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

EXTENSÃO DA Z_4-LINEARIDADE VIA GRUPO DE SIMETRIAS

João Roberto Gerônimo

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

Co-Orientador: **Prof. Dr. José Carmelo Interlando**

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação, FEEC - UNICAMP, como requisito parcial para obtenção do título de DOUTOR EM ENGENHARIA ELÉTRICA.

Fevereiro - 1997

Campinas - SP

Este exemplar corresponde à redação final da tese defendida por João Roberto Gerônimo e aprovada pela Comissão Julgadora em 20 / 02 / 97.

Reginaldo Palazzo Júnior
Orientador

UNICAMP
BIBLIOTECA CENTRAL

UNIDADE BC
N.º CHAMADA: T/UNICAMP
G319e
V. Ex.
TOMBO BC/ 30104
PROC. 281/97
C D X
PREÇO R$ 11,00
DATA 13-05-97
N.º CPD

CM-00098860-8

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

G319e

Gerônimo, João Roberto
Extensão da Z_4-linearidade via grupo de simetrias / João Roberto Gerônimo.--Campinas, SP: [s.n.], 1997.

Orientador: Reginaldo Palazzo Jr., José Carmelo Interlando.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Códigos de controle de erros (Teoria da informação). 2. Teoria dos grupos. 3. Codificação, Teoria da. 4. Isometria (Matemática). I. Palazzo Jr., Reginaldo. II. Interlando, José Carmelo. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Agradecimentos

- À Universidade Estadual de Maringá e à Coordenação do Aperfeiçoamento do Pessoal de Nível Superior (CAPES) pelo suporte financeiro.

- Aos Profs. Drs. Reginaldo Palazzo Júnior e José Carmelo Interlando, pela eficiente, segura e indispensável orientação a mim dispensada para a realização do presente trabalho.

- Ao Prof. Dr. Paulo Brumatti do IMECC - UNICAMP, pela sua colaboração dada no Capítulo 3 deste trabalho.

- À Profa. Dra. Sueli I. R. Costa do IMECC - UNICAMP, pela sua colaboração dada no Capítulo 4 deste trabalho.

- Aos colegas do Departamento de Matemática da UEM, que me antecederam num trabalho idêntico, e aos que ficaram para tornar possível a realização desse trabalho. Em particular, aos Profs. Emerson Arnault de Toledo, João César Guirado, João Ribeiro Gonçalves Filho, Carlos José de Barros Braga, Paulo Areas Burlandy e Osvaldo Germano de Roccio.

- A todos os colegas do Curso. Em particular, Carlos Eduardo Câmara, Hélio Pires, Osvaldo Milaré, Antonio de Andrade e Silva.

- À Banca Examinadora, constituída pelos Profs. Drs. Max H. M. Costa do DECOM-FEEC-UNICAMP, Ivanil S. Bonatti do DT-FEE-UNICAMP e, aos Profs. Drs. Paulo Brumatti e Sueli I. R. Costa do IMECC - UNICAMP.

- A todas as pessoas que conviveram comigo neste período e que, de alguma forma, contribuíram para tornar possível este trabalho.

"Palavras, nossas ou dos outros, nunca podem ser mais do que um comentário sobre a experiência vivida. Ler nunca pode substituir o viver. O que entendo de uma árvore? Subi nos galhos e senti o tronco balançar ao vento, e me ocultei entre as folhas, como uma maçã. Deitei-me entre os galhos, e cavalguei neles, e rasguei a pele das mãos e o pano das minhas calças subindo e descendo pela áspera casca. Descasquei salgueiro e afaguei a madeira branca e doce, e meu machado mordeu as fibras puras, e a serra deixou descobertos os velhos anéis e o cerne da madeira. Através do microscópio copiei os traços das células, e sacudi as raízes como cabelos nas minhas mãos; e masquei a goma e enrolei a língua em torno da seiva, e senti as fibras da madeira entre os meus dentes. Deitei-me entre as folhas de outono, e minhas narinas beberam o fumo de seu sacrifício. Aplainei o tronco amarelo e bati pregos, e poli a madeira macia com a minha mão. Agora dentro de mim existem grãos e folhas, uma confluência de raízes e galhos, florestas próximas e distantes, e um solo macio feito de milhares de anos de plantas caídas, e este sussurro, esta lembrança de dedos e narinas, o frágil brotar das folhas reluzindo dentro dos meus olhos. Qual é a minha compreensão das árvores se não esta realidade que está além de pobres nomes? Assim os lábios, a língua, ouvidos e olhos e dedos juntam suas vozes e falam para dentro, para a compreensão. Se eu sou sábio, não tento conduzir o outro para os meus pensamentos; mas eu o levo para a floresta e solto-o entre as árvores, até que ele descubra as árvores dentro de si mesmo, e descubra-se dentro das árvores."

(Citação de Kenneth L. Patton no Livro: Não apresse o rio (ele corre sozinho) - Barry Stevens)

Dedicatórias

À minha esposa
Iara
À minha mãe
Maria
À minha sogra
Hilda
Ao grande amigo
Jorge Cândido Lopes
(in memorian).

Resumo

Neste trabalho, temos como objetivo obter uma técnica de construção de códigos a partir de códigos de grupo sobre um grupo $\mathbb{G}$.

Nesta direção, apresentamos um estudo de possíveis extensões da $\mathbb{Z}_4$-linearidade para $\mathbb{Z}_{2^k}$-linearidade, $k \geq 2$, tendo como condições básicas para a definição de tais extensões suas principais propriedades: bijeção e preservação de pesos. Mostramos a incompatibilidade destas duas propriedades quando se considera o peso de Lee em $\mathbb{Z}_{p^k}, k \neq 2, p \neq 2$. Mostramos também que não é possível a existência da $\mathbb{Z}_{2^k}$-linearidade no sentido de estabelecer uma função $\phi : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_2^k$, que seja um mapeamento casado entre os espaços $(\mathbb{Z}_{2^k}, d)$ e $(\mathbb{Z}_{2^k}^n, \mathbb{H})$, onde d é uma distância qualquer. Estudando as propriedades da $\mathbb{Z}_4$-linearidade, no sentido do mapeamento ser uma boa técnica de construção de códigos binários geometricamente uniformes, apresentamos o conceito de $\mathbb{G}$ -linearidade, onde $\mathbb{G}$ é um grupo qualquer.

Estabelecemos o grupo de simetrias do espaço métrico de Lee n-dimensional de ordem q, isto é, $\mathbb{Z}_q^n$ e concluímos com a não-existência da $\mathbb{G}$-linearidade, para $\mathbb{G}$ cíclico, associada a $\mathbb{Z}_q^n$ cujo grupo tenha ordem máxima q^n. Todavia, mostramos que para ordem menores do que q^n é possível determinar códigos $\mathbb{Z}_q^n$ -lineares.

Abstract

In this research, our aim is to propose a code construction technique from group codes over a group $\mathbb{G}$ whose alphabet belongs to a given metric space. In this direction, we present a study of possible extensions of $\mathbb{Z}_4$-linearity to the $\mathbb{Z}_{2^k}$-linearity,$k \geq 2$, with two basic conditions: bijection and preservation of weights. We show the incompatibility of these properties where we consider the Lee weight on $\mathbb{Z}_{p^k}$,$k \neq 2, p \neq 2$. We show also that it is impossible have $\mathbb{Z}_{2^k}$-linearity in the sense of estabilishing a function $\phi : \mathbb{Z}_{2^k} \longrightarrow \mathbb{Z}_2^k$, that is an isometry and preserves weights between the spaces $(\mathbb{Z}_{2^k}, d)$ and $(\mathbb{Z}_2^k, d_H)$, where d is any distance. Studying the properties of $\mathbb{Z}_4$-linearity, in searching for construction techniques of binary codes which are geometrically uniform, we extend this concept to any group $\mathbb{G}$.

We estabilish the symmetry group of the n-dimensional Lee space of order q and we conclude with the nonexistence of the $\mathbb{G}$-linearity, where $\mathbb{G}$ is cyclic, associated with $\mathbb{Z}_q^n$ whose corresponding group has maximum order q^n. However, we show that it is possible to find $\mathbb{Z}_q^n$-linear codes for order smaller than q^n.

Lista de Símbolos

$\| \bullet \|$: Norma euclidiana.

$\cap$: Intersecção entre dois conjuntos.

$\mathbb{N}$: Conjunto dos números naturais.

$\mathbb{R}$: Conjunto dos números reais.

$\mathbb{R}^n$: Espaço euclidiano n-dimensional.

$\mathbb{Z}$: Conjunto dos números inteiros.

$\mathbb{Z}_q$: Conjunto dos números inteiros módulo q.

$\mathbb{G}$: Grupo.

$\mathbb{H}$, $\mathbb{J}$: Subgrupos de um grupo.

$\times$: Produto direto de grupos.

$\times_\varphi$: Produto semi-direto de grupos.

φ: Homomorfismo que determina o produto semi-direto.

a^{-1}: Elemento inverso de a num grupo.

$e_{\mathbb{G}}$: Elemento neutro de um grupo $\mathbb{G}$.

$\mathbb{H} \trianglelefteq \mathbb{G}$: $\mathbb{H}$ é normal em $\mathbb{G}$.

$\mathbb{G}/\mathbb{H}$: Grupo quociente de um grupo $\mathbb{G}$ por um subgrupo normal $\mathbb{H}$.

$\langle \mathbb{H} \rangle$: Subgrupo gerado por $\mathbb{H}$.

$\mathbb{G} \cong \mathbb{H}$: $\mathbb{G}$ é isomorfo a $\mathbb{H}$.

$Aut(\mathbb{G})$: Grupo de automorfismos do grupo $\mathbb{G}$.

$\Theta_{\mathbb{A}}$: Grupo das permutações ou transformações de um conjunto $\mathbb{A}$.

$\mathcal{S}_n$: Grupo das permutações de um conjunto finito com n elementos. $(= \Theta_{\{1,2,\ldots,n\}})$.

$\mathcal{A}_n$: Grupo alternante de ordem $\frac{n!}{2}$.

$(\mathbb{S}, d_{\mathbb{S}})$: Subespaço métrico com a métrica induzida.

$U(\mathbb{S})$: Grupo gerador mínimo da figura geométrica $\mathbb{S}$.

$T(\mathbb{S})$: Grupo das translações de um conjunto $\mathbb{S}$.

$\Gamma(\mathbb{S})$: Grupo das simetrias de um conjunto $\mathbb{S}$.

$\mathcal{O}(s)$: Órbita de um ponto s sob um grupo $\mathbb{G}$.

$\mathbb{Q}_8$: Grupo dos quatérnios de ordem 8.

$\mathcal{D}_3$: Grupo dicíclico de ordem 12.

$\mathbb{D}_n$: Grupo diedral com $2n$ elementos formado pelas simetrias de um polígono regular de n lados.

$\square$: Fim de demonstração.

f, g, h: Funções.

$f \equiv g$: A função f é igual a função g.

$a = b$: a é igual a b.

$\#\mathbb{A}$: Cardinalidade do conjunto $\mathbb{A}$ ou o número de elementos de $\mathbb{A}$ quando for finito.

$\prod_{i=1}^{n} \mathbb{A}_i$: Produto cartesiano dos conjuntos $\mathbb{A}_i$, formado por n-uplas com coordenadas em $\mathbb{A}_i$.

$\mathbb{A}^n = \prod_{i=1}^{n} \mathbb{A}$: Produto cartesiano do conjunto $\mathbb{A}$, formado por n-uplas com coordenadas em $\mathbb{A}$.

$\mathcal{A}$: Alfabeto de um código.

$\mathbb{C}$: Código.

$\mathbb{C}'$ Código equivalente.

k : Dimensão de um código.

n : Comprimento de um código.

q : Cardinalidade de um alfabeto finito utilizado para o código.

r: Taxa de um código.

$\mathcal{I}$: Conjunto de índices de um código.

M : Tamanho de um código ou o número de palavras-código de um código dado.

$d_{\min}$: Distância mínima num código.

$\mathbf{RM}(r, m)$: Código de Reed-Muller binário de ordem r e comprimento 2^m.

$\mathbf{R}(n)$: Código de repetição de comprimento n.

$\mathbf{U}(n)$: Código universal de comprimento n.

d_H: Métrica de Hamming.

$d_{\min}^H$: Distância de Hamming mínima.

d_{Lee}: Métrica de Lee em $\mathbb{Z}_q$.

d_L: Distância de Lee em $\mathbb{Z}_q^n$.

$d_{\min}^L$: Distância de Lee mínima.

d_{ES}: Distância esférica.

w_{ES}: Peso esférico.

w_H: Peso de Hamming.

$w_{\min}^{H}$: Peso de Hamming mínimo.

w_L: Peso de Lee.

$(\mathbb{M}, d)$: Espaço métrico munido da métrica d.

$(\mathbb{M}_i, d_i)$:Espaço métrico munido da métrica d_i.

d_i: Métrica em $\mathbb{M}_i$, $i = 1, 2, \ldots n$.

α, β, γ: Funções que caracterizam o mapeamento ϕ da $\mathbb{Z}_4$-linearidade.

ϕ: Mapeamento da $\mathbb{Z}_4$-linearidade e extensões.

μ : Mapeamento casado.

$\mathbf{i}_{\mathbb{A}}$: Função identidade definida no conjunto $\mathbb{A}$.

$\mathbf{I}_n$: Matriz identidade de ordem n.

σ: Função troca.

$b_l(j)$: l-ésimo algarismo da representação binária de j, contado da esquerda para a direita.

d: Métricas.

d_{01}: Métrica zero-um.

d_e: Distância euclidiana.

d_E: Distância euclidiana quadrática.

d_f: Métrica induzida pela função f.

$d_{\max}$: Métrica do máximo.

d_{raiz}: Métrica da raiz.

d_{soma}: Métrica da soma.

$d_{\mathbb{S}}$: Métrica induzida pela métrica d para um subespaço métrico $\mathbb{S}$.

$dist$: Métrica usual da reta $\mathbb{R}$.

$\mathbf{e}_{jn}$: Vetor canônico.

Λ: Reticulado.

M-PSK: Conjunto de M sinais do tipo chaveamento por deslocamento de fase.

MDS: Código separável a máxima distância.

$MSED$: Distância mínima euclidiana quadrática.

$AWGN$: Ruído aditivo gaussiano branco.

Lista de Tabelas

Lista de Figuras

Conteúdo

Capítulo 1

Introdução

1.1 Histórico

O objetivo de um sistema de comunicação é transmitir informação de uma fonte para um destinatário através de um canal de comunicação com a maior confiabilidade possível.

Em um célebre artigo [52], Shannon provou que para taxas de transmissão de informação menor do que a capacidade de canal, existe um código que permite uma transmissão com probabilidade de erro arbitrariamente pequena.

Assim, as pesquisas se direcionaram para a procura de "bons" códigos e "bons" conjuntos de sinais associados a esses códigos.

Na linha de códigos surgiram as classes de códigos lineares e não-lineares e na linha de conjuntos de sinais foram propostos constelações de sinais ótimas sob diversas restrições, como por exemplo potência média, potência de pico, faixa e algumas combinações destas, os códigos de Slepian, seus variantes obtidos através de grupos de transformações ortogonais, as constelações tendo como base reticulados.

Essas linhas de pesquisa sempre foram tratadas separadamente até 1982, quando Ungerboeck [59] mostrou que, através do conceito de particionamento de conjunto de sinais, ganhos de codificação significativos eram obtidos. Surgia, então, a modulação codificada.

Dentro dessa nova linha de pesquisa, Forney [27] apresentou uma nova classe de códigos

denominada códigos geometricamente uniformes que, além de englobar os códigos de Slepian e os códigos reticulados, estende o procedimento proposto por Ungerboeck.

A procura por bons códigos continua sendo relevante, porém tendo que satisfazer, sempre quando possível, a propriedade de serem geometricamente uniformes.

Os códigos lineares constituem uma classe importante de códigos por possuírem uma estrutura algébrica permitindo que principalmente a decodificação seja bastante simplificada. Em contrapartida, a capacidade de correção de erros destes códigos não é melhor do que aquela de certos códigos não-lineares.

Por outro lado, os códigos não-lineares não possuem uma estrutura algébrica como a dos lineares. Esta flexibilidade possibilita obter códigos com distâncias de Hamming maiores do que as encontradas com os códigos lineares. Porém, a falta de uma estrutura algébrica aumenta a complexidade do processo de decodificação.

Diante das vantagens e desvantagens apresentadas surge a seguinte questão: existe uma técnica de construção de códigos que possa conduzir à determinação de códigos com distâncias de Hamming grandes, porém sem que para isso aumentemos consideravelmente a complexidade de decodificação?

Hammons et al. [15] foram os primeiros a proporem tal técnica de construção. Eles mostraram que os códigos de Kerdock, Preparata, Goethals e códigos relacionados são imagens binárias de certos códigos cíclicos estendidos sobre $\mathbb{Z}_4$, através de um mapeamento específico dos símbolos de $\mathbb{Z}_4$ nos símbolos de $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Em particular, o código de Nordstron-Robinson, cujos parâmetros são $n = 16, k = 8, d = 6$, é a imagem binária do octacódigo, o único código auto-dual de comprimento 8 sobre $\mathbb{Z}_4$ com distância mínima de Lee 6. O octacódigo é formado adicionando-se um dígito de verificação de paridade nas palavras do código cíclico de comprimento 7 sobre $\mathbb{Z}_4$, cujo polinômio gerador é $g(x) = x^3 + 3x^2 + 2x + 3$ [31]. Surge assim uma nova área de pesquisa em teoria da codificação: a $\mathbb{Z}_4$-linearidade.

A $\mathbb{Z}_4$-linearidade é uma técnica eficiente de construção de códigos binários e, em particular, de códigos binários não-lineares. Neste sentido, certas classes de códigos binários não-lineares podem ser vistos como códigos lineares sobre $\mathbb{Z}_4$ e, muitas vezes, como códigos cíclicos sobre

$\mathbb{Z}_4$. Como consequência, sua complexidade de decodificação é reduzida significativamente.

1.2 Apresentação do Problema

Neste trabalho, não trataremos especificamente da $\mathbb{Z}_4$-linearidade, mas sim de investigar extensões adequadas deste conceito para a $\mathbb{Z}_{p^k}$-linearidade, onde p e k são inteiros, p é primo, $p \geq 2$ e $k \geq 2$. Além disso, consideraremos a $\mathbb{G}$-linearidade, onde $\mathbb{G}$ é um grupo finito, como uma extensão da $\mathbb{Z}_{p^k}$-linearidade.

O objetivo em considerar tais extensões é o de propor novas classes de códigos q-ários que possam ser vistos como imagens de códigos lineares sobre $\mathbb{Z}_{p^k}$ ou até mesmo sobre um grupo. Entretanto, para a $\mathbb{Z}_{p^k}$-linearidade ou a $\mathbb{G}$-linearidade, pode ser possível incluir novas classes de códigos de grupo sobre grupo. Portanto, o objetivo é encontrar uma técnica de construção de códigos p-ários cujo comprimento seja um múltiplo de k, e que sejam imagem de códigos lineares sobre $\mathbb{Z}_{p^k}$, ou de códigos sobre grupos.

1.3 Descrição do Trabalho

No Capítulo 2 apresentamos os conceitos de grupos e espaços métricos bem como de códigos, sinais casados a grupos e códigos geometricamente uniformes que darão suporte ao presente trabalho.

No Capítulo 3 apresentamos inicialmente um estudo da $\mathbb{Z}_4$-linearidade e, em seguida, apresentamos propostas de extensões como a $\mathbb{Z}_{2^k}$-linearidade, onde resultados da existência de tais extensões são considerados sob determinadas condições.

No Capítulo 4 abordamos um contexto mais amplo de extensões da $\mathbb{Z}_4$-linearidade e apresentamos a definição de $\mathbb{G}$-linearidade, onde $\mathbb{G}$ é um grupo, da qual a $\mathbb{Z}_4$-linearidade é um caso particular. Ainda neste capítulo apresentamos o grupo de simetrias de $\mathbb{Z}_q^n$ com respeito à distância de Lee e estudamos a $\mathbb{G}$-linearidade associada a $\mathbb{Z}_q^n$.

No Capítulo 5 apresentamos as conclusões e propostas para futuros trabalhos de pesquisa.

Capítulo 2

Grupos, Espaços Métricos e Códigos

2.1 Introdução

O objetivo deste capítulo é apresentar os principais conceitos sobre grupos, espaços métricos e códigos que são utilizados ao longo deste trabalho.

Na Seção 2.2, apresentamos definições e exemplos de grupos abelianos e não-abelianos, além de algumas propriedades.

Na Seção 2.3, revemos os conceitos de espaços métricos, isometrias em espaços métricos e isometrias do espaço euclidiano n-dimensional e do espaço de Hamming.

Na Seção 2.4, fazemos uma breve revisão da teoria de códigos apresentando dois tópicos importantes propostos por Loeliger e Forney, onde o primeiro caracteriza os conjuntos de sinais casados a grupos e o segundo estabelece a classe dos códigos geometricamente uniformes. Esta classe enfatiza o aspecto de simetrias existente no conjunto de sinais e estabelece propriedades básicas da $\mathbb{Z}_4$-linearidade.

Finalmente, na Seção 2.5, apresentamos as conclusões.

2.2 Grupos: Definições e Exemplos

Por razão de completitude incluímos a presente seção neste trabalho; entretanto, os conceitos apresentados podem ser encontrados em textos clássicos, e.g., [2], [3], [24], [32], [33], [34], [35]

e [54].

Definição 2.2.1 *Um **grupo** é uma dupla* $(\mathbb{G}, *)$ *onde:*

- $\mathbb{G}$ *é um conjunto não-vazio;*
- $'*'$ *é uma operação binária sobre* $\mathbb{G}$ *que satisfaz as seguintes condições:*

  1. *Existe um elemento em* $\mathbb{G}$*, denotado por* $e_{\mathbb{G}}$ *tal que,* $e_{\mathbb{G}} * a = a = a * e_{\mathbb{G}}$;
  2. $\forall a \in \mathbb{G}, \exists\ a^{-1} \in \mathbb{G}$, *tal que* $a * a^{-1} = e_{\mathbb{G}} = a^{-1} * a$;
  3. $a * (b * c) = (a * b) * c$, $\forall a, b \in \mathbb{G}$;

A primeira condição caracteriza a existência de um **elemento neutro** (ou **identidade)** do grupo. A segunda condição caracteriza a existência de um **elemento inverso** e a terceira condição é denominada **associativa**. Segue da definição que: (i) o elemento neutro de $\mathbb{G}$ é único; (ii) para cada $a \in \mathbb{G}$, a^{-1} é univocamente determinado.

Se a operação '$*$' satisfizer também a condição:

$$a * b = b * a, \forall a, b \in \mathbb{G},$$

denominada **comutativa,** dizemos que $\mathbb{G}$ é um **grupo comutativo** ou **abeliano;** caso contrário, o grupo é denominado **não-abeliano.** Se $\mathbb{G}$ é um conjunto finito, dizemos que $\mathbb{G}$ é um **grupo finito** e o número de elementos de $\mathbb{G}$ é denominado a **ordem de** $\mathbb{G}$.

Exemplo 2.2.1 *O conjunto* $(\mathbb{Z}_M, \oplus)$ *dos inteiros módulo* M *sob a adição módulo* M *forma um grupo de ordem* M.

Exemplo 2.2.2 *O subconjunto de* $\mathbb{Z}_M$*, formado pelos elementos que possuem inverso multiplicativo (denominados **unidades** de* $\mathbb{Z}_M$*), denotado por* $\mathbb{Z}_M^*$*, ou seja,*

$$\mathbb{Z}_M^* = \{\overline{x} \in \mathbb{Z}_M |\ \exists\ \overline{y} \in \mathbb{Z}_M \text{ com } \overline{x}.\overline{y} = \overline{1}\}.$$

onde '.' denota a multiplicação módulo M*, forma um grupo.*

Definição 2.2.2 *Sejam* $(\mathbb{G}, *)$ *um grupo e* $\mathbb{H}$ *um subconjunto de* $\mathbb{G}$. *Dizemos que* $\mathbb{H}$ *é um* ***subgrupo de*** $\mathbb{G}$ *se* $\mathbb{H}$ *também for um grupo com a operação* $'*'$ *herdada de* $\mathbb{G}$.

Definição 2.2.3 *Seja* $\mathbb{X} = \{x_1, x_2, \ldots, x_l\}$ *um subconjunto de um grupo* $\mathbb{G}$. *O* ***subgrupo gerado por*** $\mathbb{X}$, *denotado por* $\langle \mathbb{X} \rangle$ *é o menor subgrupo de* $\mathbb{G}$ *que contém* $\mathbb{X}$. *Se existe* $\mathbb{X}$ *com* $l = 1$ *tal que* $\mathbb{G} = \langle \mathbb{X} \rangle$, *dizemos que* $\mathbb{G}$ *é um* ***grupo cíclico.***

Exemplo 2.2.3 *Se* $\mathbb{A}$ *é um conjunto não-vazio, então a coleção de todas as funções bijetoras* $f : \mathbb{A} \to \mathbb{A}$, *forma um grupo sob a operação de composição de funções denominado* ***grupo das permutações (ou das transformações) do conjunto*** $\mathbb{A}$ *e é denotado por* $\Theta_{\mathbb{A}}$. *Se* $\mathbb{A} = \{1, 2, \ldots, n\}$, *então* $\Theta_{\mathbb{A}}$ *é denominado o* ***grupo simétrico sobre n letras*** *e é denotado por* $\mathcal{S}_n$. *A ordem de* $\mathcal{S}_n$ *é* $n!$. *Em* $\mathcal{S}_n$ *temos um subgrupo formado por permutações pares denominado* ***grupo alternante,*** *denotado por* $\mathcal{A}_n$, *cuja ordem é* $\frac{n!}{2}$.

Exemplo 2.2.4 *Definimos em um polígono regular de n lados e centro de gravidade O, um grupo de rotações planas e espaciais descritos da seguinte forma: seja r uma rotação plana centrada em O de um polígono regular de n lados no sentido anti-horário de ângulo* $\frac{2\pi}{n}$ *e s uma rotação espacial de ângulo* π *sobre um eixo de simetria do polígono. Então os elementos deste conjunto, junto com a operação composição de funções, formam um grupo, denominado* ***grupo diedral de ordem*** $\mathbf{2n}$ *e denotado por* $\mathbb{D}_n$. *Seus elementos são:*

$$e, r, r^2, r^3, ..., r^{n-1}, s, rs, r^2s, r^3s, ..., r^{n-1}s.$$

Definição 2.2.4 *Sejam* $(\mathbb{G}, *)$ *um grupo,* $\mathbb{H}$ *um subgrupo de* $\mathbb{G}$ *e* $a \in \mathbb{G}$. *O subconjunto de* $\mathbb{G}$

$$a\mathbb{H} = \{a * b |\ b \in \mathbb{H}\}$$

é denominado ***classe lateral à esquerda de*** $\mathbb{H}$ ***contendo*** a. *O subconjunto de* $\mathbb{G}$

$$\mathbb{H}a = \{b * a |\ b \in \mathbb{H}\}$$

é denominado ***classe lateral à direita de*** $\mathbb{H}$ ***contendo*** a.

Definição 2.2.5 *Sejam* $(\mathbb{G}, *)$ *um grupo e* $\mathbb{H}$ *um subgrupo. Dizemos que* $\mathbb{H}$ *é um* ***subgrupo normal de*** $\mathbb{G}$ *se*

$$\forall a \in \mathbb{G}, \quad \forall b \in \mathbb{H}, \quad a^{-1} * b * a \in \mathbb{H}.$$

Denotamos por $\mathbb{H} \trianglelefteq \mathbb{G}$. *Se os únicos subgrupos normais de um grupo* $\mathbb{G}$, *são* $\{e_{\mathbb{G}}\}$ *e* $\mathbb{G}$, *dizemos que* $\mathbb{G}$ *é* ***simples.***

Proposição 2.2.1 *[35]Sejam* $(\mathbb{G}, *)$ *um grupo e* $\mathbb{H}$ *um subgrupo normal de* $\mathbb{G}$; *então a coleção de todas as classes laterais com a operação de produto de conjuntos forma um grupo, denotado por* $\mathbb{G}/\mathbb{H}$, *denominado* ***grupo quociente.***

Exemplo 2.2.5 *Considere a coleção finita de grupos* $\mathcal{C} = \{(\mathbb{G}_1, *_1), (\mathbb{G}_2, *_2), ..., (\mathbb{G}_n, *_n)\}$ *e o produto cartesiano, denotado por* $\mathbb{G} = \prod_{i=1}^{n} \mathbb{G}_i = \mathbb{G}_1 \times \mathbb{G}_2 \times ... \times \mathbb{G}_n$, *com a operação de cada grupo coordenada-a-coordenada, ou seja, se* $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n) \in \prod_{i=1}^{n} \mathbb{G}$ *tem-se:*

$$x * y = (x_1 *_1 y_1, x_2 *_2 y_2, ..., x_n *_n y_n).$$

O grupo $(\mathbb{G}, *)$ *é denominado* ***produto direto da coleção*** $\mathcal{C}$.

Definição 2.2.6 *Sejam* $(\mathbb{G}_1, *_1)$ *e* $(\mathbb{G}_2, *_2)$ *grupos quaisquer e* $f : \mathbb{G}_1 \to \mathbb{G}_2$ *uma função. Dizemos que* f *é um* ***homomorfismo*** *de* $\mathbb{G}_1$ *em* $\mathbb{G}_2$ *se*

$$f(a *_1 b) = f(a) *_2 f(b), \ \forall a, b \in \mathbb{G}_1.$$

Se f *é uma função bijetora, então diremos que* f *é um* ***isomorfismo de*** $\mathbb{G}_1$ ***em*** $\mathbb{G}_2$ *ou, ainda, que* $\mathbb{G}_1$ ***é isomorfo a*** $\mathbb{G}_2$ *e denotaremos por* $\mathbb{G}_1 \cong \mathbb{G}_2$. *No Apêndice B, apresentamos todos os grupos de ordem menor ou igual a 15 não isomorfos.*

Um isomorfismo de $\mathbb{G}$ em $\mathbb{G}$ é denominado **automorfismo de** $\mathbb{G}$. O conjunto de todos os automorfismos de um grupo $\mathbb{G}$ sob a operação de composição forma um grupo, denotado por $Aut(\mathbb{G})$.

Definição 2.2.7 *Sejam* $(\mathbb{G}_1, *_1)$ *e* $(\mathbb{G}_2, *_2)$ *grupos e* $\varphi : \mathbb{G}_2 \to Aut(\mathbb{G}_1)$ *um homomorfismo. O* ***produto semi-direto de*** $\mathbb{G}_1$ ***e*** $\mathbb{G}_2$, ***com relação a*** φ, *denotado por* $\mathbb{G}_1 \times_\varphi \mathbb{G}_2$, *é o grupo formado pelos pares* (a_1, a_2), *tais que* $a_1 \in \mathbb{G}_1, a_2 \in \mathbb{G}_2$ *e cuja operação é definida por*

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

O produto semi-direto $\mathbb{G}_1 \times_\varphi \mathbb{G}_2$ é um grupo (em geral, não-abeliano) e quando φ é tal que $\varphi(g) = e_{Aut(\mathbb{G}_1)}$, $\forall\ g \in \mathbb{G}_2$, temos o produto direto usual.

Nos dois exemplos, a seguir, iremos mostrar que a ordem em que apresentamos os dois grupos no produto semi-direto é relevante.

Exemplo 2.2.6 *Neste exemplo determinamos todos os produtos semi-diretos de*

$$\mathbb{Z}_2 \times_\varphi \mathbb{Z}_2^2,$$

dados por homomorfismos

$$\varphi : \mathbb{Z}_2^2 \longrightarrow Aut(\mathbb{Z}_2).$$

Em primeiro lugar, lembramos que

$$Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n^*,\ \textit{(unidades de } \mathbb{Z}_n\textit{)}$$

Então, existe apenas um homomorfismo

$$\varphi : \mathbb{Z}_2^2 \longrightarrow Aut(\mathbb{Z}_2).$$

Portanto, existe um único produto semi-direto que é o produto direto usual.

Exemplo 2.2.7 *Neste exemplo, determinamos um produto semi-direto*

$$\mathbb{Z}_2^2 \times_\varphi \mathbb{Z}_2$$

que é isomorfo a $\mathbb{D}_4$, o grupo das simetrias do quadrado.

Considere o homomorfismo

$$\varphi : \mathbb{Z}_2 \longrightarrow Aut(\mathbb{Z}_2^2)$$

definido por

$$\varphi(0) \equiv e_{Aut(\mathbb{Z}_2^2)} \in\ Aut(\mathbb{Z}_2^2)$$

e

$$\varphi(1) \in\ Aut(\mathbb{Z}_2^2),$$

definido por:

$$\varphi(1)(00) = 00$$
$$\varphi(1)(01) = 10$$
$$\varphi(1)(10) = 01$$
$$\varphi(1)(11) = 11.$$

Então, a operação de (a, b) *por* (c, d) *é dada por*

$$(a, b) * (c, d) = (a.\varphi(b)(c), bd).$$

Por exemplo, $a = 10$, $c = 01$, $b = 1$, *e* $d = 0$ *produz*

$$(10, 1)(01, 0) = (10 + \varphi(1)(01), 1 + 0) = (10 + 10, 1) = (00, 1).$$

A correspondente tabela de Cayley é mostrada na Tabela 2.1. Observamos que $f : \mathbb{Z}_2^2 \times_\varphi \mathbb{Z}_2 \rightarrow D_4$

$\mathbb{Z}_2 \times_\varphi \mathbb{Z}_2^2$	*(00,0)*	*(10,1)*	*(11,0)*	*(01,1)*	*(10,0)*	*(01,0)*	*(00,1)*	*(11,1)*
(00,0)	*(00,0)*	*(10,1)*	*(11,0)*	*(01,1)*	*(10,0)*	*(01,0)*	*(00,1)*	*(11,1)*
(10,1)	*(10,1)*	*(11,0)*	*(01,1)*	*(00,0)*	*(11,1)*	*(00,1)*	*(10,0)*	*(01,0)*
(11,0)	*(11,0)*	*(01,1)*	*(00,0)*	*(10,1)*	*(01,0)*	*(10,0)*	*(11,1)*	*(00,1)*
(01,1)	*(01,1)*	*(00,0)*	*(10,1)*	*(11,0)*	*(00,1)*	*(11,1)*	*(01,0)*	*(10,0)*
(10,0)	*(10,0)*	*(00,1)*	*(01,0)*	*(11,1)*	*(00,0)*	*(11,0)*	*(10,1)*	*(01,1)*
(01,0)	*(01,0)*	*(11,1)*	*(10,0)*	*(00,1)*	*(11,0)*	*(00,0)*	*(01,1)*	*(10,1)*
(00,1)	*(00,1)*	*(01,0)*	*(11,1)*	*(10,0)*	*(01,1)*	*(10,1)*	*(00,0)*	*(11,0)*
(11,1)	*(11,1)*	*(10,0)*	*(00,1)*	*(01,0)*	*(10,1)*	*(01,1)*	*(11,0)*	*(00,0)*

Tabela 2.1: Tabela de Cayley

dado por

$$f(00, 0) \equiv R_0 \qquad f(10, 0) \equiv rs$$
$$f(10, 1) \equiv R_1 \qquad f(01, 0) \equiv r^2 s$$
$$f(11, 0) \equiv R_2 \qquad f(00, 1) \equiv r$$
$$f(01, 1) \equiv R_3 \qquad f(11, 1) \equiv r^3 s$$

é um isomorfismo e $\mathbb{D}_4 \cong \mathbb{Z}_2^2 \times_\varphi \mathbb{Z}_2$.

Exemplo 2.2.8 *Neste exemplo determinamos todos os produtos semi-diretos de*

$$\mathbb{Z}_3 \times_\varphi \mathbb{Z}_3^2,$$

dados por homomorfismos

$$\varphi : \mathbb{Z}_3^2 \longrightarrow Aut(\mathbb{Z}_3).$$

Em primeiro lugar, lembramos que

$$Aut(\mathbb{Z}_3) \cong \mathbb{Z}_3^* \cong \mathbb{Z}_2.$$

Então, existe apenas um homomorfismo

$$\varphi : \mathbb{Z}_3^2 \longrightarrow Aut(\mathbb{Z}_3).$$

Portanto, existe um único produto semi-direto que é o produto direto usual.

O seguinte resultado fornece uma maneira de se obter produtos semi-diretos:

Teorema 2.2.1 *[2]Sejam $\mathbb{H}$ e $\mathbb{J}$ subgrupos de um grupo $\mathbb{G}$. Suponhamos que:*

- $\mathbb{H} \trianglelefteq \mathbb{G}$,
- $\mathbb{H} * \mathbb{J} = \mathbb{G}$,
- $\mathbb{H} \cap \mathbb{J} = \{e_{\mathbb{G}}\}$.

Então $\mathbb{G}$ é isomorfo ao produto semi-direto $\mathbb{H} \times_\varphi \mathbb{J}$, onde $\varphi : \mathbb{J} \longrightarrow Aut(\mathbb{H})$ é o homomorfismo definido por:

$$\varphi(y)(x) = y.x.y^{-1}, x \in \mathbb{H}, y \in \mathbb{J}.$$

2.3 Espaços Métricos

2.3.1 Definições e exemplos

Definição 2.3.1 *Sejam $\mathbb{M}$ um conjunto não vazio e $d : \mathbb{M} \times \mathbb{M} \longrightarrow \mathbb{R}$ 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 $x, y, z \in \mathbb{M}$. *Dizemos, então, que* d *é uma* ***métrica*** *e o par* $(\mathbb{M}, d)$ *é um* ***espaço métrico***.

Exemplo 2.3.1 *O conjunto dos números reais* $\mathbb{R}$ *com a função* $dist : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, *definida por*

$$dist(x,y) = |x - y|,$$

é um espaço métrico. As condições 1, 2, 3 e 4 resultam imediatamente das propriedades elementares do valor absoluto de números reais [40]. Esta métrica é chamada ***"métrica usual" da reta***.

Exemplo 2.3.2 *Dado um conjunto* $\mathbb{M}$, *a função*

$$d_{01}(x,y) = \begin{cases} 1 & se \quad x = y \\ 0 & se \quad x \neq y \end{cases}.$$

é uma métrica em $\mathbb{M}$. *As condições 1, 2, 3 e 4 são facilmente verificadas. Com isto,* $(\mathbb{M}, d_{01})$ *é um espaço métrico. A métrica* d_{01} *é denominada* ***métrica zero-um*** *ou, mais comumente conhecida,* ***distância de Hamming.***

Exemplo 2.3.3 *Se* $(\mathbb{M}, d)$ *é um espaço métrico, todo subconjunto* $\mathbb{S} \subseteq \mathbb{M}$ *é um espaço métrico* $(\mathbb{S}, d_{\mathbb{S}})$ *onde a métrica* $d_{\mathbb{S}}$ *é a função restrição* $d \mid \mathbb{S} \times \mathbb{S}$. *Neste caso,* $\mathbb{S}$ *é chamado* ***subespaço métrico de*** $\mathbb{M}$ *e* $d_{\mathbb{S}}$ *é denominada a* ***métrica induzida por*** d.

Exemplo 2.3.4 *O conjunto* $\mathbb{Z}$ *dos números inteiros munido da métrica dist (Exemplo 2.3.1) é um subespaço métrico de* $(\mathbb{R}, dist_{\mathbb{Z}})$, *de acordo com o Exemplo 2.3.3.*

Exemplo 2.3.5 *[40]Sejam* $(\mathbb{M}_1, d_1), (\mathbb{M}_2, d_2), \ldots, (\mathbb{M}_n, d_n)$ *espaços métricos. O produto cartesiano* $\mathbb{M} = \mathbb{M}_1 \times \mathbb{M}_2 \times \ldots \mathbb{M}_n$, *munido de uma das três métricas,*

- *Métrica da Raiz Quadrada:*

$$d_{raiz}(x, y) = \sqrt{d_1(x_1, y_1)^2 + d_2(x_2, y_2)^2 + \ldots + d_n(x_n, y_n)^2}$$

- *Métrica da Soma:*

$$d_{soma}(x, y) = d_1(x_1, y_1) + d_2(x_2, y_2) + \ldots + d_n(x_n, y_n)$$

- *Métrica do Máximo:*

$$d_{\max}(x, y) = max\{d_1(x_1, y_1), d_2(x_2, y_2), \ldots, d_n(x_n, y_n)\}$$

forma um espaço métrico, onde $x = (x_1, x_2, \ldots, x_n)$ *e* $y = (y_1, y_2, \ldots, y_n)$.

2.3.2 Isometrias

Definição 2.3.2 *Sejam* $(\mathbb{M}_1, d_1)$ *e* $(\mathbb{M}_2, d_2)$ *espaços métricos. Uma aplicação* $f : \mathbb{M}_1 \to \mathbb{M}_2$ *é denominada uma* ***imersão isométrica*** *quando*

$$d_2(f(x), f(y)) = d_1(x, y), \forall x, y \in \mathbb{M}_1.$$

Desta igualdade segue que f *é injetora. Se* f *for sobrejetora dizemos que* f *é uma* ***isometria de*** $\mathbb{M}_1$ ***em*** $\mathbb{M}_2$.

Exemplo 2.3.6 *A função identidade* $i_{\mathbb{M}} : \mathbb{M} \to \mathbb{M}$ *é uma isometria.*

Definição 2.3.3 *Sejam* $\mathbb{X}$ *um conjunto,* $(\mathbb{M}, d)$ *um espaço métrico e* $f : \mathbb{X} \to \mathbb{M}$ *uma aplicação injetiva. Definamos a aplicação*

$$d_f : \mathbb{X} \times \mathbb{X} \to \mathbb{R},$$

com

$$d_f(x, y) = d(f(x), f(y)), \ \forall \ x, y \in \mathbb{X}.$$

A função d_f *é uma métrica no conjunto* $\mathbb{X}$ *denominada* ***métrica induzida pela função*** f. *Esta é a única métrica em* $\mathbb{X}$ *que torna a função* f *uma imersão isométrica.*

Exemplo 2.3.7 • ***Translações:*** *As funções*

$$T_{\underline{a}} : \mathbb{R}^n \to \mathbb{R}^n,\ T_{\underline{a}}(\underline{x}) = \underline{x} + \underline{a},$$

são isometrias, para cada $\underline{a} \in \mathbb{R}^n$. *Quando* $\underline{a} = \underline{0}$ *temos a função identidade. A Fig. 2.1 ilustra o caso* $n = 2$.

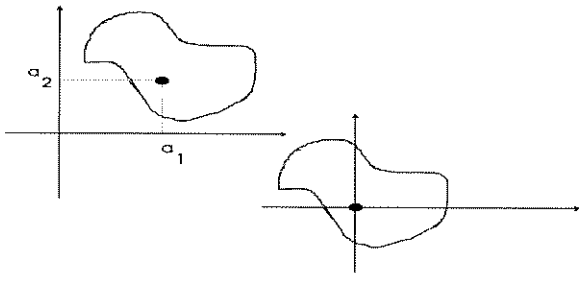

Figura 2.1: Translação no plano

- ***Transformações ortogonais:*** *São as funções*

$$R_O : \mathbb{R}^n \to \mathbb{R}^n,\ R_O(x) = O.x,$$

onde O *é uma matriz ortogonal* $n \times n$ *satisfazendo* $O^T.O = I_n$. *Esta relação implica que* $\det O = \pm 1$.

  - *Se* $\det O = 1$, *dizemos que temos uma* ***rotação pura ou própria.***
  - *Se* $\det O = -1$, *dizemos que temos uma* ***rotação imprópria ou com reflexão.***
  - *Se* $\det O = -1$ *e* $O^2 = I$ *(ordem 2), dizemos que temos uma* ***reflexão pura.***

Proposição 2.3.1 *Sejam* $f : \mathbb{M}_1 \to \mathbb{M}_2$ *uma imersão isométrica do espaço métrico* $(\mathbb{M}_1, d_1)$ *no espaço métrico* $(\mathbb{M}_2, d_2)$ *e* $(\mathbb{M}_3, d_3)$ *um outro espaço métrico. Temos então:*

- f *é injetora;*
- *Se* f *é uma isometria, então* $f^{-1} : \mathbb{M}_2 \to \mathbb{M}_1$ *é também uma isometria;*

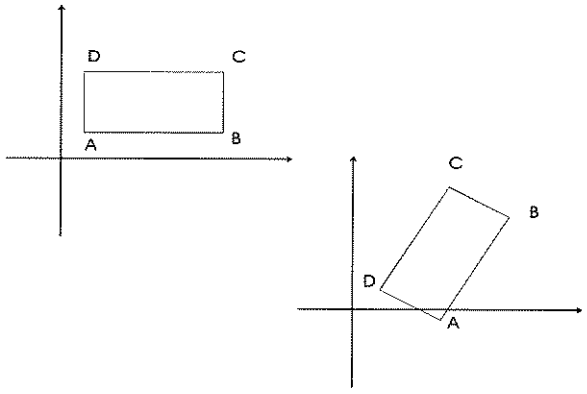

Figura 2.2: Rotaçao Própria

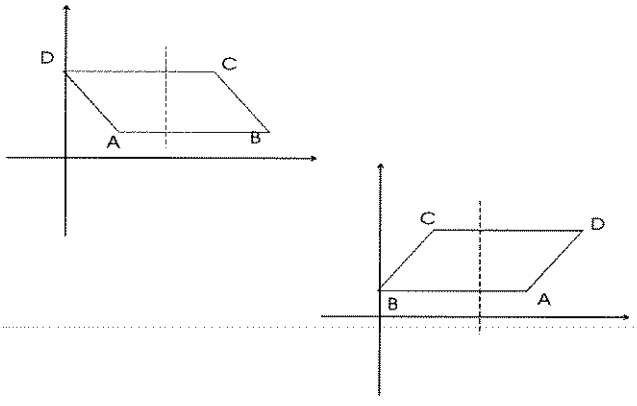

Figura 2.3: Reflexão Pura

- *Se* $g : \mathbb{M}_2 \to \mathbb{M}_3$ *é uma isometria de* $(\mathbb{M}_2, d_2)$ *em* $(\mathbb{M}_3, d_3)$*, então* $g \circ f : \mathbb{M}_1 \to \mathbb{M}_3$ *é uma isometria.*

  Demonstração: *Segue diretamente da definição de isometria.*□

Esta proposição mostra que o conjunto das isometrias $f : \mathbb{M} \to \mathbb{M}$, de um espaço métrico $(\mathbb{M}, d)$ sob a operação de composição de funções forma um grupo denominado **grupo de simetrias de** $\mathbb{M}$, denotado por $\Gamma(\mathbb{M})$.

2.3.3 Isometrias no espaço euclidiano n-dimensional

Seja $\mathbb{R}^n$ o **espaço euclidiano n-dimensional** formado pelas n-uplas reais, isto é,

$$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \ldots \mathbb{R} = \{(x_1, x_2, ..., x_n); x_i \in \mathbb{R} \ , \ i = 1, 2, ...n\},$$

e d_e a **distância euclidiana** dada por

$$d_e(x, y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}.$$

O espaço $(\mathbb{R}^n, d_e)$ é um espaço métrico para $n \geq 1$. De fato, no Exemplo 2.3.5, consideramos a métrica da raiz com

$$\mathbb{M}_1 = \mathbb{M}_2 = \ldots = \mathbb{M}_n = \mathbb{R},$$

onde

$$d_1 = d_2 = \ldots = d_n = dist \text{ (Exemplo 2.3.1)}$$

Note que **a distância euclidiana quadrática**

$$d_E(x, y) = [d_e(x, y)]^2$$

não é uma métrica pois não satisfaz as condições da Definição 2.3.1. De fato, considere

$$\begin{aligned} \mathbf{2} &= (2, 2, \ldots, 2) \\ \mathbf{1} &= (1, 1, \ldots, 1) \\ \mathbf{0} &= (0, 0, \ldots, 0) \end{aligned}$$

temos

$$\begin{aligned} d_E(\mathbf{2}, \mathbf{0}) &= 4n \geq \\ &\geq d_E(\mathbf{2}, \mathbf{1}) + d_E(\mathbf{1}, \mathbf{0}) = 2n. \end{aligned}$$

A partir da distância euclidiana temos duas outras funções importantes: a **norma**, ou seja, a função $\| \bullet \| : \mathbb{R}^n \to \mathbb{R}$, definida por

$$\|x\| = d_e(x, \mathbf{0}),$$

e o **produto interno,** a função $\langle \bullet, \circ \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, definida por

$$\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \ldots x_n y_n,$$

onde $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$. Note que $\langle x, x \rangle = \|x\|^2$.

