42} = 15 + 9x + 14x^2$ | $\longrightarrow$ | (15 9 14) |
| $x^{43} = 22 + 23x + 9x^2$ | $\longrightarrow$ | (22 23 9) | $x^{44} = 7 + 20x + 23x^2$ | $\longrightarrow$ | (7 20 23) |
| $x^{45} = 4 + 13x + 20x^2$ | $\longrightarrow$ | (4 13 20) | $x^{46} = 10 + 19x + 13x^2$ | $\longrightarrow$ | (10 19 13) |
| $x^{47} = 24 + 21x + 19x^2$ | $\longrightarrow$ | (24 21 19) | $x^{48} = 12 + 17x + 21x^2$ | $\longrightarrow$ | (12 17 21) |
| $x^{49} = 8 + 24x + 17x^2$ | $\longrightarrow$ | (8 24 17) | $x^{50} = 16 + 7x + 24x^2$ | $\longrightarrow$ | (16 7 24) |
| $x^{51} = 2 + 19x + 7x^2$ | $\longrightarrow$ | (2 19 7) | $x^{52} = 11 + 6x + 19x^2$ | $\longrightarrow$ | (11 6 19) |
| $x^{53} = 12 + 4x + 6x^2$ | $\longrightarrow$ | (12 4 6) | $x^{54} = 13 + 19x + 4x^2$ | $\longrightarrow$ | (13 19 4) |
| $x^{55} = 17 + x + 19x^2$ | $\longrightarrow$ | (17 1 19) | $x^{56} = 12 + 10x + x^2$ | $\longrightarrow$ | (12 10 1) |
| $x^{85} = 24 + 7x + 22x^2$ | $\longrightarrow$ | (24 7 22) | $x^{57} = 23 + 9x + 10x^2$ | $\longrightarrow$ | (23 9 10) |
| $x^{58} = 5 + 18x + 9x^2$ | $\longrightarrow$ | (5 18 9) | $x^{59} = 7 + 3x + 18x^2$ | $\longrightarrow$ | (2 2 4) |
| $x^{60} = 14 + 3x + 3x^2$ | $\longrightarrow$ | (14 3 3) | $x^{61} = 19 + 5x + 3x^2$ | $\longrightarrow$ | (19 5 3) |
| $x^{90} = 1 + 19x + 4x^2$ | $\longrightarrow$ | (1 19 4) | $x^{62} = 19 + 10x + 5x^2$ | $\longrightarrow$ | (19 10 5) |
| $x^{63} = 15 + 4x + 10x^2$ | $\longrightarrow$ | (15 4 10) | $x^{64} = 5 + 10x + 4x^2$ | $\longrightarrow$ | (5 10 4) |
| $x^{65} = 17 + 18x + 10x^2$ | $\longrightarrow$ | (17 18 10) | $x^{66} = 5 + 12x + 18x^2$ | $\longrightarrow$ | (5 12 18) |
| $x^{67} = 14 + x + 12x^2$ | $\longrightarrow$ | (14 1 12) | $x^{68} = 1 + 3x + x^2$ | $\longrightarrow$ | (1 3 1) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{69} = 23 + 23x + 3x^2$ | $\longrightarrow$ | (23 23 3) | $x^{70} = 19 + 14x + 23x^2$ | $\longrightarrow$ | (19 14 23) |
| $x^{71} = 4 + 14x^2$ | $\longrightarrow$ | (4 0 14) | $x^{72} = 22 + 12x$ | $\longrightarrow$ | (22 12 0) |
| $x^{73} = 22x + 12x^2$ | $\longrightarrow$ | (0 22 12) | $x^{74} = 1 + 14x + 22x^2$ | $\longrightarrow$ | (1 14 22) |
| $x^{75} = 6 + 10x + 14x^2$ | $\longrightarrow$ | (6 10 14) | $x^{76} = 22 + 14x + 10x^2$ | $\longrightarrow$ | (22 14 10) |
| $x^{77} = 5 + 17x + 14x^2$ | $\longrightarrow$ | (5 17 14) | $x^{78} = 22 + 13x + 17x^2$ | $\longrightarrow$ | (22 13 17) |
| $x^{79} = 16 + 21x + 13x^2$ | $\longrightarrow$ | (16 21 13) | $x^{80} = 24 + 2x + 21x^2$ | $\longrightarrow$ | (3 4 1) |
| $x^{81} = 8 + 11x + 2x^2$ | $\longrightarrow$ | (8 11 2) | $x^{82} = 21 + 2x + 11x^2$ | $\longrightarrow$ | (21 2 11) |
| $x^{83} = 3 + 13x + 2x^2$ | $\longrightarrow$ | (3 13 2) | $x^{84} = 21 + 22x + 13x^2$ | $\longrightarrow$ | (21 22 13) |
| $x^{85} = 24 + 7x + 22x^2$ | $\longrightarrow$ | (24 7 22) | $x^{86} = 6 + 8x + 7x^2$ | $\longrightarrow$ | (6 8 7) |
| $x^{87} = 11 + 10x + 8x^2$ | $\longrightarrow$ | (11 10 8) | $x^{88} = 9 + 12x + 10x^2$ | $\longrightarrow$ | (9 12 10) |
| $x^{89} = 5 + 4x + 12x^2$ | $\longrightarrow$ | (5 4 12) | $x^{90} = 1 + 19x + 4x^2$ | $\longrightarrow$ | (1 19 4) |
| $x^{91} = 17 + 14x + 19x^2$ | $\longrightarrow$ | (17 14 19) | $x^{92} = 12 + 10x + 14x^2$ | $\longrightarrow$ | (12 10 14) |
| $x^{93} = 22 + 20x + 10x^2$ | $\longrightarrow$ | (22 20 10) | $x^{94} = 5 + 17x + 20x^2$ | $\longrightarrow$ | (5 17 20) |
| $x^{95} = 10 + 20x + 17x^2$ | $\longrightarrow$ | (10 20 17) | $x^{96} = 16 + 9x + 20x^2$ | $\longrightarrow$ | (16 9 20) |
| $x^{97} = 10 + 6x + 9x^2$ | $\longrightarrow$ | (10 6 9) | $x^{98} = 7 + 8x + 6x^2$ | $\longrightarrow$ | (7 8 6) |
| $x^{99} = 13 + 14x + 8x^2$ | $\longrightarrow$ | (13 14 8) | $x^{100} = 9 + 14x + 14x^2$ | $\longrightarrow$ | (9 14 14) |
| $x^{101} = 22 + 17x + 14x^2$ | $\longrightarrow$ | (22 17 14) | $x^{102} = 22 + 5x + 17x^2$ | $\longrightarrow$ | (22 5 17) |
| $x^{103} = 16 + 21x + 5x^2$ | $\longrightarrow$ | (16 21 5) | $x^{104} = 15 + x + 21x^2$ | $\longrightarrow$ | (15 1 21) |
| $x^{105} = 8x + 2x + x^2$ | $\longrightarrow$ | (8 2 1) | $x^{106} = 23 + 5x + 2x^2$ | $\longrightarrow$ | (23 5 2) |
| $x^{107} = 21 + 17x + 5x^2$ | $\longrightarrow$ | (21 17 5) | $x^{108} = 15 + 6x + 17x^2$ | $\longrightarrow$ | (15 6 17) |
| $x^{109} = 16 + 14x + 6x^2$ | $\longrightarrow$ | (16 14 6) | $x^{110} = 13 + 23x + 14x^2$ | $\longrightarrow$ | (13 23 14) |
| $x^{111} = 22 + 21x + 23x^2$ | $\longrightarrow$ | (22 21 23) | $x^{112} = 4 + 3x + 21x^2$ | $\longrightarrow$ | (4 3 21) |
| $x^{113} = 8 + 16x + 3x^2$ | $\longrightarrow$ | (8 16 3) | $x^{114} = 19 + 24x + 16x^2$ | $\longrightarrow$ | (19 24 16) |
| $x^{115} = 18 + 21x + 24x^2$ | $\longrightarrow$ | (18 21 24) | $x^{116} = 2 + 21x + 21x^2$ | $\longrightarrow$ | (2 21 21) |
| $x^{117} = 8 + 14x + 21x^2$ | $\longrightarrow$ | (8 14 21) | $x^{118} = 8 + 20x + 14x^2$ | $\longrightarrow$ | (8 20 14) |
| $x^{119} = 22 + 16x + 20x^2$ | $\longrightarrow$ | (22 16 20) | $x^{120} = 10 + 12x + 16x^2$ | $\longrightarrow$ | (10 12 16) |
| $x^{121} = 18 + 12x + 12x^2$ | $\longrightarrow$ | (18 12 12) | $x^{122} = 1 + 7x + 12x^2$ | $\longrightarrow$ | (1 7 12) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{123}= 1+15x+7x^2$ | $\longrightarrow$ | $(1\ \ 15\ \ 7)$ | $x^{124}= 11+5x+15x^2$ | $\longrightarrow$ | $(11\ \ 5\ \ 15)$ |
| $x^{125}= 20+16x+5x^2$ | $\longrightarrow$ | $(20\ \ 16\ \ 5)$ | $x^{126}= 15+5x+16x^2$ | $\longrightarrow$ | $(15\ \ 5\ \ 16)$ |
| $x^{127}= 18+17x+5x^2$ | $\longrightarrow$ | $(18\ \ 17\ \ 5)$ | $x^{128}= 15+3x+17x^2$ | $\longrightarrow$ | $(15\ \ 3\ \ 17)$ |
| $x^{129}= 16+14x+3x^2$ | $\longrightarrow$ | $(16\ \ 14\ \ 3)$ | $x^{130}= 19+7x+14x^2$ | $\longrightarrow$ | $(19\ \ 7\ \ 14)$ |
| $x^{131}= 22+2x+7x^2$ | $\longrightarrow$ | $(22\ \ 2\ \ 7)$ | $x^{132}= 11+x+2x^2$ | $\longrightarrow$ | $(11\ \ 1\ \ 2)$ |
| $x^{133}= 21+5x+x^2$ | $\longrightarrow$ | $(21\ \ 5\ \ 1)$ | $x^{134}= 23+18x+5x^2$ | $\longrightarrow$ | $(23\ \ 18\ \ 5)$ |
| $x^{135}= 15+8x+18x^2$ | $\longrightarrow$ | $(15\ \ 8\ \ 18)$ | $x^{136}= 14+11x+8x^2$ | $\longrightarrow$ | $(14\ \ 11\ \ 8)$ |
| $x^{137}= 9+15x+11x^2$ | $\longrightarrow$ | $(9\ \ 15\ \ 11)$ | $x^{138}= 3+x+15x^2$ | $\longrightarrow$ | $(3\ \ 1\ \ 15)$ |
| $x^{139}= 20+8x+x^2$ | $\longrightarrow$ | $(20\ \ 8\ \ 1)$ | $x^{140}= 23+17x+8x^2$ | $\longrightarrow$ | $(23\ \ 17\ \ 8)$ |
| $x^{141}= 9+24x+17x^2$ | $\longrightarrow$ | $(9\ \ 24\ \ 17)$ | $x^{142}= 16+8x+24x^2$ | $\longrightarrow$ | $(16\ \ 8\ \ 24)$ |
| $x^{143}= 2+19x+8x^2$ | $\longrightarrow$ | $(2\ \ 19\ \ 8)$ | $x^{144}= 9+3x+19x^2$ | $\longrightarrow$ | $(9\ \ 3\ \ 19)$ |
| $x^{145}= 12+2x+3x^2$ | $\longrightarrow$ | $(11\ \ 10\ \ 8)$ | $x^{146}= 19+3x+2x^2$ | $\longrightarrow$ | $(19\ \ 3\ \ 2)$ |
| $x^{147}= 21+13x+3x^2$ | $\longrightarrow$ | $(21\ \ 13\ \ 3)$ | $x^{148}= 19+12x+13x^2$ | $\longrightarrow$ | $(19\ \ 12\ \ 13)$ |
| $x^{149}= 24+5x+12x^2$ | $\longrightarrow$ | $(24\ \ 5\ \ 12)$ | $x^{150}= 1+13x+5x^2$ | $\longrightarrow$ | $(1\ \ 13\ \ 5)$ |
| $x^{151}= 15+11x+13x^2$ | $\longrightarrow$ | $(15\ \ 11\ \ 13)$ | $x^{152}= 24+x+11x^2$ | $\longrightarrow$ | $(24\ \ 1\ \ 11)$ |
| $x^{153}= 3+16x+x^2$ | $\longrightarrow$ | $(3\ \ 16\ \ 1)$ | $x^{154}= 23+16x^2$ | $\longrightarrow$ | $(23\ \ 0\ \ 16)$ |
