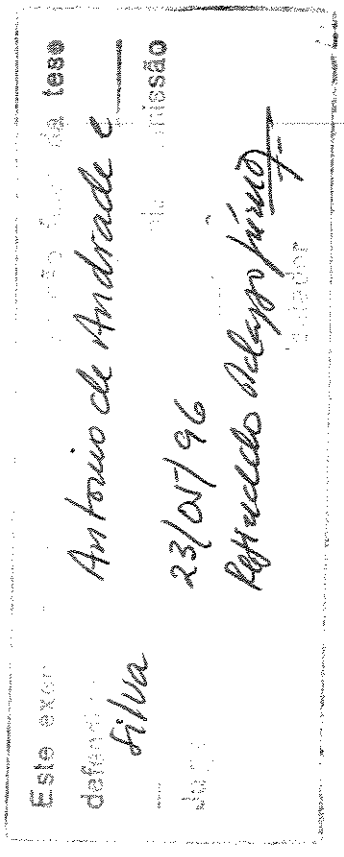
UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE COMUNICAÇÕES

UMA CONTRIBUIÇÃO À CLASSE DOS CÓDIGOS GEOMETRICAMENTE UNIFORMES



Antônio de Andrade e Silva

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

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

Maio - 1996

Campinas - SP

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

Silva, Antônio de Andrade e
Si38c Uma contribuição à classe dos códigos geometricamente uniformes / Antônio de Andrade e Silva. –Campinas, SP: [s.n.], 1996.

Orientador: Reginaldo Palazzo Jr.
Tese (Doutorado) - Universidade Estadual de Campinas Faculdade de Engenharia Elétrica e de Computação.

1. Códigos de controle e erros (Teoria da informação). 2. Teoria de grupos. 3. Codificação, Teoria da. 4. Isometria (Matemática). 5. Teoria da modulação. 6. Teoria dos reticulados. I. Palazzo Jr., Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. -+ III. Título.

Agradecimentos

- À Universidade Federal da Paraíba e à Coordenação do Aperfeiçoamento do Pessoal de Nível Superior (CAPES) pelo suporte financeiro.

- Ao Professor Doutor Reginaldo Palazzo Júnior, pela eficiente, segura e indispensável orientação a mim dispensada para a realização do presente trabalho.

- Aos colegas do Departamento de Matemática da UFPb, que me antecederam num trabalho idêntico, e aos que ficaram para tornar possível a realização desse trabalho. Em particular, aos Professores Hélio Pires, João Montenegro, Lenimar e Milaré.

- A todos os colegas do Curso. Em particular, Dinho, J. R. Gerônimo, José Carmelo, Martinho, Pingarilho, Rossini e Toninho.

- À minha esposa Rosângela e aos meus filhos José Augusto, Amanda e Fernanda pelo sacrifício, compreensão e por me esperarem sempre de braços abertos.

- À Banca Examinadora, constituída pelos Profs. Drs. Jaime Portugheis e José Carmelo Interlando do DECOM-FEEC-UNICAMP e, aos Profs. Drs. Trajano Pires da Nóbrega Neto do DM-IBILCE-UNESP, São José do Rio Preto e Valdemar Cardoso da Rocha Júnior do CIFE-UFPE.

Dedicação

À minha esposa
Rosângela e
aos meus filhos
José Augusto,
Amanda e
Fernanda.

Resumo

Neste trabalho apresentamos extensões de construções de códigos pertencentes à classe dos códigos geometricamente uniformes. São consideradas duas caracterizações de constelações de sinais casadas com grupos. Uma das caracterizações vem do uso de grupos não comutativos que são obtidos via o produto semidireto de um grupo comutativo por um grupo cíclico de ordem par. A outra caracterização vem do emprego de um algoritmo baseado no conceito da d-cadeia. Apresentamos uma construção de códigos multicamadas sobre o grupo $\mathbb{Z}_q$. Esses códigos são usados na construção multicamadas de empacotamentos esféricos, a qual é uma extensão da construção binária proposta por Costa e Silva e Palazzo em [10]. Como resultados, novos códigos de espaço Euclidiano e empacotamentos esféricos mais densos são apresentados. Em dimensões 68 e 72, novo recorde de densidades parece ter sido alcançado.

Abstract

In this research we present extensions of code constructions whose codes belong to the class of geometrically uniform codes. We consider two characterizations of signal sets matched to groups. The first characterization is derived from a noncommutative group which is the semidirect product of a commutative group by a cyclic group of even order. The second characterization is derived from an algorithm based on the concept of a d-chain. We propose a multilevel construction of codes over the group $\mathbb{Z}_q$. These codes are used in the multilevel construction of sphere packings, which is an extension of Costa e Silva and Palazzo's binary construction [10]. As a result, new Euclidean-space codes and sphere packings are presented. In dimensions 68 and 72, new record of densities appear to have been achieved.

Lista de Figuras

2.1 Ilustrações da medida entre elementos, intraconjunto, interconjunto e mínima interconjunto. 16

2.2 Os reticulados $\Lambda_0 \leftrightarrow \bullet$, $\Lambda_1 \leftrightarrow \circ$ e $\Lambda_2 \leftrightarrow \square$. 32

3.1 Hexágono casado com $\mathbb{Z}_6$. 52

3.2 Antiprisma casado com $\mathbb{Z}_6$. 52

3.3 Prisma casado com $\mathbb{Z}_6$. 52

3.4 Antiprisma casado com $\mathbb{Z}_4 \times \mathbb{Z}_2$. 53

3.5 Prisma casado com $\mathbb{Z}_4 \times \mathbb{Z}_2$. 53

3.6 Antiprisma casado com D_3. 53

3.7 Prisma casado com D_3. 53

3.8 Antiprisma casado com D_4. 54

3.9 Prisma casado com D_4. 54

Lista de Tabelas

3.1 Tabela Cayley do grupo $\mathbb{Z}_3 \times_\theta \mathbb{Z}_2 \simeq D_3$. 39

3.2 Tabela Cayley do grupo $\mathbb{Z}_4 \times_\theta \mathbb{Z}_2 \simeq D_4$. 40

3.3 Tabela de Cayley do grupo $\mathbb{Z}_4 \times_\theta \mathbb{Z}_4$. 41

3.4 Tabela de Cayley do grupo $\mathbb{Z}_3 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6$. 43

3.5 Tabela Cayley do grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$. 43

4.1 Códigos sobre D_3. 63

4.2 Códigos sobre Q_8. 64

5.1 Empacotamentos esféricos obtidos de partições do reticulado $\mathbf{D_4}$. 84

Conteúdo

1 Introdução **1**

1.1 Histórico 1

1.2 Descrição do trabalho 3

2 Grupos, Códigos e Reticulados **6**

2.1 Grupos 6

2.2 Códigos 16

2.3 Reticulados 23

3 Constelação de Sinais Casada com Grupos Finitos **33**

3.1 Introdução 33

3.2 Constelações de sinais casadas com grupos 35

3.3 d-Cadeia 44

3.4 Construindo constelações de sinais casadas com grupos 46

4 Construção de Códigos de Classes Laterais sobre Grupos **55**

4.1 Introdução 55

4.2 Construção de códigos de classes laterais generalizados 58

4.3 Exemplos 61

5 Construção de Empacotamentos Esféricos via Códigos de Classes Laterais Generalizados **65**

5.1 Introdução 65

5.2 Construção de empacotamentos esféricos 67

5.3 Decodificação de reticulados 74
5.4 Exemplos 80

6 Conclusões **85**

Capítulo 1

Introdução

1.1 Histórico

Neste trabalho serão estudados e apresentados métodos de construção de códigos geometricamente uniformes tanto no espaço Euclidiano quanto no espaço de Hamming.

Basicamente no espaço Euclidiano os grupos considerados são os não comutativos, devido ao seu potencial de excederem o limitante do MPSK. Com relação ao espaço Euclidiano duas variantes serão analisadas. A primeira variante tem a ver com a construção de códigos, cuja cardinalidade é grande, através da composição de códigos, cujas cardinalidades são menores, baseado na proposta de Zinoviev [34] sobre concatenação generalizada. A segunda variante tem a ver com a construção de empacotamentos esféricos tendo como base a construção de reticulados proposta por Costa e Silva e Palazzo em [10].

Códigos sobre grupos algébricos para um canal com Ruído Gaussiano Branco Aditivo (AWGN) foram primeiramente descritos por Slepian em [32]. Em [18] Forney mostrou que constelações de sinais geometricamente uniformes são uma generalização das constelações de sinais obtidas por Slepian. Para constelações de sinais geometricamente uniformes, existe um "rotulamento isométrico" entre um grupo e uma partição da constelação de sinais induzida pela partição do grupo gerador da constelação de sinais. Em [25] Loeliger estende para um grupo finito, a idéia de rotulamento isométrico, definindo um "mapeamento casado" de um grupo sobre uma constelação de sinais, e caracteriza todas as constelações de sinais casadas com um grupo comutativo cíclico, [25, Teorema 10]. Este resultado foi estendido por Palazzo *et al.* em [27] através de um algoritmo heurístico. Um dos métodos gerais de construções de

constelações de sinais do tipo Slepian ou "códigos esféricos" é baseado em empacotamentos de "*capas*" sobre a superfície esférica em $\mathbb{R}^N$, (cf. [8]).

Por outro lado, empacotamento esférico em $\mathbb{R}^N$, para N pequeno, tem sido considerado na literatura desde os tempos de Kepler. A conexão deste problema com outras áreas era muito fraca e o problema principal era atacado por métodos diretos. Assim, o problema de determinar a maior densidade possível de um empacotamento esférico em $\mathbb{R}^N$ parecia cada vez mais distante de ser resolvido. Embora o problema geral de encontrar empacotamentos esféricos com alta densidade permaneça aberto em grandes dimensões, a conexão com a Teoria de Códigos Corretores de Erros possibilitou a construção efetiva de empacotamentos esféricos densos, a qual foi iniciada por Leech e Sloane em [24].

Mas foi a proposta de "*particionamento de conjunto*," de Ungerboeck em [33], que motivou um grande número de pesquisadores a trabalhar nesta área de pesquisa. Construções multicamadas têm sido estudadas por vários autores. Em [21] Imai e Hirakawa descreveram um método de codificação multinível, no qual códigos de bloco binários são combinados apropriadamente para aumentar o desempenho do sistema de comunicações. A "*construção hierárquica*" de Ginzburg em [20] é uma generalização da construção de Imai e Hirakawa. Em [20], o conjunto de sinais é particionado segundo uma hierarquia de subconjuntos. Desse modo, o esquema de modulação codificada de bloco é obtida por mapeamento de códigos de bloco convencionais sobre os sinais utilizando-se os vários níveis da hierarquia. A idéia de particionamento de conjunto é também evidente no trabalho de Cusack em [11]. Mais tarde Sayegh em [30] generaliza o trabalho de Cusack aplicando códigos de bloco binários conhecidos para projetos de esquemas de modulação codificada de bloco baseada em várias constelações de sinais PSK e QAM.

Vários autores têm empregado métodos algébricos para o projeto de esquemas de modulações codificadas eficientes. Como ressalta Ginzburg, que em muitos casos importantes, o processo hierárquico de particionamento de conjuntos pode ser descrito através da teoria de grupos. Em [4] Calderbank e Sloane propõem que um reticulado seja particionado por um sub-reticulado e em suas classes laterais correspondentes e, através de um "*codificador generalizado*," utiliza destes sub-reticulados para codificação de códigos de treliças. Em [15] Forney mostra que todos os esquemas de modulação codificada conhecidos podem ser descritos por métodos algébricos de grupos e partições de grupos. Devido as suas estruturas algébricas comuns, Forney chama esses esquemas de modulações codificadas de códigos de classes laterais. Em [22] Kschischang *et al.* descreve uma construção de códigos de classes laterais de bloco para constelações MPSK de uma forma algébrica usando a teoria de grupos comutativos.

1.2 Descrição do trabalho

O presente trabalho tem seus fundamentos básicos nos artigos [10, 14, 15, 16, 18, 25], os quais reúnem e generalizam todas as construções multicamadas de códigos, reticulados e projetos de sinais.

Para descrever os problemas estudados neste trabalho procedemos como segue:

Sabe-se que um "código linear" $C = [N, K, D]$ sobre $\mathbb{Z}_2$ pode ser mapeado canonicamente em um "código do espaço Euclidiano" através do modulador

$$\mu : \mathbb{Z}_2 \longrightarrow \mathbb{R},\ \mu(0) = 1,\ \mu(1) = -1.$$

Assim, o código do espaço Euclidiano $\underline{\mu}(C)$ é um subconjunto dos vértices do cubo $[-1, 1]^N$ em $\mathbb{R}^N$, onde $\underline{\mu}(\mathbf{c}) = (\mu(c_0), \ldots, \mu(c_{N-1}))$, $\forall\, \mathbf{c} = (c_0, \ldots, c_{N-1}) \in C$ e $|\underline{\mu}(C)| = 2^K$. Neste caso, a distância Euclidiana quadrática $d(\underline{\mu}(\mathbf{c}), \underline{\mu}(\mathbf{c}'))$ é função apenas de $-\mathbf{c} + \mathbf{c}'$, isto é,

$$d(\underline{\mu}(\mathbf{c}), \underline{\mu}(\mathbf{c}')) = d(\underline{\mu}(\mathbf{0}), \underline{\mu}(-\mathbf{c} + \mathbf{c}')) = \mathbf{N}(\underline{\mu}(-\mathbf{c} + \mathbf{c}')),$$

pois $d(\underline{\mu}(\mathbf{c}), \underline{\mu}(\mathbf{c}')) = 4d_H(\mathbf{c}, \mathbf{c}') = 4d_H(\mathbf{0}, -\mathbf{c} + \mathbf{c}') = d(\underline{\mu}(\mathbf{0}), \underline{\mu}(-\mathbf{c} + \mathbf{c}'))$, onde $d_H(.,.)$ é a distância de Hamming para o código C. De um modo geral, uma constelação de sinais S é casada com um "grupo" G, (cf. [25]), se existe um mapeamento (ou um modulador abstrato) μ de G sobre S tal que

$$d(\mu(g), \mu(g')) = d(\mu(e), \mu(g^{-1}g')),\ \forall\, g, g' \in G.$$

Quando o grupo G é não comutativo Loeliger em [25] observou através de dois exemplos que a capacidade das constelações de sinais casadas com G, para o canal AWGN em faixa limitada, excedia o "PSK-limite."

- Isto nos motivou a caracterizar constelações de sinais casadas com grupos não comutativos que são "o produto semidireto" de dois grupos menores.

Sejam $\mathbb{F}_q$ o "corpo de Galois," onde $q = p^K$ e p é um número primo. É bem conhecido que $\mathbb{F}_q$ pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$ com dimensão K. Seja $\{\mathbf{v}_0, \ldots, \mathbf{v}_{K-1}\}$ uma base de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Então existe um único isomorfismo ϕ de $\mathbb{F}_q$ em $\mathbb{F}_p^K$ tal que $\phi(\mathbf{v}_i) = \mathbf{a}_i$, onde $\{\mathbf{a}_0, \ldots, \mathbf{a}_{K-1}\}$ é uma base para $\mathbb{F}_p^K$. Baseado neste isomorfismo Forney em [13], com $p = 2$, propôs um método de

concatenar dois códigos menores para obter um código longo do seguinte modo: sejam $B = [n, k, d]$ um código linear sobre $\mathbb{F}_q$ e $A = [N, K, D]$ um código linear sobre $\mathbb{F}_p$. Então, a concatenação dos códigos B e A é o código linear $C = [Nn, Kk, d']$ sobre $\mathbb{F}_p$, onde cada palavra-código é dada por

$$\mathbf{c} = (\varphi(b_0), \ldots, \varphi(b_{n-1})),$$

para todo $\mathbf{b} = (b_0, \ldots, b_{n-1}) \in B$, $\varphi(b_i) \in A$, $0 \leq i \leq n-1$, e $d' \geq Dd$, onde $\varphi = j\phi$ com $\mathbb{F}_p^K \xrightarrow{j} \mathbb{F}_p^N$. Este resultado foi generalizado por Blokh e Zyablov em [2]. Mais tarde Zinoviev em [34] generaliza os resultados de [2, 13] para obter um código concatenado generalizado (linear ou não) sobre um corpo qualquer $\mathbb{F}_q$.

- Com base na construção de [34] propomos uma subclasse de códigos do espaço Euclidiano sobre constelações de sinais casadas com grupos não comutativos do problema anterior.

A construção mais simples de um "reticulado" Λ em $\mathbb{R}^N$ de um código de bloco binário linear é a construção **A** de [24], isto é, dado um código linear $A = [N, K, D]$ sobre $\mathbb{Z}_2$,

$$\Lambda = \{\mathbf{x} \in \mathbb{Z}^N : \mathbf{x} \equiv \mathbf{a} \pmod 2, \text{ para algum } \mathbf{a} \in A\} = \bigcup_{\mathbf{a} \in A} (l(\mathbf{a}) + 2\mathbb{Z}^N),$$

onde $\mathbb{Z}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ é um grupo de "rótulos" e $l : \mathbb{Z}_2^N \longrightarrow [\mathbb{Z}/2\mathbb{Z}]^N$. Com base neste tipo de construção Costa e Silva e Palazzo em [10] propõem uma construção de reticulados baseado numa "cadeia de partições, com m-níveis e 2-maneiras," de um reticulado conhecido Λ com um sub-reticulado Λ', ambos com a mesma dimensão (posto).

