UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE TELEMÁTICA

Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares através de Aplicações Isométricas e Extensões de Galois sobre Anéis Locais

Patricia de Rezende Barbosa
Engenheira de Computação - FEEC/UNICAMP

Prof. Dr. Reginaldo Palazzo Jr.
Orientador

UNICAMP
BIBLIOTECA CENTRA
SEÇÃO CIRCULANTE

Banca Examinadora:
Prof. Dr. Reginaldo Palazzo Jr. - FEEC/UNICAMP
Prof^a. Dr^a. Shirlei Serconeck - IME/UFG
Prof. Dr. Marcelo Firer - IMECC/UNICAMP
Prof. Dr. Walter da Cunha Borelli - FEEC/UNICAMP

Dissertação de Mestrado apresentada à comissão de pós-graduação da Faculdade de Engenharia Elétrica e de Computação - FEEC/UNICAMP, como requisito parcial para obtenção do título de MESTRE EM ENGENHARIA ELÉTRICA.

Julho - 2000

Campinas - SP

Este exemplar corresponde à redação final da tese defendida por Patricia de Rezende Barbosa e aprovada pela Comissão Julgadora em
Reginaldo Palazzo Júnior
Orientador

UNICAMP

UNIDADE BC
N.º CHAMADA:
Unicamp
B234c
V. Ex.
TOMBO BC/ 42988
PROC. 16-27810-00
C [ ] D [X]
PREÇO R$ 11,00
DATA 04/11/00
N.º CPD

CM-00147150-1

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

Barbosa, Patricia de Rezende

B234c Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares através de Aplicações Isométricas e Extensões de Galois sobre Anéis Locais/ Patricia de Rezende Barbosa. –Campinas, SP: [s.n.], 2000.

Orientador: Reginaldo Palazzo Jr.

Dissertação (Mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Códigos de controle de erros (Teoria da informação). 2. Teoria da codificação. 3. Teoria dos grupos. I. Palazzo Jr., Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Agradecimentos[1]

Em primeiro lugar, ao Prof. Dr. Reginaldo Palazzo Jr., pela oportunidade de desenvolver este trabalho. Seu entusiasmo e domínio do assunto serviram de estímulo para mim. Sempre atencioso e paciente, sua orientação foi indispensável durante todo o processo. Agradeço, mais uma vez, pelas inúmeras portas abertas.

Aos membros da Banca Examinadora: Profs. Drs. Shirlei Serconeck, Marcelo Firer e Walter da Cunha Borelli, pela leitura e sugestões que levaram ao enriquecimento deste trabalho.

Aos meus pais, pelo constante apoio e compreensão.

A todos meus amigos, que souberam compreender minhas ausências e sempre me deram a força necessária para seguir em frente.

[1]**Este trabalho foi financiado pelo Centro de Apoio à Pesquisa e Eduacação Superior - CAPES**

Resumo

Neste trabalho apresentamos um procedimento para a determinação de aplicações casadas isométricas entre os espaços métricos de Lee e de Hamming. Este procedimento faz uso dos conceitos de particionamento de conjuntos e representação modular. A partir destas aplicações isométricas, apresentamos uma proposta de construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através dos códigos cíclicos provenientes da extensão de Galois de dimensão r sobre anéis locais.

Abstract

In this research we present a technique to determine matched isometric applications between Lee and Hamming metric spaces. This procedure is based on the concepts of set partitioning and modular representation. Once these applications are known, we show the construction of $\mathbb{Z}_{2^k}$-pseudolinear codes using cyclic codes which lie in a Galois extension of dimension r over local rings.

Lista de Símbolos

$*$	Operação binária sobre um conjunto
$\lvert\cdot\rvert$	Ordem de um conjunto
$\lVert\cdot\rVert$	Norma euclidiana
$\times$	Produto direto de grupos
$\times_{\varphi}$	Produto semi-direto de grupos
$\langle a \rangle$	Subgrupo gerado por a
$\overline{a}$	Classe de equivalência
$\overline{\mathrm{A}}$	Operação lógica de negação dos elementos da matriz A
$\langle p(x) \rangle$	Anel gerado pelo polinômio $p(x)$
$\overline{x}$	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
$G \cong G'$	Isomorfismo entre os grupos G e G'
α	Raiz de um polinômio
β	Elemento primitivo ou zero de um polinômio pertencente a F_q
η	Vetor localizador de um código BCH ou alternante
μ	Mapeamento casado
$\phi,\ \varphi$	Funções
$\Gamma(\cdot)$	Grupo de simetrias de um conjunto
$\mathcal{A}$	Alfabeto de um código
A	Submatriz de ordem $\lfloor n/2 \rfloor$ da matriz C_n

a^{-1}	Elemento inverso de a em um grupo
$Aut\,(G)$	Automorfismo do grupo G
$c_{i,j}$	Elemento da linha i e coluna j da matriz C
$\mathcal{C}$	Código
$\mathbb{C}$	Conjunto dos números complexos
C	Matriz utilizada na determinação da representação modular
C_n	Matriz C de ordem n
d	Métrica definida sobre um conjunto
d_{BV}	Melhor distância dos códigos binários lineares, [9]
d_H	Distância de Hamming
d_L	Distância de Lee
$d_{\min}$	Distância mínima de um código
$\mathbb{D}_n$	Grupo diedral com $2n$ elementos
e	Elemento identidade em um grupo
f	Elemento de $GR^*\left(p^k, r\right)$
E	Extensão de grau r de um corpo finito F_q
$\overline{f}$	Redução de f módulo 2
F	Corpo
G	Matriz geradora de um código
G	Grupo
$GF\,(q)$, F_q	Corpo algébrico de Galois ou corpo de Galois
$GF\,(q)\,[x]$, $F_q\,[x]$	Anel de polinômios sobre $GF\,(q)$
G_n	Subgrupo cíclico do grupo multiplicativo R^*
$GR\,(q,r)$	Extensão do anel de Galois de grau r
$GR^*\,(q,r)$	Grupo das unidades de $GR\left(p^k, r\right)$
$g\,(x)$	Polinômio gerador de um código
H	Subgrupo de um grupo
H	Matriz verificação de paridade
$\mathcal{I}$	Conjunto de índices de um código
I	Matriz identidade

J	Matriz com todos elementos iguais a 1
K	Matriz cujas linhas são todas as palavras de um código de bloco
k	Dimensão de um código
k'	Dimensão do código sobre $\mathbb{Z}_2^{2^{k-1}}$
(M,d)	Espaço métrico
$mdc(\cdot,\cdot)$	Máximo divisor comum
$m_i(x)$	Polinômio minimal associado ao elemento β^i sobre $GF(q)$
$M_i(x)$	Polinômio minimal associado ao elemento β^i sobre R^*
m_k	Aplicação casada isométrica entre $\mathbb{Z}_{2^k}$ e $\mathbb{Z}_2^{2^{k-1}}$
$mmc(\cdot,\cdot)$	Mínimo múltiplo comum
n	Comprimento de um código
n'	Comprimento do código sobre $\mathbb{Z}_2^{2^{k-1}}$
N	Vetor representação modular
Q	Subanel de um anel
$\mathbb{Q}$	Conjunto dos números racionais
r_C	Taxa de um código
r	Grau da extensão de Galois
$\mathbb{R}$	Conjunto dos números reais
R	Anel
R^*	Grupo das unidades de R
R_Q	Anel quociente de R módulo um subanel Q
$\mathbb{R}^n$	Espaço euclidiano n-dimensional
$R_p(f)$	Redução de f módulo p
S, M	Conjuntos
S_n	Grupo das permutações de um conjunto finito de n elementos
$\mathcal{S}$	Conjunto de sinais
t	Capacidade de correção de erros de um código
T	Matriz de transformação
u, v	Isometrias
$\underline{u}$	Informação a ser codificada

$U(\mathcal{S})$	Grupo gerador mínimo da figura geométrica $\mathcal{S}$
$\underline{v}$	Palavra-código
$\mathcal{V}$	Região de Voronoi
w	Vetor de elementos de G_n
w_H	Peso de Hamming
w_L	Peso de Lee
W	Vetor espectro de pesos
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Z}_n$	Conjunto dos números inteiros módulo n

Lista de Tabelas

3.1 Aplicação $m_2' : \mathbb{Z}_4^2 \to \mathbb{Z}_2^4$ 40
3.2 Aplicação $m_2 : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ 40
3.3 Aplicação $m_3 : \mathbb{Z}_8 \to \mathbb{Z}_2^4$ 42
3.4 Aplicação $m_4 : \mathbb{Z}_{16} \to \mathbb{Z}_2^8$ 44
3.5 Aplicação $m_5 : \mathbb{Z}_{32} \to \mathbb{Z}_2^{16}$ 51
3.6 Aplicação $m_6 : \mathbb{Z}_{64} \to \mathbb{Z}_2^{32}$ 52
3.7 Aplicação $m_6 : \mathbb{Z}_{64} \to \mathbb{Z}_2^{32}$ (cont.) 53
3.8 Tabela contendo as representações modulares 54
3.9 Tabela das aplicações isométricas 54

4.1 Elementos de F_4 66
4.2 Elementos de $GR^*(4,2)$ 67
4.3 Elementos de F_8 68
4.4 Elementos de $GR^*(4,3)$ 69
4.5 Elementos de F_{16} 71
4.6 Elementos de $GR^*(4,4)$ 71
4.7 Elementos de $GR^*(8,2)$ 74
4.8 Elementos de $GR^*(8,3)$ 75
4.9 Elementos de $GR^*(16,2)$ 77
4.10 Elementos de $GR^*(32,2)$ 78
4.11 Elementos de $GR^*(64,2)$ 80
4.12 Palavras-código em $\mathbb{Z}_4$ 87

4.13 Espectro de pesos em $\mathbb{Z}_4$ 88
4.14 Palavras-código em $\mathbb{Z}_2^2$ 88
4.15 Espectro de pesos em $\mathbb{Z}_2^2$ 88
4.16 Códigos $\mathbb{Z}_{2^k}$-pseudolineares a partir de códigos BCH 91
4.17 Códigos $\mathbb{Z}_{2^k}$-pseudolineares a partir de códigos BCH duais 91
4.18 Códigos $\mathbb{Z}_{2^k}$-pseudolineares a partir de códigos alternantes 92

Lista de Figuras

3-1 Arranjo $\mathbb{Z}_4 \times \mathbb{Z}_4$ com seus respectivos pares ordenados 33

3-2 Arranjo $\mathbb{Z}_8 \times \mathbb{Z}_8$ com seus respectivos pares ordenados 41

3-3 Arranjo $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ com seus respectivos pares ordenados 43

3-4 Arranjo $\mathbb{Z}_{32} \times \mathbb{Z}_{32}$ com seus respectivos pares ordenados 45

3-5 Regiões de Voronoi para um canal sem memória 47

3-6 Regiões de Voronoi para um canal com memória 48

Conteúdo

1 Introdução **1**

1.1 Histórico 1

1.2 Apresentação do Problema 2

1.3 Descrição do Trabalho 3

2 Álgebra e Códigos **5**

2.1 Introdução 5

2.2 Estruturas Algébricas 6

2.2.1 Grupos 6

2.2.2 Anéis 11

2.2.3 Corpos 15

2.3 Espaços Métricos 17

2.3.1 Isometrias 19

2.4 Códigos 22

2.4.1 Conjuntos de Sinais Casados a Grupos 25

2.4.2 Códigos Geometricamente Uniformes 26

2.5 Conclusão 27

3 Aplicações Casadas Isométricas **29**

3.1 Introdução 29

3.2 Recobrimento de Regiões $\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$ 30

3.3 Representação Modular 33
3.4 Aplicações Casadas Isométricas: Análise de Casos 38
3.4.1 O Caso $\mathbb{Z}_4$ 39
3.4.2 O Caso $\mathbb{Z}_8$ 40
3.4.3 O Caso $\mathbb{Z}_{16}$ 42
3.4.4 O Caso $\mathbb{Z}_{32}$ 44
3.4.5 O Caso $\mathbb{Z}_{64}$ 46
3.5 Conclusão 48

4 Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares **55**
4.1 Introdução 55
4.2 Códigos Cíclicos sobre Anéis de Inteiros Residuais 56
4.3 Extensão de Anéis de Galois 59
4.4 Códigos BCH sobre Anéis 62
4.4.1 Construção de Códigos BCH sobre Anéis: Exemplos 65
4.4.2 Códigos Alternantes 80
4.5 Códigos $\mathbb{Z}_{2^k}$-pseudolineares 86
4.6 Conclusão 90

5 Conclusões **93**
5.1 Contribuições 93
5.2 Propostas para Trabalhos Futuros 94

Bibliografia **96**

Capítulo 1

Introdução

UNICAMP
BIBLIOTECA CENTRAL
SEÇÃO CIRCULANTE

1.1 Histórico

A $\mathbb{Z}_4$-linearidade proposta por Hammons *et al.* em [19] foi um marco na teoria da codificação, transformando completamente o estudo dos códigos cíclicos. Podemos definir a $\mathbb{Z}_4$-linearidade como uma técnica eficiente de construção de códigos binários não-lineares com uma particularidade: estes códigos binários não lineares são tratados como imagens binárias de códigos lineares cíclicos estendidos sobre $\mathbb{Z}_4$. Esta característica faz com que a complexidade dos processos de decodificação dos códigos não lineares seja significativamente reduzida.

Outra característica importante dos códigos $\mathbb{Z}_4$-lineares é o fato de serem códigos geometricamente uniformes, ou seja, são gerados por códigos de grupo sobre um grupo de simetrias. O conceito de uniformidade geométrica foi introduzido por Forney em [13] e passou a ser uma constante dentre as características buscadas na construção de "bons" códigos.

Portanto, podemos dizer que a $\mathbb{Z}_4$-linearidade em muito contribuiu para a inserção dos códigos não lineares no contexto da transmissão da informação, bem como no estudo das características lineares inerentes a tais códigos. Assim, passou a ser possível unir as principais vantagens de duas classes de códigos: a estrutura algébrica bem definida dos

códigos lineares e a possibilidade de encontrarmos códigos não lineares com distâncias de Hamming mínimas superiores a dos correspondentes códigos lineares.

Com relação à inserção dos códigos não lineares no processo de transmissão da informação, Gerônimo *et al.* em [18] mostraram a não existência de códigos $\mathbb{Z}_{2^k}$-lineares ($k > 2$), independentemente da métrica utilizada em $\mathbb{Z}_{2^k}$, pois o grupo de simetrias de $\mathbb{Z}_2^k$ não possui um subgrupo de ordem 2^k cuja ação seja fortemente transitiva sobre $\mathbb{Z}_2^k$. Isto é, não é possível encontrar uma aplicação bijetora $m_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k$, tal que os espaços métricos de Lee $(\mathbb{Z}_{2^k}, d_L)$ e de Hamming $(\mathbb{Z}_2^k, d_H)$ sejam isométricos.

Assim, passou-se a buscar aplicações que satisfizessem esses critérios e nessa direção, em [26], Palazzo *et al.* mostraram que se a aplicação for injetora, é possível obter o casamento e a isometria entre os espaços métricos considerados. Surge então uma nova classe de códigos: os códigos $\mathbb{Z}_{2^k}$-pseudolineares.

É neste contexto que se insere o presente trabalho.

1.2 Apresentação do Problema

Diante da impossibilidade de se determinar códigos $\mathbb{Z}_{2^k}$-lineares ($k > 2$), voltamos nossa atenção para os códigos $\mathbb{Z}_{2^k}$-pseudolineares.

A pergunta que se faz agora é a seguinte: para quais aplicações injetoras as propriedades de casamento e isometria entre os espaços métricos de Lee e de Hamming são satisfeitas?

A principal motivação por trás desta pergunta é a de estabelecer novas classes de códigos binários não lineares que sejam melhores, em termos de distância de Hamming mínima, do que os correspondentes códigos lineares.

Carlet em [11] propôs uma generalização do mapeamento Gray através de funções Booleanas para construção de códigos binários não lineares a partir de códigos sobre $\mathbb{Z}_{2^k}$. Contudo, seu trabalho mostra que, para $k > 3$, o procedimento adotado passa a não ser válido, ou seja, não é possível encontrar uma aplicação $m_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^{2^{k-1}}$ isométrica

para $k > 3$ através de uma generalização do mapeamento Gray. Nosso objetivo, o qual é atingido, é mostrar ser possível encontrar tais aplicações para qualquer valor de k, porém através de outro método, utilizando os conceitos de particionamento de conjuntos e representação modular. Embora nossos resultados possam ser estendidos para qualquer valor de k, trabalhamos com valores de k no intervalo $2 \leq k \leq 6$ para efeito de cálculos computacionais.

Determinadas as aplicações casadas isométricas, desejamos então construir códigos $\mathbb{Z}_{2^k}$-pseudolineares através dos códigos cíclicos BCH provenientes da extensão de Galois de dimensão r sobre $\mathbb{Z}_{2^k}$, em busca de novas classes de códigos binários não lineares.

1.3 Descrição do Trabalho

Esta dissertação encontra-se dividida em cinco capítulos. Os próximos quatro capítulos se encontram organizados da seguinte forma:

Capítulo 2: Fazemos uma breve revisão dos principais conceitos relacionados a álgebra e códigos, nos quais se fundamenta o restante do trabalho;

Capítulo 3: Apresentamos um procedimento sistemático para determinação das aplicações casadas isométricas entre os espaços de Lee $(\mathbb{Z}_{2^k}, d_L)$ e de Hamming $\left(\mathbb{Z}_2^{2^{k-1}}, d_H\right)$, explicitando-as para $2 \leq k \leq 6$. Descrevemos também os conceitos de representação modular e particionamento de conjuntos utilizados na determinação dessas aplicações;

Capítulo 4: Baseados nas aplicações isométricas determinadas no Capítulo 3, apresentamos uma proposta para a construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através dos códigos cíclicos provenientes da extensão de Galois de dimensão r sobre anéis de inteiros módulo $q = 2^k$;

Capítulo 5: Apresentamos as conclusões e contribuições do trabalho, além de sugerir tópicos para pesquisas futuras.

Capítulo 2

Álgebra e Códigos

2.1 Introdução

Neste capítulo, apresentamos alguns dos principais conceitos de álgebra e códigos que, embora elementares, são fundamentais para a compreensão do restante do presente trabalho. Estes conceitos podem ser encontrados em [14].

A Seção 2.2 apresenta as principais definições e propriedades das estruturas de grupo, anel e corpo, assim como alguns dos exemplos mais ilustrativos destas. Estas estruturas são funadamentais na teoria de códigos corretores de erro, pois facilitam os processos de codificação, decodificação e análise de desempenho destes. Na Seção 2.3, definimos os espaços métricos de Hamming e de Lee, sobre os quais se desenvolve o restante do trabalho. É também introduzido o importante conceito de isometria. Já na Seção 2.4, revemos os conceitos relacionados a códigos de bloco e suas principais características. Fazemos também uma breve introdução aos conjuntos de sinais casados a grupos, propostos por Loeliger em [23], e aos códigos geometricamente uniformes, descritos por Forney em [13]. Este conceitos são importantes para o entendimento do Capítulo 3. Finalmente, na Seção 2.5 apresentamos as conclusões.

2.2 Estruturas Algébricas

2.2.1 Grupos

Definição 2.2.1 *Uma* ***operação binária * sobre um conjunto*** S *é uma regra que associa a cada par ordenado* (a, b) *de elementos de* S *algum elemento de* S.

Essa necessidade de que o elemento esteja também em S é conhecida como **condição de fechamento**. Assim, exigimos que S seja **fechado** sob uma operação binária em S. Note que apenas um único elemento é associado a cada par ordenado de S.

Exemplo 2.2.1 *A adição usual* $+$ *é uma operação binária sobre o conjunto* $\mathbb{R}$. *A multiplicação* $\cdot$ *é uma outra operação binária sobre* $\mathbb{R}$. *Observe que poderíamos ter substituído* $\mathbb{R}$ *por qualquer outro conjunto dentre* $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{R}^+$ *ou* $\mathbb{Z}^+$. *Por outro lado, a adição não é uma operação binária sobre o conjunto* $\mathbb{R}^*$ *de números reais diferentes de zero porque* $2 + (-2)$ *não está no conjunto* $\mathbb{R}^*$; *ou seja,* $\mathbb{R}^*$ *não é fechado sob* $+$.

Observe ainda que exigimos que uma operação binária sobre um conjunto S seja definida para todo par ordenado (a, b) de elementos de S.

Definição 2.2.2 *Uma operação binária num conjunto* S *é* ***comutativa*** *se* $a * b = b * a$ *para todo* $a, b \in S$.

Definição 2.2.3 *Uma operação binária num conjunto* S *é* ***associativa*** *se* $(a * b) * c = a * (b * c)$ *para todo* $a, b, c \in S$.

Definição 2.2.4 *Um* ***grupo*** $\langle G, * \rangle$ *é um conjunto não vazio* G *com uma operação binária* $*$ *sobre* G, *tal que os seguintes axiomas são satisfeitos:*

1. *A operação binária* $*$ *é associativa;*
2. *Há um elemento* e *em* G *tal que* $e * x = x * e = x$ *para todo* $x \in G$. *(Esse elemento* e *é o* ***elemento identidade*** *para* $*$ *sobre* G*);*

3. *Para cada a em G, existe um elemento a^{-1} em G com a propriedade que $a^{-1} * a = a * a^{-1} = e$. (O elemento a^{-1} é o* ***elemento inverso de*** *a* ***com relação à operação*** *$*$).*

Teorema 2.2.1 *O elemento identidade de um grupo G é único.*

Teorema 2.2.2 *O inverso de cada elemento pertencente a um grupo G é único.*

Definição 2.2.5 *Um grupo G é* ***abeliano*** *(ou* ***comutativo****) se sua operação binária $*$ for comutativa.*

Observação 2.2.1 *Faz-se pertinente uma observação com relação à notação utilizada: ao longo do trabalho, utilizaremos o símbolo G ao invés de $\langle G, * \rangle$ para denotar um grupo por razões de conveniência. Contudo, deve-se ter em mente que, para termos de fato um grupo, uma operação binária em G deve ser definida apropriadamente.*

Seguem exemplos de conjuntos com operações binárias que formam grupos e de outros que não formam grupos.