| $x^{155}= 18$ | $\longrightarrow$ | $(18\ \ 0\ \ 0)$ | $x^{156}= 18x$ | $\longrightarrow$ | $(0\ \ 18\ \ 0)$ |
| $x^{157}= 18x^2$ | $\longrightarrow$ | $(0\ \ 0\ \ 18)$ | $x^{158}= 14+21x$ | $\longrightarrow$ | $(14\ \ 21\ \ 0)$ |
| $x^{159}= 14x+21x^2$ | $\longrightarrow$ | $(0\ \ 14\ \ 21)$ | $x^{160}= 8+12x+14x^2$ | $\longrightarrow$ | $(8\ \ 12\ \ 14)$ |
| $x^{161}= 22+16x+12x^2$ | $\longrightarrow$ | $(4\ \ 13\ \ 20)$ | $x^{162}= 1+11x+16x^2$ | $\longrightarrow$ | $(1\ \ 11\ \ 16)$ |
| $x^{163}= 18+3x+11x^2$ | $\longrightarrow$ | $(18\ \ 3\ \ 11)$ | $x^{164}= 3+10x+3x^2$ | $\longrightarrow$ | $(12\ \ 17\ \ 21)$ |
| $x^{165}= 19+19x+10x^2$ | $\longrightarrow$ | $(19\ \ 19\ \ 10)$ | $x^{166}= 5+14x+19x^2$ | $\longrightarrow$ | $(5\ \ 14\ \ 19)$ |
| $x^{167}= 12+23x+14x^2$ | $\longrightarrow$ | $(12\ \ 23\ \ 14)$ | $x^{196}= 7+2x+15x^2$ | $\longrightarrow$ | $(7\ \ 2\ \ 15)$ |
| $x^{168}= 22+20x+23x^2$ | $\longrightarrow$ | $(22\ \ 20\ \ 23)$ | $x^{169}= 4+3x+20x^2$ | $\longrightarrow$ | $(4\ \ 3\ \ 20)$ |
| $x^{170}= 10+19x+3x^2$ | $\longrightarrow$ | $(10\ \ 19\ \ 3)$ | $x^{171}= 19+x+19x^2$ | $\longrightarrow$ | $(19\ \ 1\ \ 19)$ |
| $x^{172}= 12+12x+x^2$ | $\longrightarrow$ | $(12\ \ 12\ \ 1)$ | $x^{173}= 23+9x+12x^2$ | $\longrightarrow$ | $(23\ \ 9\ \ 12)$ |
| $x^{174}= 1+12x+9x^2$ | $\longrightarrow$ | $(1\ \ 12\ \ 9)$ | $x^{175}= 7+24x+12x^2$ | $\longrightarrow$ | $(7\ \ 24\ \ 12)$ |
| $x^{176}= 1+21x+24x^2$ | $\longrightarrow$ | $(1\ \ 21\ \ 24)$ | $x^{177}= 2+4x+21x^2$ | $\longrightarrow$ | $(2\ \ 4\ \ 21)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{178} = 8 + 14x + 4x^2$ | $\longrightarrow$ | (8 14 4) | $x^{179} = 17 + 21x + 14x^2$ | $\longrightarrow$ | (17 21 14) |
| $x^{180} = 22 + 21x^2$ | $\longrightarrow$ | (22 0 21) | $x^{181} = 8 + 9x$ | $\longrightarrow$ | (8 9 0) |
| $x^{182} = 8x + 9x^2$ | $\longrightarrow$ | (0 8 9) | $x^{183} = 7 + 23x + 8x^2$ | $\longrightarrow$ | (7 23 8) |
| $x^{184} = 9 + 8x + 23x^2$ | $\longrightarrow$ | (9 8 23) | $x^{185} = 4 + 15x + 8x^2$ | $\longrightarrow$ | (4 15 8) |
| $x^{186} = 9 + 5x + 15x^2$ | $\longrightarrow$ | (9 5 15) | $x^{187} = 20 + 14x + 5x^2$ | $\longrightarrow$ | (20 14 5) |
| $x^{188} = 15 + 5x + 14x^2$ | $\longrightarrow$ | (15 5 14) | $x^{189} = 22 + 23x + 5x^2$ | $\longrightarrow$ | (22 23 5) |
| $x^{190} = 15 + 7x + 23x^2$ | $\longrightarrow$ | (15 7 23) | $x^{191} = 4 + 21x + 7x^2$ | $\longrightarrow$ | (4 21 7) |
| $x^{192} = 11 + 8x + 21x^2$ | $\longrightarrow$ | (11 8 21) | $x^{193} = 8 + 23x + 8x^2$ | $\longrightarrow$ | (8 23 8) |
| $x^{194} = 9 + 9x + 23x^2$ | $\longrightarrow$ | (9 9 23) | $x^{195} = 4 + 15x + 9x^2$ | $\longrightarrow$ | (4 15 9) |
| $x^{196} = 7 + 2x + 15x^2$ | $\longrightarrow$ | (7 2 15) | $x^{197} = 20 + 12x + 2x^2$ | $\longrightarrow$ | (20 12 2) |
| $x^{198} = 21 + 14x + 12x^2$ | $\longrightarrow$ | (21 14 12) | $x^{199} = 1 + 10x + 14x^2$ | $\longrightarrow$ | (1 10 14) |
| $x^{200} = 22 + 9x + 10x^2$ | $\longrightarrow$ | (22 9 10) | $x^{201} = 5 + 17x + 9x^2$ | $\longrightarrow$ | (5 17 9) |
| $x^{202} = 7 + 3x + 17x^2$ | $\longrightarrow$ | (7 3 17) | $x^{203} = 16 + 6x + 3x^2$ | $\longrightarrow$ | (16 6 3) |
| $x^{175} = 7 + 24x + 12x^2$ | $\longrightarrow$ | (7 24 12) | $x^{204} = 19 + 7x + 6x^2$ | $\longrightarrow$ | (19 7 6) |
| $x^{205} = 13 + x + 7x^2$ | $\longrightarrow$ | (13 1 7) | $x^{206} = 11 + 17x + x^2$ | $\longrightarrow$ | (11 17 1) |
| $x^{207} = 23 + 8x + 17x^2$ | $\longrightarrow$ | (23 8 17) | $x^{208} = 16 + 22x + 8x^2$ | $\longrightarrow$ | (16 22 8) |
| $x^{209} = 9 + 17x + 22x^2$ | $\longrightarrow$ | (9 17 22) | $x^{210} = 6 + 18x + 17x^2$ | $\longrightarrow$ | (6 18 17) |
| $x^{211} = 16 + 5x + 18x^2$ | $\longrightarrow$ | (16 5 18) | $x^{212} = 14 + 12x + 5x^2$ | $\longrightarrow$ | (14 12 5) |
| $x^{213} = 15 + 24x + 12x^2$ | $\longrightarrow$ | (15 24 12) | $x^{214} = 1 + 4x + 24x^2$ | $\longrightarrow$ | (1 4 24) |
| $x^{215} = 2 + 4x + 4x^2$ | $\longrightarrow$ | (2 4 4) | $x^{216} = 17 + 15x + 4x^2$ | $\longrightarrow$ | (17 15 4) |
| $x^{217} = 17 + 5x + 15x^2$ | $\longrightarrow$ | (17 5 15) | $x^{218} = 20 + 22x + 5x^2$ | $\longrightarrow$ | (20 22 5) |
| $x^{219} = 15 + 5x + 22x^2$ | $\longrightarrow$ | (15 5 22) | $x^{220} = 6 + 24x + 5x^2$ | $\longrightarrow$ | (6 24 5) |
| $x^{221} = 15 + 16x + 24x^2$ | $\longrightarrow$ | (15 16 24) | $x^{222} = 2 + 18x + 16x^2$ | $\longrightarrow$ | (2 18 16) |
| $x^{223} = 18 + 4x + 18x^2$ | $\longrightarrow$ | (18 4 18) | $x^{224} = 14 + 14x + 4x^2$ | $\longrightarrow$ | (14 14 4) |
| $x^{225} = 17 + 2x + 14x^2$ | $\longrightarrow$ | (17 2 14) | $x^{226} = 22 + 2x^2$ | $\longrightarrow$ | (22 0 2) |
| $x^{227} = 21 + 16x$ | $\longrightarrow$ | (21 16 0) | $x^{228} = 21x + 16x^2$ | $\longrightarrow$ | (0 21 16) |
| $x^{229} = 18 + 2x + 21x^2$ | $\longrightarrow$ | (18 2 21) | $x^{230} = 8 + 5x + 2x^2$ | $\longrightarrow$ | (8 5 2) |
| $x^{231} = 21 + 2x + 5x^2$ | $\longrightarrow$ | (21 2 5) | $x^{232} = 15 + 6x + 2x^2$ | $\longrightarrow$ | (15 6 2) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{233} = 21 + 9x + 6x^2$ | $\longrightarrow$ | (21 9 6) | $x^{234} = 13 + 3x + 9x^2$ | $\longrightarrow$ | (13 3 9) |
| $x^{235} = 7 + 11x + 3x^2$ | $\longrightarrow$ | (7 11 3) | $x^{236} = 19 + 23x + 11x^2$ | $\longrightarrow$ | (19 23 11) |
| $x^{237} = 3 + 11x + 23x^2$ | $\longrightarrow$ | (3 11 23) | $x^{238} = 4 + 9x + 11x^2$ | $\longrightarrow$ | (4 9 11) |
| $x^{239} = 3 + 21x + 9x^2$ | $\longrightarrow$ | (3 21 9) | $x^{240} = 7 + x + 21x^2$ | $\longrightarrow$ | (7 1 21) |
| $x^{241} = 8 + 19x + x^2$ | $\longrightarrow$ | (8 19 1) | $x^{242} = 23 + 5x + 19x^2$ | $\longrightarrow$ | (23 5 19) |
| $x^{243} = 12 + 16x + 5x^2$ | $\longrightarrow$ | (12 16 5) | $x^{244} = 15 + 22x + 16x^2$ | $\longrightarrow$ | (15 22 16) |
| $x^{245} = 18 + 17x + 22x^2$ | $\longrightarrow$ | (18 17 22) | $x^{246} = 6 + 2x + 17x^2$ | $\longrightarrow$ | (6 2 17) |
| $x^{247} = 16 + 5x + 2x^2$ | $\longrightarrow$ | (16 5 2) | $x^{248} = 21 + 10x + 5x^2$ | $\longrightarrow$ | (21 10 5) |
| $x^{249} = 15 + 6x + 10x^2$ | $\longrightarrow$ | (15 6 10) | $x^{250} = 5 + 10x + 6x^2$ | $\longrightarrow$ | (5 10 6) |
| $x^{251} = 13 + 12x + 10x^2$ | $\longrightarrow$ | (13 12 10) | $x^{252} = 5 + 8x + 12x^2$ | $\longrightarrow$ | (5 8 12) |
| $x^{253} = 1 + 19x + 8x^2$ | $\longrightarrow$ | (1 19 8) | $x^{254} = 9 + 2x + 19x^2$ | $\longrightarrow$ | (9 2 19) |
| $x^{255} = 12 + 2x + 2x^2$ | $\longrightarrow$ | (12 2 2) | $x^{256} = 21 + 6x + 2x^2$ | $\longrightarrow$ | (21 6 2) |
| $x^{257} = 21 + 15x + 6x^2$ | $\longrightarrow$ | (21 15 6) | $x^{258} = 13 + 3x + 15x^2$ | $\longrightarrow$ | (13 3 15) |
| $x^{259} = 20 + 18x + 3x^2$ | $\longrightarrow$ | (20 18 3) | $x^{260} = 19 + 11x + 18x^2$ | $\longrightarrow$ | (19 11 18) |
| $x^{261} = 14 + 15x + 11x^2$ | $\longrightarrow$ | (14 15 11) | $x^{262} = 3 + 6x + 15x^2$ | $\longrightarrow$ | (3 6 15) |
| $x^{263} = 20 + 8x + 6x^2$ | $\longrightarrow$ | (20 8 6) | $x^{264} = 13 + 2x + 8x^2$ | $\longrightarrow$ | (13 2 8) |
| $x^{265} = 9 + 14x + 2x^2$ | $\longrightarrow$ | (9 14 2) | $x^{266} = 21 + 3x + 14x^2$ | $\longrightarrow$ | (21 3 14) |