- Estendemos este resultado para uma cadeia de partições, com m-níveis e q-maneiras.

Desse modo, este trabalho será dividido da seguinte forma:

No Capítulo 2, fazemos uma rápida revisão da Teoria de Grupos, Códigos e Reticulados, bem como suas caracterizações algébricas e geométricas, necessárias para o entendimento deste trabalho.

No Capítulo 3, caracterizamos todas as constelações de sinais que são casadas com um grupo não comutativo resultante do produto semidireto de um grupo comutativo por um grupo cíclico. Também, apresentamos um algoritmo para a determinação da constelação de sinais casada com um grupo que é uma "extensão" de dois grupos menores.

No Capítulo 4, apresentamos uma construção de códigos de classes laterais generalizados sobre o grupo $\mathbb{Z}_q$ e sobre um grupo casado com uma constelação de sinais. Como resultados desta construção, obtemos códigos do espaço Euclidiano sobre os grupos "Diedrais" e dos "Quatérnios".

No Capítulo 5, apresentamos uma construção multicamada para a obtenção de bons empacotamentos esféricos bem como seus principais parâmetros, através dos códigos de classes laterais generalizados. Com o propósito de completude, apresentamos um algoritmo de decodificação sub-ótimo, (cf. [10]), para os empacotamentos esféricos que são reticulados e alguns exemplos.

No Capítulo 6, apresentamos as conclusões deste trabalho bem como sugestões para futuros trabalhos.

Capítulo 2

Grupos, Códigos e Reticulados

2.1 Grupos

Nesta seção apresentamos algumas definições e resultados básicos sobre a teoria de grupos, necessárias para o entendimento deste trabalho. Para maiores detalhes, (cf. [12]).

Um *grupo* é um conjunto não vazio G junto com uma operação binária, $G \times G :\longrightarrow G, (g,h) \longmapsto goh$, tal que as seguintes propriedades valem:

(1) $g \circ (h \circ k) = (g \circ h) \circ k$, para quaisquer $g, h, k \in G$.

(2) Existe $e \in G$ tal que $g \circ e = e \circ g = g$ para todo $g \in G$.

(3) Para todo $g \in G$, existe $h \in G$ tal que $g \circ h = h \circ g = e$.

O elemento e em (2) é único e é chamado de *elemento identidade* de G, enquanto o elemento h em (3) é único e é chamado de *elemento inverso* de g. Denotamos o elemento inverso de g por g^{-1}. Se em um grupo G a propriedade:

(4) $g \circ h = h \circ g$, para todo $g, h \in G$

é verificada, dizemos que G é um *grupo comutativo.*

Um subconjunto H de um grupo G é um *subgrupo* de G, denotado por $H \leq G$, se

(1) $e \in H$.

(2) Para quaisquer $h, k \in H$ tem-se $h^{-1} \circ k \in H$.

Para simplificar, denotamos por gh o produto $g \circ h$ dos elementos g e h pertencentes a um grupo qualquer.

Sejam G e K dois grupos quaisquer. O conjunto $G \times K = \{(g,k) : g \in G, k \in K\}$ com a operação $(g,k)(g',k') = (gk, g'k')$, para todo $g, g' \in G$ e $k, k' \in K$, é um grupo chamado *produto direto externo* de G por K. Note que essa definição pode ser estendida de maneira natural a um produto qualquer de grupos. Um *homomorfismo* de um grupo G em um grupo K é um mapeamento $\varphi : G \longrightarrow K$ tal que $\varphi(gh) = \varphi(g)\varphi(h)$, para todo $g, h \in G$, intuitivamente um homomorfismo é um mapeamento que preserva as operações de grupos. Denotaremos por $Hom(G,H) = \{\varphi : G \longrightarrow K : \varphi$ é um homomorfismo$\}$. Um *isomorfismo* é homomorfismo que também é uma bijeção. Dizemos que dois grupos G e K são *isomorfos*, $G \simeq K$, se existe um isomorfismo de G em K. Intuitivamente, dois grupos isomorfos são iguais, a menos de rótulos. Denotaremos por $Iso(G,K) = \{\varphi : G \longrightarrow K : \varphi$ é um isomorfismo$\}$. Quando $G = K$ não é difícil verificar que $Iso(G,G)$ com a operação de composição de mapeamentos é um grupo. O grupo $Iso(G,G)$ é chamado de *grupo dos automorfismos* de G e denotamos por $Aut(G)$. Neste caso, $Aut(G)$ é um subgrupo do *grupo simétrico* de G, que denotamos por $S_G = \{\varphi : G \longrightarrow G : \varphi$ é uma bijeção$\}$.

Uma *partição* de um conjunto X é um conjunto $P(X) = \{Y : Y \subset X, Y \neq \emptyset\}$ tal que as seguintes propriedades valem:

(1) $X_1 \bigcap X_2 = \emptyset$, $\forall\, X_1, X_2 \in P(X)$, $X_1 \neq X_2$.

(2) $X = \bigcup_{Y \in P(X)} Y$.

Seja G um grupo e H um subgrupo de G. Dado $g \in G$, o conjunto

$$gH \triangleq \{gh : h \in H\}$$

é chamado a *classe lateral à esquerda* de H em G determinada por g. De modo semelhante, podemos definir a classe lateral à direita Hg de H em G. O conjunto de todas as classes laterais à esquerda de H em G forma uma partição de G por H, que denotamos por G/H.

Dados $g, k \in G$, dizemos que g é *congruente a* k *módulo* H se $g^{-1}k \in H$, que denotamos por $g \equiv k \pmod{H}$. Não é difícil mostrar que $g \equiv k \pmod{H}$ é uma relação de equivalência em G e que a classe de equivalência determinada por g é igual a classe lateral à esquerda gH, o elemento g é chamado um *representante* da classe de equivalência.

O número de elementos de um conjunto G é chamado de *cardinalidade* de G e o denotamos $|G|$. No caso em que G é um grupo a cardinalidade é chamada de *ordem*. O número de classes laterais (à esquerda ou à direita) de H em G é chamado o *índice* de H em G, denotado por $[G : H]$. Assim, $[G : H] = |G/H|$. G/H é um grupo com a operação $gHkH = gkH$, para todo $g, k \in G$, se, e somente se, H é um subgrupo normal de G (H é *um subgrupo normal* de G, isto é, $H \lhd G$, se $ghg^{-1} \in H$, para todo $h \in H$ e $g \in G$). Neste caso, G/H é chamado o *grupo quociente* de G por H. Pode se ver que, se G é um grupo de ordem finita, então um subconjunto não vazio H de G é o subgrupo se, e somente se, H é fechado com relação à operação de G.

Sejam G um grupo e H um subgrupo de G. Um subconjunto $[G/H]$ de G tal que as propriedades (1) e (2) abaixo valem, é chamado um *sistema de representantes de classes laterais à esquerda* de H em G.

(1) Se $x, y \in [G/H]$ e $x \neq y$, então $x^{-1}y \notin H$.

(2) Dado $g \in G$, existe $x \in [G/H]$ tal que $x^{-1}g \in H$.

Das propriedades (1) e (2) acima temos que, todo elemento $g \in G$ pode ser escrito de modo único na forma $g = xh$, onde $x \in [G/H]$ e $h \in H$.

Sejam $H \lhd G$ e $[G/H]$ um sistema de representantes de classes laterais à esquerda de H em G com e o representante da classe lateral H. Seja $x \in [G/H]$ o representante da classe lateral gH. Como duas classes laterais à esquerda são iguais ou disjuntas, segue-se que $xH = gH$, pois $x \in gH$. Note que, se $h \in H$, então o representante y da classe lateral ghH é igual a x, pois $gH = xH = ghH = yH$.

Dados x e $y \in [G/H]$, é claro que $xy \in G$ e, assim, existem únicos $z \in [G/H]$ e $h \in H$ tal que $xy = zh$. É fácil de observar que, h é univocamente determinado por x e y, por isso denotamos por $h_{x,y}$. Logo, $xy = zh_{x,y}$, para todo $x, y \in [G/H]$. Em particular, quando $h_{x,y} = e$, para quaisquer $x, y \in [G/H]$, temos que $[G/H]$ é um subgrupo de G. De fato, dados $x, y \in [G/H]$ temos que $xy = zh_{x,y} = z \in [G/H]$, isto é, $[G/H]$ é fechado com relação à operação de G. Seja $x \in [G/H]$ e $y \in [G/H]$ tal que $x^{-1}H = yH$, isto é, $xy \in H$. Como $e \in [G/H]$ temos que $xy = eh_{x,y} = e$, logo $x^{-1} \in [G/H]$.

Como $H \lhd G$ temos que $[G/H]H$ é um subgrupo de G. Por outro lado, todo elemento de G é da forma xh, com $x \in [G/H]$ e $h \in H$. Assim, $G = [G/H]H$. Como elementos distintos de $[G/H]$ pertencem a classes laterais distintas de H em G segue-se que $[G/H] \cap H = \{e\}$. Neste caso, dizemos

G é *fatorável* sobre H. Chamamos $G = [G/H]H$ a *decomposição de classes laterais* de G, pois

$$G = \bigcup_{g \in [G/H]} gH = [G/H]H.$$

Um grupo G é uma *extensão* de um grupo H' por um grupo K se existe um subgrupo **normal** H de G tal que $H \simeq H'$ e $G/H \simeq K$.

Sejam G um grupo e X um conjunto. Então G *age em* X se existe um mapeamento $\sigma : G \times X \longrightarrow X$, denotado por $\sigma((g,x)) = gx$, tal que

(1) $g(hx) = (gh)x, \ \forall g, h \in G, \ x \in X;$

(2) $ex = x, \ \forall x \in X.$

O mapeamento σ é chamado de *ação* de G em X.

Para cada $g \in G$ o mapeamento $\sigma_g : X \longrightarrow X$ definido por $\sigma_g(x) = gx$ é uma permutação de X, isto é, σ_g é um elemento do grupo simétrico S_X. O mapeamento $\varphi : G \longrightarrow S_X$ definido por $\varphi(g) = \sigma_g$ é um homomorfismo de grupo chamado uma *representação* de G em S_X. Reciprocamente, qualquer homomorfismo $\phi : G \longrightarrow S_X$ define uma ação, $gx = \phi(g)(x)$.

Sejam G um grupo agindo em um conjunto X e $x \in X$. Então o conjunto

$$O(x) \triangleq \{gx : \ g \in G\}.$$

é chamado a *órbita* de x em G.

Seja G um grupo agindo em um conjunto X. Então o conjunto dos elementos de G que deixam x fixo, isto é,

$$E(x) \triangleq \{g \in G : \ gx = x\}.$$

é chamado o *estabilizador* de $x \in X$.

É fácil verificar que $E(x)$ é um subgrupo de G e que $|O(x)| = [G : E(x)]$ se $|G| < \infty$. Quando existe somente uma órbita, isto é, quando $O(x) = G$ para algum $x \in X$ (e consequentemente, para todo $x \in X$, pois duas órbitas são iguais ou disjuntas), dizemos que a representação φ é *transitiva.*

Seja G um grupo qualquer agindo em si próprio por multiplicação à esquerda

$$g \circ a = ga, \forall g \in G \text{ e } a \in G.$$

Neste caso, a órbita de qualquer $a \in G$ é todo G, isto é,

$$O(a) = \{ga : g \in G\} = G.$$

Um *quadrado latino* de um conjunto G, com m elementos, é um arranjo $m \times m$, contendo exatamente um elemento de G em cada linha e coluna.

Se a ordem do grupo G é igual a m, então é conveniente rotular os elementos de G com inteiros $0, \ldots, m-1$ para descrever a representação φ. Assim, os elementos de G são listados como $g_0 = e, g_1, \ldots, g_{m-1}$ e para cada $g_i \in G$, a permutação σ_{g_i} (a matriz de permutação $(\sigma_{g_i})_{ij}$) pode ser descrita como uma permutação dos índices $0, 1, \ldots, m-1$ como segue

$$\sigma_{g_i}(j) = k \Longleftrightarrow g_i g_j = g_k \quad \left((\sigma_{g_i})_{ij} = \begin{cases} 1, & \text{se } g_i g_j = g_k \\ 0, & \text{se } g_i g_j \neq g_k \end{cases} \right).$$

Uma maneira prática de se obter as permutações σ_{g_i} como permutações dos índices $0, 1, \ldots, m-1$ é construindo uma tabela de Cayley T para G. Então um quadrado latino L de ordem $|G|$ pode ser obtido de T como segue

$$L_{ij} = k \Longleftrightarrow T_{ij} = g_i g_j = g_k.$$

Teorema 2.1.1 [12] *Sejam H e K dois grupos e $\theta : K \longrightarrow Aut(H)$ um homomorfismo. Seja $G = \{(h,k) : h \in H, k \in K\}$. Então definindo a operação binária em G como*

$$(h_1, k_1)(h_2, k_2) = (h_1 \theta(k_1)(h_2), k_1 k_2) \ \forall\, h_1, h_2 \in H \text{ e } k_1, k_2 \in K,$$

temos que

(1) *G é um grupo de ordem $|G| = |H||K|$.*

(2) *Os conjuntos $\tilde{H} = \{(h,e) : h \in H\}$ e $\tilde{K} = \{(e,k) : k \in K\}$ são subgrupos de G, com $H \simeq \tilde{H}$ e $K \simeq \tilde{K}$.*

Identificando H e K com suas cópias isomorfas em (2) temos que

(3) $H \lhd G$,

(4) $H \cap K = \{e\}$,

(5) $G = HK$,

(6) *para quaisquer $h \in H$ e $k \in K$, $\theta(k)(h) = khk^{-1}$.* ■

O grupo descrito pelo Teorema 2.1.1 é chamado *produto semidireto* de H por K via θ, que denotamos por $H \times_\theta K$.

Teorema 2.1.2 [12] *Seja G um grupo com subgrupos H e K tais que*

(1) $H \lhd G$,

(2) $H \cap K = \{e\}$,

(3) $G = HK$.

Então $G \simeq H \times_\theta K$. ■

Note que, pelos Teoremas 2.1.1 e 2.1.2, um grupo G é fatorável sobre H se, e somente se, G é um produto semidireto de H por G/H.

Lema 2.1.1 [12] *Seja G um grupo comutativo de ordem m. Então $\tau : G \longrightarrow G$ definido por $\tau(g) = g^k$ é um automorfismo se $mdc(m,k) = 1$.* ■

Exemplo 2.1.1 [12] *Sejam H um grupo comutativo qualquer e $K = \langle k \rangle \simeq \mathbb{Z}_{2m}$. Definimos o homomorfismo $\theta : K \longrightarrow Aut(H)$ por $\theta(k)(h) \triangleq h^{-1}$. Então $G = H \times_\theta K$ é um grupo não comutativo. Note que $\theta(k^2)(h) = \theta(k)(\theta(k)(h)) = \theta(k)(h^{-1}) = h$, isto é, $k^2hk^{-2} = h$, para todo $h \in H$. Logo, $k^2 \in Z(G)$, onde $Z(G) = \{g \in G : gh = hg, \forall\, h \in G\}$ é um subrgrupo normal de G chamado o* centro *de G. Agora, consideramos os seguintes casos particulares*

(1) *Se $H = \langle h \rangle \simeq \mathbb{Z}_n$ e $K = \langle k \rangle \simeq \mathbb{Z}_2$, então $G = H \times_\theta K$ é um grupo não comutativo de ordem $2n$ isomorfo ao* grupo diedral, *que denotamos por D_n:*

$$D_n = \langle h, k \rangle, \text{ onde } h^n = k^2 = e, \ hk = kh^{-1},$$

h é identificado com (h, e) e k é identificado com (e, k). Note que o grupo D_n é isomorfo ao grupo $L = \langle R, T \rangle$ gerado pelas matrizes

$$R = \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix} \quad e \quad T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

(2) *Se $H = \langle h \rangle \simeq \mathbb{Z}_{2^n}$ e $K = \langle k \rangle \simeq \mathbb{Z}_4$. Já observamos que $k^2 \in Z(G)$. Como $khk^{-1} = h^{-1}$ temos que $kak^{-1} = a^{-1}$ para todo $a \in \langle h^{2^{n-1}} \rangle \subset H$. Logo, $kak^{-1} = a^{-1} = a$ implica que $a \in Z(G)$. Assim, $k^2a \in Z(G)$ e $\langle k^2a \rangle \lhd G$. Seja $\overline{G} = G/\langle k^2a \rangle$, como $|\langle k^2a \rangle| = 2$ temos que $|\overline{G}| = 2^{n+1}$. Portanto, identificando k^2 com $h^{2^{n-1}}$ em $\overline{G}$ não é difícil mostrar que $\overline{G}$ tem um único subgrupo*

de ordem 2, $\langle k^2 \rangle$, o qual é igual ao centro de $\overline{G}$. O grupo $\overline{G}$ é um grupo não comutativo de ordem 2^{n+1} isomorfo ao grupo dos quatérnios generalizado, *que denotamos por $Q_{2^{n+1}}$:*

$$Q_{2^{n+1}} = \langle h, k \rangle, \text{ onde } h^{2^n} = k^4 = e,\ k^{-1}hk = h^{-1},\ h^{2^{n-1}} = k^2,$$

h é identificado com (h, e) e k é identificado com (e, k). Note que o grupo $Q_{2^{n+1}}$ é isomorfo ao grupo $L = \langle U, V \rangle$ gerado pelas matrizes

$$U = \begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix} \quad e \quad V = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

onde $u^{2^n} = 1$ e $u^{2^{n-1}} \neq 1$, $n \geq 2$. Além disso, $Q_{2^{n+1}}/Z(Q_{2^{n+1}}) \simeq D_{2^{n-1}}$.