Exemplo 2.2.2 *O conjunto $\mathbb{Z}^+$ sob a operação $+$ não é um grupo. Não há elemento identidade para $+$ em $\mathbb{Z}^+$.*

Exemplo 2.2.3 *O conjunto $\mathbb{Z}$ sob a operação $+$ é um grupo. Todas condições da definição de um grupo são satisfeitas. Este grupo é abeliano.*

Uma classe de grupos bastante usada em códigos corretores de erro são os grupos $\mathbb{Z}_n$, ou seja, os inteiros sob adição módulo n.

Definição 2.2.6 *Seja n um inteiro positivo e sejam h e k inteiros quaisquer. O resto r quando $h + k$ é dividido por n segundo o algoritmo da divisão de Euclides é a* ***soma de*** *h e k* ***módulo*** *n. Assim, temos que $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$.*

Analogamente, podemos definir **produto** de s e t **módulo** n como sendo o resto da divisão de $(s \cdot t)$ por n.

Teorema 2.2.3 *O conjunto $\mathbb{Z}_n$ é um grupo sob a operação adição módulo n.*

Definição 2.2.7 *Se G é um grupo finito, então a* ***ordem*** *de G, $|G|$, é o número de elementos de G.*

Definição 2.2.8 *Se um subconjunto H de um grupo G é fechado sob a operação binária sobre G e se H é um grupo sob esta operação binária, então H é um* ***subgrupo*** *de G. Escrevemos $H \leq G$.*

Exemplo 2.2.4 *$\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$, porém $\langle \mathbb{Q}^+, + \rangle$ não é subgrupo de $\langle \mathbb{R}, + \rangle$.*

Exemplo 2.2.5 *Todo grupo G tem como subgrupos o próprio G e $\{e\}$, onde e é o elemento identidade em G.*

Definição 2.2.9 *Se G é um grupo, então o subgrupo consistindo do próprio G é o* ***subgrupo impróprio*** *de G. Todos os demais subgrupos são* ***subgrupos próprios***. *O subgrupo $\{e\}$ é o* ***subgrupo trivial*** *de G. Todos os outros subgrupos são* ***não-triviais***.

Exemplo 2.2.6 *$\langle \mathbb{Q}^+, \cdot \rangle$ é um subgrupo próprio de $\langle \mathbb{R}^+, \cdot \rangle$*

Definição 2.2.10 *Um subgrupo H de um grupo G é dito* ***normal*** *se uma das condições equivalentes abaixo é válida:*

1. $gH = Hg \quad$ *para todo* $g \in G$;
2. $g^{-1}Hg = H \quad$ *para todo* $g \in G$;
3. $g^{-1}Hg \subset H \quad$ *para todo* $g \in G$;
4. $g^{-1}hg \in H \quad$ *para todo* $g \in G$ *e* $h \in H$.

Exemplo 2.2.7 *Todos os subgrupos de grupos abelianos são normais.*

Teorema 2.2.4 *Seja G um grupo e seja $a \in G$. Então*

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

é um subgrupo de G e é o menor subgrupo de G que contém a, ou seja, qualquer outro subgrupo que contém a contém também H.

Definição 2.2.11 *O grupo H do Teorema 2.2.4 é o* ***subgrupo cíclico de G gerado por*** *a, e o denotamos por $\langle a \rangle$.*

Definição 2.2.12 *Um elemento a de um grupo G* ***gera*** *G e é um* ***gerador de*** *G se $\langle a \rangle = G$. Um grupo G é* ***cíclico*** *se há algum elemento a em G que gera G.*

Exemplo 2.2.8 *O grupo $\mathbb{Z}$ sob adição é um grupo cíclico cujos geradores são 1 e -1.*

Definição 2.2.13 *Uma relação $\sim$ sobre um conjunto S que satisfaz as seguintes propriedades para todo $a, b, c \in S$,*

1. *$a \sim a$;*
2. *Se $a \sim b$, então $b \sim a$;*
3. *Se $a \sim b$ e $b \sim c$, então $a \sim c$,*

é uma ***relação de equivalência*** *sobre S. Cada célula $\overline{a}$ da partição dada por uma relação de equivalência é uma* ***classe de equivalência.***

Exemplo 2.2.9 *$\mathbb{Z}_8$ é cíclico e $\overline{1}, \overline{3}, \overline{5}$ e $\overline{7}$ são seus geradores, ou seja,*

$$\langle \overline{1} \rangle = \langle \overline{3} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \mathbb{Z}_8$$

Definição 2.2.14 *Seja H um subgrupo de um grupo G. O subconjunto de G*

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

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

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

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

Teorema 2.2.5 (Teorema de Lagrange) *Seja* H *um subgrupo de um grupo finito* G. *Então a ordem de* H *é um divisor da ordem de* G, *ou seja,*

$$|H| \cdot (\text{número de classes laterais de } G \text{ com relação a } H) = |G|.$$

Corolário 2.2.1 *Todo grupo cuja ordem é um número primo é cíclico.*

Teorema 2.2.6 *A ordem de qualquer elemento de um grupo finito divide a ordem do grupo.*

Teorema 2.2.7 *Seja* H *um subgrupo de um grupo* G. *Então a multiplicação de classes laterais à esquerda é definida como*

$$(aH)(bH) = (ab)H,$$

se, e somente se, H *é normal em* G.

Definição 2.2.15 *Seja* H *um subgrupo normal de* G. *Então, o conjunto das classes laterais de* H *formam um grupo, denotado por* G/H, *sob a operação binária* $(aH)(bH) = (ab)H$. *O grupo* G/H *é chamado* ***grupo quociente*** *de* G *módulo* H.

Exemplo 2.2.10 *Como* $\mathbb{Z}$ *é um grupo abeliano,* $n\mathbb{Z}$ *é um subgrupo normal. Logo, temos o grupo quociente* $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Definição 2.2.16 *A ordem* n *de um elemento* a *pertencente a um grupo* G *é o menor inteiro positivo tal que* $a^n = e$, *onde* e *é a identidade do grupo.*

Definição 2.2.17 *Uma* ***permutação de um conjunto*** S *é uma função bijetora de* S *em* S. *Em outras palavras, uma permutação de* S *é uma função um a um de* S *sobre* S.

Definição 2.2.18 *Seja* S *o conjunto finito* $\{1, 2, \cdots, n\}$. *O grupo de todas as permutações de* S *é o* ***grupo simétrico sobre*** n ***letras***, *e é denotado por* S_n.

Exemplo 2.2.11 *Considere o conjunto* $\{1, 2, 3, 4\}$. *Um elemento de* S_4 *é dado por:*

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

Exemplo 2.2.12 *O grupo diedral* $\mathbb{D}_n$ *é o grupo de simetrias de um* n*-ágono.*

Definição 2.2.19 *O subgrupo de* S_n *que consiste das permutações pares de* n *elementos é chamado* ***grupo alternante*** A_n.

Definição 2.2.20 *Considere dois grupos quaisquer* G *e* G' *e a função (ou mapeamento)* $\phi : G \to G'$. *Dizemos que* ϕ *é um* ***homomorfismo*** *de* G *em* G' *se*

$$\phi(ab) = \phi(a)\,\phi(b)$$

para todo $a, b \in G$. *(Note que o produto* ab *ocorre em* G, *enquanto que o produto* $\phi(a)\,\phi(b)$ *ocorre em* G'*).*

Definição 2.2.21 *Um* ***isomorfismo*** *de* G *em* G' *é um homomorfismo onde a função* $\phi : G \to G'$ *é bijetora. Dizemos que* G *e* G' *são isomorfos e escrevemos* $G \cong G'$.

Chamamos de **automorfismo** um isomorfismo de G em G e escrevemos $Aut(G)$.

2.2.2 Anéis

Definição 2.2.22 *Um* ***anel*** $\langle R, +, \cdot \rangle$ *é um conjunto* R *juntamente com duas operações binárias* $+$ *e* $\cdot$ *definidas sobre* R, *as quais chamamos de adição e multiplicação, tal que os seguintes axiomas são satisfeitos:*

UNICAMP
BIBLIOTECA CENTRAL
SEÇÃO CIRCULANTE

1. $\langle R, + \rangle$ *é um grupo abeliano;*

2. *A operação de multiplicação é associativa;*

3. *Para todo* $a, b, c \in R$, *é válida a lei distributiva à esquerda,* $a(b+c) = (ab) + (ac)$, *e à direita,* $(a+b)c = (ac) + (bc)$.

Exemplo 2.2.13 *São exemplos de anéis:* $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{C}, +, \cdot \rangle$ *e o conjunto dos polinômios da forma* $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ *na variável* x *e coeficientes inteiros, com as operações de adição e multiplicação de polinômios.*

Exemplo 2.2.14 $\mathbb{Z}_n$ *é um anel sob as operações de adição e multiplicação módulo* n.

Observação 2.2.2 *Novamente aqui fazemos uma observação com relação à notação utilizada, como feito anteriormente para grupos: ao utilizarmos o símbolo* R *para representar um anel, consideramos que estão implícitas as definições das operações de adição e multiplicação sobre o mesmo.*

Definição 2.2.23 *Dizemos que* Q *é um* ***subanel*** *de um anel* R *se* $Q \subseteq R$ *e* Q *também forma um anel sob as operações* $+$ *e* $\cdot$, *herdadas de* R.

Definição 2.2.24 *Sejam* R *e* R' *anéis. Uma função (mapeamento)* $\phi : R \to R'$ *é um* ***homomorfismo*** *se as condições abaixo são satisfeitas, para* $a, b \in R$:

1. $\phi(a+b) = \phi(a) + \phi(b)$;

2. $\phi(ab) = \phi(a)\,\phi(b)$.

Definição 2.2.25 *Um* ***isomorfismo*** *de* R *em* R' *é um homomorfismo* $\phi : R \to R'$ *bijetor. Dizemos então que* R *e* R' *são isomorfos.*

Definição 2.2.26 *Um anel no qual a multiplicação é comutativa é chamado* ***anel comutativo***. *Um anel* R *com identidade multiplicativa igual a* 1, *tal que* $1 \cdot x = x \cdot 1 = x$ *para todo* $x \in R$ *é um* ***anel com unidade***. *A identidade multiplicativa num anel é denominada* ***unidade***.

Teorema 2.2.8 *Se R é um anel com unidade, então esta unidade 1 é a única identidade multiplicativa do anel.*

Definição 2.2.27 *Um subanel Q de um anel R é um* ***ideal à direita*** *(ou* ***à esquerda****) em R se $Qb \subseteq Q$ ($bQ \subseteq Q$) para todo $b \in R$. Se Q é simultaneamente um ideal à direita e à esquerda em R, dizemos que Q é um* ***ideal*** *em R.*

Seja R um anel, Q um ideal em R e x um elemento em R. Assim, Q define uma relação de equivalência em R, dada por:

$$x \sim x' \Leftrightarrow x - x' \in Q.$$

Estas classes de equivalências são os conjuntos:

$$\overline{x} = x + Q = \{x + q \mid q \in Q\}$$

e são chamadas **classes laterais aditivas** de Q em R. Todo elemento em R está contido em exatamente uma classe lateral $\overline{x}$. Denotamos o conjunto de todas essas classes laterais por R/Q. A partir das operações de adição e multiplicação em R, definimos duas operações em R/Q da seguinte forma:

$$\overline{x} + \overline{y} = (x + Q) + (y + Q) = \overline{x + y} = (x + y) + Q$$

e

$$\overline{x} \cdot \overline{y} = (x + Q) \cdot (y + Q) = \overline{x \cdot y} = x \cdot y + Q.$$

Estas operações são, respectivamente, a adição e a multiplicação em R/Q. É possível mostrar que R/Q é um anel sob as operações acima, chamado **anel quociente de R módulo Q** e denotado por R_Q.

Exemplo 2.2.15 *O conjunto $\mathbb{Z}_n$, $n \geq 2$, pode ser visto como um anel quociente de $\mathbb{Z}$ módulo $n\mathbb{Z}$, ou seja, $\mathbb{Z}/n\mathbb{Z}$, pois $n\mathbb{Z}$ é um ideal em $\mathbb{Z}$. Assim, $0, 1, \cdots, n-1$ denotam as classes laterais:*

$$\overline{0} = n\mathbb{Z}, \quad \overline{1} = 1 + n\mathbb{Z}, \quad \cdots, \quad \overline{n-1} = n - 1 + n\mathbb{Z}$$

que têm estrutura de anel sob adição e multiplicação de classes laterais e que particionam $\mathbb{Z}$.

Definição 2.2.28 *Se a e b são elementos não nulos de um anel R tais que $ab = 0$ ou $ba = 0$, então a e b são* ***divisores de zero.***

Exemplo 2.2.16 *Em $\mathbb{Z}_8$ os elementos 2 e 4 são divisores de zero.*

Definição 2.2.29 *Seja R um anel com unidade. Um elemento a em R é uma* ***unidade inversível*** *("unit" em inglês) em R se existe um elemento $a^{-1} \in R$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Ou seja, a é inversível se posssui inverso multiplicativo em R.*

Exemplo 2.2.17 *Os únicos elementos inversíveis em $\mathbb{Z}$ são 1 e -1.*

Definição 2.2.30 ***Anel de divisão*** *é um anel com unidade no qual todo elemento não nulo é inversível.*

Definição 2.2.31 *Seja R um anel. Um* ***R-módulo*** *consiste de um grupo abeliano G e uma operação de multiplicação de cada elemento de G por todo elemento de R pela esquerda, tais que para todo α, $\beta \in G$ e r, $s \in R$, as seguintes condições são satisfeitas:*

1. $(r\alpha) \in G$;
2. $r(\alpha + \beta) = r\alpha + r\beta$;
3. $(r + s)\alpha = r\alpha + s\alpha$;
4. $(rs)\alpha = r(s\alpha)$.

2.2.3 Corpos

Definição 2.2.32 *Um* ***corpo*** F *é um anel de divisão comutativo.*

Portanto, dizemos que F é um corpo sob as operações binárias $+$ e $\cdot$ se, e somente se, F constitui 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 2.2.18 *São exemplos de corpos: o conjunto dos números racionais e dos números reais sob adição e multiplicação usuais e o conjunto* $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ *para* p *primo sob adição e multiplicação módulo* p.

Exemplo 2.2.19 *O conjunto dos números inteiros não forma um corpo sob as operações de adição e multiplicação usuais.*

Definição 2.2.33 *Um* ***subcorpo*** *é um subconjunto de um corpo que tem estrutura de corpo sob as operações herdadas do mesmo.*

Estamos interessados principalmente em corpos 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 F_q, onde $q \geq 2$ é o número de elementos do corpo.

Descrevemos a seguir uma série de propriedades sobre F_q úteis para se construir corpos contendo F_q como um subcorpo e que servem de fundamentação para a teoria da Seção 4.3.

Definição 2.2.34 *Um* ***polinômio*** *de grau* $n-1$ *sobre um corpo* F_q *é escrito como:*

$$p(x) = p_{n-1}x^{n-1} + p_{n-2}x^{n-2} + \cdots + p_1 x + p_0,$$

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

Definição 2.2.35 *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* F_q.

Sabemos que o conjunto de todos os polinômios sobre $GF(q)$ forma um anel sob as operações usuais de soma e multiplicação de polinômios. Este anel é denotado por $GF(q)[x]$ ou $F_q[x]$.

Definição 2.2.36 *Um elemento* $\beta \in F_q$ *é uma* ***raiz*** *ou* ***zero*** *do polinômio* $p(x) \in F_q[x]$ *se* $p(\beta) = 0$.

Teorema 2.2.9 *Se* G *é um subgrupo multiplicativo do grupo* $\langle F^*, \cdot \rangle$ *de elementos não nulos de um corpo* F, *então* G *é cíclico.*

Corolário 2.2.2 *O grupo multiplicativo de todos elementos não nulos de um corpo finito sob a operação multiplicação deste corpo é cíclico.*

Corolário 2.2.3 *Uma extensão (corpo de extensão)* E *de grau* r *de um corpo finito* F_q *é o conjunto dos polinômios sobre* F_q *módulo um polinômio irredutível de grau* r.

Teorema 2.2.10 *Considere uma extensão finita de grau* r *sobre o corpo* F_q. *Então esta extensão tem* q^r *elementos.*

Teorema 2.2.11 *Todos os corpos de ordem* p^k *são isomorfos.*

Assim, para dois corpos de ordem p^k, F_1 e F_2, existe uma bijeção entre F_1 e F_2 que preserva as operações de adição e multiplicação.

Definição 2.2.37 *Dizemos que um polinômio* $p(x)$ *sobre* F_q *é* ***primo*** *se ele for mônico e irredutível sobre* F_q.

Teorema 2.2.12 *O anel de polinômios módulo um polinômio* $p(x)$ *sobre* F_q *é um corpo se, e somente se,* $p(x)$ *é um polinômio primo.*

Definição 2.2.38 *Um gerador do grupo multiplicativo de F_q é denominado um* ***elemento primitivo*** *de F_q.*

Corolário 2.2.4 *Todo corpo finito F contém um elemento primitivo.*

Uma consequência imediata do Corolário 2.2.4 é a de que todo corpo de Galois contém um elemento β, tal que todo elemento pertencente ao grupo multiplicativo do corpo finito pode ser expresso como uma potência de β.

Os próximos teoremas se referem à existência e unicidade dos chamados polinômios minimais.

Definição 2.2.39 *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 β sobre $GF(q)$.*

Teorema 2.2.13 *Considere os corpos $GF(q')$ e $GF(q)$ como definidos acima. Cada elemento β de $GF(q')$ tem um único polinômio minimal sobre $GF(q)$. Mais do que isso, se β tem $p(x)$ como seu polinômio minimal e um polinômio $g(x)$ tem β como um zero, então $p(x)$ divide $g(x)$.*

2.3 Espaços Métricos

Definição 2.3.1 *[16] Sejam M um conjunto não vazio de ordem n e $d : M \times M \to \mathbb{R}$ uma função que satisfaz as seguintes condições:*

1. $d(x,x) = 0$;
2. $x \neq y \Rightarrow d(x,y) > 0$;
3. $d(x,y) = d(y,x)$;
4. $d(x,z) \leq d(x,y) + d(y,z)$,

para quaisquer $x, y, z \in M$. *Dizemos então que* d *é uma* ***métrica*** *e o par* (M, d) *é um* ***espaço métrico.***

Neste trabalho estamos interessados principalmente no conjunto dos números inteiros módulo q (q primo ou potência de primo), ou $\mathbb{Z}_q$. Portanto, de agora em diante passamos a considerar o conjunto M como $\mathbb{Z}_q$, lembrando porém que a teoria aqui apresentada é válida para qualquer conjunto não vazio M.

Definição 2.3.2 *Chamamos de* ***espaço métrico de Hamming*** *ao par* $(\mathbb{Z}_q, d_H)$, *onde* d_H *é uma métrica definida sobre o conjunto* $\mathbb{Z}_q$, *dada por:*

$$d_H(x, y) = w_H(x \ominus y), \qquad x, y \in \mathbb{Z}_q, \tag{2.1}$$

onde $\ominus$ *denota a subtração módulo* q *e o* ***peso de Hamming****,* w_H, *é dado por:*

$$w_H(x) = \begin{cases} 0, & se \quad x = 0 \\ 1, & se \quad x \neq 0 \end{cases},$$

obedecendo às quatro condições da definição de espaço métrico. A métrica d_H *é conhecida como* ***distância de Hamming****.*

Um espaço métrico bastante conveniente para uso em codificação e modulação sobre o conjunto $\mathbb{Z}_q$ é o espaço de Lee. Assim, temos a seguinte definição:

Definição 2.3.3 *O* ***espaço métrico de Lee*** *é denotado por* $(\mathbb{Z}_q, d_L)$, *onde* d_L *é uma métrica, denominada* ***distância de Lee*** *e definida sobre o conjunto* $\mathbb{Z}_q$, *dada por:*

$$d_L(x, y) = w_L(x \ominus y), \qquad x, y \in \mathbb{Z}_q, \tag{2.2}$$

onde $\ominus$ *denota a subtração módulo* q *e o* ***peso de Lee****,* w_L, *é dado por:*

$$w_L(x) = \begin{cases} x, & se \quad x \leq \lfloor \frac{q}{2} \rfloor \\ q - x, & se \quad x > \lfloor \frac{q}{2} \rfloor \end{cases}.$$

É fácil perceber que o espaço de Lee assim definido satisfaz as quatro condições da definição de espaço métrico.

Lema 2.3.1 *[16] O peso de Lee, w_L, satisfaz as seguintes propriedades:*

1. $w_L(x) = 0 \Leftrightarrow x = 0, \qquad \forall x \in \mathbb{Z}_q$;
2. $w_L(\ominus x) = w_L(x), \qquad \forall x \in \mathbb{Z}_q$;
3. $w_L(x \ominus y) \leq w_L(x) + w_L(y), \qquad \forall x, y \in \mathbb{Z}_q$.

As métricas de Lee e de Hamming podem ser facilmente estendidas para n dimensões utilizando-se a **métrica da soma**. Considere o conjunto $\mathbb{Z}_q^n$, produto direto do conjunto $\mathbb{Z}_q$. Podemos então escrever:

$$d(\underline{x}, \underline{y}) = \sum_{i=1}^{n} d(x_i, y_i), \qquad \forall \underline{x} = (x_1, \cdots, x_n), \underline{y} = (y_1, \cdots, y_n) \in \mathbb{Z}_q^n, \tag{2.3}$$

onde d representa tanto a distância de Hamming quanto a de Lee.