| $x^{267} = 22 + 4x + 3x^2$ | $\longrightarrow$ | (22 4 3) | $x^{268} = 19 + 13x + 4x^2$ | $\longrightarrow$ | (19 13 4) |
| $x^{269} = 17 + 7x + 13x^2$ | $\longrightarrow$ | (17 7 13) | $x^{270} = 24 + 3x + 7x^2$ | $\longrightarrow$ | (24 3 7) |
| $x^{271} = 11 + 3x + 3x^2$ | $\longrightarrow$ | (11 3 3) | $x^{272} = 19 + 2x + 3x^2$ | $\longrightarrow$ | (19 2 3) |
| $x^{273} = 19 + 10x + 2x^2$ | $\longrightarrow$ | (19 10 2) | $x^{274} = 21 + 13x + 10x^2$ | $\longrightarrow$ | (21 13 10) |
| $x^{275} = 5 + 16x + 13x^2$ | $\longrightarrow$ | (5 16 13) | $x^{276} = 24 + 16x + 16x^2$ | $\longrightarrow$ | (24 16 16) |
| $x^{277} = 18 + x + 16x^2$ | $\longrightarrow$ | (18 1 16) | $x^{278} = 18 + 20x + x^2$ | $\longrightarrow$ | (18 20 1) |
| $x^{279} = 23 + 15x + 20x^2$ | $\longrightarrow$ | (23 15 20) | $x^{280} = 10 + 13x + 15x^2$ | $\longrightarrow$ | (10 13 15) |
| $x^{281} = 20 + 15x + 13x^2$ | $\longrightarrow$ | (20 15 13) | $x^{282} = 24 + 6x + 15x^2$ | $\longrightarrow$ | (24 6 15) |
| $x^{283} = 20 + 4x + 6x^2$ | $\longrightarrow$ | (20 4 6) | $x^{284} = 13 + 2x + 4x^2$ | $\longrightarrow$ | (13 2 4) |
| $x^{285} = 17 + x + 2x^2$ | $\longrightarrow$ | (17 1 2) | $x^{286} = 21 + 11x + x^2$ | $\longrightarrow$ | (21 11 1) |
| $x^{287} = 23 + 18x + 11x^2$ | $\longrightarrow$ | (23 18 11) | $x^{288} = 3 + 15x + 18x^2$ | $\longrightarrow$ | (3 15 18) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{289} = 14 + 24x + 15x^2$ | $\longrightarrow$ | (14 24 15) | $x^{290} = 20 + 19x + 24x^2$ | $\longrightarrow$ | (20 19 24) |
| $x^{291} = 2 + 23x + 19x^2$ | $\longrightarrow$ | (2 23 19) | $x^{292} = 12 + 20x + 23x^2$ | $\longrightarrow$ | (12 20 23) |
| $x^{293} = 4 + 18x + 20x^2$ | $\longrightarrow$ | (4 18 20) | $x^{294} = 10 + 19x + 18x^2$ | $\longrightarrow$ | (10 19 18) |
| $x^{295} = 14 + 6x + 19x^2$ | $\longrightarrow$ | (14 6 19) | $x^{296} = 12 + 7x + 6x^2$ | $\longrightarrow$ | (12 7 6) |
| $x^{297} = 13 + 19x + 7x^2$ | $\longrightarrow$ | (13 19 7) | $x^{298} = 11 + 17x + 19x^2$ | $\longrightarrow$ | (11 17 19) |
| $x^{299} = 12 + 4x + 17x^2$ | $\longrightarrow$ | (12 4 17) | $x^{300} = 16 + 11x + 4x^2$ | $\longrightarrow$ | (16 11 4) |
| $x^{301} = 17 + 4x + 11x^2$ | $\longrightarrow$ | (17 4 11) | $x^{302} = 3 + 9x + 4x^2$ | $\longrightarrow$ | (3 9 4) |
| $x^{303} = 17 + 16x + 9x^2$ | $\longrightarrow$ | (17 16 9) | $x^{304} = 7 + 15x + 16x^2$ | $\longrightarrow$ | (7 15 16) |
| $x^{305} = 18 + 9x + 15x^2$ | $\longrightarrow$ | (18 9 15) | $x^{306} = 20 + 23x + 9x^2$ | $\longrightarrow$ | (20 23 9) |
| $x^{307} = 7 + 18x + 23x^2$ | $\longrightarrow$ | (7 18 23) | $x^{308} = 3 + 13x + 18x^2$ | $\longrightarrow$ | (3 13 18) |
| $x^{309} = 14 + 13x^2$ | $\longrightarrow$ | (14 0 13) | $x^{310} = 24$ | $\longrightarrow$ | (24 0 0) |
| $x^{311} = 24x$ | $\longrightarrow$ | (0 24 0) | $x^{312} = 24x^2$ | $\longrightarrow$ | (0 0 24) |
| $x^{313} = 2 + 3x$ | $\longrightarrow$ | (2 3 0) | $x^{314} = 2x + 3x^2$ | $\longrightarrow$ | (0 2 3) |
| $x^{315} = 19 + 16x + 2x^2$ | $\longrightarrow$ | (19 16 2) | $x^{316} = 21 + 13x + 16x^2$ | $\longrightarrow$ | (21 13 16) |
| $x^{317} = 18 + 23x + 13x^2$ | $\longrightarrow$ | (18 23 13) | $x^{318} = 24 + 4x + 23x^2$ | $\longrightarrow$ | (24 4 23) |
| $x^{319} = 4 + 5x + 4x^2$ | $\longrightarrow$ | (4 5 4) | $x^{320} = 17 + 17x + 5x^2$ | $\longrightarrow$ | (17 17 5) |
| $x^{321} = 15 + 2x + 17x^2$ | $\longrightarrow$ | (15 2 17) | $x^{322} = 16 + 14x + 2x^2$ | $\longrightarrow$ | (16 14 2) |
| $x^{323} = 21 + 10x + 14x^2$ | $\longrightarrow$ | (21 10 14) | $x^{324} = 22 + 4x + 10x^2$ | $\longrightarrow$ | (22 4 10) |
| $x^{325} = 5 + 17x + 4x^2$ | $\longrightarrow$ | (5 17 4) | $x^{326} = 17 + 18x + 17x^2$ | $\longrightarrow$ | (17 18 17) |
| $x^{327} = 16 + 16x + 18x^2$ | $\longrightarrow$ | (16 16 18) | $x^{328} = 14 + 12x + 16x^2$ | $\longrightarrow$ | (14 12 16) |
| $x^{329} = 18 + 16x + 12x^2$ | $\longrightarrow$ | (18 16 12) | $x^{330} = 1 + 7x + 16x^2$ | $\longrightarrow$ | (1 7 16) |
| $x^{331} = 18 + 3x + 7x^2$ | $\longrightarrow$ | (18 3 7) | $x^{332} = 11 + 22x + 3x^2$ | $\longrightarrow$ | (11 22 3) |
| $x^{333} = 19 + 2x + 22x^2$ | $\longrightarrow$ | (19 2 22) | $x^{334} = 6 + 3x + 2x^2$ | $\longrightarrow$ | (6 3 2) |
| $x^{335} = 21 + 3x^2$ | $\longrightarrow$ | (21 0 3) | $x^{336} = 19 + 12x$ | $\longrightarrow$ | (19 12 0) |
| $x^{337} = 0 + 19x + 12x^2$ | $\longrightarrow$ | (0 19 12) | $x^{338} = 1 + 14x + 19x^2$ | $\longrightarrow$ | (1 14 19) |
| $x^{339} = 12 + 19x + 14x^2$ | $\longrightarrow$ | (12 19 14) | $x^{340} = 22 + 20x + 19x^2$ | $\longrightarrow$ | (22 20 19) |
| $x^{341} = 12 + 15x + 20x^2$ | $\longrightarrow$ | (12 15 20) | $x^{342} = 10 + 2x + 15x^2$ | $\longrightarrow$ | (10 2 15) |
| $x^{343} = 20 + 15x + 2x^2$ | $\longrightarrow$ | (20 15 2) | $x^{344} = 21 + 14x + 15x^2$ | $\longrightarrow$ | (21 14 15) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{345} = 20 + x + 14x^2$ | $\longrightarrow$ | (20 1 14) | $x^{346} = 22 + 3x + x^2$ | $\longrightarrow$ | (22 3 1) |
| $x^{347} = 23 + 19x + 3x^2$ | $\longrightarrow$ | (23 19 3) | $x^{348} = 19 + 14x + 19x^2$ | $\longrightarrow$ | (19 14 19) |
| $x^{349} = 12 + 12x + 14x^2$ | $\longrightarrow$ | (12 12 14) | $x^{350} = 22 + 20x + 12x^2$ | $\longrightarrow$ | (22 20 12) |
| $x^{351} = 1 + 11x + 20x^2$ | $\longrightarrow$ | (1 11 20) | $x^{352} = 10 + 16x + 11x^2$ | $\longrightarrow$ | (10 16 11) |
| $x^{353} = 3 + 2x + 16x^2$ | $\longrightarrow$ | (3 2 16) | $x^{354} = 18 + 5x + 2x^2$ | $\longrightarrow$ | (18 5 2) |
| $x^{355} = 21 + 12x + 5x^2$ | $\longrightarrow$ | (21 12 5) | $x^{356} = 15 + 6x + 12x^2$ | $\longrightarrow$ | (15 6 12) |
| $x^{357} = 1 + 4x + 6x^2$ | $\longrightarrow$ | (1 4 6) | $x^{358} = 13 + 8x + 4x^2$ | $\longrightarrow$ | (13 8 4) |
| $x^{359} = 17 + x + 8x^2$ | $\longrightarrow$ | (17 1 8) | $x^{360} = 9 + 18x + x^2$ | $\longrightarrow$ | (9 18 1) |
| $x^{361} = 23 + 6x + 18x^2$ | $\longrightarrow$ | (23 6 18) | $x^{362} = 14 + 19x + 6x^2$ | $\longrightarrow$ | (14 19 6) |
| $x^{363} = 13 + 21x + 19x^2$ | $\longrightarrow$ | (13 21 19) | $x^{364} = 12 + 6x + 21x^2$ | $\longrightarrow$ | (12 6 21) |
| $x^{365} = 8 + 24x + 6x^2$ | $\longrightarrow$ | (8 24 6) | $x^{366} = 13 + 15x + 24x^2$ | $\longrightarrow$ | (13 15 24) |
| $x^{367} = 2 + 16x + 15x^2$ | $\longrightarrow$ | (2 16 15) | $x^{368} = 20 + 7x + 16x^2$ | $\longrightarrow$ | (20 7 16) |
| $x^{369} = 18 + 22x + 7x^2$ | $\longrightarrow$ | (18 22 7) | $x^{370} = 11 + 22x + 22x^2$ | $\longrightarrow$ | (11 22 22) |
| $x^{371} = 6 + 20x + 22x^2$ | $\longrightarrow$ | (6 20 22) | $x^{372} = 6 + 15x + 20x^2$ | $\longrightarrow$ | (6 15 20) |
| $x^{373} = 10 + 21x + 15x^2$ | $\longrightarrow$ | (10 21 15) | $x^{374} = 20 + 15x + 21x^2$ | $\longrightarrow$ | (20 15 21) |
| $x^{375} = 8 + 7x + 15x^2$ | $\longrightarrow$ | (8 7 15) | $x^{376} = 20 + 13x + 7x^2$ | $\longrightarrow$ | (20 13 7) |
| $x^{377} = 11 + 24x + 13x^2$ | $\longrightarrow$ | (11 24 13) | $x^{378} = 24 + 22x + 24x^2$ | $\longrightarrow$ | (24 22 24) |
| $x^{379} = 2 + 2x + 22x^2$ | $\longrightarrow$ | (2 2 22) | $x^{380} = 6 + 11x + 2x^2$ | $\longrightarrow$ | (6 11 2) |
| $x^{381} = 21 + 11x^2$ | $\longrightarrow$ | (21 0 11) | $x^{382} = 3 + 13x$ | $\longrightarrow$ | (3 13 0) |