(3) *Se $H = \langle h \rangle \simeq \mathbb{Z}_q$ e $K = \langle k \rangle \simeq \mathbb{Z}_p$, onde p e q são números primos com $p < q$. Se p divide $q - 1$, então $Aut(H)$ contém um único subgrupo de ordem p, pois $Aut(H)$ é cíclico de ordem $q - 1$. Assim, existe um homomorfismo não trivial θ de K em $Aut(H)$. Portanto, G é um grupo não comutativo de ordem pq. Mais geralmente, se $H = \langle h \rangle \simeq \mathbb{Z}_n$ e $K = \langle k \rangle \simeq \mathbb{Z}_m$ com $r^m \equiv 1 \pmod{n}$ e $mdc(r, n) = 1$, então G é um grupo não comutativo de ordem mn, onde $\theta(k)(h) = h^r$. O grupo G é chamado* grupo metacíclico, *que denotamos por G_{mn}:*

$$G_{mn} = \langle h, k \rangle, \text{ onde } h^n = k^m = e,\ khk^{-1} = h^r,$$

h é identificado com (h, e) e k é identificado com (e, k). ■

Uma seqüência $G_0, \ldots, G_m$ de grupos G_i é chamada *abrigada* se $G_{i+1} \leq G_i, 0 \leq i \leq m-1$. Então $G_0/\cdots/G_m$ é uma cadeia de partições de m-níveis, a partição no i-ésimo nível tem ordem $|G_i/G_{i+1}|$ e $|G_0/G_m| = \prod_{i=0}^{m-1} |G_i/G_{i+1}|$.

Dizemos que uma cadeia de partições de m-níveis $G_0/\cdots/G_m$, onde $G_m = \{e\}$, é uma *cadeia subnormal* se $G_{i+1} \lhd G_i$, $0 \leq i \leq m-1$. Uma cadeia subnormal de m-níveis $G_0/\cdots/G_m$ é uma *cadeia de composição* se cada fator de composição G_i/G_{i+1}, $0 \leq i \leq m-1$, é um grupo simples, isto é, os únicos subgrupos normais de G_i/G_{i+1}, $0 \leq i \leq m-1$, são os triviais. Se $G_0/\cdots/G_m$ é uma cadeia de composição, então todo elemento em G_0 é determinado univocamente pelo conjunto de seqüências $(g_0, \ldots, g_{m-1})$, isto é, cada classe lateral à esquerda de G_m em G_0 pode ser rotulada por $(g_0, \ldots, g_{m-1})$, onde $g_i \in [G_i/G_{i+1}]$, $0 \leq i \leq m-1$. Portanto, indutivamente, temos a decomposição de classes laterais $G_0 = [G_0/G_1] \cdots [G_{m-1}/G_m]G_m$, pois

$$G_i = \bigcup_{g_i \in [G_i/G_{i+1}]} g_i G_{i+1} = [G_i/G_{i+1}]G_{i+1},\ 0 \leq i \leq m-1.$$

Para qualquer grupo G, $G/\{e\}$ é uma cadeia subnormal de G. Se G é um grupo simples, então $G/\{e\}$ é a única cadeia de composição de G. Todo grupo finito G tem uma cadeia de composição. De fato: se $|G|= 1$ ou G é simples, então o resultado é trivial. Suponhamos que o resultado seja válido para todo grupo de ordem menor que $|G|$. Seja H um subgrupo normal maximal de G, $H \neq G$ (H sempre existe). Por hipótese de indução, H tem uma cadeia de composição, digamos

$$H/H_1/\cdots/H_{m-1}/\{e\}.$$

Portanto, G tem uma cadeia de composição

$$G/H/H_1/\cdots/H_{m-1}/\{e\}.$$

Considerando as seguintes cadeias de composições do grupo $G = \langle g\rangle \simeq \mathbb{Z}_{30}$

$$G/G_1/G_2/\{1\} \text{ e } G/H_1/H_2/\{1\},$$

onde $G_1 = \langle g^5\rangle$, $G_2 = \langle g^{10}\rangle$, $H_1 = \langle g^2\rangle$ e $H_2 = \langle g^6\rangle$. Temos que os fatores de composições da primeira cadeia são:

$$G/G_1 \simeq \mathbb{Z}_5,\ G_1/G_2 \simeq \mathbb{Z}_2 \text{ e } G_2/\{1\} \simeq \mathbb{Z}_3,$$

os fatores de composições da segunda cadeia são:

$$G/H_1 \simeq \mathbb{Z}_2,\ H_1/H_2 \simeq \mathbb{Z}_3 \text{ e } H_2/\{1\} \simeq \mathbb{Z}_5.$$

Neste caso, ambas as cadeias têm o mesmo número de níveis e os fatores de composições podem ser ordenados de modo que fatores correspondentes sejam isomorfos. Assim, temos o seguinte resultado.

Teorema 2.1.3 *(Jordan – Hölder)[12] Seja G um grupo finito. Se $G_0/\cdots/G_m$ e $H_0/\cdots/H_m$ com $G = G_0 = H_0$ é um par de cadeias de composições para G, então existe uma permutação σ de $\{0,\ldots,m-1\}$ tal que $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}$, $0 \leq i \leq m-1$.* ∎

Seja G um p-grupo, isto é, $|G|= p^m$, para algum $m \in \mathbb{N}$ e p um número primo. Então, pelo Teorema 2.1.3, G tem uma cadeia de composição

$$G_0/\cdots/G_m,$$

onde

$$G = G_0,\ G_m = \{e\},\ G_i = [G_i/G_{i+1}]G_{i+1} \text{ e } G_i/G_{i+1} \simeq \mathbb{Z}_p,$$

onde $\mathbb{Z}_p$ é um *grupo de rótulos*. Portanto, todo $g \in G$ pode ser escrito na forma

$$g = \prod_{i=0}^{m-1} g_i^{n_i},$$

onde $\mathbb{N}_p = \{0, \ldots, p-1\}$ e $[G_i/G_{i+1}] = \{g_i^{n_i} : n_i \in \mathbb{N}_p\}$, $0 \leq i \leq m-1$, pois

$$G_i = \bigcup_{n_i \in \mathbb{N}_p} g_i^{n_i} G_{i+1}.$$

Em particular, quando G é um p-grupo abeliano elementar, todo $g \in G$ pode ser escrito na forma

$$g = \sum_{i=0}^{m-1} n_i g_i,$$

onde $n_i \in \mathbb{N}_p$ e $g_i \in G$, $0 \leq i \leq m-1$. Sejam

$$\mathbf{n} = (n_0, \ldots, n_{m-1}) \in \mathbb{N}_p^m \text{ e } M = \{g_i : 0 \leq i \leq m-1\}$$

uma matriz cujas colunas são os *geradores* g_i de G. Então $g = \sum_{i=0}^{m-1} n_i g_i = M\mathbf{n}^t$. M é chamada a *matriz geradora* de G, $m = \log_p |G|$ é chamado a *dimensão* de G e a expressão $M\mathbf{n}^t$ é chamada de *combinação linear* dos geradores g_i, $0 \leq i \leq m-1$, (cf. [14]).

Seja W um conjunto qualquer não vazio. Então uma *medida de distância* sobre W, (cf. [22]), é um mapeamento

$$d : W \times W \longrightarrow \mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$$

tal que as seguintes propriedades valem:

(1) $d(g,h) \geq 0$,

(2) $d(g,h) = 0$ se, e somente se, $g = h$,

(3) $d(g,h) = d(h,g)$.

Por intermédio de d podemos definir uma *medida de distância aditiva* sobre W^m como a soma das distâncias das componentes, isto é, dados $\mathbf{g}, \mathbf{h} \in W^m$ temos que

$$d(\mathbf{g}, \mathbf{h}) \triangleq \sum_{i=1}^{m} d(g_i, h_i).$$

A definição de uma medida de distância não depende do conjunto W ser um grupo. No entanto, se $W = G$ é um grupo comutativo e $d(g,h) = d(e, g^{-1}h)$ para quaisquer $g, h \in G$, então a medida

de distância d sobre G é chamada *invariante por translação*, (cf. [22]). Note que se d é uma medida de distância invariante por translação, então a medida de distância aditiva obtida a partir de d é invariante por translação. Uma condição necessária para uma medida de distância ser invariante por translação sobre um grupo G é que o *perfil de distância* de todo elemento $g \in G$, isto é,

$$D(g) = \{d(g,h)\}_{h \in G}$$

com suas multiplicidades, não dependa de g.

A mínima distância entre elementos de G, isto é,

$$d_{\min}(G) \triangleq \min \{d(g,h) : g,h \in G,\ g \neq h\}$$

é chamada a *distância intraconjunto.*

Se $G = \{e\}$, então é conveniente definir $d_{\min}(G) = \infty$. Note que a distância intraconjunto de G^m, para todo $m \in \mathbb{N}$, é a mesma de G. Se d é uma medida de distância invariante por translação sobre um grupo G, então $d_{\min}(H) = d_{\min}(gH)$, para todo $H \leq G$ e $g \in G$, pois

$$\begin{aligned} d_{\min}(H) &= \min \{d(h,k) : h,k \in H,\ h \neq k\} \\ &= \min \{d(gh,gk) : h,k \in H,\ h \neq k,\ g \in G\} \\ &= d_{\min}(gH). \end{aligned}$$

A mínima distância entre dois subconjuntos não vazios H e K de G, isto é,

$$d_{\min}(H,K) \triangleq \inf \{d(h,k) : h \in H,\ k \in K\}$$

é chamada a *distância interconjunto.*

Note que $d_{\min}(H,K) = 0$ se, e somente se, $H \cap K \neq \emptyset$. Se d é uma medida de distância invariante por translação sobre um grupo G, então $d_{\min}(H,K) = d_{\min}(gH,gK)$, para todo $H,K \leq G$ e $g \in G$.

Seja $\mathbf{F} \subset \{H : H \subseteq G,\ H \neq \emptyset\}$, $\mathbf{F} \neq \emptyset$. Então a *mínima distância interconjunto* entre elementos de $\mathbf{F}$ é definida por,

$$d_{\min}(\mathbf{F}) \triangleq \inf \{d(H,K) : H,K \in F,\ H \neq K\}.$$

Note que $d_{\min}(\mathbf{F}) > 0$ se, e somente se, os elementos de $\mathbf{F}$ são disjuntos aos pares. Quando $\mathbf{F} = \{H\}$ é conveniente definir $d_{\min}(\mathbf{F}) = \infty$. A Figura 2.1, (cf. [22]), ilustra as várias medidas de distâncias para uma família de subconjuntos $\mathbf{F} = \{H,K,L\}$, onde cada subconjunto contêm quatro elementos.

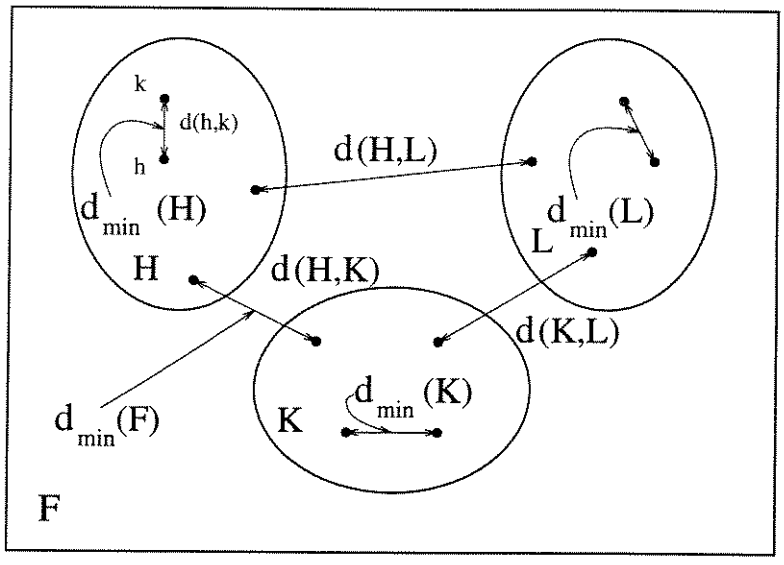


Figura 2.1: Ilustrações da medida entre elementos, intraconjunto, interconjunto e mínima interconjunto.

2.2 Códigos

Nesta seção apresentaremos algumas definições e resultadosclássicos sobre a teoria da codificação que são necessárias para o entendimento do problema a ser estudado. Uma referência excelente sobre códigos é MacWilliams e Sloane [26].

Um *anel* é um conjunto não vazio $\mathbb{R}$ junto com dua operações binárias adição $(x, y) \longmapsto x + y$ e multiplicação $(x, y) \longmapsto xy$ tal que as seguintes propriedades valem:

(1) $\mathbb{R}$ é um grupo comutativo com relação à operação de adição.

(2) $x(yz) = (xy)z$, para quaisquer $x, y, z \in \mathbb{R}$.

(3) $x(y + z) = xy + xz$, $(x + y)z = xz + yz$, para quaisquer $x, y, z \in \mathbb{R}$.

Se em um anel $\mathbb{R}$ as propriedades

(4) Existe $1 \in \mathbb{R}$ tal que $x1 = 1x = x$, para todo $x \in \mathbb{R}$ e

(5) $xy = yx$, para quaisquer $x, y \in \mathbb{R}$

são verificadas, dizemos que $\mathbb{R}$ é um *anel comutativo com unidade.*

Um anel $\mathbb{R}$ cujos elementos não nulos formam um grupo com relação à multiplicação é chamado um *anel de divisão.* Se, além disso $\mathbb{R}$ é um anel comutativo, então $\mathbb{R}$ é chamado um *corpo.*

Seja $\mathbb{R}$ um anel comutativo com unidade. Um *módulo* V sobre $\mathbb{R}$ é um grupo comutativo aditivo junto com um mapeamento $\mathbb{R} \times V \longrightarrow V$, $(x, v) \longmapsto xv$, tal que as seguintes propriedades valem:

(1) $x(yv) = (xy)v$, para quaisquer $x, y \in \mathbb{R}$ e $v \in V$.

(2) $x(u + v) = xu + xv$, para quaisquer $x \in \mathbb{R}$ e $u, v \in V$.

(3) $(x + y)v = xv + yv$, para quaisquer $x, y \in \mathbb{R}$ e $v \in V$.

(4) $1v = v$, para todo $v \in V$.

Note que, se $\mathbb{R}$ é um corpo, então um módulo sobre $\mathbb{R}$ é um *espaço vetorial* sobre $\mathbb{R}$.

Um subconjunto W de um módulo V sobre $\mathbb{R}$ é um *submódulo* de V se

(1) Para quaisquer $w, w' \in W$ tem-se $w - w' \in W$.

(2) Para todo $x \in \mathbb{R}$ e $w \in W$ tem-se $xw \in W$.

Seja S um subconjunto de um módulo V sobre $\mathbb{R}$. Seja $\mathcal{A} = \{W : W \text{ submódulo de } V \text{ e } S \subset W\}$. Então,

$$\langle S \rangle = \bigcap_{W \in \mathcal{A}} W$$

é o menor submódulo de V contendo S e será chamado de *submódulo gerado por* S.

Seja V um módulo sobre $\mathbb{R}$. Se $v \in V$ pode ser escrito como $v = \sum_{i=1}^{n} x_i v_i$, $x_i \in \mathbb{R}$ e $v_i \in V$, então dizemos que v é uma *combinação linear* dos elementos $v_1, \ldots, v_n$ sobre $\mathbb{R}$. Neste caso,

$$\langle v_1, \ldots, v_n \rangle = \left\{ \sum_{i=1}^{n} x_i v_i : x_i \in \mathbb{R} \right\}.$$

Quando existe um subconjunto finito S de um módulo V sobre $\mathbb{R}$ tal que $V = \langle S \rangle$, dizemos que V é um *módulo finitamente gerado.*

Uma seqüência finita $v_1, \ldots, v_n$ de elementos de um módulo V sobre $\mathbb{R}$ é chamada *linearmente independente* se para quaisquer $x_1, \ldots, x_n \in \mathbb{R}$,

$$\sum_{i=1}^{n} x_i v_i = 0 \Longrightarrow x_1 = x_2 = \cdots = x_n = 0.$$

Caso contrário, dizemos que a seqüência é linearmente dependente. Um subconjunto S de um módulo V sobre $\mathbb{R}$ é chamado linearmente independente se qualquer seqüência finita de elementos distintos de S é linearmente independente. Caso contrário S é chamado linearmente dependente.