2.3.1 Isometrias

Definição 2.3.4 *[16] Sejam (M_1, d_1) e (M_2, d_2) espaços métricos. Uma aplicação $u : M_1 \to M_2$ é denominada uma **imersão isométrica** quando*

$$d_2(u(x), u(y)) = d_1(x, y), \quad \forall x, y \in M_1.$$

*Desta igualdade segue que u é injetora. Se u for sobrejetora, dizemos que u é uma **isometria de M_1 em M_2**.*

Portanto, podemos dizer que uma isometria é uma transformação de um espaço métrico que preserva as distâncias.

Definição 2.3.5 *[16] Seja N um conjunto, (M, d) um espaço métrico e $u : N \to M$ uma aplicação injetiva. Definimos então a aplicação*

$$d_u : N \times N \to \mathbb{R},$$

onde

$$d_u(x, y) = d(u(x), u(y)), \quad \forall x, y \in N.$$

A função d_u é uma métrica no conjunto N denominada ***métrica induzida pela função*** *u. Esta é a única métrica em N que torna a função u uma imersão isométrica.*

Proposição 2.3.1 *[16] Sejam $u : M_1 \to M_2$ uma imersão isométrica do espaço métrico (M_1, d_1) no espaço métrico (M_2, d_2) e (M_3, d_3) um outro espaço métrico. Temos então:*

- *u é injetora;*
- *Se u é uma isometria, então $u^{-1} : M_2 \to M_1$ é também uma isometria;*
- *Se $v : M_2 \to M_3$ é uma isometria de (M_2, d_2) em (M_3, d_3), então $v \circ u : M_1 \to M_3$ é uma isometria.*

Esta proposição mostra que o conjunto das isometrias $u : M \to M$ de um espaço métrico (M, d), sob a operação de composição de funções, forma um grupo denominado **grupo de simetrias de** M, denotado por $\Gamma(M)$. Assim, considere a seguinte definição:

Definição 2.3.6 ***Simetria*** *é uma isometria u que, quando aplicada ao grupo de simetrias Γ de uma figura, mantém este grupo invariante, ou seja,*

$$u(\Gamma) = \Gamma.$$

Isometrias no Espaço Euclidiano n-dimensional

No espaço Euclidiano de dimensão n, representado por $\mathbb{R}^n$, a métrica utilizada é a **distância Euclidiana**, cuja forma quadrática é dada por:

$$d^2(\underline{x},\underline{y}) = \|\underline{x}-\underline{y}\|^2, \qquad \underline{x},\underline{y}\in\mathbb{R}^n,$$

onde o quadrado da norma, $\|\underline{x}\|^2$, é o produto interno $(\underline{x},\underline{x}) = \underline{x}^T\underline{x}$.

Podemos então definir o que vem a ser uma isometria neste espaço da seguinte forma:

Definição 2.3.7 *[13] Uma isometria u no espaço Euclidiano n-dimensional é uma transformação*

$$u : \mathbb{R}^n \to \mathbb{R}^n,$$

que preserva as distâncias Euclidianas,

$$\|u(\underline{x}) - u(\underline{y})\|^2 = \|\underline{x}-\underline{y}\|^2, \qquad \underline{x},\underline{y}\in\mathbb{R}^n,$$

onde $u(\underline{x})$ e $u(\underline{y})$ são as imagens de $\underline{x}$ e $\underline{y}$ sob a transformação u.

Os principais exemplos de classes de isometrias no espaço Euclidiano são as translações e as transformações ortogonais (rotação pura, rotação imprópria e reflexão pura), mostradas em [13]. Podemos dizer que, a menos de translação, toda isometria de $\mathbb{R}^n$ é determinada por uma matriz ortogonal, ou seja, toda isometria é da forma:

$$u(\underline{x}) = \underline{x}_0 + \mathrm{A}\underline{x},$$

onde $\underline{x}_0 \in \mathbb{R}^n$ e $\mathrm{AA}^T = \mathrm{I}$, I matriz identidade.

Isometrias no Espaço de Hamming n-dimensional

No espaço de Hamming n-dimensional, utilizamos a métrica zero-um, ou métrica de Hamming d_H, definida em (2.3). Esta distância é simplesmente o número em que as coordenadas das n-uplas diferem.

UNICAMP
BIBLIOTECA CENTRAL

Um importante resultado sobre o grupo de simetrias deste espaço, demonstrado em [16], é apresentado abaixo. Antes, porém, considere a seguinte definição:

Definição 2.3.8 *[16] Sejam* $(G_1, *_1)$ *e* $(G_2, *_2)$ *grupos e* $\varphi : G_2 \to Aut(G_1)$ *um homomorfismo. O* ***produto semi-direto de*** G_1 ***e*** G_2 ***com relação a*** φ*, denotado por* $G_1 \times_\varphi G_2$*, é o grupo formado pelos pares* (a_1, a_2)*, tais que* $a_1 \in G_1$*,* $a_2 \in G_2$ *e cuja operação é definida por:*

$$(a_1, a_2) \times_\varphi (b_1, b_2) = (a_1 *_1 \varphi(a_2)(b_1), a_2 *_2 b_2).$$

Teorema 2.3.1 *O grupo de simetrias do espaço de Hamming n-dimensional* $(\mathbb{Z}_2^n, d_H)$*,* $\Gamma(\mathbb{Z}_2^n)$*, é dado por*

$$\Gamma(\mathbb{Z}_2^n) = \mathbb{Z}_2^n \times_\varphi S_n,$$

onde $\times_\varphi$ *denota o produto semi-direto e* S_n *é o grupo das permutações de n elementos.*

Isometrias no Espaço de Lee n-dimensional

Analogamente ao espaço de Hamming n-dimensional, no espaço de Lee de dimensão n a métrica utilizada é a distância de Lee definida em (2.3).

Uma importante classe de isometrias no espaço de Lee é formada pelas translações e reflexões em $\mathbb{Z}_q^n$, definidas em [16]. No caso unidimensional, temos a seguinte definição para o grupo de simetrias do espaço métrico de Lee:

Definição 2.3.9 *[16] Para* $q > 2$*, o grupo de simetrias de* $(\mathbb{Z}_q, d_L)$ *é isomorfo à* $\mathbb{Z}_q \times_\varphi \mathbb{Z}_2 \simeq \mathbb{D}_q$*, onde* $\mathbb{D}_q$ *é o grupo diedral com* $2q$ *elementos formado pelas simetrias de um polígono regular de* q *lados.*

2.4 Códigos

Definição 2.4.1 *Um* ***código*** C *sobre um conjunto* $\mathcal{A}$ *é qualquer subconjunto não vazio do espaço de sequências* $\mathcal{A}^I$*, onde* $\mathcal{A}$ *é chamado* ***alfabeto*** *do código e* I *é o* ***conjunto de***

índices *das sequências* $c = \{c_i \mid i \in I\}$. *Chamamos de* ***palavra-código*** *os elementos, ou* ***símbolos*** *, no alfabeto* $\mathcal{A}$ *que compõem o código* $\mathcal{C}$.

Neste trabalho estamos interessados em alfabetos finitos. Quando isto acontece e, além disto, o conjunto de índices é finito (por exemplo de tamanho n), dizemos que o código é um código de bloco de **comprimento** n, ou seja, suas palavras-código possuem comprimento n. Assim, temos a seguinte definição:

Definição 2.4.2 *Um* ***código de bloco*** $\mathcal{C}$ ***de comprimento*** n *sobre um alfabeto* $\mathcal{A}$ *é qualquer subconjunto do conjunto* $\mathcal{A}^n$ *das sequências* $c = \{c_i \mid 1 \leq i \leq n\}$.

Um código de bloco é caracterizado por três parâmetros principais: seu comprimento, sua dimensão e sua distância mínima. A seguir temos a definição destes dois últimos.

Definição 2.4.3 *A* ***dimensão*** *de um código* $\mathcal{C}$ *é dada por*

$$k = \log_{|\mathcal{A}|} |\mathcal{C}| ,$$

onde $|\cdot|$ *é a cardinalidade do conjunto.*

Definição 2.4.4 *A* ***distância mínima*** *de um código de bloco* $\mathcal{C}$ *é definida como:*

$$d_{\min}(\mathcal{C}) = \min_{x,y \in \mathcal{C},\ x \neq y} d(x,y) .$$

A distância d utilizada na caracterização do código depende da métrica utilizada no alfabeto em questão. Nos próximos capítulos, estaremos utilizando as métricas de Hamming e de Lee, definidas em (2.1) e (2.2), respectivamente.

Assim, representamos um código de bloco pela terna ordenada $(n, k, d_{\min})$. Quando a métrica utilizada é a de Hamming, é válido o seguinte teorema:

Teorema 2.4.1 *Para qualquer código de bloco* $(n, k, d_{\min})$, *vale a seguinte desigualdade:*

$$d \leq n - k + 1.$$

Um outro parâmetro muito importante na caracterização de um código de bloco, indicador de desempenho deste, é a chamada **taxa** do código, definida pela razão entre a dimensão do código e seu comprimento, ou seja,

$$r_C = \frac{k}{n}.$$

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

$$d_{\min} \leq 2t + 1.$$

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

A maioria dos códigos conhecidos até hoje pertencem à classe dos códigos lineares. Um código (n, k, d) é dito linear se, e somente se, todas as suas palavras-código formam um subespaço vetorial de dimensão k do espaço vetorial F_q^n, o conjunto das n-uplas do corpo F_q. Portanto, podemos representar este código matricialmente como

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

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

$$\underline{v} = \underline{u}\mathrm{G},$$

onde $\underline{u}$ é a palavra a ser codificada ou informação e $\underline{v}$ é a palavra-código correspondente. Para toda palavra-código $\underline{v}$ vale a relação

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

onde a matriz $(n-k)\times n$, denotada por H, é chamada **matriz verificação de paridade** e qualquer vetor ortogonal a 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 $\mathcal{C}$.

2.4.1 Conjuntos de Sinais Casados a Grupos

O conceito de um conjunto de sinais casados a grupos foi definido por Loeliger em [23] e surgiu como uma forma de se associar uma palavra-código a um sinal a ser transmitido. A seguir, apresentamos os principais conceitos relacionados a esta teoria.

Definição 2.4.5 *[23] Seja (M,d) um espaço métrico. Dizemos que um* ***conjunto de sinais*** *finito $\mathcal{S}$ em M está* ***casado a um grupo*** *G se existe uma uma função sobrejetora $\mu : G \to \mathcal{S}$, tal que,*

$$d\left(\mu\left(g\right),\mu\left(g'\right)\right) = d\left(\mu\left(g^{-1} * g'\right),\mu\left(e\right)\right), \quad \forall g, g' \in G,$$

onde e é o elemento neutro de G. A função μ é denominada ***mapeamento casado****. Se μ é uma injetora, então μ^{-1} é chamada* ***rotulamento casado****.*

Observe que neste caso temos em $\mathcal{S}$ uma estrutura de grupo na qual as operações são isometrias.

Definição 2.4.6 *[23] Um mapeamento casado $\mu : G \to \mathcal{S}$, tal que H é um subgrupo de G (ou seja, $H = \mu^{-1}\mu\left(e\right)$, onde e é o elemento neutro em G), e não contém subgrupos normais não triviais de G, é chamado de* ***mapeamento efetivamente casado****. Nesse caso, dizemos que $\mathcal{S}$ está efetivamente casado a G.*

2.4.2 Códigos Geometricamente Uniformes

Forney em [13], ao estender os conceitos de códigos de Slepian e de códigos reticulado, introduziu o conceito de uma importante classe de códigos: os códigos geometricamente uniformes, definidos abaixo.

Definição 2.4.7 *[13] Um conjunto de sinais $\mathcal{S}$ definidos sobre um espaço métrico (M, d) é um código* ***geometricamente uniforme*** *se, dados s_1 e s_2 em $\mathcal{S}$, existe uma isometria u_{s_1,s_2} que transforma s_1 em s_2 mantendo $\mathcal{S}$ invariante, ou seja,*

$$u_{s_1,s_2}(s_1) = s_2,$$

$$u_{s_1,s_2}(\mathcal{S}) = \mathcal{S}.$$

Em outras palavras, $\mathcal{S}$ é geometricamente uniforme se a ação do grupo de simetrias $\Gamma(\mathcal{S})$ de $\mathcal{S}$ é transitiva.

Definição 2.4.8 *[13] O* ***grupo gerador*** *$U(\mathcal{S})$ de $\mathcal{S}$ é um subgrupo do grupo de simetrias $\Gamma(\mathcal{S})$, onde, para qualquer $s_0 \in \mathcal{S}$, temos:*

$$\mathcal{S} = \{u(s_0), \quad u \in U(\mathcal{S})\}$$

e a função

$$m : U(\mathcal{S}) \to \mathcal{S},$$

definida como

$$m(u) = u(s_0),$$

é injetora.

Para um código $\mathcal{S}$ geometricamente uniforme, podemos definir, para cada ponto $s \in \mathcal{S}$, uma região formada por todos os pontos pertencentes ao espaço métrico onde está definido o código que se encontram, no mínimo, tão próximos a s quanto qualquer

outro ponto $s' \in \mathcal{S}$. Em outras palavras, essas regiões são as regiões de decisão do código. Formalmente, temos a seguinte definição:

Definição 2.4.9 *[13] Seja $\mathcal{S}$ um conjunto de sinais geometricamente uniforme em um espaço métrico (M, d). A* ***região de Voronoi*** *associada a um ponto $s \in \mathcal{S}$, denotada por $\mathcal{V}(\mathcal{S})$, é o conjunto*

$$\mathcal{V}_{\mathcal{S}}(s) = \left\{ x \in M \mid d(x,s) \leq \min_{s' \in \mathcal{S}} d(x,s') \right\}.$$

A uniformidade geométrica é uma forma mais forte de simetria, apresentando propriedades como: a distância entre quaisquer duas palavras-código de $\mathcal{S}$ é a mesma, todas as regiões de Voronoi são congruentes, todas palavras-código possuem mesma probabilidade de erro e o grupo gerador $U(\mathcal{S})$ é isomorfo a um grupo de permutações transitivo sobre as palavras do código. Todas essas características são buscadas na construção de novas classes de códigos, pois facilitam o processo de decodificação dos mesmos, no sentido de que não é necessário conhecer a região de decisão de cada palavra-código; basta conhecer a região de Voronoi associada a uma das palavras do código e determinar as demais regiões a partir de translações da região conhecida.

Com relação aos códigos já existentes utilizados em comunicações digitais, a maioria é geometricamente uniforme, como por exemplo as constelações de sinais M-PSK.

2.5 Conclusão

Neste capítulo, procuramos apresentar de maneira sucinta os principais conceitos a serem utilizados ao longo deste trabalho.

Descrevemos as principais estruturas algébricas: grupos, anéis e corpos. É sempre desejável que um código apresente uma estrutura algébrica bem definida.

Os parâmetros que caracterizam os códigos de bloco foram definidos, bem como os principais espaços métricos sobre os quais estão fundamentados estes códigos, os espaços

de Hamming e Lee. Veremos, no Capítulo 3 que é possível haver um casamento isométrico entre estes espaços métricos.

Por fim, os conceitos de casamento e de uniformidade geométrica utilizados nos próximos capítulos foram brevemente descritos.

Capítulo 3

Aplicações Casadas Isométricas

3.1 Introdução

Carlet em [11] propôs uma generalização do mapeamento Gray para construção de códigos binários não lineares a partir de códigos sobre $\mathbb{Z}_{2^k}$. Contudo, seu trabalho mostra que, para $k > 3$, o procedimento adotado não resulta num código cujos rótulos (palavras-código) apresentem somente pesos de Hamming pares, o que é desejável pois facilita o processo de decodificação. Em outro trabalho, Gerônimo *et al.*, [18] mostraram a não existência de códigos $\mathbb{Z}_{2^k}$-lineares para $k \geq 3$ (para $k = 2$ temos a $\mathbb{Z}_4$-linearidade), pois não é possível conseguir uma aplicação $m_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k$ bijetora, tal que os espaços métricos de Lee $(\mathbb{Z}_{2^k}, d_L)$ e de Hamming $\left(\mathbb{Z}_2^k, d_H\right)$ sejam isométricos. Nesta direção, em [26] foi mostrada a possibilidade de que se a aplicação m_k for injetora, então é possível obter o casamento e a isometria entre os espaços métricos $(\mathbb{Z}_{2^k}, d_L)$ e $\left(\mathbb{Z}_2^{2^{k-1}}, d_H\right)$. A esta classe de códigos foi dado o nome de códigos $\mathbb{Z}_{2^k}$-pseudolineares, explicitados no Capítulo 4.

Neste capítulo, apresentamos um procedimento sistemático para a determinação das aplicações isométricas entre os espaços de Lee e de Hamming. Estas aplicações apresentam a propriedade de que os rótulos possuem peso de Lee e de Hamming múltiplos de 4, e que os mesmos constituem um conjunto geometricamente uniforme, simplificando

consideravelmente o processo de decodificação (Seção 2.4.2).

Para determinarmos essas aplicações isométricas fazemos uso dos conceitos de uniformidade geométrica, particionamento de conjuntos e representação modular. O conceito de particionamento de conjuntos, descrito na Seção 3.2, diz respeito ao recobrimento de regiões $2^k \times 2^k$ através de subregiões associadas aos elementos do alfabeto do código. Já na Seção 3.3, apresentamos o importante conceito de representação modular (referimos o leitor para [21]), que nos permitirá conhecer, a partir do vetor espectro de pesos de um código binário linear, sua matriz geradora associada. Por sua vez, esta matriz geradora é a matriz que define a aplicação isométrica em questão. Na Seção 3.4, estabelecemos as aplicações casadas isométricas entre os símbolos de $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{16}$, $\mathbb{Z}_{32}$ e $\mathbb{Z}_{64}$, e os símbolos de $\mathbb{Z}_2^2$, $\mathbb{Z}_2^4$, $\mathbb{Z}_2^8$, $\mathbb{Z}_2^{16}$ e $\mathbb{Z}_2^{32}$. Por fim apresentamos as conclusões na Seção 3.5.

3.2 Recobrimento de Regiões $\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$

Dada uma célula básica de ordem 2^k, onde por célula básica de ordem q denotamos o arranjo de pontos (formando células menores) de q linhas e q colunas num reticulado $\mathbb{Z}_q^2 = \mathbb{Z}_q \times \mathbb{Z}_q$, a pergunta que se faz é a seguinte: qual a melhor distribuição desses pontos que recobrem a célula básica, sob a restrição de que estes pontos mantenham a maior distância mínima entre si? Analogamente, podemos enunciar o problema da seguinte forma: quais os possíveis formatos S_j destas células menores que recobrem a célula básica, onde para uma célula demarcada em S_j a distância entre essas células na justaposição dos formatos S_j's é a maior possível?

Nesta seção, o conceito de particionamento de conjuntos proposto por Ungerboeck em [29] é aplicado ao particionamento do número inteiro 2^k. Esta partição nos fornece todos os possíveis formatos com 2^k células. A técnica de particionamento de conjuntos será utilizada neste caso para determinar a localização dos dígitos do alfabeto do código e também as possíveis regiões de Voronoi em um arranjo $2^k \times 2^k$, células com a maior distância de Lee possível. De posse da localização desses dígitos do alfabeto do código,

podemos calcular seu vetor espectro de pesos W e então determinar, através da representação modular, a matriz geradora do código que traduz a aplicação isométrica procurada. É importante ressaltar porém ser possível, a partir de uma certa partição, não conseguir encontrar uma matriz geradora para o código. Isto está relacionado com as condições de existência desta matriz geradora, abordadas na Seção 3.3.

Em [1], de Almeida apresenta uma generalização do particionamento de conjuntos através da representação de números inteiros por formas quadráticas binárias, ou seja, através de equações de Diofanto com duas variáveis. Chamamos de equação de Diofanto a equação polinomial com coeficientes inteiros cujas soluções são também números inteiros. Estamos particularmente interessados nas equações de Diofanto associadas ao reticulado bidimensional regular $\mathbb{Z}_q^2$, isto é, equações da forma:

$$x^2 + y^2 = q, \tag{3.1}$$

onde q é a ordem do anel em questão. Dentre as possíveis soluções desta equação, tomamos aquela que resulta na partição ótima, ou seja, onde a distância de Lee mínima entre os elementos de uma mesma célula é máxima. Estas células são as regiões de Voronoi que recobrem a região $2^k \times 2^k$ considerada.

As soluções da Equação (3.1) são garantidas pelos seguintes teoremas:

Teorema 3.2.1 (Genus) *A equação $x^2 + y^2 = q$ pode ser resolvida para x e y inteiros e com q primo se e somente se, $q = 1 \bmod (4)$ ou $q = 2$.*

Teorema 3.2.2 (Composição) *Seja $A(x, y) = x^2 + y^2 = q$. Então,*

$$A(x, y)\, A(x', y') = A(xx' - yy', xy' + x'y).$$

Assim, dado o número q de elementos do anel considerado, fatoramos q tal que seus fatores primos obedeçam ao Teorema 3.2.1 e aplicamos a Equação (3.1) para cada um desses fatores, utilizando o Teorema 3.2.2 na determinação de todas as soluções possíveis de (3.1).