| $x^{383} = 3x + 13x^2$ | $\longrightarrow$ | (0 3 13) | $x^{384} = 24 + 11x + 3x^2$ | $\longrightarrow$ | (24 11 3) |
| $x^{385} = 19 + 15x + 11x^2$ | $\longrightarrow$ | (19 15 11) | $x^{386} = 3 + 11x + 15x^2$ | $\longrightarrow$ | (3 11 15) |
| $x^{388} = 3 + 12x + 8x^2$ | $\longrightarrow$ | (3 12 8) | $x^{389} = 9 + 4x + 12x^2$ | $\longrightarrow$ | (9 4 12) |
| $x^{390} = 1 + 23x + 4x^2$ | $\longrightarrow$ | (1 23 4) | $x^{391} = 17 + 14x + 23x^2$ | $\longrightarrow$ | (17 14 23) |
| $x^{392} = 4 + 23x + 14x^2$ | $\longrightarrow$ | (4 23 14) | $x^{393} = 22 + 12x + 23x^2$ | $\longrightarrow$ | (22 12 23) |
| $x^{394} = 4 + 3x + 12x^2$ | $\longrightarrow$ | (4 3 12) | $x^{395} = 1 + 18x + 3x^2$ | $\longrightarrow$ | (1 18 3) |
| $x^{396} = 19 + 17x + 18x^2$ | $\longrightarrow$ | (19 17 18) | $x^{397} = 14 + 15x + 17x^2$ | $\longrightarrow$ | (14 15 17) |
| $x^{398} = 16 + 13x + 15x^2$ | $\longrightarrow$ | (16 13 15) | $x^{399} = 20 + 21x + 13x^2$ | $\longrightarrow$ | (20 21 13) |
| $x^{400} = 24 + 6x + 21x^2$ | $\longrightarrow$ | (24 6 21) | $x^{401} = 8 + 11x + 6x^2$ | $\longrightarrow$ | (8 11 6) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{402} = 13 + 15x + 11x^2$ | $\longrightarrow$ | (13 15 11) | $x^{403} = 3 + 5x + 15x^2$ | $\longrightarrow$ | (3 5 15) |
| $x^{404} = 20 + 8x + 5x^2$ | $\longrightarrow$ | (20 8 5) | $x^{405} = 15 + 5x + 8x^2$ | $\longrightarrow$ | (15 5 8) |
| $x^{406} = 9 + 16x + 5x^2$ | $\longrightarrow$ | (9 16 5) | $x^{407} = 15 + 19x + 6x^2$ | $\longrightarrow$ | (15 19 6) |
| $x^{408} = 18 + 17x + 19x^2$ | $\longrightarrow$ | (18 17 19) | $x^{409} = 12 + 11x + 17x^2$ | $\longrightarrow$ | (12 11 17) |
| $x^{410} = 16 + 11x + 11x^2$ | $\longrightarrow$ | (16 11 11) | $x^{411} = 3 + 8x + 11x^2$ | $\longrightarrow$ | (3 8 11) |
| $x^{412} = 3 + 20x + 8x^2$ | $\longrightarrow$ | (3 20 8) | $x^{413} = 9 + 4x + 20x^2$ | $\longrightarrow$ | (9 4 20) |
| $x^{414} = 10 + 24x + 4x^2$ | $\longrightarrow$ | (10 24 4) | $x^{415} = 17 + 23x + 24x^2$ | $\longrightarrow$ | (17 23 24) |
| $x^{416} = 2 + 20x + 23x^2$ | $\longrightarrow$ | (2 20 23) | $x^{417} = 4 + 8x + 20x^2$ | $\longrightarrow$ | (4 8 20) |
| $x^{418} = 10 + 19x + 8x^2$ | $\longrightarrow$ | (10 19 8) | $x^{419} = 9 + 11x + 19x^2$ | $\longrightarrow$ | (9 11 19) |
| $x^{420} = 12 + 2x + 11x^2$ | $\longrightarrow$ | (12 2 11) | $x^{421} = 3 + 4x + 2x^2$ | $\longrightarrow$ | (3 4 2) |
| $x^{422} = 21 + 22x + 4x^2$ | $\longrightarrow$ | (21 22 4) | $x^{423} = 17 + 9x + 22x^2$ | $\longrightarrow$ | (17 9 22) |
| $x^{424} = 6 + x + 9x^2$ | $\longrightarrow$ | (6 1 9) | $x^{425} = 7 + 4x + x^2$ | $\longrightarrow$ | (7 4 1) |
| $x^{426} = 23 + 4x + 4x^2$ | $\longrightarrow$ | (23 4 4) | $x^{427} = 17 + 11x + 4x^2$ | $\longrightarrow$ | (17 11 4) |
| $x^{428} = 17 + 5x + 11x^2$ | $\longrightarrow$ | (17 5 11) | $x^{429} = 3 + 9x + 5x^2$ | $\longrightarrow$ | (3 9 5) |
| $x^{430} = 15 + 13x + 9x^2$ | $\longrightarrow$ | (15 13 9) | $x^{431} = 7 + 13x + 13x^2$ | $\longrightarrow$ | (7 13 13) |
| $x^{432} = 24 + 18x + 13x^2$ | $\longrightarrow$ | (24 18 13) | $x^{433} = 24 + 10x + 18x^2$ | $\longrightarrow$ | (24 10 18) |
| $x^{434} = 14 + 20x + 10x^2$ | $\longrightarrow$ | (14 20 10) | $x^{435} = 5 + 9x + 20x^2$ | $\longrightarrow$ | (5 9 20) |
| $x^{436} = 10 + 20x + 9x^2$ | $\longrightarrow$ | (10 20 9) | $x^{437} = 7 + 8x + 20x^2$ | $\longrightarrow$ | (7 8 20) |
| $x^{438} = 10 + 22x + 8x^2$ | $\longrightarrow$ | (10 22 8) | $x^{439} = 9 + 11x + 22x^2$ | $\longrightarrow$ | (9 11 22) |
| $x^{440} = 6 + 18x + 11x^2$ | $\longrightarrow$ | (6 18 11) | $x^{441} = 3 + 23x + 18x^2$ | $\longrightarrow$ | (3 23 18) |
| $x^{442} = 14 + 24x + 23x^2$ | $\longrightarrow$ | (14 24 23) | $x^{443} = 4 + 20x + 24x^2$ | $\longrightarrow$ | (4 20 24) |
| $x^{444} = 2 + 7x + 20x^2$ | $\longrightarrow$ | (2 7 20) | $x^{445} = 10 + 17x + 7x^2$ | $\longrightarrow$ | (10 17 7) |
| $x^{446} = 11 + 14x + 17x^2$ | $\longrightarrow$ | (11 14 17) | $x^{447} = 16 + 10x + 14x^2$ | $\longrightarrow$ | (16 10 14) |
| $x^{448} = 22 + 24x + 10x^2$ | $\longrightarrow$ | (22 24 10) | $x^{449} = 5 + 17x + 24x^2$ | $\longrightarrow$ | (5 17 24) |
| $x^{450} = 2 + 8x + 17x^2$ | $\longrightarrow$ | (2 8 17) | $x^{451} = 16 + x + 8x^2$ | $\longrightarrow$ | (16 1 8) |
| $x^{452} = 9 + 17x + x^2$ | $\longrightarrow$ | (9 17 1) | $x^{453} = 23 + 6x + 17x^2$ | $\longrightarrow$ | (23 6 17) |
| $x^{454} = 16 + 22x + 6x^2$ | $\longrightarrow$ | (16 22 6) | $x^{455} = 13 + 23x + 22x^2$ | $\longrightarrow$ | (13 23 22) |
| $x^{456} = 6 + 22x + 23x^2$ | $\longrightarrow$ | (6 22 23) | $x^{457} = 4 + 12x + 22x^2$ | $\longrightarrow$ | (4 12 22) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{458} = 6 + 13x + 12x^2$ | $\longrightarrow$ | (6 13 12) | $x^{459} = 1 + 20x + 13x^2$ | $\longrightarrow$ | (1 20 13) |
| $x^{460} = 24 + 12x + 20x^2$ | $\longrightarrow$ | (24 12 20) | $x^{461} = 10 + 14x + 12x^2$ | $\longrightarrow$ | (10 14 12) |
| $x^{462} = 1 + 24x + 14x^2$ | $\longrightarrow$ | (1 24 14) | $x^{463} = 22 + 9x + 24x^2$ | $\longrightarrow$ | (22 9 24) |
| $x^{464} = 2 + 9x^2$ | $\longrightarrow$ | (2 0 9) | $x^{465} = 7$ | $\longrightarrow$ | (7 0 0) |
| $x^{466} = 7x$ | $\longrightarrow$ | (0 7 0) | $x^{467} = 7x^2$ | $\longrightarrow$ | (0 0 7) |
| $x^{468} = 11 + 4x$ | $\longrightarrow$ | (11 4 0) | $x^{469} = 11x + 4x^2$ | $\longrightarrow$ | (0 11 4) |
| $x^{470} = 17 + 13x + 11x^2$ | $\longrightarrow$ | (17 13 11) | $x^{471} = 3 + 9x + 13x^2$ | $\longrightarrow$ | (3 9 13) |
| $x^{472} = 24 + 14x + 9x^2$ | $\longrightarrow$ | (24 14 9) | $x^{473} = 14 + 22x + 7x^2$ | $\longrightarrow$ | (14 22 7) |
| $x^{474} = 22 + 15x + 22x^2$ | $\longrightarrow$ | (22 15 22) | $x^{475} = 6 + 6x + 15x^2$ | $\longrightarrow$ | (6 6 15) |
| $x^{476} = 20 + 11x + 6x^2$ | $\longrightarrow$ | (20 11 6) | $x^{477} = 13 + 2x + 11x^2$ | $\longrightarrow$ | (13 2 11) |
| $x^{478} = 3 + 5x + 2x^2$ | $\longrightarrow$ | (3 5 2) | $x^{479} = 21 + 22x + 5x^2$ | $\longrightarrow$ | (21 22 5) |
| $x^{480} = 15 + 6x + 22x^2$ | $\longrightarrow$ | (15 6 22) | $x^{481} = 6 + 24x + 6x^2$ | $\longrightarrow$ | (6 24 6) |
| $x^{482} = 13 + 13x + 24x^2$ | $\longrightarrow$ | (13 13 24) | $x^{483} = 2 + 16x + 13x^2$ | $\longrightarrow$ | (2 16 13) |
| $x^{484} = 24 + 13x + 16x^2$ | $\longrightarrow$ | (24 13 16) | $x^{485} = 18 + x + 13x^2$ | $\longrightarrow$ | (18 1 13) |
| $x^{486} = 24 + 4x + x^2$ | $\longrightarrow$ | (24 4 1) | $x^{487} = 23 + 21x + 4x^2$ | $\longrightarrow$ | (23 21 4) |
| $x^{488} = 17 + 11x + 21x^2$ | $\longrightarrow$ | (17 11 21) | $x^{489} = 8 + 4x + 11x^2$ | $\longrightarrow$ | (8 4 11) |
| $x^{490} = 3 + 4x^2$ | $\longrightarrow$ | (3 0 4) | $x^{491} = 17 + 16x$ | $\longrightarrow$ | (17 16 0) |
| $x^{492} = 17x + 16x^2$ | $\longrightarrow$ | (0 17 16) | $x^{493} = 18 + 2x + 17x^2$ | $\longrightarrow$ | (18 2 17) |
| $x^{494} = 16 + 17x + 2x^2$ | $\longrightarrow$ | (16 17 2) | $x^{495} = 21 + 10x + 17x^2$ | $\longrightarrow$ | (21 10 17) |
| $x^{496} = 16 + 20x + 10x^2$ | $\longrightarrow$ | (16 20 10) | $x^{497} = 5 + 11x + 20x^2$ | $\longrightarrow$ | (5 11 20) |