Um subconjunto B de um módulo V sobre $\mathbb{R}$ é chamado uma *base* se as seguintes propriedades valem:

(1) $V = \langle B \rangle$.

(2) B é conjunto linearmente independente.

Um módulo V sobre $\mathbb{R}$ é chamado um *módulo livre* se V possui uma base.

Um *espaço de seqüências* $\mathbb{F}^{\mathbb{I}}$ é o conjunto de todas as seqüências $\mathbf{c} = (c_i)_{i \in \mathbb{I}}$, cujos elementos c_i pertencem ao alfabeto $\mathbb{F}$, onde o conjunto de índices $\mathbb{I}$ é um subconjunto dos inteiros, ($\mathbb{I} \subseteq \mathbb{Z}$). Quando $\mathbb{I} = \{i : 1 \leq i \leq n\}$ denotamos $\mathbb{F}^{\mathbb{I}}$ por $\mathbb{F}^n$.

Um *código* C sobre um alfabeto $\mathbb{F}$ é qualquer subconjunto não-vazio do espaço de seqüências $\mathbb{F}^{\mathbb{I}}$. Um *código de bloco* C de comprimento n sobre um alfabeto $\mathbb{F}$ é qualquer subconjunto não-vazio do conjunto $\mathbb{F}^n$ de todas as n-uplas $\mathbf{c} = (c_i)_{i=1}^n$. A *dimensão* do código C é o número $k = \log_{|\mathbb{F}|} |C|$. Note que k não é necessariamente inteiro. Um código de bloco C de comprimento n e dimensão k é chamado um $[n, k]$-código. A *taxa* do código é o número $R = \frac{k}{n}$ símbolos por bloco. Observe que $|C|$ é limitado, pois $1 \leq |C| \leq |\mathbb{F}|^n$.

A *distância de Hamming* $d_H(\mathbf{c}, \mathbf{c}')$ entre duas palavras $\mathbf{c}, \mathbf{c}' \in \mathbb{F}^n$ é o número de componentes onde elas diferem:

$$d_H(\mathbf{c}, \mathbf{c}') = |\{i \in \mathbb{I} : c_i \neq c_i'\}|$$

Se $|C| \geq 2$, então a *mínima distância de Hamming* de C é definida por,

$$d_H(C) \triangleq \min\{d_H(\mathbf{c}, \mathbf{c}') : \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'\}.$$

Note que $1 \leq d_H(C) \leq n$. Quando $C = \{0\}$ é conveniente definir $d_H(C) = \infty$. Um código de bloco C de comprimento n com dimensão k e mínima distância de Hamming $d = d_H(C)$ é chamado um $[n, k, d]$-código. Um $[n, k, d]$-código tal que $d = n - k + 1$ é chamado um *código separável à máxima distância* ou, simplesmente $[n, k, d]$-código MDS.

Quando $\mathbb{F}$ é um grupo, um código de comprimento n sobre $\mathbb{F}$ é de grupo se ele é um subgrupo do grupo $\mathbb{F}^n$. Quando $\mathbb{F}$ é um anel comutativo com unidade, um código de comprimento n sobre $\mathbb{F}$ é

linear se ele é um submódulo livre do módulo $\mathbb{F}^n$. Em particular, se $\mathbb{F} = \mathbb{F}_q$ o corpo de Galois com $q = p^t$, onde p é um número primo, um código de comprimento n sobre $\mathbb{F}_q$ é "*quasilinear*" se ele é um subespaço vetorial do espaço vetorial $\mathbb{F}_p^n$ e é *linear* se ele é um subespaço vetorial do espaço vetorial $\mathbb{F}_q^n$ e, neste caso a dimensão do código é um número inteiro.

Seja $C = [n, k, d]$ um código linear sobre $\mathbb{F}_q$. Então dado uma base $\{\mathbf{c}_1, \ldots, \mathbf{c}_k\}$ de C a imersão $C : \mathbb{F}^k \hookrightarrow \mathbb{F}^n$ dado por,

$$C((u_1, \ldots, u_k)) = \sum_{i=1}^{k} u_i \mathbf{c}_i = \left(\sum_{i=1}^{k} u_i c_{i1}, \ldots, \sum_{i=1}^{k} u_i c_{in} \right),$$

onde $\mathbf{c}_i = (c_{i1}, \ldots, c_{in})$, $1 \leq i \leq k$, é um *codificador* para o código C, onde usamos a mesma notação tanto para o código quanto para o codificador. A $k \times n$ matriz $M = (c_{ij})$ que descreve o mapeamento linear C é chamada uma *matriz geradora* do código. Assim, C consiste de q^k combinações lineares $\mathbf{u}M$, onde $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ é chamada uma *seqüência de informação* ou *mensagem.*

O *peso de Hamming* $w_H(\mathbf{c})$ de uma palavra-código não nula $\mathbf{c} \in C$ é o número de componentes diferentes de zero, portanto

$$d_H(\mathbf{c}, \mathbf{c}') = w_H(\mathbf{c} - \mathbf{c}').$$

Assim, para um código linear C sobre $\mathbb{F}_q$

$$d_H(\mathbf{c}, \mathbf{c}') = d_H(\mathbf{c} - \mathbf{c}', \mathbf{0}) = w_H(\mathbf{c} - \mathbf{c}'), \forall \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'.$$

Seja $C = [n, k, d]$ um código linear sobre $\mathbb{F}_q$. A "*esfera de Hamming*" de raio $\rho = \lfloor (d-1)/2 \rfloor$ e centro $\mathbf{c} \in C$ é o conjunto de todas as palavras $\mathbf{r} \in \mathbb{F}_q^n$ tal que $w_H(\mathbf{r} - \mathbf{c}) \leq \rho$, isto é,

$$E_\rho(\mathbf{c}) = \{\mathbf{r} \in \mathbb{F}_q^n : w_H(\mathbf{r} - \mathbf{c}) \leq \rho\}$$

e, neste caso, o código C pode corrigir até ρ erros, onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x.

Um *algoritmo de decodificação pelo vizinho mais próximo* para um código C sobre $\mathbb{F}_q$ é um algoritmo que, dada uma palavra $\mathbf{r} \in \mathbb{F}_q^n$, encontra uma palavra-código em C mais próxima de $\mathbf{r}$ do que qualquer outra palavra-código de C, isto é, dada uma palavra $\mathbf{r} \in \mathbb{F}_q^n$ existe $\mathbf{c} \in C$ tal que $d_H(\mathbf{c}, \mathbf{r}) \leq d_H(\mathbf{c}', \mathbf{r})$, para todo $\mathbf{c}' \in C$, com $\mathbf{c} \neq \mathbf{c}'$.

Para qualquer corpo $\mathbb{F}_q$ e qualquer inteiro positivo n existem os seguintes códigos lineares MDS:

(1) O $[n, n, 1]$-código universal $C = \mathbb{F}_q^n$.

(2) O $[n, n-1, 2]$-código de verificação de paridade simples

$$C = \left\{ (c_1, \ldots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} c_i = 0 \right\}.$$

(3) O $[n, 1, n]$-código de repetição $C = \{(\alpha, \ldots, \alpha) \in \mathbb{F}_q^n : \alpha \in \mathbb{F}_q\}$.

Dois códigos C_1 e C_2 com parâmetros $[n, k_1, d_1]$ e $[n, k_2, d_2]$ são *comparáveis* se:

(1) eles têm a mesma taxa ($R_1 = R_2$), ou

(2) eles têm a mesma distância mínima ($d_1 = d_2$), ou

(3) $R_1 > R_2$ e $d_1 > d_2$.

Um código C_1 é *melhor* do que um código comparável C_2 se os dois códigos satisfazem (1) e $d_1 > d_2$, ou satisfazem (2) e $R_1 > R_2$, ou satisfazem (3).

Se n é relativamente primo com q, isto é, $mdc(n, q) = 1$ e m a ordem de q módulo n, isto é, o menor inteiro positivo tal que $q^m \equiv 1 \pmod{n}$, então $q^m - 1 = kn$, para algum $k \in \mathbb{Z}$. Como qualquer elemento de $\mathbb{F}_{q^m}$ é raiz do polinômio $x^{q^m} - x$ e $x^n - 1$ divide $x^{kn} - 1 = x^{q^m - 1} - 1$, pois

$$x^n + x^{2n} + \cdots + x^{kn} = \frac{x^n(x^{kn} - 1)}{x^n - 1},$$

temos que $\mathbb{F}_{q^m}$ é o corpo das raízes de $x^n - 1$ sobre $\mathbb{F}_q$. Se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de $x^n - 1$, então $\beta^n = 1$ e β é chamada uma *raiz n-ésima da unidade*. Suponhamos que α é um elemento primitivo em $\mathbb{F}_{q^m}$, de modo que $\alpha^{q^m - 1} = 1$. Então, $\alpha^k = \alpha^{\frac{q^m - 1}{n}}$ tem ordem n e é uma raiz de $x^n - 1$, neste caso α^k é chamado uma raiz n-ésima primitiva da unidade.

Dados $a, b \in \mathbb{Z}$, definimos $a \sim b$ se, e somente se, existe $j \in \mathbb{Z}$ tal que $a \equiv bq^j \pmod{n}$. Assim, se $mdc(n, q) = 1$, então $\sim$ é uma relação de equivalência módulo n. Seja $[a] = \{b \in \mathbb{Z} : b \sim a\}$ a classe de equivalência determinada por a e $\mathbb{Z}/\sim = \{[a] : a \in \mathbb{Z}\}$ o espaço quociente de $\mathbb{Z}$ por $\sim$. Então, $\mathbb{Z}_n = \bigcup_{[a] \in \mathbb{Z}/\sim} [a]$. Portanto, $|\mathbb{Z}/\sim|$ é o número de fatores irredutíveis de $x^n - 1$ sobre $\mathbb{F}_q$, (cf. [26]).

Um código C em $\mathbb{F}_q^n$ é um *código cíclico* se $\mathbf{c} = (c_1, \ldots, c_n) \in C$, então $\tilde{\mathbf{c}} = (c_n, c_1, \ldots, c_{n-1}) \in C$. É conveniente representar a palavra-código $\mathbf{c} = (c_1, \ldots, c_n) \in C$ pelo polinômio $c(x) = c_1 + c_2 x + \cdots + c_n x^{n-1}$ no anel $R_n(x) = \mathbb{F}_q[x]/(x^n - 1)$. Então $xc(x)$ representa um deslocamento cíclico da palavra-código $\mathbf{c}$ e, assim, um código cíclico linear é representado por um ideal em $R_n(x)$. Portanto, C pode ser gerado por um único polinômio $g(x)$, chamado *polinômio gerador* do código.

Se $mdc(n,q) = 1$ e α é uma raiz n-ésima primitiva da unidade em alguma extensão de $\mathbb{F}_q$, então

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i).$$

Se m é o menor inteiro positivo tal que $q^m \equiv 1 \pmod{n}$, então $\alpha \in \mathbb{F}_{q^m}$. Assim,

$$g(x) = \prod_{i \in \mathbb{J}}(x - \alpha^i),$$

para algum $\mathbb{J} \subseteq \{0, \ldots, n-1\}$, isto é, $\mathbb{J} = [a]$. Os elementos α^i para $i \in \mathbb{J}$ são chamados *os zeros* do código.

Um $[n = q-1, k, d = q-k]$-*código Reed-Solomon* C sobre $\mathbb{F}_q$ é um código cíclico com polinômio gerador

$$g(x) = \prod_{i=0}^{d-2}(x - \alpha^{t+i}),$$

onde α é qualquer elemento primitivo em alguma extensão de $\mathbb{F}_q$. Então cada palavra-código $\mathbf{c} = (c_1, \ldots, c_n) \in C$ satisfaz a seguinte equação

$$\sum_{i=1}^{n} c_i \alpha^{i(j+t)} = 0,$$

para $j = 0, \ldots, d-2$ $(d \geq 2)$. Logo,

$$c(x) \equiv 0 \pmod{g(x)}.$$

Usualmente, tomamos $t = 0$ ou $t = 1$. Os códigos Reed-Solomon são denotados por $RS(n,d)$.

Lema 2.2.1 [19] *Se $n \leq q+1$ e $1 \leq k \leq n$, então existe um $[n, k, n-k+1]$-código linear sobre $\mathbb{F}_q$.* ■

Lema 2.2.2 [23] *Seja C um $[q+1, 2, q]$-código linear sobre $\mathbb{F}_q$ com uma matriz geradora M. Então existe um $[m(q+1), 2, mq]$-código linear C_m sobre $\mathbb{F}_q$ com uma matriz geradora*

$$M_m = [\overbrace{M \cdots M}^{m-vezes}].$$

Além disso, para $1 \leq r \leq q$, existe um $[m(q+1) - r, 2, mq - r]$-código linear sobre $\mathbb{F}_q$. ■

Seja $C = \langle \mathbf{c}_1, \ldots, \mathbf{c}_k \rangle$ um $[n, k, d]$-código linear sobre $\mathbb{F}_q$ gerado pelas palavras-código $\mathbf{c}_1, \ldots, \mathbf{c}_k$ (formando as linhas de uma matriz geradora M). Fazendo

$$C_i = \langle \mathbf{c}_1, \ldots, \mathbf{c}_{k-i} \rangle,\ 0 \leq i \leq k-1 \text{ e } C_k = \{\mathbf{0}\},$$

obtemos uma cadeia de partições, com k-níveis e q-maneiras,

$$C_0/C_1/\cdots/C_k, \text{ onde } C_0 = C,\ C_i = [C_i/C_{i+1}] + C_{i+1} \text{ e } C_i/C_{i+1} \simeq \mathbb{F}_q,\ 0 \leq i \leq k-1,$$

onde $\mathbb{F}_q$ é um corpo de rótulos.

Agora, sejam C e C' códigos lineares sobre $\mathbb{Z}_q$ de comprimento n tal que $C' \subset C$. Então C' induz uma partição C/C' em C com $|C/C'| = q^m$, $1 \leq m \leq \log_q |C|$, classes laterais de C'. Se

$$[C/C'] = \left\{ \sum_{i=0}^{m-1} a_i \mathbf{g}_i : a_i \in \mathbb{N}_q,\ 0 \leq i \leq m-1 \right\},$$

onde $\mathbf{g}_i \in C$, $\mathbf{g}_i \notin C'$ e $\mathbb{N}_q = \{0, \ldots, q-1\}$, é um sistema de representantes de classes laterais fixo de C' em C, então uma cadeia de partições, com m-níveis e q-maneiras,

$$C_0/C_1/\cdots/C_m$$

pode ser definida como um refinamento de C/C', fazendo

$$C_0 = C,\ C_m = C',\ C_i = [C_i/C_{i+1}] + C_{i+1}, \text{ e } |C_i/C_{i+1}| = q,$$

onde

$$[C_i/C_{i+1}] = \{a_i \mathbf{g}_i : a_i \in \mathbb{N}_q\} \text{ e } \mathbf{g}_i \in C_i,\ \mathbf{g}_i \notin C_{i+1},\ 0 \leq i \leq m-1.$$

Como

$$C_i = \bigcup_{a_i \in \mathbb{N}_q} (a_i \mathbf{g}_i + C_{i+1}),\ 0 \leq i \leq m-1$$

temos que toda classe lateral à esquerda de C_m em C_0 é determinada de modo único pelo conjunto de seqüências $(a_0, \ldots, a_{m-1})$, isto é, existe uma correspondência biunívoca de $\mathbb{F}_q^m$ em C_0/C_m, a qual não é necessariamente um isomorfismo de $\mathbb{F}_q^m$ em C_0/C_m. Note que as palavras-código $\mathbf{g}_0, \ldots, \mathbf{g}_{m-1}$ são linearmente independentes sobre C', isto é, se $\sum_{i=0}^{m-1} a_i \mathbf{g}_i \in C'$, $a_i \in \mathbb{F}_q$, $0 \leq i \leq m-1$, então $a_0 = a_1 = \cdots = a_{m-1} = 0$.

Lema 2.2.3 [37] *Se $1 \leq m \leq q$, então existe uma cadeia de partições, com m-níveis e q-maneiras, $C_0/C_1/\cdots/C_m$, onde $C_i = RS(m, i+1)$, $i = 0, \ldots, m-1$ e $C_m = RS(m, \infty)$.* ∎

2.3 Reticulados

Nesta seção apresentaremos algumas caracterizações algébricas e geométricas sobre empacotamentos esféricos necessárias para o entendimento dos próximos capítulos. Uma excelente referência para estudar empacotamentos esféricos é Cassels [6] ou Conway e Sloane [8].