Em $\mathbb{R}^n$, temos uma caracterização precisa do grupo de simetrias $\Gamma(\mathbb{S})$ de um subespaço métrico $\mathbb{S}$ de $\mathbb{R}^n$. Tal caracterização é dada pelo seguinte teorema:

Teorema 2.3.1 *Seja $f : \mathbb{R}^m \to \mathbb{R}^n$ uma imersão isométrica. Então existem $\underline{a} \in \mathbb{R}^n$ e uma transformação linear $T : \mathbb{R}^m \to \mathbb{R}^n$ tais que*

$$f(\underline{x}) = T(\underline{x}) + \underline{a}, \ \forall \ \underline{x} \in \mathbb{R}^m.$$

Em particular, se $m = n$ então f é uma isometria. Além disso, T é ortogonal. T é denominada ***constituinte linear de*** *f e a constante $\underline{a}$ é denominada* ***constituinte de translação de*** *f.*

Demonstração: *Considere $\underline{a} = f(\mathbf{0})$ e $T(\underline{x}) = f(\underline{x}) - f(\mathbf{0})$ com isso*

- $T(\mathbf{0}) = f(\mathbf{0}) - \underline{a} = \underline{a} - \underline{a} = \mathbf{0}$.
- *T é uma imersão isométrica de $\mathbb{R}^m$ em $\mathbb{R}^n$, pois*

$$d(T(\underline{x}), T(\underline{y})) = d(f(\underline{x}) - f(\mathbf{0}), f(\underline{y}) - f(\mathbf{0})) =$$
$$\|f(\underline{x}) - f(\mathbf{0}) - (f(\underline{y}) - f(\mathbf{0}))\| = \|f(\underline{x}) - f(\underline{y})\| = d(\underline{x}, \underline{y}).$$

- $\|T(\underline{x}) - T(\underline{y})\| = d(T(\underline{x}), T(\underline{y})) = d(\underline{x}, \underline{y}) = \|\underline{x} - \underline{y}\|$.
- $\|T(\underline{x})\| = d(T(\underline{x}), \mathbf{0}) = d(T(\underline{x}), T(\mathbf{0})) = d(\underline{x}, \mathbf{0}) = \|\underline{x}\|$.

  Além disso,

$$\|T(\underline{x}) - T(\underline{y})\|^2 = \|T(\underline{x})\|^2 + \|T(\underline{y})\|^2 - 2\langle T(\underline{x}), T(\underline{y}) \rangle = \|\underline{x}\|^2 + \|\underline{y}\|^2 - 2\langle T(\underline{x}), T(\underline{y}) \rangle$$

  e

$$\|\underline{x} - \underline{y}\|^2 = \|\underline{x}\|^2 + \|\underline{y}\|^2 - 2\langle \underline{x}, \underline{y} \rangle.$$

Logo,

$$\langle T(\underline{x}), T(\underline{y})\rangle = \langle \underline{x}, \underline{y}\rangle.$$

Desta forma, podemos verificar que T é linear,

$$\|T(c\underline{x}+\underline{y}) - cT(\underline{x}) - T(\underline{y})\| =$$

$$\begin{aligned}
&= \langle T(c\underline{x}+\underline{y}) - cT(\underline{x}) - T(\underline{y}), T(c\underline{x}+\underline{y}) - cT(\underline{x}) - T(\underline{y})\rangle = \\
&= \langle T(c\underline{x}+\underline{y}), T(c\underline{x}+\underline{y})\rangle - \langle T(c\underline{x}+\underline{y}), cT(\underline{x})\rangle - \langle T(c\underline{x}+\underline{y}), T(\underline{y})\rangle \\
&\quad -\langle cT(\underline{x}), T(c\underline{x}+\underline{y})\rangle + \langle cT(\underline{x}), cT(\underline{x})\rangle + \langle cT(\underline{x}), T(\underline{y})\rangle - \\
&\quad -\langle T(\underline{y}), T(c\underline{x}+\underline{y})\rangle + \langle T(\underline{y}), cT(\underline{x})\rangle + \langle T(\underline{y}), T(\underline{y})\rangle \\
&= \langle c\underline{x}+\underline{y}, c\underline{x}+\underline{y}\rangle - \langle c\underline{x}+\underline{y}, c\underline{x}\rangle - \langle c\underline{x}+\underline{y}, \underline{y}\rangle - \langle c\underline{x}, c\underline{x}+\underline{y}\rangle + \\
&\quad +\langle c\underline{x}, c\underline{x}\rangle + \langle c\underline{x}, \underline{y}\rangle - \langle \underline{y}, c\underline{x}+\underline{y}\rangle + \langle \underline{y}, c\underline{x}\rangle + \langle \underline{y}, \underline{y}\rangle \\
&= \langle c\underline{x}, c\underline{x}\rangle + \langle c\underline{x}, \underline{y}\rangle + \langle \underline{y}, c\underline{x}\rangle + \langle \underline{y}, \underline{y}\rangle - \langle c\underline{x}, c\underline{x}\rangle - \langle \underline{y}, c\underline{x}\rangle - \\
&\quad -\langle c\underline{x}, \underline{y}\rangle - \langle \underline{y}, \underline{y}\rangle - \langle c\underline{x}, c\underline{x}\rangle - \langle c\underline{x}, \underline{y}\rangle + \langle c\underline{x}, c\underline{x}\rangle \\
&\quad +\langle c\underline{x}, \underline{y}\rangle - \langle \underline{y}, c\underline{x}\rangle - \langle \underline{y}, \underline{y}\rangle + \langle \underline{y}, c\underline{x}\rangle + \langle \underline{y}, \underline{y}\rangle \\
&= 0
\end{aligned}$$

Disto segue que

$$T(c\underline{x}+\underline{y}) = cT(\underline{x}) + T(\underline{y}).$$

Portanto, T é ortogonal por [36].□

2.3.4 Isometrias no espaço de Hamming n-dimensional

Seja $\mathbb{A}$ um conjunto finito com q elementos. Pelo Exemplo 2.3.2, definimos a métrica zero-um d_{01} em $\mathbb{A}$. A **distância de Hamming** em $\mathbb{A}^n$, denotada por d_H, é definida pela métrica da soma d_{soma} (Exemplo 2.3.5, com $d_1 = d_2 = \ldots = d_n = d_{01}$). Desta forma, $d_H : \mathbb{A}^n \times \mathbb{A}^n \longrightarrow \mathbb{R}$ é uma métrica e o par $(\mathbb{A}^n, d_H)$ é um espaço métrico denominado **espaço de Hamming.** Observe que a distância de Hamming entre duas n-uplas é simplesmente o número de coordenadas em que elas diferem.

No espaço de Hamming $\mathbb{Z}_2^n$, apresentamos um resultado (citado em [31] mas não demonstrado) que fornece uma caracterização precisa de seu grupo de simetrias :

Teorema 2.3.2 *O grupo de simetrias do espaço de Hamming n-dimensional* $\mathbb{Z}_2^n$, $\Gamma(\mathbb{Z}_2^n)$, *é dado por*

$$\Gamma(\mathbb{Z}_2^n) = \mathbb{Z}_2^n \times_\varphi \mathcal{S}_n.$$

Para demonstrar este teorema utilizaremos os seguintes lemas:

Lema 2.3.1 *Toda isometria* $\phi : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ *é da forma*

$$\phi(\underline{x}) = T_{\underline{a}} \circ \psi(\underline{x}),$$

onde $T_{\underline{a}} : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ *é dado por* $T_{\underline{a}}(x) = \underline{x} + \underline{a}$, *com* $\underline{a} = \phi(\underline{0})$ *e* $\psi : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ *possui as seguintes propriedades:*

- $\psi(\underline{0}) = \underline{0}$;
- ψ *é isometria;*
- ψ *preserva pesos de Hamming.*

Além disso, o subgrupo gerado pelas translações é isomorfo ao grupo $\mathbb{Z}_2^n$.

Demonstração: *Basta considerar* $\psi(\underline{x}) = \phi(\underline{x}) - \underline{a}$ *e o isomorfismo de grupos é dado por* $h : \mathbb{Z}_2^n \to T(\mathbb{Z}_2^n), \quad h(\underline{a}) = T_{\underline{a}}$.□

Lema 2.3.2 *Toda isometria* $\psi : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, *tal que* $\psi(\underline{0}) = \underline{0}$ *é uma permutação de coordenadas. Além disso, o subgrupo gerado por estas isometrias,* $\Psi(\mathbb{Z}_2^n)$, *é isomorfo a* $\mathcal{S}_k$.

Demonstração: *Em primeiro lugar, observamos que toda permutação de coordenadas* $\rho : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, *é uma isometria tal que* $\psi(\underline{0}) = \underline{0}$. *Reciprocamente, temos que como* ψ *preserva pesos de Hamming, então o número de 1's nas coordenadas da imagem deverá ser o mesmo e portanto isto deverá ser uma permutação de coordenadas. O isomorfismo com o grupo de permutações é óbvio.* □

Observe que $\Psi(\mathbb{Z}_2^n)$ pode ser representado por um conjunto de matrizes, denominado **matrizes de permutação,** que são aquelas cujas linhas e colunas possuem 1 numa única posição e nas posições restantes é zero. Desta forma,

$$\psi(x_1, x_2, \ldots, x_n) = P. \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

onde P é uma matriz de permutação. A função ϕ pode ser expressa na forma matricial

$$\phi(x_1, x_2, \ldots, x_n) = P. \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}.$$

Utilizando coordenadas homogêneas e identificando

$$(x_1, x_2, \ldots, x_n) \rightarrow (x_1, x_2, \ldots, x_n, 1),$$

as translações podem ser incluídas também na forma matricial:

$$\begin{aligned} \phi(x_1, x_2, \ldots, x_n, 1) &= \begin{bmatrix} & & & a_1 \\ & P & & a_2 \\ & & & \vdots \\ & & & a_n \\ 0 & \ldots & 0 & 1 \end{bmatrix} . \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ 1 \end{bmatrix} \bmod 2 = \\ &= \tilde{P}. \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ 1 \end{bmatrix}. \end{aligned}$$

Lema 2.3.3 *O subgrupo $T(\mathbb{Z}_2^n)$ é normal em $\Gamma(\mathbb{Z}_2^n)$.*

Demonstração: *Através da representação matricial de $\Psi(\mathbb{Z}_2^n)$ e do produto de matrizes por blocos, verificamos que*

$$\psi^{-1} \circ T_{\underline{a}} \circ \psi(x) = \psi^{-1}(\psi(\underline{x}) + \underline{a}) = \underline{x} + \psi^{-1}(\underline{a}) \in T(\mathbb{Z}_2^n).$$

□

Demonstração do teorema: Como toda isometria é uma combinação de uma translação com uma isometria que fixa o vetor nulo temos que

$$\Gamma(\mathbb{Z}_2^n) = T(\mathbb{Z}_2^n) \circ \Psi(\mathbb{Z}_2^n).$$

Mas $T(\mathbb{Z}_2^n) \cap \Psi(\mathbb{Z}_2^n) = \{e\}$ e $T(\mathbb{Z}_2^n)$ é normal em $\Gamma(\mathbb{Z}_2^n)$, portanto pelo Teorema 2.2.1, obtemos o resultado desejado.□

2.4 Códigos

2.4.1 Definições, exemplos e propriedades

Definição 2.4.1 *Dados um espaço métrico $(\mathcal{A}, d)$ e um conjunto enumerável $\mathcal{I}$, um* ***código sobre $\mathcal{A}$,*** *denotado por $\mathbb{C}$, é qualquer subconjunto não-vazio do produto cartesiano $\mathcal{A}^{\mathcal{I}}$.*

- *$\mathcal{A}$ é denominado* ***alfabeto*** *do código $\mathbb{C}$.*
- *$\mathcal{I}$ é denominado* ***conjunto de índices*** *do código $\mathbb{C}$.*
- *Um elemento do código é denominado* ***palavra-código.***
- *Os elementos do alfabeto $\mathcal{A}$ são chamados* ***símbolos*** *que compõem a palavra-código.*
- *Se $\mathbb{C}$ é um conjunto finito, diremos que $\mathbb{C}$ é um* ***código finito.***
- *A cardinalidade de um código finito é denominada* ***tamanho*** *do código, denotado por M.*

- *Quando $\mathcal{I}$ é finito, o código $\mathbb{C}$ é denominado* ***código de bloco****. Neste caso, a cardinalidade de $\mathcal{I}$, denotada por n, é denominada* ***comprimento da palavra-código****.*

- *Quando $\mathcal{I}$ é infinito diz-se que o código é um* ***código de treliça****.*

- *Quando o alfabeto $\mathcal{A}$ é finito de cardinalidade q, a* ***dimensão*** *de um código finito de tamanho M, denotada por k, é definida por*

$$k = log_q M.$$

e a ***taxa*** *do código, denotada por r, é definida por*

$$r = \frac{k}{n} \text{ símbolos/bloco.}$$

Quando k for inteiro, diremos que a palavra-código contém k ***dígitos de informação****. Se, além disso, $\mathcal{I}$ for finito, diremos que a palavra código contém $(n-k)$* ***dígitos de redundância****.*

- *Um código $\mathbb{C}'$ obtido de outro código $\mathbb{C}$ através de uma permutação de coordenadas, é denominado* ***equivalente*** *a $\mathbb{C}$.*

- *A* ***distância mínima*** *de um código $\mathbb{C}$, denotada por $d_{\min}$, $\mathbb{C}$ é definida por*

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

A métrica no alfabeto $\mathcal{A}$ induz uma métrica no código $\mathbb{C}$ que pode ser uma das métricas, porém não exclusivamente, a métrica da soma, a métrica do máximo ou a métrica da raiz quadrada. A capacidade de correção de erros de um código é estabelecida através da métrica em consideração.

Exemplo 2.4.1 *O código $\mathbb{C} = \mathcal{A}^{\mathcal{I}}$ é denominado* ***código universal*** *e quando $\mathcal{A}$ e $\mathcal{I}$ tem cardinalidade q e n, temos*

- $k = log_q M = log_q q^n = n$;

- *n dígitos de informação;*

- 0 *dígitos de redundância;*
- $r = 1$.

Exemplo 2.4.2 *Seja* $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ *um alfabeto com uma métrica qualquer e*

$$\mathbb{C} = \{(a_1, a_1, \ldots, a_1, \ldots), (a_2, a_2, \ldots, a_2, \ldots), \ldots, (a_q, a_q, \ldots, a_q, \ldots)\}.$$

Então, $\mathbb{C}$ *é denominado* ***código de repetição****. Se* $\mathcal{I}$ *é finito, o mesmo possui os seguintes parâmetros:*

- 1 *dígito de informação q-ário;*
- $(n-1)$ *dígitos de redundância q-ário;*
- $r = \frac{1}{n}$.

Exemplo 2.4.3 *Se* $\mathcal{A} \subseteq \mathbb{R}$ *com a métrica euclidiana, onde* $\mathcal{A}$ *é um conjunto discreto, o código* $\mathbb{C}$ *é denominado* ***conjunto de sinais*** *e denotado por* $\mathbb{S}$.

Exemplo 2.4.4 *Sejam* $\mathcal{A} = \mathbb{F}_q$ *um corpo com q elementos,* $\mathcal{I} = \{1, 2, \ldots, n\}$ *e a métrica de Hamming. Um código* $\mathbb{C}$ *é denominado um* $(n, k, d_{\min})$-***código linear q-ário*** *se for um subespaço vetorial de* $\mathbb{F}_q^n$*. Um código* $\mathbb{C}$ *que não possui a estrutura de um subespaço vetorial, é denominado* ***código q-ário não linear.***

Exemplo 2.4.5 *Seja* $\mathcal{A} = \mathbb{G}$, $\mathbb{G}$ *um grupo finito, com uma determinada métrica (por exemplo, a de Hamming). Então, o código* $\mathbb{C}$ *é denominado* ***código de grupo sobre o grupo*** $\mathbb{G}$ *se* $\mathbb{C}$ *for um subgrupo de* $\mathbb{G}^{\mathcal{I}}$*. Se* $\mathbb{C}$ *é um subgrupo normal de* $\mathbb{G}^{\mathcal{I}}$ *dizemos que* $\mathbb{C}$ *é um* ***código de grupo normal sobre*** $\mathbb{G}$.

Mencionaremos, a seguir, alguns resultados sobre códigos de grupos sobre grupos não-abelianos. Estes resultados serão importantes para se verificar a viabilidade de se procurar códigos de grupo sobre grupos não-abelianos como forma de se obter bons códigos binários.

Teorema 2.4.1 *[30] Seja $n \geq 3$. Existe um $(n, n-1, 2)$-código de grupo sobre um grupo $\mathbb{G}$ se, e somente se, $\mathbb{G}$ é abeliano.*

Corolário 2.4.1 *[30] Para $1 < k < n$, não existe um $(n, k, n-k+1)$-código MDS sobre um grupo $\mathbb{G}$ não-abeliano.*

Desta forma, vemos que para códigos de grupo sobre grupos não abelianos a propriedade de grupo é, em geral, incompatível com o objetivo de atingir a melhor distância de Hamming mínima possível. Vejamos agora os códigos lineares sobre grupos não abelianos que são normais.

Definição 2.4.2 *Dado um código de grupo $\mathbb{C}$ sobre o grupo $\mathbb{G}$ e $k \in \mathcal{I}$, o* ***grupo de saída****, denotado por $\mathbb{G}_k$, é o conjunto de todos os elementos de $\mathbb{G}$ que ocorrem na k-ésima coordenada. O* ***espaço de saída****, denotado por W, é dado por $\prod_{k=1}^{n} G_k$.*

Teorema 2.4.2 *[30] Se $\mathbb{C}$ é um código de grupo normal sobre um grupo $\mathbb{G}$ e o espaço de saída $W = \prod_{k=1}^{n} G_k$ é não-abeliano, então a distância de Hamming mínima é $d_H(\mathbb{C}) = 1$.*

O próximo teorema estabelece que os códigos sobre grupos não-abelianos são assintoticamente ruins.

Teorema 2.4.3 *[37] Um limitante superior para a distância de Hamming mínima de um código de bloco sistemático de grupo sobre um grupo não abeliano é dado por*

$$d_{\min}^{H} \leq \lfloor \frac{n}{k} \rfloor.$$

Além disso, para uma taxa fixa r, a razão $\delta = \frac{d_{\min}^{H}}{n}$ aproxima-se de zero quando n tende a infinito.

2.4.2 Conjuntos de sinais casados a grupos

A principal motivação para considerar o codificador e o modulador como um só bloco é estabelecer a melhor forma de associar uma palavra-código a um sinal a ser transmitido. Conjunto de sinais casado a um grupo, segundo Loeliger [43], constitui a forma mais adequada de estabelecer esta associação.

As definições e os resultados aqui apresentados são extensões dos propostos em [43] para espaços métricos quaisquer quando o contexto permitir.

Definição 2.4.3 *[43]Seja $(\mathbb{M}, d)$ um espaço métrico. Dizemos que um conjunto de sinais $\mathbb{S}$, finito, em $\mathbb{M}$ está* ***casado a um grupo*** *$\mathbb{G}$ se existe uma função μ de $\mathbb{G}$ sobre $\mathbb{S}$ tal que,*

$$d(\mu(g), \mu(g')) = d(\mu(g^{-1} * g'), \mu(e_{\mathbb{G}})), \ \forall \ g, g' \in \mathbb{G}$$

onde $e_{\mathbb{G}}$ é o elemento neutro de $\mathbb{G}$. A função μ é denominada ***mapeamento casado****. Se μ é injetora, então μ^{-1} é denominada* ***rotulamento casado****.*

Exemplo 2.4.6 *O conjunto de sinais M-PSK contido no espaço euclidiano bidimensional $(\mathbb{R}^2, d_e)$ está casado ao grupo $(\mathbb{Z}_M, \oplus)$. De fato, considere a função*

$$\mu : \mathbb{Z}_M \to \mathbb{R}^2, \ \mu(a) = \left(r\cos\left(\frac{2\pi a}{M}\right), r sen\left(\frac{2\pi a}{M}\right)\right).$$

Identificando $\mathbb{R}^2$ com $\mathbb{C}$, escrevemos μ na forma

$$\mu(a) = r.e^{\frac{i2\pi a}{M}}.$$

Seguindo esta notação temos

$$\begin{aligned} d_e(\mu(a), \mu(b)) &= \|r.e^{\frac{i2\pi a}{M}} - r.e^{\frac{i2\pi b}{M}}\| = \|e^{\frac{i2\pi a}{M}}\|.\|r - r.e^{\frac{i2\pi(b-a)}{M}}\| = \|r.e^{\frac{i2\pi(b-a)}{M}} - r\| = \\ &= d_e(\mu(b-a), \mu(0)). \end{aligned}$$

Além disso, como μ é uma bijeção entre $\mathbb{Z}_M$ e o conjunto M-PSK, temos que a função inversa μ^{-1} : M-PSK$\longrightarrow \mathbb{Z}_M$ é um rotulamento casado.

Lema 2.4.1 *[43] Seja μ a função tal que o conjunto de sinais $\mathbb{S}$ em um espaço métrico $(\mathbb{M}, d)$ esteja casado a um grupo $\mathbb{G}$. Se $s_{e_{\mathbb{G}}} = \mu(e_{\mathbb{G}})$, onde $e_{\mathbb{G}}$ é o elemento neutro de $\mathbb{G}$ e $\mathbb{H} = \mu^{-1}(s_{e_{\mathbb{G}}})$, então $\mathbb{H}$ é um subgrupo de $\mathbb{G}$ e, além disso,*

$$\mu(g) = \mu(g') \Longleftrightarrow g\mathbb{H} = g'\mathbb{H}, \tag{2.1}$$

ou seja, g e g' estão na mesma classe lateral à esquerda de $\mathbb{H}$ em $\mathbb{G}$.

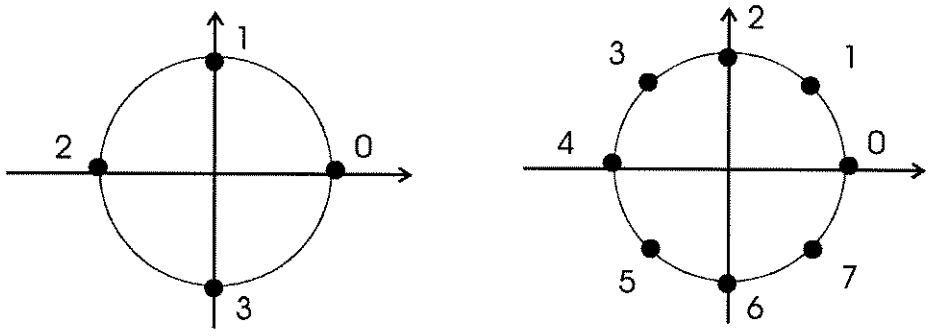

Figura 2.4: Conjuntos de sinais 4-PSK e 8-PSK casados a $\mathbb{Z}_{\not\leftarrow}$ e $\mathbb{Z}_{\leftarrow}$, respectivamente.

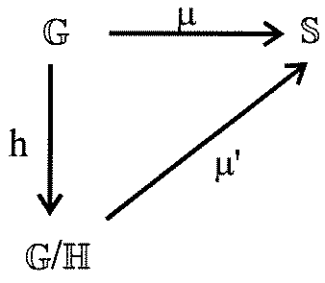

Figura 2.5: $\mathbb{S}$ está casado a $\mathbb{G}/\mathbb{H}$.

Proposição 2.4.1 *[43] Seja $\mathbb{S}$ um conjunto de sinais em um espaço métrico $(\mathbb{M}, d)$. Se $\mathbb{S}$ está casado a um grupo $\mathbb{G}$ e $\mathbb{H}$ é um subgrupo normal em $\mathbb{G}$, então $\mathbb{S}$ está casado a $\mathbb{G}/\mathbb{H}$. (veja Fig. 2.5).*

Definição 2.4.4 *[43] Seja μ a função tal que o conjunto de sinais $\mathbb{S}$ em um espaço métrico $(\mathbb{M}, d)$ esteja casado a um grupo $\mathbb{G}$, e $\mathbb{H}$ definido como no Lema 2.4.1. Se $\mathbb{H}$ não contém subgrupos normais não triviais de $\mathbb{G}$, então dizemos que μ é um* ***mapeamento efetivamente casado*** *e $\mathbb{S}$ está* ***efetivamente casado*** *a $\mathbb{G}$.*

Teorema 2.4.4 *[43] Seja μ a função tal que o conjunto de sinais $\mathbb{S}$ em um espaço métrico $(\mathbb{M}, d)$ esteja casado ao grupo $\mathbb{G}$,e $\mathbb{H}$ definido como no Lema 2.4.1. Então $\mathbb{S}$ está efetivamente casado ao grupo quociente $\mathbb{G}/\mathbb{H}'$, onde $\mathbb{H}'$ é o maior subgrupo normal de $\mathbb{G}$ contido em $\mathbb{H}$.*

Demonstração: *Definindo $\mu'(h(g)) = \mu(g)$, onde h é a projeção canônica, temos que*

- *μ' está bem definida pois*

$$\begin{aligned} g_1\mathbb{H}' &= g_2\mathbb{H}' \Rightarrow g_2^{-1} * g_1 \in \mathbb{H}' \Rightarrow g_2^{-1} * g_1 \in \mathbb{H} \Rightarrow g_1\mathbb{H} = g_2\mathbb{H} \\ &\Rightarrow \mu(g_1) = \mu(g_2) \Rightarrow \mu'(h(g_1)) = \mu'(h(g_2)); \end{aligned}$$

- *μ' é uma transformação casada pois*

$$\begin{aligned} &d(\mu'(g_1\mathbb{H}'), \mu'(g_2\mathbb{H}')) = d(\mu'(h(g_1)), \mu'(h(g_2))) = \\ &= d(\mu(g_1), \mu(g_2)) = d(\mu(g_1^{-1} * g_2), \mu(e_{\mathbb{G}})) = \\ &= d(\mu'(g_1^{-1} * g_2\mathbb{H}'), \mu'(\mathbb{H}')). \end{aligned}$$

- *μ' é efetivamente casada, pois considerado*

$$\mathcal{M} = \{g.\mathbb{H}' \mid \mu'(g\mathbb{H}') = \mu'(\mathbb{H}')\},$$

isto é, $\mathcal{M}$ é o conjunto equivalente a $\mathbb{H}$ considerando em $\mathbb{G}/\mathbb{H}'$.

Suponhamos que exista um subgrupo normal não trivial $\mathcal{N} \subset \mathcal{M}$ de $\mathbb{G}/\mathbb{H}'$. Temos

1. $\mathbb{H}' \subset h^{-1}(\mathcal{N}) \subset \mathbb{H}$;
2. *$h^{-1}(\mathcal{N})$ é um subgrupo normal de $\mathbb{G}$.*

Mas isto contradiz a hipótese de que $\mathbb{H}'$ é o maior subgrupo normal de $\mathbb{G}$ contido em $\mathbb{H}$. Portanto, não existe um subgrupo normal não trivial em $\mathcal{M}$.□

Com isso, podemos ignorar transformações casadas que não são efetivas porque mesmo que $\mathbb{S}$ não esteja efetivamente casado a $\mathbb{G}$ ele será, pelo Teorema 2.4.4, efetivamente casado a $\mathbb{G}/\mathbb{H}'$.

Teorema 2.4.5 *[43] Se $\mathbb{S}$, um conjunto de sinais em um espaço métrico $(\mathbb{M}, d)$, está casado a um grupo $\mathbb{G}$ e se $f : \mathbb{S} \to \mathbb{T} = f(\mathbb{S})$ é uma isometria, então $f(\mathbb{S})$ também está casado a $\mathbb{G}$.*

Demonstração: *Considere o diagrama mostrado na Fig. 2.6. Seja $\mu' : \mathbb{G} \to \mathbb{T} = f(\mathbb{S})$, $\mu'(g) = f(\mu(g))$, temos que*

- *μ' é sobrejetora pois, dado $t \in \mathbb{T}$, existe $s \in \mathbb{S}$ tal que $f(s) = t$; para $s \in \mathbb{S}$ existe $g \in \mathbb{G}$, tal que $\mu(g) = s$. Portanto, $f(\mu(g)) = f(s) = t$;*

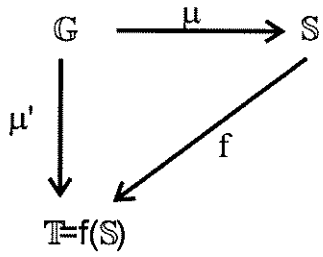

Figura 2.6: O conjunto de sinais $f(\mathbb{S})$ é casado a $\mathbb{G}$, pelo mapeamento μ'.

- *μ' é uma transformação casada pois para $g_1, g_2 \in \mathbb{G}$*

$$d(\mu'(g_1), \mu'(g_2)) = d(f \circ \mu(g_1), f \circ \mu(g_2)) =^{f \text{ é isometria}} d(\mu(g_1), \mu(g_2)) =$$
$$=^{\mu \text{ é transf. casada}} d(\mu(g_1^{-1} * g_2), \mu(e_{\mathbb{G}})) =^{f \text{ é isometria}} d(f \circ \mu(g_1^{-1} * g_2), f \circ \mu(e_{\mathbb{G}})) =$$
$$= d(\mu'(g_1^{-1} * g_2), \mu'(e_{\mathbb{G}})).$$

□

Podemos estender naturalmente $\mu : \mathbb{G} \to \mathbb{S}$, para uma transformação definida em $\mathbb{G}^n$.

Definição 2.4.5 *[43] Sejam $\mu : \mathbb{G} \to \mathbb{S}$ um mapeamento casado e n um inteiro positivo. A n-**ésima-extensão de** μ é uma transformação $\mu^n : \mathbb{G}^n \to \mathbb{S}^n$, definida por*

$$\mu^n(g_1, g_2, \ldots, g_n) = (\mu(g_1), \mu(g_2), \ldots, \mu(g_n)),$$

onde a métrica em $\mathbb{S}^n$ pode ser dada por uma das métricas mencionadas no Exemplo 2.3.5.

Teorema 2.4.6 *[43] Sejam $\mu : \mathbb{G} \to \mathbb{S}$ um mapeamento casado e $\mathbb{C}$ um código de grupo sobre o grupo $\mathbb{G}$. Então, $\mu^n(\mathbb{C})$ está casado a $\mathbb{C}$ e $\mu^n : \mathbb{C} \to \mu^n(\mathbb{C})$ é um mapeamento casado.*

Demonstração: *Vamos demonstrar utilizando a métrica da soma (para as outras métricas o raciocínio é análogo): Sejam $c_1, c_2 \in \mathbb{C}$,*

$$d_{soma}(\mu^n(c_1), \mu^n(c_2)) = \sum_{i=1}^{n} d(\mu(c_{1i}), \mu(c_{2i})) = \sum_{i=1}^{n} d(\mu(c_{1i}^{-1} * c_{2i}), \mu(e_{\mathbb{G}})) =$$
$$= d_{soma}(\mu^n(c_1^{-1} * c_2), \mu^n(e_{\mathbb{G}}^n)).$$

□

A noção definida a seguir, relaciona um grupo com um espaço métrico. Esta noção é mais restritiva do que se conhece normalmente e foi motivada pelo fato de que estamos lidando com um conjunto que possui uma estrutura de espaço métrico. Desta forma, procuramos uma "ação" do grupo que respeite esta estrutura.

Definição 2.4.6 *Um grupo* $(\mathbb{G}, *)$ ***atua em um conjunto de sinais*** $\mathbb{S}$, *se existe um homomorfismo* $h : \mathbb{G} \to \Gamma(\mathbb{S})$. *Nestas condições, se* $s \in \mathbb{S}$, *a* ***órbita de*** s ***sob*** $\mathbb{G}$, *denotada por* $\mathcal{O}(s)$, *é o conjunto:*

$$\mathcal{O}(s) = \{h(a)(s); a \in \mathbb{G}\}.$$

Se para cada $s_1, s_2 \in \mathbb{S}$, *existe* $a \in \mathbb{G}$, *tal que* $h(a)(s_1) = s_2$, *dizemos que* $\mathbb{G}$ *é* ***transitivo sobre*** $\mathbb{S}$.

Quando $\mathbb{G}$ é transitivo sobre $\mathbb{S}$ a órbita de um ponto $s_0 \in \mathbb{S}$ fornece uma função $\phi : \mathbb{G} \to \mathbb{S}$. De fato, para cada $s \in \mathbb{S}$ existe um elemento $a \in \mathbb{G}$, tal que $h(a)(s_0) = s$ e, com isso, definimos a função $\phi : \mathbb{G} \to \mathbb{S}$ como $\phi(a) = h(a)(s_0)$.

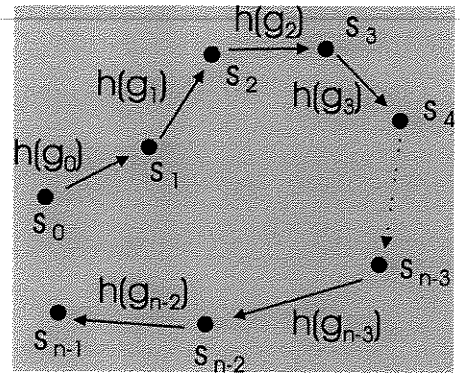

Figura 2.7: Órbita de um ponto

Teorema 2.4.7 *[43] Seja* Θ *um grupo transitivo sobre* $\mathbb{S}$ *em um espaço métrico* $(\mathbb{M}, d)$, *ou seja,* $\mathbb{S}$ *é a órbita de um dado ponto sob* Θ. *Então* $\mathbb{S}$ *está casado a* Θ *e, para todo* $s \in \mathbb{S}$, *a transformação*

$$\mu_{\mathbb{S}} : \Theta \to \mathbb{S};\ \mu_{\mathbb{S}}(f) = f(s)$$

é uma transformação casada.

Reciprocamente, se o conjunto de sinais $\mathbb{S}$ *está casado a um grupo* $\mathbb{G}$*, então existe um homomorfismo de* $\mathbb{G}$ *sobre um subgrupo transitivo de* $\Gamma(\mathbb{S})$.

Demonstração: *Como* Θ *é um grupo transitivo,* $\mu_{\mathbb{S}}$ *é sobrejetor. Além disso,*

$$\forall f, f' \in \Theta, \quad d(\mu_{\mathbb{S}}(f), \mu_{\mathbb{S}}(f')) = d(f(s), f'(s)) = d(f^{-1} \circ f(s), f^{-1} \circ f'(s)) =$$
$$= d(s, f^{-1} \circ f'(s)) = d(\mu_{\mathbb{S}}(e_\Theta), \mu_{\mathbb{S}}(f^{-1} \circ f')).$$

Reciprocamente, seja $\Theta = \{f_h; h \in \mathbb{G}\} \subset \Gamma(\mathbb{S})$. *Temos então*

$$f_{h*h'}(s) = f_h(f_{h'}(s)) = (f_h \circ f_{h'})(s)$$

e, portanto, $h \longrightarrow f_h$ *é um homomorfismo de* $\mathbb{G}$ *sobre* Θ. *Logo,* Θ *é um grupo. Falta mostrar que* Θ *é transitivo. De fato, seja* $e_{\mathbb{G}}$ *a unidade de* $\mathbb{G}$ *e* $s = \mu(e_{\mathbb{G}})$. *Então,* $f_h(s) = s'$ *e, portanto,* $\Theta(s) = \mathbb{S}$.□

O próximo corolário desempenha um papel importante no estabelecimento da extensão da $\mathbb{Z}_4$-linearidade.

Corolário 2.4.2 *Se um conjunto de sinais* $\mathbb{S}$ *está efetivamente casado a um grupo* $\mathbb{G}$*, então* $\mathbb{G}$ *é isomorfo a um subgrupo transitivo de* $\Gamma(\mathbb{S})$.

Exemplo 2.4.7 *A recíproca do Corolário 2.4.2 nem sempre é verdadeira. O conjunto M-PSK possui* $\mathbb{D}_M$ *como grupo de simetrias, ou seja, o grupo diedral com* $2M$ *elementos. Este grupo é transitivo em* $\mathbb{S}$. *O subgrupo das rotações em* $\mathbb{D}_M$*, que é isomorfo a* $\mathbb{Z}_M$*, é também transitivo em* $\mathbb{S}$. *Se* M *é par,* $\mathbb{D}_{M/2}$ *é um outro subgrupo de* $\mathbb{D}_M$ *que é transitivo em* $\mathbb{S}$. *Portanto, pelo Corolário 2.4.2 o conjunto de sinais M-PSK é efetivamente casado a grupos que são isomorfos a* $\mathbb{Z}_M$ *ou* $\mathbb{D}_{M/2}$ *(M par). É claro que o M-PSK está casado ao grupo de simetrias* $\mathbb{D}_M$*, porém este casamento não é efetivo.*

2.4.3 Códigos geometricamente uniformes

Forney [27] generalizou os códigos de grupo de Slepian e códigos reticulado permitindo que os elementos do grupo gerador sejam isometrias arbitrárias do espaço euclidiano $\mathbb{R}^n$, ao invés de

transformações ortogonais ou translações consideradas de forma separada. Tais códigos foram denominados **códigos geometricamente uniformes** apresentando propriedades simétricas altamente desejáveis tais como: todas as regiões de Voronoi são congruentes; o perfil de distâncias é o mesmo para qualquer palavra-código; as palavras-código possuem a mesma probabilidade de erro; e o grupo gerador é isomorfo a um grupo de permutações transitivo sobre as palavras-código. As definições e resultados aqui apresentados estão em [27] e quando possível foram adaptados para espaços métricos quaisquer.

Definição 2.4.7 *[27]Seja* $\mathbb{S}$ *um conjunto de sinais em um espaço métrico* $(\mathbb{M}, d)$. *Dizemos que* $\mathbb{S}$ *é um* ***código geometricamente uniforme*** *se para quaisquer* $s_1, s_2 \in \mathbb{S}$, *existe uma isometria* μ_{s_1,s_2} *tal que:*

$$\mu_{s_1,s_2}(s_1) = s_2, \quad \mu_{s_1,s_2}(\mathbb{S}) = \mathbb{S}. \tag{2.2}$$

Em outras palavras, a ação do grupo de simetrias, $\Gamma(\mathbb{S})$, de $\mathbb{S}$ é transitiva. Se $\mathbb{S}$ for finito, dizemos que $\mathbb{S}$ é uma **constelação uniforme** e se $\mathbb{S}$ for infinito dizemos que $\mathbb{S}$ é um **arranjo regular**. Observe que uma constelação uniforme no espaço euclidiano é um código de grupo (código de Slepian).

Em geral, o grupo de simetrias de um conjunto de sinais geometricamente uniforme possui mais elementos do que o necessário para gerá-lo. Para isto, consideraremos a seguinte definição

Definição 2.4.8 *[27]Seja* $\mathbb{S}$ *um código geometricamente uniforme. Um* ***grupo gerador mínimo*** $U(\mathbb{S})$ ***de*** $\mathbb{S}$, *é um subgrupo do grupo de simetrias de* $\mathbb{S}$ *que satisfaz*

$$\forall s_0 \in \mathbb{S},\ \mathbb{S} = \{\mu(s_0),\ \mu \in U(\mathbb{S})\},$$

e a função $m : U(\mathbb{S}) \longrightarrow \mathbb{S}$, *dada por* $m(\mu) = \mu(s_0)$ *é injetora.*

Exemplo 2.4.8 *O espaço de Hamming* $\mathbb{Z}_2^2$ *é um código geometricamente uniforme e seu grupo de simetrias é dado pelo produto semi-direto*

$$\mathbb{Z}_2^2 \times_\varphi \mathbb{Z}_2.$$

Este grupo é isomorfo a $\mathbb{D}_4$, o grupo das simetrias do quadrado. Dois grupos geradores mínimos de $\mathbb{Z}_2^2$ são:

$$\{e, r, r^2, r^3\} \cong \mathbb{Z}_4 \qquad e \qquad \{e, r^2, rs, r^3 s\} \cong \mathbb{Z}_2^2.$$

Um conjunto de sinais não precisa possuir um grupo gerador mínimo ([56]). Por outro lado, existem conjuntos de sinais que possuem mais do que dois grupos geradores mínimos.

Exemplo 2.4.9 *A constelação de sinais M-PSK é um código geometricamente uniforme. De fato, seu grupo de simetrias é $\mathbb{D}_M$ e um grupo gerador natural é o subgrupo das rotações R_M que é isomorfo a $\mathbb{Z}_M$.*

Exemplo 2.4.10 *O conjunto de sinais do tipo* ***reticulado,*** *dado por*

$$\mathbb{S} = \mathbb{Z}^2 + (\frac{1}{2}, \frac{1}{2}),$$

possui $T(\mathbb{Z}^2)$ como seu grupo gerador, o conjunto de todas as translações por inteiros em cada coordenada. O grupo de simetrias de $\mathbb{S}$, $\Gamma(\mathbb{S})$, não inclui somente $T(\mathbb{Z}^2)$, mas também o $\mathbb{D}_4$. Na verdade, $\Gamma(\mathbb{S})$ é o conjunto de todas as composições dos elementos de $\mathbb{D}_4$ com os elementos de $T(\mathbb{Z}^2)$, ou seja,

$$\Gamma(\mathbb{S}) = T(\mathbb{Z}^2) \times_\varphi \mathbb{D}_4.$$

Como $T(\mathbb{Z}^2)$ é normal em $\Gamma(\mathbb{S})$ e sua interseção com $\mathbb{D}_4$ é o elemento neutro, temos que $\Gamma(\mathbb{S})$ é o produto semi-direto de $T(\mathbb{Z}^2)$ com $\mathbb{D}_4$. Os outros dois grupos geradores, com ponto inicial $(\frac{1}{2}, \frac{1}{2})$ são:

- *O grupo $R_4 \circ T(2\mathbb{Z}^2)$, rotações compostas com translações de ordem par;*
- *O grupo $Re^2 \circ T(2\mathbb{Z}^2)$, reflexões compostas com translações de ordem par.*

Teorema 2.4.8 *[27]O produto cartesiano de conjuntos de sinais geometricamente uniformes é um conjunto de sinais geometricamente uniforme.*

Um subgrupo normal U' de um grupo gerador mínimo $U(\mathbb{S})$ induz uma partição de um conjunto de sinais geometricamente uniforme $\mathbb{S}$ em subconjuntos geometricamente uniformes.

Definição 2.4.9 *[27]Seja $\mathbb{S}$ um conjunto de sinais geometricamente uniforme com grupo gerador mínimo $U(\mathbb{S})$. Uma* ***partição geometricamente uniforme*** *$\mathbb{S}/\mathbb{S}'$, é uma partição de $\mathbb{S}$, induzida por um subgrupo normal $\mathbb{U}'$ de $\mathbb{U}(\mathbb{S})$. Os elementos de $\mathbb{S}/\mathbb{S}'$ são os subconjuntos de $\mathbb{S}$ que correspondem às classes laterais de $\mathbb{U}'$ em $\mathbb{U}(\mathbb{S})$.*

Exemplo 2.4.11 *Com respeito ao Exemplo 2.4.8, sejam $\mathbb{U}(\mathbb{S})$ e $\mathbb{U}'(\mathbb{S})$ dados por*

$$\mathbb{U}(\mathbb{S}) = \{e, r, r^2, r^3\} \quad e \quad \mathbb{U}'(\mathbb{S}) = \{e\}.$$

Então $\mathbb{S}/\mathbb{S}' = \{00, 10, 11, 01\}$.

Exemplo 2.4.12 *Se M' é um divisor de M, um conjunto de sinais M-PSK pode ser particionado em $|R_M/R_{M'}| = \frac{M}{M'}$ M'-PSK conjuntos de sinais pelo subgrupo $R_{M'}$ de seu grupo de rotações R_M.*

O grupo quociente $R_M/R_{M'}$ é isomorfo a $\mathbb{Z}_{\frac{M}{M'}}$. Quando M e M' são potências de 2, obtém-se as partições do tipo utilizada por Ungerboeck [59] para códigos de treliça do tipo PSK.

Definição 2.4.10 *[27] Sejam $\mathbb{S}/\mathbb{S}'$ uma partição geometricamente uniforme e $\mathbb{G}$ um grupo isomorfo a $\mathbb{U}(\mathbb{S})/\mathbb{U}'(\mathbb{S})$. Um* ***rotulamento isométrico*** *é uma função injetora $\mathbf{m} : \mathbb{G} \to \mathbb{S}/\mathbb{S}'$ dada pela composição do isomorfismo entre $\mathbb{G}$ e $\mathbb{U}(\mathbb{S})/\mathbb{U}'(\mathbb{S})$ e a função injetora induzida por $\mathbf{m}$ de $\mathbb{U}(\mathbb{S})/\mathbb{U}'(\mathbb{S})$ em $\mathbb{S}/\mathbb{S}'$.*

O grupo $\mathbb{G}$ é denominado **grupo de rótulos**. No Exemplo 2.4.11, temos que $\mathbb{U}(\mathbb{S})/\mathbb{U}'(\mathbb{S})$ é isomorfo a $\mathbb{Z}_4$. Este isomorfismo nos leva ao rotulamento isométrico dos elementos de $\mathbb{Z}_2^2$, apresentado na Tabela 2.2, sob a métrica de Hamming e dos elementos de $\mathbb{Z}_4$ sob a métrica de Lee.

2.4.4 Propriedades de simetria

Definição 2.4.11 *[27] Seja $\mathbb{S}$ um conjunto de sinais geometricamente uniforme em um espaço métrico $(\mathbb{M}, d)$. A região de Voronoi associada a um ponto $s \in \mathbb{S}$, denotada por $\mathcal{V}(\mathbb{S})$, é o conjunto*

$$\mathcal{V}_{\mathbb{S}}(s) = \{x \in \mathbb{M} \quad | \, d(x, s) = \min_{s' \in \mathbb{S}} d(x, s')\}.$$

00	$\rightarrow$	0
10	$\rightarrow$	1
11	$\rightarrow$	2
01	$\rightarrow$	3

Tabela 2.2: Tabela do Rotulamento Isométrico

Definição 2.4.12 *[27] Seja $\mathbb{S}$ um conjunto de sinais geometricamente uniforme em um espaço métrico $(\mathbb{M}, d)$. O perfil de distância global associado a um ponto $s \in \mathbb{S}$, denotado por $\mathcal{DP}_{\mathbb{S}}(s)$, é o conjunto*

$$\mathcal{DP}_{\mathbb{S}}(s) = \{d(s, s'); s' \in \mathbb{S}\}.$$

Exemplo 2.4.13 *Seja $\mathbb{S} = \mathbb{Z}^2 + (\frac{1}{2}, \frac{1}{2})$. A Fig. 2.8 mostra a região de Voronoi $\mathcal{V}_{\mathbb{S}}(\frac{1}{2}, \frac{1}{2})$:*

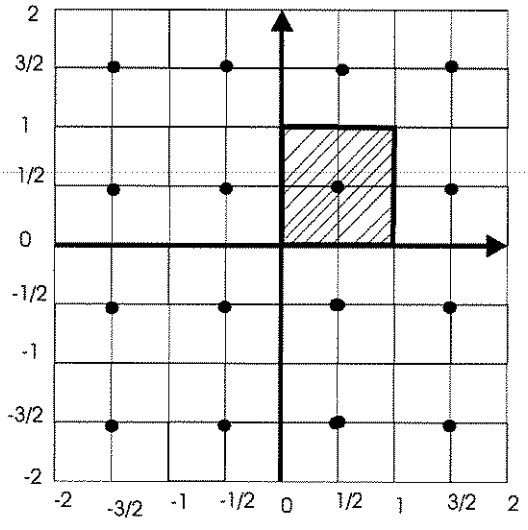

Figura 2.8: Região de Voronoi $\mathcal{V}_{\mathbb{S}}(\frac{1}{2}, \frac{1}{2})$ em $\mathbb{S} = \mathbb{Z}^2 + (\frac{1}{2}, \frac{1}{2})$.

Teorema 2.4.9 *[27] Se $\mathbb{S}$ é um conjunto de sinais geometricamente uniforme, então:*

- *Todas as regiões de Voronoi possuem a mesma forma, ou seja,*

$$s, s' \in \mathbb{S} \Rightarrow \mathcal{V}_{\mathbb{S}}(s') = f(\mathcal{V}_{\mathbb{S}}(s)),$$

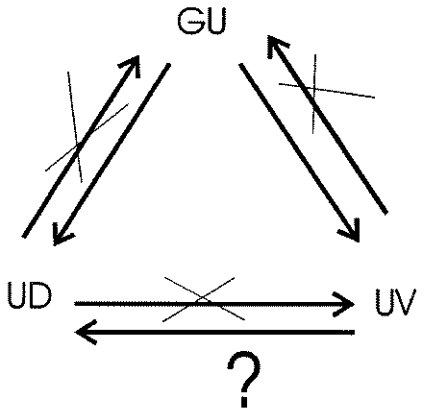

Figura 2.9: GU: Geometricamente uniforme, UD: O perfil de distâncias independe do ponto considerado, UV: As regiões de Voronoi possuem a mesma forma.

onde f é uma isometria;

- *O perfil de distâncias global é o mesmo para todo $s \in \mathbb{S}$.*

Este teorema fornece uma propriedade simétrica muito forte porque o formato das regiões de Voronoi de um conjunto de sinais $\mathbb{S}$ determina quase todas as propriedades de $\mathbb{S}$ que são importantes no estabelecimento do sistema de comunicações.