Ainda em [1], encontram-se tabeladas as soluções da Equação (3.1) para $q < 100$. Estas soluções vão ajudar a determinar as matrizes de transformação T, cujas linhas são vetores linearmente independentes e cujo determinante é igual a q. Além disso, é desejável que pelo menos uma das linhas de T seja uma das soluções da equação de Diofanto definida em (3.1). Contudo, isto nem sempre é possível, uma vez que a geração de um conjunto cíclico via transformação T pode estar fora do espaço das soluções de Diofanto. Nossos casos de interesse são aqueles para os quais $q = p^k$, $p = 2$ e $2 \leq k \leq 6$. Logo, $q = 0 \bmod (4)$. Dessa forma, devemos fazer uma busca exaustiva por estas transformações.

Como exemplo, considere o reticulado $\mathbb{Z}_4 \times \mathbb{Z}_4$. A equação de Diofanto associada é dada por:

$$x^2 + y^2 = 4.$$

Neste caso, por inspeção, é fácil perceber que o conjunto solução é: $\{(\pm 2, 0), (0, \pm 2)\}$. Porém, se usarmos as soluções $(2, 0)$ e $(0, 2)$ como vetores linha da matriz T, então o correspondente código não será cíclico: $\{00, 02, 20, 22\}$. A fim de obtermos um código cíclico, um dos vetores linha deverá ser o par $(2, 1)$ (ou $(1, 2)$), com o outro vetor linha sendo uma das soluções da equação de Diofanto, tal que o determinante de T tenha valor 4. Assim, uma das possíveis matrizes de transformação é mostrada abaixo:

$$\mathrm{T} = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}$$

Esta trasformação nos fornece o código de grupo cíclico cujas palavras-código, $\{00, 12, 20, 32\}$, estão representadas como pares ordenados na Figura 3-1.

Na Figura 3-1, note que os pesos de Lee são dados pelo menor número de quadrados necessários para se atingir uma palavra-código a partir da palavra-código 00. Assim, o vetor espectro de pesos é dado por $W = (3, 2, 3)$.

É fácil notar que, para o código representado na Figura 3-1, o critério de distância é

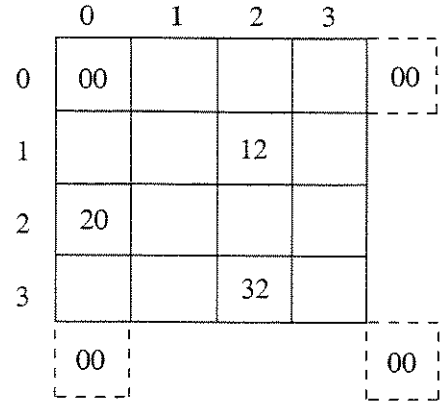

Figura 3-1: Arranjo $\mathbb{Z}_4 \times \mathbb{Z}_4$ com seus respectivos pares ordenados

satisfeito, ou seja, as palavras deste código apresentam-se separadas pela maior distância mínima possível, que neste caso é $d_L = 2$.

Na Seção 3.4 apresentaremos as transformações para os demais reticulados, $\mathbb{Z}^2_{2^k}$ e $3 \leq k \leq 6$, bem como as aplicações isométricas derivadas destas transformações.

Além da determinação das aplicações casadas isométricas $m_k : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_2^{2^{k-1}}$ que nos levam aos códigos $\mathbb{Z}_{2^k}$-pseudolineares, vários outros problemas podem ser resolvidos através da técnica de particionamento de conjuntos, tais como: armazenagem de dados em meios ópticos ou magnéticos de forma a minimizar os erros que ocorrem em surtos, modulações digitais tipo M-QAM, alocação de frequência em telefonia móvel, etc, considerados em [3], [8], [10], [1], [4] e [2].

3.3 Representação Modular

A importância do conceito de representação modular está relacionada ao seguinte problema: dada a matriz geradora de um código de bloco binário (n, k), então o vetor espectro de pesos de Hamming, W, das palavras-código é facilmente determinado; contudo, dado um vetor espectro de pesos de Hamming, o que se deseja é determinar a existência de uma matriz geradora G associada a este espectro de pesos. Nesta direção é que iremos apresentar um procedimento para resolver este problema.

Seja G a matriz geradora de um código de bloco (n, k). Então G pode ser interpretada como tendo k linhas e n $\left(n = 2^k - 1\right)$ diferentes tipos de colunas, onde por tipo queremos dizer a representação binária de um inteiro. Geralmente, rearranjos das colunas implicam em códigos equivalentes; como estes não são importantes no sentido de não acrescentarem novos resultados, podemos descrever um código por um conjunto de colunas de cada tipo. Isto é denominado **representação modular**.

Seja M uma matriz $k \times 2^k - 1$, ou seja, uma matriz com todas as possíveis combinações de k elementos binários, a menos da coluna toda nula por razões óbvias, representando k números inteiros em ordem crescente. Suponha que a j-ésima coluna, $1 \leq j \leq 2^k - 1$, corresponda à coluna de tipo j. Assim, a representação modular de M é dada pelo vetor N de comprimento $2^k - 1$, consistindo de um elemento de cada tipo, isto é, $N = (1, 1, \cdots, 1)$. Por exemplo, seja $k = 3$. Logo, M é a matriz mostrada abaixo:

$$\mathrm{M} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

e seu correspondente vetor representação modular é dado por:

$$N = (1, 1, 1, 1, 1, 1, 1).$$

De modo geral, a matriz geradora G de um código binário pode ser descrita como um vetor de m componentes, onde cada componente é um inteiro positivo n_i, representando o número de colunas do tipo i, isto é,

$$N = (n_1, n_2, \cdots, n_m),$$

tal que

$$\sum_{i=1}^{m} n_i = n.$$

O vetor N é chamado **vetor representação modular**.

Considere a matriz K dada por:

$$\mathrm{K} = \mathrm{M}^T\mathrm{G}.$$

Então, K tem como linhas todas as possíveis combinações lineares das linhas de G e, portanto, apresenta todas as palavras-código como linhas.

Seja agora a matriz simétrica C definida através do seguinte produto binário:

$$\mathrm{C} = \mathrm{M}^T\mathrm{M}. \tag{3.2}$$

Teorema 3.3.1 *[25]O vetor espectro de pesos de Hamming, W, das $2^k - 1$ palavras-código não nulas de um código de grupo binário pode ser definido como as componentes do vetor resultante da multiplicação, como matrizes de números reais, do vetor representação modular N pela matriz C, isto é,*

$$W = N\mathrm{C},$$

ou, analogamente,

$$W^T = \mathrm{C}^T N^T = \mathrm{C}N^T.$$

Note que se a matriz C for vista como uma matriz de números reais, a mesma é não singular. Sua inversa pode ser determinada como sendo

$$\mathrm{C}^{-1} = \frac{2\mathrm{C} - \mathrm{J}}{2^{k-1}}, \tag{3.3}$$

onde J é a matriz com todos os elementos iguais a 1.

Uma outra forma de se calcular a inversa da matriz C, é fazer a troca dos elementos 0 de C por -1 e dividir cada elemento da matriz resultante por 2^{k-1}.

A matriz C_n, isto é, C é uma matriz quadrada de ordem n, pode ser facilmente expandida para ordens superiores. Considere a matriz C_3, dada por:

$$C_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \tag{3.4}$$

Observe que esta matriz pode ser vista como:

$$C_3 = \begin{bmatrix} A & 0 & A \\ 0 & 1 & 1 \\ A & 1 & \overline{A} \end{bmatrix},$$

onde A é a matriz unitária de ordem 1 e $\overline{A}$ representa a operação lógica de negação aplicada a cada elemento da matriz A, ou seja, $\overline{A} = 0$ neste caso.

Assim, para construirmos a matriz C_7, fazemos $A = C_3$, como mostrado em (3.5).

$$C_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{3.5}$$

Portanto, para obtermos a matriz simétrica C_n, onde n é ímpar, basta fazermos $A = C_{\lfloor n/2 \rfloor}$ e mantermos o padrão dos elementos que formam uma "cruz" no centro da matriz, ou seja:

$$c_{n/2,n/2} = 1;$$

$$c_{n/2,j} = 0, \quad 1 \leq j \leq n/2 - 1;$$

$$c_{n/2,j} = 1, \quad n/2 + 1 \leq j \leq n;$$

$$c_{i,n/2} = 0, \quad 1 \leq i \leq n/2 - 1;$$

$$c_{i,n/2} = 1, \qquad n/2+1 \leq j \leq n;$$

onde $c_{i,j}$ é o elemento da linha i e coluna j da matriz C.

Como estamos interessados em estabelecer as aplicações isométricas entre os símbolos de $\mathbb{Z}_{2^k}$ e $\mathbb{Z}_2^{2^k-1}$, para $2 \leq k \leq 6$, devemos conhecer as matrizes C_3, C_7, C_{15}, C_{31} e C_{63}. Portanto, a construção mostrada acima é bastante útil, pois poupa cálculos desnecessários, permitindo que, a partir da matriz C_3, conheçamos todas as demais matrizes C_n, $n = 2^k - 1$.

Logo, sabendo calcular as matrizes C_n e dado o vetor espectro de pesos, W, podemos encontrar o vetor representação modular N e, a partir deste, determinar a matriz geradora do código, G. Assim, considere a equação abaixo:

$$N = WC^{-1} \tag{3.6}$$

Do Teorema 3.3.1, temos que um dado conjunto de pesos é factível, ou seja, corresponde a um código de bloco binário (n, k), se o mesmo puder ser arranjado em um vetor W tal que o correspondente vetor N, obtido pela Equação (3.6), seja formado exclusivamente por números inteiros não negativos. Quando isto não é possível, ou seja, quando N apresenta elementos não inteiros e/ou negativos, permutamos o vetor espectro de pesos e recalculamos o vetor representação modular. Observe que, para um vetor N de comprimento n, pode ser necessário realizar, no pior caso, $n!$ permutações até que encontremos uma solução factível ou cheguemos à conclusão de que esta solução não existe para o vetor W dado, tornando a busca por uma solução para a Equação (3.6) computacionalmente inviável para valores grandes de n. Este é um problema de otimização combinatorial e algoritmos eficientes para sua solução devem ser investigados. No nosso caso, a implementação baseou-se na busca exaustiva.

Em contrapartida, há casos em que existe mais de uma solução para a Equação (3.6), ou seja, permutações do vetor W implicam em vetores N cujos elementos são números inteiros não negativos. Contudo, estas diferentes representações modulares descrevem

UNICAMP
BIBLIOTECA CENTRAL

códigos equivalentes (matrizes geradoras equivalentes), os quais não trazem novos resultados com relação às aplicações procuradas, [21]. Assim, a abordagem adotada foi a de buscar apenas uma solução factível, desconsiderando outras possíveis soluções equivalentes.

Podemos dizer que a Equação (3.6) é o ponto central deste trabalho e, através de suas soluções, podemos chegar às contribuições mais importantes do mesmo, descritas no Capítulo 5. Na Seção 3.4, apresentamos as aplicações isométricas derivadas das matrizes geradoras construídas através do conceito de representação modular.

3.4 Aplicações Casadas Isométricas: Análise de Casos

Nas Seções 3.2 e 3.3 foram introduzidos os importantes conceitos de particionamento de conjuntos e representação modular, respectivamente. Estes conceitos são agora utilizados na determinação de aplicações casadas isométricas entre os símbolos de $\mathbb{Z}_{2^k}$ e os símbolos de $\mathbb{Z}_2^{2^{k-1}}$. Assim, mostraremos que, embora não seja possível encontrar códigos $\mathbb{Z}_{2^k}$-lineares para $k \geq 3$, [18], existe casamento e isometria entre os espaços métricos $(\mathbb{Z}_{2^k}, d_L)$ e $\left(\mathbb{Z}_2^{2^{k-1}}, d_H\right)$, ou seja, códigos $\mathbb{Z}_{2^k}$-pseudolineares para qualquer valor de k.

Na busca por estas aplicações, as seguintes características são desejadas:

- Uma das linhas da matriz de transformação T corresponde a uma das soluções da equação de Diofanto;
- O determinante da matriz de transformação T é igual ao número de elementos do anel considerado;
- A transformação T distribui as células (palavras-código) com a maior distância mínima entre si;
- O código gerado pela matriz de transformação T é cíclico;

- O vetor representação modular N obedece à Equação (3.6).

Dessa forma, considere os casos a seguir.

3.4.1 O Caso $\mathbb{Z}_4$

A Figura 3-1 mostra a representação das palavras-código como pares ordenados do código de grupo cíclico sobre o reticulado $\mathbb{Z}_4 \times \mathbb{Z}_4$, dado por: $\mathcal{C} = \{00, 12, 20, 32\}$. Este código foi obtido aplicando-se a transformação

$$\mathrm{T} = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}$$

a um certo ponto inicial. Observe que esta matriz de transformação apresenta as características desejadas: suas linhas são vetores linearmente independentes, uma delas é solução da equação de Diofanto e a outra impõe ciclicidade ao código, mantendo o determinante de T igual a q, onde neste caso $q = 4$. Além disso, a distância mínima entre estas palavras-código é a maior possível.

Vimos na Seção 3.2 que a distribuição de pesos de Lee é dada pelo vetor $W = (3, 2, 3)$. Portanto, utilizando a matriz C_3, temos o vetor representação modular $N = (2, 1, 1)$. A representação modular nos fornece os tipos de colunas e o número de colunas destes determinados tipos que existem na matriz geradora da aplicação procurada. Assim, a matriz geradora G do código binário associado é dada pela matriz (3.7).

$$\mathrm{G} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \tag{3.7}$$

Isto nos dá o mapeamento mostrado na Tabela 3.1.

Todavia estamos interessados em obter um mapeamento isométrico entre os espaços de Lee e de Hamming, isto é, desejamos uma função que reproduza os pesos de Lee dos elementos de $\mathbb{Z}_4$ com os pesos de Hamming das palavras-código binárias correspondentes.

Código 4-ário	Pesos de Lee	Código binário	Pesos de Hamming
0 0	0	$(0\ 0\ 0\ 0)$	0
1 2	3	$(1\ 1\ 0\ 1)$	3
2 0	2	$(0\ 0\ 1\ 1)$	2
3 2	3	$(1\ 1\ 1\ 0)$	3

Tabela 3.1: Aplicação $m_2' : \mathbb{Z}_4^2 \to \mathbb{Z}_2^4$

Observe que a palavra-código 20 do código 4-ário possui peso de Lee igual a 2, logo a palavra-código binária correspondente terá que apresentar peso de Hamming 2. Isto implica na representação 11 para o símbolo 4-ário 2 e 00 para o símbolo 4-ário 0. Dessa forma, o símbolo 3 deve ser representado por 10 (ou 01) e o símbolo 1 por 01 (ou 10).

Note que é possível obter esta isometria utilizando-se apenas os dois últimos dígitos (da direita) dos símbolos em $\mathbb{Z}_2^4$, obtendo-se símbolos em $\mathbb{Z}_2^2$. Portanto, temos a seguinte aplicação isométrica entre os símbolos de $\mathbb{Z}_4$ e os símbolos de $\mathbb{Z}_2^2$:

Símbolos em $\mathbb{Z}_4$	Símbolos em $\mathbb{Z}_2^2$
0	$(0\ 0)$
1	$(0\ 1)$
2	$(1\ 1)$
3	$(1\ 0)$

Tabela 3.2: Aplicação $m_2 : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

Assim, reproduzimos o mapeamento utilizado na $\mathbb{Z}_4$-linearidade, e portanto, o código obtido é $\mathbb{Z}_4$-linear, cujas características facilitam significativamente sua decodificação, [19].

3.4.2 O Caso $\mathbb{Z}_8$

Para o alfabeto em $\mathbb{Z}_8$, a equação de Diofanto é dada por:

$$x^2 + y^2 = 8.$$

As soluções inteiras desta equação são $\{(2,2), (-2,-2), (2,-2), (-2,2)\}$. Todavia,

a fim de satisfazer as características apresentadas no início desta seção e obtermos um código cíclico com o maior número de palavras possível, considere a seguinte matriz de transformação T:

$$\mathrm{T} = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}.$$

Observe que esta matriz de transformação não é a única que satisfaz nossos propósitos: poderíamos ter escolhido os pares $(1,5)$ e $(5,1)$ para formar a matriz T. A partir de T, temos o código de grupo cíclico cujas palavras-código estão representadas na Figura 3-2.

	0	1	2	3	4	5	6	7
0	00							
1				13				
2							26	
3		31						
4					44			
5								57
6			62					
7						75		

Figura 3-2: Arranjo $\mathbb{Z}_8 \times \mathbb{Z}_8$ com seus respectivos pares ordenados

Portanto, temos o código $\mathcal{C} = \{00, 13, 26, 31, 44, 57, 62, 75\}$, cuja distribuição de pesos de Lee é $W = (4, 4, 4, 8, 4, 4, 4)$. Note que todas as palavras-código apresentam pesos de Lee múltiplos de 4. Aqui, da mesma forma como feito para o caso $\mathbb{Z}_4$, calculamos o peso de Lee como sendo o menor número de quadrados necessários para se atingir uma palavra-código a partir da palavra 00. O vetor representação modular deste código é dado por $N = (0, 0, 0, 2, 2, 2, 2)$. Como os dígitos que formam as palavras-código têm peso de

Lee par e as regiões de Voronoi correspondentes são congruentes, podemos escrever o vetor representação modular como $N = (0,0,0,1,1,1,1)$. Isto nos fornece a seguinte matriz geradora:

$$\mathrm{G} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Logo, temos a aplicação mostrada na Tabela 3.3.

Símbolos em $\mathbb{Z}_8$	Símbolos em $\mathbb{Z}_2^4$
0	(0 0 0 0)
1	(0 1 0 1)
2	(0 0 1 1)
3	(0 1 1 0)
4	(1 1 1 1)
5	(1 0 1 0)
6	(1 1 0 0)
7	(1 0 0 1)

Tabela 3.3: Aplicação $m_3 : \mathbb{Z}_8 \to \mathbb{Z}_2^4$

3.4.3 O Caso $\mathbb{Z}_{16}$

No caso $\mathbb{Z}_{16}$ procedemos da mesma forma que nos casos $\mathbb{Z}_4$ e $\mathbb{Z}_8$. A matriz de transformação que distribui as palavras-código de um código cíclico de $q = 16$ elementos com a maior distância mínima entre si é dada pela matriz T mostrada abaixo:

$$\mathrm{T} = \begin{bmatrix} 7 & 1 \\ 1 & 7 \end{bmatrix}. \tag{3.8}$$

Note que poderíamos ter escolhido os pares $(1,9)$ e $(9,1)$ como linhas da matriz de

transformação e que a matriz (3.8) é equivalente à matriz

$$T = \begin{bmatrix} 7 & -2 \\ 1 & 2 \end{bmatrix},$$

cujo determinante é 16.

Aplicando a matriz (3.8) a um determinado ponto inicial temos o código cíclico mostrado na Figura 3-3.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	00															
1								17								
2															214	
3						35										
4													412			
5				53												
6											610					
7		71														
8									88							
9																915
10							106									
11														1113		
12					124											
13												1311				
14			142													
15										159						

Figura 3-3: Arranjo $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ com seus respectivos pares ordenados

Pela Figura 3-3, é fácil notar que o vetor espectro de pesos de Lee deste código é dado por $W = \{8, 4, 8, 8, 8, 12, 8, 16, 8, 12, 8, 8, 8, 4, 8\} = \{8, 4, 8^3, 12, 8, 16, 8, 12, 8^3, 4, 8\}$. O correspondente vetor representação modular pode ser representado por $N = (0^7, 1^4, 2^2, 0^2)$.

a matriz geradora do código binário mostrada em (3.9).

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{3.9}$$

Dessa forma, a aplicação entre os símbolos de $\mathbb{Z}_{32}$ e $\mathbb{Z}_2^{16}$ é dada pela Tabela 3.5.

3.4.5 O Caso $\mathbb{Z}_{64}$

Neste caso, utilizamos como transformação a matriz

$$T = \begin{bmatrix} 63 & 1 \\ 1 & 63 \end{bmatrix}, \tag{3.10}$$

através da qual obtemos um código, cujos vetores distribuição de pesos e representação modular são dados, respectivamente, por: $W = (4^2, 8^2, 12^2, 16^2, 20^2, 24^2, 28^2, 32^2, 36^2, 40^2, 44^2, 48^2, 52^2, 56^2, 60^2, 64^{66}, 68^2, 72^2, 76^2, 80^2, 84^2, 88^2, 92^2, 96^2, 100^2, 104^2, 108^2, 112^2, 116^2, 120^2, 124^2, 128)$ e $N = (2^2, 0, 4, 0^3, 8, 0^7, 16, 0^{15}, 32, 0^{30}, 32, 0^{32}, 2^2, 0, 4, 0^3, 8, 0^7, 16, 0^{15})$. Observe que a matriz (3.10) não apresenta determinante igual a 64, porém ela é equivalente à matriz

$$T = \begin{bmatrix} 63 & -1 \\ 1 & 1 \end{bmatrix},$$

cujo determinante é 64.

A correspondente matriz geradora do código binário é mostrada a seguir.

$$G = \begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
0&1&0&1&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1
\end{bmatrix}$$

Assim, temos a aplicação mostrada nas Tabelas 3.6 e 3.7.

Chamamos a atenção do leitor ao fato de que as regiões de Voronoi associadas às palavras dos códigos cíclicos apresentados estão relacionadas ao canal através do qual estes códigos serão transmitidos. Considere, por exemplo, o código cíclico 8-ário. No caso do canal utilizado ser simétrico (sem memória), as regiões de decisão do código são quadrados de lado $2\sqrt{2}$, centrados em cada palavra-código. Na Figura 3-5, a região $\mathbb{Z}_8 \times \mathbb{Z}_8$ é totalmente recoberta pelo quadrado mostrado através de translações deste.