| $x^{498} = 10 + 20x + 11x^2$ | $\longrightarrow$ | (10 20 11) | $x^{499} = 3 + 2x + 20x^2$ | $\longrightarrow$ | (3 2 20) |
| $x^{500} = 10 + 18x + 2x^2$ | $\longrightarrow$ | (10 18 2) | $x^{501} = 21 + 4x + 18x^2$ | $\longrightarrow$ | (21 4 18) |
| $x^{502} = 14 + 17x + 4x^2$ | $\longrightarrow$ | (14 17 4) | $x^{503} = 17 + 2x + 17x^2$ | $\longrightarrow$ | (17 2 17) |
| $x^{504} = 16 + 16x + 2x^2$ | $\longrightarrow$ | (16 16 2) | $x^{505} = 21 + 10x + 16x^2$ | $\longrightarrow$ | (21 10 16) |
| $x^{506} = 18 + 23x + 10x^2$ | $\longrightarrow$ | (18 23 10) | $x^{507} = 5 + 13x + 23x^2$ | $\longrightarrow$ | (5 13 23) |
| $x^{508} = 4 + 11x + 13x^2$ | $\longrightarrow$ | (4 11 13) | $x^{509} = 24 + 15x + 11x^2$ | $\longrightarrow$ | (24 15 11) |
| $x^{510} = 3 + 16x + 15x^2$ | $\longrightarrow$ | (3 16 15) | $x^{511} = 20 + 8x + 16x^2$ | $\longrightarrow$ | (20 8 16) |
| $x^{512} = 18 + 22x + 8x^2$ | $\longrightarrow$ | (18 22 8) | $x^{513} = 9 + 19x + 22x^2$ | $\longrightarrow$ | (9 19 22) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{514}= 6+18x+19x^2$ | $\longrightarrow$ | (6 18 19) | $x^{515} = 12+24x+18x^2$ | $\longrightarrow$ | (12 24 18) |
| $x^{516} = 14+8x+24x^2$ | $\longrightarrow$ | (14 8 24) | $x^{517} = 2+17x+8x^2$ | $\longrightarrow$ | (2 17 8) |
| $x^{518} = 9+3x+17x^2$ | $\longrightarrow$ | (9 3 17) | $x^{519} = 16+8x+3x^2$ | $\longrightarrow$ | (16 8 3) |
| $x^{520} = 19+7x+8x^2$ | $\longrightarrow$ | (19 7 8) | $x^{521}= 9+20x+7x^2$ | $\longrightarrow$ | (9 20 7) |
| $x^{522} = 11+13x+20x^2$ | $\longrightarrow$ | (11 13 20) | $x^{523}= 10+x+13x^2$ | $\longrightarrow$ | (10 1 13) |
| $x^{524} = 24+21x+x^2$ | $\longrightarrow$ | (24 21 1) | $x^{525} = 23+21x+21x^2$ | $\longrightarrow$ | (23 21 21) |
| $x^{526} = 8+10x+21x^2$ | $\longrightarrow$ | (8 10 21) | $x^{527} = 8+20x+10x^2$ | $\longrightarrow$ | (8 20 10) |
| $x^{528} = 5+3x+20x^2$ | $\longrightarrow$ | (5 3 20) | $x^{529} = 10+20x+3x^2$ | $\longrightarrow$ | (10 20 3) |
| $x^{530} = 19+x+20x^2$ | $\longrightarrow$ | (19 1 20) | $x^{531} = 10+9x+x^2$ | $\longrightarrow$ | (10 9 1) |
| $x^{532} = 23+7x+9x^2$ | $\longrightarrow$ | (23 7 9 ) | $x^{533} = 7+21x+7x^2$ | $\longrightarrow$ | (7 21 7) |
| $x^{534} = 11+11x+21x^2$ | $\longrightarrow$ | (11 11 21) | $x^{535} = 8+23x+11x^2$ | $\longrightarrow$ | (8 23 11) |
| $x^{536} = 3+23x^2$ | $\longrightarrow$ | (3 0 23) | $x^{537} = 4+9x$ | $\longrightarrow$ | (4 9 0) |
| $x^{538} = 4x+9x^2$ | $\longrightarrow$ | (0 4 9) | $x^{539} = 7+23x+4x^2$ | $\longrightarrow$ | (7 23 4) |
| $x^{540} = 17+20x+23x^2$ | $\longrightarrow$ | (17 20 23) | $x^{541} = 4+23x+20x^2$ | $\longrightarrow$ | (4 23 20) |
| $x^{542} = 10+19x+23x^2$ | $\longrightarrow$ | (10 19 23) | $x^{543} = 4+16x+19x^2$ | $\longrightarrow$ | (4 16 19) |
| $x^{544} = 12+22x+16x^2$ | $\longrightarrow$ | (12 22 16) | $x^{545} = 18+14x+22x^2$ | $\longrightarrow$ | (18 14 22) |
| $x^{546} = 6+2x+14x^2$ | $\longrightarrow$ | (6 2 14) | $x^{547} = 22+14x+2x^2$ | $\longrightarrow$ | (22 14 2) |
| $x^{548} = 21+16x+14x^2$ | $\longrightarrow$ | (21 16 14) | $x^{549} = 22+4x+16x^2$ | $\longrightarrow$ | (22 4 16) |
| $x^{550} = 18+24x+4x^2$ | $\longrightarrow$ | (18 24 4) | $x^{551} = 17+6x+24x^2$ | $\longrightarrow$ | (17 6 24) |
| $x^{552} = 2+20x+6x^2$ | $\longrightarrow$ | (2 20 6) | $x^{553} = 13+9x+20x^2$ | $\longrightarrow$ | (13 9 20) |
| $x^{554} = 10+3x+9x^2$ | $\longrightarrow$ | (10 3 9) | $x^{555} = 7+8x+3x^2$ | $\longrightarrow$ | (7 8 3) |
| $x^{556} = 19+23x+8x^2$ | $\longrightarrow$ | (19 23 8) | $x^{557} = 9+20x+23x^2$ | $\longrightarrow$ | (9 20 23) |
| $x^{558}= 4+15x+20x^2$ | $\longrightarrow$ | (4 15 20) | $x^{559} = 10+19x+15x^2$ | $\longrightarrow$ | (10 19 15) |
| $x^{560} = 20+15x+19x^2$ | $\longrightarrow$ | (20 15 19) | $x^{561} = 12+13x+15x^2$ | $\longrightarrow$ | (12 13 15) |
| $x^{562} = 20+17x+13x^2$ | $\longrightarrow$ | (20 17 13) | $x^{563}= 24+6x+17x^2$ | $\longrightarrow$ | (24 6 17) |
| $x^{564} = 16+23x+6x^2$ | $\longrightarrow$ | (16 23 6) | $x^{565}= 13+23x+23x^2$ | $\longrightarrow$ | (13 23 23) |
| $x^{566} = 4+19x+23x^2$ | $\longrightarrow$ | (4 19 23) | $x^{567} = 4+10x+19x^2$ | $\longrightarrow$ | (4 10 19) |
| $x^{568} = 12+22x+10x^2$ | $\longrightarrow$ | (12 22 10) | $x^{569} = 5+7x+22x^2$ | $\longrightarrow$ | (5 7 22) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{570}= 6+14x+7x^2$ | $\longrightarrow$ | (6 14 7) | $x^{571}= 11+10x+14x^2$ | $\longrightarrow$ | (11 10 14) |
| $x^{572}= 22+19x+10x^2$ | $\longrightarrow$ | (22 19 10) | $x^{573}= 5+17x+19x^2$ | $\longrightarrow$ | (5 17 19) |
| $x^{574}= 12+23x+17x^2$ | $\longrightarrow$ | (12 23 17) | $x^{575}= 16+11x+23x^2$ | $\longrightarrow$ | (16 11 23) |
| $x^{576}= 4+22x+11x^2$ | $\longrightarrow$ | (4 22 11) | $x^{577}= 3+21x+22x^2$ | $\longrightarrow$ | (3 21 22) |
| $x^{578}= 6+12x+21x^2$ | $\longrightarrow$ | (6 12 21) | $x^{579}= 8+18x+12x^2$ | $\longrightarrow$ | (8 18 12) |
| $x^{580}= 1+22x+18x^2$ | $\longrightarrow$ | (1 22 18) | $x^{581}= 14+22x+22x^2$ | $\longrightarrow$ | (14 22 22) |
| $x^{582}= 6+23x+22x^2$ | $\longrightarrow$ | (6 23 22) | $x^{583}= 6+15x+23x^2$ | $\longrightarrow$ | (6 15 23) |
| $x^{584}= 4+12x+15x^2$ | $\longrightarrow$ | (4 12 15) | $x^{585}= 20+9x+12x^2$ | $\longrightarrow$ | (20 9 12) |
| $x^{586}= 1+9x+9x^2$ | $\longrightarrow$ | (1 9 9) | $x^{587}= 7+24x+9x^2$ | $\longrightarrow$ | (7 24 9) |
| $x^{588}= 7+5x+24x^2$ | $\longrightarrow$ | (7 5 24) | $x^{589}= 2+10x+5x^2$ | $\longrightarrow$ | (2 10 5) |
| $x^{590}= 15+12x+10x^2$ | $\longrightarrow$ | (15 12 10) | $x^{591}= 5+10x+12x^2$ | $\longrightarrow$ | (5 10 12) |
| $x^{592}= 1+19x+10x^2$ | $\longrightarrow$ | (1 19 10) | $x^{593}= 5+21x+19x^2$ | $\longrightarrow$ | (5 21 19) |
| $x^{594}= 12+23x+21x^2$ | $\longrightarrow$ | (12 23 21) | $x^{595}= 8+24x+23x^2$ | $\longrightarrow$ | (3 4 2) |
| $x^{596}= 4+14x+24x^2$ | $\longrightarrow$ | (4 14 24) | $x^{597}= 2+7x+14x^2$ | $\longrightarrow$ | (2 7 14) |
| $x^{598}= 22+10x+7x^2$ | $\longrightarrow$ | (22 10 7) | $x^{599}= 11+x+10x^2$ | $\longrightarrow$ | (11 1 10) |
| $x^{600}= 5+6x+x^2$ | $\longrightarrow$ | (5 6 1) | $x^{601}= 23+2x+6x^2$ | $\longrightarrow$ | (23 2 6) |
| $x^{602}= 13+5x+2x^2$ | $\longrightarrow$ | (13 5 2) | $x^{603}= 21+7x+5x^2$ | $\longrightarrow$ | (21 7 5) |
| $x^{604}= 15+6x+7x^2$ | $\longrightarrow$ | (15 6 7) | $x^{605}= 11+19x+6x^2$ | $\longrightarrow$ | (11 19 6) |
| $x^{606}= 13+18x+19x^2$ | $\longrightarrow$ | (13 18 19) | $x^{607}= 12+6x+18x^2$ | $\longrightarrow$ | (12 6 18) |
| $x^{608}= 14+8x+6x^2$ | $\longrightarrow$ | (14 8 6) | $x^{609}= 13+21x+8x^2$ | $\longrightarrow$ | (13 21 8) |
| $x^{610}= 9+14x+21x^2$ | $\longrightarrow$ | (9 14 21) | $x^{611}= 8+21x+14x^2$ | $\longrightarrow$ | (8 21 14) |
| $x^{612}= 22+16x+21x^2$ | $\longrightarrow$ | (22 16 21) | $x^{613}= 8+9x+16x^2$ | $\longrightarrow$ | (8 9 16) |
| $x^{614}= 18+10x+9x^2$ | $\longrightarrow$ | (18 10 9) | $x^{615}= 7+16x+10x^2$ | $\longrightarrow$ | (7 16 10) |
| $x^{616}= 5+2x+16x^2$ | $\longrightarrow$ | (5 2 16) | $x^{617}= 18+7x+2x^2$ | $\longrightarrow$ | (18 7 2) |
| $x^{618}= 21+12x+7x^2$ | $\longrightarrow$ | (21 12 7) | $x^{619}= 11+12x^2$ | $\longrightarrow$ | (11 0 12) |
| $x^{620}= x^0$ | $\longrightarrow$ | (1 0 0) | | | |