A recíproca deste teorema não é verdadeira. Em [9], é mostrado que conjunto de sinais, cujas regiões de Voronoi tenham a mesma forma não implica que o mesmo seja geometricamente uniforme. Em [56], é mostrado que se um conjunto de sinais apresenta o mesmo perfil de distâncias, independente do ponto considerado, isto não implica que o mesmo seja geometricamente uniforme.

É mostrado também em [9] que no conjunto de sinais o perfil de distâncias ser independente do ponto considerado não implica que as regiões de Voronoi possuam a mesma forma. Entretanto, a validade ou não da recíproca não é conhecida.

2.4.5 Métrica de grupo

Seja $(\mathbb{G}, d, *)$ um espaço métrico com a operação de grupo '$*$' em $\mathbb{G}$. Como existem duas estruturas distintas em $\mathbb{G}$ é importante que se estabeleça uma propriedade que relacione estas duas estruturas. Para saber que propriedade é adequada, vejamos um exemplo de medida: a distância de Hamming em $\mathbb{Z}_2^n$ é dada por

$$d_H(x,y) = \sum_{i=1}^{n} \delta(x_i, y_i)$$

onde

$$\delta(x_i, y_i) = \begin{cases} 1 & se\ x_i \neq y_i \\ 0 & c.c. \end{cases}$$

Agora, δ pode ser escrita da seguinte maneira

$$\begin{aligned} \delta(x_i, y_i) &= \begin{cases} 1 & se\ x_i - y_i \neq 0 \\ 0 & c.c. \end{cases} = \\ &= \delta(x_i - y_i, 0). \end{aligned}$$

Logo,

$$\begin{aligned} d_H(x,y) &= \sum_{i=1}^{n} \delta(x_i, y_i) = \sum_{i=1}^{n} \delta(x_i - y_i, 0) = \\ &= d_H(x - y, \underline{0}). \end{aligned}$$

Esta é a propriedade desejada e será formalizada na seguinte definição.

Definição 2.4.13 *Seja $(\mathbb{G}, *)$ um grupo, dizemos que uma função $d : \mathbb{G} \times \mathbb{G} \to \mathbb{R}$ é compatível com a operaçãp do grupo $\mathbb{G}$ se*

$$d(x,y) = d(x * y^{-1}, e_{\mathbb{G}}).$$

Se, além disso, d é uma métrica em $\mathbb{G}$ (portanto, um espaço métrico $(\mathbb{G}, d)$) diremos que d é uma métrica de grupo.

Exemplo 2.4.14 *A função $d' : \mathbb{G}^n \times \mathbb{G}^n \to \mathbb{R}$ dada por*

$$d'(x,y) = \sum_{i=1}^{n} d(x_i, y_i),$$

onde $d : \mathbb{G} \times \mathbb{G} \to \mathbb{R}$ possui a propriedade de grupo, também possui a propriedade de grupo.

Exemplo 2.4.15 *A distância euclidiana d_e é uma métrica de grupo. A distância euclidiana quadrática d_E possui a propriedade de grupo mas não é uma métrica de grupo.*

Em um espaço métrico $(\mathbb{G}, d)$, se d é uma métrica de grupo, então

$$\begin{aligned} \mathcal{DP}_{\mathbb{G}}(g) &= \{d(g', g); g' \in \mathbb{G}\} = \{d(g' * g^{-1}, e_{\mathbb{G}}); g' \in \mathbb{G}\} = \\ &= \{d(g', e_{\mathbb{G}}); g' \in \mathbb{G}\}, \end{aligned}$$

ou seja, o perfil de distâncias global é independente do ponto considerado.

2.5 Conclusão

Neste capítulo apresentamos os principais conceitos que serão utilizados neste trabalho, a saber: grupos, espaços métricos e códigos.

A estrutura algébrica utilizada no estabelecimento da extensão da $\mathbb{Z}_4$-linearidade é a de grupos, onde $\mathbb{Z}_4$ é considerado como um caso particular.

À estrutura algébrica de grupos, associaremos uma métrica adequada, conduzindo desse modo a um espaço métrico assim como foi considerada a métrica de Hamming associada à $\mathbb{Z}_2^2$.

Uma das condições a ser satisfeita quando da extensão é a de propriedade de grupo no espaço métrico do código de grupo. A outra condição é a de isometria entre os espaços métricos considerados. Estas duas condições implicam no casamento entre os códigos considerados que, por sua vez, implica na uniformidade geométrica do código imagem.

Capítulo 3

$\mathbb{Z}_{2^k}$-Linearidade

3.1 Introdução

A $\mathbb{Z}_4$-linearidade é um conceito inovador e importante em teoria da codificação porque possibilita que certas classes de códigos binários não-lineares de comprimento par possam ser vistos como códigos lineares sobre $\mathbb{Z}_4$. Obtém-se, com isso, uma redução significativa na complexidade do processo de decodificação dos códigos não-lineares.

Diante deste fato, a $\mathbb{Z}_4$-linearidade surgiu como uma nova linha de pesquisa em Teoria da Codificação dada a sua eficácia como técnica de construção de códigos binários de comprimento par, em geral, não lineares. É interessante, então, responder a seguinte questão: É possível estender esta técnica de construção para códigos binários de outros comprimentos?

A análise desta questão nos leva a estabelecer a definição da $\mathbb{Z}_{2^k}$-linearidade, e com isso possibilitar que códigos binários de comprimento múltiplo de k possam ser construídos.

Tendo como motivação este fato, iremos estabelecer neste capítulo o conceito da $\mathbb{Z}_{2^k}$-linearidade. Para isso, organizaremos este capítulo da seguinte forma.

Na Seção 3.2 apresentaremos a definição da $\mathbb{Z}_4$-linearidade e suas principais propriedades, além de uma caracterização. Através do algoritmo de otimização combinatorial proposto por Said e Palazzo [50], apresentamos tabelas de códigos $\mathbb{Z}_4$-lineares de comprimento par menor ou igual a 20. Através de um algoritmo computacional exaustivo, apresentamos tabelas de códigos

$\mathbb{Z}_4$-lineares de comprimento par menor ou igual a 20 mapeados por códigos de grupo cíclicos quaternários. Na Seção 3.3 serão analisadas as possíveis considerações da $\mathbb{Z}_{2^k}$-linearidade, culminando com a definição da $\mathbb{Z}_{2^k}$-linearidade e das condições essenciais para a utilização como técnica de construção de códigos. Na Seção 3.4, sob a condição da existência de um subgrupo cíclico transitivo em $\Gamma(\mathbb{Z}_2^k)$ de ordem 2^k, mostramos que não existem códigos $\mathbb{Z}_{2^k}$-lineares. Finalmente, na Seção 3.5 apresentamos as conclusões.

3.2 $\mathbb{Z}_4$-Linearidade: Definição, Propriedades e Exemplos

Apresentaremos nesta seção os principais conceitos e resultados relacionados com a $\mathbb{Z}_4$-linearidade. Estes resultados servirão de base para o estabelecimento de extensões para alfabetos 2^k-ários, $k \geq 3$, possibilitando dessa forma construir códigos binários com comprimentos múltiplos de k.

Definição 3.2.1 *[15] Um* ***mapeamento*** *é uma função*

$$\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n},$$

definida por

$$\phi(\underline{c}) = (\beta(\underline{c}), \gamma(\underline{c})) = (\beta(c_1), \beta(c_2), \ldots, \beta(c_n), \gamma(c_1), \gamma(c_2), \ldots, \gamma(c_n)), \forall \underline{c} = (c_1, \ldots, c_n) \in \mathbb{Z}_4^n;$$

onde as funções $\beta : \mathbb{Z}_4 \to \mathbb{Z}_2$ *e* $\gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ *são especificadas na Tabela 3.1.*

c	$\beta(c)$	$\gamma(c)$
0	0	0
1	0	1
2	1	1
3	1	0

Tabela 3.1: Definição das funções β *e* γ.

Lema 3.2.1 *Se* $\alpha : \mathbb{Z}_4 \to \mathbb{Z}_2$ *é dada por* $\alpha(c) = c \bmod 2$, *então as funções* α, β *e* γ *satisfazem as seguintes propriedades:*

1. $c = \alpha(c) + 2\beta(c)$, *ou seja,* α *e* β *são os dígitos binários na expansão binária de* $c \in \mathbb{Z}_4$.

2. $\alpha(c) + \beta(c) + \gamma(c) = 0, \forall c \in \mathbb{Z}_4$.

3. $\phi(-c) = (\gamma(c), \beta(c)), \forall c \in \mathbb{Z}_4$.

4. *O conjunto* $\{(\beta(c), \gamma(c)); c \in \mathbb{Z}_4\}$ *forma um código de Gray, ou seja, a distância entre os vizinhos é* 1.

5. *O conjunto* $\{(\alpha(c), \beta(c), \gamma(c)); c \in \mathbb{Z}_4\}$ *forma o* $(3, 2, 2)$*-código verificação de paridade.*

6. *Para todo* $\underline{a} \in \mathbb{Z}_2^n$, $\underline{b} \in \mathbb{Z}_4^n$ *tem-se*

$$\phi(2\underline{a} + \underline{b}) = \phi(2) + \phi(\underline{b}).$$

Demonstração: *Segue diretamente das definições das funções* α, β *e* γ.□

O teorema a seguir estabelece a propriedade mais relevente do mapeamento ϕ. É esta propriedade que determina a $\mathbb{Z}_4$-linearidade.

Teorema 3.2.1 *[15]O mapeamento* ϕ *é uma isometria de* $(\mathbb{Z}_4^n, d_L)$ *em* $(\mathbb{Z}_2^{2n}, d_H)$.

O rótulo apresentado na Tabela 3.1 é único, a menos de uma troca de coordenadas e que determina a isometria entre os espaços $(\mathbb{Z}_4^n, d_L)$ e $(\mathbb{Z}_2^{2n}, d_H)$. De fato, o elemento 2 em $\mathbb{Z}_4$ possui peso de Lee 2 e o único elemento em $\mathbb{Z}_2^2$ com peso de Hamming 2 é o elemento 11.

Se um código binário de comprimento par é a imagem de um código de grupo quaternário através do mapeamento ϕ, nada garante que um código binário equivalente também o seja. De fato, considere o código quaternário

$$\{(000), (012), (020), (032)\},$$

Sua imagem através do mapeamento ϕ é o código binário

$$\mathbb{C} = \{(000000), (001011), (010010), (011001)\}$$

Porém, o código equivalente

$$\mathbb{C}' = \{(000000), (000111), (010010), (010101)\},$$

não é imagem de um código de grupo quaternário, pois

$$\phi^{-1}(\mathbb{C}') = \{(000), (111), (020), (131)\}$$

não é um código de grupo quaternário.

Desta forma, vemos que a definição de $\mathbb{Z}_4$-linearidade deve incluir os códigos equivalentes. Com isso temos:

Definição 3.2.2 *[15]Um código $\mathbb{C} \subset \mathbb{Z}_2^{2n}$ é $\mathbb{Z}_4$-**linear** se ele ou seu equivalente for imagem de um código de grupo sobre $\mathbb{Z}_4$ de comprimento n através do mapeamento ϕ.*

A imagem do código de grupo quaternário através do mapeamento ϕ possui as seguintes propriedades:

- O comprimento do código binário é o dobro do código quaternário;
- A dimensão do código binário é dobro da dimensão do código quaternário;
- A taxa do código binário é a mesma que a do código quaternário;
- Em valor numérico a distância mínima de Hamming no código binário é igual à distância mínima de Lee no código quaternário

Um aspecto importante destas propriedades é que através da procura de códigos de grupo quaternários podemos encontrar códigos binários, não necessariamente lineares, com parâmetros possivelmente melhores do que os conhecidos e com características muito próximas do que os lineares possuem.

A seguir iremos estabelecer algumas condições para que um código $\mathbb{C}$ seja $\mathbb{Z}_4$-linear.

Definição 3.2.3 *A **função troca** do produto cartesiano A^{2n} de um conjunto A é uma função definida por:*

$$\sigma : A^{2n} \to A^{2n}; \quad \sigma(a_1, a_2, \ldots, a_n, a_{n+1}, a_{n+2}, \ldots, a_{2n}) = (a_{n+1}, \ldots, a_{2n}, a_1, \ldots, a_n).$$

Observe que a função σ é uma permutação da forma:

$$(1, n+1)(2, n+2)\ldots(n, 2n).$$

A função troca possui algumas propriedades relevantes para o estudo da $\mathbb{Z}_4$-linearidade:

Lema 3.2.2 *1.* $\sigma(\sigma(a)) = a, \forall a \in A^{2n}$;

2. Se '$*$' é uma operação binária em A^{2n} então:

$$\sigma(a * b) = \sigma(a) * \sigma(b).$$

Por indução, isto também é válido para um número finito de termos.

3. Definindo

$$v_l = (b_l(0), b_l(1), \ldots, b_l(2^m - 1)),\ m \in \mathbb{N},\ l = 1, 2, \ldots, m,$$

onde $b_l(j)$ são os algarismos da representação binária de j, ou seja,

$$j = \sum_{l=1}^{m} b_l(j).2^{m-l}.$$

temos

- $\sigma(v_l) = \begin{cases} v_l & l > 1 \\ (1, 1, \ldots, 1) + v_l & l = 1 \end{cases}$
- $\sigma(v_l^i) = (\sigma(v_l))^i$.

Agora, iremos mostrar duas propriedades importantes do mapeamento ϕ:

Lema 3.2.3 *[15]Para todo $a, b \in \mathbb{Z}_4^n$ tem-se*

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

2. $\phi(a) + \phi(b) + \phi(a + b) = \phi(2\alpha(a) * \alpha(b))$.

Demonstração:

1. Devemos mostrar que

(a) $\beta(a_i + b_i) = \beta(a_i) + \beta(b_i) + [\beta(a_i) + \gamma(a_i)].[\beta(b_i) + \gamma(b_i)]$;

(b) $\gamma(a_i + b_i) = \gamma(a_i) + \gamma(b_i) + [\beta(a_i) + \gamma(a_i)].[\beta(b_i) + \gamma(b_i)]$.

A verificação de (a) é realizada através do teste de todos os 16 possíveis valores. Para o caso (b) temos:

$$\begin{aligned}\gamma(a_i + b_i) &= \alpha(a_i + b_i) + \beta(a_i + b_i) = \alpha(a_i) + \alpha(b_i) + \\ &+\beta(a_i) + \beta(b_i) + [\beta(a_i) + \gamma(a_i)].[\beta(b_i) + \gamma(b_i)] \\ &= \gamma(a_i) + \gamma(b_i) + [\beta(a_i) + \gamma(a_i)].[\beta(b_i) + \gamma(b_i)].\end{aligned}$$

2. *Devemos mostrar que*

(a) $\beta(2\alpha(a_i)\alpha(b_i)) = \beta(a_i) + \beta(b_i) + \beta(a_i + b_i)$;

(b) $\gamma(2\alpha(a_i)\alpha(b_i)) = \gamma(a_i) + \gamma(b_i) + \gamma(a_i + b_i)$.

A verificação dos casos 2(a) e (b) é realizada através da verificação dos 16 casos possíveis.□

Teorema 3.2.2 *[15] Um código binário* $\mathbb{C}$ *de comprimento par é* $\mathbb{Z}_4$*-linear se, e somente se, suas coordenadas podem ser permutadas de tal modo que*

$$\forall u, v \in \mathbb{C} \Rightarrow u + v + (u + \sigma(u)) * (v + \sigma(v)) \in \mathbb{C}$$

Demonstração: *Se* $\mathbb{C}$ *é* $\mathbb{Z}_4$*-linear, então existe um código de grupo quaternário* $\overline{\mathbb{C}}$ *tal que*

$$\mathbb{C}' = \phi(\overline{\mathbb{C}}),$$

para algum código $\mathbb{C}'$ *equivalente a* $\mathbb{C}$*. Assim, temos*

$$u, v \in \mathbb{C}' \Rightarrow u = \phi(a), v = \phi(b), a, b \in \overline{\mathbb{C}}.$$

Pelo Lema 3.2.3, temos

$$u + v + (u + \sigma(u)) * (v + \sigma(v)) = \phi(a + b) \in \mathbb{C}'.$$

Reciprocamente, seja $\overline{\mathbb{C}} = \phi^{-1}(\mathbb{C}')$, *onde* $\mathbb{C}'$ *é equivalente a* $\mathbb{C}$. *Então* $\overline{\mathbb{C}}$ *é um código de grupo quaternário. De fato,*

$$a, b \in \overline{\mathbb{C}} \Rightarrow \phi(a) = u, \phi(b) = v,\ u,\ v \in \mathbb{C}'$$

$$\Rightarrow \phi(a+b) = \phi(a) + \phi(b) + (\phi(a) + \sigma(\phi(a))) * (\phi(b) + \sigma(\phi(b))) =$$
$$= u + v + (u + \sigma(u)) * (v + \sigma(v)) \in \mathbb{C}'.$$

Logo, $a + b \in \overline{\mathbb{C}}$ *e, portanto,* $\overline{\mathbb{C}}$ *é linear.* □

Corolário 3.2.1 *[15] Um código binário linear* $\mathbb{C}$ *de comprimento par é* $\mathbb{Z}_4$*-linear se, e somente se, suas coordenadas podem ser permutadas de tal forma que*

$$u, v \in \mathbb{C} \Rightarrow (u + \sigma(u)) * (v + \sigma(v)) \in \mathbb{C}. \tag{3.1}$$

Demonstração: *Consequência direta do teorema anterior.*□

Teorema 3.2.3 *[15] Um código binário* $\mathbb{C} = \phi(\overline{\mathbb{C}})$, *imagem de um código de grupo quaternário* $\overline{\mathbb{C}}$, *é linear se, e somente se,*

$$a, b \in \overline{\mathbb{C}} \Rightarrow 2.\alpha(a) * \alpha(b) \in \overline{\mathbb{C}}.$$

Demonstração: *Sejam* $a, b \in \mathbb{C}$; *então, pelo Lema 3.2.3 temos*

$$\phi(2\alpha(a) * \alpha(b)) = \phi(a) + \phi(b) + \phi(a+b),$$

que pertence a $\phi(\overline{\mathbb{C}})$, *pois* $\phi(\overline{\mathbb{C}})$ *é linear, por hipótese. Logo,* $2\alpha(a)\alpha(b) \in \overline{\mathbb{C}}$

Reciprocamente, sejam $u, v \in \phi(\overline{\mathbb{C}})$, *então,*

$$u = \phi(a), v = \phi(b),\ com\ a, b \in \overline{\mathbb{C}}.$$

Disto segue que

$$u + v = \phi(a) + \phi(b) = \phi(a+b) + \phi(2\alpha(a) * \alpha(b)) = \phi(a + b + 2\alpha(a) * \alpha(b)) \in \phi(\overline{\mathbb{C}})$$

(a última igualdade foi obtida através da Propriedade 6 do Lema 3.2.1).□

Observamos que as condições acima são bastante restritivas, o que faz crer que muitos códigos binários não são $\mathbb{Z}_4$-lineares.

Exemplo 3.2.1 *O $(2n, 1, 2n)$-código de repetição de comprimento par $R(2n)$ é $\mathbb{Z}_4$-linear pois*

$$(u + \sigma(u)) = \mathbf{0}_{2n}, \ \forall u \in R(2n).$$

O código de grupo sobre $\mathbb{Z}_4$ é o sub-código do código de repetição $(n, 1, 2n)$ formado pelas palavras-código $(0, 0, 0, \ldots, 0)$ e $(2, 2, 2, \ldots, 2)$.

Exemplo 3.2.2 *O $(2n, 2n-1, 2)$-código verificação de paridade par $P(2n)$ também é $\mathbb{Z}_4$-linear pois*

- *Se u tem peso par, então $\phi(u)$ tem peso par;*
- *Se a e b têm peso par, então $(a + b)$ tem peso par.*

  Como todo elemento neste código tem peso par, a imagem inversa pelo mapeamento ϕ terá peso par. Teremos $\# \ \phi^{-1}(P(2n)) = 2^{2n-1} = \frac{4^n}{2}$. Esta imagem inversa constitui-se de todas as palavras-código do código universal sobre $\mathbb{Z}_4$, $U(n)$, que possuem peso par e formam um código de grupo.

Teorema 3.2.4 *[15] Os códigos Reed-Muller $RM(r, m)$ de comprimento $n = 2^m$, $m \geq 1$ são $\mathbb{Z}_4$-lineares para os seguintes parâmetros:*

$$r = 0, 1, 2, m-1, m.$$

Demonstração: *Como o código binário é linear, utilizaremos o Corolário 3.2.1 para mostrar que o código Reed-Muller $RM(r, m)$, $m \geq 1$, $r = 0, 1, 2, m-1, m$, satisfaz a relação (3.1). De fato, sejam $u, v \in RM(r, m)$. Então*

$$u = \sum_{i=(i_1, i_2, \ldots, i_m) \in \mathbb{Z}_2^m, \ w_H(i) \leq r} a_i . v_1^{i_1} . v_2^{i_2} \ldots v_m^{i_m},$$

e

$$v = \sum_{j=(j_1, j_2, \ldots, j_m) \in \mathbb{Z}_2^m, \ w_H(j) \leq r} b_j . v_1^{j_1} . v_2^{j_2} \ldots v_m^{j_m}.$$

Disto temos

$$\sigma(u) = \sum_{i=(i_1,i_2,\ldots,i_m)\in\mathbb{Z}_2^m,\ w_H(i)\leq r} a_i.[\sigma(v_1)]^{i_1}.[\sigma(v_2)]^{i_2}\ldots[\sigma(v_m)]^{i_m} =$$

$$= \sum_{i=(i_1,i_2,\ldots,i_m)\in\mathbb{Z}_2^m,\ w_H(i)\leq r} a_i.(1+v_1)^{i_1}.v_2^{i_2}\ldots v_m^{i_m};$$

$$\sigma(v) = \sum_{j=(j_1,j_2,\ldots,j_m)\in\mathbb{Z}_2^m,\ w_H(j)\leq r} b_j.[\sigma(v_1)]^{j_1}.[\sigma(v_2)]^{j_2}\ldots[\sigma(v_m)]^{j_m} =$$

$$= \sum_{j=(j_1,j_2,\ldots,j_m)\in\mathbb{Z}_2^m,\ w_H(j)\leq r} b_j.(1+v_1)^{j_1}.v_2^{j_2}\ldots v_m^{j_m}.$$

Desenvolvendo $\sigma(u)$ e $\sigma(v)$, obtemos:

$$\sigma(u) = \sum_{i=(0,i_2,\ldots,i_m)\in\mathbb{Z}_2^m,\ w_H(i)\leq r} a_i.v_2^{i_2}\ldots v_m^{i_m} + \sum_{i=(1,i_2,\ldots,i_m)\in\mathbb{Z}_2^m,\ w_H(i)\leq r} a_i.(1+v_1).v_2^{i_2}\ldots v_m^{i_m} =$$

$$= u + \sum_{i=(1,i_2,\ldots,i_m)\in\mathbb{Z}_2^m,\ w_H(i)\leq r} a_i.v_2^{i_2}\ldots v_m^{i_m};$$

e

$$\sigma(v) = \sum_{j=(0,j_2,\ldots,j_m)\in\mathbb{Z}_2^m,\ w_H(j)\leq r} b_j.v_2^{j_2}\ldots v_m^{j_m} + \sum_{j=(1,j_2,\ldots,j_m)\in\mathbb{Z}_2^m,\ w_H(j)\leq r} b_j.(1+v_1).v_2^{j_2}\ldots v_m^{j_m} =$$

$$= v + \sum_{j=(1,j_2,\ldots,j_m)\in\mathbb{Z}_2^m,\ w_H(j)\leq r} b_j.v_2^{j_2}\ldots v_m^{j_m}.$$

Isto implica que

$$(u+\sigma(u)) * (v+\sigma(v)) =$$

$$= \Big(\sum_{i=(1,i_2,\ldots,i_m)\in\mathbb{Z}_2^m,\ w_H(i)\leq r} a_i.v_2^{i_2}\ldots v_m^{i_m}\Big) * \Big(\sum_{j=(1,j_2,\ldots,j_m)\in\mathbb{Z}_2^m,\ w_H(j)\leq r} b_j.v_2^{j_2}\ldots v_m^{j_m}\Big). \qquad (3.2)$$

No primeiro fator temos no máximo $(r-1)$ vetores distintos v_k. No segundo fator temos no máximo $(r-1)$ vetores distintos v_k. No produto temos no máximo $(2r-2)$ vetores distintos v_k. Assim, quando $r \leq 2$, temos

$$2r-2 \leq r.$$

Quando $r = m-1$ não ocorrerá m vetores distintos v_k pois v_i não pertence aos fatores. Quando $r = m$ fica trivialmente satisfeito. Nestes casos, temos então que

$$(u+\sigma(u)) * (v+\sigma(v)) \in RM(r,m).$$

□

Vemos da demonstração do Teorema 3.2.4 que o mesmo argumento é válido para mostrar que $RM(r,m)$, $m \geq 1$, $3 \leq r \leq m-2$, não é imagem de um código de grupo quaternário pelo mapeamento ϕ. Vejamos o contra-exemplo.

Contra-Exemplo 3.2.1 *Vamos mostrar agora que para $r = 3,4,5,...,m-2$, os códigos de Reed-Muller $RM(r,m)$ não são imagens de códigos de grupo quaternários. Para isso, considere*

$$u = v_1.v_2 \ldots v_r;$$

e

$$v = v_1.v_{r+1}.v_{r+2}.$$

Assim,

$$(u + \sigma(u)) * (v + \sigma(v)) = v_2v_3 \ldots v_r.v_{r+1}.v_{r+2} \notin RM(r,m).$$

Porém, devemos lembrar que este contra-exemplo não é suficiente para provar que o código $RM(r,m)$ não é $\mathbb{Z}_4$-linear, pois algum código equivalente poderia satisfazer esta condição. O teorema a seguir resolve a questão para $r = m-2$:

Teorema 3.2.5 *[15]O código $RM(m-2,m)$ binário, ou seja, o código de Hamming estendido de comprimento $n = 2^m$ não é $\mathbb{Z}_4$-linear para $m \geq 5$.*

Para os parâmetros restantes conjectura-se que também não sejam $\mathbb{Z}_4$-lineares.

Contra-Exemplo 3.2.2 (Código de Golay) *Vamos mostrar através de um contra-exemplo que o código de Golay estendido $(24,12,8)$ não é $\mathbb{Z}_4$-linear. Sejam*

$$u = (110000000000011011100010)$$

e

$$v = (101000000000001101110001)$$

as duas primeiras linhas da matriz geradora do código de Golay estendido. Assim,

$$(u + \sigma(u)) * (v + \sigma(v)) = (100001100000100001100000),$$

possui peso de Hamming 6 e, portanto, não pertence ao Código de Golay estendido. Observe que um rearranjo das coordenadas continua sendo uma palavra-código de peso de Hamming 6. Portanto, o Código de Golay estendido não é $\mathbb{Z}_4$-linear.

Teorema 3.2.6 *Seja $\mathbb{C}$ um código $\mathbb{Z}_4$-linear e, portanto, imagem de um código de grupo quaternário $\mathcal{C}$. Então*

1. *$\mathbb{C}$ é efetivamente casado a $\mathcal{C}$;*
2. *$\mathbb{C}$ é um código geometricamente uniforme.*

Demonstração:

1. *Pelo Teorema 2.4.6, é suficiente mostrar que $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ é um rotulamento casado. De fato,*

$$d_H(\phi(g), \phi(g')) = d_L(g, g') = d_L(g - g', 0) = d_H(\phi(g - g'), \phi(0)).$$

   Como ϕ é bijetora, o resultado segue.

2. *Como $\mathbb{C}$ é efetivamente casado a $\mathcal{C}$, o grupo $\mathcal{C}$ é isomorfo a um subgrupo transitivo do grupo de simetrias de $\mathbb{C}$, o que implica naturalmente que $\mathbb{C}$ é geometricamente uniforme.*□

3.2.1 Tabela de códigos de grupo quaternários cuja imagem é um código binário geometricamente uniforme

Utilizando do algoritmo de otimização combinatorial proposto por Said e Palazzo [50], um grande número de códigos de grupo quaternários foi determinado. Este algoritmo apresenta, para um dado comprimento e uma dada dimensão, o código de grupo quaternário com maior distância de Lee mínima. Estes códigos são apresentados nas Tabelas 3.2, 3.3, 3.4, 3.5 e 3.6, onde:

- n é o comprimento do código de grupo quaternário;
- k é a dimensão do código de grupo quaternário;

- d é a distância de Lee mínima correspondente à distância de Hamming no código binário associado pelo mapeamento ϕ;
- N é comprimento do código binário;
- K é a dimensão do código binário;
- U é a melhor distância alcançada pelos códigos binários lineares segundo a tabela de Verhoeff [12].
- Matriz geradora: Esta é a matriz geradora do código quaternário.
- Espectro de pesos: Este é o espectro de pesos de Lee do código quaternário que é igual à dos pesos de Hamming do código binário correspondente.

As Tabelas 3.7 e 3.8 apresentam códigos binários que são imagens de códigos de grupo quaternários cíclicos e seus dados são organizados como segue:

- n é o comprimento do código de grupo quaternário cíclico;
- k é a dimensão do código de grupo quaternário cíclico;
- d é a melhor distância de Lee encontrada para o código quaternário cíclico que corresponde à distância de Hamming no código binário correspondente;
- d' é a distância correspondente ao código de grupo de mesmos parâmetros, porém não necessariamente cíclico;
- Espectro de Pesos: Este é o espectro de pesos do código de grupo quaternário cíclico que é igual a do código binário correspondente.

As tabelas apresentam códigos binários $\mathbb{Z}_4$-lineares cujo comprimento é menor ou igual a 10. Em [15], são apresentadas classes de códigos binários não lineares como as de Preparata, Goethals e de Kerdock, além do código de Nordstron-Robinson que é apresentado como imagem binária de um código de grupo quaternário cíclico estendido.

n	k	d	N	K	U	matriz geradora	espectro de pesos
2	1	2	4	2	2	paridade	
3	1	3	6	2	4	repetição	
3	2	2	6	4	2	paridade	
4	1	4	8	2	5	repetição	
4	2	4	8	4	4	2 3 1 0	0(1) 4(14) 8(1)
						1 0 2 3	
4	3	2	8	6	2	paridade	
5	1	5	10	2	6	repetição	
5	2	4	10	4	4	2 1 0 3 3	0(1) 4(2) 5(8) 6(4) 8(1)
						3 2 3 1 3	
5	3	3	10	6	3	3 3 0 1 3	0(1) 3(8) 4(18) 5(16) 6(8)
						1 1 3 2 2	7(8) 8(5)
						0 3 3 2 3	
5	4	2	10	8	2	paridade	
6	1	6	12	2	8	repetição	
6	2	6	12	4	6	0 3 3 1 2 3	0(1) 6(12) 8(3)
						3 2 3 3 1 0	
6	3	4	12	6	4	0 1 3 1 2 0	0(1) 4(6) 5(24) 6(16) 8(9)
						2 2 3 1 3 3	9(8)
						1 3 0 1 2 3	
6	4	3	12	8	3	2 2 0 2 3 3	0(1) 3(16) 4(39) 5(48)
						3 1 2 2 2 0	6(48) 7(48)8(39) 9(16)
						1 2 0 3 2 3	12(1)
						1 1 3 3 2 0	
6	5	2	12	10	2	paridade	
7	1	7	14	2	9	repetição	
7	2	6	14	4	7	1 3 2 2 0 1 3	0(1) 6(2) 7(8) 8(3) 10(2)
						2 0 1 1 3 3 3	

Tabela 3.2: Códigos de grupo quaternários obtidos pela técnica de otimização

n	k	d	N	K	U	matriz geradora	espectro de pesos
7	3	6	14	6	5	1 3 0 3 2 1 0	0(1) 6(42) 8(7) 10(14)
						0 2 3 1 1 1 0	
						0 3 2 0 3 1 1	
7	4	4	14	8	4	3 2 3 3 1 0 0	0(1) 4(14) 5(56) 6(49) 7(16)
						0 1 1 3 2 2 2	8(49) 9(56) 10(14) 14(1)
						0 3 0 1 3 0 1	
						2 3 0 2 2 1 1	
7	5	2	14	10	3	1 2 3 2 1 2 2	0(1) 2(1) 3(28) 4(71) 5(112)
						1 3 3 1 2 3 2	6(183) 7(232) 8(183) 9(112)
						2 0 1 3 2 0 1	10(71) 11(28) 12(1)14(1)
						1 3 0 3 0 2 0	
						3 0 0 3 0 2 0	
7	6	2	14	12	2	paridade	
8	1	8	16	2	10	repetição	
8	2	8	16	4	8	1 0 0 1 2 1 3 2	0(1) 8(11) 10(4)
						3 2 1 1 2 2 0 3	
8	3	6	16	6	6	0 0 1 2 3 0 1 2	0(1) 6(8) 7(24) 8(13) 10(8)11(8)
						3 3 0 3 0 3 3 2	12(2)
						2 1 0 2 3 0 3 3	
8	4	6	16	8	5	0 3 0 0 3 3 2 3	0(1) 6(112) 8(30) 10(112) 16(1)
						3 2 0 1 3 0 0 3	
						3 3 0 2 3 2 1 2	
						1 0 3 0 3 1 2 0	
8	5	4	16	10	4	1 1 3 1 1 1 2 1	0(1) 4(47) 5(72) 6(98) 7(192)
						1 3 1 0 3 0 3 0	8(207) 9(176) 10(124) 11(64)
						3 0 0 2 2 3 2 1	12(33) 13(8)14(2)
						3 2 1 3 3 0 2 1	
						3 3 1 2 2 2 2 2	

Tabela 3.3: Códigos de grupo quaternários obtidos pela técnica de otimização (cont.)

n	k	d	N	K	U	matriz geradora	espectro de pesos
8	6	2	16	12	2	3 1 0 1 0 2 3 2	0(1) 2(2) 3(40) 4(128) 5(264)
						0 3 2 3 2 1 1 1	6(478) 7(720) 8(830) 9(720)
						3 3 2 0 0 1 0 1	10(478)11(264)12(128) 13(40)
						1 2 3 2 0 1 1 2	14(2) 16(1)
						2 1 2 3 1 2 0 3	
						3 1 3 2 2 2 3 3	
8	7	2	16	14	2	paridade	
9	1	9	18	2	12	repetição	
9	2	8	18	4	8	1 1 2 1 2 0 1 3 0	0(1) 8(1) 9(8) 10(4) 12(2)
						2 0 3 0 2 2 3 3 3	
9	3	8	18	6	8	2 1 0 0 1 0 2 3 1	0(1) 8(46) 12(16) 16(1)
						0 3 3 2 1 2 1 2 2	
						3 3 3 0 1 3 3 3 3	
9	4	6	18	8	6	3 1 2 3 1 3 0 0 3	0(1) 6(23) 7(56) 8(45) 9(16)
						2 3 1 0 1 1 1 0 1	10(34)11(56) 12(18) 14(7)
						1 0 1 0 0 2 0 2 1	
						0 0 0 2 1 2 0 3 3	
9	5	4	18	10	4	3 1 0 1 1 2 3 2 3	0(1) 4(3) 5(40) 6(104) 7(128)
						1 3 2 1 2 1 3 1 0	8(113) 9(176) 10(232)
						3 1 2 0 3 1 2 3 1	11(128) 12(41) 13(40)
						1 2 1 0 0 1 3 2 3	14(16) 16(2)
						3 3 3 0 3 1 3 0 0	
9	6	4	18	12	4	2 0 0 1 1 1 2 3 2	0(1) 4(78) 5(144) 6(228)7(528)
						2 0 2 3 3 2 1 1 1	8(708) 9(736) 10(696) 11(480)
						0 0 3 3 1 1 0 2 0	12(298) 13(144) 14(36)
						3 0 3 1 1 2 3 2 0	15(16) 16(3)
						3 1 0 3 2 3 2 3 0	
						1 2 1 0 3 3 2 3 3	

Tabela 3.4: Códigos de grupo quaternários obtidos pela técnica de otimização (cont.)

n	k	d	N	K	U	matriz geradora	espectro de pesos
9	7	2	18	14	2	1 3 0 3 0 0 3 3 1	0(1) 2(3) 3(60) 4(210) 5(504)
						0 3 3 0 3 2 2 1 1	6(1134)7(2052) 8(2748)
						2 1 0 3 1 3 0 2 0	9(2960) 10(2748)11(2052)
						0 3 3 2 0 0 3 2 3	12(1134)13(504)14(210)
						0 1 3 3 2 0 0 2 2	15(60) 16(3)18(1)
						1 2 2 3 1 3 3 0 0	
						3 2 3 3 3 1 3 2 2	
9	8	2	18	16	2	paridade	
10	1	10	20	2	13	repetição	
10	2	10	20	4	10	2 1 1 3 1 1 3 3 0 1	0(1) 10(12) 12(2) 16(1)
						3 0 0 3 1 3 2 2 3 3	
10	3	8	20	6	8	2 2 3 1 2 1 0 2 3 3	0(1) 8(7) 9(24) 10(16)12(6)
						1 2 0 1 0 3 2 1 1 0	13(8)16(2)
						3 3 2 2 3 2 3 2 0 1	
						1 0 1 3 3 3 3 1 1 0	
						2 0 1 1 1 0 3 0 2 0	
						0 3 3 1 0 2 2 0 0 3	
10	5	6	20	10	6	3 0 2 1 0 1 0 2 0 3	0(1) 6(90) 8(255) 10(332)
						2 3 2 1 0 2 2 2 3 3	12(255) 14(90)20(1)
						3 2 3 3 2 0 3 0 3 3	
						1 3 1 2 0 3 0 3 0 3	
						0 3 1 0 3 3 0 0 3 1	
10	6	4	20	12	4	0 0 2 3 3 0 1 0 3 1	0(1) 4(5) 5(64) 6(240)7(320)
						2 1 3 0 3 3 0 0 2 3	8(250)9(640) 10(1056)
						1 0 0 3 3 1 2 1 2 1	11(640) 12(250)13(320)
						1 0 2 3 2 2 1 0 3 3	14(240)15(64) 16(5) 20(1)
						1 1 3 0 1 2 3 2 3 0	
						0 1 2 0 3 3 2 3 3 2	

Tabela 3.5: Códigos de grupo quaternários obtidos pela técnica de otimização (cont.)

n	k	d	N	K	U	matriz geradora	espectro de pesos
10	7	4	20	14	4	2 0 2 3 1 0 2 0 1 0	0(1) 4(125) 5(256) 6(480)
						0 2 3 1 0 2 1 3 1 1	7(1280) 8(2050)9(2560)
						1 3 0 3 1 1 0 3 3 3	10(2880) 11(2560) 12(2050)
						3 0 0 2 3 0 1 3 2 1	13(1280) 14(480)15(256)
						2 2 2 2 0 1 3 2 0 2	16(125) 20(1)
						3 0 2 0 0 3 2 0 1 1	
						2 1 3 2 3 3 2 2 0 0	
10	8	2	20	16	2	1 2 1 1 2 1 1 2 3 1	0(1) 2(5) 3(82) 4(324)5(928)
						3 1 1 0 3 1 1 2 2 0	6(2388)7(4936) 8(7902)
						1 3 3 1 2 3 0 0 0 2	9(10368) 10(11542)11(10620)
						0 0 1 2 0 1 1 0 2 3	12(7860)13(4768) 14(2436)
						0 0 3 3 0 2 1 2 0 3	15(1000) 16(297) 17(64)
						2 0 2 3 2 3 3 1 3 3	18(13)19(2)
						2 0 0 2 0 0 2 3 3 3	
						3 0 0 3 1 3 2 2 2 3	
10	9	2	20	18	2	paridade	

Tabela 3.6: Códigos de grupo quaternários obtidos pela técnica de otimização (cont.)

UNICAMP
BIBLIOTECA CENTRAL

n	k	d	d'	pol.gerador	espectro de pesos
2	1	2	2	paridade	
3	1	3	3	repetição	
3	2	2	2	paridade	
4	1	4	4	repetição	
4	2	4	4	1 2 1 0	0(1) 4(14) 8(1)
4	3	2	2	paridade	
5	1	5	5	repetição	
5	2				Não existe código cíclico com estes parâmetros.
5	3				Não existe código cíclico com estes parâmetros.
5	4	2	2	paridade	
6	1	6	6	repetição	
6	2	6	6	1 3 2 1 1 0	0(1) 6(12) 8(3)
6	3	4	4	1 2 0 1 0 0	0(1) 4(15) 6(32) 8(15) 12(1)
6	4	3	3	3 1 1 0 0 0	0(1) 3(16) 4(39) 5(48) 6(48)7(48) 8(39) 9(16) 12(1)
6	5	2	2	paridade	
7	1	7	7	repetição	
7	2				Não existe código cíclico com estes parâmetros.
7	3	6	6	1 2 3 1 1 0 0	0(1) 6(42) 8(7) 10(14)
7	4	4	4	3 1 2 1 0 0 0	0(1) 4(14) 5(56) 6(49) 7(16) 8(49) 9(56)10(14) 14(1)
7	5				Não existe código cíclico com estes parâmetros.
7	6	2	2	paridade	
8	1	8	8	repetição	
8	2	8	8	1 2 1 0 1 2 1 0	0(1) 8(14) 16(1)
8	3	6	6	3 1 2 0 1 1 0 0	0(1) 6(16) 8(30) 10(16) 16(1)
8	4	4	6	3 0 2 0 1 0 0 0	0(1) 4(28) 8(198) 12(28) 16(1)
8	5	4	4	3 1 1 1 0 0 0 0	0(1) 4(60) 6(256) 8(390) 10(256) 12(60) 16(1)
8	6	2	2	1 2 1 0 0 0 0 0	0(1) 2(8) 4(252) 6(952) 8(1670) 10(952)12(252) 14(8) 16(1)

Tabela 3.7: Códigos de grupo quaternários cíclicos obtidos por procura computacional exaustiva

n	k	d	d'	pol. gerador	espectro de pesos
8	7	2	2	paridade	
9	1	9	9	repetição	
9	2	6	8	3 1 0 3 1 0 3 1 0	0(1) 6(6) 12(9)
9	3	3	8	1 0 0 1 0 0 1 0 0	0(1) 3(6) 6(15) 9(20) 12(15) 15(6) 18(1)
9	4				Não existe código cíclico com estes parâmetros.
9	5				Não existe código cíclico com estes parâmetros.
9	6	2	4	3 0 0 1 0 0 0 0 0	0(1) 2(18) 4(135) 6(540) 8(1215) 10(1458)
					12(729)
9	7	2	2	1 1 1 0 0 0 0 0 0	0(1) 2(18) 3(54) 4(135)
					5(540) 6(1269) 7(1962) 8(2673)
					9(3080) 10(2673) 11(1962) 12(1269)
					13(540) 14(135)15(54) 16(18) 18(1)
9	8	2	2	paridade	
10	1	10	10	repetição	
10	2	5	10	1 0 1 0 1 0 1 0 1 0	0(1) 5(4) 10(6) 15(4) 20(1)
10	3				Não existe código cíclico com estes parâmetros.
10	4	8	8	3 3 2 0 2 1 1 0 0 0	0(1) 8(130) 12(120) 16(5)
10	5	4	6	1 2 0 0 0 1 0 0 0 0	0(1) 4(25) 6(40) 8(230) 10(432) 12(230) 14(40)
					16(25) 20(1)
10	6	4	4	3 3 1 3 3 0 0 0 0 0	0(1) 4(5) 5(64) 6(240) 7(320) 8(250)
					9(640) 10(1056) 11(640) 12(250) 13(320)
					14(240)15(64) 16(5) 20(1)
10	7				Não existe código cíclico com estes parâmetros.
10	8	2	2	3 0 1 0 0 0 0 0 0 0	0(1) 2(40) 4(620) 6(4600) 8(16150) 10(23000)
					12(15500) 14(5000) 16(625)
10	9	2	2	paridade	

Tabela 3.8: Códigos de grupo quaternários cíclicos obtidos por procura computacional exaustiva (cont.)

3.3 $\mathbb{Z}_{2^k}$-Linearidade: Análise de Casos

Nesta seção iremos apresentar a análise de casos de possíveis extensões da $\mathbb{Z}_4$-linearidade para uma $\mathbb{Z}_2^k$-linearidade. Para isto, devemos em primeiro lugar, estabelecer as principais propriedades da $\mathbb{Z}_4$-linearidade. Lembramos, da seção anterior, que as propriedades da $\mathbb{Z}_4$-linearidade estão ligadas ao rotulamento $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$, isto é,

P1. O rotulamento $\phi(c) = (\beta(c), \gamma(c))$ é um código de Gray dos símbolos de $\mathbb{Z}_4$ pelos símbolos de $\mathbb{Z}_2^2$;

P2. O rotulamento ϕ é uma bijeção de $\mathbb{Z}_4$ em $\mathbb{Z}_2^2$;

P3. O rotulamento ϕ preserva pesos de $(\mathbb{Z}_4, w_L)$ para $(\mathbb{Z}_2^2, w_H)$;

P4. O rotulamento estendido $\overline{\phi}(c) = (\alpha(c), \beta(c), \gamma(c))$ pode ser construído da seguinte maneira:

   (a) Escreva a expansão binária de c: isto é, $c = \alpha(c) + 2.\beta(c)$;

   (b) $\gamma(c)$ é escolhido de forma que $\alpha(c) + \beta(c) + \gamma(c) = 0 \bmod 2$;

P5. A imagem do rotulamento estendido

$$\overline{\phi} : \mathbb{Z}_4 \to \mathbb{Z}_2^3; \overline{\phi}(c) = (\alpha(c), \beta(c), \gamma(c)),$$

é um $(3, 2)$-código cíclico cujas palavras-código são o deslocamento cíclico de um vetor constante.

Estas cinco propriedades são consideradas *propriedades chaves* da $\mathbb{Z}_4$-linearidade. Nas próximas subseções estaremos analisando casos de possíveis extensões da $\mathbb{Z}_4$-linearidade para a $\mathbb{Z}_{2^k}$-linearidade ($k \geq 3$), tendo como objetivo preservar a maioria das propriedades da $\mathbb{Z}_4$-linearidade. Apresentaremos também as desvantagens de tais definições em considerá-las como técnica de construção de códigos corretores de erros.

3.3.1 Análise da $\mathbb{Z}_{2^k}$-Linearidade sob P1, P3 e P5

Nesta subseção, iremos analisar a $\mathbb{Z}_{2^k}$-linearidade ($k \geq 3$) sob as propriedades P1, P3 e P5. Para isso, definimos novas funções ϕ, α, e $\overline{\phi}$, que possuem as seguintes condições:

P1. O mapeamento $\phi(c) = (\beta(c), \gamma(c))$ é um código de Gray dos símbolos de $\mathbb{Z}_{2^k}$ pelos símbolos de $\mathbb{Z}_2^k$;

P3. O mapeamento ϕ preserva pesos;

P5. A imagem do mapeamento estendido $\overline{\phi}(c) = (\alpha(c), \phi(c))$ é um código cíclico cujas palavras-código são deslocamentos cíclicos de um vetor constante.

Em princípio, não conhecemos o mapeamento ϕ nem sua imagem que deve ser $\mathbb{Z}_2^q$, para algum inteiro positivo q. O inteiro q e o mapeamento ϕ serão determinados afim de satisfazerem as duas primeiras propriedades acima. O mapeamento estendido $\overline{\phi}$ será especificado pela terceira propriedade.

Como $\mathbb{Z}_{2^k}$ possui um elemento cujo peso de Lee é 2^{k-1}, a imagem de ϕ deve estar contida em $\mathbb{Z}_2^{2^{k-1}}$. Então, precisamos encontrar um mapeamento ϕ que preserva pesos de $(\mathbb{Z}_{2^k}, w_L)$ em $(\mathbb{Z}_2^{2^{k-1}}, w_H)$. Escreveremos ϕ_k ao invés de ϕ, dada a dependência de ϕ em relação a k. Observe que $\phi_k(0) = (0, 0, \ldots, 0)$, o vetor nulo de comprimento n, e $\phi_k(2^{k-1}) = (1, 1, \ldots, 1)$, o vetor todo um de comprimento n.

Definição 3.3.1 *Seja $k \geq 1$. Um k-**rótulo de** $\mathbb{Z}_{2^k}$ **por** $\mathbb{Z}_2^{2^{k-1}}$ é uma função $\phi_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^{2^{k-1}}$ dada por:*

$$\phi_k(c) = \begin{cases} \sum_{i=0}^{2^{k-1}-c} \mathbf{e}_{2^{k-1}}(i), & se \quad c \leq 2^{k-1} \\ \sum_{i=1}^{2^k-c} \mathbf{e}_{2^{k-1}}(i), & se \quad 2^{k-1} < c < 2^k \end{cases},$$

onde $\mathbf{e}_n(j)$ é um vetor de n componentes das quais a j-ésima componente é 1 e as restantes são zero. O vetor $\mathbf{e}_n(0)$ é definido como o vetor cujas componentes são todas iguais a 1.