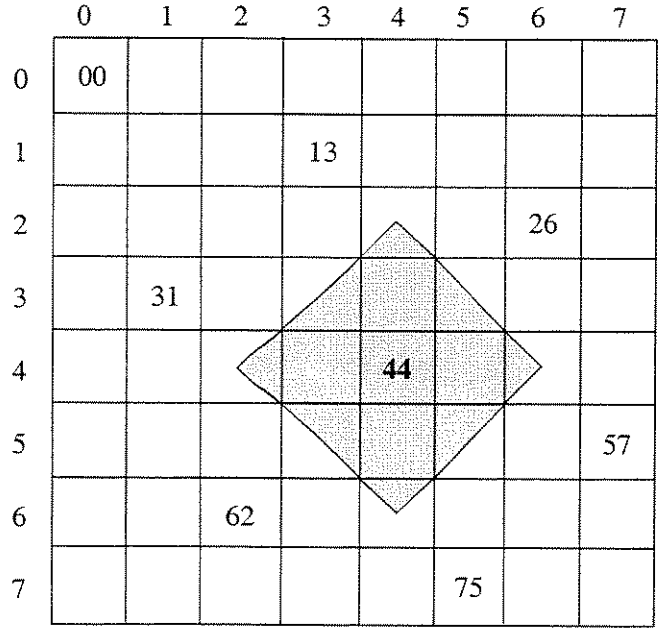

Figura 3-5: Regiões de Voronoi para um canal sem memória

Por outro lado, quando o canal não é simétrico, ou seja, apresenta memória, podemos ter como regiões de decisão as figuras geométricas apresentadas abaixo:

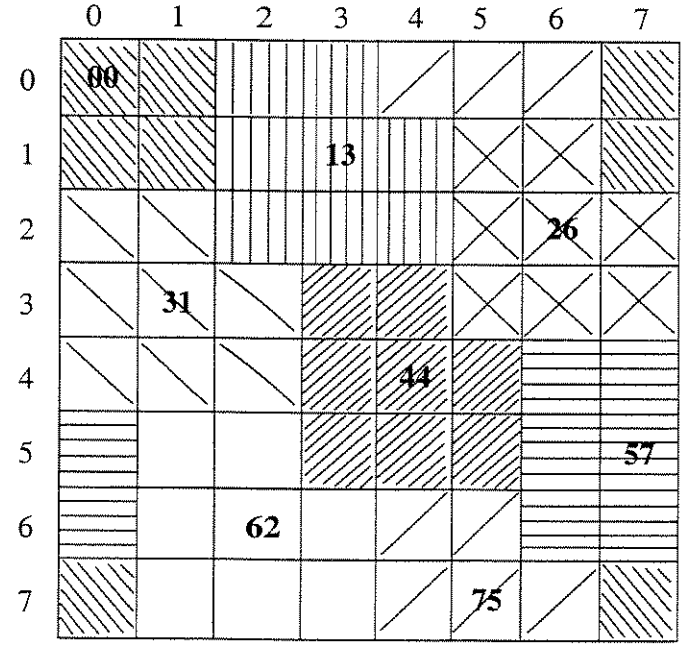

Figura 3-6: Regiões de Voronoi para um canal com memória

Como o estudo dos diferentes canais de comunicação não faz parte do escopo deste trabalho, referimos o leitor para [12] e [15].

3.5 Conclusão

Apresentamos neste capítulo um procedimento para a determinação de aplicações casadas isométricas entre os espaços de Lee e Hamming. Este procedimento baseia-se nos conceitos de particionamento de conjuntos e representacão modular e é importante pois estabelece uma forma sistemática de obtermos códigos cíclicos geometricamente uniformes em $\mathbb{Z}_{2^k}$ que usufruem da maior parte das propriedades da $\mathbb{Z}_4$-linearidade, facilitando, portanto, sua decodificação.

Podemos resumir na Tabela 3.9 as aplicações casadas isométricas obtidas e, na Tabela 3.8, se encontram as representações modulares para os alfabetos estudados.

Dentre as possíveis aplicações dos resultados obtidos, citamos: construção de códigos pseudolineares, armazenamento de dados em meios ópticos ou magnéticos, modulações digitais do tipo M-QAM e alocação de frequência em telefonia móvel, abordadas em [3], [8], [10], [1], [4] e [2].

Símbolos em $\mathbb{Z}_{32}$	Símbolos em $\mathbb{Z}_2^{16}$
0	(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
1	(0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 1)
2	(0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1)
3	(0 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0)
4	(0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0)
5	(0 1 0 1 1 1 1 1 0 0 0 0 0 1 0 1)
6	(0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 1)
7	(0 1 1 0 1 1 1 1 0 0 0 0 0 1 1 0)
8	(0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
9	(0 1 0 1 0 0 0 0 1 1 1 1 1 0 1 0)
10	(0 0 1 1 0 0 0 0 1 1 1 1 1 1 0 0)
11	(0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 1)
12	(0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1)
13	(0 1 0 1 1 1 1 1 1 1 1 1 1 0 1 0)
14	(0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0)
15	(0 1 1 0 1 1 1 1 1 1 1 1 1 0 0 1)
16	(1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
17	(1 0 1 0 1 1 1 1 1 1 1 1 1 0 1 0)
18	(1 1 0 0 1 1 1 1 1 1 1 1 1 1 0 0)
19	(1 0 0 1 1 1 1 1 1 1 1 1 1 0 0 1)
20	(1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1)
21	(1 0 1 0 0 0 0 0 1 1 1 1 1 0 1 0)
22	(1 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0)
23	(1 0 0 1 0 0 0 0 1 1 1 1 1 0 0 1)
24	(1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
25	(1 0 1 0 1 1 1 1 0 0 0 0 0 1 0 1)
26	(1 1 0 0 1 1 1 1 0 0 0 0 0 0 1 1)
27	(1 0 0 1 1 1 1 1 0 0 0 0 0 1 1 0)
28	(1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0)
29	(1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 1)
30	(1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1)
31	(1 0 0 1 0 0 0 0 0 0 0 0 0 1 1 0)

Tabela 3.5: Aplicação $m_5 : \mathbb{Z}_{32} \to \mathbb{Z}_2^{16}$

$\mathbb{Z}_{64}$	Símbolos em $\mathbb{Z}_2^{32}$
0	(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
1	(0 1 0 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
2	(0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
3	(0 1 1 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
4	(0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
5	(0 1 0 1 1 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
6	(0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
7	(0 1 1 0 1 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
8	(0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
9	(0 1 0 1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
10	(0 0 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
11	(0 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
12	(0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
13	(0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
14	(0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
15	(0 1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
16	(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
17	(0 1 0 1 0 0 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
18	(0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
19	(0 1 1 0 0 0 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
20	(0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
21	(0 1 0 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
22	(0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
23	(0 1 1 0 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
24	(0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
25	(0 1 0 1 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
26	(0 0 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
27	(0 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
28	(0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
29	(0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
30	(0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
31	(0 1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
32	(1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
33	(1 0 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
34	(1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
35	(1 0 0 1 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)

Tabela 3.6: Aplicação $m_6 : \mathbb{Z}_{64} \to \mathbb{Z}_2^{32}$

$\mathbb{Z}_{64}$	Símbolos em $\mathbb{Z}_2^{32}$
36	(1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
37	(1 0 1 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
38	(1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
39	(1 0 0 1 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
40	(1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
41	(1 0 1 0 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
42	(1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
43	(1 0 0 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
44	(1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
45	(1 0 1 0 0 0 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
46	(1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1)
47	(1 0 0 1 0 0 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0)
48	(1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
49	(1 0 1 0 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
50	(1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
51	(1 0 0 1 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
52	(1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
53	(1 0 1 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
54	(1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
55	(1 0 0 1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
56	(1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
57	(1 0 1 0 1 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
58	(1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
59	(1 0 0 1 1 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
60	(1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
61	(1 0 1 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)
62	(1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
63	(1 0 0 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1)

Tabela 3.7: Aplicação $m_6 : \mathbb{Z}_{64} \to \mathbb{Z}_2^{32}$ (cont.)

Alfabeto	Vetor Peso (W)	Vetor Tipo (N)
$\mathbb{Z}_4$	$(3,2,3)$	$(2,1,1)$
$\mathbb{Z}_8$	$(4,4,4,8,4,4,4)$	$(0,0,0,2,2,2,2)$
$\mathbb{Z}_{16}$	$(8,4,8^3,12,8,16,8,12,8^3,4,8)$	$(0^7,2,2,2,2,4,4,0,0)$
$\mathbb{Z}_{32}$	$(8^4,16^7,24^4,32,24^4,16^7,8^4)$	$(0^{15},2,2,2,2,8,0^3,10,2,2,2,0^4)$
$\mathbb{Z}_{64}$	$(4^2,8^2,12^2,16^2,20^2,24^2,28^2,32^2,36^2,40^2,44^2,48^2,$ $52^2,56^2,60^2,64^{66},68^2,72^2,76^2,80^2,84^2,88^2,92^2,$ $96^2,100^2,104^2,108^2,112^2,116^2,120^2,124^2,128)$	$(2^2,0,4,0^3,8,0^7,16,0^{15},32,$ $0^{30},32,0^{32},2^2,0,4,0^3,8,0^7,16,0^{15})$

Tabela 3.8: Tabela contendo as representações modulares

Alfabeto	Vetor Tipo (N)	Aplicação Isométrica
$\mathbb{Z}_4$	$(0,1^2)$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
$\mathbb{Z}_8$	$(0^3,1^4)$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$\mathbb{Z}_{16}$	$(0^7,1^4,2^2,0^2)$	$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$
$\mathbb{Z}_{32}$	$(0^{15},1^4,4,0^3,5,1^3,0^4)$	$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$
$\mathbb{Z}_{64}$	$(1^2,0,2,0^3,4,0^7,8,0^{15},16,$ $0^{30},16,0^{32},1^2,0,2,0^3,4,0^7,8,0^{15})$	Ver Tabelas 3.6 e 3.7

Tabela 3.9: Tabela das aplicações isométricas

UNICAMP
BIBLIOTECA CENTRAL
SEÇÃO CIRCULANTE

Capítulo 4

Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares

4.1 Introdução

Neste capítulo, apresentamos uma proposta para a construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através de códigos cíclicos BCH provenientes de extensões de Galois de dimensão r sobre anéis locais. Este procedimento faz uso das aplicações isométricas entre $(\mathbb{Z}_{2^k}, d_L)$ e $(\mathbb{Z}_2^{2^{k-1}}, d_H)$, apresentadas no Capítulo 3.

Mostramos, através de exemplos, que é possível conseguir códigos não lineares com distâncias de Hamming iguais às dos melhores códigos lineares binários já encontrados, [9]. Portanto, apresentando a mesma capacidade de correção de erros. Porém, como os rótulos das aplicações isométricas utilizadas apresentam pesos de Lee que são múltiplos de 4 e constituem um conjunto geometricamente uniforme, a complexidade do processo de decodificação é bem menor quando comparada com a complexidade de decodificação dos códigos lineares binários conhecidos que não apresentam estas características, [13] e [19].

Em contrapartida, comprovamos o fato que pôde ser observado no capítulo anterior de que o comprimento n do código cresce exponencialmente com sua ordem k. Isto acaba

por impossibilitar que um código, cuja diferença $n - k$ é grande, apresente uma boa distância mínima, ou seja, uma distância igual ou superior a do código linear binário equivalente.

Primeiramente, na Seção 4.2, fazemos uma revisão dos fundamentos necessários para a construção de códigos cíclicos sobre anéis comutativos finitos locais. Na Seção 4.3, apresentamos os principais conceitos relacionados à extensão de Galois sobre anéis e sua relação com a extensão de Galois sobre corpos. A seguir, na Seção 4.4, fazemos uma breve descrição dos códigos BCH sobre anéis e, em seguida, consideramos a construção de códigos BCH sobre os anéis $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{16}$, $\mathbb{Z}_{32}$ e $\mathbb{Z}_{64}$. Definimos os códigos alternantes sobre $\mathbb{Z}_4$ e $\mathbb{Z}_8$ através de uma pequena modificação na matriz verificação de paridade dos códigos BCH na Subseção 4.4.2. Na Seção 4.5, descrevemos o procedimento proposto para a construção dos códigos $\mathbb{Z}_{2^k}$-pseudolineares e apresentamos os códigos obtidos através dos códigos cíclicos provenientes da extensão de Galois de dimensão r sobre anéis de inteiros finitos. Finalmente, na Seção 4.6, apresentamos as conclusões sobre este capítulo.

4.2 Códigos Cíclicos sobre Anéis de Inteiros Residuais

Apresentamos nesta seção definições e teoremas relacionados a códigos cíclicos sobre anéis $\mathbb{Z}_q$ ($q \geq 4$ e inteiro). Esta teoria servirá de base para o desenvolvimento dos códigos BCH, a ser feito na Seção 4.4. Nossa principal referência é [20].

Definição 4.2.1 *Seja R um anel. Um* ***módulo livre*** *é um R-módulo gerado por um conjunto de vetores linearmente independentes.*

Definição 4.2.2 *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 4.2.3 *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 $v_i \in \mathbb{Z}_q$, $0 \leq i \leq n-1$.*

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

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

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

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

que corresponde à palavra-código:

$$\underline{v}^{(1)} = (v_{n-1}\ v_0\ v_1\ \ldots\ v_{n-2}),$$

a qual é um deslocamento cíclico da palavra:

$$\underline{v} = (v_0\ v_1\ v_2\ \ldots\ v_{n-1}).$$

Portanto, $v^{(1)}(x)$ é obtido através do produto $x.v(x)$ 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 $\mathbb{Z}_q[x]$.

Note 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 do que n.

Teorema 4.2.1 *Um conjunto S de elementos em R_n é um código cíclico se, e somente se, S é um ideal em R_n.*

Exemplo 4.2.1 *Considere o anel* $\mathbb{Z}_4$ *e o anel quociente* $R_2 = \dfrac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}$. *Pelo Teorema 4.2.1, temos que o ideal* $\mathcal{C} = \{0, 2, 2x, 2+2x, 1+3x, 3+x, 3+3x, 1+x\}$ *de* R_2 *é um código cíclico.*

Proposição 4.2.1 *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 inversível em* $\mathbb{Z}_q$, *então o polinômio mônico (ou seja, aquele cujo coeficiente dominante é um) de grau mínimo em* $\mathcal{C}$ *é único.*

Teorema 4.2.2 *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* $\mathcal{C}$. *Assim,* $\mathcal{C} = \langle g(x)\rangle$, *e portanto, o código* $\mathcal{C}$ *consiste de todos os múltiplos de* $g(x)$. *Dizemos então que* $\mathcal{C}$ *é um* ***ideal principal.***

Teorema 4.2.3 *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 inversível, então* $g(x)$ *divide* (x^n-1). *Note que se este polinômio for mônico, então* $g(x)$ *divide* (x^n-1).

Teorema 4.2.4 *Se* $g(x) \in \mathcal{C}$ *e* $g(x)$ *divide* (x^n-1), *então* $g(x)$ *tem grau mínimo em* $\mathcal{C} = \langle g(x)\rangle$.

Os Teoremas 4.2.3 e 4.2.4 fornecem um método de construção de códigos cíclicos sobre anéis de inteiros residuais análogo ao método de construção de códigos cíclicos sobre corpos finitos, ou seja, através da fatoração do polinômio (x^n-1) sobre o anel de interesse para então tomar um fator (ou produto de fatores) como polinômio gerador do código em questão.

O próximo teorema está relacionado à representação matricial dos códigos cíclicos sobre anéis que possuem uma matriz geradora.

Teorema 4.2.5 *Se* $g(x)$ *divide* (x^n-1) *e o grau de* $g(x)$ *é* $(n-k)$, *então a dimensão de* $\mathcal{C} = \langle g(x)\rangle$ *é* k. *Se*

$$g(x) = g_0 + g_1x + g_2x^2 + ... + x^{n-k},$$

então a matriz geradora do código $\mathcal{C}$ é dada por:

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

Proposição 4.2.2 *Se $\mathcal{C}$ é um código cíclico sobre $\mathbb{Z}_q$ onde $q = p_1^{k_1} p_2^{k_2} ... p_q^{k_q}$, então*

$$\mathcal{C} = \bigoplus_{i=1}^{q} \mathcal{C}_i,$$

onde $\mathcal{C}_i$ é um código cíclico sobre $\mathbb{Z}_{p_i^{k_i}}$, $1 \leq i \leq q$.

4.3 Extensão de Anéis de Galois

A motivação para se utilizar o 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, $q = p^k$, $k \geq 2$.

A principal diferença da construção de códigos cíclicos sobre anéis para a construção de códigos cíclicos 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 $F_q \cong GF(p^r)$.

Neste sentido, temos a seguinte definição:

Definição 4.3.1 *Um código cíclico sobre $\mathbb{Z}_q$ com comprimento $n = q^r - 1$, onde $q = p^k$ e r é o grau da extensão de Galois, é denominado* ***código cíclico primitivo.***

Iremos considerar o caso em que p e n são relativamente primos, isto é, o máximo divisor comum é um, denotado por $mdc(n, p) = 1$, pois assim garantimos que $(x^n - 1)$

não apresenta fatores quadráticos. Da Seção 4.2, sabemos que um código cíclico de comprimento n sobre $\mathbb{Z}_q$ é o ideal principal no anel de polinômios sobre $\mathbb{Z}_q$ 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 $GF(p)$ e, consequentemente, sobre $\mathbb{Z}_q$. Representamos por $GR(p^k, r)$ o quociente $\mathbb{Z}_q[x]$ pelo ideal gerado por $p(x)$, ou seja,

$$R \cong GR(p^k, r) \cong \frac{\mathbb{Z}_q[x]}{\langle p(x) \rangle}.$$

Assim, o anel R é formado por todas as classes laterais de polinômios em x sobre $\mathbb{Z}_q \bmod p(x)$, isto é, consiste do conjunto dos polinômios de grau menor ou igual a $r-1$ cujas operações binárias de adição e multiplicação são tomadas módulo $p(x)$. 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 [25].

Dizemos que o anel $R \cong GR(p^k, r)$ é um **anel local** [25], 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 $\mathbb{Z}_q$. Um polinômio $p(x) \in R$ com pelo menos um coeficiente inversível em $\mathbb{Z}_q$ não é um divisor de zero em R e, portanto, pertence a R^* (grupo das unidades de R), ou seja, é sempre possível encontrar um polinômio $q(x) \in R$, tal que $p(x) \cdot q(x) = 1$.

Vale lembrar que, da Definição 4.2.3, temos:

Definição 4.3.2 *[21]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 4.3.3 *[21]Um polinômio $p(x)$ é dito **regular** se ele não é um divisor de zero no anel $\mathbb{Z}_q[x]$.*

Definição 4.3.4 *[21]Um polinômio regular $p(x)$ é chamado **local** se $\frac{\mathbb{Z}_q[x]}{\langle p(x) \rangle}$ é uma extensão local de $\mathbb{Z}_q$.*

A irredutibilidade do polinômio $p(x)$ sobre $\mathbb{Z}_q$ é garantida pelo seguinte teorema:

Teorema 4.3.1 *[21] Seja $p(x)$ um polinômio regular em $\mathbb{Z}_q$. Se existe uma aplicação μ, chamada projeção natural, tal que $\mu(p(x))$ seja diferente de zero e irredutível em $GF(p)$, então $p(x)$ é irredutível em $\mathbb{Z}_q$.*

Como estamos interessados na classe dos códigos cíclicos, nosso objetivo é fornecer um procedimento para a construção de tais códigos. O primeiro passo está relacionado com a fatoração de $(x^n - 1)$. Como o grupo das unidades de R, R^*, é um grupo abeliano multiplicativo, ele pode ser expresso como um produto de grupos cíclicos. Uma vez encontrado este grupo multiplicativo, 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 $(x^n - 1)$.

Os resultados a seguir fornecem os elementos necessários para a construção do subgrupo cíclico G_n do grupo multiplicativo R^*, que contém todas as raízes de $(x^n - 1)$.

Teorema 4.3.2 *[25] Existe um único subgrupo cíclico de R^* cuja ordem é relativamente prima a p. Este subgrupo tem ordem $p^r - 1$.*

Teorema 4.3.3 *[28] 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 $x^n - 1 = (x - f)(x - f^2) \cdots (x - f^n)$ se, e somente se, $R_p(f)$ tem ordem n em F^* (grupo multiplicativo de $GF(p^r)$), onde $R_p(f)$ é o resto da divisão de f por p (redução de f módulo p).*

Corolário 4.3.1 *[28] Um polinômio $h(x)$, que divide $(x^n - 1)$ e tem coeficientes em $\mathbb{Z}_q$, pode ser fatorado sobre G_n como:*

$$h(x) = (x - \beta^{e_1})(x - \beta^{e_2}) \cdots (x - \beta^{ej}),$$

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

$$R_p(h(x)) = (x - (R_p(\beta))^{e_1})(x - (R_p(\beta))^{e_2}) \cdots \left(x - (R_p(\beta))^{ej}\right),$$

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

Teorema 4.3.4 *[28] Suponha que* $\overline{f} = R_p(f)$ *gere um subgrupo cíclico de ordem* n *em* 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_n *de* R^*.

O subgrupo cíclico G_n é obtido do Teorema 4.3.4, enquanto que, pelo Corolário 4.3.1, o polinômio minimal $M_i(x)$ associado ao elemento β^i sobre R^* (onde β é um elemento primitivo em G_n), tem como suas raízes todos elementos na sequência

$$\beta^i, (\beta^i)^p, (\beta^i)^{p^2}, \cdots, (\beta^i)^{p^{r-1}}.$$

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

Temos ainda a seguinte propriedade:

Teorema 4.3.5 *[20]Seja* β *um elemento primitivo em* G_n, *onde* $n = p^r - 1$. *Então o elemento* $\delta = \beta^{l_1} - \beta^{l_2}$ *possui inverso em* R *se* $0 \leq l_1 \neq l_2 \leq n - 1$.