A *norma quadrática* ou *peso Euclidiano* $\mathrm{N}(\mathbf{x}) = \| \mathbf{x} \|^2$ de um vetor $\mathbf{x} \in \mathbb{R}^N$ é a soma dos quadrados de suas componentes, isto é, $\mathrm{N}(\mathbf{x}) = (\mathbf{x}, \mathbf{x}) = \mathbf{x}\mathbf{x}^t$, onde $(\mathbf{x}, \mathbf{x})$ é o produto interno de $\mathbf{x}$ por $\mathbf{x}$. A *distância Euclidiana quadrática* entre dois vetores $\mathbf{x}, \mathbf{y} \in \mathbb{R}^N$ é a norma quadrática de sua diferença, isto é, $d^2(\mathbf{x}, \mathbf{y}) = \mathrm{N}(\mathbf{x} - \mathbf{y})$. Isto implica que $\mathbb{R}^N$ está equipado com uma medida de distância aditiva, a qual é invariante por translação.

Uma *isometria* ou um *movimento rígido* de $\mathbb{R}^N$ é um mapeamento $\varphi : \mathbb{R}^N \longrightarrow \mathbb{R}^N$ que preserva distância, isto é,

$$\mathrm{N}(\varphi(\mathbf{x}) - \varphi(\mathbf{y})) = \mathrm{N}(\mathbf{x} - \mathbf{y}),$$

para todo $\mathbf{x}, \mathbf{y} \in \mathbb{R}^N$. Não é difícil verificar que o conjunto de todas as isometrias de $\mathbb{R}^N$, denotado por $Isom(\mathbb{R}^N)$, é um subgrupo do grupo simétrico $S_{\mathbb{R}^N}$. Uma *translação* por um vetor $\mathbf{x_0} \in \mathbb{R}^N$ é um mapeamento $t_{\mathbf{x_0}} : \mathbb{R}^N \longrightarrow \mathbb{R}^N$ dado por $t_{\mathbf{x_0}}(\mathbf{x}) = \mathbf{x} + \mathbf{x_0}$, para todo $\mathbf{x} \in \mathbb{R}^N$. Uma translação é completamente determinada quando sabemos seu valor na origem, isto é, $t_{\mathbf{x_0}}(0) = \mathbf{x_0}$. É claro que $t_{\mathbf{x_0}} \in Isom(\mathbb{R}^N)$, para todo $\mathbf{x_0} \in \mathbb{R}^N$. O conjunto das translações de $\mathbb{R}^N$, denotado por $T(\mathbb{R}^N)$, é um subgrupo normal de $Isom(\mathbb{R}^N)$. Além disso, $T(\mathbb{R}^N)$ é isomorfo ao grupo aditivo dos vetores de translações $\mathbf{x_0} \in \mathbb{R}^N$.

Uma transformação linear $T : \mathbb{R}^N \longrightarrow \mathbb{R}^N$ é chamada *ortogonal* se a mesma preserva o produto interno, isto é,

$$(T(\mathbf{x}), T(\mathbf{y})) = (\mathbf{x}, \mathbf{y}),$$

para todo $\mathbf{x}, \mathbf{y} \in \mathbb{R}^N$. É claro que $T \in Isom(\mathbb{R}^N)$. O conjunto das transformações ortogonais de $\mathbb{R}^N$, denotado por $O(\mathbb{R}^N)$, é um subgrupo de $Isom(\mathbb{R}^N)$. Note que os elementos $O(\mathbb{R}^N)$ são rotações em torno da origem e/ou reflexões sobre o hiperplano passando pela origem (um *hiperplano* H em $\mathbb{R}^N$ é uma translação de um subespaço W de dimensão $N - 1$). Seja R a matriz que representa T na base canônica para $\mathbb{R}^N$. Então $\sum_{k=1}^{N} r_{ki} r_{kj} = \delta_{ij}$, pois $RR^t = I$. Logo, cada coluna de R tem comprimento igual a 1 e são perpendiculares entre si, formando uma base ortonormal para $\mathbb{R}^N$. Além disso, se $\det(R) = 1$ dizemos que T_R é uma *rotação própria*; se $\det(R) = -1$ dizemos que T_R é uma *rotação*

imprópria; se $\det(R) = -1$ e $R^2 = I$ dizemos que T_R é uma *reflexão.*

Teorema 2.3.1 [18] *Todo elemento de* $Isom(\mathbb{R}^N)$ *pode ser escrito como a composição de uma única transformação ortogonal com uma única translação, isto é, como uma transformação afim*

$$T_{R,\mathbf{x}_0}(\mathbf{x}) = R\mathbf{x} + \mathbf{x}_0, \ \forall \mathbf{x} \in \mathbb{R}^N,$$

onde R *é uma matriz ortogonal e* $\mathbf{x}_0$ *é um vetor arbitrário de* $\mathbb{R}^N$. ■

Uma *esfera* em $\mathbb{R}^N$ com centro $\mathbf{c}$ e raio ρ consiste de todos os pontos $\mathbf{x} \in \mathbb{R}^N$ tal que $\mathbf{N}(\mathbf{x}-\mathbf{c}) = \rho^2$, isto é,

$$E_\rho(\mathbf{c}) = \{\mathbf{x} \in \mathbb{R}^N : \mathbf{N}(\mathbf{x} - \mathbf{c}) = \rho^2\}.$$

O *volume* de $E_\rho(\mathbf{0})$ é definido por,

$$V(E_\rho(\mathbf{0})) \triangleq \frac{\pi^{\frac{N}{2}}\rho^N}{G\left(\frac{N+2}{2}\right)},$$

onde

$$G(\alpha) = \int_0^\infty e^{-x}x^{\alpha-1}dx, \ \alpha > 0,$$

é a função Gama. Sendo N um inteiro positivo há dois casos a serem considerados:

(1) Se N é par, digamos $N = 2k$, então

$$V(E_\rho(\mathbf{0})) = \frac{\pi^k\rho^{2k}}{k!},$$

(2) Se N é ímpar, digamos $N = 2k + 1$, então

$$V(E_\rho(\mathbf{0})) = \frac{2^{2k+1}k!\pi^k\rho^{(2k+1)}}{(2k+1)!}.$$

Note que $V(E_\rho(\mathbf{c}))$ =$V(E_\rho(\mathbf{0}))$, pois o volume é invariante por translação.

Um *empacotamento esférico* Γ em $\mathbb{R}^N$ de raio ρ consiste de uma seqüência infinita de pontos $\mathbf{c}_1, \mathbf{c}_2, \ldots$ em $\mathbb{R}^N$, os centros das esferas, tal que $\mathbf{N}(\mathbf{c}_i - \mathbf{c}_j) \geq 4\rho^2$ para todo $i \neq j$. O raio ρ é chamado de *raio de empacotamento* ou *raio de correção de erro* e, neste caso

$$d^2_{\min}(\Gamma) = 4\rho^2,$$

onde $d^2_{\min}(\Gamma)$ é a mínima distância Euclidiana quadrática entre os elementos de Γ, isto é, a distância intraconjunto de Γ.

Um *reticulado* Λ é um subgrupo aditivo discreto em $\mathbb{R}^N$ ou, equivalentemente, os centros do empacotamento esférico de Λ formam um grupo aditivo sob a adição de vetores. Um *código reticulado* é um subconjunto finito de pontos de um reticulado Λ ou de uma translação $\mathbf{x} + \Lambda$.

Um subgrupo aditivo em $\mathbb{R}^N$ é *discreto* se sua interseção com qualquer subconjunto compacto em $\mathbb{R}^N$ é finita (um *compacto* em $\mathbb{R}^N$ é um subconjunto fechado e limitado).

Teorema 2.3.2 [6] *Seja Λ um reticulado em $\mathbb{R}^N$. Então Λ é gerado, como $\mathbb{Z}$-módulo, por k vetores linearmente independentes sobre $\mathbb{R}$, neste caso $k \leq N$.* ■

Seja $\Lambda = \langle \mathbf{x}_1, \ldots, \mathbf{x}_k \rangle$ um reticulado em $\mathbb{R}^N$ gerado por k vetores linearmente independentes $\mathbf{x}_1, \ldots, \mathbf{x}_k$ sobre $\mathbb{R}$. Se

$$\mathbf{x}_i = (x_{i1}, \ldots, x_{iN}),$$

então a matriz

$$M = \left\{ \mathbf{x}_i^t : 1 \leq i \leq k \right\},$$

cujas colunas são os vetores $\mathbf{x}_i^t$ é chamada uma *matriz geradora* do reticulado Λ, e os elementos do reticulado Λ consistem de todos os vetores $M\mathbf{u}^t$, onde $\mathbf{u} \in \mathbb{Z}^N$.

A matriz $A = M^t M$ é chamada *matriz de Gramm* para o reticulado Λ. O *determinante* do reticulado Λ é a raiz quadrada do determinante da matriz A, isto é

$$d(\Lambda) \triangleq \sqrt{|\det(A)|}.$$

Um *sub-reticulado* do reticulado Λ é qualquer subgrupo de Λ. Como todo reticulado de dimensão $k \leq N$ pode ser mergulhado (imerso como um sub-reticulado) em um reticulado de dimensão N, então salvo menção explicita em contrário, todos os reticulados e sub-reticulados deste trabalho são de dimensão N. Neste caso, se Λ é um reticulado em $\mathbb{R}^N$, então

$$d(\Lambda) = |\det(M)| .$$

Lema 2.3.1 [6] *Sejam Λ_1 e Λ_2 reticulados em $\mathbb{R}^N$ com matrizes geradoras M_1 e M_2, respectivamente. Então Λ_2 é um sub-reticulado de Λ_1 se, e somente se, $M_2 = BM_1$, onde $B = (b_{ij})$ com $b_{ij} \in \mathbb{Z}$.* ■

Uma matriz quadrada $U = (u_{ij})$, com $u_{ij} \in \mathbb{Z}$ e $\det(U) = \pm 1$ é chamada *unimodular*. Assim, U é unimodular se, e somente se, $U^{-1} = (v_{ij})$ existe e $v_{ij} \in \mathbb{Z}$. Sejam Λ e Λ' reticulados em $\mathbb{R}^N$, dizemos

que Λ é *similar* a Λ', (cf. [8]), se existe $T \in O(\mathbb{R}^N)$ e $\alpha \in \mathbb{R} - \{0\}$ tal que $\Lambda' = \alpha T(\Lambda)$. Neste caso, se M' e M são matrizes geradoras para Λ' e Λ, respectivamente, então

$$M' = \alpha RMU,$$

onde U é uma matriz unimodular e R é uma matriz ortogonal.

Corolário 2.3.1 [6] *Sejam Λ_1 e Λ_2 reticulados em $\mathbb{R}^N$ com matrizes geradoras M_1 e M_2, respectivamente. Então $\Lambda_2 = \Lambda_1$ se, e somente se, existe uma matriz unimodular U tal que $M_2 = UM_1$.* ■

Note que, do Corolário 2.3.1, $d(\Lambda)$ é independente da escolha da base para Λ.

Exemplo 2.3.1 *Sejam Λ o reticulado hexagonal em $\mathbb{R}^2$, (cf. [8]), com uma matriz geradora*

$$M = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

e $\Lambda' = \{(x, y, z) \in \mathbb{Z}^3 : x + y + z = 0\}$ o reticulado laminado em $\mathbb{R}^3$, (cf. [8]), com uma matriz geradora

$$M' = \begin{bmatrix} 1 & 0 \\ 0 & -1 \\ -1 & 1 \end{bmatrix}.$$

Então $M' = \alpha RMU$, onde $\alpha = \sqrt{2}$, $U = I_2$ e

$$R = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ 0 & -\frac{2}{\sqrt{6}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \end{bmatrix}.$$

Portanto, o reticulado Λ' é similar ao reticulado Λ. ■

Lema 2.3.2 [6] *Sejam Λ_2 um sub-reticulado de Λ_1. Então para toda base $\{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$ de Λ_1 existe uma base $\{\mathbf{y}_1, \ldots, \mathbf{y}_N\}$ para Λ_2 tal que*

$$\mathbf{y}_j = \sum_{k=1}^{j} b_{kj}\mathbf{x}_k,$$

onde $b_{kj} \in \mathbb{Z}$, $b_{kk} > 0$, para todo k, e reciprocamente. ■

Corolário 2.3.2 [6] *Sejam Λ_2 um sub-reticulado de Λ_1 e $B = (b_{kj})$, $b_{kj} \in \mathbb{Z}$, $b_{kk} > 0$. Então o índice* $[\Lambda_1 : \Lambda_2] = |\det(B)|$. ■

Lema 2.3.3 [6] *Sejam Λ_2 um sub-reticulado de Λ_1 em $\mathbb{R}^N$. Então existe somente um número finito de sub-reticulados intermediários, isto é, reticulados Λ em $\mathbb{R}^N$ tais que $\Lambda_2 \subseteq \Lambda \subseteq \Lambda_1$.* ■

Corolário 2.3.3 [6] *Seja Λ_1 um reticulado em $\mathbb{R}^N$ e $r \in \mathbb{N}$. Então existe somente um número finito de reticulados Λ em $\mathbb{R}^N$ que contêm Λ_1 e tal que $[\Lambda : \Lambda_1] = r$.* ■

Seja Λ um reticulado em $\mathbb{R}^N$. Então obtemos uma partição de $\mathbb{R}^N$ em classes de equivalência módulo Λ, isto é, dados $\mathbf{x}, \mathbf{y} \in \mathbb{R}^N$, $\mathbf{x} \equiv \mathbf{y} \pmod{\Lambda}$ se, e somente se, $-\mathbf{x} + \mathbf{y} \in \Lambda$. Assim, a classe de equivalência de $\mathbf{x}$ ou a translação do reticulado Λ por $\mathbf{x}$ é o conjunto $\mathbf{x} + \Lambda = \{\mathbf{x} + \lambda : \lambda \in \Lambda\}$. Note que, $\mathbf{x} + \Lambda$ pode ser caracterizado como o conjunto de pontos em $\mathbb{R}^N$ que são gerados pelo grupo das translações por elementos de Λ

$$T(\Lambda) = \left\{ t_\lambda : \mathbf{y} \longmapsto \mathbf{y} + \lambda : \mathbf{y} \in \mathbb{R}^N, \lambda \in \Lambda \right\},$$

agindo no ponto inicial $\mathbf{x}$

$$\mathbf{x} + \Lambda = \{ t_\lambda(\mathbf{x}) : t_\lambda \in T(\Lambda) \}.$$

Em outras palavras, $\mathbf{x} + \Lambda$ é a órbita de $\mathbf{x}$ sob o grupo $T(\Lambda)$.

Uma região em $\mathbb{R}^N$ que contém um e somente um ponto de cada classe lateral à esquerda de Λ em $\mathbb{R}^N$ é chamada de *região fundamental*, (cf. [14]). Fixado um sistema de representantes de classes laterais de Λ em $\mathbb{R}^N$, denotamos por $R(\Lambda)$, temos $\mathbb{R}^N = R(\Lambda) + \Lambda$. Note que região fundamental não é única mas toda região fundamental deve ter o mesmo volume, pois o volume é invariante por translação. O *volume fundamental* de um reticulado Λ é o volume de uma região fundamental $R(\Lambda)$, o qual será denotado por $V(\Lambda)$.

Seja $\{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$ uma base para o reticulado Λ. Então o conjunto

$$P = P(\mathbf{x}_1, \ldots, \mathbf{x}_N) \triangleq \left\{ \sum_{i=1}^{N} a_i \mathbf{x}_i : 0 \leq a_i < 1 \right\},$$

é uma região fundamental de Λ. De fato, dado $\mathbf{x} \in \mathbb{R}^N$, digamos $\mathbf{x} = b_1\mathbf{x}_1 + \cdots + b_N\mathbf{x}_N$, $b_i \in \mathbb{R}$, como para cada i, $b_i = c_i + a_i$, onde $c_i \in \mathbb{Z}$ e $0 \leq a_i < 1$, temos que $\mathbf{x} = \mathbf{y} + \mathbf{r}$ com $\mathbf{y} \in \Lambda$ e $\mathbf{r} \in P$. Finalmente, se $\mathbf{x} = \mathbf{y}' + \mathbf{r}'$ com $\mathbf{y}' \in \Lambda$ e $\mathbf{r}' \in P$, então $\mathbf{y} + \mathbf{r} = \mathbf{y}' + \mathbf{r}'$ se, e somente se, $\mathbf{y} = \mathbf{y}'$ e $\mathbf{r} = \mathbf{r}'$, pois $0 \leq |a_i - a_i'| < 1$ e $c_i - c_i' \in \mathbb{Z}$. A região fundamental P é chamada *região fundamental básica* para Λ.

Lema 2.3.4 [6] *Seja* Λ *um reticulado em* $\mathbb{R}^N$. *Então* $V(\Lambda) = d(\Lambda) = V(P)$.