O teorema a seguir é uma consequência direta da Definição 3.3.1.

Teorema 3.3.1 *O k-rótulo ϕ_k é uma imersão isométrica de*

$$(\mathbb{Z}_{2^k}, d_L) \text{ em } (\mathbb{Z}_2^{2^{k-1}}, d_H).$$

Demonstração: Sejam $c_1, c_2 \in \mathbb{Z}_{2^k}$, tal que $c_2 \leq c_1 \leq 2^{k-1}$, então $c_1 - c_2 = p \leq 2^{k-1}$ implica que o peso de Lee de $c_1 - c_2$ é igual a p, isto é,

$$w_L(c_1 - c_2) = p$$

Agora

$$\begin{aligned} d_H(\phi_k(c_1), \phi_k(c_2)) &= w_H(\phi_k(c_1) - \phi_k(c_2)) = w_H\left(\sum_{i=0}^{2^{k-1}-c_1} \mathbf{e}_{2^{k-1}}(i) - \sum_{i=0}^{2^{k-1}-c_2} \mathbf{e}_{2^{k-1}}(i)\right) = \\ &= w_H\left(\sum_{i=2^{k-1}-c_2+1}^{2^{k-1}-c_2+p} \mathbf{e}_{2^{k-1}}(i)\right) = \sum_{i=2^{k-1}-c_2+1}^{2^{k-1}-c_2+p} w_H(\mathbf{e}_{2^{k-1}}(i))) = p = \\ &= w_L(c_1 - c_2) = d_L(c_1, c_2). \end{aligned}$$

Para outros casos, a situação é análoga.□

O k-rótulo ϕ_k possui também a seguinte propriedade, repetindo de forma sutil o que ocorre na $\mathbb{Z}_4$-linearidade:

Teorema 3.3.2 *Para todos $a, b \in \mathbb{Z}_{2^k}$, temos*

$$\phi_k(a + b) = \phi_k(a) + [-a]\,\phi_k(b),$$

onde $[-a]\mathbf{u}$ é a 2^{k-1}-upla resultante do deslocamento cíclico das componentes de $\mathbf{u}$ $(a \bmod 2^{k-1})$ coordenadas para a esquerda.

Demonstração: Temos 4 casos a analisar:

1. $a + b \geq 2^k$ e $(a + b) \bmod 2^k \leq 2^{k-1}$;
2. $a + b \geq 2^k$ e $(a + b) \bmod 2^k > 2^{k-1}$;
3. $a + b < 2^k$ e $(a + b) \bmod 2^k \leq 2^{k-1}$;
4. $a + b < 2^k$ e $(a + b) \bmod 2^k > 2^{k-1}$.

No primeiro caso temos:

- $(a+b) \bmod 2^k = (a+b) - 2^k \leq 2^{k-1}$;
- $\phi_k((a+b) \bmod 2^k) = \sum_{i=0}^{2^{k-1}-(a+b-2^k)} \mathbf{e}(i) = \sum_{i=2^{k-1}-(a+b-2^k)+1}^{2^{k-1}} \mathbf{e}(i)$.

Para cada um destes casos temos dois subcasos para os valores de a e b:

(a) $a < 2^{k-1}$ e $b \geq 2^{k-1}$;

(b) $a \geq 2^{k-1}$ e $b \geq 2^{k-1}$.

No primeiro subcaso temos:

- $a \bmod 2^{k-1} = a$;
- $\phi_k(a) = \sum_{i=0}^{2^{k-1}-a} \mathbf{e}(i)$;
- $\phi_k(b) = \sum_{i=1}^{2^k-b} \mathbf{e}(i)$;

e então

$$[-a]\phi_k(b) = \sum_{i=1}^{2^k-b} [-a]\mathbf{e}(i).$$

Mas:

- O deslocamento cíclico de $\mathbf{e}_{2^{k-1}}(i)$ em a coordenadas é dado por $\mathbf{e}_{2^{k-1}}(2^{k-1} - a + i)$;
- O deslocamento cíclico de $\mathbf{e}_{2^{k-1}}(2^k - b)$ depende de $(2^k - b) - a = 2^k - (a+b)$.

e

$$-2^{k-1} \leq 2^k - (a+b) \leq 0.$$

Então o deslocamento cíclico é dado por

$$\mathbf{e}_{2^{k-1}}(2^{k-1} - (a+b-2^k)).$$

Portanto,

$$[-a]\phi_k(b) = \sum_{i=2^{k-1}-a+1}^{2^{k-1}-(a+b-2^k)} \mathbf{e}(i) = \sum_{i=2^{k-1}-(a+b-2^k}^{2^{k-1}} \mathbf{e}(i) + \sum_{i=0}^{2^{k-1}-a} \mathbf{e}(i) = \phi_k(a+b) + \phi_k(a).$$

Os outros casos e subcasos seguem de forma análoga.□

A justificativa para a busca do resultado do Teorema 3.3.2 está no fato do mapeamento não ser, em geral, uma função linear no sentido de que $\phi_k(a+b) \neq \phi_k(a) + \phi_k(b)$. Com isso, é necessário saber que resíduo está acrescentado a esta soma, pois o conhecimento do mesmo permite encontrar as condições para que um código seja $\mathbb{Z}_{2^k}$-linear.

Exemplo 3.3.1 *Para $k = 2$, o 2-rótulo $\phi_2(c) = (\phi_{21}(c), \phi_{22}(c)) = (\beta(c), \gamma(c))$ é dado por:*

c	$\beta(c)$	$\gamma(c)$
0	0	0
1	0	1
2	1	1
3	1	0

Tabela 3.9: Mapeamento de Gray

que é a $\mathbb{Z}_4$-linearidade como caso particular apresentado na subseção anterior.

Exemplo 3.3.2 *Para $k = 3$, o 3-rótulo $\phi_3(c) = (\phi_{31}(c), \phi_{32}(c), \phi_{33}(c), \phi_{34}(c))$ é dado pela Tabela 3.10:*

c	$\phi_{31}(c)$	$\phi_{32}(c)$	$\phi_{33}(c)$	$\phi_{34}(c)$
0	0	0	0	0
1	0	0	0	1
2	0	0	1	1
3	0	1	1	1
4	1	1	1	1
5	1	1	1	0
6	1	1	0	0
7	1	0	0	0

Tabela 3.10: Mapeamento sobre $\mathbb{Z}_8$

Vamos agora explorar o problema da definição da função $\alpha_k(c)$, similar ao da $\mathbb{Z}_4$-linearidade, um mapeamento estendido $\overline{\phi}_k(c) = (\alpha_k(c), \phi_k(c))$, cuja imagem forma um código cíclico. Este código cíclico, apesar de não ser linear, é tal que suas palavras-código (exceto a palavra toda nula) são deslocamentos cíclicos de uma palavra-código dada. Temos, então

$$\alpha_k(c) = \begin{cases} \sum_{i=1}^{2^{k-1}-c} \mathbf{e}_{2^{k-1}-1}(i), & se \quad c < 2^{k-1} \\ \sum_{i=0}^{2^k-c-1} \mathbf{e}_{2^{k-1}-1}(i), & se \quad 2^{k-1} \leq c \leq 2^k - 1 \end{cases}$$

Definição 3.3.2 *Um k-rótulo estendido é uma função*

$$\overline{\phi}_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^{2^k-1},$$

definida por

$$\overline{\phi}_k(c) = (\alpha_k(c), \phi_k(c)).$$

Exemplo 3.3.3 *Para $k = 3$, o 3-rótulo estendido é mostrado na Tabela 3.11:*

c	$\alpha_{31}(c)$	$\alpha_{32}(c)$	$\alpha_{33}(c)$	$\phi_{31}(c)$	$\phi_{32}(c)$	$\phi_{33}(c)$	$\phi_{34}(c)$
0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	1
2	1	1	0	0	0	1	1
3	1	0	0	0	1	1	1
4	0	0	0	1	1	1	1
5	0	0	1	1	1	1	0
6	0	1	1	1	1	0	0
7	1	1	1	1	0	0	0

Tabela 3.11: Mapeamento estendido sobre $\mathbb{Z}_8$

Observe que as 7-uplas binárias nesta tabela formam um código (não-linear) cíclico, ou seja, elas são geradas por deslocamentos cíclicos do vetor (0 0 0 1 1 1 1). Mais geralmente, o k-rótulo

estendido é gerado por deslocamentos cíclicos do vetor $\mathbf{0}_{2^{k-1}-1}\,\mathbf{1}_{2^{k-1}}$ que é imagem de 2^{k-1}. De fato,

$$\begin{aligned}\overline{\phi}_k(2^{k-1}) &= (\alpha_k(2^{k-1}), \phi_k(2^{k-1})) = (\sum_{i=0}^{2^{k-1}-2^{k-1}-1} \mathbf{e}_{2^{k-1}-1}(i), \sum_{i=0}^{2^{k-1}-2^{k-1}} \mathbf{e}_{2^{k-1}}(i)) = \\ &= (\sum_{i=0}^{2^{k-1}-1} \mathbf{e}_{2^{k-1}-1}(i), \sum_{i=0}^{0} \mathbf{e}_{2^{k-1}}(i)) = \mathbf{0}_{2^{k-1}-1}\mathbf{1}_{2^{k-1}}.\end{aligned}$$

Quanto à ciclicidade, temos, para $c < 2^{k-1}$,

$$\begin{aligned}\overline{\phi}_k(c) &= (\sum_{i=1}^{2^{k-1}-c} \mathbf{e}_{2^{k-1}-1}(i), \sum_{i=0}^{2^{k-1}-c} \mathbf{e}_{2^{k-1}}(i)) = (\sum_{i=1}^{2^{k-1}-c} \mathbf{e}_{2^{k-1}-1}(i), \mathbf{1}_{2^{k-1}} + \sum_{i=1}^{2^{k-1}-c} \mathbf{e}_{2^{k-1}}(i)) = \\ &= \mathbf{0}_{2^{k-1}-1}\mathbf{1}_{2^{k-1}} + \sum_{i=1}^{2^{k-1}-c} \mathbf{e}_{2^k-1}(i) + \sum_{i=2^{k-1}}^{2^{k-1}-c} \mathbf{e}_{2^k-1}(i) = \sum_{i=1}^{2^{k-1}-c} \mathbf{e}_{2^k-1}(i) + \sum_{i=2^k-c}^{2^k-1} \mathbf{e}_{2^k-1}(i),\end{aligned}$$

e, então para $a = 1, 2, \ldots, 2^{k-1} - 1$,

$$\begin{aligned}\overline{\phi}_k(2^{k-1} - a) &= \sum_{i=1}^{2^{k-1}-2^{k-1}+a} \mathbf{e}_{2^k-1}(i) + \sum_{i=2^k-2^{k-1}+a}^{2^k-1} \mathbf{e}_{2^k-1}(i) = \\ &= \sum_{i=1}^{a} \mathbf{e}_{2^k-1}(i) + \sum_{i=2^{k-1}+a}^{2^k-1} \mathbf{e}_{2^k-1}(i) = [a] \sum_{i=2^{k-1}}^{2^k-1} \mathbf{e}_{2^k-1}(i) = \\ &= [a]\overline{\phi}_k(2^{k-1}).\end{aligned}$$

Para $c \geq 2^{k-1}$ o raciocínio é análogo.

Definição 3.3.3 *Um k-mapeamento em $\mathbb{Z}_{2^k}^n$ é definido por*

$$\Phi_k : \mathbb{Z}_{2^k}^n \longrightarrow \mathbb{Z}_2^{2^{k-1}n}$$

$$\Phi_k(c) = \Phi_k(c_1, c_2, \ldots, c_n) = (\phi_k(c_1), \phi_k(c_2), \ldots, \phi_k(c_n)) =$$

$$\begin{aligned}&(\phi_{k1}(c_1), \phi_{k2}(c_1), \ldots, \phi_{k2^{k-1}}(c_1), \phi_{k1}(c_2), \phi_{k2}(c_2), \ldots, \\ &\phi_{k2^{k-1}}(c_2), \ldots, \phi_{k1}(c_n), \phi_{k2}(c_n), \ldots, \phi_{k2^{k-1}}(c_n)).\end{aligned}$$

O resultado a seguir é uma consequência imediata do Teorema 3.3.2:

Teorema 3.3.3 *Para todo* $\boldsymbol{a}$, $\boldsymbol{b} \in \mathbb{Z}_{2^k}^n$, *temos*

$$\Phi_k(\mathbf{a}+\mathbf{b}) = \Phi_k(\mathbf{a}) + [-\mathbf{a}]\,\Phi_k(\mathbf{b}) =$$

$$\Phi_k(\mathbf{a}) + ([-a_1]\phi_k(b_1), [-a_2]\phi_k(b_2), \ldots, [-a_n]\phi_k(b_n))$$

Definição 3.3.4 *Sejam* $k \geq 1, n \geq 1$. *Dizemos que um código binário* $\mathbb{C}$ *de comprimento* $(2^k-1)n$ *é* $\mathbb{Z}_{2^k}$*-linear se existe um código de grupo* 2^k*-ário* $\overline{\mathbb{C}}$ *de comprimento* n, *tal que*

$$\Phi_k(\overline{\mathbb{C}}) = \mathbb{C}',$$

para algum código $\mathbb{C}'$ *equivalente a* $\mathbb{C}$.

Observe que, apesar de preservar distâncias, Φ_k não é uma bijeção e isto não é interessante para a construção de códigos. De fato, considere o código de grupo octário $(4, 2, 5)$ com matriz geradora

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

e espectro de pesos de Lee

Peso	0	5	6	7	8	9	10	11	12
No. de Palavras	1	8	12	8	9	8	4	8	6

obtido através de uma procura computacional exaustiva.

Este código mapeado por Φ_3 leva a um código binário $(16, 8, 5)$ com o espectro de pesos de Hamming igual ao do octário. Em termos de distância, é um bom código pois tem a mesma capacidade de correção de erros que o linear correspondente. Porém, como não existe a bijeção no mapeamento, o processo de decodificação, apesar de ser simplificado pela linearidade do código octário, é comprometido quando ocorrer um erro que não possua a correspondente imagem inversa.

O próximo teorema aborda este problema e mostra que, em geral, não é possível conseguir uma bijeção que preserve pesos de Lee/Hamming. Portanto, não existe isometria.

Antes disso, precisamos de um lema auxiliar cuja demonstração encontra-se no Apêndice A.

Lema 3.3.1 *A equação*

$$\prod_{i=1}^{l} m_i = \sum_{i=1}^{l} m_i, \quad l \geq 2,$$

nas incógnitas m_i, l, *sobre* $\mathbb{N}$ *somente tem solução para* $l = 2$, *e* $m_1 = m_2 = 2$.

Teorema 3.3.4 *Seja* $M \in \mathbb{N}$ *um inteiro positivo tal que*

$$M = m_1 \cdot m_2 \ldots m_l.$$

Então uma função

$$f : \mathbb{Z}_M \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_l}$$

preserva peso de Lee se, e somente se, $M = 4$.

Demonstração:

- M par: Sejam

$$I = \{i; m_i \text{ é par}\} \quad \text{e} \quad J = \{i; m_i \text{ é ímpar}\}.$$

Em $\mathbb{Z}_M$ o maior peso de Lee é $\frac{M}{2} = \frac{\prod_{i=i}^{l} m_i}{2}$.

Em $\bigotimes_{i=1}^{l} \mathbb{Z}_{m_i}$ o maior peso de Lee é $\sum_{i \in I} \frac{m_i}{2} + \sum_{i \in J} \frac{m_i - 1}{2}$

$$\frac{\prod_{i=1}^{l} m_i}{2} > \frac{\sum_{i=1}^{l} m_i}{2} = \sum_{i=1}^{l} \frac{m_i}{2} = \sum_{i \in I} \frac{m_i}{2} + \sum_{i \in J}^{l} \frac{m_i}{2} > \sum_{i \in I} \frac{m_i}{2} + \sum_{i \in J} \frac{m_i - 1}{2}.$$

Então, neste caso não se pode preservar pesos de Lee.

- M ímpar: Todos os m_i's são ímpares. Em $\mathbb{Z}_M$ existe um elemento com peso de Lee $\frac{M-1}{2} = \frac{\left(\prod_{i=i}^{l} m_i\right) - 1}{2}$. Em $\mathbb{Z}_{m_i}$ o maior peso de Lee é $\frac{m_i - 1}{2}$. Então em $\otimes_{i=1}^{l} \mathbb{Z}_{m_i}$, o maior peso de Lee é

$$\sum_{i=1}^{l} \frac{m_i - 1}{2}.$$

Entretanto,

$$\frac{(\prod_{i=1}^{l} m_i) - 1}{2} = \frac{\prod_{i=1}^{l} m_i}{2} - \frac{1}{2} > \frac{\sum_{i=1}^{l} m_i}{2} - \frac{1}{2} = \frac{l-1}{2} + \sum_{i=1}^{l} \frac{m_i - 1}{2} > \sum_{i=1}^{l} \frac{m_i - 1}{2}.$$

Então, neste caso não é possível preservar pesos de Lee. □

Como consequência deste teorema, temos que uma bijeção de $\mathbb{Z}_M$ em $\bigotimes_{i=1}^{l} \mathbb{Z}_{m_i}$ não permite preservar pesos de Lee a menos que $M = 4$. Desse modo, invalidando a $\mathbb{Z}_M$-linearidade com distâncias de Lee.

Concluímos esta subseção lembrando que, como técnica de construção de códigos binários, a definição de $\mathbb{Z}_{2^k}$-linearidade apresentada não é adequada, dado o fato de Φ_k não ser bijeção. De fato, existem $(2^k - 1)$-uplas que não estão associadas a nenhum elemento em $\mathbb{Z}_{2^k}$, o que dificulta o processo de decodificação.

Uma maneira de resolver isto é estabelecer uma correspondência com os elementos de $\mathbb{Z}_{2^k}$ vendo as 2^{k-1}-uplas como representantes de classes laterais. Desta forma, teremos uma bijeção, apesar do processo de decodificação ficar um pouco mais complexo.

Esta não é a situação ideal que procuramos como extensão da $\mathbb{Z}_4$-linearidade. Assim, devemos analisar outras situações que permitam estar mais próximo do que a $\mathbb{Z}_4$-linearidade nos oferece. Na subseção a seguir, a bijeção será uma das propriedades a ser exigida.

3.3.2 Análise da $\mathbb{Z}_{2^k}$-linearidade sob P1 e P2

Como a condição de isometria não é satisfeita, apresentaremos nesta subseção uma outra proposta para a definição de códigos $\mathbb{Z}_{2^k}$-lineares. O novo mapeamento é definido tal que as seguintes condições sejam satisfeitas:

P1. O mapeamento $\phi(c) = (\beta(c), \gamma(c))$ é um código de Gray dos símbolos de $\mathbb{Z}_4$ pelos símbolos de $\mathbb{Z}_2^2$;

P2. O mapeamento ϕ é uma bijeção de $\mathbb{Z}_4$ em $\mathbb{Z}_2^2$;

Definição 3.3.5 *Seja $k \geq 2$. Um k-rótulo de $\mathbb{Z}_{2^k}$ por $\mathbb{Z}_2^k$ é uma função*

$$\phi_k : \mathbb{Z}_{2^k} \longrightarrow \mathbb{Z}_2^k : c \longmapsto (\phi_{k1}(c), \phi_{k2}(c), \ldots, \phi_{kk}(c))$$

de forma que se a composição binária de c é

$$c = c_1 \cdot 2^0 + c_2 \cdot 2^1 + c_3 \cdot 2^2 + \ldots + c_{k-1} \cdot 2^{k-2} + c_k \cdot 2^{k-1},$$

então

$$\phi_{ki}(c) = \begin{cases} c_k & , se \quad i = 1 \\ (c_{k-i+2} + c_{k-i+1}) \bmod 2 & , se \quad i \neq 1 \end{cases}$$

Observamos que ϕ_k é uma composição de duas funções, ou seja,

$$\phi_k(c) = g_k(b_k(c))$$

onde:

a) a função $b_k : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_2^k$ associa a um número $c \in \mathbb{Z}_{2^k}$ um vetor $b_k(c) \in \mathbb{Z}_2^k$, que corresponde à expansão binária de c.

b) a função $g_k : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^k$ rearranja os vetores tais que os símbolos de $\mathbb{Z}_{2^k}$ formam um código de Gray [62] por vetores de $\mathbb{Z}_2^k$.

Exemplo 3.3.4 *Para $k = 2$, o mapeamento $\phi_2(c) = (\beta(c), \gamma(c))$ de códigos $\mathbb{Z}_4$-lineares [15] é reproduzido se*

$$b_2(c) = (\alpha(c), \beta(c)),$$

onde

$$\alpha(c) = c \bmod 2.$$

Com isso,

$$\phi_2(c) = g_2(b_2(c)) = (\beta(c), \gamma(c)).$$

Exemplo 3.3.5 *Para $k = 3$, temos o mapeamento dado pela Tabela 3.12.*

.

Observamos que ϕ_k é uma bijeção mas não é uma isometria entre $(\mathbb{Z}_{2^k}, d_L)$ e $(\mathbb{Z}_2^k, d_L)$, para $k > 2$.

Iremos a seguir obter a fórmula de $\phi_2(x + y)$ notando, primeiramente, que a função $b_2 : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ satisfaz:

$$b_2(x + y) = b_2(x) + b_2(y) + (0, b_{21}(x) \cdot b_{21}(y)).$$

p	$b_{21}(p)$	$b_{22}(p)$	$b_{23}(p)$	$\phi_{21}(p)$	$\phi_{22}(p)$	$\phi_{23}(p)$
0	0	0	0	0	0	0
1	1	0	0	0	0	1
2	0	1	0	0	1	1
3	1	1	0	0	1	0
4	0	0	1	1	1	0
5	1	0	1	1	1	1
6	0	1	1	1	0	1
7	1	1	1	1	0	0

Tabela 3.12: Mapeamento sobre $\mathbb{Z}_8$

Lembrando que

$$b_2(x) = (\alpha(x), \beta(x)),$$

temos

$$b_2(x+y) = b_2(x) + b_2(y) + (0, \alpha(x) \cdot \alpha(y)).$$

Como

$$\alpha(c) = \beta(c) + \gamma(c),$$

então

$$\begin{aligned} b_2(x+y) &= b_2(x) + b_2(y) + (0, (\beta(x) + \gamma(x)) \cdot (\beta(y) + \gamma(y)) \\ &= (\alpha(x) + \alpha(y), \beta(x) + \beta(y) + (\beta(x) + \gamma(x)) \cdot (\beta(y) + \gamma(y)). \end{aligned}$$

Usando o fato de que $\phi_2(c) = g(b_2(c))$, temos

$$\phi_2(x+y) = g(b_2(x+y)) =$$

$$= g(\alpha(x) + \alpha(y), \beta(x) + \beta(y) + (\beta(x) + \gamma(x)) \cdot (\beta(y) + \gamma(y)) \cdot (\beta(y) + \gamma(y))) =$$

$$= (\beta(x) + \beta(y) + (\beta(x) + \gamma(x)) \cdot (\beta(y) + \gamma(y)),$$

$$\alpha(x) + \alpha(y) + \beta(x) + \beta(y) + (\beta(x) + \gamma(x)) \cdot (\beta(y) + \gamma(y)) =$$

$$= (\beta(x), \gamma(x)) + (\beta(y), \gamma(y)) + ((\beta(x) + \gamma(x)) \cdot (\beta(y) + \gamma(y)),$$

$$(\beta(x) + \gamma(x)).(\beta(y) + \gamma(y))) =$$

$$= \phi_2(x) + \phi_2(y) + (\phi_2(x) + \sigma(\phi_2(x))) * ((\phi_2(y) + \sigma(\phi_2(y))),$$

onde $\sigma(\cdot)$ é a função "swap" [15], que permuta a metade esquerda e direita de cada palavra-código, ou seja,

$$\sigma : (u_1, u_2, \ldots, u_n, u_{n+1}, \ldots, u_{2n}) \mapsto (u_{n+1}, \ldots, u_{2n}, u_1, u_2, \ldots, u_n).$$

Para $k = 3$, temos:

Proposição 3.3.1 *A função $b_3 : \mathbb{Z}_8 \to \mathbb{Z}_2^3$ satisfaz:*

$$b_3(x + y) = b_3(x) + b_3(y) + (0, b_{31}(x) \cdot b_{31}(y), b_{32}(x) \cdot b_{32}(y) +$$
$$+ b_{31}(x) \cdot b_{31}(y) \cdot b_{32}(x) + b_{31}(x) \cdot b_{31}(y) \cdot b_{32}(y)).$$

Observe que neste caso é muito mais difícil computar $b_3(x + y)$ com o objetivo de verificar as condições de linearidade.

Utilizando a Definição 3.3.3, que é apropriada para este k-rótulo, temos

Definição 3.3.6 *Sejam k e n inteiros tais que $k \geq 1$ e $n \geq 1$. Dizemos que um código binário $\mathbb{C}$ de comprimento $2^k n$ é $\mathbb{Z}_{2^k}$-linear se existe um código de grupo 2^k-ário $\overline{\mathbb{C}}$ de comprimento n, tal que*

$$\Phi_k(\overline{\mathbb{C}}) = \mathbb{C}',$$

para algum código binário $\mathbb{C}'$ equivalente a $\mathbb{C}$.

Com esta definição, vemos que este caso é similar à da $\mathbb{Z}_4$-linearidade no que diz respeito à forma de construção do rotulamento. Entretanto, este rotulamento não preserva distâncias. Sem a garantia de isometria entre os espaços métricos fica mais difícil a utilização da proposta como técnica de construção de códigos binários.

De fato, ao considerarmos uma código 2^k-ário de peso de Lee mínimo $d_{\min}^L$, não temos conhecimento do peso de Hamming mínimo do código binário associado e, portanto, de sua capacidade de correção de erros.

Vemos assim que a isometria é uma propriedade fundamental para se obter uma técnica de construção de códigos similar a da $\mathbb{Z}_4$-linearidade. Antes de considerarmos a isometria propriamente dita, vamos fazer, na subseção a seguir, uma análise onde consideraremos uma bijeção que preserve pesos.

3.3.3 Análise da $\mathbb{Z}_{2^k}$- linearidade sob P2 e P3

Apresentamos, nesta subseção uma terceira possibilidade de definição de códigos $\mathbb{Z}_{2^k}$-lineares. Para isso, iremos propor que o mapeamento ϕ_k satisfaça as seguintes condições:

P2. O mapeamento ϕ é uma bijeção de $\mathbb{Z}_{2^k}$ em $\mathbb{Z}_2^k$;

P3. O mapeamento ϕ preserva pesos de $(\mathbb{Z}_{2^k}, w)$ para $(\mathbb{Z}_2^k, w_H)$, ou seja, $w(c) = w_H(\phi(c))$ $\forall c \in \mathbb{Z}_{2^k}$;

A condição P3 preserva pesos somente e não distâncias. Além disso, o peso w atribuído aos elementos de $\mathbb{Z}_{2^k}$ não é o peso de Lee, mas uma escolha que seja adequada ao contexto, já que o peso de Lee não permite, em geral, bijeção.

Estas duas condições permitem uma quantidade muito grande de mapeamentos e serão aqueles que levam o elemento 0 de $\mathbb{Z}_{2^k}$ no vetor todo nulo $\mathbf{0}_k$ em $\mathbb{Z}_2^k$.

Vamos definir o peso e a distância em $\mathbb{Z}_2^k$ de forma a obter a preservação de pesos.

Definição 3.3.7 *Seja $\mathbb{Z}_2^k$ o espaço de Hamming k-dimensional e*

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

uma função bijetora, tal que $\phi_k(0) = \mathbf{0}_k$. O peso esférico de $a \in \mathbb{Z}_{2^k}$ é dado por

$$w_{ES}(a) = w_H(\phi_k(a)).$$

A distância esférica de $a, b \in \mathbb{Z}_{2^k}$ é dado por

$$d_{ES}(a, b) = w_{ES}(a - b).$$

A exigência $\phi_k(0) = \mathbf{0}_k$ é essencial para que ocorra $d_{ES}(a,a) = 0$, pois

$$d_{ES}(a,a) = w_{ES}(a-a) = w_{ES}(0) = w_H(\phi_k(0)) = w_H(\mathbf{0}_k) = 0.$$

Observe que a distância esférica não é, em geral, uma métrica. Ainda não sabemos se este mapeamento preserva distâncias, ou seja, é verdade que

$$d_{ES}(a,b) = d_H(\phi_k(a), \phi_k(b))?$$

Vejamos dois exemplos de rotulamento bijetivo que exploram e respondem negativamente a esta questão.

Exemplo 3.3.6 *O k-rótulo apresentado na Subseção 3.3.2 é um rotulamento bijetivo e possui, no caso $k = 3$, o rótulo como mostrado na Tabela 3.13, onde $\phi_3(c) = (\beta(c), \gamma(c), \delta(c))$.*

c	$\beta(c)$	$\gamma(c)$	$\delta(c)$
0	0	0	0
1	0	0	1
2	0	1	1
3	0	1	0
4	1	1	0
5	1	1	1
6	1	0	1
7	1	0	0

Tabela 3.13: Rotulamento para $k = 3$

A relação de pesos esféricos dos elementos de $\mathbb{Z}_8$ é dada por:

$$\begin{aligned}
\mathbf{0} &\to 0 \\
\mathbf{1} &\to 1 \\
\mathbf{2} &\to 2 \\
\mathbf{3} &\to 1 \\
\mathbf{4} &\to 2 \\
\mathbf{5} &\to 3 \\
\mathbf{6} &\to 2 \\
\mathbf{7} &\to 1
\end{aligned}$$

Vamos analisar se o k-rótulo proposto preserva distâncias. A distância esférica entre os elementos 6 e 3 de $\mathbb{Z}_8$ é

$$d_{ES}(6,3) = w_{ES}(6-3) = w_{ES}(3) = 1.$$

Por outro lado,

$$d_H(\phi_3(6), \phi_3(3)) = d_H(010, 101) = 3.$$

Portanto, este mapeamento não preserva distâncias.

Vejamos agora um outro exemplo de rotulamento

Exemplo 3.3.7 *O rótulo apresentado neste exemplo é construído de forma a satisfazer a Propriedade P4. Seja $k \geq 2$. Um k-rótulo de $\mathbb{Z}_{2^k}$ por $\mathbb{Z}_2^k$ é uma função $\phi_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k$ definida por:*

1. *Escreva a expansão 2-ádica de $c \in \mathbb{Z}_{2^k}$ como*

$$c = c_1 \cdot 2^0 + c_2 \cdot 2^1 + \ldots + c_{k-1} \cdot 2^{k-2} + c_k \cdot 2^{k-1};$$

2. *Adicione um dígito de verificação de paridade c_{k+1} ao vetor $(c_1, c_2, \ldots, c_{k-1}, c_k)$;*

3. *Considere*

$$\phi_k(c) = (c_2, \ldots, c_{k-1}, c_k, c_{k+1}).$$

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$	$\delta(c)$
0	0	0	0	0
1	1	0	0	1
2	0	1	0	1
3	1	1	0	0
4	0	0	1	1
5	1	0	1	0
6	0	1	1	0
7	1	1	1	1

Tabela 3.14: Rotulamento para $k = 3$

Esta função sendo bijetora, permite definir o peso e a distância esférica em $\mathbb{Z}_{2^k}$. Para $k = 2$ temos naturalmente o caso $\mathbb{Z}_4$; para $k = 3$, o rotulamento obtido é mostrado na Tabela 3.14, onde $\phi_3(c) = (\beta(c), \gamma(c), \delta(c))$.

A relação de pesos esféricos dos elementos de $\mathbb{Z}_8$ é dada por:

$$\begin{aligned}
\mathbf{0} &\rightarrow 0 \\
\mathbf{1} &\rightarrow 1 \\
\mathbf{2} &\rightarrow 2 \\
\mathbf{3} &\rightarrow 1 \\
\mathbf{4} &\rightarrow 2 \\
\mathbf{5} &\rightarrow 1 \\
\mathbf{6} &\rightarrow 2 \\
\mathbf{7} &\rightarrow 3
\end{aligned}$$

Analisando se este k-rótulo preserva distâncias, temos que a distância esférica entre os elementos 2 e 1 de $\mathbb{Z}_8$ é

$$d_{ES}(2,1) = w_{ES}(1-2) = w_{ES}(-1) = w_{ES}(7) = 3.$$

Por outro lado,

$$d_H(\phi_3(2), \phi_3(1)) = d_H(001, 101) = 1.$$

Portanto, este mapeamento também não preserva distâncias.

Estes dois exemplos nos mostram que os rotulamentos considerados não são interessantes como técnica de construção de códigos similar a da $\mathbb{Z}_4$-linearidade. De fato, apesar de se verificar que os pesos são preservados não é garantido, em geral, que as distâncias são preservadas.

Esta análise nos levou a duas situações que serão colocadas nas subseções a seguir: a primeira é obter bons códigos 2^k-ários através da escolha adequada de pesos a serem associadas aos elementos de $\mathbb{Z}_{2^k}$. Apresentaremos para $k = 3$ tabelas com estes códigos.

A segunda situação é saber se existe de fato algum mapeamento que, preservando pesos, preservará distâncias.

3.3.4 Tabela de códigos sobre $\mathbb{Z}_8$ com distância esférica

Vamos apresentar nesta subseção códigos sobre $\mathbb{Z}_8$ com distância esférica. Foram obtidos os melhores códigos através da escolha otimizada do melhor rotulamento.

Tais códigos são apresentados nas Tabelas 3.15-3.24 no final deste capítulo e seus dados são organizados como segue:

- n é o comprimento do código octário;
- k é a dimensão do código octário;
- d_{ES} é a distância esférica do código octário;
- rótulo: é o melhor mapeamento encontrado;
- Matriz geradora: é a matriz geradora do código octário.
- Espectro de pesos: é o espectro de pesos do código octário.

Apresentamos também uma tabela com os mesmos parâmetros mas a procura se processou através de códigos cíclicos octários e o resultado se apresenta nas Tabelas 3.25-3.27 no final deste capítulo. Os dados são organizados como segue:

- n é o comprimento do código octário cíclico;
- k é a dimensão do código octário cíclico;
- d é a melhor distância de Lee encontrada para este código octário cíclico que corresponde a distância de Hamming no código binário correspondente;
- d' é a distância correspondente ao código linear de mesmos parâmetros que não é necessariamente cíclico;
- rótulo: é o mapeamento encontrado;
- polinômio gerador: é o polinômio gerador do código encontrado;
- Espectro de Pesos: é o espectro de pesos do código octário cíclico;

Observe que os rótulos definidos nas Subseções 3.3.2 e 3.3.3 não aparecem como os melhores nas tabelas apresentadas.

3.4 Definição da $\mathbb{Z}_{2^k}$-Linearidade e a Não-Existência de Códigos $\mathbb{Z}_{2^k}$-Lineares

Nesta seção iremos apresentar a definição da $\mathbb{Z}_{2^k}$-linearidade ($k > 2$) como extensão da $\mathbb{Z}_4$-linearidade.

O objetivo principal em considerar tal extensão é a de prover uma técnica de construção de bons códigos binários que são imagens de códigos sobre $\mathbb{Z}_{2^k}$. Tais códigos binários são denominados códigos $\mathbb{Z}_{2^k}$-lineares. Por um bom código binário queremos dizer um código geometricamente uniforme no espaço de Hamming, cujos parâmetros (taxa e distância mínima) são pelo menos tão bons quanto os parâmetros de qualquer código linear previamente conhecido.

Por exemplo, os códigos de Kerdock e Preparata são bons códigos neste sentido. Mostraremos, entretanto, que o objetivo principal não poderá ser alcançado.

O aspecto mais importante relacionado à extensão da técnica de construção de bons códigos é o mapeameno ϕ. Assim, a questão que se coloca é a seguinte: Existe um mapeamento

$\phi_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k$ que possa produzir bons códigos binários a partir de códigos lineares sobre $\mathbb{Z}_{2^k}$, $k > 2$.

Em primeiro lugar, como no caso $\mathbb{Z}_4$-linear, precisamos munir $\mathbb{Z}_{2^k}$ de uma métrica d tal que o mapeamento $\phi_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k$ seja uma isometria do espaço métrico $(\mathbb{Z}_{2^k}, d)$ no espaço métrico $(\mathbb{Z}_2^k, d_H)$, onde d_H é a distância de Hamming. Em segundo lugar, necessitamos que o código seja geometricamente uniforme. Esta última condição é muito importante não somente por simplificar a análise de desempenho mas por reduzir significativamente a complexidade de decodificação.

Estas duas propriedades ocorrem se, e somente se, as seguintes igualdades ocorrem:

$$d(u,v) = d_H(\phi_k(u), \phi_k(v)) = d_H(\phi_k(u-v), \phi_k(0)) = d(u-v, 0),$$

para qualquer u, v no código 2^k-ário. Em outras palavras, $\mathbb{Z}_2^k$ interpretado como um conjunto de sinais no espaço de Hamming, deve ser efetivamente casado a $\mathbb{Z}_{2^k}$, através do mapeamento ϕ_k, para que as igualdades anteriores sejam satisfeitas.

Definição 3.4.1 *Seja $(\mathbb{Z}_2^k, d_H)$, $k \geq 2$, o espaço de Hamming k-dimensional. Se $\mathbb{Z}_2^k$ é efetivamente casado com $\mathbb{Z}_{2^k}$ dizemos que existe a $\mathbb{Z}_{2^k}$-linearidade, ou seja, existem códigos $\mathbb{Z}_{2^k}$-lineares $(k \geq 2)$.*

É exatamente esta propriedade que precisamos e que não tínhamos nos casos anteriores. De fato, $\mathbb{Z}_2^k$ sendo casado a $\mathbb{Z}_{2^k}$ implica que os códigos binários obtidos serão geometricamente uniformes.Sabemos que esta condição é equivalente a encontrar um grupo cíclico de ordem 2^k no grupo de simetrias de $\mathbb{Z}_2^k$, o grupo $\Gamma(\mathbb{Z}_2^k)$.

Exemplo 3.4.1 *Se $k = 2$ então $\Gamma(\mathbb{Z}_2^2) \cong \mathbb{D}_4 \supset \mathbb{Z}_4$. Então, temos a $\mathbb{Z}_4$-linearidade.*

Para $k \geq 2$, $\Gamma(\mathbb{Z}_2^k) \cong \mathbb{Z}_2^k \times_\varphi \mathcal{S}_k$ (produto semi-direto). Neste caso, colocamos a seguinte questão: Existe um subgrupo cíclico em $\Gamma(\mathbb{Z}_2^k)$ de ordem 2^k que é isomorfo ao grupo $\mathbb{Z}_{2^k}$?

A seguir, mostraremos que tal subgrupo não existe quando $k > 2$. Em primeiro lugar, provaremos o seguinte lema.

Lema 3.4.1 *Seja $\mathcal{S}_n$ $(n \geq 3)$ o grupo de permutações de n letras. Se σ é um elemento de $\mathcal{S}_n$, então a ordem σ é menor do que 2^{n-1}.*

Demonstração:

A afirmação é óbvia para $n = 3, 4$. Vamos supor $n \geq 5$. Seja $\sigma \in \mathcal{S}_n$, uma permutação não identidade e $O(\sigma)$ a ordem σ. Então, σ é o produto de ciclos disjuntos, ou seja,

$$\sigma = \prod_{i=1}^{s} \sigma_i \neq I$$

onde $\sigma_i = (i_1, i_2, \ldots, i_{n_i})$ são disjuntos com $n \geq n_1 \geq n_2 \geq \ldots \geq n_s \geq 2$.

Por indução em s, para $s = 1$, temos $O(\sigma) = n_1 \leq n < 2^{n-1}$ e a afirmação é verdadeira. Seja $s > 1$ e suponhamos que seja verdadeira para todo r, $1 \leq r \leq s-1$. Neste caso

$$n - n_s \geq 3^2$$

e, então

$$\sigma' = \prod_{i=1}^{s-1} \sigma_i \in S_{n-n_{s+1}},$$

e

$$O(\sigma') < 2^{n-n_s-1}$$

mas

$$\sigma = \sigma'.\sigma_s$$

consequentemente,

$$O(\sigma) \leq O(\sigma').O(\sigma_s) < 2^{n-n_s-1}.n_s < 2^{n-n_s-1}.2^{n_s} = 2^{n-1}.$$

□

Teorema 3.4.1 *O grupo de simetrias de $\mathbb{Z}_2^k$, que é isomorfo a $\mathbb{Z}_2^k \times_\varphi \mathcal{S}_k$, não contém um subgrupo cíclico de ordem 2^k isomorfo a $\mathbb{Z}_{2^k}$.*

Demonstração: *Seja $\varphi : \mathcal{S}_k \to Aut(\mathbb{Z}_2^k)$ um homomorfismo de grupos. Seja (t, P) uma dupla denotando a translação $\mathbb{Z}_2^k$ e a permutação associada à cada elemento de $\mathcal{S}_k$, respectivamente. Para um dado t_1 e P_1, se a dupla (t_1, P_1) for o gerador do subgrupo cíclico deverá ter ordem 2^k. Calculando as potências de $(t_1, P_1) \in \mathbb{Z}_2^k \times_\varphi \mathcal{S}_k$, temos*

$$(t_1, P_1)^2 = (t_1, P_1) \times_\varphi (t_1, P_1) = (t_1 + \varphi(P_1)(t_1), P_1^2)$$

$$(t_1, P_1)^3 = (t_1 + \varphi(P_1)(t_1) + \varphi(P_1^2)(t_1), P_1^3)$$

$$(t_1, P_1)^4 = (t_1 + \varphi(P_1)(t_1) + \varphi(P_1^2)(t_1) + \varphi(P_1^3)(t_1), P_1^4)$$

$$(t_1, P_1)^5 = (t_1 + \varphi(P_1)(t_1) + \varphi(P_1^2)(t_1) + \varphi(P_1^3)(t_1) + \varphi(P_1^4)(t_1), P_1^5)$$

$$\vdots$$

$$(t_1, P_1)^l = (t_1 + \varphi(P_1)(t_1) + \varphi(P_1^2)(t_1) + \varphi(P_1^3)(t_1) + \varphi(P_1^4)(t_1) + \ldots + \varphi(P_1^{l-1})(t_1), P_1^l)$$

Pelo Lema 3.4.1, existe um $m < 2^{k-1}$, tal que

$$P_1^m = I, P_1^{m+1} = P_1, P_1^{m+2} = P_1^2, \ldots, P_1^{2m-1} = P_1^{m-1}.$$

Então

$$\begin{aligned}(t_1, P_1)^{2m} &= (t_1 + \varphi(P_1)(t_1) + \varphi(P_1^2)(t_1) + \varphi(P_1^3)(t_1) + \ldots + \varphi(P_1^{m-1})(t_1) + \\ &\quad + \varphi(P_1^m)(t_1) + \varphi(P_1^{m+1})(t_1) + \varphi(P_1^{m+2})(t_1) + \ldots + \varphi(P_1^{2m-1})(t_1), P_1^{2m}) \\ &= (0, I).\end{aligned}$$

Portanto, todo elemento de $\Gamma\left(\mathbb{Z}_2^k\right) \cong \mathbb{Z}_2^k \times_\varphi \mathcal{S}_k$ tem ordem menor do que 2^k, e daí segue que não existe um subgrupo cíclico de ordem 2^k. □

Apesar de não existir um subgrupo cíclico de ordem 2^k, podem existir outros grupos transitivos de ordem 2^k, que também possam ser interessantes para os objetivos definidos. A existência de subgrupos transitivos não cíclicos será discutida no próximo capítulo.

3.5 Conclusão

Neste capítulo, apresentamos a definição de códigos $\mathbb{Z}_4$-lineares e suas principais propriedades [15]. Isto foi feito na Seção 2 dando ênfase apenas aos aspectos conceituais da $\mathbb{Z}_4$-linearidade. Foi apresentada também uma tabela de códigos quaternários de comprimento ≤ 10 com distância de Lee, utilizando uma técnica de procura computacional por otimização [50] e uma tabela de códigos cíclicos quaternários de comprimento ≤ 10 com a distância de Lee.

Na Seção 3, através das propriedades mais importantes da $\mathbb{Z}_4$-linearidade, analisamos três propostas de extensão para $\mathbb{Z}_{2^k}$-linearidade como técnica de construção de códigos binários de comprimento múltiplo de k. Uma tabela de códigos octários com distância esférica foi apresentada seguindo a mesma técnica de [50], além de uma tabela de códigos cíclicos octários.

Com a escolha apropriada de alguma de suas propriedades estabelecemos as condições necessárias da $\mathbb{Z}_{2^k}$-linearidade para que a mesma possa ser utilizada como uma técnica para construção de códigos binários. Sob estas condições mostramos que não existe a $\mathbb{Z}_{2^k}$-linearidade.