Tabela B.1: Grupo das unidades de $GR(25,3)$

# APÊNDICE C

# ELEMENTOS DO GRUPO DAS UNIDADES DO ANEL $GR(27,3)$

Apresentamos a Tabela C.1 que corresponde aos elementos do grupo das unidades de GR(27,3). As operações em $GR^*(27,3)$ são realizadas módulo $(x^3 + 2x + 1)$. Logo, $x^3 = -2x - 1$, porém, como os coeficientes de $GR^*(27,3)$ estão em $\mathbb{Z}_{27}$, temos que $x^3 = 25x + 26$. Portanto, através da última igualdade encontrada, por intermédio do programa Matlab pudemos obter todos os elementos do grupo das unidades.

| | | | | | |
|---|---|---|---|---|---|
| $1 = x^0$ | $\longrightarrow$ | $(1\ \ 0\ \ 0)$ | $x = x^1$ | $\longrightarrow$ | $(0\ \ 1\ \ 0)$ |
| $x^2 = x^2$ | $\longrightarrow$ | $(0\ \ 0\ \ 1)$ | $x^3 = 26 + 25x$ | $\longrightarrow$ | $(26\ \ 25\ \ 0)$ |
| $x^4 = 26x + 25x^2$ | $\longrightarrow$ | $(0\ \ 26\ \ 25)$ | $x^5 = 2 + 4x + 26x^2$ | $\longrightarrow$ | $(2\ \ 4\ \ 26)$ |
| $x^6 = 1 + 4x + 4x^2$ | $\longrightarrow$ | $(1\ \ 4\ \ 4)$ | $x^7 = 23 + 20x + 4x^2$ | $\longrightarrow$ | $(23\ \ 20\ \ 4)$ |
| $x^8 = 23 + 15x + 20x^2$ | $\longrightarrow$ | $(23\ \ 15\ \ 20)$ | $x^9 = 7 + 10x + 15x^2$ | $\longrightarrow$ | $(7\ \ 10\ \ 15)$ |
| $x^{10} = 12 + 4x + 10x^2$ | $\longrightarrow$ | $(12\ \ 4\ \ 10)$ | $x^{11} = 17 + 19x + 4x^2$ | $\longrightarrow$ | $(17\ \ 19\ \ 4)$ |
| $x^{12} = 23 + 9x + 19x^2$ | $\longrightarrow$ | $(23\ \ 9\ \ 19)$ | $x^{13} = 8 + 12x + 9x^2$ | $\longrightarrow$ | $(8\ \ 12\ \ 9)$ |
| $x^{14} = 18 + 17x + 12x^2$ | $\longrightarrow$ | $(18\ \ 17\ \ 12)$ | $x^{15} = 15 + 21x + 17x^2$ | $\longrightarrow$ | $(15\ \ 21\ \ 17)$ |
| $x^{16} = 10 + 8x + 21x^2$ | $\longrightarrow$ | $(10\ \ 8\ \ 21)$ | $x^{17} = 6 + 22x + 8x^2$ | $\longrightarrow$ | $(6\ \ 22\ \ 8)$ |