Prova. Seja $\{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$ uma base para o reticulado Λ em $\mathbb{R}^N$. Por definição

$$V(P) = \int_P dt_1 \cdots dt_N.$$

Se $\mathbf{x}_i = (x_{1i}, \ldots, x_{Ni})$, então fazendo a mudança de variáveis

$$t_i = \sum_{j=1}^{N} x_{ji} t'_j,$$

onde $0 \leq t'_j < 1$, obtemos

$$V(P) = \int_0^1 |\det(x_{ji})|\, dt'_1 \cdots dt'_N = |\det(x_{ji})|\,.$$

Portanto, $V(\Lambda) = d(\Lambda) = V(P)$. ∎

Seja $T : \mathbb{R}^N \longrightarrow \mathbb{R}^N$ uma transformação linear não singular. Então o reticulado Λ em $\mathbb{R}^N$ é transformado por T no reticulado $T(\Lambda) = \{T(\lambda) : \lambda \in \Lambda\}$ em $\mathbb{R}^N$. Se $T(\Lambda) \subset \Lambda$, então dizemos que T é um *endomorfismo* para Λ. Em particular, se $T(\Lambda) = \Lambda$, então dizemos que T é um *automorfismo* para Λ. Uma transformação linear não singular $T : \mathbb{R}^N \longrightarrow \mathbb{R}^N$ que preserva ângulo é chamada uma *similaridade*, isto é, T é igual ao produto de um escalar não nulo por uma transformação ortogonal.

Lema 2.3.5 [14] *Sejam* Γ *um reticulado em* $\mathbb{R}^N$ *e* Λ *um sub-reticulado de* Γ. *Então* Γ^m *é um reticulado em* $\mathbb{R}^{Nm}$ *e* $(\Gamma/\Lambda)^m$ *é isomorfo a* Γ^m/Λ^m, *para todo* $m \geq 1$. ∎

Note que, se Γ é um reticulado em $\mathbb{R}^N$ e Λ um sub-reticulado de Γ, então, pelo Corolário 2.3.2 e o Lema 2.3.4, $V(\Lambda) = [\Gamma : \Lambda]V(\Gamma)$. Neste caso, $[\Gamma/\Lambda] = \Gamma \cap R(\Lambda)$, (cf. [10]), é um sistema de representantes de classes laterais de Λ em Γ, selecionado na região fundamental básica de Λ. Em particular, se Λ é um sub-reticulado do reticulado cúbico $\mathbb{Z}^N$, então $V(\Lambda) = [\mathbb{Z}^N : \Lambda]$.

A mínima distância Euclidiana quadrática interclasses laterais de um reticulado Λ em $\mathbb{R}^N$, será denotada por $d^2_{\min}(\mathbf{x}+\Lambda, \Lambda) = \mathrm{N}(\mathbf{x}+\Lambda)$. Neste caso, o raio de empacotamento de Λ é $\rho = d_{\min}(\Lambda)/2$. O *número de contatos* ou *coeficiente de erro*, (cf. [14]), de um reticulado Λ é o número de vizinhos mais próximos de Λ, isto é, o número de elementos $\lambda \in \Lambda$, com $\mathrm{N}(\lambda) = d^2_{\min}(\Lambda)$ e, denotamos por $E(\Lambda)$.

Seja Γ um reticulado em $\mathbb{R}^N$ e Λ um sub-reticulado de Γ. Então,

$$d^2_{\min}(\Gamma) = \min\left\{d^2_{\min}(\Lambda),\, d^2_{\min}(\Gamma/\Lambda)\right\},$$

onde $d^2_{\min}(\Gamma/\Lambda) = \min\{\mathbf{N}(\gamma+\Lambda) : \gamma \in \Gamma, \gamma \neq 0\}$. Portanto, (cf. [10]),

$$E(\Gamma) = \begin{cases} E(\Lambda), & \text{se } d^2_{\min}(\Lambda) > d^2_{\min}(\Gamma/\Lambda) \\ E(\Lambda) + E(\Gamma/\Lambda), & \text{se } d^2_{\min}(\Lambda) = d^2_{\min}(\Gamma/\Lambda) \\ E(\Gamma/\Lambda), & \text{se } d^2_{\min}(\Lambda) < d^2_{\min}(\Gamma/\Lambda) \end{cases}.$$

Seja Λ um reticulado em $\mathbb{R}^N$. Então o conjunto $\Lambda^* = \{\mathbf{x} \in \mathbb{R}^N : (\mathbf{x}, \lambda) \in \mathbb{Z}, \forall \lambda \in \Lambda\}$ é um reticulado em $\mathbb{R}^N$ chamado *reticulado dual* de Λ. Se M é uma matriz geradora para Λ, então $M^* = (M^{-1})^t$ é uma matriz geradora para Λ^*, Quando $\Lambda \subseteq \Lambda^*$ dizemos que Λ é um *reticulado inteiro* e, neste caso, $\Lambda^* = \bigcup_{i=0}^{m-1}(\mathbf{g}_i + \Lambda)$, onde m é o índice de Λ em Λ^* e $g_i \in [\Lambda^*/\Lambda]$, $0 \leq i \leq m-1$. Em particular, quando $\Lambda = \Lambda^*$ dizemos que Λ é um *reticulado auto-dual.*

Seja Γ um empacotamento esférico em $\mathbb{R}^N$, a *região de Voronoi* $R_v(\lambda)$ associada a qualquer ponto $\lambda \in \Gamma$ é o conjunto de todos os pontos em $\mathbb{R}^N$ que estão mais próximos de λ do que qualquer outro ponto $\lambda' \in \Gamma$, isto é,

$$R_v(\lambda) = \left\{\mathbf{x} \in \mathbb{R}^N : \mathbf{N}(\mathbf{x}-\lambda) \leq \mathbf{N}(\mathbf{x}-\lambda'),\, \forall \lambda' \in \Gamma\right\}.$$

Um *buraco* de um empacotamento esférico Γ em $\mathbb{R}^N$ é um ponto de $\mathbb{R}^N - \Gamma$ cuja distância de Γ é um máximo local, isto é, um ponto $\mathbf{x}_0 \in R_v(\lambda)$ tal que $\mathbf{N}(\mathbf{x}-\lambda) \leq \mathbf{N}(\mathbf{x}_0-\lambda)$, para todo $\mathbf{x} \in V(\mathbf{x}_0) \cap R_v(\lambda)$, onde $V(\mathbf{x}_0)$ é uma vizinhança de $\mathbf{x}_0$. Um *buraco profundo* de um empacotamento esférico Γ em $\mathbb{R}^N$ é um ponto de $\mathbb{R}^N - \Gamma$ cuja distância de Γ é um máximo absoluto, isto é, um ponto $\mathbf{x}_0 \in R_v(\lambda)$ tal que $\mathbf{N}(\mathbf{x}-\lambda) \leq \mathbf{N}(\mathbf{x}_0-\lambda)$, para todo $\mathbf{x} \in R_v(\lambda)$.

A *densidade* $\Delta(\Gamma)$ do empacotamento esférico Γ em $\mathbb{R}^N$ é a relação entre o volume ocupado pelas esferas na região fundamental e o volume da região fundamental, isto é,

$$\Delta(\Gamma) = \limsup_{r\to\infty}\left\{\frac{V(D \bigcap E_r(\mathbf{0}))}{V(E_r(\mathbf{0}))}\right\},$$

onde

$$D = \{\mathbf{x} \in \mathbb{R}^N :\, \exists\, \lambda \in \Gamma,\, \mathbf{N}(\mathbf{x}-\lambda) < \frac{d^2_{\min}(\Gamma)}{4}\}.$$

Um empacotamento esférico Γ em $\mathbb{R}^N$ que é obtido localizando uma configuração fixa de s esferas em cada região fundamental de um reticulado Λ em $\mathbb{R}^N$ é chamado um *empacotamento periódico.*

Neste caso

$$\Delta(\Gamma) = \frac{sV(E_\rho(0))}{d(\Lambda)},$$

onde $\rho = \frac{d_{\min}(\Gamma)}{2}$.

A *densidade de centro* de um empacotamento esférico Γ em $\mathbb{R}^N$ é definida por,

$$\delta(\Gamma) \triangleq \frac{\Delta(\Gamma)}{V_N} \text{ e } \nu(\Gamma) = log_2(\delta(\Gamma)),$$

onde V_N é o volume de uma esfera de raio 1 em $\mathbb{R}^N$. Em particular, quando Γ é um reticulado temos que

$$\Delta(\Gamma) = \frac{V_N \rho^N}{d(\Gamma)}, \ \delta(\Gamma) = \frac{\rho^N}{d(\Gamma)} \text{ e } \gamma(\Gamma) = 4(\delta(\Gamma))^{\frac{2}{N}},$$

onde $\gamma(\Gamma)$ é o *parâmetro de Hermite* do reticulado Γ em $\mathbb{R}^N$. O *expoente de densidade* de um empacotamento esférico Γ em $\mathbb{R}^N$é definido por,

$$\lambda(\Gamma) \triangleq -log_2\left(\frac{\Delta(\Gamma)}{N}\right).$$

O cálculo do coeficiente de erro $E(\Gamma)$ de um empacotamento esférico Γ em $\mathbb{R}^N$ é facilitado quando definimos a *função* θ_Γ de Γ, (cf. [8]), por

$$\begin{aligned} \theta_\Gamma(z) &= \sum_{\lambda \in \Gamma} q^{\mathbf{N}(\lambda)} \\ &= \sum_{m=0}^{\infty} \mathbf{N}_m q^m, \end{aligned}$$

onde $q = e^{\pi i z}$, $z \in \{w \in \mathbb{C} : Im(w) > 0\}$ e $\mathbf{N}_m = \{\lambda \in \Gamma : \mathbf{N}(\lambda) = m\}$, ($\mathbb{C}$ é o conjunto dos números complexos e $Im(w)$ é a parte imaginária do número complexo w).

Se Γ é um empacotamento periódico em $\mathbb{R}^N$ tal que

$$\Gamma = \bigcup_{j=0}^{s-1} (\mathbf{g}_j + \Lambda),$$

onde Λ é um reticulado em $\mathbb{R}^N$, então

$$\begin{aligned} \theta_\Gamma(z) &= \frac{1}{s} \sum_{j=0}^{s-1} \sum_{k=0}^{s-1} \sum_{\lambda \in \Lambda} q^{\mathbf{N}(\lambda + \mathbf{g}_j - \mathbf{g}_k)} \\ &= \theta_\Lambda(z) + \frac{2}{s} \sum_{j<k} \sum_{\lambda \in \Lambda} q^{\mathbf{N}(\lambda + \mathbf{g}_j - \mathbf{g}_k)}. \end{aligned}$$

Em particular, se Γ for invariante por translação, então

$$\theta_\Gamma(z) = \sum_{j=0}^{s-1} \sum_{\lambda \in \Lambda} q^{\mathbf{N}(\lambda + \mathbf{g}_j - \mathbf{g}_0)}.$$

Note que, quando Γ é um reticulado em $\mathbb{R}^N$, o raio de empacotamento ρ, o coeficiente de erro $E(\Gamma)$ e a densidade $\Delta(\Gamma)$, (cf. [8]), são dados pela função θ_Γ, pois

$$\theta_\Gamma(z) = 1 + E(\Gamma)q^{4\rho^2} + \cdots \text{ e } \Delta(\Gamma) = \lim_{r\to\infty}\left(\frac{\rho}{r}\right)^N = \sum_{m\leq r^2} \mathbf{N}_m.$$

Exemplo 2.3.2 *Seja $\Lambda_0/\Lambda_1/\Lambda_2$ uma cadeia de partições, com 2-níveis e 3-maneiras, onde $\Lambda_0 = \mathbf{A}_2$ é o reticulado hexagonal em $\mathbb{R}^2$ com uma matriz geradora*

$$M_0 = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix},$$

e $\Lambda_i = T_3^i(\Lambda_0)$, $i = 1, 2$, os sub-reticulados de Λ_0 induzidos pelo endomorfismo T_3 definido pela matriz

$$[T_3] \triangleq \begin{bmatrix} \frac{3}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{3}{2} \end{bmatrix},$$

que escala Λ_0 por $\sqrt{3}$ e rotaciona por $30°$. Neste caso

$$[\Lambda_0/\Lambda_2] = \{\sum_{i=0}^{1} a_i\mathbf{g}_i : a_i \in \{0,1,2\},\ i = 0,1\},$$

é um sistema de representantes de classes laterais de Λ_2 em Λ_0, onde $\mathbf{g}_0 = (0,1)$ e $\mathbf{g}_1 = (\frac{3}{2}, -\frac{\sqrt{3}}{2})$. Também, $d^2_{\min}(\Lambda_i) = 3^i$ e $V(\Lambda_i) = 3^i\frac{\sqrt{3}}{2}$, $i = 0,1,2$. O raio de empacotamento $\rho = \frac{1}{2}$, o coeficiente de erro $E(\Lambda_0) = 6$ e o parâmetro de Hermite $\gamma(\Lambda_0) = 1.155$. As regiões fundamentais básicas P_0, P_1 e P_2 dos reticulados Λ_0, Λ_1 e Λ_2, respectivamente, são mostradas na Figura 2.2. ■

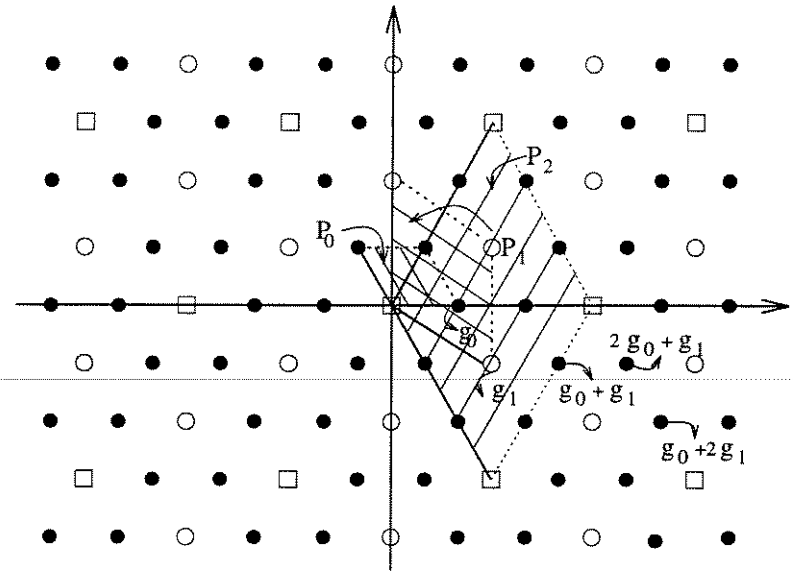


Figura 2.2: Os reticulados $\Lambda_0 \leftrightarrow \bullet$, $\Lambda_1 \leftrightarrow \circ$ e $\Lambda_2 \leftrightarrow \square$.

Capítulo 3

Constelação de Sinais Casada com Grupos Finitos

3.1 Introdução

Uma *constelação de sinais* S é qualquer subconjunto discreto em $\mathbb{R}^N$. Os elementos de uma constelação de sinais S são chamados *pontos de sinais*. Um *código do espaço Euclidiano* é um subconjunto de $S^{\mathbb{I}}$, onde $\mathbb{I} \subseteq \mathbb{Z}$.

Uma constelação de sinais S é *geometricamente uniforme*, (cf. [18]), se dados $\mathbf{s}_1, \mathbf{s}_2 \in S$ existe $\varphi \in Isom(\mathbb{R}^N)$ tal que

$$\varphi(\mathbf{s}_1) = \mathbf{s}_2 \quad \text{e} \quad \varphi(S) = S.$$

Se $\Gamma(S) = \{\varphi \in Isom(\mathbb{R}^N) : \varphi(S) = S\}$, então S é a órbita de qualquer ponto $\mathbf{s}_0 \in S$ sob $\Gamma(S)$, isto é,

$$S = \{\varphi(\mathbf{s}_0) : \varphi \in \Gamma(S)\} = \bigcup_{\varphi \in \Gamma(S)} \{\varphi(\mathbf{s}_0)\}.$$

Em geral, o grupo das simetrias $\Gamma(S)$ de uma constelação de sinais geometricamente uniforme é mais do que o necessário para gerar S. Assim, um *grupo gerador* $G(S)$ de S é um subgrupo de $\Gamma(S)$ que é minimamente suficiente para gerar S de qualquer ponto $\mathbf{s}_0 \in S$ ou, equivalentemente, a cardinalidade do conjunto $|\{\mathbf{s} \in S : \varphi(\mathbf{s}) = \mathbf{s}\}| = 0$, $\forall \varphi \in G(S)$, $\varphi \neq I_S$, onde I_S é o elemento identidade de $\Gamma(S)$. Note que o grupo gerador $G(S)$ de uma constelação de sinais geometricamente uniforme pode não existir (cf. [18]). Se $G(S)$ é o grupo gerador de uma constelação de sinais geometricamente uniforme

S e $\mathbf{s}_0 \in S$, então

$$S = \bigcup_{\varphi \in G(S)} \{\varphi(\mathbf{s}_0)\}$$

e o mapeamento $\mu : G(S) \longrightarrow S$ definido por $\mu(\varphi) = \varphi(\mathbf{s}_0)$ é bijetivo. O mapeamento μ induz uma estrutura de grupo em S, isto é, dados $\mathbf{s}_1, \mathbf{s}_2 \in S$, a operação $\mathbf{s}_1 * \mathbf{s}_2 = \mu(\mu^{-1}(\mathbf{s}_1)\mu^{-1}(\mathbf{s}_2))$ define uma estrutura de grupo em S e, neste caso, $(S, *)$ é isomorfo a $G(S)$. Assim, se o grupo S não é simples, então cada subgrupo normal S' de S induz em S uma fatoração de S' por S/S'. Isto sugere o estudo de uma constelação de sinais S através de constelações de sinais menores S' e S/S', que será feito na Seção 3.2.