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
2	1	2		paridade	
3	1	3		repetição	
3	2	2		paridade	
4	1	4		repetição	
4	2	4	2312211	6675	0(1) 4(6) 5(24) 6(16) 8(9) 9(8)
				7566	
			2112231	7311	0(1) 4(6) 5(24) 6(16) 8(9) 9(8)
				0354	
			1322112	4750	0(1) 4(6) 5(24) 6(16) 8(9) 9(8)
				3225	
			1122132	3522	0(1) 4(6) 5(24) 6(16) 8(9) 9(8)
				6657	
4	3	2		paridade	
5	1	5		repetição	
5	2	6	2213121	32106	0(1) 6(13) 7(18) 8(9) 9(4) 10(15)
				10667	12(2) 13(2)
			1223121	51460	0(1) 6(13) 7(18) 8(9) 9(4) 10(15)
				23667	12(2) 13(2)
			1213221	42545	0(1) 6(13) 7(18) 8(9) 9(4) 10(15)
				52467	12(2) 13(2)
			1213122	66507	0(1) 6(13) 7(18) 8(9) 9(4) 10(15)
				45021	12(2) 13(2)

Tabela 3.15: Códigos octários obtidos pela técnica de otimização

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
5	3	4	2312211	37410	0(1) 4(22) 5(72) 6(65) 7(92) 8(97)
				45261	9(84) 10(62) 11(4) 12(8) 13(4)
				46173	14(1)
			2112231	60575	0(1) 4(22) 5(72) 6(65) 7(92) 8(97)
				74326	9(84) 10(62) 11(4) 12(8) 13(4)
				55007	14(1)
			1322112	23727	0(1) 4(22) 5(72) 6(65) 7(92) 8(97)
				45277	9(84) 10(62) 11(4) 12(8) 13(4)
				15776	14(1)
			1122132	36274	0(1) 4(22) 5(72) 6(65) 7(92) 8(97)
				37164	9(84) 10(62) 11(4) 12(8) 13(4)
				32777	14(1)
5	4	2		paridade	
6	1	6		repetição	
6	2	8	2312211	163110	0(1) 8(45) 12(18)
				650531	
			2112231	355304	0(1) 8(45) 12(18)
				227517	
			1322112	740755	0(1) 8(45) 12(18)
				653536	
			1122132	255754	0(1) 8(45) 12(18)
				754677	
6	3	6	1223121	210504	0(2) 6(40) 7(74) 8(52) 9(42)
				222600	10(108) 11(76) 12(46) 13(46)
				442176	14(20) 15(2) 16(4)
			1213122	406442	0(2) 6(42) 7(120) 8(104) 9(52)
				115377	10(52) 11(56) 12(38) 13(28)
				527347	14(16) 18(2)

Tabela 3.16: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
6	4	4	2312211	367302	0(1) 4(57) 5(176) 6(299) 7(384)
				671520	8(667) 9(928) 10(667) 11(384)
				45434	12(299) 13(176) 14(57) 18(1)
				677405	
			1322112	445552	0(1) 4(57) 5(176) 6(299) 7(384)
				326231	8(667) 9(928) 10(667) 11(384)
				372770	12(299) 13(176) 14(57) 18(1)
				523070	
			1122132	307632	0(1) 4(57) 5(176) 6(299) 7(384)
				746736	8(667) 9(928) 10(667) 11(384)
				774677	12(299) 13(176) 14(57) 18(1)
				157724	
			2312211	367302	0(1) 4(57) 5(176) 6(299) 7(384)
				671520	8(667) 9(928) 10(667) 11(384)
				045434	12(299) 13(176) 14(57) 18(1)
				677405	
6	5	2		paridade	
7	1	7		repetição	
7	2	9	2213121	1631634	0(1) 9(16) 10(10) 11(14) 12(11)
				3056661	13(4) 14(2) 15(4) 17(2)
			1213221	5625776	0(1) 9(16) 10(10) 11(14) 12(11)
				3470456	13(4) 14(2) 15(4) 17(2)
			1213122	6667557	0(1) 9(16) 10(10) 11(14) 12(11)
				766365	13(4) 14(2) 15(4) 17(2)
			1223121	2605727	0(1) 9(16) 10(10) 11(14) 12(11)
				1424330	13(4) 14(2) 15(4) 17(2)

Tabela 3.17: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
7	3	8	2112231	4647731	0(1) 8(196) 10(56) 12(196) 14(56)
				5034156	16(7)
				7745764	
			1322112	7155640	0(1) 8(196) 10(56) 12(196) 14(56)
				1474125	16(7)
				2750510	
7	4	5	2312211	1063672	0(1) 5(21) 6(154) 7(318) 8(308)
				5566613	9(462) 10(756) 11(700) 12(588)
				3236603	13(462) 14(178) 15(70)
				7612156	16(63) 17(14) 21(1)
			1122132	7771620	0(1) 5(21) 6(154) 7(318) 8(308)
				1357131	9(462) 10(756) 11(700) 12(588)
				7454436	13(462) 14(178) 15(70)
				7740235	16(63) 17(14) 21(1)
7	5	4	01322121	3130072	0(1) 4(155) 5(245) 6(1024)
				715731	7(1559) 8(3155) 9(4804) 10(5572)
				2634045	11(5292) 12(4595) 13(3436)
				4424370	14(1665) 15(790) 16(321))
				3361344	17(127) 18(23) 19(3) 20(1)
			1312122	3266304	0(1) 4(155) 5(245) 6(1024) 7(1559) 8(3155)
7	6	2		paridade	9(4804) 10(5572) 11(5292) 12(4595) 13(3436)
8	1	8		repetição	14(1665) 15(790) 16(321) 17(127) 18(23) 19(3) 20(1)

Tabela 3.18: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
8	2	11	2213211	40317665	0(1) 11(16) 12(30) 13(16) 24(1)
				75351357	
			2113221	71335755	0(1) 11(16) 12(30) 13(16) 24(1)
				37142250	
			1223112	55775177	0(1) 11(16) 12(30) 13(16) 24(1)
				46077561	
			1123122	40366571	0(1) 11(16) 12(30) 13(16) 24(1)
				57157375	
8	3	8	2213121	52167346	0(1) 8(12) 9(71) 10(59) 11(66)
				60276017	12(79) 13(73) 14(47) 15(50)
				66143031	16(20) 17(25) 18(6) 21(3)
			1213221	14371662	0(1) 8(12) 9(71) 10(59) 11(66)
				13504647	12(79) 13(73) 14(47) 15(50)
				77353763	16(20) 17(25) 18(6) 21(3)
			1223121	31562700	0(1) 8(12) 9(66) 10(39) 11(74)
				32261724	12(83) 13(48) 14(54) 15(78)
				35042007	16(25) 17(22) 18(7) 20(3)
			1213122	44421510	0(1) 8(12) 9(66) 10(39) 11(74)
				64234723	12(83) 13(48) 14(54) 15(78)
				66547507	16(25) 17(22) 18(7) 20(3)
8	4	6	2213121	67047655	0(1) 6(4) 7(48) 8(321) 9(432)
				2627652	10(436) 11(448) 12(788) 13(400)
				34506000	14(468) 15(384) 16(241) 17(64)
				40235576	18(36) 19(16) 20(8) 24(1)
			1223121	47566433	0(1) 6(4) 7(50) 8(321) 9(426)
				22256160	10(407) 11(517) 12(713) 13(455)
				56407233	14(495) 15(359) 16(192) 17(91)
				57361015	18(34) 19(22) 20(8) 24(1)

Tabela 3.19: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
			1213221	52042603	0(1) 6(4) 7(48) 8(321) 9(432)
				45567742	10(436) 11(448) 12(788) 13(400)
				6650270	14(468) 15(384) 16(241) 17(64)
				53657453	18(36) 19(16) 20(8) 24(1)
			1213122	21600067	0(1) 6(4) 7(48) 8(321) 9(432)
				10117556	10(436) 11(448) 12(788) 13(400)
				53152545	14(468) 15(384) 16(241) 17(64)
				52366422	18(36) 19(16) 20(8) 24(1)
8	5	5	2213211	36351743	0(1) 5(56) 6(460) 7(592) 8(1073)
				70243767	9(3440) 10(2988) 11(3976)
				20355706	12(7596) 13(3976) 14(2988)
				31126744	15(3440) 16(1073) 17(592)
				25736454	18(460) 19(56) 24(1)
			2113221	26145217	0(1) 5(56) 6(460) 7(592) 8(1073)
				72651542	9(3440) 10(2988) 11(3976)
				57517555	12(7596) 13(3976) 14(2988)
				41716247	15(3440) 16(1073) 17(592)
				31555454	18(460) 19(56) 24(1)
			1223112	55233550	0(1) 5(56) 6(460) 7(592) 8(1073)
				65154250	9(3440) 10(2988) 11(3976)
				76442777	12(7596) 13(3976) 14(2988)
				53764250	15(3440) 16(1073) 17(592)
				45777060	18(460) 19(56) 24(1)
			1123122	65243152	0(1) 5(56) 6(460) 7(592) 8(1073)
				51240103	9(3440) 10(2988) 11(3976)
				74772036	12(7596) 13(3976) 14(2988)
				53553357	15(3440) 16(1073) 17(592)
				73743435	18(460) 19(56) 24(1)

Tabela 3.20: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
8	6	3	2213121	25323017	0(2) 3(2) 4(148) 5(854) 6(2156)
				67774325	7(4948) 8(11880) 9(20144)
				47304616	10(30064) 11(40244) 12(41570)
				47272025	13(39008) 14(31752) 15(19884)
				35575167	16(11010) 17(5392) 18(1968)
				74204445	19(810) 20(238) 21(42) 22(28)
8	7	2		paridade	
9	1	9		repetição	
9	2	12	2213121	620632557	0(1) 12(9) 13(12) 14(18) 15(12)
				216067617	16(6) 20(6)
			1223121	734401616	0(1) 12(9) 13(12) 14(18) 15(12)
				321632210	16(6) 20(6)
			1213221	666235075	0(1) 12(9) 13(12) 14(18) 15(12)
				507665636	16(6) 20(6)
			1213122	725260576	0(1) 12(9) 13(12) 14(18) 15(12)
				61472475	16(6) 20(6)
9	3	9	2213211	554117426	0(1) 9(1) 10(54) 11(75) 12(83)
				125330734	13(75) 14(48) 15(41) 16(45)
				650701357	17(57) 18(24) 19(6) 21(1) 24(1)
			2113221	255115706	0(1) 9(1) 10(54) 11(75) 12(83)
				420671001	13(75) 14(48) 15(41) 16(45)
				352336477	17(57) 18(24) 19(6) 21(1) 24(1)
			1123122	764070575	0(1) 9(1) 10(54) 11(75) 12(83)
				542357714	13(75) 14(48) 15(41) 16(45)
				53766155	17(57) 18(24) 19(6) 21(1) 24(1)
			2213211	554117426	0(1) 9(1) 10(54) 11(75) 12(83)
				125330734	13(75) 14(48) 15(41) 16(45)
				650701357	17(57) 18(24) 19(6) 21(1) 24(1)

Tabela 3.21: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
9	4	7	2213121	134706254	0(1) 8(54) 9(233) 10(320)
				267457060	11(421) 12(463) 13(583) 14(545)
				427622127	15(547) 16(313) 17(336) 18(147)
				356417660	19(96) 20(12) 21(20) 23(4) 24(1)
			1223121	342421167	0(1) 8(54) 9(233) 10(320)
				341567113	11(421) 12(463) 13(583) 14(545)
				10271247	15(547) 16(313) 17(336) 18(147)
				257532400	19(96) 20(12) 21(20) 23(4) 24(1)
			1213221	673135033	0(1) 8(54) 9(233) 10(320)
				47025010	11(421) 12(463) 13(583) 14(545)
				751556355	15(547) 16(313) 17(336) 18(147)
				321017555	19(96) 20(12) 21(20) 23(4) 24(1)
			1213122	145535516	0(1) 8(54) 9(233) 10(320)
				245366434	11(421) 12(463) 13(583) 14(545)
				314070421	15(547) 16(313) 17(336) 18(147)
				713377325	19(96) 20(12) 21(20) 23(4) 24(1)
9	5	6	2213121	417473376	0(1) 6(44) 7(297) 8(601) 9(1122) 10(2089)
				300746423	11(3165) 12(4217) 13(4990) 14(5051)
				2301660	15(4008) 16(2931)17(1981) 18(1214) 19(657)
				470100625	20(260) 21(95) 22(38)23(4) 24(2) 27(1)
				774016743	
			1213122	777011642	0(1) 6(44) 7(289) 8(625) 9(1106) 10(2081)
				566307351	11(3165) 12(4225) 13(5014) 14(5003)
				146111201	15(4032) 16(2939)17(1981) 18(1206)
				771275617	19(641) 20(284) 21(87) 22(38)
				353167065	23(4) 24(2) 27(1)

Tabela 3.22: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
9	8	2		paridade	
10	1	10		repetição	
10	2	13	2213211	7476015326	0(1) 13(6) 14(15) 15(24) 16(11) 17(2)
				7513371175	18(4) 30(1)
			2113221	4553361046	0(1) 13(6) 14(15) 15(24) 16(11) 17(2)
				3577177711	18(4) 30(1)
			1223112	7146403565	0(1) 13(6) 14(15) 15(24) 16(11) 17(2)
				7717735751	18(4) 30(1)
			1123122	516721534	0(1) 13(6) 14(23) 15(12) 16(13) 18(3)
				7437072155	19(4) 21(2)
10	3	11	1213221	4015666767	0(1) 11(12) 12(65) 13(46) 14(79) 15(57)
				6067423156	16(44) 17(56) 18(46) 19(44) 20(44) 21(10)
				6127041047	22(1) 23(7)
			1213122	2256453247	0(1) 11(12) 12(65) 13(46) 14(79) 15(57)
				2052652374	16(44) 17(56) 18(46) 19(44) 20(44) 21(10)
				235420471	22(1) 23(7)
10	4	8	2312211	5447403114	0(1) 8(3) 9(58) 10(148) 11(217) 12(369)
				30755431	13(425) 14(534) 15(575) 16(546) 17(475)
				4445144577	18(328)19(223) 20(103) 21(63)
				540274175	22(14) 23(9) 24(2)25(3)
10	5	7	2312211	4442437534	0(1) 7(6) 8(359) 9(228) 10(1198) 11(1212)
				770706216	12(3326) 13(2868) 14(5306) 15(3720)
				4321470115	16(5461) 17(2796)18(3238) 19(1188) 20(1306)
				1670414166	21(252) 22(238) 23(18)24(43) 26(4)
				6455206552	

Tabela 3.23: Códigos octários obtidos pela técnica de otimização (cont.)

n	k	d_{ES}	mapeamento	m.geradora	espectro de pesos
10	6	6	2213121	1756327443	0(1) 6(189) 7(462) 8(1701) 9(3256) 10(7130)
				3164411574	11(13627) 12(20940) 13(29045) 14(36242)
				6603444331	15(37530) 16(35072)17(29519) 18(21170)
				5023276074	19(13231) 20(7598) 21(3387) 22(1341)
				6021254077	23(486) 24(168) 25(17) 26(32)
				5042511453	
10	7	4	2213121	102306064	0(1) 4(17) 5(344) 6(1257) 7(3903) 8(11280)
				2377124173	9(27896) 10(59418) 11(105528) 12(168783)
				106434052	13(234733)14(282227) 15(305084) 16(285435)
				4421553240	17(232287) 18(169672)19(106950) 20(56864)
				1232331616	21(27963) 22(11654) 23(4005)
				776566647	24(1394) 25(377) 26(60) 27(18) 28(2)
				7733071515	
10	9	2		paridade	

Tabela 3.24: Códigos octários obtidos pela técnica de otimização (cont.)

n	**k**	**d**	**d'**	**mapeamento**	pol. gerador	**espectro de pesos**
2	1	2	2		paridade	
3	1	3	3		repetição	
3	2	2	2		paridade	
4	1	4	4		repetição	
4	2	4	4	01122132	5470	0(1) 4(6) 5(24) 6(16) 8(9) 9(8)
				01322112	5470	
				02112231	5470	
				02312211	5470	
4	3	2	2		paridade	
5	1	5	5		repetição	
5	2					Não existe código cíclico com estes parâmetros.
5	3					Não existe código cíclico com estes parâmetros.
5	4	2	2		paridade	
6	1	6	6		repetição	
6	2	8	8	01122132	514770	0(1) 8(45) 12(18)
				01322112		
				02112231		
				02312211		
6	3	5	6	02213121	126700	0(1) 5(24) 6(35) 7(78) 8(84) 9(68) 10(120)
				01223121		11(30) 12(35) 13(24) 14(12) 18(1)
				01213221		
				01213122		
6	4	3	4	02213121	531000	0(1) 3(12) 4(42) 5(132) 6(330) 7(510) 8(609)
				01223121		9(752) 10(723) 11(492) 12(318) 13(132)
				01213221		
				01213122		

Tabela 3.25: Códigos octários cíclicos obtidos por procura computacional exaustiva

n	**k**	**d**	**d′**	**mapeamento**	pol. gerador	**espectro de pesos**
6	5	2	2		paridade	
7	1	7	7		repetição	
7	2	9	9			Não existe código cíclico com estes parâmetros.
7	3	8	8	02112231	1572100	0(1) 8(196) 10(56) 12(196) 14(56) 16(7)
				01322112		
7	4	5	5	02312211	7231000	0(1) 5(21) 6(154) 7(318) 8(308) 9(462)
				01122132		10(756) 11(700) 12(588) 13(462) 14(178) 15(70)
7	5					Não existe código cíclico com estes parâmetros.
7	6	2	2		paridade	
8	1	8	8		repetição	
8	2	10	11	02223111	56541210	0(1) 10(12) 12(38) 14(12) 24(1)
				01223211		
				02123121		
				01123221		
				02213112		
				01213212		
				02113122		
				01113222		
8	3	8	8	02312211	71403100	0(1) 8(103) 10(64) 12(176) 14(64)
				02112231		16(103) 24(1)
				01322112		
				01122132		

Tabela 3.26: Códigos octários cíclicos obtidos por procura computacional exaustiva (cont.)

n	**k**	**d**	**d'**	**mapeamento**	pol. gerador	**espectro de pesos**
8	4	4	6	02312121	34401000	0(1) 4(4) 5(8) 6(96) 7(192) 8(230)
				01322121		9(248) 10(352) 11(584) 12(684) 13(568) 14(376)
				01312221		13(568) 14(376)
				02212131		
				01222131		
				01212231		
				01312122		
				01212132		
8	5	4	5	02312211	71310000	0(1) 4(12) 5(48) 6(384) 7(336) 8(2407) 9(1264)
				02112231		10(5120) 11(2448) 12(8728) 13(2448)
				01322112		14(5120) 15(1264) 16(2407) 17(336) 18(384)
				01122132		19(48) 20(12) 24(1)
8	7	2	2		paridade	

Tabela 3.27: Códigos octários cíclicos obtidos por procura computacional exaustiva (cont.)

Capítulo 4

$\mathbb{G}$-Linearidade

4.1 Introdução

No Capítulo 3, apresentamos o conceito da $\mathbb{Z}_{2^k}$-linearidade como extensão da $\mathbb{Z}_4$-linearidade. Sob as mesmas condições que a da $\mathbb{Z}_{2^k}$-linearidade, estabeleceremos neste capítulo o conceito da $\mathbb{G}$-linearidade, onde $\mathbb{G}$ é um grupo, como sendo a extensão da $\mathbb{Z}_{2^k}$-linearidade. Veremos também que a existência da $\mathbb{G}$-linearidade, sob o ponto de vista da construção de códigos geometricamente uniformes, está vinculada à determinação do grupo de simetrias do conjunto de sinais associado.

De fato, revendo o caso $\mathbb{Z}_4$, observamos que o mapeamento ϕ foi obtido com a característica de associar um código quaternário linear a um código binário que, mesmo não sendo necessariamente linear, satisfaz a propriedade de que o perfil de distâncias é o mesmo para qualquer palavra-código considerada. Em outras palavras, o mapeamento da $\mathbb{Z}_4$-linearidade transportou de uma forma bastante sutil para o código binário a "linearidade" do código quaternário. Esta propriedade é uma consequência imediata da uniformidade geométrica do código binário.

Para que esta condição seja satisfeita, é necessário que a distância de Lee seja compatível com a operação do grupo $\mathbb{Z}_4$ e que haja uma isometria entre os espaços considerados. Isto implica diretamente na propriedade de casamento (no sentido proposto por Loeliger [43]) entre o grupo $\mathbb{Z}_4$ e o conjunto de sinais $\mathbb{Z}_2^2 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Mais precisamente, considere $\mathbb{Z}_2^2$ como o espaço métrico de Hamming bidimensional de ordem 2. Note que a propriedade relevante neste caso é o casamento efetivo entre $\mathbb{Z}_4$ e $\mathbb{Z}_2^2$. Então pelo Teorema 2.4.7, temos que esta propriedade é equivalente a encontrar o grupo de simetrias do conjunto de sinais $\mathbb{Z}_2^2$. O grupo de simetrias de $\mathbb{Z}_2^2$ é o grupo diedral de ordem 8, $\mathbb{D}_4$, que possui um subgrupo cíclico de ordem 4 isomorfo a $\mathbb{Z}_4$.

Então do Teorema 2.4.7, temos que $\mathbb{Z}_2^2$ é casado a $\mathbb{Z}_4$ e a função

$$\mu_{\mathbb{Z}_2^2} : \mathbb{Z}_4 \to \mathbb{Z}_2^2, \quad \mu_{\mathbb{Z}_2^2}(f) = f(s)$$

é um rotulamento casado para todo $s \in \mathbb{Z}_2^2$. Escolhendo o ponto inicial $s = (0,0)$ obtemos o rotulamento isométrico:

0	0	0
1	1	0
2	1	1
3	0	1

Tabela 4.1: Mapeamento por rotulamento isométrico

A escolha do ponto inicial dependerá da aplicação sendo considerada. No caso em consideração, isto é, $\mathbb{Z}_4$ e $\mathbb{Z}_2^2$, o interesse é relacionar códigos sobre $\mathbb{Z}_4$ com códigos sobre $\mathbb{Z}_2^2$. Como em $\mathbb{Z}_4$ a distância de interesse é a distância de Lee e em $\mathbb{Z}_2^2$ a distância natural é a distância de Hamming vemos que o rotulamento preserva o perfil de distâncias e o peso de cada elemento em cada espaço. Assim temos uma isometria entre os espaços métricos $(\mathbb{Z}_4, d_{Lee})$ e $(\mathbb{Z}_2^2, d_H)$.

Vemos assim que a $\mathbb{G}$-linearidade, quando utilizada na obtenção de códigos geometricamente uniformes, está vinculada ao fato de que o grupo $\mathbb{G}$ seja um subgrupo do grupo de simetrias correspondente ao conjunto de sinais de interesse.

Este capítulo está organizado da seguinte maneira. Na Seção 4.2 apresentaremos a definição de $\mathbb{G}$-linearidade e exemplos que incluem a $\mathbb{Z}_4$-linearidade e a $\mathbb{Z}_{2^k}$-linearidade como casos particulares.

Na Seção 4.3, faremos um estudo do grupo de simetrias do espaço de Lee $\mathbb{Z}_q^n, q \geq 2, n \geq 2$.

Na Seção 4.4, estabeleceremos a $\mathbb{Z}_{q^n}$-linearidade associada a $\mathbb{Z}_q^n$ através do estudo dos subgrupos cíclicos de ordem q^n de seu grupo de simetrias.

Na Seção 4.5, apresentaremos alguns casos especiais como exemplos da $\mathbb{G}$-linearidade.

Na Seção 4.6, apresentaremos as conclusões do capítulo.

4.2 $\mathbb{G}$-Linearidade

Todos os códigos binários não-lineares estudados em [15] são imagens de códigos lineares sobre $\mathbb{Z}_4$ através de um mapeamento adequado.

Para estender este mapeamento para alfabetos não necessariamente binários precisamos conhecer a estrutura do domínio e da imagem do mapeamento $\phi : \mathbb{Z}_4^n \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}_2)^n$. Desse modo, temos as seguintes considerações:

- O domínio básico $\mathbb{Z}_4$ será visto como um grupo e a distância de Lee associada a $\mathbb{Z}_4$ é compatível com sua estrutura de grupo, ou seja, é uma métrica de grupo em $\mathbb{Z}_4$.
- A imagem básica $\mathbb{Z}_2 \times \mathbb{Z}_2$ será vista como um espaço métrico onde a métrica associada é a métrica de Hamming.

Tendo como base estas considerações, a questão que se coloca é a seguinte: para um grupo $\mathbb{G}$ (como o $\mathbb{Z}_4$) e um espaço métrico $\mathbb{M}$ (como o $\mathbb{Z}_2 \times \mathbb{Z}_2$) quais devem ser as condições de existência do mapeamento $\phi : \mathbb{G}^n \rightarrow \mathbb{M}^n$, como no caso da $\mathbb{Z}_4$-linearidade?

A resposta a esta questão poderá fornecer uma técnica de construção de classes de códigos geometricamente uniformes sobre o alfabeto $\mathbb{M}$, através de códigos de grupo sobre o grupo $\mathbb{G}$. Além de ser possível a construção de códigos sob uma determinada estrutura algébrica a partir de códigos sob uma estrutura mais adequada, permitirá também fornecer uma técnica de associação das palavras-códigos aos elementos do conjunto de sinais.

Considerando o mesmo procedimento que no caso $\mathbb{Z}_4$, iremos estabelecer condições suficientes para que um código $\mathbb{C}$, sobre um alfabeto $\mathcal{A}$, seja geometricamente uniforme, mesmo que este não seja linear. Esta última condição deverá ser herdada do código de grupo sobre o grupo $\mathbb{G}$.

Estas considerações nos levam a seguinte definição.

Definição 4.2.1 *Sejam $\mathbb{G}$ um grupo, d uma métrica de grupo em $\mathbb{G}$ e $\mathbb{C}$ um código de comprimento n sobre o alfabeto $\mathcal{A}$ e cuja métrica é d'. Diremos que $\mathbb{C}$ é* **$\mathbb{G}$-linear se $\mathbb{C}$, ou um código equivalente $\mathbb{C}'$, for imagem de um código de grupo C sobre o grupo $\mathbb{G}$, isto é, $\mathbb{C} = \phi(C)$, onde $\phi : \mathbb{G}^n \to \mathcal{A}^n$ é uma isometria entre os espaços métricos.**

Com esta definição, temos as seguintes propriedades do código $\mathbb{C}$:

Proposição 4.2.1 *Se um código $\mathbb{C}$ é $\mathbb{G}$-linear, então:*

1. *O alfabeto $\mathcal{A}$ está efetivamente casado ao grupo $\mathbb{G}$, e consequentemente, o código $\mathbb{C}$ está casado ao código de grupo correspondente obtido pelo mapeamento estendido.*

2. *O código $\mathbb{C}$ é geometricamente uniforme.*

Demonstração:

1. *Como d' é uma métrica de grupo em $\mathbb{G}$*

$$d'(\phi(x), \phi(y)) = d(x, y) = d(x * y^{-1}, 0) = d'(\phi(x * y^{-1}), \phi(0)).$$

Como ϕ é uma bijeção, o mapeamento ϕ é um rotulamento efetivamente casado.

2. *Seja C um código de grupo sobre o grupo $\mathbb{G}$, tal que $\mathbb{C} = \phi(C)$. Como $\mathbb{C}$ é efetivamente casado a C, temos que C é isomorfo a um subgrupo transitivo do grupo de simetrias de $\mathbb{C}$. Portanto, $\mathbb{C}$ é geometricamente uniforme.*□

Encontrar o mapeamento $\phi : \mathbb{G} \to \mathcal{A}$ é, em princípio, um problema difícil. Todavia, como o alfabeto $\mathcal{A}$ está casado ao grupo $\mathbb{G}$ e ϕ é uma bijeção, a procura por este mapeamento é equivalente a determinar um subgrupo transitivo isomorfo ao grupo de simetrias de $\mathcal{A}$ conforme o Teorema 2.4.7

Exemplo 4.2.1 *Seja $(\mathbb{Z}_2^2, d_H)$ o espaço métrico como mostra a Fig. 4.1. Este é o espaço de Hamming bidimensional. Assim, o grupo de simetrias de $\mathbb{Z}_2^2$ é*

$$\Gamma(\mathbb{Z}_2^2) \cong \mathbb{D}_4 \supseteq \mathbb{Z}_4.$$

Além disso, $\mathbb{Z}_4$ é transitivo sobre $\mathbb{Z}_2^2$ e, portanto, $\mathbb{Z}_2^2$ está efetivamente casado a $\mathbb{Z}_4$. Se em $\mathbb{Z}_4$ utilizarmos a métrica de Lee, então concluímos que $(\mathbb{Z}_4, d_L)$ é isométrico a $(\mathbb{Z}_2^2, d_H)$ segundo o rótulo escolhido a partir do ponto inicial $(0,0)$. Portanto, existem códigos $\mathbb{Z}_4$-lineares. Em [15], algumas classes importantes de códigos binários não-lineares são obtidas através de códigos quaternários lineares.

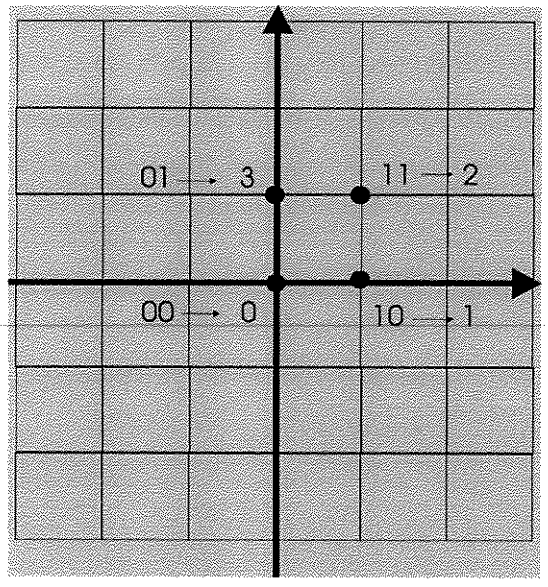

Figura 4.1: Rotulamento do espaço de Hamming bidimensional de ordem 2

Exemplo 4.2.2 *Seja $(\mathbb{Z}_2^k, d_H)$ o conjunto de sinais constituindo o espaço de Hamming k-dimensional. Assim, o grupo de simetrias de $\mathbb{Z}_2^k$ é*

$$\Gamma(\mathbb{Z}_2^k) \cong \mathbb{Z}_2^k \times_\varphi \mathcal{S}_k.$$

Como vimos no Capítulo 3, $\Gamma(\mathbb{Z}_2^k)$ não contém um subgrupo transitivo e cíclico de ordem 2^k. Desta forma, não existem códigos $\mathbb{Z}_{2^k}$-lineares.

Exemplo 4.2.3 *No Exemplo 4.2.2 vimos que não existe um subgrupo transitivo cíclico de ordem 2^k no grupo de simetrias de $(\mathbb{Z}_2^k, d_H)$. Porém, $\Gamma(\mathbb{Z}_2^3)$ possui dois subgrupos transitivos de ordem 8: um é abeliano não-cíclico isomorfo ao produto direto $\mathbb{Z}_4 \times \mathbb{Z}_2$, o outro é não-abeliano isomorfo ao grupo diedral $\mathbb{D}_4$. Vamos estudar estes dois casos.*

- *Caso $\mathbb{Z}_4 \times \mathbb{Z}_2$. Considere o subgrupo de $\Gamma(\mathbb{Z}_2^3)$ gerado pelas simetrias obtidas por uma rotação de $\frac{\pi}{2}$ em torno do eixo paralelo ao eixo oz e passando pelo centro de gravidade do cubo e por uma reflexão em relação ao plano xOy passando pelo centro de gravidade do cubo (como mostra a Fig. 4.2). Estas duas simetrias geram um subgrupo isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$. A representação matricial deste grupo tem como geradores as matrizes*

$$Ro = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad e \quad Re = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

A primeira gera as rotações e a segunda corresponde à reflexão. O mapeamento de $\mathbb{Z}_4 \times \mathbb{Z}_2$ em $\mathbb{Z}_2^3$ é apresentado na Fig. 4.3.

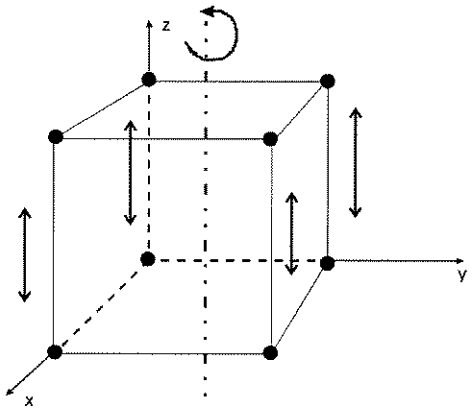

Figura 4.2: Simetrias do cubo que geram o grupo transitivo abeliano

- *Caso $\mathbb{D}_4$. Considere o subgrupo de $\Gamma(\mathbb{Z}_2^3)$ gerado pelas simetrias obtidas por uma rotação de $\frac{\pi}{2}$ em torno do eixo paralelo ao eixo oz e passando pelo centro de gravidade do cubo*

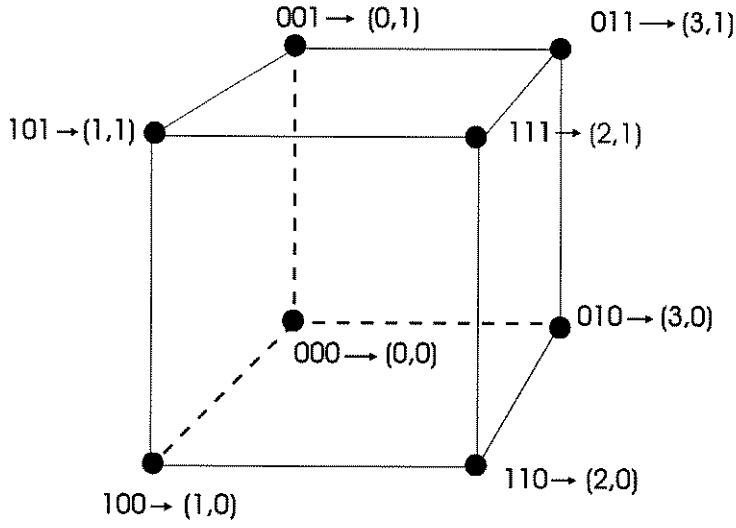

Figura 4.3: Espaço de Hamming tridimensional rotulado por $\mathbb{Z}_4 \times \mathbb{Z}_2$.

e por uma rotação de π em torno do eixo paralelo ao eixo oy passando pelo centro de gravidade do cubo (como mostra a Fig. 4.4). Estas duas simetrias geram um subgrupo isomorfo a $\mathbb{D}_4$. A representação matricial deste grupo tem como geradores as matrizes

$$Ro(\frac{\pi}{2}, oz) = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad e \quad Ro(\pi, oy) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

O mapeamento de $\mathbb{D}_4$ em $\mathbb{Z}_2^3$ é apresentado na Fig. 4.5.

Obtém-se também $\mathbb{D}_4$ por simetrias dadas por uma rotação de $\frac{\pi}{2}$ em torno do eixo paralelo a eixo oz e passando pelo centro de gravidade do cubo e por uma rotação de π em torno do eixo que passa pelos pontos médios de duas arestas paralelas do cubo como mostra a Fig. 4.6. Estes são os únicos subgrupos transitivos não-triviais do grupo de simetrias $\Gamma(\mathbb{Z}_2^3)$, a menos de um isomorfismo. De fato, os subgrupos transitivos deverão ser de ordem 8 e temos 5 grupos não isomorfos de ordem 8: um cíclico, dois abelianos isomorfos a $\mathbb{Z}_2^3$ ou $\mathbb{Z}_4 \times \mathbb{Z}_2$, o diedral e os quatérnios. Já foi demonstrado que o o grupo cíclico não é subgrupo. Quanto aos quatérnios observamos que ele possui um elemento de ordem 2 e cinco elementos de ordem 4.

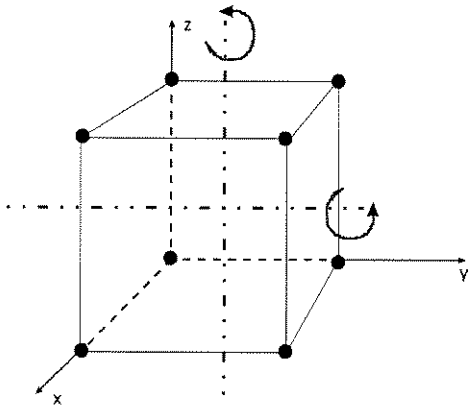

Figura 4.4: Simetrias do cubo que geram o grupo diedral

Os elementos de ordem 4 no grupo de simetrias do cubo são dados por rotações de $\frac{\pi}{2}$ em torno do eixos paralelos aos eixos ox, oy e oz. Qualquer subgrupo que contenha cinco elementos de ordem 4 deverá conter pelo menos duas destas rotações e isto implica na existência de mais elementos de ordem 2. Logo o grupo dos quatérnios não poderá ser um subgrupo transitivo de $\Gamma(\mathbb{Z}_2^3)$. Portanto, temos que os únicos subgrupos transitivos não triviais de $\Gamma(\mathbb{Z}_2^3)$ são o grupo diedral e o grupo abeliano $\mathbb{Z}_4 \times \mathbb{Z}_2$. Utilizando a métrica induzida por d_H em cada um desses subgrupos temos como consequência uma métrica de grupo na qual é possível construir códigos de grupo. Mais adiante, apresentaremos subgrupos transitivos abelianos não-cíclicos de ordem 2^k do grupo de simetrias de $(\mathbb{Z}_2^k, d_H)$ que estendem o procedimento utilizado neste exemplo.

4.3 Grupo de Simetrias do Espaço de Lee $\mathbb{Z}_q^n$

Da seção anterior, fica bastante clara a importância do conhecimento do grupo de simetrias de um alfabeto. Além disso, se este alfabeto possui uma estrutura algébrica associada, então é mais interessante para aplicações em codificação e/ou modulação. Este é o caso do espaço de Lee n-dimensional de ordem q, $(\mathbb{Z}_q^n, d_L)$. Este espaço contém o espaço de Hamming n-dimensional como caso particular, pois a métrica de Hamming coincide com a métrica de Lee para $q = 2$ e $q = 3$. Este espaço métrico constitui um objeto importante de estudo, dado que sua métrica

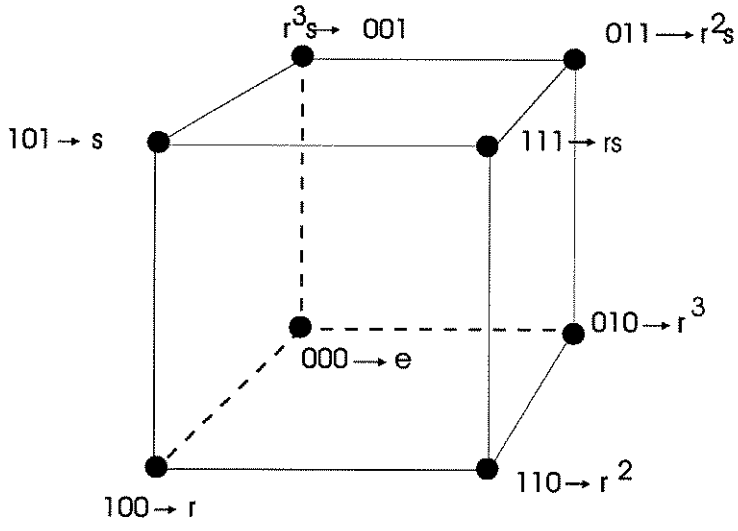

Figura 4.5: Espaço de Hamming tridimensional rotulado por $\mathbb{D}_4$.

é adequada para problemas de codificação e modulação sobre $\mathbb{Z}_q$, q um primo ou potência de primo.

Desta forma, é um espaço métrico que merece um estudo detalhado de seu grupo de simetrias para que possamos investigar a existência ou não de códigos $\mathbb{G}$-lineares sobre um alfabeto q-ário.

4.3.1 Definição e propriedades

No grupo $(\mathbb{Z}_q, \oplus)$, definimos uma métrica que respeita a natureza da operação '$\oplus$' no conjunto $\mathbb{Z}_q$ constituindo a forma mais adequada de análise de um código q-ário, assim como determina a capacidade de correção de erros deste código. No que segue, apresentaremos as definições e propriedades que se referem ao espaço de Lee.

Definição 4.3.1 *A distância de Lee entre dois pontos a e $b \in \mathbb{Z}_q$ é dada pela função d_{Lee} : $\mathbb{Z}_q \times \mathbb{Z}_q \rightarrow R$, definida por*

$$d_{Lee}(a,b) = w_{Lee}(a \ominus b),\ a,b \in \mathbb{Z}_q$$

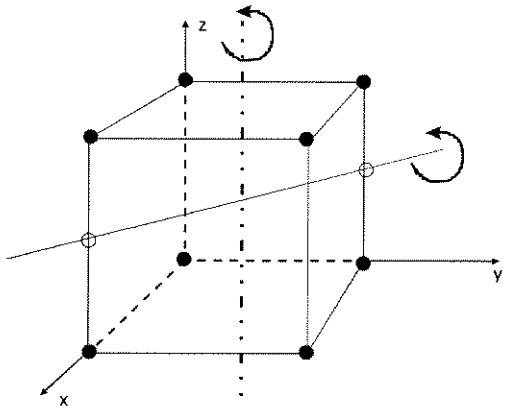

Figura 4.6: Outras simetrias do cubo que geram o grupo diedral

onde $w_{Lee} : \mathbb{Z}_q \to \mathbb{R}$ *é dado por*

$$w_{Lee}(a) = \begin{cases} a, & se \quad a \leq \left\lfloor \frac{q}{2} \right\rfloor \\ q - a, & se \quad a > \left\lfloor \frac{q}{2} \right\rfloor \end{cases}, \tag{4.1}$$

onde $\lfloor x \rfloor$ *denota o maior inteiro menor ou igual a* x*. A função* w_{Lee} *é denominada peso de Lee do ponto* $a \in \mathbb{Z}_q$*.*

Observe que no lado esquerdo da igualdade (4.1), a é um número inteiro entre 0 e $q-1$ que é um representante de classe que pertence ao conjunto $\mathbb{Z}_q$. Antes de calcular o peso de Lee devemos ter como representante de classe este elemento.

A propriedade constante no Lema 4.3.1 permitirá a demonstração do fato de que a distância de Lee d_{Lee} é uma métrica em $\mathbb{Z}_q$.

Lema 4.3.1 *O peso de Lee,* w_{Lee}*, satisfaz as seguintes propriedades:*

1. $w_{Lee}(a) = 0 \Leftrightarrow a = 0, \forall a \in \mathbb{Z}_q$;
2. $w_{Lee}(\ominus a) = w_{Lee}(a), \forall a \in \mathbb{Z}_q$;
3. $w_{Lee}(a \oplus b) \leq w_{Lee}(a) + w_{Lee}(b), \forall a, b \in \mathbb{Z}_q$.

Demonstração:1. Imediata.

2. Seja $a \in \mathbb{Z}_q$,

$$w_{Lee}(\ominus a) = w_{Lee}(q-a) = \begin{cases} q-a, & se \quad q-a \leq \left\lfloor \frac{q}{2} \right\rfloor \\ q-(q-a), & se \quad q-a > \left\lfloor \frac{q}{2} \right\rfloor \end{cases} =$$

$$= \begin{cases} q-a, & se \quad a \geq \left\lfloor \frac{q}{2} \right\rfloor \\ a, & se \quad a < \left\lfloor \frac{q}{2} \right\rfloor \end{cases} = \begin{cases} a, & se \quad a \leq \left\lfloor \frac{q}{2} \right\rfloor \\ q-a, & se \quad a > \left\lfloor \frac{q}{2} \right\rfloor \end{cases} = w_{Lee}(a)$$

3. Sejam $a, b \in \mathbb{Z}_q$,

- *(Caso 1)* $0 \leq a \leq \frac{q}{2}, 0 \leq b \leq \frac{q}{2}, 0 \leq a+b \leq \frac{q}{2}$:

$$w_{Lee}(a \oplus b) = w_{Lee}(a+b) = a+b = w_{Lee}(a) + w_{Lee}(b).$$

- *(Caso 2)* $0 \leq a \leq \frac{q}{2}, 0 \leq b \leq \frac{q}{2}, \frac{q}{2} < a+b < q$:

$$w_{Lee}(a \oplus b) = w_{Lee}(a+b) = q-(a+b) <$$
$$< a+b = w_{Lee}(a) + w_{Lee}(b).$$

- *(Caso 3)* $0 \leq a \leq \frac{q}{2}, 0 \leq b \leq \frac{q}{2}, a+b = q$:

$$w_{Lee}(a \oplus b) = w_{Lee}((a+b) \bmod q) = w_{Lee}(0) = 0 \leq a+b = w_{Lee}(a) + w_{Lee}(b).$$

- *(Caso 4)* $0 \leq a \leq \frac{q}{2}, \frac{q}{2} < b < q, \frac{q}{2} < a+b < q$:

$$w_{Lee}(a \oplus b) = w_{Lee}(a+b) = q-(a+b) = q-b-a \leq q-b+a = w_{Lee}(a) + w_{Lee}(b).$$

- *(Caso 5)* $0 \leq a \leq \frac{q}{2}, \frac{q}{2} < b < q, q \leq a+b < \frac{3q}{2}$:

$$w_{Lee}(a \oplus b) = w_{Lee}(a+b-q) = a+b-q < a+(q-b) = w_{Lee}(a) + w_{Lee}(b).$$

- *(Caso 6)* $\frac{q}{2} < a < q, \frac{q}{2} < b < q, q < a+b \leq \frac{3q}{2}$:

$$w_{Lee}(a \oplus b) = w_{Lee}(a+b-q) = a+b-q \leq 2q-(a+b) =$$
$$= (q-a)+(q-b) = w_{Lee}(a) + w_{Lee}(b).$$

- *(Caso 7)* $\frac{q}{2} < a < q, \frac{q}{2} < b < q, \frac{3q}{2} < a + b < 2q$:

$$w_{Lee}(a \oplus b) = w_{Lee}(a + b - q) = q - (a + b - q) = 2q - (a + b) =$$
$$= (q - a) + (q - b) == w_{Lee}(a) + w_{Lee}(b).$$

3. Segue de 2.□

Proposição 4.3.1 $(\mathbb{Z}_q, d_{Lee})$ *é um espaço métrico.*

Demonstração:

- $d_{Lee}(a, b) = 0 \Leftrightarrow w_{Lee}(a \ominus b) = 0 \Leftrightarrow a \ominus b = 0 \Leftrightarrow a = b.$
- $d_{Lee}(a, b) = w_{Lee}(a \ominus b) = w_{Lee}(-(a \ominus b)) = w_{Lee}(b \ominus a) = d_{Lee}(b, a).$
- $d_{Lee}(a, c) = w_{Lee}(a \ominus c) = w_{Lee}(a \oplus b \ominus b \ominus c) = w_{Lee}((a \ominus b) \oplus (b \ominus c)) \leq$

$$\leq w_{Lee}(a \ominus b) + w_{Lee}(b \ominus c) = d_{Lee}(a, b) + d_{Lee}(b, c).$$

□

Podemos estender a distância de Lee para o grupo $\mathbb{Z}_q^n$, produto direto do grupo $\mathbb{Z}_q$, utilizando a métrica da soma, isto é $d_1 = d_2 = \ldots = d_n = d_{Lee}$ (Exemplo 2.3.5), ou seja,

$$d_L(\underline{a}, \underline{b}) = \sum_{i=1}^{n} d_{Lee}(a_i, b_i), \ \forall \underline{a} = (a_1, \ldots, a_n), \underline{b} = (b_1, \ldots, b_n) \in \mathbb{Z}_q^n$$

Podemos estender também o peso de Lee para $\mathbb{Z}_q^n$, de maneira natural, ou seja,

$$w_L(\underline{a}) = \sum_{i=1}^{n} w_{Lee}(a_i), \ \forall \underline{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_q^n,$$

e é óbvio que

$$d_L(\underline{a}, \underline{b}) = w_L(\underline{a} \ominus \underline{b}).$$

e

$$w_L(\underline{a}) = w_L(\sigma(\underline{a})),$$

onde σ é uma permutação com mudança de sinal nas coordenadas de $\underline{a}$.

Definição 4.3.2 *A métrica d_L é denominada distância de Lee entre duas* $\boldsymbol{n}$*-uplas em $\mathbb{Z}_q^n$, e o espaço métrico $(\mathbb{Z}_q^n, d_L)$ é denominado espaço de Lee n-dimensional de ordem q. A função w_L é denominada peso de Lee de uma* $\boldsymbol{n}$*-upla em $\mathbb{Z}_q^n$.*

Esta métrica possui algumas propriedades importantes:

Teorema 4.3.1 *1. O maior peso de Lee em $\mathbb{Z}_q$ é*

$$\begin{cases} \frac{q}{2} & se \quad q \text{ é par} \\ \frac{q-1}{2} & se \quad q \text{ é ímpar} \end{cases}.$$

2. O maior peso de Lee em $\mathbb{Z}_q^2$ é

$$\begin{cases} q & se \quad q \text{ é par} \\ q-1 & se \quad q \text{ é ímpar} \end{cases}.$$

3. O número de pontos na esfera de Lee de raio r em $\mathbb{Z}_q^2$ é:

(a) q ímpar

$$| S_L(0,r) | = \begin{cases} 1 & se \quad r = 0 \\ 4.r & se \quad 0 < r \leq \frac{q-1}{2} \\ 4.(q-r) & se \quad \frac{q-1}{2} \leq r \leq q-1 \end{cases}.$$

(b) q par maior do que 2 (o valor $q = 3$ consta na Tabela 4.2)

$$| S_L(0,r) | = \begin{cases} 1 & se \quad r = 0 \text{ ou } r = q \\ 4.r & se \quad 0 < r < \frac{q}{2} \\ 4.r - 2 & se \quad r = \frac{q}{2} \\ 4.(q-r) & se \quad \frac{q}{2} \leq r < q \end{cases}.$$

Demonstração:

1. Imediata.

2. Imediata.

$Raio_{\downarrow}$ $q\rightarrow$	1	2	3	4	5	6	7	8	9
0	1	1	1	1	1	1	1	1	1
1		2	4	4	4	4	4	4	4
2		1	4	6	8	8	8	8	8
3				4	8	10	12	12	12
4				1	4	8	12	14	16
5						4	8	12	16
6						1	4	8	12
7								4	8
8								1	4

Tabela 4.2: Alguns valores para o número de pontos na esfera de Lee bidimensional

(a) q é ímpar

i. Para $r = 0$ temos 1 ponto.

ii. Para $1 \leq r \leq \frac{q-1}{2}$ temos os seguintes pontos

$$\begin{array}{cccc} (r,0) & (r-1,1) & \ldots & (0,r) \\ (-1,r-1) & (-2,r-2) & \ldots & (-r,0) \\ (-r+1,-1) & (-r+2,-2) & \ldots & (0,-r) \\ (1,-r+1) & (2,-r+2) & \ldots & (r-1,-1) \end{array}$$

que totalizam $4r$ pontos.

iii. Para $\frac{q-1}{2} < r \leq q-1$ temos os seguintes pontos

$$\begin{array}{cccc} (\frac{q-1}{2}, r-\frac{q-1}{2}) & (\frac{q-1}{2}-1, r-\frac{q-1}{2}+1) & \ldots & (r-\frac{q-1}{2}, \frac{q-1}{2}) \\ (\frac{q-1}{2}, \frac{q-1}{2}-r) & (\frac{q-1}{2}-1, \frac{q-1}{2}-r-1) & \ldots & (r-\frac{q-1}{2}, -\frac{q-1}{2}) \\ (\frac{q-1}{2}-r, \frac{q-1}{2}) & (\frac{q-1}{2}-r-1, \frac{q-1}{2}-1) & \ldots & (-\frac{q-1}{2}, r-\frac{q-1}{2}) \\ (\frac{q-1}{2}-r, -\frac{q-1}{2}) & (\frac{q-1}{2}-r-1, -\frac{q-1}{2}+1) & \ldots & (-\frac{q-1}{2}, \frac{q-1}{2}-r) \end{array}$$

que totalizam $4(q-r)$ pontos. Note que

$$1 + \sum_{r=1}^{\frac{q-1}{2}} (4r) + \sum_{r=\frac{q-1}{2}+1}^{q-1} (4(q-r)) = q^2.$$

(b) q é par

i. Para $r = 0$ ou $r = q$ temos 1 ponto.

ii. Para $1 \leq r < \frac{q}{2}$ temos os seguintes pontos

$$\begin{array}{cccc} (r,0) & (r-1,1) & \ldots & (0,r) \\ (-1,r-1) & (-2,r-2) & \ldots & (-r,0) \\ (-r+1,-1) & (-r+2,-2) & \ldots & (0,-r) \\ (1,-r+1) & (2,-r+2) & \ldots & (r-1,-1) \end{array}$$

que totalizam $4r$ pontos.

iii. Para $r = \frac{q}{2}$ temos os seguintes pontos

$$\begin{array}{cccccc} (\frac{q}{2},0) & (\frac{q}{2}-1,1) & \ldots & (0,\frac{q}{2}) & \rightarrow & r+1 \text{ pontos} \\ (\frac{q}{2}-1,-1) & (\frac{q}{2}-2,-2) & \ldots & (1,-\frac{q-2}{2}) & \rightarrow & r-1 \text{ pontos} \\ (-1,\frac{q-2}{2}) & (-1,\frac{q-2}{2}-1) & \ldots & (-\frac{q-2}{2},1) & \rightarrow & r-1 \text{ pontos} \\ (-1,-\frac{q-2}{2}) & (-2,-\frac{q-2}{2}+1) & \ldots & (-\frac{q-2}{2},-1) & \rightarrow & r-1 \text{ pontos} \end{array}$$

que totalizam $4r-2$ pontos.

iv. Para $\frac{q}{2} < r < q$ temos os seguintes pontos

$$\begin{array}{cccccc} (\frac{q}{2},r-\frac{q}{2}) & (\frac{q}{2}-1,r-\frac{q}{2}+1) & \ldots & (r-\frac{q}{2},\frac{q}{2}) & \rightarrow & q-r+1 \text{ pontos} \\ (\frac{q}{2},\frac{q}{2}-r) & (\frac{q}{2}-1,\frac{q}{2}-r-1) & \ldots & (r-\frac{q-2}{2},-\frac{q-2}{2}) & \rightarrow & q-r \text{ pontos} \\ (\frac{q}{2}-r,\frac{q}{2}) & (\frac{q}{2}-r-1,\frac{q}{2}-1) & \ldots & (-\frac{q-2}{2},r-\frac{q-2}{2}) & \rightarrow & q-r \text{ pontos} \\ (\frac{q-2}{2}-r,-\frac{q-2}{2}) & (\frac{q-2}{2}-r-1,-\frac{q-2}{2}+1) & \ldots & (-\frac{q-2}{2},\frac{q-2}{2}-r) & \rightarrow & q-r-1 \text{ pontos} \end{array}$$

que totalizam $4(q-r)$ pontos. Note que

$$1+1+\sum_{r=1}^{\frac{q}{2}-1}(4r)+(2q-2)+\sum_{r=\frac{q}{2}+1}^{q-1}(4(q-r))=q^2.$$

4.3.2 Isometrias no espaço de Lee

Uma classe de isometrias no espaço métrico de Lee é dada pelas translações em $\mathbb{Z}_q^n$ e estas constituem um tipo de transformação muito semelhante a que existe no espaço euclidiano.