4.4 Códigos BCH sobre Anéis

Os códigos BCH formam uma importante classe de códigos cíclicos devido, principalmente, à simplicidade dos processos de codificação e decodificação associados, o que os torna bons candidatos a serem utilizados em aplicações práticas. Os códigos BCH foram descobertos por R. C. Bose, D. K. Chaudhuri e A. Hocquenghem e representam uma excelente generalização dos códigos de Hamming, permitindo a múltipla correção de er-

ros. Formam assim a classe dos melhores códigos construtivos para canais onde os erros afetam os símbolos de forma independente.

Apesar de ser sempre possível projetar um código BCH que corrija até t erros, para um t qualquer, devemos interpretar esta afirmação com uma certa restrição, pois as taxas desses códigos são assintoticamente ruins. Ou seja, quando o comprimento das palavras-código não é grande, existem bons códigos BCH, caso contrário, o desempenho destes é prejudicado devido às baixas taxas de transmissão. Contudo, a real importância dos códigos BCH vem da facilidade de implementação do algoritmo de correção de erros, algoritmo de Berlekamp-Massey modificado [20]. A seguir, fazemos algumas considerações sobre os códigos BCH e posteriormente passamos à construção de tais códigos. Referimos o leitor para [20].

Definição 4.4.1 *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*

$$\beta^m, \beta^{m+1}, \beta^{m+2}, \cdots, \beta^{m+d-2},$$

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

Assim, analogamente à Definição 4.3.1, temos:

Definição 4.4.2 *Se $n = p^r - 1$, ou seja, se β for um elemento primitivo em F_q, então o código BCH é chamado de* ***primitivo.***

Normalmente, consideramos $m = 1$, 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 $\beta, \beta^2, \beta^3, \cdots, \beta^{2t}$ e seus conjugados como raízes

de cada um de seus polinômios. Esta propriedade, juntamente com a Definição 4.2.3 de códigos cíclicos sobre anéis $\mathbb{Z}_q$, nos permite especificar a seguinte matriz:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \left(\beta^2\right)^2 & \cdots & \left(\beta^2\right)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{2t} & \left(\beta^{2t}\right)^2 & \cdots & \left(\beta^{2t}\right)^{n-1} \end{bmatrix} \tag{4.1}$$

A matriz H em (4.1) é a matriz verificação de paridade para um código BCH. Note que os elementos β^i, $1 \leq i \leq 2t$ de H pertencem a G_n, e portanto, os coeficientes de β são tomados módulo n. Substituindo os elementos β^i pelos vetores linha de comprimento r (r-uplas) correspondentes, temos a matriz H sobre $\mathbb{Z}_q$.

Estamos interessados na construção de códigos BCH sobre anéis $\mathbb{Z}_q$, para $q = p^k$ e $k \geq 2$, a qual é análoga à construção de códigos BCH sobre corpos [28]. A diferença entre essas duas construções reside 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 F_q, como visto na Seção 4.3. Vale lembrar também que iremos considerar o caso no qual $mdc\,(n, p) = 1$.

Podemos especificar um código BCH de comprimento n sobre $\mathbb{Z}_q$, onde $n = p^r - 1$, em termos das raízes de seu polinômio gerador $g\,(x)$, que pertencem ao subgrupo cíclico G_n (vide Seção 4.3). Seja β um elemento primitivo de G_n. Se $\beta^{e_1}, \beta^{e_2}, ..., \beta^{e_j}$ são raízes de $g\,(x)$, então podemos gerar um código BCH com símbolos de $\mathbb{Z}_q$ se escolhermos $g\,(x)$ como:

$$g\,(x) = mmc\left(M_{e_1}\,(x), M_{e_2}\,(x), \cdots, M_{e_j}\,(x)\right),$$

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

$$\overline{g}\,(x) = R_p\left(g\,(x)\right) = mmc\left(m_{e_1}\,(x), m_{e_2}\,(x), \cdots, m_{e_j}\,(x)\right),$$

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

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

Observação 4.4.1 *O método sistemático para o cálculo do mínimo múltiplo comum de um conjunto de polinômios* $\{p_1(x), p_2(x), \cdots, p_n(x)\}$ *é computar o máximo divisor comum, mdc, através do Algoritmo de Euclides e então utilizar a seguinte relação:*

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

Os próximos teoremas estabelecem um limitante inferior para a distância de Hamming do código BCH construído:

Teorema 4.4.1 *Seja* $g(x)$ *o polinômio gerador de um código cíclico de comprimento* n *com símbolos de* $\mathbb{Z}_q$ *e sejam também* $\beta^{e_1}, \beta^{e_2}, ..., \beta^{e_j}$ *as raízes de* $g(x)$ *em* G_n*, onde* β *tem ordem* n*. Então, a distância mínima do código é maior que o número máximo de inteiros consecutivos módulo* n *no conjunto* $\{e_1, e_2, \cdots, e_j\}$.

Teorema 4.4.2 *A distância de Hamming mínima de um código BCH satisfaz a relação:*

$$d \geq 2t + 1,$$

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

Note que os polinômios geradores dos códigos BCH cíclicos são construídos de forma a respeitar o limitante para a distância mínima indicado nos Teoremas 4.4.1 e 4.4.2.

4.4.1 Construção de Códigos BCH sobre Anéis: Exemplos

Nesta subseção, apresentamos a construção de códigos BCH sobre anéis locais $\mathbb{Z}_q$ de ordem $n = p^r - 1$, onde $q = p^k$, $p = 2$, $2 \leq k \leq 6$ e r é o grau da extensão de Galois.

Mais especificamente, estamos interessados em códigos BCH sobre anéis locais $\mathbb{Z}_{p^k}$, com $2 \leq k \leq 6$. Os códigos BCH aqui apresentados, juntamente com as aplicações casadas isométricas obtidas no Capítulo 3, servirão de base para a construção dos códigos $\mathbb{Z}_{2^k}$-pseudolineares na Seção 4.5. Sendo assim, considere os exemplos a seguir.

Códigos BCH sobre $\mathbb{Z}_4$

Apresentamos aqui a construção de códigos BCH sobre o anel $\mathbb{Z}_4$ através de extensões de Galois de grau 2, 3 e 4.

Primeiramente, considere o anel $GR\left(p^k, r\right) = GR\left(4, 2\right)$ dado pela extensão de Galois de grau 2:

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

Considere ainda o corpo $GF\left(p^r\right) = GF\left(4\right)$:

$$GF\left(4\right)\left[x\right] \cong F_4[x] \cong \frac{F_2[x]}{\langle x^2 + x + 1\rangle} = \left\{a' + b'x;\ a', b' \in F_2\right\} = \left\{0, 1, x, 1 + x\right\}. \qquad (4.2)$$

Seja α um elemento primitivo em F_4, equivalentemente, α é uma raiz de $x^2+x+1 = 0$, ou seja, $\alpha^2 = \alpha + 1$. Assim, F_4 apresenta os seguintes elementos:

$0 \rightarrow \begin{pmatrix} 0 & 0 \end{pmatrix}$
$1 \rightarrow \begin{pmatrix} 1 & 0 \end{pmatrix}$
$\alpha \rightarrow \begin{pmatrix} 0 & 1 \end{pmatrix}$
$\alpha^2 \rightarrow \begin{pmatrix} 1 & 1 \end{pmatrix}$

Tabela 4.1: Elementos de F_4

Seja $f = (0\ 1) \in GR^*\left(4, 2\right)$, onde $GR^*\left(4, 2\right)$ denota o grupo das unidades de $GR\left(4, 2\right)$. Então, $\overline{f} = R_2\left(f\right) = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = \left(p^r - 1\right) = 3$ em F_4, onde lembramos que $R_2\left(f\right)$ é a redução módulo 2 do elemento f. Assim, pelo Teorema 4.3.4, temos que f deve gerar um grupo de ordem $nd = 3d$ em $GR^*\left(4, 2\right)$, 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 feitas 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 de $GR^*(4,2)$ é como mostrada na Tabela 4.2.

$0 \rightarrow$	$(0\ \ 0)$
$1 \rightarrow$	$(1\ \ 0)$
$f \rightarrow$	$(0\ \ 1)$
$f^2 \rightarrow$	$(3\ \ 3)$
$f^3 \rightarrow$	$(1\ \ 0)$

Tabela 4.2: Elementos de $GR^*(4,2)$

Portanto, $nd=3$ implicando que $d=1$. Logo, f gera um grupo de ordem 1 em $GR^*(4,2)$ e, consequentemente, $f=x=(0\ 1)$ gera 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 $\mathbb{Z}_4$. Considerando que a distância de projeto (distância de Hamming) do código seja $d\geq 3$, o polinômio gerador $g(x)$ do código tem como raízes β e β^2. Este polinômio é dado por $g(x)=mmc\left(M_1(x),M_2(x)\right)$, onde $M_i(x)$ é o polinômio minimal de β^i, $i=1,2$.

O polinômio minimal de β é dado por:

$$M_1(x)=(x-\beta)\left(x-\beta^2\right)=1+x+x^2.$$

Note que os polinômios minimais de β e β^2 são iguais, isto é,

$$M_2(x)=M_1(x).$$

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

$$\mathrm{G}=\begin{bmatrix}1 & 1 & 1\end{bmatrix}. \tag{4.3}$$

A matriz verificação de paridade correspondente, geradora do código dual associado, é dada por:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 3 & 3 \\ 1 & 0 & 3 & 3 & 0 & 1 \end{bmatrix}. \tag{4.4}$$

Considere agora o anel $GR\left(p^k, r\right) = GR\left(4, 3\right)$ dado pela extensão de grau 3 abaixo:

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

Considere ainda o corpo $GF\left(p^r\right) = GF\left(8\right)$:

$$GF\left(8\right)[x] \cong F_8[x] \cong \frac{F_2[x]}{\langle x^3 + x + 1\rangle} = \left\{a' + b'x + c'x^2;\ a', b', c' \in F_2\right\} =$$

$$= \left\{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\right\}.$$

Analogamente à extensão de Galois de grau 2, F_8 apresenta os seguintes elementos:

$0 \rightarrow$	$(\ 0\ \ 0\ \ 0\ )$
$1 \rightarrow$	$(\ 1\ \ 0\ \ 0\ )$
$\alpha \rightarrow$	$(\ 0\ \ 1\ \ 0\ )$
$\alpha^2 \rightarrow$	$(\ 0\ \ 0\ \ 1\ )$
$\alpha^3 \rightarrow$	$(\ 1\ \ 1\ \ 0\ )$
$\alpha^4 \rightarrow$	$(\ 0\ \ 1\ \ 1\ )$
$\alpha^5 \rightarrow$	$(\ 1\ \ 1\ \ 1\ )$
$\alpha^6 \rightarrow$	$(\ 1\ \ 0\ \ 1\ )$

Tabela 4.3: Elementos de F_8

Seja $f = (0\ 1\ 0) \in GR^*\left(4,3\right)$. Então, $\overline{f} = R_2\left(f\right) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (p^r - 1) = 7$ em F_8. Assim, pelo Teorema 4.3.4, 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, $x^3 = 3x + 3$, pois os coeficientes de $GR^*(4,3)$ estão em $\mathbb{Z}_4$. Assim, considerando $f = (0\ 1\ 0) = x$, temos a seguinte representação dos elementos de $GR^*(4,3)$:

$0 \rightarrow (0\ 0\ 0)$	$f^7 \rightarrow (3\ 0\ 2)$
$1 \rightarrow (1\ 0\ 0)$	$f^8 \rightarrow (2\ 1\ 0)$
$f \rightarrow (0\ 1\ 0)$	$f^9 \rightarrow (0\ 2\ 1)$
$f^2 \rightarrow (0\ 0\ 1)$	$f^{10} \rightarrow (3\ 2\ 2)$
$f^3 \rightarrow (3\ 3\ 0)$	$f^{11} \rightarrow (2\ 1\ 3)$
$f^4 \rightarrow (0\ 3\ 3)$	$f^{12} \rightarrow (1\ 3\ 1)$
$f^5 \rightarrow (1\ 1\ 3)$	$f^{13} \rightarrow (3\ 0\ 3)$
$f^6 \rightarrow (1\ 2\ 1)$	$f^{14} \rightarrow (1\ 0\ 0)$

Tabela 4.4: Elementos de $GR^*(4,3)$

Portanto, $nd = 14$ implicando que $d = 2$. Logo, f gera um grupo de ordem 14 em $GR^*(4,3)$ e, consequentemente, $f^2 = x^2 = (0\ 1\ 0)$ gera 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 de projeto do código seja $d \geq 3$, o polinômio gerador $g(x)$ do código tem como raízes β e β^2.

Os polinômios minimais de β e β^2 são dados por:

$$M_1(x) = M_2(x) = (x - \beta)\left(x - \beta^2\right) = 3 + x + 2x^2 + x^3.$$

O polinômio gerador deste código é dado por $g(x) = mmc(M_1(x), M_2(x))$ e gera o

código BCH desejado, correspondendo à seguinte matriz geradora:

$$\mathrm{G} = \begin{bmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{bmatrix} \tag{4.5}$$

A matriz verificação de paridade correspondente, geradora do código dual associado, é dada por:

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

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

Considere ainda o anel $GR\left(p^k, r\right) = GR\left(4, 4\right)$ dado pela extensão de grau 4 abaixo:

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

O corpo de Galois $GF\left(p^r\right) = GF\left(16\right)$ é dado por:

$$GF\left(16\right)[x] \cong F_{16}[x] \cong \frac{F_2[x]}{\langle x^4 + x + 1 \rangle} = \left\{ a' + b'x + c'x^2 + d'x^3;\ a', b', c', d' \in F_2 \right\} =$$

$$= \left\{ \begin{array}{c} 0, 1, x, x^2, x^3, 1 + x, 1 + x^2, 1 + x^3, x + x^2, x + x^3, x^2 + x^3, \\ 1 + x + x^2, 1 + x + x^3, x + x^2 + x^3, 1 + x + x^2 + x^3 \end{array} \right\}.$$

Assim, F_{16} é formado pelos elementos contidos na Tabela 4.5.

Seja $f = (0\ 1\ 0\ 0) \in GR^*\left(4, 4\right)$. Então, $\overline{f} = (0\ 1\ 0\ 0) = f$ gera um subgrupo cíclico

$0 \rightarrow$	0	0	0	0	$\alpha^7 \rightarrow$	1	1	0	1
$1 \rightarrow$	1	0	0	0	$\alpha^8 \rightarrow$	1	0	1	0
$\alpha \rightarrow$	0	1	0	0	$\alpha^9 \rightarrow$	0	1	0	1
$\alpha^2 \rightarrow$	0	0	1	0	$\alpha^{10} \rightarrow$	1	1	1	0
$\alpha^3 \rightarrow$	0	0	0	1	$\alpha^{11} \rightarrow$	0	1	1	1
$\alpha^4 \rightarrow$	1	1	0	0	$\alpha^{12} \rightarrow$	1	1	1	1
$\alpha^5 \rightarrow$	0	1	1	0	$\alpha^{13} \rightarrow$	1	0	1	1
$\alpha^6 \rightarrow$	0	0	1	1	$\alpha^{14} \rightarrow$	1	0	0	1

Tabela 4.5: Elementos de F_{16}

de ordem $n = 15$ em F_{16}. Pelo Teorema 4.3.4, f deve gerar um grupo de ordem $nd = 15d$ em $GR^*(4,4)$.

As operações em $GR^*(4,4)$ são feitas módulo $x^4 + x + 1$. Logo, $x^4 = 3x + 3$, pois os coeficientes de $GR^*(4,4)$ estão em $\mathbb{Z}_4$. Assim, considerando $f = (0\ 1\ 0\ 0) = x$, os elementos de $GR^*(4,4)$ são dados na Tabela 4.6.

$0 \rightarrow$	0	0	0	0	$f^{10} \rightarrow$	3	3	1	2	$f^{21} \rightarrow$	2	2	1	3
$1 \rightarrow$	1	0	0	0	$f^{11} \rightarrow$	2	1	3	1	$f^{22} \rightarrow$	1	3	2	1
$f \rightarrow$	0	1	0	0	$f^{12} \rightarrow$	3	1	1	3	$f^{23} \rightarrow$	3	0	3	2
$f^2 \rightarrow$	0	0	1	0	$f^{13} \rightarrow$	1	0	1	1	$f^{24} \rightarrow$	2	1	0	3
$f^3 \rightarrow$	0	0	0	1	$f^{14} \rightarrow$	3	0	0	1	$f^{25} \rightarrow$	1	3	1	0
$f^4 \rightarrow$	3	3	0	0	$f^{15} \rightarrow$	3	2	0	0	$f^{26} \rightarrow$	0	1	3	1
$f^5 \rightarrow$	0	3	3	0	$f^{16} \rightarrow$	0	3	2	0	$f^{27} \rightarrow$	3	3	1	3
$f^6 \rightarrow$	0	0	3	3	$f^{17} \rightarrow$	0	0	3	2	$f^{28} \rightarrow$	1	0	3	1
$f^7 \rightarrow$	1	1	0	3	$f^{18} \rightarrow$	2	2	0	3	$f^{29} \rightarrow$	3	0	0	3
$f^8 \rightarrow$	1	2	1	0	$f^{19} \rightarrow$	1	3	2	0	$f^{30} \rightarrow$	1	0	0	0
$f^9 \rightarrow$	0	1	2	1	$f^{20} \rightarrow$	0	1	3	2					

Tabela 4.6: Elementos de $GR^*(4,4)$

Portanto, $nd = 30$ e, consequentemente, $d = 2$. Logo, f gera um grupo de ordem 30 em $GR^*(4,4)$ e $f^2 = x^2 = (0\ 0\ 1\ 0)$ gera um grupo de ordem 15 em $GR^*(4,4)$. Logo, $\beta = x^2$ é um elemento primitivo em G_{15}.

Podemos agora construir um código BCH de comprimento $n = 15$ sobre $\mathbb{Z}_4$. Considerando que a distância de projeto do código seja $d \geq 7$, o polinômio gerador $g(x)$ do código tem como raízes β, β^2, β^3, β^4, β^5 e β^6. Este polinômio é dado por

UNICAMP
BIBLIOTECA CENTRAL

$g(x) = mmc(M_1(x), M_2(x), M_3(x), M_4(x), M_5(x), M_6(x))$, onde $M_i(x)$ é o polinômio minimal de β^i, $i = 1, 2, 3, 4, 5, 6$. Assim, temos:

$$M_1(x) = (x-\beta)\left(x-\beta^2\right)\left(x-\beta^4\right)\left(x-\beta^8\right) = 1 + 3x + 2x^2 + x^4$$

$$M_3(x) = \left(x-\beta^3\right)\left(x-\beta^6\right)\left(x-\beta^9\right)\left(x-\beta^{12}\right) = 1 + x + x^2 + x^3 + x^4$$

$$M_5(x) = \left(x-\beta^5\right)\left(x-\beta^{10}\right) = 1 + x + x^2$$

Note que $M_1(x) = M_2(x) = M_4(x)$ e que $M_6(x) = M_3(x)$.

O polinômio gerador $g(x)$ é dado por:

$$g(x) = mmc(M_1(x), M_3(x), M_5(x)).$$

Assim, $g(x) = 1 + x + 3x^2 + 3x^4 + 3x^5 + 2x^7 + x^8 + 2x^9 + x^{10}$ gera o código BCH desejado. Este polinômio gerador está relacionado à seguinte matriz geradora:

$$\mathrm{G} = \begin{bmatrix} 1 & 1 & 3 & 0 & 3 & 3 & 0 & 2 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 3 & 0 & 3 & 3 & 0 & 2 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 3 & 0 & 3 & 3 & 0 & 2 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 3 & 0 & 3 & 3 & 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 & 3 & 3 & 0 & 2 & 1 & 2 & 1 \end{bmatrix}$$

A matriz verificação de paridade correspondente, geradora do código dual associado,

é dada por:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 & \beta^{10} & \beta^{11} & \beta^{12} & \beta^{13} & \beta^{14} \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} & \beta^{12} & \beta^{14} & \beta & \beta^3 & \beta^5 & \beta^7 & \beta^9 & \beta^{11} & \beta^{13} \\ 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} \\ 1 & \beta^4 & \beta^8 & \beta^{12} & \beta & \beta^5 & \beta^9 & \beta^{13} & \beta^2 & \beta^6 & \beta^{10} & \beta^{14} & \beta^3 & \beta^7 & \beta^{11} \\ 1 & \beta^5 & \beta^{10} & 1 & \beta^5 & \beta^{10} & 1 & \beta^5 & \beta^{10} & 1 & \beta^5 & \beta^{10} & 1 & \beta^5 & \beta^{10} \\ 1 & \beta^6 & \beta^{12} & \beta^3 & \beta^9 & 1 & \beta^6 & \beta^{12} & \beta^3 & \beta^9 & 1 & \beta^6 & \beta^{12} & \beta^3 & \beta^9 \end{bmatrix},$$

onde $\beta = x^2 = (0\ 0\ 1\ 0)$.

Códigos BCH sobre $\mathbb{Z}_8$

Consideramos agora a construção de códigos BCH sobre o anel $\mathbb{Z}_8$ através de extensões de Galois de grau 2 e 3. O procedimento adotado é análogo ao desenvolvido nos exemplos da construção de códigos BCH sobre o anel $\mathbb{Z}_4$. Dessa forma, omitiremos algumas passagens redundantes, cuja omissão não prejudica o entendimento do trabalho, a fim de evitar que a leitura deste se torne repetitiva e tediosa.