Um *código de bloco de mesma energia* ou um *código esférico* S, (cf. [32]), é qualquer constelação finita de sinais sobre uma esfera que gera $\mathbb{R}^N$ como um espaço vetorial e denotamos por $\{N, M, d\}$, onde M é o número pontos de sinais ou palavras-código e d é a mínima distância Euclidiana quadrática de S. Em particular, quando um código esférico S é geometricamente uniforme dizemos que S é uma *constelação uniforme.* Constelações uniformes foram introduzidas por Slepian em [32] sob o nome de *códigos de grupo para o canal Gaussiano* e generalizada por Forney em [18] para uma constelação de sinais qualquer.

Para constelações de sinais geometricamente uniformes, existe um rotulamento isométrico entre um grupo e uma partição da constelação de sinais induzida pela partição do grupo gerador da constelação de sinais. Mais precisamente, seja H um subgrupo normal de $G(S)$. Então,

$$S_g = \bigcup_{\phi \in \varphi_g H} \{\phi(\mathbf{s}_0)\} = \bigcup_{\varphi \in H} \{\varphi_g(\varphi(\mathbf{s}_0))\},\ \varphi_g \in G(S)$$

é a órbita de $\mathbf{s}_0$ sob a classe lateral $\varphi_g H$. Assim,

$$S = \bigcup S_g.$$

Se S' é a órbita de $\mathbf{s}_0$ sob H, então a partição S/S' de S induzida por H é chamada uma *partição geometricamente uniforme.*

Teorema 3.1.1 [18] *Seja S/S' uma partição geometricamente uniforme. Então os subconjuntos de S nesta partição são geometricamente uniformes, mutuamente congruentes e têm H como um grupo gerador comum.* ■

Um *grupo de rótulos* G para uma partição geometricamente uniforme S/S' é um grupo isomorfo ao grupo quociente $G(S)/G(S')$. Um *rotulamento isométrico*, (cf. [18]), da partição geometricamente

uniforme S/S' é um mapeamento $\mu : G \longrightarrow S/S'$ definido por

$$\mu(g) = \varphi_g(S').$$

Em [25] Loeliger generaliza para um grupo finito, a idéia de rotulamento isométrico, definindo um mapeamento casado de um grupo sobre uma constelação de sinais e mostra que toda constelação de sinais casada com um grupo é, a menos de translação, uma constelação uniforme, [25, Corolário 1], e caracteriza todas as constelações de sinais casadas com um grupo comutativo cíclico, [25, Teorema 10]. Este resultado é generalizado por Palazzo *et al.* em [27] através de um algoritmo heurístico. Em todos estes casos, a motivação foi a introdução de alguma "*linearidade*" no estudo de códigos do espaço Euclidiano via um grupo. Na Seção 3.2 caracterizamos todas as constelações de sinais que são casadas com um grupo não comutativo resultante do produto semidireto de um grupo comutativo por um grupo cíclico de ordem par. Na Seção 3.3 apresentamos alguns resultados sobre a d-cadeia. Finalmente, na Seção 3.4 apresentamos um algoritmo para a obtenção de uma constelação de sinais casada com um grupo que é uma extensão de dois grupos menores.

3.2 Constelações de sinais casadas com grupos

Nesta seção caracterizamos todas as constelações de sinais que são casadas com um grupo não comutativo que é fatorável em um grupo comutativo por um grupo cíclico de ordem par.

Sejam U o grupo das raízes m-ésimas da unidade no conjunto dos números complexos $\mathbb{C}$ e G um grupo qualquer. Definimos

$$\widehat{G} \triangleq \{\chi : G \longrightarrow U : \chi \text{ é um homomorfismo}\}.$$

Definiremos uma operação binária, $(\chi, \psi) \longmapsto \chi\psi$, em $\widehat{G}$ como segue

$$\chi\psi(g) = \chi(g)\psi(g), \forall \chi, \psi \in \widehat{G} \text{ e } g \in G.$$

Não é difícil verificar que com esta operação $\widehat{G}$ é um grupo comutativo com elemento identidade $\chi(g) = 1$ e $\psi(g) = \chi(g^{-1})$ o elemento inverso de χ em $\widehat{G}$. O grupo $\widehat{G}$ é chamado *grupo dual* de G.

Sejam $G = \langle g \rangle$ um grupo cíclico de ordem m e $u \in U$ uma raiz m-ésima da unidade. Seja $\chi \in \widehat{G}$ tal que $\chi(g) = u$ e, portanto, $\chi(g^k) = u^k$. Uma vez que $\chi(g^k) = u^k$, temos que $I = \chi^m, \chi, \chi^2, \ldots, \chi^{m-1}$ são todos distintos. Logo, $\widehat{G} = \langle \chi \rangle$ e, neste caso, identificamos $\widehat{G}$ com a constelação de sinais $mPSK$.

Mais geralmente, seja G um grupo comutativo finito. Então todo elemento $g \in G$ pode ser escrito na forma, (cf. [12]),

$$g = \prod_{i=1}^{s} g_i^{k_i}, \text{ onde } g_i \in G.$$

Assim

$$\chi(g) = \prod_{i=1}^{s} \chi(g_i)^{k_i},$$

de modo que, cada $\chi \in \widehat{G}$ é completamente determinado por $\chi(g_1), \ldots, \chi(g_s)$. Portanto, se a ordem de g_j é igual a m_j, então $\chi(g_j)^{m_j} = 1$. Por outro lado, para $j = 1, \ldots, s$, seja $u_j \in U$, $u_j^{m_j} = 1$ e como

$$g = \prod_{i=1}^{s} g_i^{k_i},$$

obtemos que

$$\chi(g) = \prod_{i=1}^{s} u_i^{k_i}.$$

É claro que χ está bem definido, pois χ independe dos k_j, os quais são somente definidos módulo m_j e, assim, $\chi \in \widehat{G}$. Cada raiz pode ser escolhida de m_j-maneiras, de modo que existem $\prod_{j=1}^{s} m_j$ homomorfismos distintos χ. Logo, existe uma correspondência biunívoca entre os elementos de G e os elementos de $\widehat{G}$.

Lema 3.2.1 [12] *Se G é um grupo comutativo finito, então $G \simeq \widehat{G}$.* ■

Uma constelação de sinais S é *casada* com um grupo G, (cf. [25]), se existe um mapeamento μ de G sobre S tal que

$$d(\mu(g), \mu(h)) = d(\mu(e), \mu(g^{-1}h)),$$

para todo $g, h \in G$, onde $d(.,.)$ é a distância Euclidiana quadrática. O mapeamento μ é chamado de *mapeamento casado*. Quando o mapeamento μ é injetivo dizemos que μ é um *rotulamento casado*, isto é, se G é isomorfo a $G(S)$ então μ é um rotulamento isométrico. Salvo menção explicita em contrário, todos os mapeamentos casados deste trabalho são rotulamentos casados. Neste caso, se C é um código linear sobre G de comprimento n, isto é, C é um subgrupo de G^n, então $\underline{\mu}(C)$ é um código do espaço Euclidiano sobre S, (cf. Teorema 3.2.1 a seguir). Assim, as regiões de decisões de $\underline{\mu}(C)$ são todas congruentes.

Seja C um código linear sobre $\mathbb{Z}_m$ de comprimento n. Definimos, (cf. [25]),

$$\phi : C \longrightarrow \mathbb{R}^{2n}, \ \phi((c_1, \ldots, c_n)) \triangleq \sum_{j=1}^{n} A_j B_j,$$

onde

$$A_j = \left[r_j \cos(\frac{2\pi c_j}{m}),\ r_j sen(\frac{2\pi c_j}{m}) \right],\quad B_j = \begin{bmatrix} b_{2j-1} \\ b_{2j} \end{bmatrix}$$

e $\{b_1, b_2, \ldots, b_{2n}\}$ é uma base ortonormal fixada de $\mathbb{R}^{2n}$. Note que r_j é apenas um parâmetro de energia que só depende de j e não da palavra-código. Em geral, tomamos $r_j = 1$, para todo $j = 1, \ldots, n$. O mapeamento ϕ é chamado de *mapeamento canônico.*

Teorema 3.2.1 ([25]) *Sejam μ um rotulamento casado de G sobre S e C um código linear sobre G. Então $\underline{\mu}(C)$ é casada com C, onde $\underline{\mu}((c_1, \ldots, c_n)) \triangleq (\mu(c_1), \ldots, \mu(c_n))$.* ■

Teorema 3.2.2 ([25]) *Uma constelação de sinais S é casada com o grupo $\mathbb{Z}_m$ se, e somente se, $S = \phi(C) + \mathbf{x}$, onde ϕ é o mapeamento canônico, C é um subgrupo cíclico de $\mathbb{Z}_m^n$ e $\mathbf{x} \in \mathbb{R}^N$.* ■

No próximo teorema caracterizamos todas as constelações de sinais que são casadas com um grupo não comutativo, o qual é um produto semidireto de dois grupos cíclico.

Teorema 3.2.3 *Sejam $H = \langle h \rangle \simeq \mathbb{Z}_n$ e $K = \langle k \rangle \simeq \mathbb{Z}_{2m}$. Então, uma constelação de sinais S é casada com um grupo $G = H \times_\theta K$ se, e somente se, $S = S_1 \times_\varphi S_2$, para $\varphi(\mu_2(k)) = \mu_1\theta(k)\mu_1^{-1}$, onde $\mu_1 : H \longrightarrow S_1$, $\mu_2 : K \longrightarrow S_2$ são rotulamentos casados, $\theta(k) \in Aut(H)$, $\forall\, k \in K$ e $\theta(k)(h) = h^{-1}$, $\forall\, h \in H$.*

Prova. Suponhamos que S seja uma constelação de sinais casada com G. Seja μ o rotulamento casado de G sobre S. Então μ induz uma estrutura de grupo em S. Definindo

$$S_1 \triangleq \mu(H \times_\theta \{e\}) \quad \text{e} \quad S_2 \triangleq \mu(\{e\} \times_\theta K)$$

temos que S_1 e S_2 são subgrupos de S, com $S_1 \lhd S$. Agora, definimos $\mu_1 : H \longrightarrow S_1$ e $\mu_2 : K \longrightarrow S_2$ por

$$\mu_1(h) \triangleq \mu(h, e) \quad \text{e} \quad \mu_2(k) \triangleq \mu(e, k).$$

Então é claro que μ_1, μ_2 são isomorfismos e $S = S_1 \times_\varphi S_2$, onde $\varphi(\mu_2(k)) = \mu_1\theta(k)\mu_1^{-1}$, $\forall\, k \in K$. Além disso, dados $h_1, h_2 \in H$,

$$d(\mu_1(h_1), \mu_1(h_2)) = d(\mu_1(e), \mu_1(h_1^{-1}h_2)).$$

De modo análogo, mostra-se que μ_2 é um rotulamento casado.

Reciprocamente, sejam $\mu_1 : H \longrightarrow S_1$ e $\mu_2 : K \longrightarrow S_2$ rotulamentos casados. Então é claro que μ_1 e μ_2 induzem estruturas de grupos em S_1 e S_2, respectivamente. Assim, $S = S_1 \times_\varphi S_2$ é um grupo, onde $\varphi(s_2) \in Aut(S_1)$, $\forall\, s_2 \in S_2$, com $\varphi(s_2)(s_1) = s_1^{-1}$, $\forall\, s_1 \in S_1$. Uma vez que $\mu_1^{-1}\tau\mu_1 \in Aut(H)$, para todo $\tau \in Aut(S_1)$ segue-se que $G = H \times_\theta K$ é um grupo com $\theta(k) = \mu_1^{-1}\varphi(\mu_2(k))\mu_1$, $\forall\, k \in K$. Definimos $\mu : G \longrightarrow S$ por

$$\mu(h,k) \triangleq (\mu_1(h), \mu_2(k)).$$

Então é fácil verificar que μ é um isomorfismo de G sobre S. Além disso, dados $(h_1,k_1),(h_2,k_2) \in G$,

$$\begin{aligned} d(\mu(h_1,k_1),\mu(h_2,k_2)) &= d((\mu_1(h_1),\mu_2(k_1)),(\mu_1(h_2),\mu_2(k_2))) \\ &= d(\mu_1(h_1),\mu_1(h_2)) + d(\mu_2(k_1),\mu_2(k_2)) \\ &= d(\mu_1(e),\mu_1(h_1^{-1}h_2)) + d(\mu_2(e),\mu_2(k_1^{-1}k_2)), \end{aligned}$$

por outro lado,

$$\begin{aligned} d(\mu(e,e),\mu((h_1,k_1)^{-1}(h_2,k_2)) &= d((\mu_1(e),\mu_2(e)),(\mu_1(h_1),\mu_2(k_1))^{-1}(\mu_1(h_2),\mu_2(k_2))) \\ &= d((\mu_1(e),\mu_2(e)),(\varphi(\mu_2(k_1^{-1}))\mu_1(h_1^{-1}h_2),\mu_2(k_1^{-1}k_2))) \\ &= d((\mu_1(e),\mu_2(e)),(\mu_1(\theta(k_1^{-1}))(h_1^{-1}h_2),\mu_2(k_1^{-1}k_2))) \\ &= d(\mu_1(e),\mu_1(h_1h_2^{-1})) + d(\mu_2(e),\mu_2(k_1^{-1}k_2)). \end{aligned}$$

das expressões acima vemos que

$$d(\mu(h_1,k_1),\mu(h_2,k_2)) = d(\mu(e,e),\mu((h_1,k_1)^{-1}(h_2,k_2))),$$

pois $d(\mu_1(e),\mu_1(h_1^{-1}h_2)) = d(\mu_1(e),\mu_1(h_1h_2^{-1}))$. Portanto, μ é um rotulamento casado. ∎

Corolário 3.2.1 *Sejam H um grupo comutativo e $K = \langle k \rangle \simeq \mathbb{Z}_{2m}$. Então, uma constelação de sinais S é casada com um grupo $G = H \times_\theta K$ se, e somente se, $S = S_1 \times_\varphi S_2$, para $\varphi(\mu_2(k)) = \mu_1\theta(k)\mu_1^{-1}$, onde $\mu_1 : H \longrightarrow S_1$, $\mu_2 : K \longrightarrow S_2$ são rotulamentos casados, $\theta(k) \in Aut(H)$, $\forall\, k \in K$ e $\theta(k)(h) = h^{-1}$, $\forall\, h \in H$.* ∎

Exemplo 3.2.1 *Sejam $H = \mathbb{Z}_3 = \{0,1,2\}$, $K = \mathbb{Z}_2 = \{0,1\}$ e o homomorfismo $\theta : K \longrightarrow Aut(H)$ definido por $\theta(k) = \tau^k$, $k = 0,1$, onde $\tau(h) = -h$, $h = 0,1,2$. Então $G = H \times_\theta K$ é um grupo não comutativo de ordem 6 com a operação*

$$(h,k) +_\theta (h',k') = (h + \theta(k)(h'), k + k'),\ \forall h,h' \in H \ \text{ e } \ k,k' \in K.$$

$+_\theta$	0	1	2	3	4	5	G
0	0	1	2	3	4	5	$(0,0)$
1	1	2	0	4	5	3	$(1,0)$
2	2	0	1	5	3	4	$(2,0)$
3	3	5	4	0	2	1	$(0,1)$
4	4	3	5	1	0	2	$(1,1)$
5	5	4	3	2	1	0	$(2,1)$

Tabela 3.1: Tabela Cayley do grupo $\mathbb{Z}_3 \times_\theta \mathbb{Z}_2 \simeq D_3$.