Definição 4.3.3 *As funções*

$$T_{i_1 i_2 \ldots i_n} : \mathbb{Z}_q^n \to \mathbb{Z}_q^n;\ 0 \leq i_1, i_2, \ldots, i_n \leq q-1,$$

definidas por

$$T_{i_1 i_2 \ldots i_n}(a_1, a_2, \ldots, a_n) = (a_1 \oplus i_1, a_2 \oplus i_2, \ldots, a_n \oplus i_n).$$

são denominadas translações de $\mathbb{Z}_q^n$ em $\mathbb{Z}_q^n$.

Proposição 4.3.2 *As translações são isometrias de $\mathbb{Z}_q^n$ em $\mathbb{Z}_q^n$.*

Demonstração:

$$d_L(T_{i_1 i_2 \ldots i_n}(a_1, \ldots, a_n), T_{i_1 i_2 \ldots i_n}(b_1, \ldots, b_n)) =$$

$$\begin{aligned}
&= d_L((a_1 \oplus i_1, \ldots, a_n \oplus i_n), (b_1 \oplus i_1, \ldots, b_n \oplus i_n)) = \\
&= w_L((a_1 \oplus i_1) \ominus (b_1 \oplus i_1), \ldots, (a_n \oplus i_n) \ominus (b_n \oplus i_n)) = \\
&= w_L(a_1 \ominus b_1, \ldots, a_n \ominus b_n) = \\
&= d_L((a_1, \ldots, a_n), (b_1, \ldots, b_n)).
\end{aligned}$$

□

Através da representação matricial, toda translação $T_{i_1 i_2 \ldots i_n}$ pode ser escrita da seguinte forma:

$$T_{i_1 i_2 \ldots i_n} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \left[\begin{pmatrix} & & \\ & \mathbf{I_n} & \\ & & \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} i_1 \\ \vdots \\ i_n \end{pmatrix} \right] \ mod\ q,$$

onde $0 \leq a_i \leq q-1$, $1 \leq i \leq n$, $\mathbf{I}_n$ é a matriz identidade de ordem n. Utilizando coordenadas homogêneas através da identificação

$$\left(a_1, \ \cdots, \ a_n \right) \leftrightarrow \left(a_1, \ \cdots, \ a_n, \ 1 \right),$$

temos uma forma simplificada de representação matricial das translações (4.2),

$$T_{i_1 i_2 \ldots i_n} \begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ a_n \\ 1 \end{pmatrix} = \left[\begin{pmatrix} & & & i_1 \\ & \mathbf{I_n} & & \vdots \\ & & & i_n \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ a_n \\ 1 \end{pmatrix} \right] \ mod\ q = \widetilde{\mathbf{I}_n} \begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ a_n \\ 1 \end{pmatrix} \ mod\ q \qquad (4.2)$$

e a operação dada é o produto de matrizes no subgrupo das matrizes do tipo $\widetilde{\mathbf{I}_n}$.

O próximo teorema reproduz, de uma certa maneira, o que ocorre no espaço euclidiano n-dimensional, quando consideramos o espaço de Lee.

Teorema 4.3.2 *Seja $f : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$, uma isometria no espaço de Lee $(\mathbb{Z}_q^n, d_L)$. Então existem $\underline{a} \in \mathbb{Z}_q^n$ e uma função $\psi : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$, tais que:*

1. $f(\underline{x}) = \underline{a} + \psi(\underline{x})$;
2. $\psi(\underline{0}) = \underline{0}$;
3. *ψ é uma isometria;*
4. $w_L(\psi(\underline{x})) = w_L(\underline{x})$.

Demonstração:

1. *Considere* $\underline{a} = f(\underline{0})$ *e* $\psi(\underline{x}) = f(\underline{x}) - \underline{a}$;
2. $\psi(\underline{0}) = f(\underline{0}) - \underline{a} = \underline{0}$;
3. $d_L(\psi(\underline{x}), \psi(\underline{y})) = w_L(\psi(\underline{x}) - \psi(\underline{y})) = w_L(f(\underline{x}) - f(\underline{y})) = d_L(f(\underline{x}), f(\underline{y})) = d_L(\underline{x}, \underline{y})$;
4. $w_L(\psi(\underline{x})) = d_L(\psi(\underline{x}), \underline{0}) = d_L(\psi(\underline{x}), \psi(\underline{0})) = d_L(\underline{x}, \underline{0}) = w_L(\underline{x})$.□

Este teorema mostra que toda isometria pode ser escrita como a composição de duas funções: T_a e ψ, ou seja,

$$f(\underline{x}) = T_{\underline{a}} \circ \psi(\underline{x}),$$

onde

$$T_{\underline{a}} : \mathbb{Z}_q^n \to \mathbb{Z}_q^n, \quad T_{\underline{a}}(\underline{x}) = \underline{x} + \underline{a}$$

e

$$\psi : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$$

é uma isometria que fixa o vetor nulo.

Corolário 4.3.1 *Sejam*

$$T(\mathbb{Z}_q^n) = \{T_a : \mathbb{Z}_q^n \to \mathbb{Z}_q^n; \quad T_a(x) = x + a\}$$

e

$$\Psi = \{\psi : \mathbb{Z}_q^n \to \mathbb{Z}_q^n; \quad \psi(0) = 0, \quad \psi \textit{é isometria}\}.$$

Se

$$\psi(a+b) = \psi(a) + \psi(b), \quad \forall a, b \in \mathbb{Z}_q^n,$$

então

$$\Gamma(\mathbb{Z}_q^n) \cong T(\mathbb{Z}_q^n) \times_\varphi \Psi.$$

Demonstração: De fato, observe que

$$T(\mathbb{Z}_q^n) \cap \Psi = \{i_{\mathbb{Z}_q^n}\}.$$

$$\psi \circ T_a \circ \psi^{-1}(x) = \psi(\psi^{-1}(x) + a) = \psi(\psi^{-1}(x)) + \psi(a) =$$
$$= x + \psi(a) \in T(\mathbb{Z}_q^n).$$

Portanto, $T(\mathbb{Z}_q^n)$ é normal em $\Gamma(\mathbb{Z}_q^n)$ e utilizando o teorema anterior obtemos o desejado.□

Em alguns casos, este corolário permite caracterizar facilmente o grupo de simetrias $\Gamma(\mathbb{Z}_q^n)$.

O problema principal no estudo das simetrias no espaço de Lee é caracterizar as funções ψ. No espaço euclidiano estas funções são dadas por transformações lineares ortogonais. No espaço de Lee, veremos que o comportamento deste espaço não é muito diferente do caso euclidiano.

O grupo de simetrias de $\mathbb{Z}_q$

O espaço de Lee unidimensional pode ser representado geometricamente como mostrado na Fig. 4.7 e seu grupo de simetrias é dado pelo teorema:

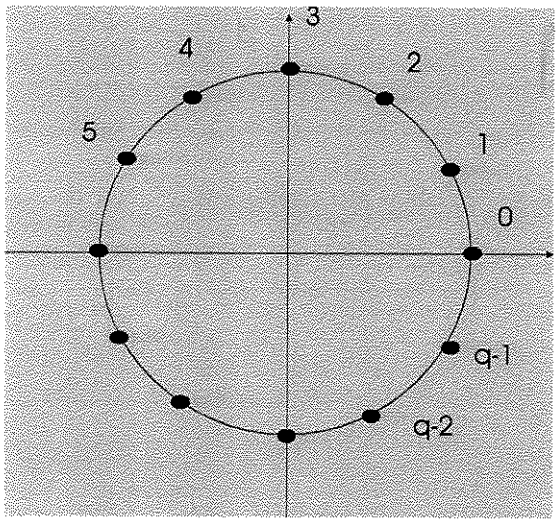

Figura 4.7: Representação geométrica do espaço de Lee unidimensional

Teorema 4.3.3 *Para $q > 2$, o grupo de simetrias de $(\mathbb{Z}_q, d_L)$ é isomorfo à $\mathbb{Z}_q \times_\varphi \mathbb{Z}_2 \cong \mathbb{D}_q$.*

Para a demonstração deste teorema, utilizaremos o seguinte lema:

Lema 4.3.2 *Se $\psi : \mathbb{Z}_q \to Z_q$, é uma isometria (não trivial) tal que $\psi(0) = 0$, então ψ é a reflexão através da reta $y = 0$, ou seja,*

$$\psi(a) = q - a.$$

Demonstração: Como ψ é isometria e $\psi(0) = 0$ temos, para todo $a \in \mathbb{Z}_q$,

$$w_L(\psi(a)) = d_L(\psi(a), 0) = d_L(\psi(a), \psi(0)) = d_L(a, 0) = w_L(a).$$

Portanto, $\psi(a) = a$ ou $\psi(a) = q - a$. Como ψ não é a identidade, $\psi(a) = q - a$.□

Observe que se q é ímpar então o ponto 0 é o único ponto fixo e se q é par a isometria ψ fixa também o ponto $\frac{q}{2}$.

Demonstração do Teorema: No Teorema 4.3.2, a função ψ é uma reflexão ou a identidade pelo Lema 4.3.2, e estas duas funções formam um subgrupo de $\Gamma(\mathbb{Z}_q)$ isomorfo a $\mathbb{Z}_2$. Como a reflexão e a identidade são lineares, pelo Corolário 4.3.1, o resultado é imediato.□

Assim, toda isometria $\phi : \mathbb{Z}_q \rightarrow Z_q$, pode ser escrita da seguinte forma:

$$\phi(a) = [Ma + i] \mod q,$$

onde $0 \leq a \leq q-1$, $M = (\pm 1)$. Utilizando coordenadas homogêneas através da identificação

$$(a) \leftrightarrow (a, 1),$$

temos uma forma de representação matricial das translações (4.3),

$$\phi \begin{pmatrix} a \\ 1 \end{pmatrix} = \left[\begin{pmatrix} M & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ 1 \end{pmatrix} \right] \mod q = \widetilde{M} \begin{pmatrix} a \\ 1 \end{pmatrix} \mod q \tag{4.3}$$

e a operação dada é o produto de matrizes no subgrupo das matrizes do tipo $\widetilde{M}$.

O grupo de simetrias de $\mathbb{Z}_q^2$ ($q \neq 2$ e $q \neq 4$)

Para $q \neq 2$ e $q \neq 4$, o grupo de simetrias de $\mathbb{Z}_q^2$ possui, além das translações, isometrias similares a do espaço euclidiano. Estas isometrias são as reflexões em $\mathbb{Z}_q^2$, obtidas por 4 eixos básicos imaginários de simetria que permitem reflexões (os outros eixos de simetria são obtidos por translações):

- q ímpar
  - (a) $y = x$;
  - (b) $y = -x$;
  - (c) $y = 0$;
  - (d) $x = 0$.

- q par

  (a) $y = x$;

  (b) $y = 1 - x$;

  (c) $y = \frac{1}{2}$;

  (d) $x = \frac{1}{2}$.

As Figuras 4.8 e 4.9 mostram estes casos.

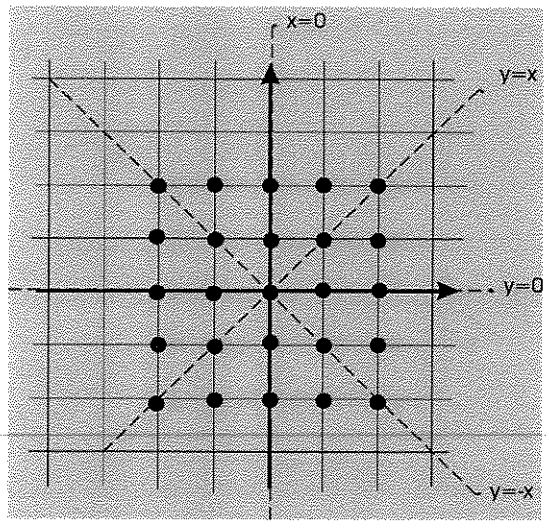

Figura 4.8: Eixos de simetria para o caso $q = 5$ (ímpar)

Isto nos fornece 4 funções:

- q ímpar:
  - $Re_{y=x}(a, b) = (b, a)$;
  - $Re_{y=-x}(a, b) = (-b, -a)$;
  - $Re_{y=0}(a, b) = (a, -b)$;
  - $Re_{x=0}(a, b) = (-a, b)$.
- q par:

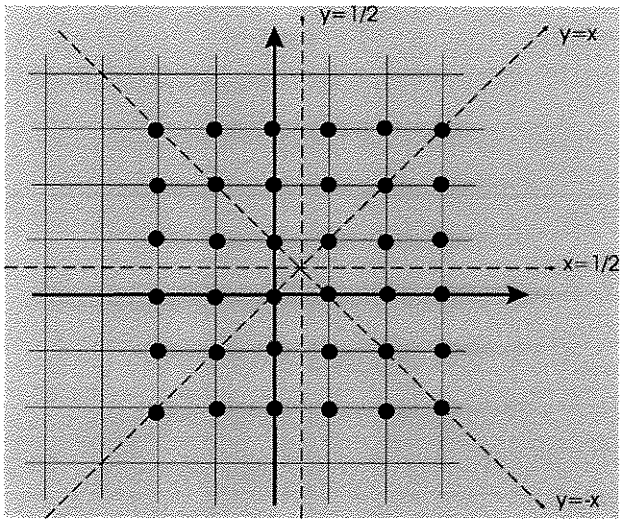

Figura 4.9: Eixos de simetria para o caso $q = 6$ (par)

- $Re_{y=x}(a,b) = (b,a)$;
- $Re_{y=1-x}(a,b) = (1-b, 1-a)$;
- $Re_{y=\frac{1}{2}}(a,b) = (a, 1-b)$;
- $Re_{x=\frac{1}{2}}(a,b) = (1-a, b)$.

onde Re_τ denota reflexão em torno do eixo τ.

Proposição 4.3.3 *As reflexões são isometrias de $\mathbb{Z}_q^2$ em $\mathbb{Z}_q^2$.*

Demonstração:

- *q ímpar:*
  - $Re_{y=x}(a,b) = (b,a)$;

$$\begin{aligned} d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((b,a),(d,c)) = w_L(b \ominus d, a \ominus c) = \\ = w_L(d \ominus b, c \ominus a) = w_L(b \ominus d, a \ominus c) \\ = w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)). \end{aligned}$$

- $Re_{y=-x}(a,b) = (-b,-a)$;

$$d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((\ominus a, \ominus b), (\ominus c, \ominus d)) = w_L(\ominus a \oplus c, \ominus b \oplus d) =$$
$$= w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)).$$

- $Re_{y=0}(a,b) = (a,-b)$;

$$d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((a, \ominus b), (c, \ominus d)) = w_L(a \ominus c, \ominus b \oplus d) =$$
$$= w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)).$$

- $Re_{x=0}(a,b) = (-a,b)$.

$$d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((\ominus a, b), (\ominus c, d)) = w_L(\ominus a \oplus c, b \ominus d) =$$
$$= w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)).$$

- *q par:*

  - $Re_{y=x}(a,b) = (b,a)$*: Idêntico ao caso ímpar.*
  - $Re_{y=1-x}(a,b) = (1-b, 1-a)$;

$$d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((1 \ominus b, 1 \ominus a), (1 \ominus d, 1 \ominus c)) = w_L(\ominus b + d, \ominus a + c) =$$
$$= w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)).$$

  - $Re_{y=\frac{1}{2}}(a,b) = (a, 1-b)$;

$$d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((a, 1 \ominus b), (c, 1 \ominus d)) = w_L(a \ominus c, \ominus b + d) =$$
$$= w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)).$$

  - $Re_{x=\frac{1}{2}}(a,b) = (1 \ominus a, b)$.

$$d_L(Re_{y=x}(a,b), Re_{y=x}(c,d)) = d_L((1 \ominus a, b), (1 \ominus c, d)) = w_L(\ominus a + c, b \ominus d) =$$
$$= w_L(a \ominus c, b \ominus d) = d_L((a,b),(c,d)).$$

□

Observe que as rotações conhecidas no espaço euclidiano estão presentes também neste espaço e são dadas por composições de reflexões.

No caso ímpar, as reflexões geram o grupo

$$\{(b,a),(-b,-a),(a,-b),(-a,b),(a,b),(-a,-b),(b,-a),(-b,a)\}$$

onde cada par ordenado representa a imagem do ponto (a,b). Neste grupo temos um elemento neutro dado pela função identidade (a,b), 4 elementos de ordem 2 dados por

$$(b,a),(-b,-a),(a,-b) \text{ e } (-a,b),$$

um elemento de ordem 4 $(-b,a)$ que gera os outros dois elementos restantes. Este grupo é, portanto, isomorfo à $\mathbb{D}_4$.

No caso ímpar, as reflexões geram o grupo

$$\{(b,a),(1-b,1-a),(a,1-b),(1-a,b),(a,b),(1-a,1-b),(b,1-a),(1-b,a)\}$$

Neste grupo temos um elemento neutro dado pela função identidade (a,b), 4 elementos de ordem 2 dados por

$$(b,a),(1-b,1-a),(a,1-b) \text{ e } (1-a,b),$$

um elemento de ordem 4 $(1-b,a)$ que gera os outros dois elementos restantes. Portanto, este grupo é, também, isomorfo à $\mathbb{D}_4$.

A questão que surge é a seguinte: Existem outras isometrias diferentes destas? Responderemos a esta questão analisando as isometrias que não são translações de $\mathbb{Z}_q^2$. Para isto, precisamos de algumas definições:

Definição 4.3.4 *Sejam $a \in \mathbb{Z}_q$ Um circuito horizontal passando por a, e denotado por $\mathfrak{C}_a^h$, é um subconjunto de $\mathbb{Z}_q^2$ da seguinte forma*

$$\mathfrak{C}_a^h = \mathbb{Z}_q \times \{a\}.$$

Um circuito vertical passando por a, e denotado por $\mathfrak{C}_a^v$, é um subconjunto de $\mathbb{Z}_q^2$ da seguinte forma

$$\mathfrak{C}_a^v = \{a\} \times \mathbb{Z}_q.$$

Um circuito passando por a, e denotado por $\mathfrak{C}_a$, é qualquer ciclo horizontal ou vertical passando por a.

O número a é denominado nível do circuito.

Quando dois circuitos forem ambos horizontais ou ambos verticais diremos que eles são paralelos.

A distância entre dois circuitos paralelos $\mathfrak{C}_a$ e $\mathfrak{C}_b$, denotada por $dc(\mathfrak{C}_a, \mathfrak{C}_b)$, é dada por

$$dc(\mathfrak{C}_a, \mathfrak{C}_b) = d_L(a, b).$$

Observe que os circuitos constituem cópias do espaço de Lee $\mathbb{Z}_q$ no espaço de Lee $\mathbb{Z}_q^2$. O comportamento destas cópias, quando se opera com isometrias em $\mathbb{Z}_q^2$, fornecerá quem são as isometrias de $\mathbb{Z}_q^2$.

Lema 4.3.3 *Seja $\psi : \mathbb{Z}_q^2 \to \mathbb{Z}_q^2$, uma isometria tal que $\psi(0) = 0$, então*

1. *ψ leva circuito em circuito de mesmo nível ou nível oposto, ou seja,*

$$\forall a \in \mathbb{Z}_q, \psi(\mathfrak{C}_a) = \mathfrak{C}_a \quad ou \quad \psi(\mathfrak{C}_a) = \mathfrak{C}_{q-a}.$$

2. *ψ preserva paralelismo;*

3. *ψ preserva distância entre circuitos.*

Demonstração:

1. *Num circuito $\mathfrak{C}_a$, duas bolas fechadas de raio unitário centradas em pontos do tipo (i, a) e $(i+2, a)$, como na Fig. 4.10(a), possuem um único ponto em comum. A imagem deverá satisfazer esta condição também mas se não for um circuito teremos uma situação como da Fig. 4.10(b), o que é uma contradição.*

2. *Se dois circuitos são paralelos e distintos, a distância entre seus pontos é maior do que zero. Suponha que as imagens não sejam circuitos paralelos, então teremos dois elementos da imagem com distância nula que é o cruzamento dos dois circuitos não paralelos;*

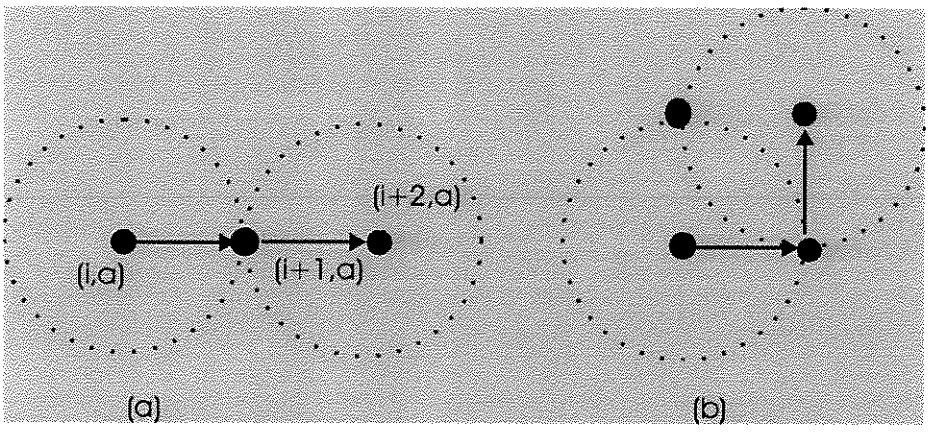

Figura 4.10: Bolas fechadas de raio 1 em circuitos e não-circuitos

3. Segue diretamente do item anterior e da definição de distância entre circuitos.

Teorema 4.3.4 *Para $q \neq 2$ e $q \neq 4$, $\Gamma(\mathbb{Z}_q^2)$ é formado por translações, reflexões que geram o grupo diedral e composições destas.*

Demonstração: A solução se resume em determinar como a ψ age nos ciclos

$$\mathfrak{C}_0^v, \mathfrak{C}_i^h \text{ e } \mathfrak{C}_i^v \quad \text{para } i = 0, 1, \ldots, q-1.$$

O Lema 4.3.3 nos fornece as seguintes opções:

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^v, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_i^h, i = 0, 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_i^v, i = 0, 1, \ldots, q-1,$$

  o que nos leva à função identidade.

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^v, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_i^h, i = 0, 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_{q-i}^v, i = 1, \ldots, q-1,$$

  o que nos leva à função reflexão em torno de $x = 0$, se q é ímpar, ou $x = \frac{1}{2}$, se q é par.

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^v, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_{q-i}^h, i = 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_i^v, i = 0, 1, \ldots, q-1,$$

  o que nos leva à função reflexão em torno de $y = 0$, *se* q *é ímpar, ou* $y = \frac{1}{2}$, *se* q *é par.*

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^v, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_{q-i}^h, i = 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_{q-i}^v, i = 1, \ldots, q-1,$$

  o que nos leva à função rotação de π;

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^h, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_i^h, i = 0, 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_i^v, i = 1, \ldots, q-1,$$

  o que nos leva à função rotação de $\frac{3\pi}{2}$.

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^h, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_i^h, i = 0, 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_{q-i}^v, i = 1, \ldots, q-1,$$

  o que nos leva à função reflexão em torno de $y = -x$, *se* q *é ímpar, ou* $x = 1 - x$, *se* q *é par.*

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^h, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_{q-i}^h, i = 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_i^v, i = 1, \ldots, q-1,$$

  o que nos leva à função rotação de $\frac{\pi}{2}$.

- $$\psi(\mathfrak{C}_0^v) = \mathfrak{C}_0^h, \psi(\mathfrak{C}_i^h) = \mathfrak{C}_{q-i}^h, i = 1, \ldots, q-1,$$

  e

  $$\psi(\mathfrak{C}_i^v) = \mathfrak{C}_{q-i}^v, i = 1, \ldots, q-1,$$

  o que nos leva à função reflexão em torno de $y = x$.

Este grupo é isomorfo ao grupo diedral de ordem 8, $\mathbb{D}_4$.

Desta forma, podemos dizer que

$$f \in \Gamma(\mathbb{Z}_q^2) \Rightarrow f \in T(\mathbb{Z}_q^2)$$

ou

$$f \in \mathbb{D}_4$$

ou

$$f = g \circ h, \text{ onde } g \in T(\mathbb{Z}_q^2) \text{ e } h \in \mathbb{D}_4$$

□

Corolário 4.3.2 *Se* q *é ímpar então*

$$\Gamma(\mathbb{Z}_q^2) \cong T(\mathbb{Z}_q^2) \times_\varphi \mathbb{D}_4 \cong \mathbb{Z}_q^2 \times_\varphi \mathbb{D}_4.$$

Demonstração: De fato, quando q *é ímpar*

$$\psi(a+b) = \psi(a) + \psi(b).$$

Pelo Corolário 4.3.1, temos

$$\Gamma(\mathbb{Z}_q^2) \cong T(\mathbb{Z}_q^2) \times_\varphi \mathbb{D}_4 \cong \mathbb{Z}_q^2 \times_\varphi \mathbb{D}_4 \cong \mathbb{Z}_q^2 \times_\varphi \left(\mathbb{Z}_2^2 \times_\varphi S_2\right). \tag{4.4}$$

□

Quando q é par, não é possível utilizar o Corolário 4.3.1, mas através da representação matricial deste grupo chegaremos ao mesmo resultado da relação (4.4). Em primeiro lugar, observamos que toda isometria $\phi : \mathbb{Z}_q^2 \to \mathbb{Z}_q^2$ pode ser escrita da seguinte forma:

$$\phi \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \left[\begin{pmatrix} & M & \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} \right] \ mod\ q,$$

onde $0 \leq a_i \leq q-1$, $1 \leq i \leq 2$, e $M \in \mathfrak{M}$ é uma das seguintes 8 matrizes:

$$\mathfrak{M} = \left\{ \begin{array}{ccccc} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; & \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; & \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}; & \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & & \end{array} \right\}.$$

Utilizando coordenadas homogêneas através da identificação:

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \leftrightarrow \begin{pmatrix} x_1, & x_2, & 1 \end{pmatrix},$$

incluímos as translações na representação matricial (4.4),

$$\phi \begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix} = \left[\begin{pmatrix} M & & i_1 \\ & & i_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ 1 \end{pmatrix} \right] \ mod\ q \ = \ \widetilde{M} \begin{pmatrix} a_1 \\ a2 \\ 1 \end{pmatrix} \ mod\ q, \qquad (4.5)$$

Observe que as matrizes M que geram o grupo isomorfo ao grupo diedral são a segunda (rotação de $\pi/2$) e a quinta (reflexão horizontal) matrizes em $\mathfrak{M}$, respectivamente.

Para obter a relação (4.4), ou seja, a condição de ser um produto semi-direto, é necessário verificar que as translações formam um subgrupo normal de $\Gamma(\mathbb{Z}_q^2)$. Mas, para isto, basta observar que as translações são caracterizadas pelas matrizes $\widetilde{M}$ tendo M como matriz identidade e, considerando produto de matrizes por blocos, verifica-se facilmente que se T_{i_1,i_2} é uma translação, $\phi^{-1}T_{i_1,i_2}\phi$ é também uma translação para qualquer $\phi \in \Gamma(\mathbb{Z}_q^2)$.

Os elementos de $\Gamma(\mathbb{Z}_q^2)$ são os quatro casos considerados para isometrias de Lee induzidas por isometrias euclidianas. A ordem de um elemento em $\mathbb{Z}_q^2$ pode ser: 1 (identidade); 2 (rotações

por π ou reflexões); 4 (rotações por $\pi/2$ ou $3\pi/2$); q (translações); $2q$ ou $2(q/2j)$ se q é divisível por $2j$, por glisso-reflexões de passo j. Portanto, a ordem máxima de um elemento em $\Gamma(\mathbb{Z}_q^2)$ (e de um subgrupo cíclico) é $2q$.

O grupo de simetrias de $\mathbb{Z}_q^n$ ($q \neq 2$ e $q \neq 4$)

No caso $q \neq 2$ e $q \neq 4$, para estudar o grupo de simetrias de $\Gamma(\mathbb{Z}_q^n)$ é essencial analisar a imagem de "circuitos" através de isometrias.

Definição 4.3.5 *Um l-circuito, denotado por $\mathfrak{C}_l$, é um subconjunto de $\mathbb{Z}_q^n$ isométrico a $\mathbb{Z}_l$, ou seja, $\mathfrak{C}_P = \{P_0, P_1, ..., P_l\}$ tal que*

$$d(P_i, P_j) = \min\{\mid i-j \mid, q- \mid i-j \mid\}, \forall P_i, P_j \in \mathfrak{C}_l.$$

Um caso especial de l-circuitos é dado pelos circuitos passando por um ponto $P = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_q^n$, denotado por $\mathfrak{C}_P$, que é o subconjunto de $\mathbb{Z}_q^n$ tal que todas as coordenadas são fixas exceto a j-ésima coordenada,

$$\mathfrak{C}_P = \{(a_1, a_2, ..., a_{j-1}, x, a_{j+1}, ..., a_n) : x \in \mathbb{Z}_q\}.$$

Exemplo 4.3.1 *Considere o caso $\mathbb{Z}_5^2$. Dado um par (x, y), os movimentos horizontais (mantendo o valor de y fixo) e os movimentos verticais (mantendo o valor de x fixo) representam os circuitos $\mathfrak{C}_{(x,y)}$. Observe que estes movimentos lembram o movimento da torre no jogo de xadrez. Chamaremos, de forma geral, estes circuitos de circuito-torre.*

Lema 4.3.4 *a) Uma isometria $\phi : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ leva l-circuitos em l-circuitos; b) Em particular, se $q \neq 4$, uma isometria leva um circuito-torre em um circuito-torre (circuitos dados por eixos coordenados).*

Demonstração:A condição (a) é uma consequência direta de ϕ preservar distâncias. Para verificar (b) note que para $q \neq 4$, dados dois pontos P_i e P_{i+2} num circuito-torre (cuja distância é 2), as bolas n-dimensionais de raio 1 (conjunto de pontos de $\mathbb{Z}_q^n$ cuja distância ao ponto dado é) centrada nestes dois pontos terá um único ponto em comum que é P_{i+1}. Esta condição é preservada por uma isometria. Por outro lado, se a imagem de um circuito-torre não é um

circuito-torre teremos que os três pontos da imagem não estarão alinhados e formarão uma quina, como mostra a Fig. 4.11, e as bolas com centros em $\phi(P_i)$ e $\phi(P_{i+2})$ com raio 1 terão dois pontos em comum. Então ϕ não será uma isometria.□

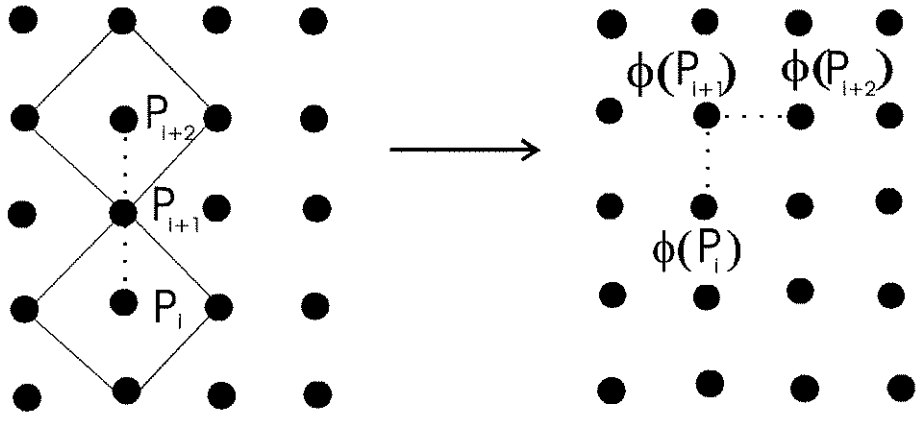

Figura 4.11: Imagem de duas bolas através de ϕ

Lema 4.3.5 *Toda isometria $\psi : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$, $q \neq 4$ e $q \neq 2$, tal que $\psi(\underline{0}) = \underline{0}$ pode ser escrita como*

$$\psi = \theta \circ \rho,$$

onde ρ é uma permutação de coordenadas e θ é uma isometria que leva cada circuito-torre passando por $\underline{0}$ sobre ele mesmo, esta sendo a identidade ou uma reflexão quando restrita ao circuito-torre.

Demonstração: Do Lema 4.3.4, ψ leva um circuito-torre em circuito-torre. Seja ρ a permutação de eixos coordenados definidos por ψ. Considerando $\theta = \psi \circ \rho^{-1}$, temos que θ é uma isometria,

$$\theta(\underline{0}) = \psi \circ \rho^{-1}(\underline{0}) = \underline{0}$$

e θ leva cada circuito-torre sobre ele mesmo. Por outro lado, uma isometria $\theta : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ que deixa o vetor nulo fixo e leva circuitos-torre passando por $\underline{0}$ sobre eles mesmo tem que ser a identidade ou a reflexão nestes circuitos uma vez que os circuitos-torre são isométricos a $\mathbb{Z}_q$. Então, θ é necessariamente da forma

$$\theta\left(a_1, a_2, \cdots, a_n\right) = \left(\pm a_1, \pm a_2, \cdots, \pm a_n\right).$$

□

Teorema 4.3.5 *Dados $\mathbb{Z}_q^n$ com a métrica de Lee, $q \neq 2$ e $q \neq 4$, $n \geq 2$, o grupo de simetrias de $\mathbb{Z}_q^n$, $\Gamma(\mathbb{Z}_q^n)$, satisfaz o seguinte isomorfismo:*

$$\Gamma(\mathbb{Z}_q^n) \cong \mathbb{Z}_q^n \times_\varphi \left(\mathbb{Z}_2^n \times_\varphi S_n\right),$$

onde $\times_\varphi$ denota o produto semi-direto.

Observação 4.3.1 *Note que $\mathrm{C}(n) \cong \Gamma(\mathbb{Z}_2^n) \cong \mathbb{Z}_2^n \times_\varphi S_n$ é o grupo de simetrias do n-cubo, $\mathbb{Z}_2^n$, com a métrica de Lee e é também o grupo de simetrias euclidianas do cubo n-dimensional $[0,1]^n$. Note que $\mathbb{Z}_2^n$ com a métrica de Lee e $\mathbb{Z}_2^n$ com a métrica euclidiana possuem a mesma configuração métrica, ou seja, existe uma bijeção $\gamma : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, tal que $\psi : (\mathbb{Z}_2^n, d_L) \to (\mathbb{Z}_2^n, d_L)$ é uma isometria se e somente se $\gamma^{-1}\psi\gamma : (\mathbb{Z}_2^n, d_e) \to (\mathbb{Z}_2^n, d_e)$ é também uma isometria.*

Demonstração: Das demonstrações dos Lemas 4.3.4 e 4.3.3, temos que

$$\phi \in \Gamma(\mathbb{Z}_q^n), \qquad \phi = t \circ \theta \circ \rho, \tag{4.6}$$

onde $t \in T(\mathbb{Z}_q^n)$ é o subgrupo das translações; $\theta \in R(\mathbb{Z}_q^n, \underline{0})$ é o subgrupo gerado por reflexões no plano coordenado passando por $\underline{0}$; $\rho \in P(n)$ é o subgrupo das isometrias dadas por permutações de coordenadas; e $\vartheta = \theta \circ \rho \in C(n)$ é o subgrupo das isometrias de $\mathbb{Z}_q^n$ que deixam o vetor nulo fixo.

Temos que a intersecção de qualquer par dos grupos anteriores é a identidade e temos também os seguintes isomorfismos:

$$T(\mathbb{Z}_q^n) \cong \mathbb{Z}_q^n; \qquad R(\mathbb{Z}_q^n, \underline{0}) \cong \mathbb{Z}_2^n; \qquad P(n) \cong \mathcal{S}_n.$$

Então, através de representação matricial (ver equação (4.4)) para toda isometria em $\Gamma(\mathbb{Z}_q^n)$, temos

$$\phi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \left[\begin{pmatrix} & M & \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right] \ mod\ q,$$

onde $0 \leq x_i \leq q-1$, $1 \leq i \leq n$, $M \in \mathfrak{M}$ *são matrizes ortogonais euclidianas cujas entradas assumem valores* 0, *ou* ± 1 *(estas são as matrizes que realizam as permutações e mudanças de orientação dos eixos coordenados). Utilizando coordenadas homogêneas através da identificação:*

$$\left(\begin{array}{ccc} x_1, & \cdots, & x_n \end{array} \right) \leftrightarrow \left(\begin{array}{ccc} x_1, & \cdots, & x_n, \quad 1 \end{array} \right),$$

podemos incluir translações nesta representação matricial como mostra a equação (4.7),

$$\phi \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \left[\begin{pmatrix} & & & a_1 \\ & M & & \vdots \\ & & & a_n \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \\ 1 \end{pmatrix} \right] \ mod\ q \ = \ \widetilde{M} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \\ 1 \end{pmatrix} \ mod\ q, \qquad (4.7)$$

e a operação de grupo em $\Gamma(\mathbb{Z}_q^n)$ *dada por composições de isometrias será o produto no subgrupo das matrizes da forma* $\widetilde{M}$.

A condição de ser um produto semi-direto segue do do fato de que os subgrupos considerados são normais. Para mostrar que o subgrupo $T(\mathbb{Z}_q^n)$ *é normal em* $\Gamma(\mathbb{Z}_q^n)$ *é suficiente mostrar que uma translação é caracterizada por* $\widetilde{M}$ *tendo* M *como a matriz identidade. Considerando produto de matrizes por blocos, é fácil ver que para qualquer translação dada* t, $\phi^{-1}t\phi$ *ainda é uma translação para qualquer* $\phi \in \Gamma(\mathbb{Z}_q^n)$.

Para verificar que o subgrupo das reflexões $R(\mathbb{Z}_q^n, \underline{0})$ *é normal no subgrupo* $C(n)$ *das isometrias em* $\Gamma(\mathbb{Z}_q^n)$ *que deixam o vetor nulo fixo, notemos que este subgrupo é identificado com o subgrupo* $\mathfrak{N} \subset \mathfrak{M}$ *das* $n \times n$ *matrizes da forma diagonal* $(n_{ii} = \pm 1, n_{ij} = 0,\ j \neq i)$. *Além disso, verificamos que* $M^{-1}NM \in \mathfrak{N}$, $\forall\ M \in \mathfrak{M}$, *para* $M^{-1}NM = M^{t'}NM \in \mathfrak{N}$, *onde* t' *denota a transposta. Isto conclui a demonstração da normalidade de* $\mathfrak{N}$ *em* $\mathfrak{M}$ *e também a demonstração do teorema.*□

Finalmente, observamos que:

1. da representação matricial das isometrias e dos isomorfismos referentes;

2. de [13];

3. e do fato que $\mathbb{Z}_2^n$ com a métrica de Lee e com a métrica euclidiana possuem a mesma configuração métrica e que espaços com a mesma configuração métrica tem grupos de simetrias isomorfos, concluímos com os próximos dois corolários.

Corolário 4.3.3 $\Gamma(\mathbb{Z}_q^n) \cong \mathbb{Z}_q^n \times_\varphi C(n)$, $q \neq 4$ *e* $q \neq 2$, *onde* $C(n)$ *é o grupo de simetrias do n-cubo* $\mathbb{Z}_2^n$ *com a métrica de Lee e é também o grupo de simetrias euclidiano do n-cubo* $[0,1]^n \subset \mathbb{R}^n$. *A ordem de* $\Gamma(\mathbb{Z}_q^n)$ *é* $q^n 2^n n!$.

Corolário 4.3.4 *As isometrias de* $\Gamma(\mathbb{Z}_q^n)$ *são dadas pela equação (4.7).*

Casos especiais: $n = 3$ **e** $q = 4$

Caso $n = 3$. Para $q \neq 4$ e $q \neq 2$, o grupo de simetrias satisfaz o isomorfismo

$$\Gamma(\mathbb{Z}_q^3) \cong \mathbb{Z}_q^3 \times_\varphi C(3) \cong \mathbb{Z}_q^3 \times_\varphi (\mathbb{Z}_2^3 \times_\varphi S_3),$$

cuja cardinalidade é $\left|\Gamma(\mathbb{Z}_q^3)\right| = 48q^3$.

As isometrias de $\mathbb{Z}_q^3$ serão dadas pelas simetrias do cubo em $\mathbb{R}^3$ (centradas na origem) compostas por translações em $\mathbb{Z}_q^3$. O grupo de simetrias do cubo $C(3)$ é bem conhecido. Ele tem 48 elementos expressos pelas matrizes M, equação (4.4). A ordem de cada isometria que deixa o vetor nulo fixado pode ser $1, 2, 3, 4$, [5]. As composições destas isometrias com as translações completará todas as isometrias próprias do espaço, isto é, movimentos rígidos, glisso-reflexões e inversões rotatórias.

A ordem máxima de uma isometria (e portanto de um subgrupo cíclico) em $\Gamma(\mathbb{Z}_q^3)$, $q \neq 4$ e $q \neq 2$, é $4q$, dada por exemplo por um movimento rígido com rotação de $\pi/4$ e translação de 1 na direção do eixo de rotação..

Caso $q = 4$. Este caso não está incluído nos teoremas anteriores. Entretanto, por considerar a Observação 4.3.1, $\mathbb{Z}_4$ é isométrico a $\mathbb{Z}_2^2$ com respeito a métrica de Lee. Então, $\mathbb{Z}_4^n$ é isométrico a $\mathbb{Z}_2^{2n}$, isto é, $\Gamma(\mathbb{Z}_4^n) \cong \Gamma(\mathbb{Z}_2^{2n}) \cong \mathbb{Z}_2^{2n} \times_\varphi \mathcal{S}_{2n}$.

É interessante considerar este caso, uma vez que é o único que possui isometrias que não são isometrias euclidianas de simetrias do $\mathbb{R}^n$. De fato, vemos que neste caso as isometrias são dadas por simetrias de um cubo euclidiano $2n$-dimensional.

Vamos considerar o caso $n = 2$. Observamos que distintamente do que foi provado no Lema 4.3.4, aqui podemos ter isometrias que levam circuitos-torre em outros circuitos como mostra a Fig. 4.12.

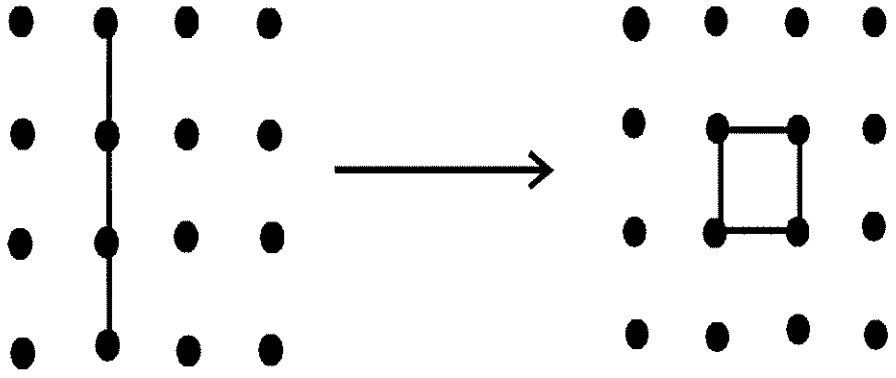

Figura 4.12: Para $q = 4$ isometrias não levam, necessariamente, circuitos-torre em circuitos-torre.

Isto pode ser visto se associarmos $\mathbb{Z}_4^2$ com os vértices de um hipercubo em $\mathbb{R}^4$ cuja configuração euclidiana coincide com a configuração de Lee.

4.4 A Não-Existência de Códigos $\mathbb{Z}_{q^n}$-Lineares

Vamos mostrar nesta seção que não é possível obter códigos $\mathbb{Z}_{q^n}$-lineares associados a $\mathbb{Z}_q^n$, com $(q, n) \neq (2, 2)$. Veremos que a não existência de um grupo cíclico de ordem q^n em $\Gamma(\mathbb{Z}_q^n)$ para $q = 2$ é também verificada para qualquer valor de n.

Teorema 4.4.1 *Sejam n e q inteiros, $n \geq 2$ e $q \geq 2$, tal que $(n, q) \neq (2, 2)$. O grupo de simetrias de $\mathbb{Z}_q^n$, $\Gamma(\mathbb{Z}_q^n)$, não possui um subgrupo cíclico de ordem maior ou igual a q^n.*

A demonstração deste teorema é uma consequência do seguinte lema que tem uma demonstração algébrica direta e que é também uma consequência direta da equação (4.7), onde $T = T(\mathbb{Z}_q^n)$ é o subgrupo das translações e $S = C(n)$ é o subgrupo das isometrias que deixam o vetor nulo fixo.

Lema 4.4.1 *Seja $\mathbb{G}$ um grupo. Sejam S e T subgrupos de $\mathbb{G}$, com T normal e abeliano, tal que $\mathbb{G} = S \times_\varphi T$. Então*

$$|gt| \leq |g| \,.\, |t| \,, \qquad \forall\, g \in S, \qquad \forall\, t \in T,$$

onde $|x|$ denota a ordem de x.

Demonstração do Teorema: O caso $q = 2$ foi considerado em [13]. O caso $(n, q) = (2, 3)$ e o caso $q = 4$ se reduz a $q = 2$. Os casos restantes, $q \neq 2$, $q \neq 4$, $(n, q) \neq (2, 3)$, implicam em

$$\Gamma(\mathbb{Z}_q^n) \cong \Gamma(\mathbb{Z}_2^n) \times_\varphi \mathbb{Z}_q^n.$$

Então,

$$z \in \Gamma(\mathbb{Z}_q^n) \Rightarrow z = x.y, x \in \Gamma(\mathbb{Z}_2^n),$$

$$y \in \mathbb{Z}_q^n \Rightarrow |x| < 2^n \; e \; |y| \leq q.$$

Portanto,

$$|z| = |x.y| \leq |x|\,|y| < 2^n q < q^{n-1} q = q^n.$$

□

Portanto, concluímos que não existe subgrupo de ordem q^n em $\Gamma(\mathbb{Z}_q^n)$ que é isomorfo a $\mathbb{Z}_{q^n}$ e também transitivo em $\mathbb{Z}_q^n$. Conseqüentemente, não existem códigos $\mathbb{Z}_{q^n}$-lineares.