| | | | | | |
|---|---|---|---|---|---|
| $x^{18} = 19 + 17x + 22x^2$ | $\longrightarrow$ | (19 17 22) | $x^{19} = 5 + 2x + 17x^2$ | $\longrightarrow$ | (5 2 17) |
| $x^{20} = 10 + 25x + 2x^2$ | $\longrightarrow$ | (10 25 2) | $x^{21} = 25 + 6x + 25x^2$ | $\longrightarrow$ | (2 2 6) |
| $x^{22} = 2 + 2x + 6x^2$ | $\longrightarrow$ | (2 2 6) | $x^{23} = 21 + 17x + 2x^2$ | $\longrightarrow$ | (21 17 2) |
| $x^{24} = 25 + 17x + 17x^2$ | $\longrightarrow$ | (25 17 17) | $x^{25} = 10 + 18x + 17x^2$ | $\longrightarrow$ | (10 18 17) |
| $x^{26} = 10 + 3x + 18x^2$ | $\longrightarrow$ | (10 3 18) | $x^{27} = 9 + x + 3x^2$ | $\longrightarrow$ | (9 1 3) |
| $x^{28} = 24 + 3x + x^2$ | $\longrightarrow$ | (24 3 1) | $x^{29} = 26 + 22x + 3x^2$ | $\longrightarrow$ | (26 22 3) |
| $x^{30} = 24 + 20x + 22x^2$ | $\longrightarrow$ | (24 20 22) | $x^{31} = 5 + 7x + 20x^2$ | $\longrightarrow$ | (5 7 20) |
| $x^{32} = 7 + 19x + 7x^2$ | $\longrightarrow$ | (7 19 7) | $x^{33} = 20 + 20x + 19x^2$ | $\longrightarrow$ | (20 20 19) |
| $x^{34} = 8 + 9x + 20x^2$ | $\longrightarrow$ | (8 9 20) | $x^{35} = 7 + 22x + 9x^2$ | $\longrightarrow$ | (7 22 9) |
| $x^{36} = 18 + 16x + 22x^2$ | $\longrightarrow$ | (18 16 22) | $x^{37} = 5 + x + 16x^2$ | $\longrightarrow$ | (5 1 16) |
| $x^{38} = 11 + x^2$ | $\longrightarrow$ | (11 0 1) | $x^{39} = 26 + 9x$ | $\longrightarrow$ | (26 9 0) |
| $x^{40} = 26x + 9x^2$ | $\longrightarrow$ | (0 26 9) | $x^{41} = 18 + 9x + 26^2$ | $\longrightarrow$ | (18 9 26) |
| $x^{42} = 1 + 20x + 9x^2$ | $\longrightarrow$ | (1 20 9) | $x^{43} = 18 + 10x + 20x^2$ | $\longrightarrow$ | (18 10 20) |
| $x^{44} = 7 + 5x + 10x^2$ | $\longrightarrow$ | (7 5 10) | $x^{45} = 17 + 14x + 5x^2$ | $\longrightarrow$ | (17 14 5) |
| $x^{46} = 22 + 7x + 14x^2$ | $\longrightarrow$ | (22 7 14) | $x^{47} = 13 + 21x + 7x^2$ | $\longrightarrow$ | (13 21 7) |
| $x^{48} = 20 + 26x + 21x^2$ | $\longrightarrow$ | (20 26 21) | $x^{49} = 6 + 5x + 26x^2$ | $\longrightarrow$ | (6 5 26) |
| $x^{50} = 1 + 8x + 5x^2$ | $\longrightarrow$ | (1 8 5) | $x^{51} = 22 + 18x + 8x^2$ | $\longrightarrow$ | (22 18 8) |
| $x^{52} = 19 + 6x + 18x^2$ | $\longrightarrow$ | (19 6 18) | $x^{53} = 9 + 10x + 6x^2$ | $\longrightarrow$ | (9 10 6) |
| $x^{54} = 21 + 24x + 10x^2$ | $\longrightarrow$ | (21 24 10) | $x^{55} = 17 + x + 24x^2$ | $\longrightarrow$ | (17 1 24) |
| $x^{56} = 3 + 23x + x^2$ | $\longrightarrow$ | (3 23 1) | $x^{57} = 26 + x + 23x^2$ | $\longrightarrow$ | (26 1 23) |
| $x^{58} = 4 + 7x + x^2$ | $\longrightarrow$ | (4 7 1) | $x^{59} = 26 + 2x + 7x^2$ | $\longrightarrow$ | (26 2 7) |
| $x^{60} = 20 + 12x + 2x^2$ | $\longrightarrow$ | (20 12 2) | $x^{61} = 25 + 16x + 12x^2$ | $\longrightarrow$ | (25 16 12) |
| $x^{62} = 15 + x + 16x^2$ | $\longrightarrow$ | (15 1 16) | $x^{63} = 11 + 10x + x^2$ | $\longrightarrow$ | (11 10 1) |
| $x^{64} = 26 + 9x + 10x^2$ | $\longrightarrow$ | (26 9 10) | $x^{65} = 17 + 6x + 9x^2$ | $\longrightarrow$ | (17 6 9) |
| $x^{66} = 18 + 26x + 6x^2$ | $\longrightarrow$ | (18 26 6) | $x^{67} = 21 + 6x + 26x^2$ | $\longrightarrow$ | (21 6 26) |
| $x^{68} = 1 + 23x + 6x^2$ | $\longrightarrow$ | (1 23 6) | $x^{69} = 21 + 16x + 23x^2$ | $\longrightarrow$ | (21 16 23) |
| $x^{70} = 4 + 2x + 16x^2$ | $\longrightarrow$ | (4 2 16) | $x^{71} = 11 + 26x + 2x^2$ | $\longrightarrow$ | (11 26 2) |
| $x^{72} = 25 + 7x + 26x^2$ | $\longrightarrow$ | (25 7 26) | $x^{73} = 1 + 7x^2$ | $\longrightarrow$ | (1 0 7) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{74}= 20 + 14x$ | $\longrightarrow$ | (20 14 0) | $x^{75} = 20x + 14x^2$ | $\longrightarrow$ | (0 20 14) |
| $x^{76} = 13 + 26x + 20x^2$ | $\longrightarrow$ | (13 26 20) | $x^{77} = 7 + 26x^2$ | $\longrightarrow$ | (7 0 26) |
| $x^{78} = 1 + 9x$ | $\longrightarrow$ | (1 9 0) | $x^{79}= x + 9x^2$ | $\longrightarrow$ | (0 1 9) |
| $x^{80} = 18 + 9x + x^2$ | $\longrightarrow$ | (18 9 1) | $x^{81}= 26 + 16x + 9x^2$ | $\longrightarrow$ | (26 16 9) |
| $x^{82} = 18 + 8x + 16x^2$ | $\longrightarrow$ | (18 8 16) | $x^{83} = 11 + 13x + 8x^2$ | $\longrightarrow$ | (11 13 8) |
| $x^{84} = 19 + 22x + 13x^2$ | $\longrightarrow$ | (19 22 13) | $x^{85} = 14 + 20x + 22x^2$ | $\longrightarrow$ | (14 20 22) |
| $x^{86}= 5 + 24x + 20x^2$ | $\longrightarrow$ | (5 24 20) | $x^{87} = 7 + 19x + 24x^2$ | $\longrightarrow$ | (7 19 24) |
| $x^{88}= 3 + 13x + 19x^2$ | $\longrightarrow$ | (3 13 19) | $x^{89} = 8 + 19x + 13x^2$ | $\longrightarrow$ | (8 19 13) |
| $x^{90} = 14 + 9x + 19x^2$ | $\longrightarrow$ | (14 9 19) | $x^{91} = 8 + 3x + 9x^2$ | $\longrightarrow$ | (8 3 9) |
| $x^{92} = 18 + 17x + 3x^2$ | $\longrightarrow$ | (18 17 3) | $x^{93} = 24 + 12x + 17x^2$ | $\longrightarrow$ | (24 12 17) |
| $x^{94} = 10 + 17x + 12x^2$ | $\longrightarrow$ | (10 17 12) | $x^{95}= 15 + 13x + 17x^2$ | $\longrightarrow$ | (15 13 17) |
| $x^{96} = 10 + 8x + 13x^2$ | $\longrightarrow$ | (10 8 13) | $x^{97}= 14 + 11x + 8x^2$ | $\longrightarrow$ | (14 11 8) |
| $x^{98} = 19 + 25x + 11x^2$ | $\longrightarrow$ | (19 25 11) | $x^{99} = 16 + 24x + 25x^2$ | $\longrightarrow$ | (16 24 25) |
| $x^{100} = 2 + 20x + 24x^2$ | $\longrightarrow$ | (2 20 24) | $x^{101} = 3 + 8x + 20x^2$ | $\longrightarrow$ | (3 8 20) |
| $x^{102}= 7 + 17x + 8x^2$ | $\longrightarrow$ | (7 17 8) | $x^{103} = 19 + 18x + 17x^2$ | $\longrightarrow$ | (19 18 17) |
| $x^{104}= 10 + 12x + 8x^2$ | $\longrightarrow$ | (10 12 8) | $x^{105} = 9 + x + 12x^2$ | $\longrightarrow$ | (9 1 12) |
| $x^{106} = 12x + 15x^2$ | $\longrightarrow$ | (0 12 15) | $x^{107} = 26 + 13x + 12x^2$ | $\longrightarrow$ | (26 13 12) |
| $x^{108} = 15 + 2x + 13x^2$ | $\longrightarrow$ | (15 2 13) | $x^{109} = 14 + 16x + 2x^2$ | $\longrightarrow$ | (14 16 2) |
| $x^{110} = 25 + 10x + 16x^2$ | $\longrightarrow$ | (25 10 16) | $x^{111} = 11 + 20x + 10x^2$ | $\longrightarrow$ | (11 20 10) |
| $x^{112} = 17 + 18x + 20x^2$ | $\longrightarrow$ | (17 18 20) | $x^{113} = 7 + 4x + 18x^2$ | $\longrightarrow$ | (7 4 18) |
| $x^{114} = 9 + 25x + 4x^2$ | $\longrightarrow$ | (9 25 4) | $x^{115} = 23 + x + 25x^2$ | $\longrightarrow$ | (23 1 25) |
| $x^{116} = 2 + x^2$ | $\longrightarrow$ | (2 0 1) | $x^{117} = 26$ | $\longrightarrow$ | (26 0 0) |
| $x^{118} = 26x$ | $\longrightarrow$ | (0 26 0) | $x^{119} = 26x^2$ | $\longrightarrow$ | (0 0 26) |
| $x^{120} = 1 + 2x$ | $\longrightarrow$ | (1 2 0) | $x^{121} = x + 2x^2$ | $\longrightarrow$ | (0 1 2) |
| $x^{122} = 25 + 23x + x^2$ | $\longrightarrow$ | (25 23 1) | $x^{123} = 26 + 23x + 23^2$ | $\longrightarrow$ | (26 23 23) |
| $x^{124} = 4 + 7x + 23x^2$ | $\longrightarrow$ | (4 7 23) | $x^{125} = 4 + 12x + 7x^2$ | $\longrightarrow$ | (4 12 7) |
| $x^{126} = 20 + 17x + 12x^2$ | $\longrightarrow$ | (20 17 12) | $x^{127} = 15 + 23x + 17x^2$ | $\longrightarrow$ | (15 23 17) |
| $x^{128} = 10 + 8x + 23x^2$ | $\longrightarrow$ | (10 8 23) | $x^{129} = 4 + 18x + 8x^2$ | $\longrightarrow$ | (4 18 8) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{130} = 19 + 15x + 18x^2$ | $\longrightarrow$ | (19 15 18) | $x^{131} = 9 + 10x + 15x^2$ | $\longrightarrow$ | (9 10 15) |
| $x^{132} = 12 + 6x + 10x^2$ | $\longrightarrow$ | (12 6 10) | $x^{133} = 17 + 19x + 6x^2$ | $\longrightarrow$ | (17 19 6) |
| $x^{134} = 21 + 5x + 19x^2$ | $\longrightarrow$ | (21 5 19) | $x^{135} = 8 + 10x + 5x^2$ | $\longrightarrow$ | (8 10 5) |
| $x^{136} = 22 + 25x + 10x^2$ | $\longrightarrow$ | (22 25 10) | $x^{137} = 17 + 2x + 25x^2$ | $\longrightarrow$ | (17 2 25) |
| $x^{138} = 2 + 21x + 2x^2$ | $\longrightarrow$ | (2 21 2) | $x^{139} = 25 + 25x + 21x^2$ | $\longrightarrow$ | (25 25 21) |
| $x^{140} = 6 + 10x + 25x^2$ | $\longrightarrow$ | (6 10 25) | $x^{141} = 2 + 10x + 10x^2$ | $\longrightarrow$ | (2 10 10) |
| $x^{142} = 17 + 9x + 10x^2$ | $\longrightarrow$ | (17 9 10) | $x^{143} = 17 + 24x + 9x^2$ | $\longrightarrow$ | (17 24 9) |
| $x^{144} = 18 + 26x + 24x^2$ | $\longrightarrow$ | (18 26 24) | $x^{145} = 3 + 24x + 26x^2$ | $\longrightarrow$ | (3 24 26) |
| $x^{146} = 1 + 5x + 24x^2$ | $\longrightarrow$ | (1 5 24) | $x^{147} = 3 + 7x + 5x^2$ | $\longrightarrow$ | (3 7 5) |
| $x^{148} = 22 + 20x + 7x^2$ | $\longrightarrow$ | (22 20 7) | $x^{149} = 20 + 8x + 20x^2$ | $\longrightarrow$ | (20 8 20) |
| $x^{150} = 7 + 7x + 8x^2$ | $\longrightarrow$ | (7 7 8) | $x^{151} = 19 + 18x + 7x^2$ | $\longrightarrow$ | (19 18 7) |
| $x^{152} = 20 + 5x + 18x^2$ | $\longrightarrow$ | (20 5 18) | $x^{153} = 9 + 11x + 5x^2$ | $\longrightarrow$ | (9 11 5) |
| $x^{154} = 22 + 26x + 11x^2$ | $\longrightarrow$ | (22 26 11) | $x^{155} = 16 + 26x^2$ | $\longrightarrow$ | (16 0 26) |
| $x^{156} = 1 + 18x$ | $\longrightarrow$ | (1 18 0) | $x^{157} = x + 18x^2$ | $\longrightarrow$ | (0 1 18) |
| $x^{158} = 9 + 18x + x^2$ | $\longrightarrow$ | (9 18 1) | $x^{159} = 26 + 7x + 18x^2$ | $\longrightarrow$ | (26 7 18) |
| $x^{160} = 9 + 17x + 7x^2$ | $\longrightarrow$ | (9 17 7) | $x^{161} = 20 + 22x + 17x^2$ | $\longrightarrow$ | (20 22 17) |
| $x^{162} = 10 + 13x + 22x^2$ | $\longrightarrow$ | (10 13 22) | $x^{163} = 5 + 20x + 13x^2$ | $\longrightarrow$ | (5 20 13) |
| $x^{164} = 14 + 6x + 20x^2$ | $\longrightarrow$ | (14 6 20) | $x^{165} = 7 + x + 6x^2$ | $\longrightarrow$ | (7 1 6) |
| $x^{166} = 21 + 22x + x^2$ | $\longrightarrow$ | (21 22 1) | $x^{167} = 26 + 19x + 22x^2$ | $\longrightarrow$ | (26 19 22) |
| $x^{168} = 5 + 9x + 19x^2$ | $\longrightarrow$ | (5 9 19) | $x^{169} = 8 + 21x + 9x^2$ | $\longrightarrow$ | (8 21 9) |
| $x^{170} = 18 + 17x + 21x^2$ | $\longrightarrow$ | (18 17 21) | $x^{171} = 6 + 3x + 17^2$ | $\longrightarrow$ | (6 3 17) |
| $x^{172} = 10 + 26x + 3x^2$ | $\longrightarrow$ | (10 26 3) | $x^{173} = 24 + 4x + 26x^2$ | $\longrightarrow$ | (24 4 26) |
| $x^{174} = 1 + 26x + 4x^2$ | $\longrightarrow$ | (1 26 4) | $x^{175} = 23 + 20x + 26x^2$ | $\longrightarrow$ | (23 20 26) |
| $x^{176} = 1 + 25x + 20x^2$ | $\longrightarrow$ | (1 25 20) | $x^{177} = 7 + 15x + 25x^2$ | $\longrightarrow$ | (7 15 25) |
| $x^{178} = 2 + 11x + 15x^2$ | $\longrightarrow$ | (2 11 15) | $x^{179} = 12 + 26x + 11x^2$ | $\longrightarrow$ | (12 26 11) |
| $x^{180} = 16 + 17x + 26x^2$ | $\longrightarrow$ | (16 17 26) | $x^{181} = 1 + 18x + 17x^2$ | $\longrightarrow$ | (1 18 17) |
| $x^{182} = 10 + 21x + 18x^2$ | $\longrightarrow$ | (10 21 18) | $x^{183} = 9 + x + 21x^2$ | $\longrightarrow$ | (9 1 21) |
| $x^{184} = 6 + 21x + x^2$ | $\longrightarrow$ | (6 21 1) | $x^{185} = 26 + 4x + 21x^2$ | $\longrightarrow$ | (26 4 21) |