Sendo assim, sejam o anel R e o corpo F_4 gerados pelas seguintes extensões de grau 2:

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

$$GF\,(4)\,[x] \cong F_4[x] \cong \frac{F_2[x]}{\langle x^2+x+1\rangle} = \{a'+b'x;\ a',b' \in F_2\} = \{0,1,x,1+x\}\,.$$

Observe que corpo F_4 acima é idêntico ao obtido na Equação (4.2), já que o polinômio utilizado em ambas extensões é o mesmo. Portanto, para α primitivo em F_4, os elementos deste corpo são aqueles mostrados na Tabela 4.2.

Seja $f = (0\ 1) \in GR^*\,(8,2)$. Então, $\overline{f} = (0\ 1) = f$ gera um subgrupo cíclico de ordem

$n = 3$ em F_4. Assim, pelo Teorema 4.3.4, 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 $x^2 = 7x + 7$. Assim, para $f = (0\ 1) = x$, a representação dos elementos de $GR^*(8,2)$ é como mostrada na Tabela 4.7.

$0 \rightarrow$	$(0\ \ 0)$
$1 \rightarrow$	$(1\ \ 0)$
$f \rightarrow$	$(0\ \ 1)$
$f^2 \rightarrow$	$(7\ \ 7)$
$f^3 \rightarrow$	$(1\ \ 0)$

Tabela 4.7: Elementos de $GR^*(8,2)$

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

Para a distância mínima de projeto do código BCH sobre $\mathbb{Z}_8$ igual a 3, o polinômio gerador $g(x)$ tem como raízes β e β^2, o que nos fornece $g(x) = mmc(M_1(x), M_2(x))$. Assim, temos:

$$M_1(x) = M_2(x) = (x - \beta)\left(x - \beta^2\right) = 1 + x + x^2.$$

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

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

A matriz verificação de paridade correspondente é dada por:

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

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

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

$$GF\,(8)\,[x] \cong F_8[x] \cong \frac{F_2[x]}{\langle x^3+x+1\rangle} = \left\{a'+b'x+c'x^2;\ a',b',c' \in F_2\right\} =$$

$$= \left\{0,1,x,x^2,1+x,1+x^2,x+x^2,1+x+x^2\right\}.$$

O corpo F_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 F_8. Pelo Teorema 4.3.4, f deve gerar um grupo de ordem $nd = 7d$ em $GR^*\,(8,3)$.

Em $GR^*(8,3)$, temos $x^3 = 3x+3$ (coeficientes em $\mathbb{Z}_8$). Assim, para $f = (0\ 1\ 0) = x$, os elementos de $GR^*(8,3)$ são os representados na Tabela 4.8.

$0 \to (0\ 0\ 0)$	$f^9 \to (0\ 6\ 5)$	$f^{19} \to (5\ 1\ 3)$
$1 \to (1\ 0\ 0)$	$f^{10} \to (3\ 3\ 6)$	$f^{20} \to (5\ 2\ 1)$
$f \to (0\ 1\ 0)$	$f^{11} \to (2\ 5\ 3)$	$f^{21} \to (7\ 4\ 2)$
$f^2 \to (0\ 0\ 1)$	$f^{12} \to (5\ 7\ 5)$	$f^{22} \to (6\ 5\ 4)$
$f^3 \to (7\ 7\ 0)$	$f^{13} \to (3\ 0\ 7)$	$f^{23} \to (4\ 2\ 5)$
$f^4 \to (0\ 7\ 7)$	$f^{14} \to (1\ 4\ 0)$	$f^{24} \to (3\ 7\ 2)$
$f^5 \to (1\ 1\ 7)$	$f^{15} \to (0\ 1\ 4)$	$f^{25} \to (6\ 1\ 7)$
$f^6 \to (1\ 2\ 1)$	$f^{16} \to (4\ 4\ 1)$	$f^{26} \to (1\ 7\ 1)$
$f^7 \to (7\ 0\ 2)$	$f^{17} \to (7\ 3\ 4)$	$f^{27} \to (7\ 0\ 7)$
$f^8 \to (6\ 5\ 0)$	$f^{18} \to (4\ 3\ 3)$	$f^{28} \to (1\ 0\ 0)$

Tabela 4.8: Elementos de $GR^*\,(8,3)$

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

Para a distância mínima de projeto do código BCH sobre $\mathbb{Z}_8$ igual a 3, $g(x)$ tem como raízes β e β^2, o que nos fornece $g(x) = mmc(M_1(x), M_2(x))$. Assim, temos:

$$M_1(x) = M_2(x) = (x-\beta)\left(x-\beta^2\right) = 7 + 5x + 6x^2 + x^3.$$

Assim, $g(x) = 7 + 5x + 6x^2 + x^3$ gera o código BCH desejado e está relacionado à seguinte matriz geradora:

$$G = \begin{bmatrix} 7 & 5 & 6 & 1 & 0 & 0 & 0 \\ 0 & 7 & 5 & 6 & 1 & 0 & 0 \\ 0 & 0 & 7 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 7 & 5 & 6 & 1 \end{bmatrix}.$$

A matriz verificação de paridade correspondente é dada por:

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

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

Códigos BCH sobre $\mathbb{Z}_{16}$

Apresentamos agora a construção de um código BCH sobre o anel $\mathbb{Z}_{16}$ através da extensão de Galois de grau 2. O procedimento adotado é análogo ao desenvolvido nos exemplos da construção de códigos BCH sobre os anéis $\mathbb{Z}_4$ e $\mathbb{Z}_8$.

Seja o anel R gerado pela seguinte extensão de grau 2:

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

Seja $f = (0\ 1) \in GR^*(16,2)$. Então, $\overline{f} = (0\ 1) = f$ gera um subgrupo cíclico

de ordem $n = 3$ em F_4, corpo apresentado na expressão (4.2) e que possui os elementos contidos na Tabela 4.2, sendo α um elemento primitivo deste corpo. Assim, pelo Teorema 4.3.4, temos que f deve gerar um grupo de ordem $nd = 3d$ em $GR^*(16, 2)$.

Em $GR^*(16, 2)$, temos $x^2 = 15x + 15$. Assim, para $f = (0\ 1) = x$, a representação dos elementos de $GR^*(16, 2)$ é mostrada na Tabela 4.9.

$0 \rightarrow \begin{pmatrix} 0 & 0 \end{pmatrix}$
$1 \rightarrow \begin{pmatrix} 1 & 0 \end{pmatrix}$
$f \rightarrow \begin{pmatrix} 0 & 1 \end{pmatrix}$
$f^2 \rightarrow \begin{pmatrix} 15 & 15 \end{pmatrix}$
$f^3 \rightarrow \begin{pmatrix} 1 & 0 \end{pmatrix}$

Tabela 4.9: Elementos de $GR^*(16, 2)$

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

Para a distância mínima de projeto do código BCH sobre $\mathbb{Z}_{16}$ igual a 3, o polinômio gerador $g(x)$ tem como raízes β e β^2. Assim, temos:

$$M_1(x) = M_2(x) = (x - \beta)\left(x - \beta^2\right) = 1 + x + x^2.$$

Assim, $g(x) = mmc(M_1(x), M_2(x)) = 1 + x + x^2$ gera o código BCH desejado. Este polinômio gerador corresponde à seguinte matriz geradora:

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

A matriz verificação de paridade correspondente, geradora do código dual associado, é dada por:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 15 & 15 \\ 1 & 0 & 15 & 15 & 0 & 1 \end{bmatrix}.$$

Códigos BCH sobre $\mathbb{Z}_{32}$

Segue a construção de um código BCH sobre o anel $\mathbb{Z}_{32}$ através da extensão de Galois de grau 2. O procedimento adotado é análogo ao desenvolvido nos exemplos da construção de códigos BCH sobre os anéis $\mathbb{Z}_4$, $\mathbb{Z}_8$ e $\mathbb{Z}_{16}$.

Seja o anel R gerado pela seguinte extensão de grau 2:

$$R \cong GR(32,2)[x] \cong \frac{\mathbb{Z}_{32}[x]}{\langle x^2+x+1\rangle} = \{a+bx;\ a,b \in \mathbb{Z}_{32}\}.$$

Considere ainda o corpo F_4, dado pela expressão (4.2), e que apresenta os elementos contidos na Tabela 4.2, sendo α um elemento primitivo deste corpo.

Seja $f = (0\ 1) \in GR^*(32,2)$. Então, $\overline{f} = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = 3$ em F_4. Assim, pelo Teorema 4.3.4, temos que f deve gerar um grupo de ordem $nd = 3d$ em $GR^*(32,2)$.

Em $GR^*(32,2)$, temos $x^2 = 31x + 31$. Assim, para $f = (0\ 1) = x$, a representação dos elementos de $GR^*(32,2)$ é mostrada na Tabela 4.10.

$0 \rightarrow$	$\begin{pmatrix} 0 & 0 \end{pmatrix}$
$1 \rightarrow$	$\begin{pmatrix} 1 & 0 \end{pmatrix}$
$f \rightarrow$	$\begin{pmatrix} 0 & 1 \end{pmatrix}$
$f^2 \rightarrow$	$\begin{pmatrix} 31 & 31 \end{pmatrix}$
$f^3 \rightarrow$	$\begin{pmatrix} 1 & 0 \end{pmatrix}$

Tabela 4.10: Elementos de $GR^*(32,2)$

Portanto, $nd = 3$ e, assim, $d = 1$. Logo, $f = x = (0\ 1)$ gera um grupo de ordem 1 em $GR^*(32,2)$ e também um grupo de ordem 3 neste mesmo grupo multiplicativo. Logo, $\beta = x$ é um elemento primitivo em G_3.

Para a distância mínima de projeto do código BCH sobre $\mathbb{Z}_{32}$ igual a 3, o polinômio gerador $g(x)$ tem como raízes β e β^2. Assim, temos:

$$M_1(x) = M_2(x) = (x-\beta)\left(x-\beta^2\right) = 1+x+x^2.$$

Assim, $g(x) = mmc(M_1(x), M_2(x)) = 1 + x + x^2$ gera o código BCH desejado. Este polinômio gerador está relacionado à seguinte matriz geradora:

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

A matriz verificação de paridade correspondente, geradora do código dual associado, é dada por:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 31 & 31 \\ 1 & 0 & 31 & 31 & 0 & 1 \end{bmatrix}.$$

Códigos BCH sobre $\mathbb{Z}_{64}$

Desenvolvemos agora a construção de códigos BCH sobre o anel $\mathbb{Z}_{64}$ através da extensão de Galois de grau 2. O procedimento adotado é análogo ao desenvolvido nos exemplos da construção de códigos BCH sobre os anéis $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ e $\mathbb{Z}_{32}$.

Seja o anel R gerado pela extensão de grau 2 abaixo:

$$R \cong GR(64,2)[x] \cong \frac{\mathbb{Z}_{64}[x]}{\langle x^2 + x + 1 \rangle} = \{a + bx;\ a, b \in \mathbb{Z}_{64}\}.$$

O corpo F_4, desenvolvido na expressão (4.2), apresenta os elementos dados na Tabela 4.2, sendo α um elemento primitivo deste corpo.

Seja $f = (0\ 1) \in GR^*(64,2)$. Então, $\overline{f} = (0\ 1) = f$ gera um subgrupo cíclico de ordem $n = 3$ em F_4. Assim, pelo Teorema 4.3.4, temos que f deve gerar um grupo de ordem $nd = 3d$ em $GR^*(64,2)$.

Em $GR^*(64,2)$, temos $x^2 = 63x + 63$. Assim, para $f = (0\ 1) = x$, a representação dos elementos de $GR^*(64,2)$ é como mostrada na Tabela 4.11.

Portanto, $nd = 3$ e, assim, $d = 1$. Logo, $f = x = (0\ 1)$ gera um grupo de ordem 1 em $GR^*(64,2)$ e também um grupo de ordem 3 em $GR^*(64,2)$. Logo, $\beta = x$ é um elemento primitivo em G_3.

$0 \rightarrow \begin{pmatrix} 0 & 0 \end{pmatrix}$
$1 \rightarrow \begin{pmatrix} 1 & 0 \end{pmatrix}$
$f \rightarrow \begin{pmatrix} 0 & 1 \end{pmatrix}$
$f^2 \rightarrow \begin{pmatrix} 63 & 63 \end{pmatrix}$
$f^3 \rightarrow \begin{pmatrix} 1 & 0 \end{pmatrix}$

Tabela 4.11: Elementos de $GR^*(64, 2)$

Para a distância mínima de projeto do código BCH sobre $\mathbb{Z}_{64}$ igual a 3, o polinômio gerador $g(x)$ tem como raízes β e β^2. Assim, temos:

$$M_1(x) = M_2(x) = (x - \beta)\left(x - \beta^2\right) = 1 + x + x^2.$$

Assim, $g(x) = mmc(M_1(x), M_2(x)) = 1 + x + x^2$ gera o código BCH desejado. Este polinômio gerador corresponde à seguinte matriz geradora:

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

A matriz verificação de paridade correspondente, geradora do código dual associado, é dada por:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 63 & 63 \\ 1 & 0 & 63 & 63 & 0 & 1 \end{bmatrix}.$$

Observação 4.4.2 *Poderíamos ter escolhido outros polinômios irredutíveis sobre o corpo F_2 para as extensões de grau maior ou igual a 3, porém é fácil perceber que isto não resultaria em novos resultados.*

4.4.2 Códigos Alternantes

Nesta subseção, analisamos os códigos alternantes, que formam uma classe de códigos que podem ser obtidos através dos códigos BCH. Os conceitos aqui apresentados podem

ser encontrados em [21].

Podemos definir a matriz verificação de paridade de um código alternante através do chamado vetor localizador da seguinte forma:

Definição 4.4.3 *Um código alternante $\mathcal{C}(\eta, w, n)$ de comprimento n sobre um anel R tem sua matriz verificação de paridade definida como:*

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

para algum $r \geq 1$ (indicador da capacidade de correção de erros do código), onde $\eta = (\alpha_1\ \alpha_2 \cdots\ \alpha_n)$ é o ***vetor localizador****, consistindo de elementos distintos do grupo G_n, e $w = (w_1\ w_2 \cdots\ w_n)$ é um vetor que consiste de quaisquer elementos de G_n.*

Esta matriz pode ser decomposta como o produto de outras duas matrizes como feito a seguir:

$$\mathrm{H} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \cdot \begin{bmatrix} w_1 & 0 & \cdots & 0 \\ 0 & w_2 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & w_n \end{bmatrix}$$

Observe que se considerarmos o vetor $w = (\alpha_1\ \alpha_2\ \cdots\ \alpha_n)$, com $\alpha_i \in G_n$, $1 \leq i \leq n$,

tomando $\alpha_i = \beta^{i-1}$, $1 \leq i \leq n$, temos:

$$\mathrm{H} = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \left(\beta^2\right)^2 & \cdots & \left(\beta^2\right)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{r-1} & \left(\beta^{r-1}\right)^2 & \cdots & \left(\beta^{r-1}\right)^{n-1} \end{bmatrix}. \tag{4.6}$$

Considere agora o seguinte teorema:

Teorema 4.4.3 *O código alternante $\mathcal{C}(\eta, w, n)$ tem distância de Hamming mínima dada por:*

$$d \geq r + 1.$$

Portanto, é fácil perceber que r no Teorema 4.4.3 é equivalente a $2t$ utilizado no Teorema 4.4.2. Fazendo esta substituição na matriz (4.6), obtemos a matriz verificação de paridade de um código BCH como definida em (4.1). Ou seja, através de uma escolha apropriada do vetor localizador e do vetor w, a Definição 4.4.3 nos fornece a matriz verificação de paridade de um código BCH ou de um código alternante.

Descrevemos a seguir as matrizes verificação de paridade dos códigos alternantes utilizados na construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares na Seção 4.5.

Códigos alternantes sobre $\mathbb{Z}_4$

Seja um código alternante de comprimento 3. Para distância de projeto igual a 3, temos que $r = 2$. Sendo assim, considere β elemento primitivo em G_3. Logo, $\eta = \left(1\ \beta\ \beta^2\right)$, onde $1 = \beta^3$ e, da Tabela 4.2, $\beta = x = f = (0\ 1)$. Fazendo $w = (1\ 1\ 1)$, temos a seguinte matriz de verificação de paridade:

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

Analogamente, podemos construir um código alternante de comprimento 7 e distância

3 considerando os vetores $\eta = \left(1\ \beta\ \beta^2\ \beta^3\ \beta^4\ \beta^5\ \beta^6\right)$ e w=(1 1 1 1 1 1 1), onde $1 = \beta^7$ e $\beta = x^2 = f^2 = (0\ 1\ 0) \in G_7$, pela Tabela 4.4, $\beta = x^2 = f^2 = (0\ 1\ 0)$. Logo, temos a seguinte matriz verificação de paridade:

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

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

$$\mathrm{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 3 & 1 & 2 & 1 & 2 & 1 & 0 & 3 & 2 & 2 & 1 & 3 & 1 \end{bmatrix}.$$

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

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

Logo,

$$\mathrm{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 3 & 1 & 2 & 1 & 2 & 1 & 0 & 3 & 2 & 2 & 1 & 3 & 1 \\ 1 & 0 & 0 & 0 & 3 & 3 & 2 & 1 & 0 & 1 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 1 & 3 & 2 & 2 \end{bmatrix}.$$

O código alternante de comprimento 7 e distância 5 ($r = 4$) apresenta matriz verifi-

cação de paridade mostrada abaixo:

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

Portanto,

$$\mathrm{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 3 & 1 & 2 & 1 & 2 & 1 & 0 & 3 & 2 & 2 & 1 & 3 & 1 \\ 1 & 0 & 0 & 0 & 3 & 3 & 2 & 1 & 0 & 1 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 1 & 3 & 2 & 2 \\ 1 & 0 & 0 & 1 & 2 & 1 & 1 & 3 & 1 & 0 & 3 & 3 & 3 & 2 & 2 & 0 & 0 & 1 & 2 & 1 & 0 \end{bmatrix}.$$

Finalmente, para um código alternante de comprimento 7 e distância 6, temos a seguinte matriz H:

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

Logo,

$$\mathrm{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 3 & 1 & 2 & 1 & 2 & 1 & 0 & 3 & 2 & 2 & 1 & 3 & 1 \\ 1 & 0 & 0 & 0 & 3 & 3 & 2 & 1 & 0 & 1 & 3 & 1 & 0 & 0 & 1 & 1 & 2 & 1 & 3 & 2 & 2 \\ 1 & 0 & 0 & 1 & 2 & 1 & 1 & 3 & 1 & 0 & 3 & 3 & 3 & 2 & 2 & 0 & 0 & 1 & 2 & 1 & 0 \\ 1 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 & 3 & 2 & 2 & 0 & 3 & 3 & 1 & 3 & 1 & 1 & 2 & 1 \end{bmatrix}.$$

Códigos alternantes sobre $\mathbb{Z}_8$

Seja um código alternante de comprimento 3 e distância de projeto igual a 3 ($r = 2$). Sendo assim, considere β elemento primitivo em G_3. Logo, $\eta = \left(1\ \beta\ \beta^2\right)$, onde $1 = \beta^3$ e, da Tabela 4.7, $\beta = x = f = (0\ 1)$. Fazendo $w = (1\ 1\ 1)$, temos a seguinte matriz de verificação de paridade:

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

Da mesma forma, podemos construir um código alternante de comprimento 7 e distância 3 considerando os vetores $\eta = \left(1\ \beta\ \beta^2\ \beta^3\ \beta^4\ \beta^5\ \beta^6\right)$ e w=(1 1 1 1 1 1 1), onde $1 = \beta^7$ e, pela Tabela 4.8, $\beta = x^4 = f^4 = (0\ 7\ 7)$. Logo, temos a seguinte matriz verificação de paridade:

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

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

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

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

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

Portanto,

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

Por fim, o código alternante de comprimento 7 e distância 5 ($r = 4$) apresenta a seguinte matriz H:

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

Logo,

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

4.5 Códigos $\mathbb{Z}_{2^k}$-pseudolineares

Em sua tese de doutorado, [16], J. R. Gerônimo mostra que, para $k \geq 3$, não conseguimos obter uma aplicação bijetiva m_k isométrica entre os espaços de Lee e Hamming, onde:

$$m_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k.$$

Ou seja, não existem códigos $\mathbb{Z}_{2^k}$-lineares. Por outro lado, para $k = 2$, temos os já conhecidos códigos $\mathbb{Z}_4$-lineares, [19]. No Capítulo 3 mostramos que é possível, através de aplicações injetivas, manter a isometria entre os espaços de Lee $(\mathbb{Z}_{2^k}, d_L)$ e de Hamming

$(\mathbb{Z}_2^{2^{k-1}}, d_H)$. Isto é, as aplicações

$$m_k : \mathbb{Z}_{2^k} \longrightarrow \mathbb{Z}_2^{2^{k-1}}, \quad k \geq 3,$$

nos fornecem os chamados códigos $\mathbb{Z}_{2^k}$-pseudolineares, definidos em [26].

Uma vez estabelecidas as aplicações casadas isométricas entre o espaço de Lee $(\mathbb{Z}_{2^k}, d_L)$ e o espaço de Hamming $(\mathbb{Z}_2^{2^{k-1}}, d_H)$ no Capítulo 3, e fazendo uso do conceito de extensão de Galois de dimensão r sobre $\mathbb{Z}_{2^k}$, apresentamos a seguir os códigos $\mathbb{Z}_{2^k}$-pseudolineares gerados através dos códigos BCH sobre $\mathbb{Z}_{2^k}$.

O procedimento adotado na geração desses códigos $\mathbb{Z}_{2^k}$-pseudolineares é bastante simples: partimos do código em $\mathbb{Z}_{2^k}$, cuja matriz geradora foi obtida na Subseção 4.4.1, e então substituímos os símbolos em $\mathbb{Z}_{2^k}$ de cada palavra-código pelos correspondentes símbolos em $\mathbb{Z}_2^{2^{k-1}}$. A correspondência entre estes símbolos nada mais é do que a aplicação casada isométrica obtida no Capítulo 3.