4.5 Casos Especiais de $\mathbb{G}$-Linearidade

4.5.1 $\mathbb{Z}_4^n$-linearidade associada ao espaço de Hamming n-dimensional $\mathbb{Z}_2^{2n}$

Consideremos o espaço de Hamming $2n$-dimensional $\mathbb{Z}_2^{2n}$. Sabemos que

$$\mathbb{Z}_4^n \quad \text{é isométrico a} \quad \mathbb{Z}_2^{2n}.$$

Como d_L é uma métrica de grupo em $\mathbb{Z}_4^n$ temos que existem códigos $\mathbb{Z}_4^n$-lineares. Desta forma, ao obtermos códigos de grupo sobre o grupo $\mathbb{Z}_4^n$, obtemos códigos binários geometricamente uniformes mapeados através destes códigos de grupo.

Este caso é similar à $\mathbb{Z}_4$-linearidade pois os códigos de grupo sobre $\mathbb{Z}_4^n$ serão códigos de grupo sobre $\mathbb{Z}_4$ com comprimentos múltiplos de n que levam a códigos binários de comprimento múltiplo de $2n$.

Desta forma, em termos de obtenção de códigos binários, a $\mathbb{Z}_4^n$-linearidade não apresenta nada além do que a $\mathbb{Z}_4$-linearidade já havia apresentado. Porém, é importante observar o seguinte fato: o grupo de simetrias de $(\mathbb{Z}_2^{2n}, d_H)$ é o isomorfo ao produto semi-direto $\mathbb{Z}_2^{2n} \times_\varphi \mathcal{S}_{2n}$ que contém as translações sobre $\mathbb{Z}_2^{2n}$ e formam um subgrupo isomorfo a $\mathbb{Z}_2^{2n}$. A existência de $\mathbb{Z}_4^n$ como subgrupo transitivo vem do fato de que estas translações no espaço $2n$-dimensional são obtidas isometricamente por translação no espaço de Lee n-dimensional.

4.5.2 $\mathbb{G}_n$-linearidade associada a $\mathbb{Z}_2^n$

Vamos mostrar que apesar de não existirem códigos $\mathbb{Z}_{2^n}$-lineares associados ao espaço de Hamming n-dimensional $\mathbb{Z}_2^n$, ou seja, códigos binários geometricamente uniformes imagens de códigos de grupo sobre $\mathbb{Z}_{2^n}$ através de um mapeamento casado, podemos obter códigos $\mathbb{G}$-lineares, onde $\mathbb{G}$ é um grupo abeliano obtido através de reflexões sobre hiperplanos iniciadas pelo grupo cíclico $\mathbb{Z}_4$.

Vamos apresentar um subgrupo abeliano e transitivo do grupo de simetrias de $\mathbb{Z}_2^n$, $\Gamma(\mathbb{Z}_2^n)$. Para isto, vamos considerar alguns casos conhecidos e através de um processo indutivo-iterativo chegaremos no subgrupo abeliano e transitivo de $\Gamma(\mathbb{Z}_2^n)$.

Caso $n = 2$

Para este caso, $\Gamma(\mathbb{Z}_2^2) \cong \mathbb{D}_4$, e o subgrupo das rotações

$$\{i_{\mathbb{Z}_2^n}, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\}$$

é um subgrupo cíclico de $\mathbb{D}_4$ isomorfo a $\mathbb{Z}_4$ que age transitivamente sobre $\mathbb{Z}_2^2$. Este é o primeiro grupo que denotaremos por $\mathbb{G}_2$ e corresponde a $\mathbb{Z}_4$-linearidade. A representação matricial deste subgrupo tem como gerador

$$R_{\frac{\pi}{2}} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Caso $n = 3$

Para este caso, $\Gamma(\mathbb{Z}_2^3) \cong \mathbb{Z}_2^3 \times_\varphi \mathcal{S}_3$ e para obter um subgrupo transitivo consideramos o subgrupo das rotações ao redor de um eixo passando pelo centro das duas faces horizontais do cubo que pode ser dado por

$$\{i_{\mathbb{Z}_2^n}, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\} \text{ (caso } n = 2)$$

Considerando também a reflexão no plano horizontal pelo centro do cubo, ou seja, a função

$$Re_3 : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3, \quad Re(a, b, c) = (a, b, c \oplus 1).$$

O subgrupo gerado por $R_{\frac{\pi}{2}}$ e Re_3 forma, naturalmente um grupo que age transitivamente sobre $\mathbb{Z}_2^3$ e é isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$. Este grupo será denotado por $\mathbb{G}_3$. A representação matricial deste grupo tem como geradores as matrizes

$$\begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Caso $n = 4$

Para estudar este caso, observamos que existe um homomorfismo injetivo de grupos

$$i_3 : \mathbb{G}_3 \to \Gamma(\mathbb{Z}_2^4), \quad i_3(g) = i,$$

onde

$$i : \mathbb{Z}_2^3 \times \mathbb{Z}_2 \to \mathbb{Z}_2^3 \times \mathbb{Z}_2, \quad i(p, q) = i_3(g(p), q), \quad p \in \mathbb{Z}_2^3, q \in \mathbb{Z}_2$$

O subgrupo transitivo procurado, denotado por $\mathbb{G}_3$, será então definido como o grupo gerado por $i_3(\mathbb{G}_3)$ e pela reflexão Re_4, ou seja, a função

$$Re_4 : \mathbb{Z}_2^4 \to \mathbb{Z}_2^4, \quad Re(a, b, c, d) = (a, b, c, d \oplus 1).$$

Desta forma, obtemos naturalmente um subgrupo transitivo de $\Gamma(\mathbb{Z}_2^4)$, que denotaremos por

$\mathbb{G}_4$. A representação matricial deste grupo tem como geradores

$$\begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Caso geral

Neste caso, obtemos uma imersão natural (homomorfismo injetivo de grupos) dada por

$$\begin{aligned} \Gamma(\mathbb{Z}_2^n) &\longrightarrow \Gamma(\mathbb{Z}_2^{n+1}) \\ i_n(g)(p,q) &= (g(p),q). \end{aligned}$$

Isto ocorre porque $\mathbb{G}_4$ apresenta uma construção tipo abeliano (isto é, $\mathbb{G}_4$ é gerado por todos os elementos de $i_n(\mathbb{G}_3)$ mais uma reflexão Re_4.

Vamos construir, por indução, todos os subgrupos $\mathbb{G}_n \subset \Gamma(\mathbb{Z}_2^n)$ identificando

$$g \equiv i_2(g) \equiv i_3(i_2(g)) \equiv \ldots \equiv i_n(i_{n-1}(g)),$$

e denotando a reflexão vertical

$$Re_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^n, \quad Re(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_{n-1}, a_n \oplus 1).$$

Teorema 4.5.1 *$\mathbb{G}_n$ atua transitivamente sobre $\mathbb{Z}_2^n$.*

Demonstração: Vamos provar por indução. É verdade para $n = 2$. Suponhamos válido para $n = k$ e teremos $\mathbb{G}_{k+1} = \langle g, Re_{k+1} \circ g \rangle$. Dados $a = (a_1, a_2, \ldots, a_{k+1})$ e $b = (b_1, b_2, \ldots, b_{k+1})$, sabemos que

$$(b_1, b_2, \ldots, b_k) = g(a_1, a_2, \ldots, a_k),$$

para $g \in \mathbb{G}_k$. Assim, se $a_{k+1} = b_{k+1}$, então $b = g(a)$. Se $a_{k+1} \neq b_{k+1}$, então $b = Re_k \circ g(a)$.□

Identificando o hipercubo $\mathbb{Z}_2^n$ com $\{-1, 1\}^n$ podemos representar $\mathbb{G}_n$ através de matrizes $n \times n$. De fato, considere a matriz

$$\xi = \begin{bmatrix} 0 & -1 & \mathbf{0}_{2\times(n-2)} \\ 1 & 0 & \\ \mathbf{0}_{(n-2)\times 2} & & \mathbf{I}_{(n-2)\times(n-2)} \end{bmatrix},$$

que geram as 4 rotações no plano das 2 primeiras coordenadas. Sejam

$$P_k = [a_{ij}], a_{ij} = \begin{cases} 1 & se \quad i \neq k \\ 0 & se \quad i \neq j \\ -1 & se \quad i = j = k \end{cases}, k \geq 3,$$

que são as projeções sobre a k-ésima coordenada. Por exemplo,

$$P_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & & & \\ \vdots & \vdots & \vdots & & \mathbf{I_{(n-3)\times(n-3)}} & \\ 0 & 0 & 0 & & & \end{bmatrix}$$

faz a projeção da terceira coordenada no cubo.

Desta forma, $\mathbb{G}_n$ é o subgrupo abeliano gerado por ξ e P_k com a operação de multiplicação de matrizes e isomorfo a

$$\mathbb{Z}_4 \times \mathbb{Z}_2^{n-2}.$$

Encontramos, desta forma, condições para se obter códigos $\mathbb{G}_n$-lineares. Os códigos de grupo sobre $\mathbb{G}_n$ nos levarão através do mapeamento a códigos binários geometricamente uniformes. Estes códigos de grupo, dada a característica do alfabeto $\mathbb{G}_n$, sugere o estudo de códigos concatenados onde códigos de grupo sobre $\mathbb{Z}_4$ e códigos binários lineares deverão ser utilizados.

4.5.3 $\mathbb{G}$-linearidade segundo grupos não-abelianos e códigos de grupo normais

A $\mathbb{G}$-linearidade nos coloca em alguns casos a seguinte pergunta: É possível encontrar códigos de grupo sobre grupos não-abelianos (por exemplo, sobre o grupo diedral $\mathbb{D}_4$) com distâncias que sejam suficientes para levar a códigos binários melhores do que os já apresentados?

O Teorema 2.4.2 estabelece que códigos de grupo normais e sistemáticos sobre grupos não-abelianos possuem distância de Hamming 1. Considere o mapeamento $\phi : \mathbb{G} \rightarrow \mathcal{A}$ em $(\mathcal{A}, d)$,

então

$$l = \max\{d(x,0), x \in \mathcal{A}\}.$$

Desta forma teremos que a maior distância em um código de grupo sobre $\mathbb{G}$ é l, independente de qual seja o comprimento do código. Assim, quando o comprimento do código é suficientemente grande a distância é ruim.

Quando o código de grupo sistemático sobre um grupo não-abeliano não for normal temos pelo Teorema 2.4.3 que os códigos são assintoticamente ruins.

4.5.4 Códigos $\mathbb{Z}_9$-lineares e $\mathbb{Z}_8$-lineares através de uma definição mais fraca

Apresentaremos nesta seção dois exemplos de códigos binários e ternários que podem ser construídos através da escolha de mapeamentos cuja propriedade é mais fraca do que a exigida na definição da $\mathbb{G}$-linearidade.

Considere o código 9-ário e seus respectivos pesos,

Palavra-Código	**Peso de Lee**
00	0
13	4
26	5
30	3
43	7
56	7
60	3
73	5
86	4

este é um $(2,1,3)$-código de grupo sobre $\mathbb{Z}_9$.

Através do rótulo mostrado na Tabela 4.3 e do mapeamento dado pela função $\phi : \mathbb{Z}_9^2 \to \mathbb{Z}_3^4$,

$$\phi(a,b) = (\beta(a), \alpha(a), \beta(a+b), \gamma(a+b)),$$

$\mathbf{c}$	$\alpha(\mathbf{c})$	$\beta(\mathbf{c})$	$\gamma(\mathbf{c})$
0	0	0	0
1	1	0	2
2	2	0	1
3	0	1	2
4	1	1	1
5	2	1	0
6	0	2	1
7	1	2	0
8	2	2	2

Tabela 4.3: Tabela do rotulamento

obtemos o código ternário

Palavra-Código	**Peso de Lee**
0000	0
0111	3
0222	3
1012	3
1120	3
1201	3
2021	3
2102	3
2210	3

Este é um $(4, 2, 3)$-código de grupo ternário. Observe que não temos uma isometria mas a distância mínima do código é mantida. A compatibilidade da distância de Lee com a operação do grupo em $\mathbb{Z}_9$ é mantida. Apesar de não estar incluído na definição apresentada da $\mathbb{G}$-linearidade, esta é uma situação atípica que merece ser estudada.

Considere agora o mapeamento $\phi : \mathbb{Z}_8 \to \mathbb{Z}_2^4$, mostrado na Tabela 4.4.

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$	$\delta(c)$
0	0	0	0	0
1	0	0	1	1
2	0	1	0	1
3	0	1	1	0
4	1	1	1	1
5	1	1	0	0
6	1	0	1	0
7	1	0	0	1

Tabela 4.4: Tabela do mapeamento octário

Este é um mapeamento não sobrejetor apesar da distância de Lee estar casada com a operação do grupo octário. Este mapeamento não é uma imersão isométrica. Por outro lado, se considerarmos o código e sua imagem através deste mapeamento concluímos que

$\mathcal{C} \subset \mathbb{Z}_8^2$	d_L	$\mathbb{C} \subset \mathbb{Z}_2^4$
00	0	00000000
13	4	00110110
26	4	01011010
30	4	11111111
44	8	11111111
57	4	11001001
62	4	10100101
75	4	10011100

Desta forma, apresentamos um mapeamento que, apesar de não satisfazer as condições básicas da $\mathbb{G}$-linearidade, quando consideramos um código particular temos as propriedades desejadas.

4.6 Conclusões

Neste capítulo, apresentamos o conceito de códigos $\mathbb{G}$-lineares $\mathbb{C}$ como sendo uma extensão do conceito da $\mathbb{Z}_{2^k}$-linearidade.

Para a extensão, foi exigida a isometria entre os dois alfabetos considerados. Além disso, exigiu-se que a métrica do primeiro alfabeto seja compatível com a operação do grupo obtendo assim códigos geometricamente uniformes. Esta foi a base da definição da $\mathbb{G}$-linearidade definida na Seção 4.2, onde foram apresentados alguns exemplos.

Na Seção 4.3 foram apresentados uma caracterização exata do grupo de simetrias de $\mathbb{Z}_q^n$. Através da demonstração da não-existência de um sugrupo cíclico transitivo de ordem q^n do grupo de simetrias de $\mathbb{Z}_q^n$ mostramos que não existem códigos $\mathbb{Z}_{q^n}$-lineares.

Finalmente, na Seção 4.5, consideramos alguns casos especiais da $\mathbb{G}$-linearidade.

Capítulo 5

Conclusões e Propostas para Trabalhos Futuros

5.1 Objetivos

Neste trabalho o objetivo principal foi propor uma extensão da $\mathbb{Z}_4$-linearidade de forma que a técnica de construção de códigos binários de comprimento par seja aplicável para outros alfabetos.

Dentro deste objetivo foram consideradas propriedades básicas para obtenção desta extensão:

- A métrica de Lee em $\mathbb{Z}_4$ é uma métrica de grupo o que permite calcular a distância de Lee mínima através do peso de Lee mínimo.
- Existe uma isometria entre os espaços métricos $\mathbb{Z}_4$ e $\mathbb{Z}_2^2$.
- A primeira e a segunda propriedades determinam que o espaço de Hamming $\mathbb{Z}_2^2$ está casado ao grupo $\mathbb{Z}_4$.
- Os códigos binários obtidos através da $\mathbb{Z}_4$-linearidade são geometricamentes uniformes.

5.2 Contribuições

As principais contribuições deste trabalho podem ser resumidas como segue:

No Capítulo 3 apresentamos uma extensão da $\mathbb{Z}_4$-linearidade para $\mathbb{Z}_{2^k}$-linearidade de forma que à existência de códigos $\mathbb{Z}_{2^k}$-lineares esteja vinculada a existência de um subgrupo cíclico transitivo do grupo de simetrias de $\mathbb{Z}_2^k$. Foram apresentadas três formas de definição mas que não constituíram a maneira mais adequada de obter uma técnica de construção códigos binários tão eficiente quanto a da $\mathbb{Z}_4$-linearidade.

Mostramos a não-existência de subgrupos cíclicos e, portanto, para $k > 2$,não é possível obter códigos $\mathbb{Z}_{2^k}$-lineares neste contexto. Além disso, apresentamos tabelas de códigos binários $\mathbb{Z}_4$-lineares de comprimento menor ou igual a 20 e códigos octários com distância esférica.

Concluímos esta análise com a apresentação de tabelas de códigos sobre $\mathbb{Z}_4$ e $\mathbb{Z}_8$, com distância de Lee e distância esférica.

No Capítulo 4, estendemos o conceito da $\mathbb{Z}_{2^k}$-linearidade para a $\mathbb{G}$-linearidade, onde $\mathbb{G}$ é um grupo, com o objetivo de propor uma técnica de construção de códigos geometricamente uniformes sobre alfabetos quaisquer, a partir de códigos de grupo sobre um grupo $\mathbb{G}$.

Verificamos que esta definição está diretamente relacionada com a existência de um subgrupo transitivo do grupo de simetrias do conjunto de sinais considerado. Diante disto, estudou-se o grupo de simetrias do espaço de Lee n-dimensional de ordem q, um espaço métrico muito relevante para codificação e modulação.

Através da obtenção do grupo de simetrias do espaço de Lee n-dimensional de ordem q mostramos que não é possível obter códigos $\mathbb{Z}_{q^n}$-lineares associados a $\mathbb{Z}_q^n$.

Finalmente foram apresentados alguns casos especiais de $\mathbb{G}$-linearidade.

5.3 Propostas e Sugestões

- Estudo de códigos não-normais sobre grupos não-abelianos para verificar a viabilidade de utilização dos mesmos para a construção de bons códigos binários. Por exemplo, o estudo de códigos de grupo sobre o grupo $\mathbb{D}_4$, para a construção de códigos binários de

comprimento múltiplo de 3 através do mapeamento $\phi : \mathbb{D}_4^n \rightarrow \mathbb{Z}_2^{3n}$.

- Dada a existência $\mathbb{G}$-linearidade associada a $\mathbb{Z}_2^n$ através de grupos abelianos do tipo $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-2}$, é relevante o estudo de códigos concatenados construídos a partir de códigos de grupo quaternários e códigos binários lineares. Este estudo permitirá verificar a viabilidade dos mesmos para construção de códigos binários de qualquer comprimento.

- Estabelecimento em $(\mathbb{Z}_q^n, d_L)$ de todos os subgrupos transitivos não-cíclicos (abelianos ou não) que possam permitir obter códigos $\mathbb{G}$-lineares.

- Estudo da viabilidade de considerar a $\mathbb{G}$-linearidade associada a $(\mathbb{Z}_q^n, d)$, onde d é uma distância diferente da distância de Lee.

- Construção de outros mapeamentos não necessariamente isométricos mas que a distância mínima seja preservada. De uma maneira geral, enfraquecer a propriedade de isometria de forma a se obter casos similares ao apresentado na subseção 4.5.4.

Apêndice A

Prova do Lema 3.3.1

Lema: A equação

$$\prod_{i=1}^{l} m_i = \sum_{i=1}^{l} m_i, \quad l \geq 2, m_i \geq 2,$$

nas incógnitas m_i, l, sobre $\mathbb{N}$ somente tem solução para $l = 2$, e $m_1 = m_2 = 2$.

Demonstração: Quando $l = 2$, temos:

- $m_1 = m_2 = 2 \Rightarrow m_1.m_2 = m_1 + m_2.$
- $m_1 \geq 2, m_2 > 2 \rightarrow \begin{cases} m_1 = 2 + m_1', & m_1' \geq 0 \\ m_2 = 2 + m_2', & m_2' > 0 \end{cases}$

  Então

$$\begin{aligned} m_1 \cdot m_2 = (2 + m_1') \cdot (2 + m_2') &= 4 + 2m_1' + 2m_2' + m_1' \cdot m_2' \\ &= (2 + m_1') + (2 + m_2') + (m_1' + m_2' + m_1' \cdot m_2') > \\ &> (2 + m_1') + (2 + m_2') = m_1 + m_2. \end{aligned}$$

Quando $l = 3$, temos

$$\begin{cases} m_1 = 1 + m_1', & m_1' > 0 \\ m_2 = 1 + m_2', & m_2' > 0 \\ m_3 = 1 + m_3', & m_3' > 0 \end{cases}$$

Então

$$m_1 \cdot m_2 \cdot m_3 = ((m_1' + 1) \cdot (m_2' + 1) \cdot (m_3' + 1) =$$

$$m_1' \cdot m_2' \cdot m_3' + m_1' \cdot m_2' + m_1' \cdot m_3' + m_2' \cdot m_3' + m_1' + m_2' + m_3' + 1 =$$

$$(m_1' + 1) + (m_2' + 1) + (m_3' + 1) + \underbrace{\underbrace{(\underbrace{m_1' \cdot m_2' \cdot m_3'}_{>1} + \underbrace{m_1' \cdot m_2'}_{>1} + \underbrace{m_1' \cdot m_3'}_{>1} + \underbrace{m_2' \cdot m_3'}_{>1} - 2)}_{>4}}_{>2}$$

$$> \quad m_1 + m_2 + m_3.$$

Afirmamos que para $l \geq 3$,

$$\prod_{i=1}^{l} m_i > \sum_{i=1}^{l} m_i.$$

Por indução, suponhamos verdadeiro para $l = k$, isto é,

$$\prod_{i=1}^{k} m_i > \sum_{i=1}^{k} m_i.$$

Então

$$\prod_{i=1}^{k+1} m_i = m_{k+1} \prod_{i=1}^{k} m_i > \underbrace{m_{k+1}}_{>1} \underbrace{\sum_{i=1}^{k} m_i}_{\geq 3} > m_{k+1} + \sum_{i=1}^{k} m_i = \sum_{i=1}^{k+1} m_i. \square$$

Apêndice B

Classificação de Grupos Finitos de Ordem ≤ 15

O problema de classificar grupos finitos é o problema central da Teoria de Grupos Finitos. Como o número de tabelas de Cayley é finito, pois é elaborada a partir de um número finito de elementos, existe um número finito de grupos não-isomorfos de uma ordem dada qualquer.

Apresentaremos uma tabela com as seguintes informações:

- Coluna 1: Ordem do grupo ou o número de elementos do grupo;
- Coluna 2: Número de grupos não-isomorfos que possuam a ordem fixada na coluna 1;
- Coluna 3: Identificação de cada um dos grupos através de grupos isomorfos conhecidos;
- Coluna 4: Justificativa do que foi apresentado.
- Coluna 5: Referência à figura que apresenta a cadeia de subgrupos.

Alguns teoremas são importantes para esta classificação e serão lembrados aqui:

Teorema B.1 *[32][34]Para todo $n \in \mathbb{N}^*$, existe um grupo cíclico de ordem n, $(\mathbb{Z}_n, \oplus)$. Além disso, se n é primo este grupo é único, a menos de um isomorfismo.*

Teorema B.2 *[2]Se p é um número primo, então qualquer grupo de ordem p^2 ou é cíclico ou é isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Teorema B.3 *[2]Se p é um primo í mpar, então qualquer grupo de ordem $2p$ ou é cíclico ou é o grupo diedral $\mathbb{D}_p$.*

Teorema B.4 *[2]Todo grupo de ordem 8 é isomorfo a um dos seguintes grupos:*

- $(\mathbb{Z}_8, \oplus)$,
- $(\mathbb{Z}_4 \times \mathbb{Z}_2, \oplus)$,
- $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$,
- $(\mathbb{D}_4, \circ)$ ou
- $\mathbb{Q}_8$.

Teorema B.5 *[2]Todo grupo de ordem 12 é isomorfo a um dos seguintes grupos:*

- $(\mathbb{Z}_{12}, \oplus)$,
- $(\mathbb{Z}_6 \times \mathbb{Z}_2, \oplus)$,
- $(\mathbb{D}_6, \circ)$,
- $\mathcal{D}_4$ ou
- $\mathcal{A}_4$.

Teorema B.6 *[32]Se p e q são primos distintos com $p < q$, então todo grupo $\mathbb{G}$ de ordem pq tem um subgrupo simples de ordem q e este subgrupo é normal em $\mathbb{G}$. Então $\mathbb{G}$ não é simples. Se q não é congruente a 1 módulo p, então $\mathbb{G}$ é abeliano e cíclico.*

Ordem	No.	Grupos	Prova	Figura
1	1	$\{e_{\mathbb{G}}\}$	Definição 2.2.1	
2	1	$(\mathbb{Z}_2, \oplus)$	Teorema B.1	B.1
p (primo)	1	$(\mathbb{Z}_p, \oplus)$	Teorema B.1	B.1
4	1.2	$(\mathbb{Z}_4, \oplus)$	Teorema B.1	B.1
	2.2	$(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$	Teorema B.2	B.1
6	1.2	$(\mathbb{Z}_6, \oplus)$	Teorema B.3	B.2
	2.2	$(\mathcal{S}_3, \circ) \cong (\mathbb{D}_3, \circ)$	Teorema B.3	B.2
8	1.5	$(\mathbb{Z}_8, \oplus)$	Teorema B.4	B.3
	2.5	$(\mathbb{Z}_4 \times \mathbb{Z}_2, \oplus)$	Teorema B.4	B.4
	3.5	$(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$	Teorema B.4	B.5
	4.5	$(\mathbb{D}_4, \circ)$	Teorema B.4	B.6
	5.5	$(\mathbb{Q}_8, \otimes) \cong \mathcal{D}_2$	Teorema B.4	B.3
9	1.2	$(\mathbb{Z}_9, \oplus)$	Teorema B.2	B.7
	2.2	$(\mathbb{Z}_3 \times \mathbb{Z}_3, \oplus)$	Teorema B.2	B.8
10	1.2	$(\mathbb{Z}_{10}, \oplus)$	Teorema B.3	B.9
	2.2	$(\mathbb{D}_5, \circ)$	Teorema B.3	B.10

O	No.	Grupos	Justificativa	Figura
12	1.5	$(\mathbb{Z}_{12}, \oplus)$	Teorema B.5	B.11
	2.5	$(\mathbb{Z}_6 \times \mathbb{Z}_2, \oplus)$	Teorema B.5	B.12
	3.5	$\mathbb{D}_6$	Teorema B.5	B.13
	4.5	$\mathcal{D}_3$	Teorema B.5	B.14
	5.5	$\mathcal{A}_4$	Teorema B.5	B.15
14	1.2	$(\mathbb{Z}_{14}, \oplus)$	Teorema B.3	B.16
	2.2	$(\mathbb{D}_7, \circ)$	Teorema B.3	B.17
15	1	$(\mathbb{Z}_{15}, \oplus)$	Teorema B.6	B.18

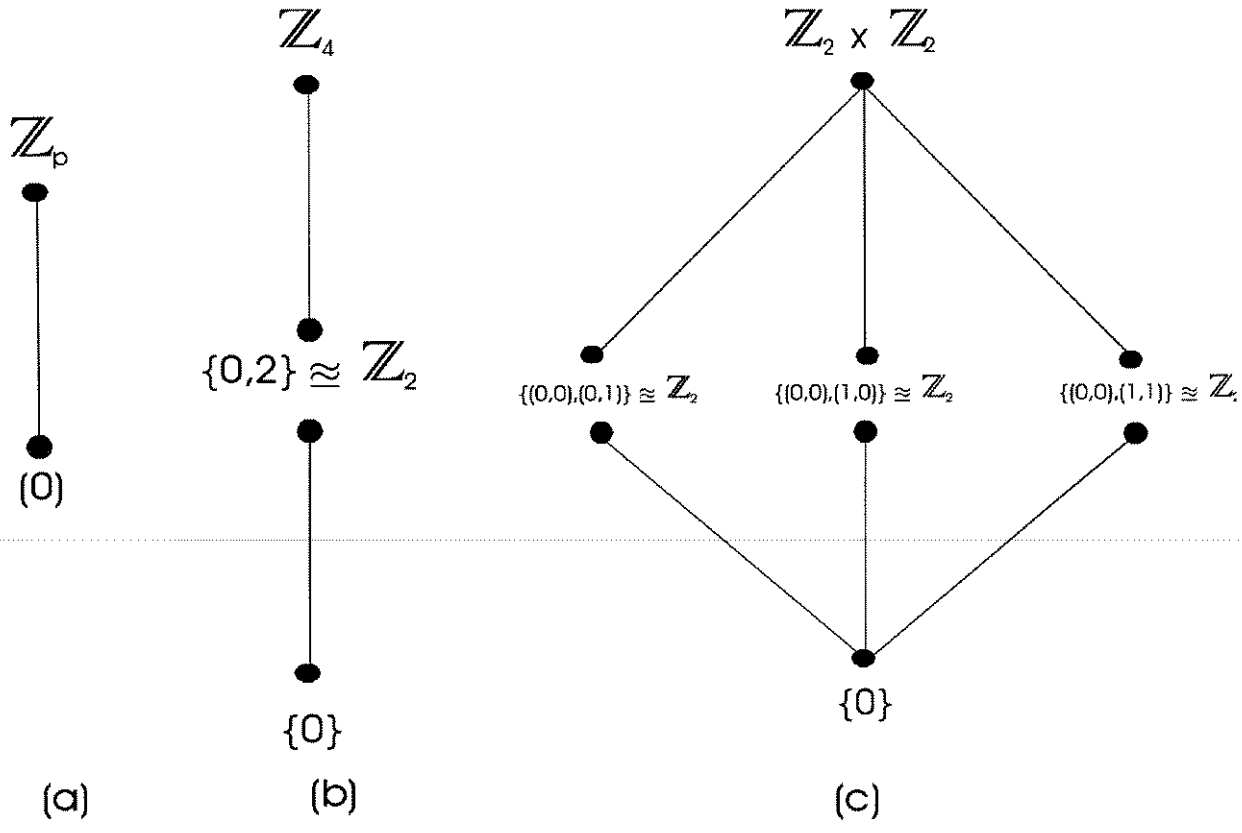

Figura B.1: (a) Grupo de ordem p, p primo, (b) Grupo de ordem 4: cíclico (c) Grupo de ordem 4: não-cíclico