| | | | | | |
|---|---|---|---|---|---|
| $x^{186} = 6 + 11x + 4x^2$ | $\longrightarrow$ | (6 11 4) | $x^{187} = 23 + 25x + 11x^2$ | $\longrightarrow$ | (23 25 11) |
| $x^{188} = 16 + x + 25x^2$ | $\longrightarrow$ | (16 1 25) | $x^{189} = 2 + 20x + x^2$ | $\longrightarrow$ | (2 20 1) |
| $x^{190} = 26 + 20x^2$ | $\longrightarrow$ | (26 0 20) | $x^{191} = 7 + 13x$ | $\longrightarrow$ | (7 13 0) |
| $x^{192} = 7x + 13x^2$ | $\longrightarrow$ | (7 0 13) | $x^{193} = 14 + x + 7x^2$ | $\longrightarrow$ | (14 1 7) |
| $x^{194} = 20 + x^2$ | $\longrightarrow$ | (20 0 1) | $x^{195} = 26 + 18x$ | $\longrightarrow$ | (26 18 0) |
| $x^{196} = 26x + 18x^2$ | $\longrightarrow$ | (0 26 18) | $x^{197} = 9 + 18x + 26x^2$ | $\longrightarrow$ | (9 18 26) |
| $x^{198} = 1 + 11x + 18x^2$ | $\longrightarrow$ | (1 11 18) | $x^{199} = 9 + 19x + 11x^2$ | $\longrightarrow$ | (9 19 11) |
| $x^{200} = 16 + 14x + 19x^2$ | $\longrightarrow$ | (16 14 19) | $x^{201} = 8 + 5x + 14x^2$ | $\longrightarrow$ | (8 5 14) |
| $x^{202} = 13 + 7x + 5x^2$ | $\longrightarrow$ | (13 7 5) | $x^{203} = 22 + 3x + 7x^2$ | $\longrightarrow$ | (22 3 7) |
| $x^{204} = 20 + 8x + 3x^2$ | $\longrightarrow$ | (20 8 3) | $x^{205} = 24 + 14x + 8x^2$ | $\longrightarrow$ | (24 14 8) |
| $x^{206} = 19 + 8x + 14x^2$ | $\longrightarrow$ | (19 8 14) | $x^{207} = 13 + 18x + 8x^2$ | $\longrightarrow$ | (13 18 8) |
| $x^{208} = 19 + 24x + 18x^2$ | $\longrightarrow$ | (19 24 18) | $x^{209} = 9 + 10x + 24x^2$ | $\longrightarrow$ | (9 10 24) |
| $x^{210} = 3 + 15x + 10x^2$ | $\longrightarrow$ | (3 15 10) | $x^{211} = 17 + 10x + 15x^2$ | $\longrightarrow$ | (17 10 15) |
| $x^{212} = 12 + 14x + 10x^2$ | $\longrightarrow$ | (12 14 10) | $x^{213} = 17 + 19x + 14x^2$ | $\longrightarrow$ | (17 19 14) |
| $x^{214} = 13 + 16x + 19x^2$ | $\longrightarrow$ | (13 16 19) | $x^{215} = 8 + 2x + 16x^2$ | $\longrightarrow$ | (8 2 16) |
| $x^{216} = 11 + 3x + 2x^2$ | $\longrightarrow$ | (11 3 2) | $x^{217} = 25 + 7x + 3x^2$ | $\longrightarrow$ | (25 7 3) |
| $x^{218} = 24 + 19x + 7x^2$ | $\longrightarrow$ | (24 19 7) | $x^{219} = 20 + 10x + 19x^2$ | $\longrightarrow$ | (20 10 19) |
| $x^{220} = 8 + 9x + 10x^2$ | $\longrightarrow$ | (8 9 10) | $x^{221} = 17 + 15x + 9x^2$ | $\longrightarrow$ | (17 15 9) |
| $x^{222} = 18 + 26x + 15x^2$ | $\longrightarrow$ | (18 26 15) | $x^{223} = 12 + 15x + 26x^2$ | $\longrightarrow$ | (12 15 26) |
| $x^{224} = 1 + 14x + 15x^2$ | $\longrightarrow$ | (1 14 15) | $x^{225} = 12 + 25x + 14x^2$ | $\longrightarrow$ | (12 25 14) |
| $x^{226} = 13 + 11x + 25x^2$ | $\longrightarrow$ | (13 11 25) | $x^{227} = 2 + 17x + 11x^2$ | $\longrightarrow$ | (2 17 11) |
| $x^{228} = 16 + 7x + 17x^2$ | $\longrightarrow$ | (16 7 17) | $x^{229} = 10 + 9x + 7x^2$ | $\longrightarrow$ | (10 9 7) |
| $x^{230} = 20 + 23x + 9x^2$ | $\longrightarrow$ | (20 23 9) | $x^{231} = 18 + 2x + 23x^2$ | $\longrightarrow$ | (18 2 23) |
| $x^{232} = 4 + 26x + 2x^2$ | $\longrightarrow$ | (4 26 2) | $x^{233} = 25 + 26x^2$ | $\longrightarrow$ | (25 0 26) |
| $x^{234} = x^0$ | $\longrightarrow$ | (1 0 0) | | | |

Tabela C.1: Grupo das Unidades de $GR(27, 3)$

# REFERÊNCIAS BIBLIOGRÁFICAS


[1] A. A. Andrade, R. Palazzo Jr., "Decoding of BCH and alternant codes by using Fourier transform in a Galois ring", *Int. J. Applied Mathematics*, Vol. 16, N. 1, pp. 69-83, 2004.

[2] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, Owego, NY, 1984.

[3] J. C. Interlando, *Uma Contribuição a Construção e Decodificação de Códigos Lineares sobre Grupos Abelianos via Concatenação de Códigos sobre Anéis Inteiros Residuais*, Tese de Doutorado, FEEC-UNICAMP, 1994.

[4] P. de R. Barbosa, *Construções de Códigos $\mathbb{Z}_{2^k}-$pseudo-lineares através de Aplicações Isométricas e Extensões de Galois sobre Anéis Locais*, Dissertação de Mestrado, FEEC-UNICAMP, 2000.

[5] B. R. McDonald, *Finite Rings With Identity*, Departament of Mathematics, University of Oklahoma, Norman Oklahoma,Marcel Dekker, New York, 1974.

[6] H. H. Domingues, G. Iezzi, *Álgebra Moderna*, Atual Editora Ltda, 1982.

[7] A. A. Andrade, R. Palazzo Jr., "A note on units of a local finite rings", *Revista de Matemática e Estatística*, Vol. 18, pp. 213-222, 2000.

[8] A. A. Andrade, R. Palazzo Jr. , J. C. Interlando, "Alternat and BCH codes over certain rings", *Computational and Applied Mathematics*, Vol. 22, N. 2, pp. 233-247, 2003.

[9] A. A. Andrade, R., Palazzo,“ Construction and decoding of BCH codes over finite commutative rings”, *Linear Algebra its Applications*, Vol. 286, pp. 69-85, 1999.

[10] A. A., Andrade, *Uma Contribuição à Construção e Decodificação de Códigos de Bloco Lineares sobre Anéis Finitos*, Tese de Doutorado, FEEC-UNICAMP, Campinas 1996.

[11] S. Lin, D. J. Costello Jr., *Error Control Coding: Fundamentals and Aplications*, Prentice -Hall, Inc., 1983.

[12] J. B. Fraleigh, *A First Course in Abstract Álgebra*, Addison-Wesley Publishing Co., 1989.

[13] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland Publishing Company, 1997.

[14] J. L. Massey, “Shift-register synthesis and BCH decoding”, *IEEE Trans. Inform. Theory*, Vol. IT-15, pp. 122-127, January 1969.

[15] R. Palazzo Jr., J. C. Interlando, J. R. Gerônimo, A. A. Andrade, O. M. Favareto, T. P. Nóbrega Neto, M. C. Araújo e G. O. Santos, *Fundamentos Algébricos e Geométricos dos Códigos Corretores de Erros*, DT-FEEC-UNICAMP, 2003.

[16] P. Shankar, “On BCH codes over arbitrary integer rings”, *IEEE Trans. Inform. Theory*, Vol. IT-25, pp. 480-483, July 1979.

[17] R. D. Valença, *Métodos para a Construção de Códigos Espaço-temporais sobre Grupos, Corpos e Anéis para Canais com Desvanecimento Quasi-estático e Plano*, Dissertação de Mestrado, FEEC-UNICAMP, 2001.

[18] A. Hefez *Curso de Álgebra*, Volume 1, Terceira edição, IMPA, Rio de Janeiro, 2002.

[19] A. Hefez, M. L. T. Vilela, *Còdigos Corretores de Erros*, Primeira edição, IMPA, Rio de Janeiro, 2002.