Assim, considere o código $\mathbb{Z}_{2^k}$-pseudolinear proveniente do anel $GR(4,2)$. Sejam os vetores $\underline{u}$ e $\underline{v}$ tais que $\underline{v} = \underline{u}$G, ou seja, $\underline{v}$ é uma palavra-código e $\underline{u}$ contém os símbolos de entrada no codificador. A partir da matriz geradora obtida em (4.3), temos as seguintes palavras-código em $\mathbb{Z}_4$:

$\underline{u}$	$\underline{v}$
0	(0 0 0)
1	(1 1 1)
2	(2 2 2)
3	(3 3 3)

Tabela 4.12: Palavras-código em $\mathbb{Z}_4$

Portanto, em $\mathbb{Z}_4$ temos um código $(n, k, d_L) = (3, 1, 3)$, cujo espectro de pesos é dado pela Tabela 4.13.

Substituindo os símbolos em $\mathbb{Z}_4$ das palavras-código na Tabela 4.12 pelos símbolos em $\mathbb{Z}_2^2$ dados pela aplicação isométrica mostrada na Tabela 3.2, temos as palavras-código em $\mathbb{Z}_2^2$, como mostradas na Tabela 4.14:

Peso de Lee	0	3	6
N°de palavras	1	2	1

Tabela 4.13: Espectro de pesos em $\mathbb{Z}_4$

$\underline{u}$	$\underline{v}$
0	(0 0 0 0 0 0)
1	(0 1 0 1 0 1)
2	(1 1 1 1 1 1)
3	(1 0 1 0 1 0)

Tabela 4.14: Palavras-código em $\mathbb{Z}_2^2$

Logo, temos um código $(n, k, d_L) = (6, 2, 3)$. Seu espectro de pesos é dado pela Tabela 4.15.

Peso de Hamming	0	3	6
N°de palavras	1	2	1

Tabela 4.15: Espectro de pesos em $\mathbb{Z}_2^2$

Note que o espectro de pesos de Lee e de Hamming é o mesmo, assim como a taxa de transmissão do código e sua distância mínima. Estas características já eram esperadas, uma vez que este código também pertence à classe dos códigos $\mathbb{Z}_4$-lineares, [16].

O procedimento descrito acima foi aplicado para os demais códigos BCH considerados na Seção 4.4. Os resultados obtidos foram organizados na Tabela 4.16, onde:

- n é o comprimento do código sobre $\mathbb{Z}_{2^k}$;
- k é a dimensão do código sobre $\mathbb{Z}_{2^k}$;
- d_L é a distância de Lee mínima do código;
- n' é o comprimento do código sobre $\mathbb{Z}_2^{2^{k-1}}$ (código binário);
- k' é a dimensão do código sobre $\mathbb{Z}_2^{2^{k-1}}$ (código binário);
- d_H é a distância de Hamming mínima do código;

- d_{BV} é a melhor distância alcançada pelos códigos binários lineares com parâmetros (n', k') segundo a tabela de Brouwer e Verhoeff, [9].
- $g(x)$ é o polinômio gerador do código cíclico BCH correspondente.
- a notação $(0, 3^2, 6)$ utilizada na tabela significa $(0, 3, 3, 6)$, ou seja, o código em questão apresenta uma palavra de peso zero, duas palavras de peso três e uma palavra de peso seis.

Em seguida temos o espectro de pesos do código $\mathbb{Z}_{2^k}$-pseudolinear (note que este espectro é o mesmo tanto para o código sobre $\mathbb{Z}_{2^k}$, quanto para o código sobre $\mathbb{Z}_2^{2^{k-1}}$, pois a aplicação utilizada é isométrica) e, na última coluna, dizemos se o código em questão é linear ou não. Na primeira coluna da tabela, apresentamos as extensões de Galois utilizadas na construção dos códigos.

Observe que, através do método empregado, foi possível obter códigos $\mathbb{Z}_{2^k}$-pseudolineares cujas distâncias de Hamming mínimas são iguais às dos códigos lineares binários tabelados em [9] e, portanto, apresentam a mesma capacidade de correção de erros. Além disso, as distâncias mínimas são preservadas entre os espaços métricos de Lee e de Hamming.

Os códigos quaternários provenientes de $GR(4, 2)$, $GR(4, 3)$ e $GR(4, 4)$ apresentam a mesma distância de Lee que os códigos obtidos através de um algoritmo de otimização combinatorial proposto por Said e Palazzo em [27] e utilizado em [17] e [16].

As Tabelas 4.17 e 4.18 a seguir apresentam os códigos $\mathbb{Z}_{2^k}$-pseudolineares obtidos através dos códigos BCH duais (Subseção 4.4.1) e dos códigos alternantes (Subseção 4.4.2). A notação utilizada é a mesma da Tabela 4.16, onde H é a matriz verificação de paridade do código.

Todos os códigos das Tabelas 4.17 e 4.18 são não lineares, contudo podemos observar que eles não são bons códigos no sentido de que suas distâncias mínimas são consideravelmente inferiores às distâncias dos códigos lineares binários obtidos por Brouwer e Verhoeff, [9], e, consequentemente, apresentam menor capacidade de correção de erros. Is-

to ocorre principalmente quando a relação k/n, ou seja, a taxa de transmissão do código é baixa. Podemos dizer que esta é uma característica dos códigos $\mathbb{Z}_{2^k}$-pseudolineares construídos através das aplicações casadas isométricas apresentadas no Capítulo 3, ou seja, o comprimento do código cresce exponencialmente, enquanto sua dimensão cresce linearmente, implicando em baixas taxas de transmissão. No caso dos códigos $\mathbb{Z}_{2^k}$-pseudolineares, estas baixas taxas de transmissão vêm acompanhadas de distâncias mínimas também pequenas.

4.6 Conclusão

Neste capítulo foi apresentada uma proposta para construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através de códigos cíclicos provenientes de extensões de Galois de dimensão r sobre anéis de inteiros módulo $q = 2^k$, utilizando as aplicações isométricas desenvolvidas no Capítulo 3. Foi feita uma breve introdução aos conceitos de códigos cíclicos, extensão de Galois e códigos BCH sobre anéis comutativos finitos locais. Posteriormente, apresentamos os códigos $\mathbb{Z}_{2^k}$-pseudolineares obtidos e verificamos que, embora seja possível conseguir códigos cujas distâncias mínimas são equivalentes àquelas dos melhores códigos lineares binários conhecidos, para baixas taxas de transmissão não é possível conseguir bons códigos corretores de erros.

Extensão de Galois	$g(x)$	(n,k,d_L)	(n,k,d_H)	d_{BV}	Espectro de pesos	Código
$GR(4,2)$	$1+x+x^2$	$(3,1,3)$	$(6,2,3)$	4	$(0,3^2,6)$	linear
$GR(4,3)$	$3+x+2x^2+x^3$	$(7,4,4)$	$(14,8,4)$	4	$(0,4^{14},5^{56},6^{49},7^{16},$ $8^{49},9^{56},10^{14},14)$	não linear
$GR(4,4)$	$1+x+3x^2$ $+3x^4+3x^5+2x^7$ $+x^8+2x^9+x^{10}$	$(15,5,10)$	$(30,10,10)$	11	$(0,10^{30},11^{120},12^{90},$ $14^{135},15^{272},16^{135},$ $18^{90},19^{120},20^{30},30)$	não linear
$GR(8,2)$	$1+x+x^2$	$(3,1,6)$	$(12,3,6)$	6	$(0,6^6,12)$	linear
$GR(8,3)$	$7+5x+6x^2+x^3$	$(7,4,8)$	$(28,12,8)$	8	$(0,8^{154},10^{224},$ $12^{1253},14^{832},16^{1253},$ $18^{224},20^{154},28)$	não linear
$GR(8,4)$	$1+5x+7x^2+4x^3$ $+7x^4+3x^5+6x^7$ $+x^8+6x^9+x^{10}$	$(15,5,14)$	$(60,15,14)$	$21-23$	$(0,14^6,16^4,18^2,20^4,$ $22^{14},24^{14},26^{26},28^{31},30^{92},$ $32^{157},34^{486},36^{660},38^{980},$ $40^{686},42^{566},44^{196},46^{118},$ $48^{34},50^8,52^4,54^6,60^1)$	não linear
$GR(16,2)$	$1+x+x^2$	$(3,1,6)$	$(24,4,6)$	12	$(0,6^2,12^{10},18^2,24)$	linear
$GR(32,2)$	$1+x+x^2$	$(3,1,12)$	$(48,5,12)$	24	$(0,12^8,24^{14},36^8,48)$	linear
$GR(64,2)$	$1+x+x^2$	$(3,1,6)$	$(96,6,6)$	48	$(0,6^2,12^2,18^2,24^2,$ $30^2,36^2,42^2,48^{34},$ $54^2,60^2,66^2,72^2,$ $78^2,84^2,90^2,96)$	linear

Tabela 4.16: Códigos $\mathbb{Z}_{2^k}$-pseudolineares a partir de códigos BCH

Extensão de Galois	H	(n,k,d_L)	(n,k,d_H)	d_{BV}	Espectro de pesos
$GR(4,2)$	100133 $\quad$ 103301	$(6,2,4)$	$(12,4,4)$	6	$(0,4^7,6^6,8^2)$
$GR(4,3)$	100001033121210322131 $\quad$ 100033210131001121322	$(21,2,16)$	$(42,4,16)$	22	$(0,16,18^2,19^8,20^2,22^2)$
$GR(8,2)$	100177 $\quad$ 107701	$(6,2,6)$	$(24,6,6)$	10	$(0,6^4,8^{19},10^{16},12^{18},14^4,16^2)$
$GR(8,3)$	100077650575441521372 $\quad$ 100650441372077575521	$(21,2,32)$	$(84,6,32)$	41	$(0,32,34^8,36^{16},38^{16},40^4,42^8,44^8,48^2)$

Tabela 4.17: Códigos $\mathbb{Z}_{2^k}$-pseudolineares a partir de códigos BCH duais

Alfabeto	H	(n,k,d_L)	(n,k,d_H)	d_{BV}	Espectro de pesos
$\mathbb{Z}_4$	101010 100133	$(6,2,3)$	$(12,4,3)$	6	$(0,3^2,4^2,5^4,$ $6^4,7^2,8)$
$\mathbb{Z}_4$	100100100100100100 100001033121210322131	$(21,2,7)$	$(42,4,7)$	22	$(0,7^2,14,18^2,$ $19^2,20,21^4,22^3)$
$\mathbb{Z}_4$	100100100100100100 100001033121210322131 100033210131001121322	$(21,3,7)$	$(42,6,7)$	20	$(0,7^2,14,16^3,$ $17^4,18^{12},19^{12},20^4,$ $21^{12},22^{10},23^2,30)$
$\mathbb{Z}_4$	100100100100100100 100001033121210322131 100033210131001121322 100121131033322001210	$(21,4,7)$	$(42,8,7)$	18	$(0,7^2,10^2,11^4,12^2,14^9,$ $15^{16},16^{21},17^{18},18^{22},$ $19^{42},20^{30},21^{28},22^{30},$ $23^{10},24^{10},25^2,27^6,30)$
$\mathbb{Z}_4$	100100100100100100 100001033121210322131 100033210131001121322 100121131033322001210 100210001322033131121	$(21,5,7)$	$(42,10,7)$	16	$(0,7^4,8^2,9^4,10^4,11^6,12^{15},$ $13^{18},14^{37},15^{42},16^{67},$ $17^{98},18^{122},19^{150},20^{123},$ $21^{118},23^{42},24^{45},25^{18},$ $26^2,27^{12},28^2,30^3,32)$
$\mathbb{Z}_8$	101010 100177	$(6,2,6)$	$(24,6,6)$	10	$(0,6^6,8^{14},10^{20},$ $12^{16},14^6,16)$
$\mathbb{Z}_8$	100100100100100100 100077650575441521372	$(21,2,14)$	$(83,6,14)$	40	$(0,14^6,28,34^2,36^{14},38^{16},$ $40^{14},42^2,44,46^6,48)$
$\mathbb{Z}_8$	100100100100100100 100077650575441521372 100650441372077575521	$(21,3,14)$	$(84,9,14)$	$38-39$	$(0,14^6,28,32^9,34^{40},$ $36^{116},38^{152},40^{116},$ $42^{40},44^{10},46^{18},48^2,60)$
$\mathbb{Z}_8$	100100100100100100 100077650575441521372 100650441372077575521 100575372650521077441	$(21,4,14)$	$(84,12,14)$	$34-37$	$(0,14^6,16^4,18^2,20^4,22^{14},$ $24^{14},26^{26},28^{31},30^{92},$ $32^{157},34^{486},36^{660},38^{980},$ $40^{686},42^{566},44^{196},46^{118},$ $48^{34},50^8,52^4,54^6,60)$

Tabela 4.18: Códigos $\mathbb{Z}_{2^k}$-pseudolineares a partir de códigos alternantes

Capítulo 5

Conclusões

Este trabalho teve como principal motivação a busca por novas classes de códigos não lineares cujas distâncias mínimas, e portanto a capacidade de correção de erros destes códigos, fossem superiores às distâncias dos melhores códigos lineares conhecidos até então, [9]. Estes códigos não lineares deveriam ser cíclicos e geometricamente uniformes, reproduzindo as principais propriedades encontradas na $\mathbb{Z}_4$-linearidade, e portanto, facilitando o processo de decodificação. Contudo, diante da impossibilidade de se obter códigos $\mathbb{Z}_{2^k}$-lineares para $k \geq 3$, consideramos aplicações injetoras, tais que o casamento e a isometria entre os espaços métricos de Lee e de Hamming fossem possíveis. Neste sentido, apresentamos os códigos $\mathbb{Z}_{2^k}$-pseudolineares para $2 \leq k \leq 6$.

5.1 Contribuições

As contribuições deste trabalho encontram-se nos Capítulos 3 e 4. No primeiro, mostramos ser possível, através do uso dos conceitos de particionamento de conjuntos e representação modular, determinar aplicações isométricas entre os espaços $(\mathbb{Z}_{2^k}, d_L)$ e $(\mathbb{Z}_2^{2^{k-1}}, d_H)$, cujas palavras apresentam somente pesos pares, mais do que isso, as palavras das aplicações apresentadas possuem pesos múltiplos de 4, sendo que para $k = 2$, reproduzimos a $\mathbb{Z}_4$-linearidade. Esta é uma contribuição importante, pois Carlet mostra

em [11] não ser possível, através de uma generalização do mapeamento Gray por funções Booleanas, determinar tais aplicações.

É importante notar que os resultados do Capítulo 3 não se limitam à construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares. Podemos aplicar as transformações encontradas na solução de problemas relacionados a armazenamento de dados em meios ópticos ou magnéticos, modulações digitais do tipo M-QAM e alocação de frequência em telefonia móvel, discutidos em [3], [8], [10], [1], [4] e [2].

No Capítulo 4, construímos os códigos $\mathbb{Z}_{2^k}$-pseudolineares para $2 \leq k \leq 6$ através de extensões de Galois de dimensão r sobre anéis locais. Para tanto, consideramos os códigos cíclicos BCH, pois estes são muito utilizados em situações práticas devido à facilidade de codificação e decodificação. Contudo, comprovamos o fato já conhecido de que os códigos BCH não apresentam bom desempenho quando o comprimento de suas palavras-código é grande. Além disso, podemos dizer que, os códigos cíclicos são assintoticamente ruins, pois a relação entre a distância de Lee mínima e o comprimento dos códigos cíclicos tende a zero, $(\frac{d_L}{n} \to 0)$, fazendo com que o código binário não linear equivalente apresente uma capacidade corretora de erros significativamente inferior a dos melhores códigos binários correspondentes. Portanto, concluímos que a proposta de construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares apresentada é adequada para $k = 2$ e $k = 3$, ou seja, para os casos $\mathbb{Z}_4$ e $\mathbb{Z}_8$ conseguimos códigos não lineares tão bons quanto os melhores códigos lineares conhecidos. Porém, para $k \geq 4$, mostramos que a proposta não é adequada. Assim, outra contribuição deste trabalho é mostrar não ser possível, através do uso de códigos cíclicos no procedimento adotado, encontrar bons códigos binários não lineares para $k \geq 4$.

5.2 Propostas para Trabalhos Futuros

Como sugestão para futuras pesquisas, propomos os seguintes tópicos:

- Considerando o fato de que a proposta adotada não se mostrou adequada para construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares para $k \geq 4$, é interessante estudar a

possibilidade de se encontrar bons códigos nesta classe a partir de códigos lineares (não cíclicos);

- Com relação ao problema de recobrimento de regiões, propomos a extensão do método utilizado para três dimensões, ou seja, considerar o reticulado tridimensional $\mathbb{Z}_{2^k}^3$. Para tanto, se faz necessário resolver o problema de representação de um inteiro na forma quadrática em três dimensões. Os códigos então obtidos poderiam ser aplicados na correção de erros que ocorrem em surtos no armazenamento holográfico, por exemplo;

- Estudar o processo de transmissão dos códigos $\mathbb{Z}_{2^k}$-pseudolineares construídos.

Bibliografia

[1] C. de Almeida, *Modulação Codificada Generalizada via Equação de Diofanto*, Tese de Doutorado, FEEC-UNICAMP, 1990.

[2] C. de Almeida, e R. Palazzo, Jr., "Binary quadratic forms: a solution to the set partitioning problem over $GF(q)$", *IEEE Intl. Symposium on Information Theory*, San Diego, USA, 1990.

[3] C. de Almeida, and R. Palazzo, Jr., "Efficient two-dimensional interleaving technique by use of the set partitioning concept", *IEEE Electronics Letters*, vol. 32, March 1996.

[4] C. de Almeida, e R. Palazzo, Jr., "On the frequency allocation for mobile radio telephone systems", *IEEE Intl. Symposium on Personal, Indoor and Mobile Radio Communications*, Toronto, Canada, pp. 96-99, 1995.

[5] M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, 1988.

[6] P. R. Barbosa, e R. Palazzo, Jr., "Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares através de Mapeamentos Isométricos e Extensões de Galois sobre Anéis Locais", *XVIII Simpósio Brasileiro de Telecomunicações*, Setembro 2000.

[7] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Company, 1968.

[8] M. Blaum, J. Bruck, and A. Vardy, "Interleaving Schemes for Multidimensional Cluster Errors", *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 730-743, March 1998.

[9] A. E. Brower, and T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory,* vol.IT-39, pp. 662-677, March 1993.

[10] R. M. Campello de Souza, A. N. Kauffman, M. A. C. Moraes, e R. C. C. Lima, "Transformações Lineares para Correção de Surtos Bidimensionais", *Revista da Sociedade Brasileira de Telecomunicações*, vol. 13, Junho 1998.

[11] C. Carlet, "$\mathbb{Z}_{2^k}$-Linear Codes", *IEEE Trans. Inform. Theory*, vol. IT-44, pp.1543-1547, July 1998.

[12] T. M. Cover, and J. A. Thomas, *Elements of Information Theory*, Wiley, 1991.

[13] G.D. Forney, "Geometrically uniform codes," *IEEE Trans. Inform. Theory,* vol. IT-37, pp. 1241-1260, Sept. 1991.

[14] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley Publishing Co., 1989.

[15] R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, 1968.

[16] J. R. Gerônimo, *Extensões da $\mathbb{Z}_4$-linearidade via Grupos de Simetrias*, Tese de Doutorado, FEEC-UNICAMP, 1997.

[17] J. R. Gerônimo, R. Palazzo, Jr., e J. C. Interlando, "New quaternary codes obtained from a combinatorial optimization algorithm", *Acta Scientiarum*, 21(4):881-889, 1999.

[18] J. R. Gerônimo, R. Palazzo, Jr., S. I. R. Costa, J. C. Interlando, e P. Brumatti, "Sobre a não existência de códigos $\mathbb{Z}_{2^k}$-lineares binários, onde $k \geq 3$", *XV Simpósio Brasileiro de Telecomunicações*, 1997, Recife.

[19] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes", *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 301-319, March 1994.

[20] J. C. Interlando, *Uma Contribuição aos Códigos Lineares sobre Anéis Locais*, Tese de Doutorado, FEEC-UNICAMP, 1994.

[21] J. C. Interlando, R. Palazzo, Jr., J. R. Gerônimo, A. A. Andrade, O. M. Favareto, e T. P. da Nóbrega Neto, *Códigos Corretores de Erros sobre Estruturas de Corpos, Anéis e Grupos*, DT-FEEC-UNICAMP, 1998.

[22] S. Lin, and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, Inc., 1983.

[23] H. A. Loeliger, "Signal sets matched to groups", *IEEE Trans. Inf. Theory*, vol. IT-37, pp.1675-1682, Nov. 1991.

[24] F. J. MacWilliams, and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[25] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[26] R. Palazzo, Jr., J. R. Gerônimo, e J. A. F. Afonso, "Proposta de construção de códigos $\mathbb{Z}_8$ e $\mathbb{Z}_9$ pseudolineares", *XV Simpósio Brasileiro de Telecomunicações*, 1997, Recife, pp. 493-497.

[27] A. Said, and R. Palazzo, Jr., "Using combinatorial optimization to design good unit-memory convolutional codes", *IEEE Trans. Inform. Theory*, vol.IT-39, pp. 1100-1108, 1993.

[28] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 480-483, July 1979.

[29] G. Ungerboeck, "Channel coding with multilevel/phase signals", *IEEE Trans. Inf. Theory*, vol. IT-28, pp. 55-67, Jan. 1982.