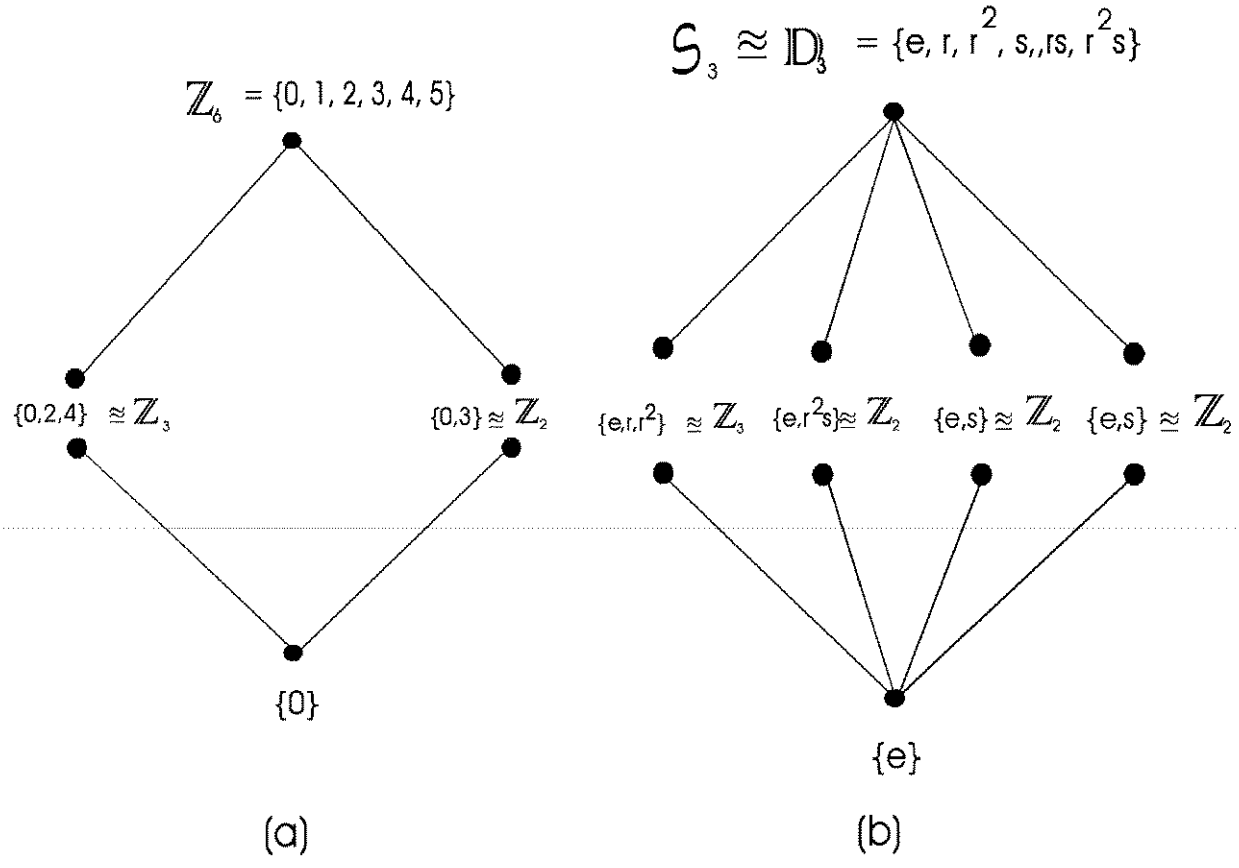

Figura B.2: (a) Grupo de ordem 6: cíclico (b) Grupo de ordem 6: não-abeliano

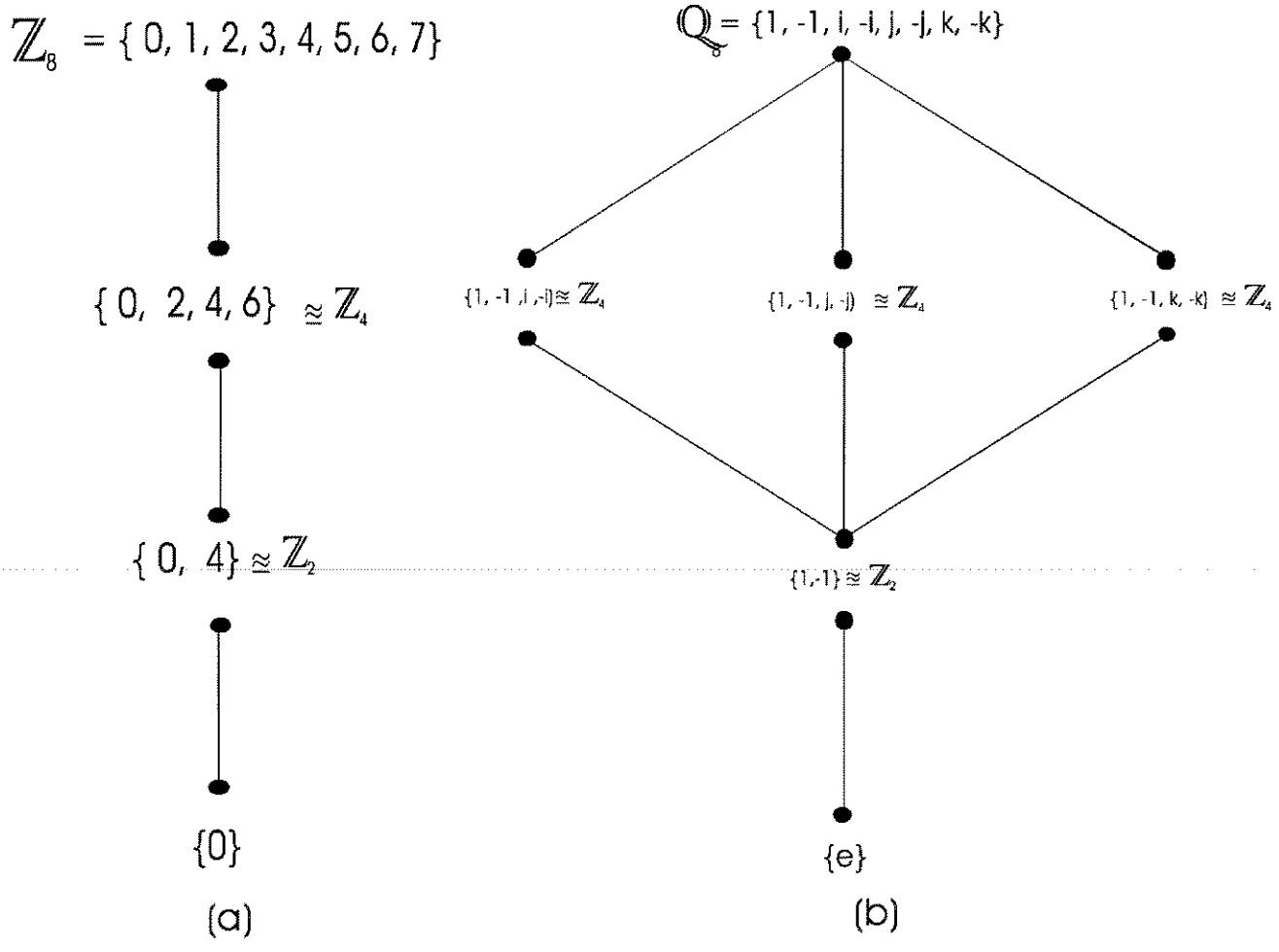

Figura B.3: (a) Grupo de ordem 8: cíclico (b) Grupo de ordem 8: quatérnios

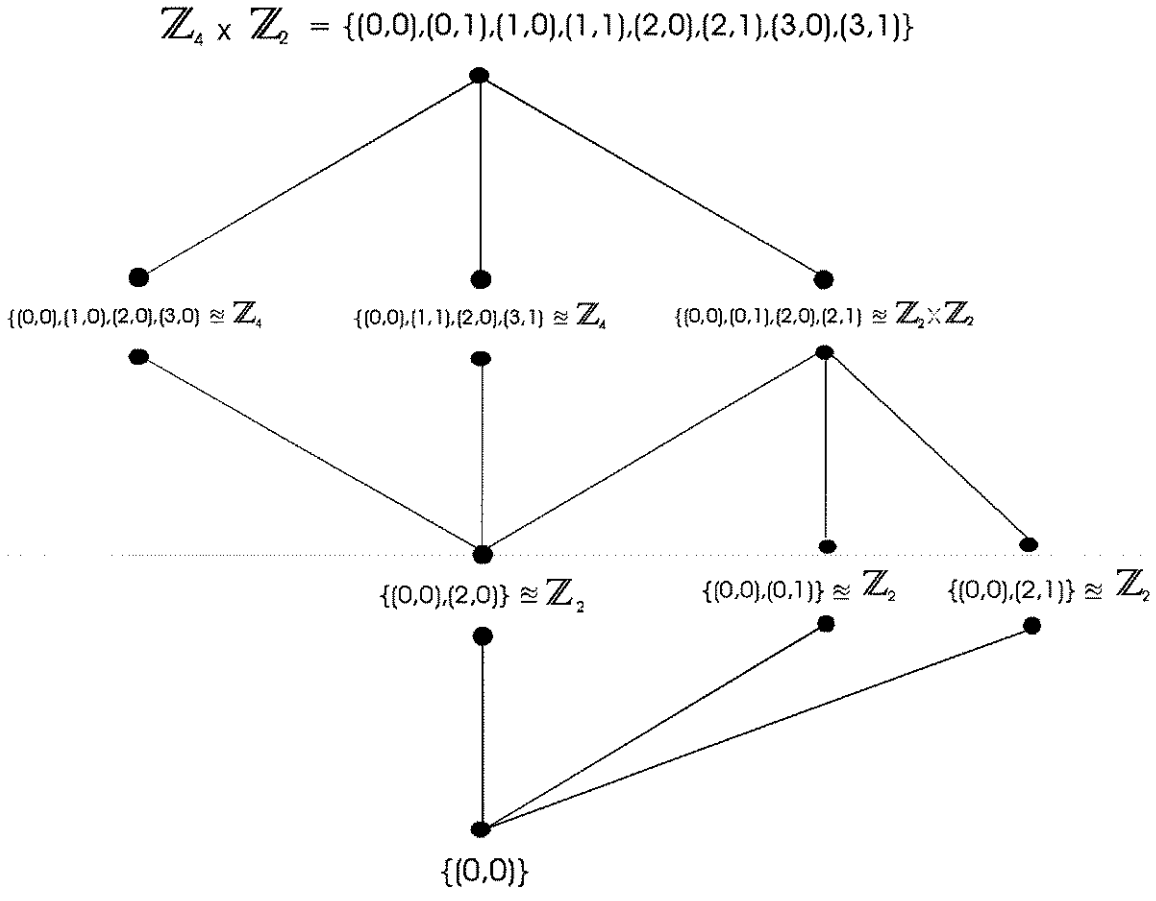

Figura B.4: Grupo de ordem 8: abeliano não-cíclico

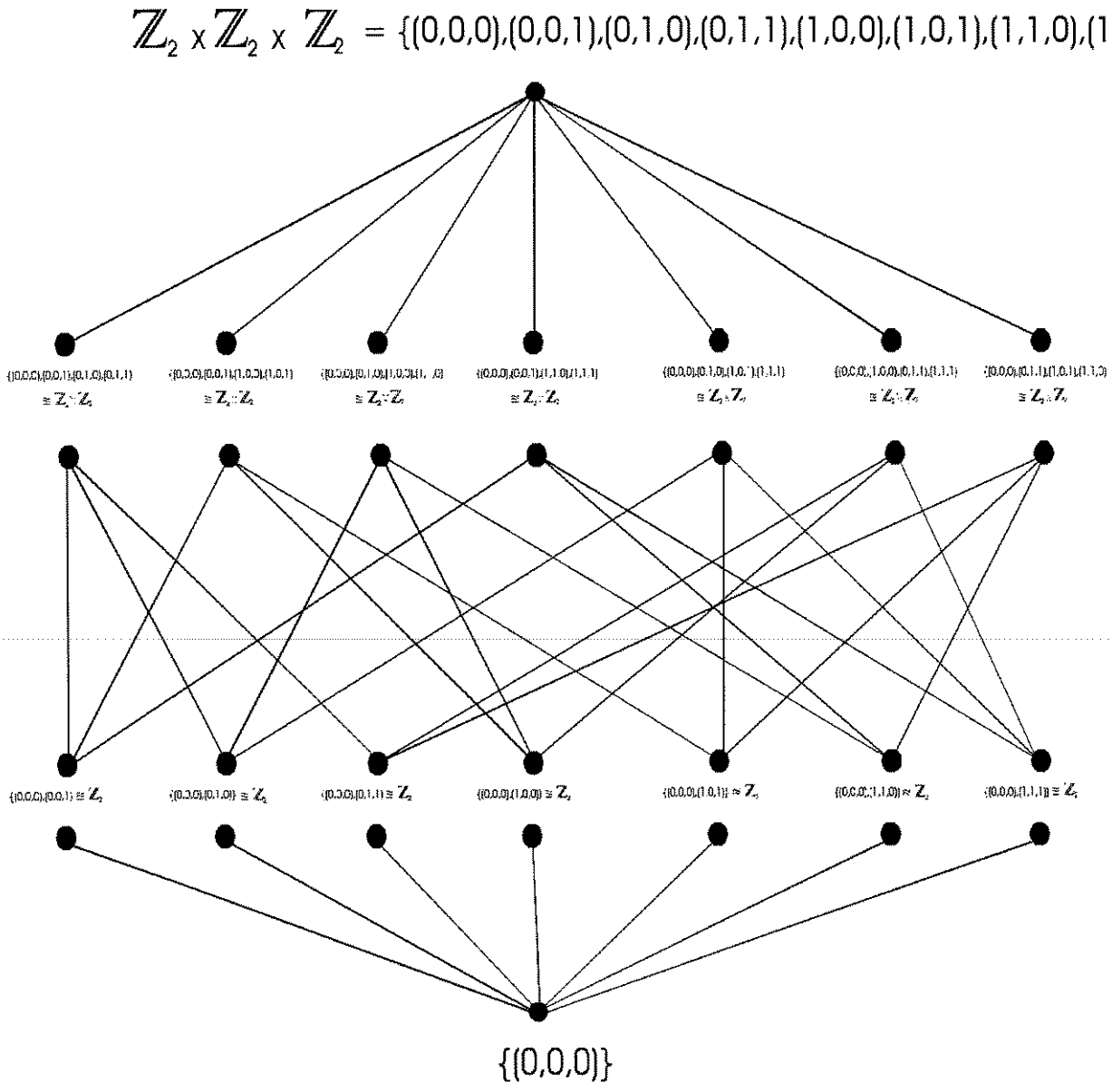

Figura B.5: Grupo de ordem 8: abeliano não-cíclico

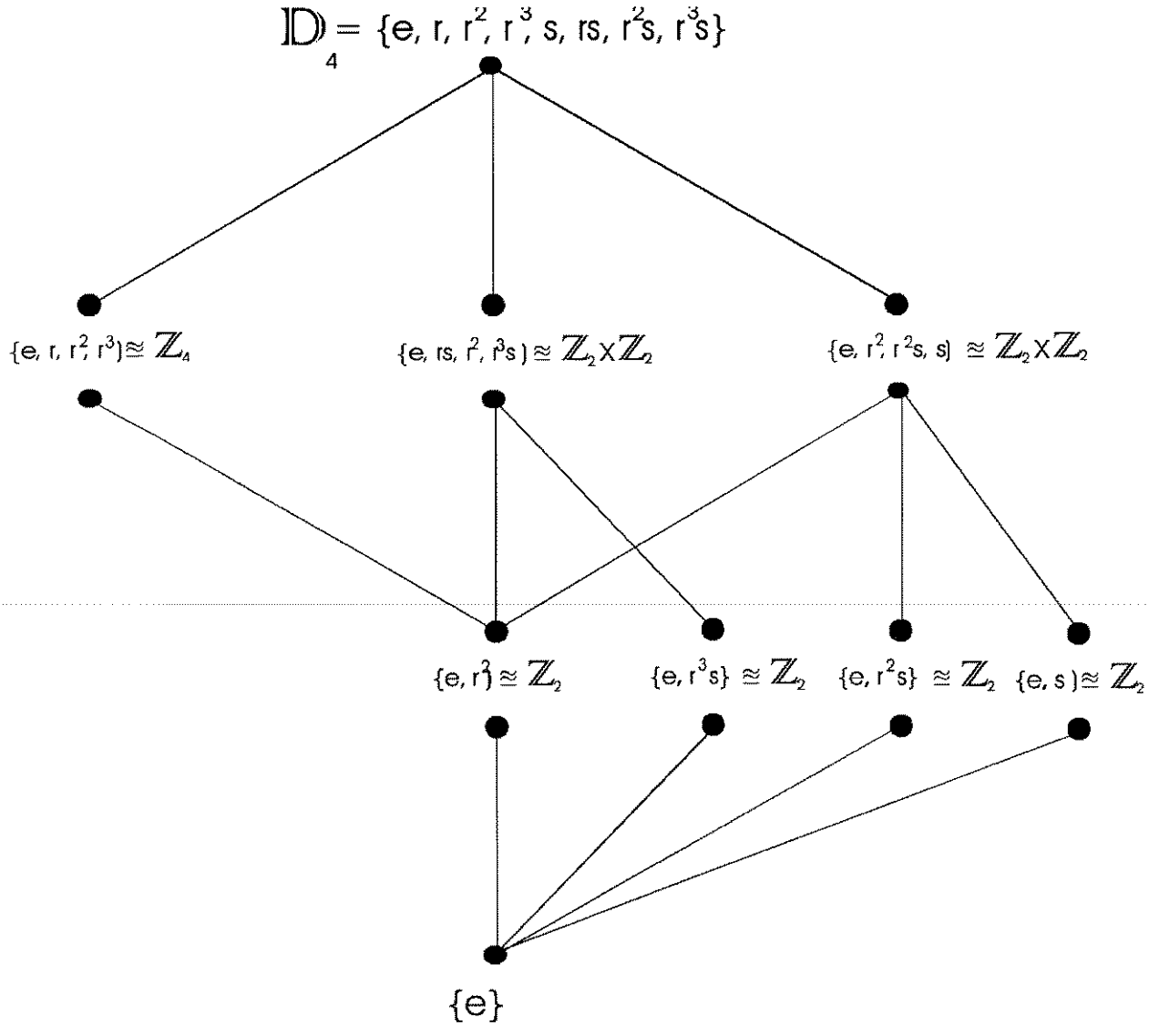

Figura B.6: Grupo de ordem 8: diedral

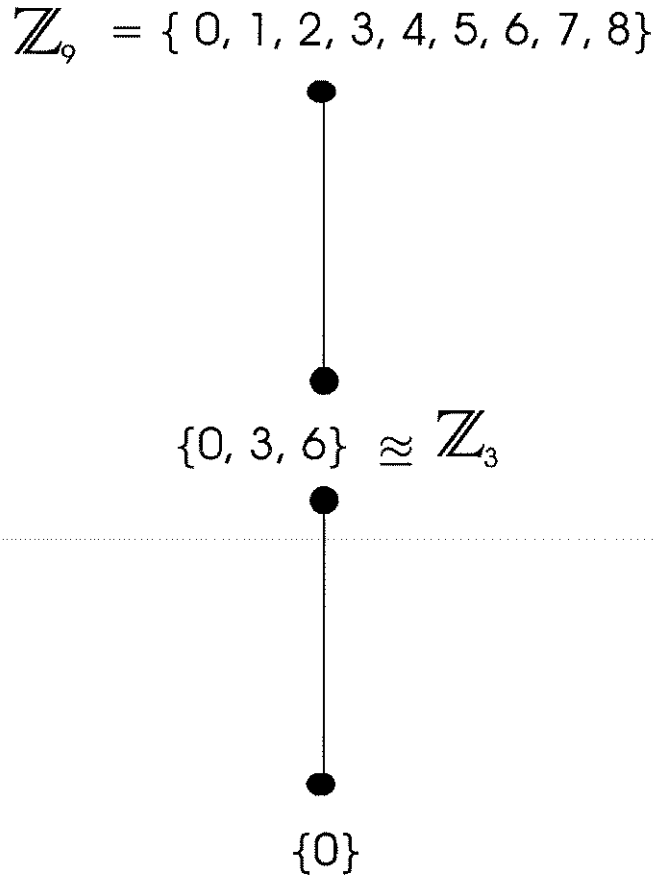

Figura B.7: Grupo de ordem 9: cíclico

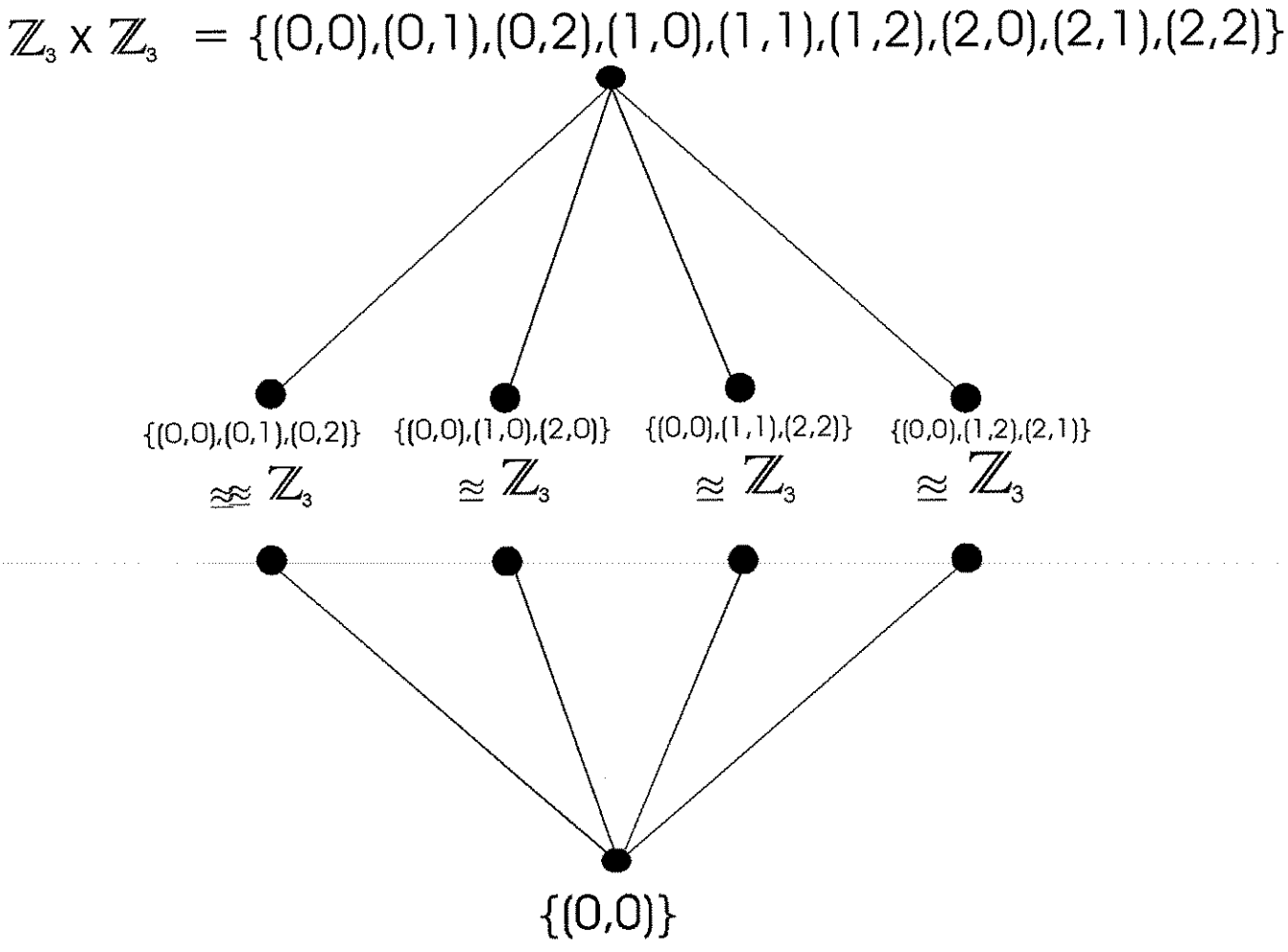

Figura B.8: Grupo de ordem 9: não-cíclico

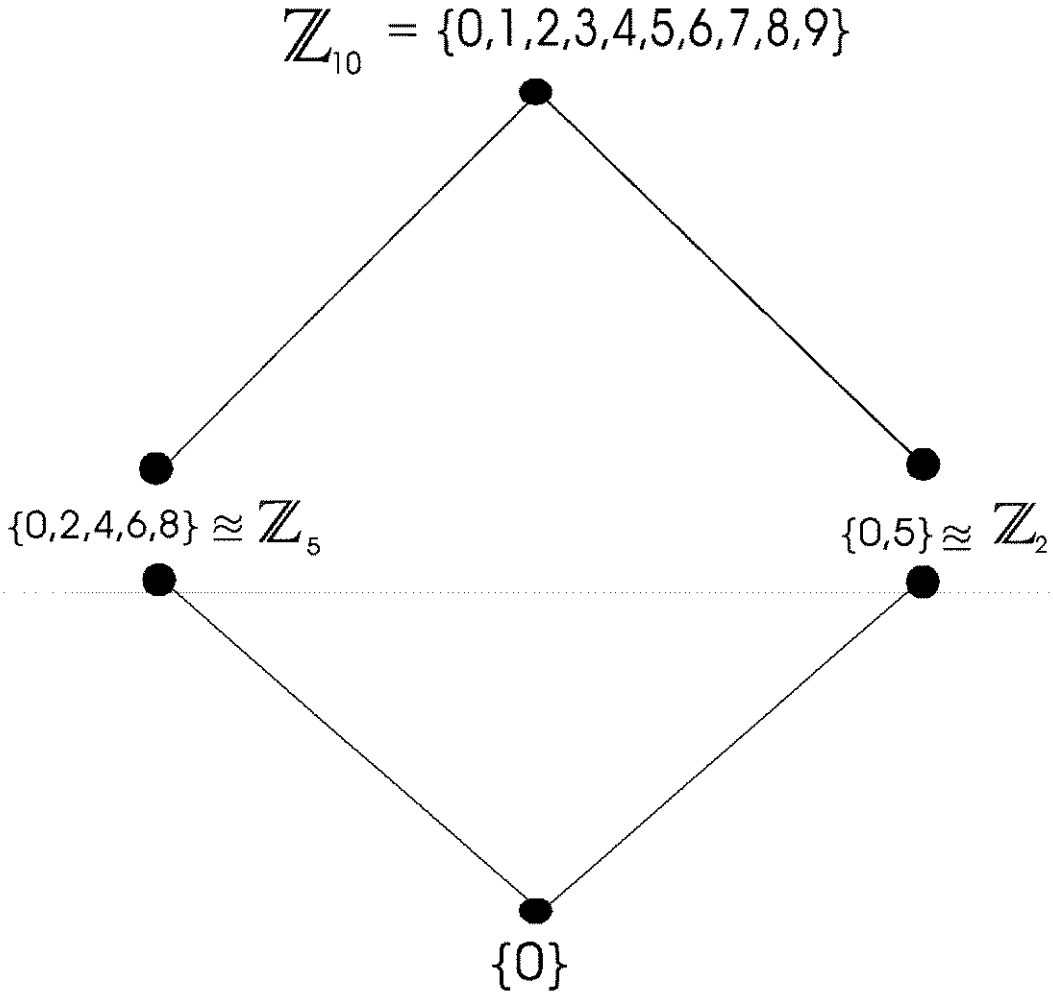

Figura B.9: Grupo de ordem 10: cíclico

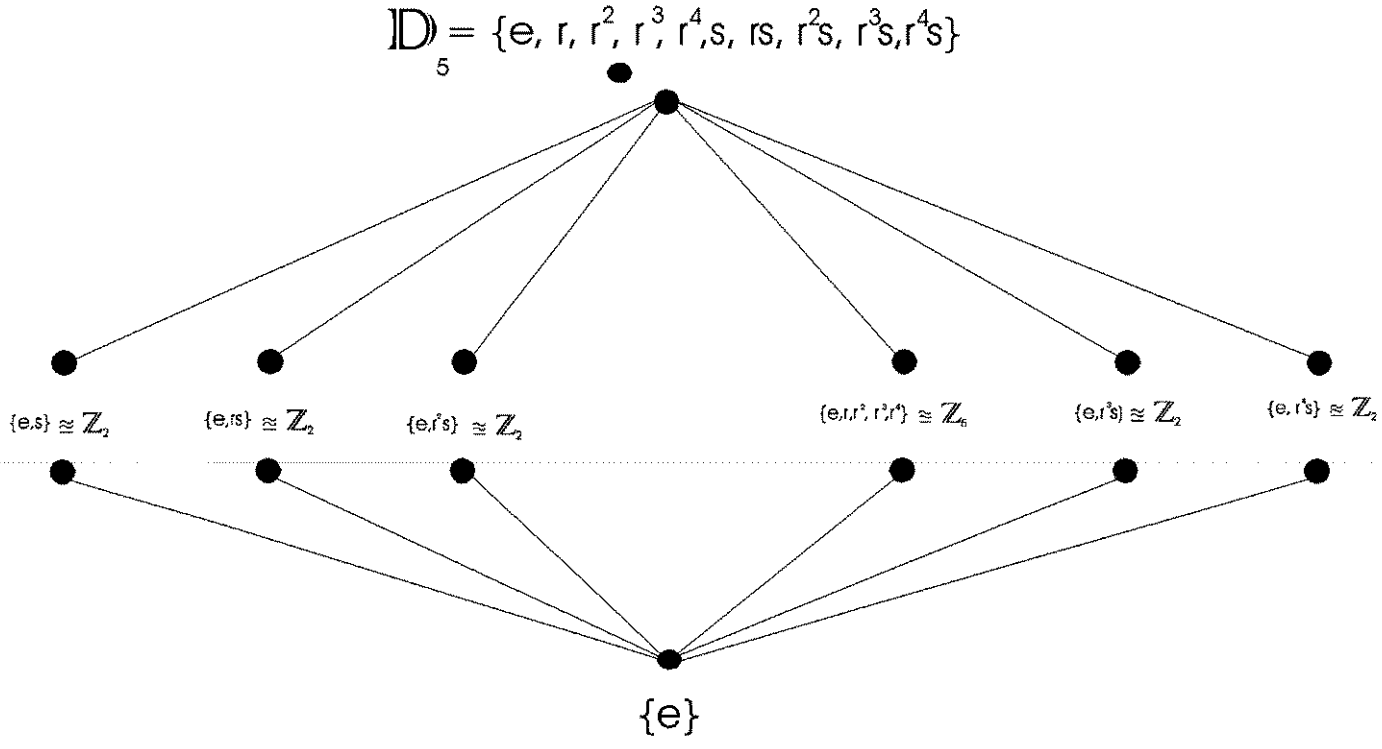

Figura B.10: Grupo de ordem 10: não-cíclico - diedral

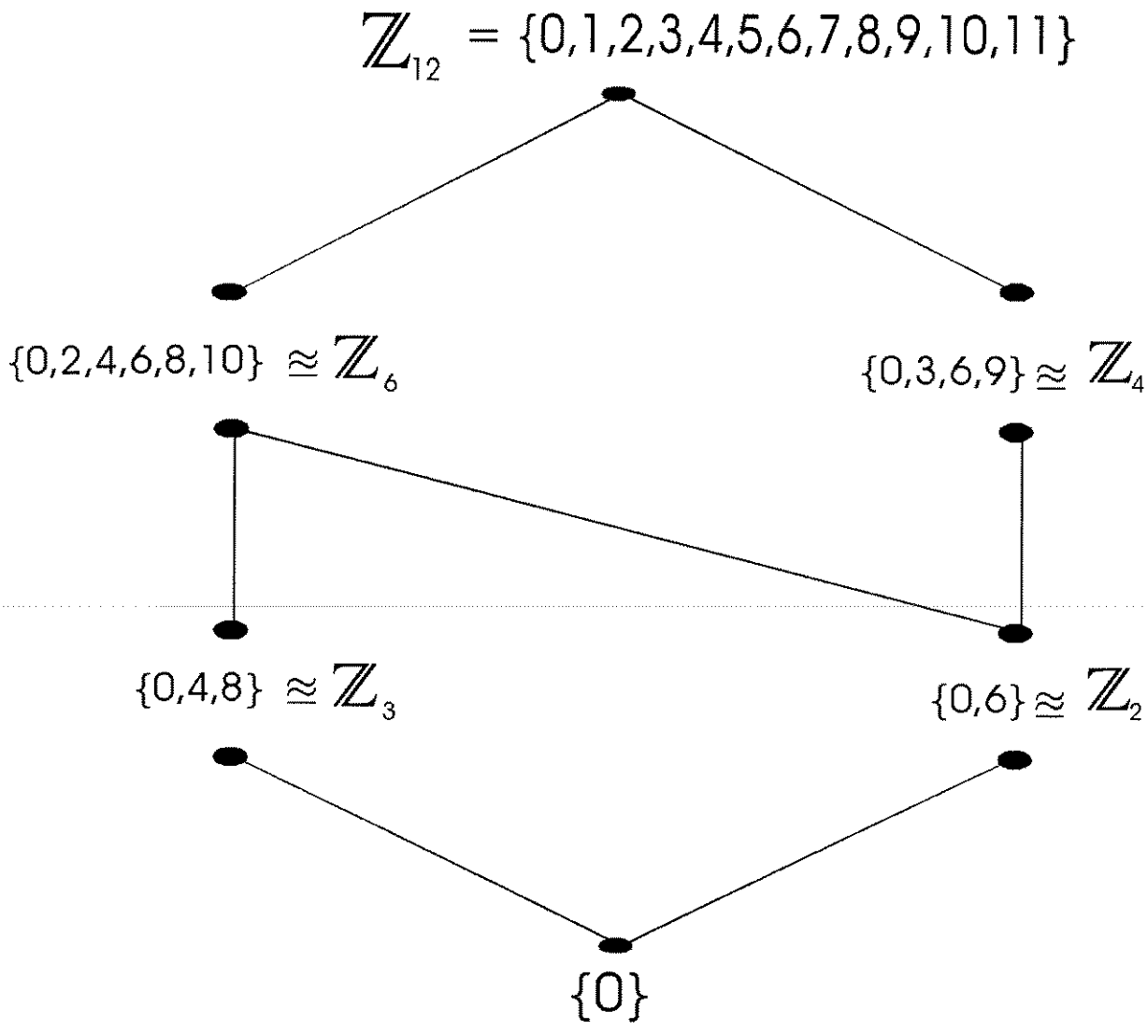

Figura B.11: Grupo de ordem 12: cíclico

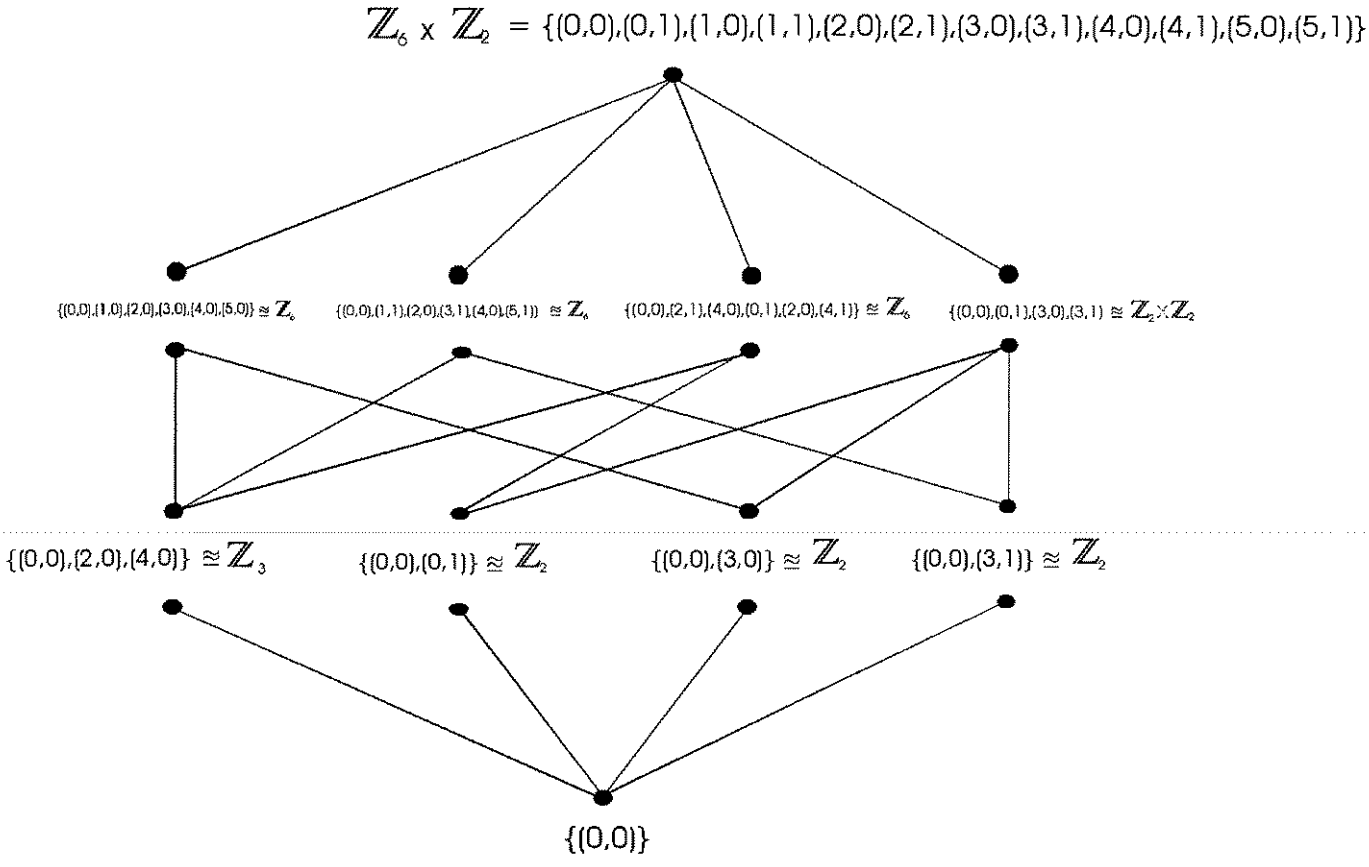

Figura B.12: Grupo de ordem 12: abeliano não-cíclico

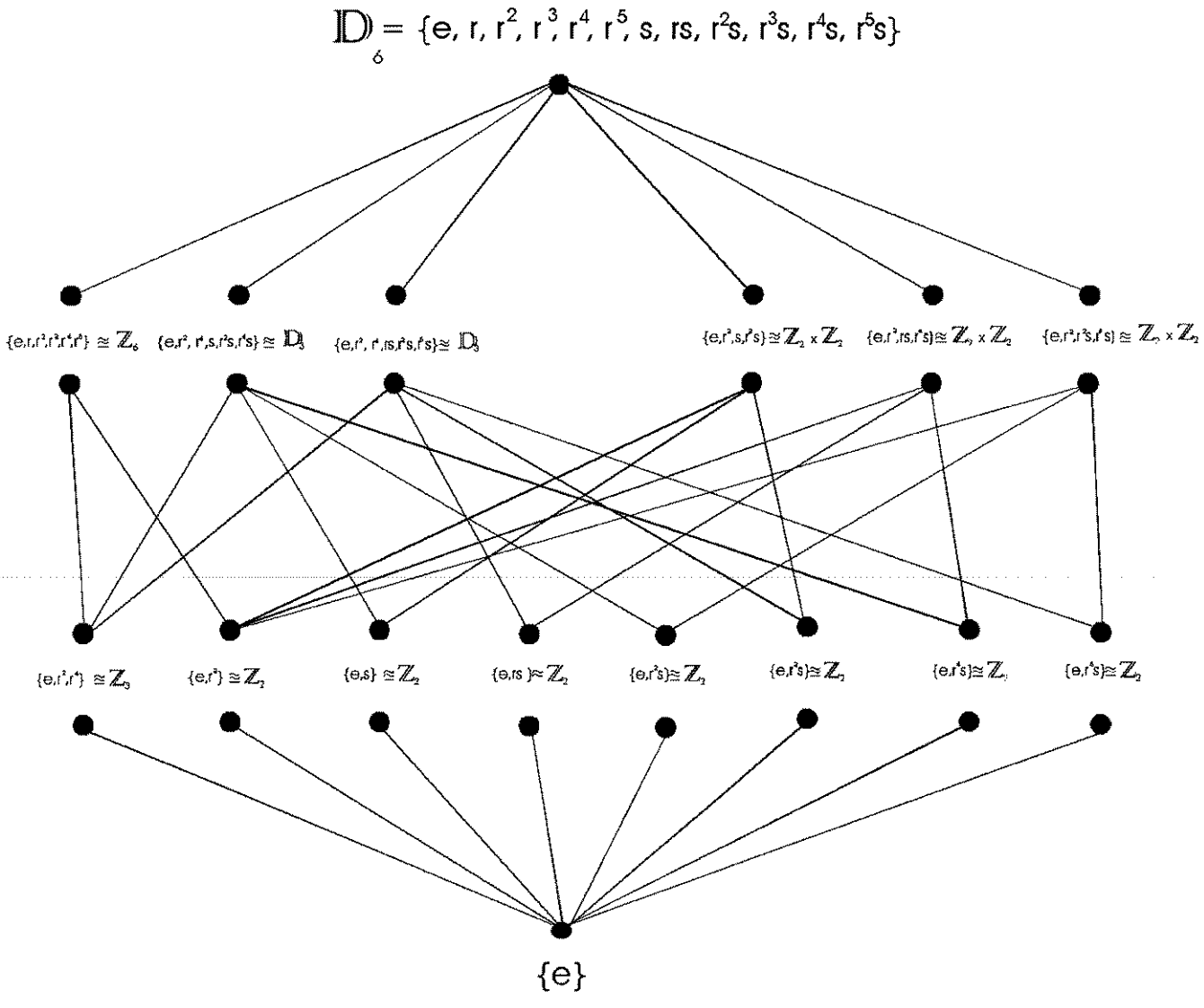

Figura B.13: Grupo de ordem 12: não-abeliano - diedral

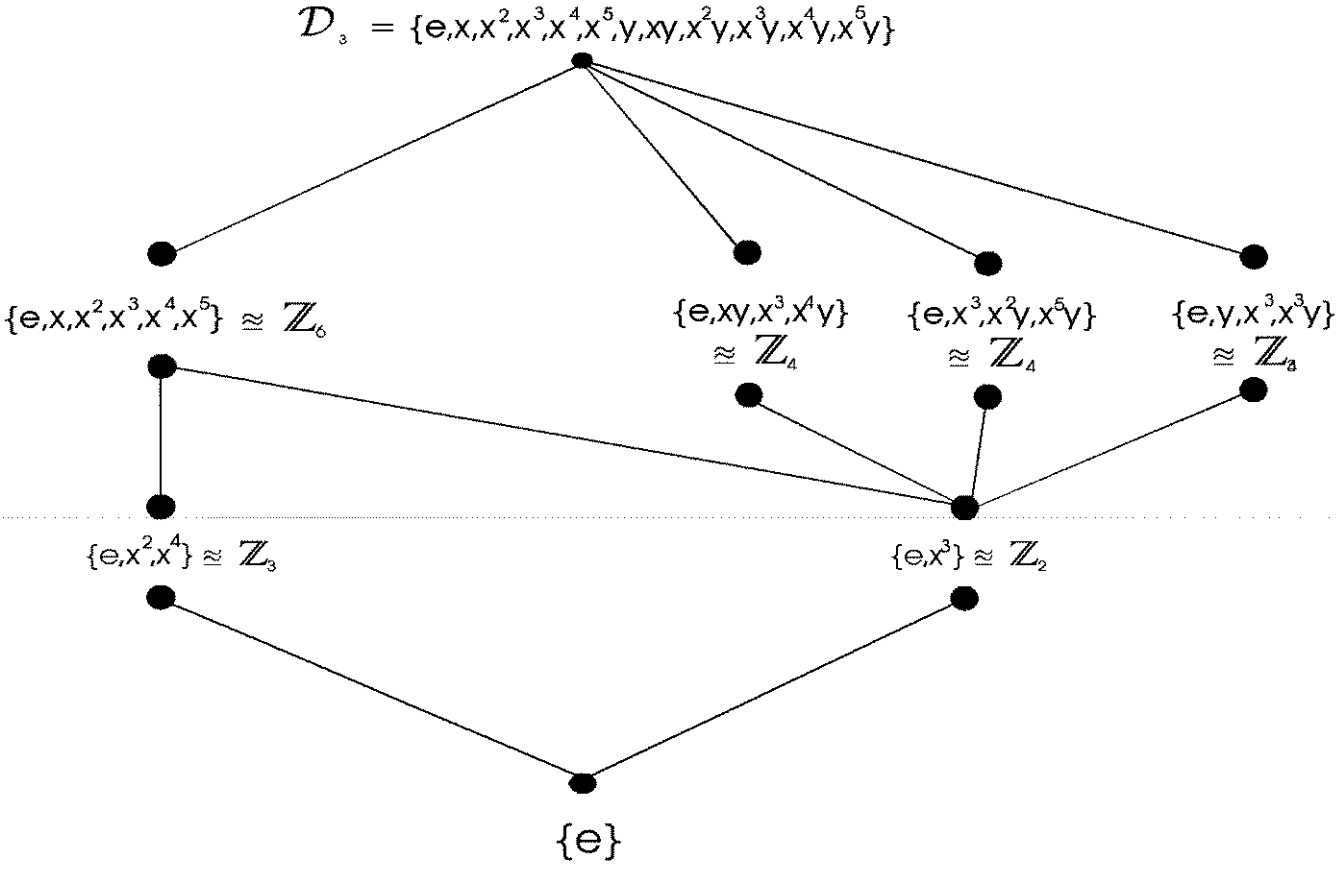

Figura B.14: Grupo de ordem 12: dicíclico

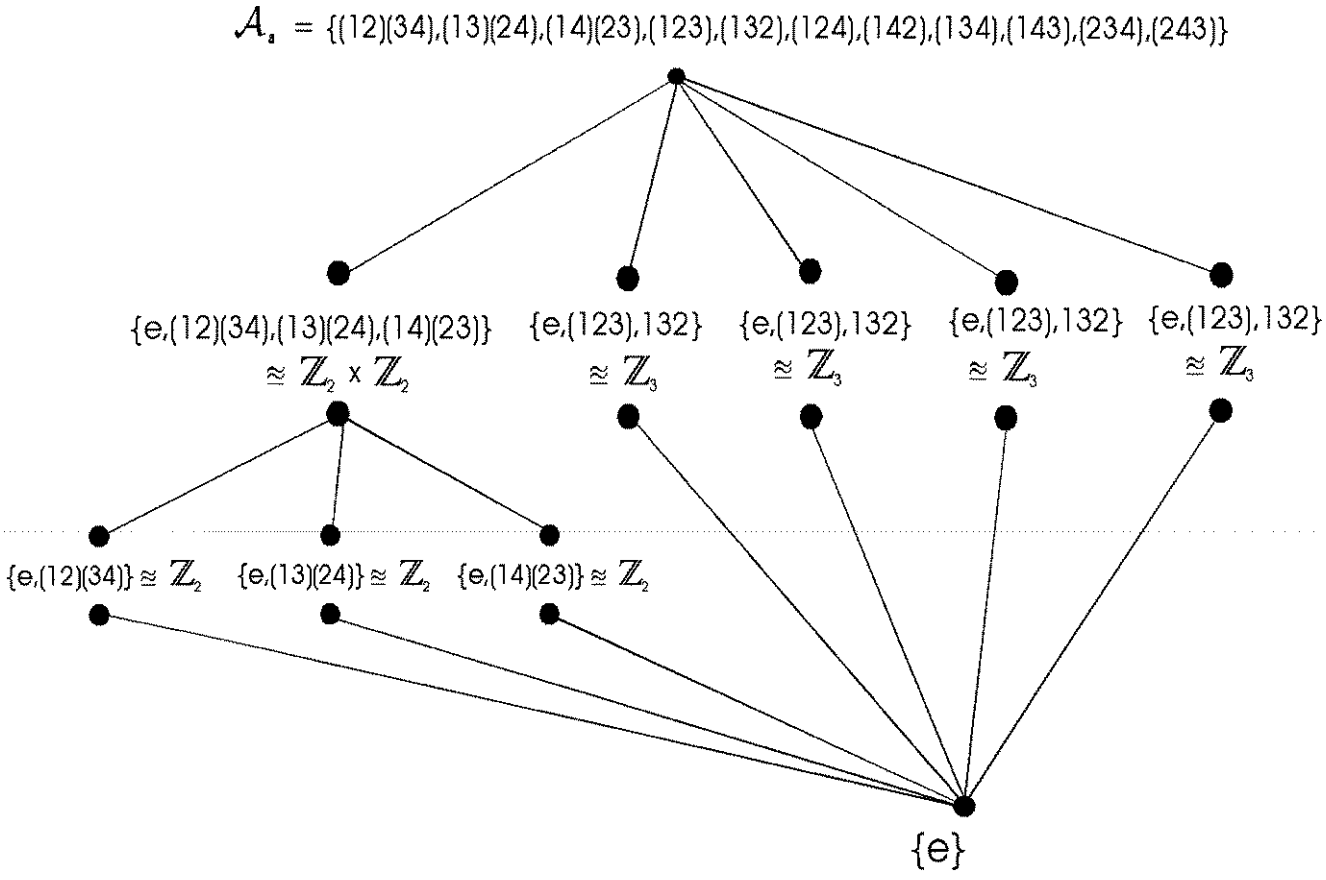

Figura B.15: Grupo de ordem 12: alternante

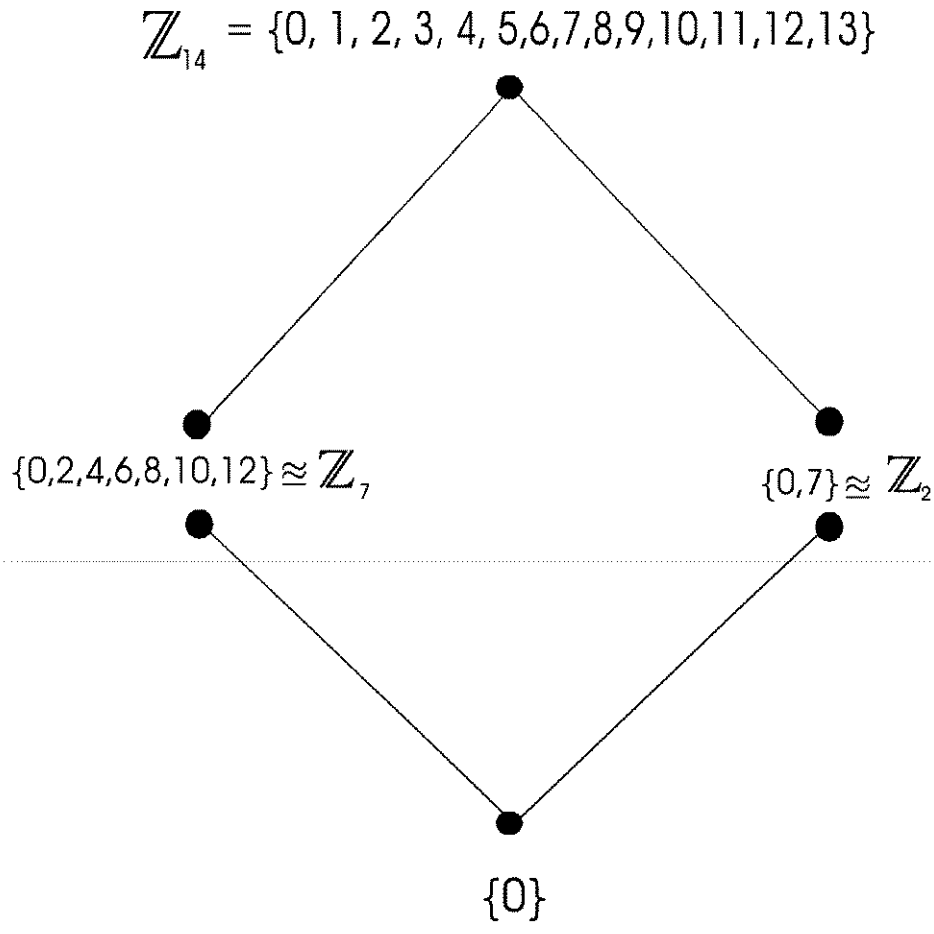

Figura B.16: Grupo de ordem 14: cíclico

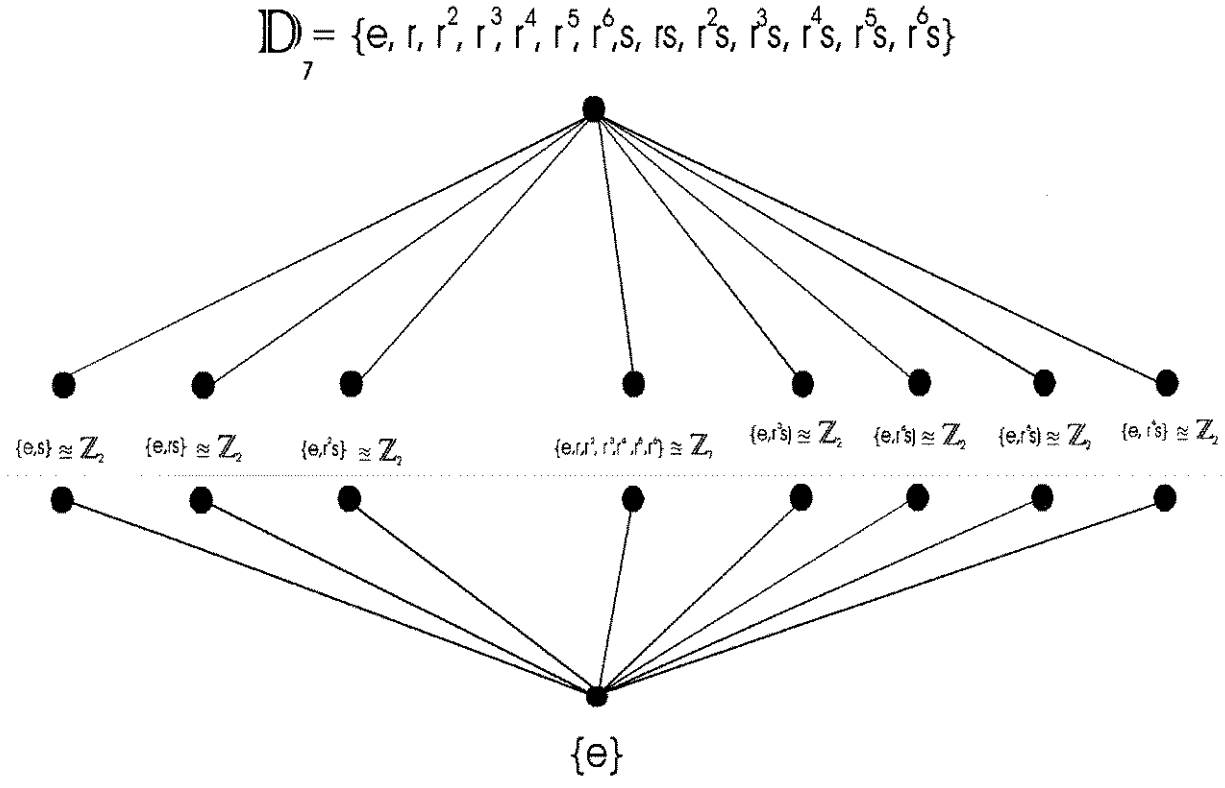

Figura B.17: Grupo de ordem 14: diedral

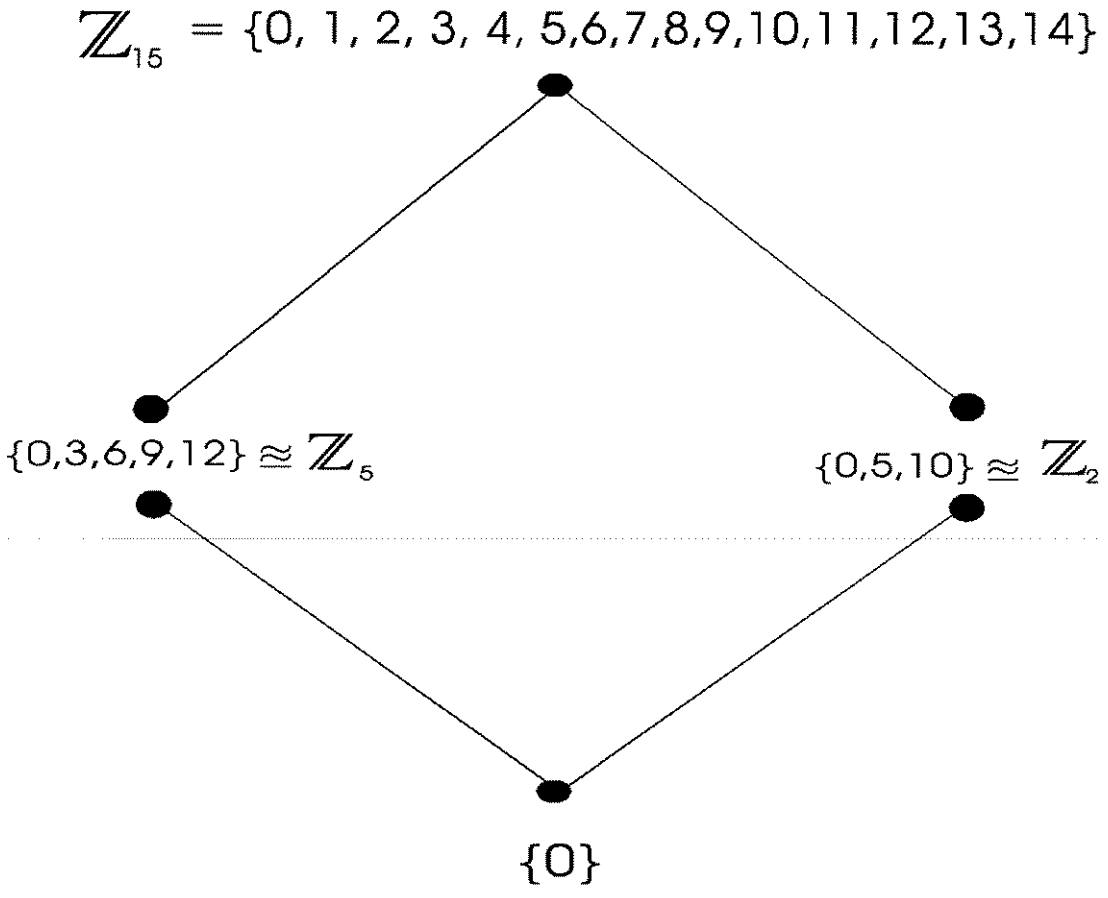

Figura B.18: Grupo de ordem 15: cíclico

Bibliografia

[1] S. R. Costa, J. R. Gerônimo, R. Palazzo Jr., J. C. Interlando and M. S. Alves. "The Symmetry Group of $\mathbb{Z}_q^n$ in the Lee Space and the $\mathbb{Z}_q^n$-Linear Codes. Submetido para 12th Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Toulouse, França,23 à 27 de junho, 1997.

[2] M.A. Armstrong, *Groups and Symmetry.* New York: Springer-Verlag, 1988.

[3] A. Azevedo e R. Piccinini, *Introdução à Teoria dos Grupos.* Rio de Janeiro: IMPA-CNPq, 1983.

[4] S. Benedetto, E. Biglieri, V. Castellani. *Digital Transmission Theory.* New Jersey: Prentice Hall, 1987.

[5] M. Berger, *Geometry I and II*, Springer-Verlag, New York, 1987.

[6] E. R. Berlekamp. *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[7] E. Biglieri, D. Divsalar, P. J. McLane, and M. K. Simon, *Introduction to Trellis-Coded Modulation with Applications.* New York: MacMillan, 1991.

[8] E. Biglieri and M. Elia, "On the Construction of Group Block Codes," *Annales des Télécommunications,* tome 50, no. 9-10, p.817-823,setembro-outubro 1995.

[9] E. Biglieri and M. Elia, "The Isometry Group of Geometrically Uniform Spherical Signal Sets," in *IEEE International Symposium on Information Theory,* agosto 1991.

[10] I. F. Blake, "Codes Over Certain Rings," *Information and Control*, vol. 20, p. 396-404, 1972.

[11] I. F. Blake, "Codes Over Integer Residue Rings," *Information and Control*, vol. 29, p. 295-300, 1975.

[12] A. E. Brouwer and T. Verhoeff, "An update table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-39, p. 662-671, março 1993.

[13] J. R. Gerônimo, R. Palazzo Jr, J. C Interlando and P. Brumatti, "On the Nonexistence $\mathbb{Z}_{2^k}$-Linear Codes for $k > 2$", a ser submetido para a revista IEEE *Tans. Inform. Theory.*

[14] P. G. Buda, F. R. Kschischang and S. Pasupathy, "Block coset codes for M-ary Phase Shift Keying," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 6, p. 900-912, agosto 1989.

[15] A. R. Hammons, Jr., A. R. Calderbank, P. V. Kumar, 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, p. 301-319, março 1994.

[16] J. P. de Carvalho, *Introdução à Álgebra Linear.* Rio de Janeiro: Livros Técnicos e Científicos Editora S.A. e Editora Universidade de Brasília, 1974

[17] J. N. Cederberg. *A Course in Modern Geometries.* New York: Springer-Verlag, 1989.

[18] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups.* New York: Springer-Verlag, 1987.

[19] J. H. Conway and N. J. A. Sloane, "Quaternary constructions for the binary single-error correcting codes of Julin, Best, and others," *Designs, Codes and Cryptography*, vol. 41, p. 31-42, 1994.

[20] D. J. Costello Jr. and S. Lin. *Error Control Coding: Fundamentals and Applications.* New Jersey: Prentice Hall, 1983.

[21] H. S. M. Coxeter. *Regular Polytopes.* New York: Wiley, 1975.

[22] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* New York: Wiley, 1962.

[23] C. W. Dodge, *Euclidean Geometry and Transformations.* Philippines: Addison-Wesley Publishing Company, Inc., 1972.

[24] D. S. Dummit and R. M. Foote. *Abstract Algebra.* New Jersey: Prentice-Hall, 1991.

[25] F. M. Eccles. *An Introduction to Transformational Geometry.* Phillipines: Addison-Wesley Publishing Company, Inc., 1971.

[26] S. B. Encheva, "On Linear $\mathbb{Z}_4$-linear Codes", ISICT'94.

[27] G. D. Forney, Jr., "Geometrically Uniform Codes," *IEEE Trans. Inform. Theory*, vol. IT-37, p. 1241-1260, setembro 1991.

[28] G. D. Forney, Jr. "Coset Codes - Part I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, vol. IT-34, p. 1123-1151, setembro 1988.

[29] G. D. Forney, Jr. "Coset Codes - Part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. IT-34, p. 1152-1187, setembro 1988.

[30] G. D. Forney, Jr. "On the Hamming Distance Properties of Group Codes," *IEEE Trans. Inform. Theory*, vol. IT-38, p.1797-1801,novembro 1992.

[31] G. D. Forney, Jr., N. J. A. Sloane, and M. D. Trott, "The Nordstrom-Robinson code is the binary image of the octacode," in *Coding and Quantization: DIMACS/IEEE Workshop,* October 19-21, 1992, A. R. Calderbank, G. D. Forney, Jr., and N. M. Koayeri, Eds. Amer. Math. Soc., 1993, p. 19-26.

[32] J. B. Fraleigh. *A First Course in Abstract Algebra.* New York: Addison-Wesley Publishing Company, 1989.

[33] A. Garcia and Y. Lequain. *Álgebra: Uma Introdução.* Rio de Janeiro: IMPA-CNPq, 1983.

[34] A. Gonçalves. *Introdução à Álgebra.* Rio de Janeiro: IMPA, 1979.

[35] I. N. Hernstein. *Tópicos de Álgebra.* São Paulo: USP-POLÍGONO, 1975.

[36] K. Hoffman and R. Kunze, *Álgebra Linear.* Rio de Janeiro: Livros Técnicos e Científicos, 1979.

[37] J. C. Interlando, R. Palazzo Jr. and M. Elia, Jr. "Group Block Codes Over Nonabelian Groups are Asymptotically Bad," *IEEE Trans. Inform. Theory*, vol. IT-42, p. 1277-1280, julho 1996.

[38] I.M. Jacobs and J.M. Wozencraft, *Principles of Communications in Engineering.* New York: Wiley, 1965.

[39] S. Lang, *Álgebra Linear.* São Paulo: Editora Edgard Blücher Ltda, 1971.

[40] E. L. Lima. *Espaços Métricos.* Rio de Janeiro: IMPA, 1977.

[41] E. L. Lima, *Curso de Análise, vol. 1.* Rio de Janeiro: IMPA, 1976.

[42] S. Lipschutz. *Teoria dos Conjuntos.* Rio de Janeiro: McGraw-Hill, 1972.

[43] H. A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. IT-37, p. 1675-1682, novembro 1991.

[44] R. C. Lyndon, *Groups and Geometry.* Cambridge: Cambridge University Press, 1987.

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

[46] R. J. McEliece, *The Theory of Information and Coding - A Mathematical Framework for Communication.* Cambridge: Cambridge Univ. Press, 1984.

[47] V. V. Nikulin and I. R. Shafarevich. *Geometry and Groups.* Germany: Springer Verlag Berlin Heidelberg, 1987.

[48] J.K. Omura and A.J. Viterbi, *Principles of Digital Communication and Coding.* New York: McGraw-Hil, 1979.

[49] J. G. Proakis, *Digital Communications.* New York: McGraw-Hill, Inc., 1983.

[50] A. Said, and R. Palazzo Jr., "Using combinatorial optimization to design good unit-memory convolutional codes" *IEEE Trans. Inform. Theory*, vol. IT-39-3, p. 1100-1108, maio 1993.

[51] C. Satyanarayara, "Lee metrics codes over integers," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 2, p. 250-254, março 1979.

[52] C. E. Shannon, "A mathematical theory of communication", *Bell Syst. Tech. J.*, vol. 27, p. 379-423, julho 1948, and p. 623-656, outubro 1948.

[53] Sociedade Brasileria de Matemática, "O leitor pergunta," *Revista do Professor de Matemática*, no. 5, p. 58, 2o. sem. 1994.

[54] A. Simis, *Introdução à Algebra.* Rio de Janeiro: IMPA-CNPq, 1977.

[55] D. Slepian, "Groups codes for the gaussian channel," *Bell Syst. Tech. J.*, vol. 47, p. 576-602, abril 1968.

[56] D. Slepian, "On neighbor distances and symmetry in group codes," *IEEE Trans. Inform. Theory*, vol. IT-17, p. 630-632, setembro 1971..

[57] E. Spiegel, "Codes over $\mathbb{Z}_m$," *Information and Control*, vol. 35, p. 48-51, setembro 1977.

[58] E. Spiegel. "Codes over $\mathbb{Z}_m$, Revisited," *Information and Control*, vol. 37, p. 100-104, abril 1978.

[59] G Ungerboeck, "Channel coding with multilevel/phase signals", *IEEE Trans. Inform. Theory*, vol. IT-28, p. 56-67, janeiro 1982

[60] J. H. van Lint, *Introduction to Coding Theory.* New York: Springer, 1982.

[61] J. F. Voloch. *Códigos Corretores de Erros.* Rio de Janeiro: IMPA-CNPq, 1987.

[62] S. K. Wasan, "On Codes over $\mathbb{Z}_m$", *IEEE Trans. Inform. Theory*, vol. IT-28, p. 117-120, janeiro 1982.