Assim, G é isomorfo ao grupo diedral D_3. Seja $A = \{0,1,2,3,4,5\}$ um conjunto de rótulos para G. A tabela de Cayley de A é mostrada na Tabela 3.1. Portanto, pelo Teorema 3.2.3, a constelação de sinais

$$S = \left\{(1,0,1),(-\frac{1}{2},\frac{\sqrt{3}}{2},1),(-\frac{1}{2},-\frac{\sqrt{3}}{2},1),(1,0,-1),(-\frac{1}{2},\frac{\sqrt{3}}{2},-1),(-\frac{1}{2},-\frac{\sqrt{3}}{2},-1)\right\}$$

ou a constelação de sinais normalizada $\tilde{S} = \frac{1}{\sqrt{2}}S$ é casada com o grupo D_3. ■

Exemplo 3.2.2 *Sejam $H = \mathbb{Z}_4 = \{0,1,2,3\}$, $K = \mathbb{Z}_2 = \{0,1\}$ e o homomorfismo $\theta : K \longrightarrow Aut(H)$ definido por $\theta(k) = \tau^k$, $k = 0,1$, onde $\tau(h) = -h$, $h = 0,1,2,3$. Então $G = H \times_\theta K$ é um grupo não comutativo de ordem 8 com a operação*

$$(h,k) +_\theta (h',k') = (h + \theta(k)(h'), k + k'),\ \forall h, h' \in H \ \ e\ \ k, k' \in K.$$

Seja $A = \{0,1,2,3,4,5,6,7\}$ um conjunto de rótulos para G. A tabela de Cayley de A é mostrada na Tabela 3.2, da qual podemos concluir que $G = \langle 1,4 \rangle$ é isomorfo ao grupo diedral D_4. Portanto, pelo Teorema 3.2.3, a constelação de sinais

$$S = \{(1,0,1),(0,1,1),(-1,0,1),(0,-1,1),(1,0,-1),(0,1,-1),(-1,0,-1),(0,-1,-1)\}$$

ou a constelação de sinais normalizada $\tilde{S} = \frac{1}{\sqrt{2}}S$ é casada com o grupo D_4. ■

Exemplo 3.2.3 *Sejam $H = \mathbb{Z}_4 = \{0,1,2,3\}$, $K = \mathbb{Z}_4 = \{0,1,2,3\}$ e o homomorfismo $\theta : K \longrightarrow Aut(H)$ definido por $\theta(k) = \tau^k$, $k = 0,1,2,3$, onde $\tau(h) = -h$, $h = 0,1,2,3$. Então $G = H \times_\theta K$ é um grupo não comutativo de ordem 16 com a operação*

$$(h,k) +_\theta (h',k') = (h + \theta(k)(h'), k + k'),\ \forall h, h' \in H \ \ e\ \ k, k' \in K.$$

$+_\theta$	0	1	2	3	4	5	6	7	G
0	0	1	2	3	4	5	6	7	$(0,0)$
1	1	2	3	0	5	6	7	4	$(1,0)$
2	2	3	0	1	6	7	4	5	$(2,0)$
3	3	0	1	2	7	4	5	6	$(3,0)$
4	4	7	6	5	0	3	2	1	$(0,1)$
5	5	4	7	6	1	0	3	2	$(1,1)$
6	6	5	4	7	2	1	0	3	$(2,1)$
7	7	6	5	4	3	2	1	0	$(3,1)$

Tabela 3.2: Tabela Cayley do grupo $\mathbb{Z}_4 \times_\theta \mathbb{Z}_2 \simeq D_4$.

Seja $A = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$ *um conjunto de rótulos para* G. *A tabela de Cayley de* A *é mostrada na Tabela* 3.3. *Seja* $L = \langle 10 \rangle = \{0,10\}$ *um subgrupo normal de* G. *Então*

$$\overline{G} = G/L = \{L,\ 1 +_\theta L,\ 2 +_\theta L,\ 3 +_\theta L,\ 4 +_\theta L,\ 5 +_\theta L,\ 6 +_\theta L,\ 7 +_\theta L\}.$$

Identificando 2 *com* 8 *temos que* $L = \{0\}$ *e, assim, pelo item (2) do Exemplo 2.1.1*

$$\overline{G} = \{0,1,2,3,4,5,6,7\} \simeq Q_8.$$

Portanto, pelo Teorema 3.2.3, *a constelação de sinais*

$$S = \{(1,0,1,0),(0,1,1,0),(-1,0,1,0),(0,-1,1,0),(1,0,0,1),(0,1,0,1),(-1,0,0,1),(0,-1,0,1)\}$$

ou a constelação de sinais normalizada $\tilde{S} = \frac{1}{\sqrt{2}}S$ *é casada com o grupo* $\overline{G}$, *o qual é isomorfo ao grupo dos quatérnios* Q_8. ■

No próximo teorema caracterizamos todas as constelações de sinais que são casadas com um grupo comutativo da forma $G = \mathbb{Z}_n \times \mathbb{Z}_m$, onde m e n são número inteiros positivos quaisquer. De forma indutiva, temos a generalização para $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$.

Teorema 3.2.4 *Sejam* $H = \langle h \rangle \simeq \mathbb{Z}_n$ *e* $K = \langle k \rangle \simeq \mathbb{Z}_m$. *Então, uma constelação de sinais* S *é casada com um grupo* $G = H \times K$ *se, e somente se,* $S = S_1 \times S_2$, *onde* S_1 *e* S_2 *são constelações de sinais casadas com* H *e* K, *respectivamente.*

$+_\theta$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	G
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$(0,0)$
1	1	2	3	0	5	6	7	4	9	10	11	8	13	14	15	12	$(1,0)$
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13	$(2,0)$
3	3	0	1	2	7	4	5	6	11	8	9	10	15	12	13	14	$(3,0)$
4	4	7	6	5	8	11	10	9	12	15	14	13	0	3	2	1	$(0,1)$
5	5	4	7	6	9	8	11	10	13	12	15	14	1	0	3	2	$(1,1)$
6	6	5	4	7	10	9	8	11	14	13	12	15	2	1	0	3	$(2,1)$
7	7	6	5	4	11	10	9	8	15	14	13	12	3	2	1	0	$(3,1)$
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7	$(0,2)$
9	9	10	11	8	13	14	15	12	1	2	3	0	5	6	7	4	$(1,2)$
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5	$(2,2)$
11	11	8	9	10	15	12	13	14	3	0	1	2	7	4	5	6	$(3,2)$
12	12	15	14	13	0	3	2	1	4	7	6	5	8	11	10	9	$(0,3)$
13	13	12	15	14	1	0	3	2	5	4	7	6	9	8	11	10	$(1,3)$
14	14	13	12	15	2	1	0	3	6	5	4	7	10	9	8	11	$(2,3)$
15	15	14	13	12	3	2	1	0	7	6	5	4	11	10	9	8	$(3,3)$

Tabela 3.3: Tabela de Cayley do grupo $\mathbb{Z}_4 \times_\theta \mathbb{Z}_4$.

Prova. Suponhamos que S seja uma constelação de sinais casada com G. Seja μ o rotulamento casado de G sobre S. Então μ induz uma estrutura de grupo em S. Definindo

$$S_1 \triangleq \mu(H \times \{e\}) \quad \text{e} \quad S_2 \triangleq \mu(\{e\} \times K)$$

temos que S_1 e S_2 são subgrupos de S. Agora, definimos $\mu_1 : H \longrightarrow S_1$ e $\mu_2 : K \longrightarrow S_2$ por

$$\mu_1(h) \triangleq \mu(h, e), \quad \text{e} \quad \mu_2(k) \triangleq \mu(e, k).$$

Então é claro que μ_1, μ_2 são isomorfismos e $S = S_1 \times S_2$. Além disso, dados $h_1, h_2 \in H$,

$$d(\mu_1(h_1), \mu_1(h_2)) = d(\mu_1(e), \mu_1(h_1^{-1}h_2)).$$

De modo análogo, mostra-se que μ_2 é um rotulamento casado.

Reciprocamente, sejam $\mu_1 : H \longrightarrow S_1$ e $\mu_2 : K \longrightarrow S_2$ rotulamentos casados. Então é claro que μ_1 e μ_2 induzem estruturas de grupos em S_1 e S_2, respectivamente. Assim, $S = S_1 \times S_2$ é um grupo. Definimos $\mu : G \longrightarrow S$ por

$$\mu(h, k) \triangleq (\mu_1(h), \mu_2(k)).$$

Então é fácil verificar que μ é um isomorfismo de G sobre S. Além disso, dados $(h_1, k_1), (h_2, k_2) \in G$,

$$\begin{aligned}
d(\mu(h_1, k_1), \mu(h_2, k_2)) &= d((\mu_1(h_1), \mu_2(k_1)), (\mu_1(h_2), \mu_2(k_2))) \\
&= d(\mu_1(h_1), \mu_1(h_2)) + d(\mu_2(k_1), \mu_2(k_2)) \\
&= d(\mu_1(e), \mu_1(h_1^{-1}h_2)) + d(\mu_2(e), \mu_2(k_1^{-1}k_2)) \\
&= d((\mu_1(e), \mu_2(e)), (\mu_1(h_1^{-1}h_2), \mu_2(k_1^{-1}k_2))) \\
&= d(\mu(e, e), \mu(h_1^{-1}h_2, k_1^{-1}k_2)) \\
&= d(\mu(e, e), \mu((h_1, k_1)^{-1}(h_2, k_2))).
\end{aligned}$$

Portanto, μ é um rotulamento casado. ■

Exemplo 3.2.4 *Sejam $H = \mathbb{Z}_3 = \{0, 1, 2\}$ e $K = \mathbb{Z}_2 = \{0, 1\}$. Então $G = H \times K$ é um grupo comutativo de ordem 6 com a operação*

$$(h, k) + (h', k') = (h + h', k + k'), \forall h, h' \in H \text{ e } k, k' \in K.$$

Assim, G é isomorfo ao grupo $\mathbb{Z}_6$. Seja $A = \{0, 1, 2, 3, 4, 5\}$ um conjunto de rótulos para G. A tabela de Cayley de A é mostrada na Tabela 3.4. *Portanto, pelo Teorema* 3.2.4, *a constelação de sinais*

$$S = \left\{(1, 0, 1), (-\frac{1}{2}, \frac{\sqrt{3}}{2}, -1), (-\frac{1}{2}, -\frac{\sqrt{3}}{2}, 1), (1, 0, -1), (-\frac{1}{2}, \frac{\sqrt{3}}{2}, 1), (-\frac{1}{2}, -\frac{\sqrt{3}}{2}, -1)\right\}$$

ou a constelação de sinais normalizada $\tilde{S}_1 = \frac{1}{\sqrt{2}}S$ é casada com o grupo $\mathbb{Z}_6$. ■

$+$	0	1	2	3	4	5	G
0	0	1	2	3	4	5	$(0,0)$
1	1	2	3	4	5	0	$(1,1)$
2	2	3	4	5	0	1	$(2,0)$
3	3	4	5	0	1	2	$(0,1)$
4	4	5	0	1	2	3	$(1,0)$
5	5	0	1	2	3	4	$(2,1)$

Tabela 3.4: Tabela de Cayley do grupo $\mathbb{Z}_3 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6$.

$+$	0	1	2	3	4	5	6	7	G
0	0	1	2	3	4	5	6	7	$(0,0)$
1	1	2	3	0	5	6	7	4	$(1,0)$
2	2	3	0	1	6	7	4	5	$(2,0)$
3	3	0	1	2	7	4	5	6	$(3,0)$
4	4	5	6	7	0	1	2	3	$(0,1)$
5	5	6	7	4	1	2	3	0	$(1,1)$
6	6	7	4	5	2	3	0	1	$(2,1)$
7	7	4	5	6	3	0	1	2	$(3,1)$

Tabela 3.5: Tabela Cayley do grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Exemplo 3.2.5 *Sejam* $H = \mathbb{Z}_4 = \{0,1,2,3\}$ *e* $K = \mathbb{Z}_2 = \{0,1\}$. *Então* $G = H \times K$ *é um grupo comutativo de ordem* 8 *com a operação*

$$(h,k) + (h',k') = (h+h', k+k'),\ \forall h,h' \in H \ \text{ e } \ k,k' \in K.$$

Seja $A = \{0,1,2,3,4,5,6,7\}$ *um conjunto de rótulos para* G. *A tabela de Cayley de* A *é mostrada na Tabela* 3.5. *Portanto, pelo Teorema* 3.2.4, *a constelação de sinais*

$$S = \{(1,0,1),(0,1,1),(-1,0,1),(0,-1,1),(1,0,-1),(0,1,-1),(-1,0,-1),(0,-1,-1)\}$$

ou a constelação de sinais normalizada $\tilde{S} = \frac{1}{\sqrt{2}}S$ *é casada com o grupo* $\mathbb{Z}_4 \times \mathbb{Z}_2$. ■

Mais exemplos de constelações de sinais casadas com grupos comutativos bem como particionamentos de tais constelações de sinais podem ser encontrados em Câmara [5].

Note que, pelos Teoremas 3.2.3 e 3.3.4, podemos conjecturar que as constelações de sinais casadas com o grupo diedral D_n são similares as constelações de sinais casadas com o grupo comutativo $\mathbb{Z}_n \times \mathbb{Z}_2$.

3.3 d-Cadeia

Nesta seção apresentamos uma construção de constelações de sinais a partir de um grupo qualquer via o conceito da d-cadeia baseado na construção proposta em [27].

Sejam $S = \{\mathbf{x}_{g_i} : 0 \leq i \leq N-1\} \subset \mathbb{R}^N$, onde $\mathbf{x} = (x_0, \ldots, x_{N-1}) \in \mathbb{R}^N$,

$$\mathbf{x}_{g_i} = (x_{\sigma_{g_i}(0)}, \ldots, x_{\sigma_{g_i}(N-1)})$$

com $g_i \in G, g_0 = e$ e $\sigma_{g_i} \in S_G$, $0 \leq i \leq N-1$. Suponhamos que todos os vetores distantes d de $\mathbf{x} = \mathbf{x}_{g_0}$ são $\mathbf{x}_{g_1}, \ldots, \mathbf{x}_{g_r}$. Vamos construir uma tabela dos elementos do grupo associados com os vetores $\mathbf{x}_{g_i}, 0 \leq i \leq r$, da seguinte forma: a primeira linha da tabela será $g_0, \ldots, g_r$. O primeiro elemento a ser localizado na primeira coluna da tabela na (k+1)-ésima linha será o primeiro elemento na k-ésima linha que ainda não apareceu na primeira coluna da tabela. Seja g o primeiro elemento na k-ésima linha que ainda não apareceu na primeira coluna da tabela. Então a (k+1)-ésima linha será $g, gg_1, \ldots, gg_r$. Portanto, temos a seguinte tabela

	g_0	g_1	$\cdots$	g_r
g_0	g_0	g_1	$\cdots$	g_r
g_1	g_1	g_1^2	$\cdots$	$g_1 g_r$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g	g	gg_1	$\cdots$	gg_r
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$

Quando a j-ésima linha tiver sido escrita e todo elemento nessa j-ésima linha tenha aparecido uma vez na primeira coluna da tabela, o processo é interrompido e a tabela é considerada completa. Note que a tabela tem no máximo $|G|$ linhas. Agora, de $d(\mathbf{x}_{g_i}, \mathbf{x}) = d(\mathbf{x}_{g_j g_i}, \mathbf{x}_{g_j})$, $0 \leq i, j \leq N-1$, segue-se que os vetores representados pelos elementos do grupo na $2^{\underline{a}}, \ldots$, r-ésima coluna na k-ésima linha estão distantes d do vetor representado pelo elemento do grupo na primeira coluna dessa linha. Assim, os elementos do grupo na primeira coluna da tabela representam vetores com a propriedade de que todo

vetor subsequente está à distância d do vetor anterior e também do próximo. O conjunto de vetores que podem ser alcançados de $\mathbf{x}$ dessa maneira é chamado de *d-cadeia iniciando de* $\mathbf{x}$. Note que o vetor $\mathbf{x}$ está incluído nessa d-cadeia e todas as d-cadeias iniciando de $\mathbf{x}$ são obtidas da tabela. Logo, temos o seguinte resultado.

Teorema 3.3.1 ([32]) *Seja* $\mathbf{x}, \mathbf{x}_{g_1}, \ldots, \mathbf{x}_{g_k}$ *uma d-cadeia iniciando de* $\mathbf{x}$. *Então,*

(1) $H = \{g_0, g_1, \ldots, g_k\}$ *é um subgrupo de* G *gerado pelos elementos do grupo diferentes de* g_0 *na primeira linha da tabela.*

(2) *Se* $H \neq G$, *então para todo* $g \in G - H$ *existe uma nova d -cadeia iniciando de* $\mathbf{x}_g$ *e os elementos do grupo dessa nova d-cadeia formam as classes laterais à esquerda* gH *de* H *em* G. ■

Sejam S uma constelação de sinais e $P(S)$ uma partição de S. Dizemos que S é *casada* com o grupo G se existe um mapeamento μ de G sobre $P(S)$ tal que

$$d(\mu(g), \mu(h)) = d(\mu(e), \mu(g^{-1}h)),$$

para todos $g, h \in G$, onde $d(.,.)$ é a distância Euclidiana quadrática interclasses laterais.

Teorema 3.3.2 *Seja* G *um grupo e seja* H *um subgrupo de* G *como no Teorema* 3.3.1. *Se* $S = \bigcup_{g \in G} S_g$, *onde* S_g *são constelações de sinais associadas às classes laterais de* H *em* G, *então* S *é casada com* G.

Prova. Por construção cada S_g tem a mesma distância Euclidiana quadrática intraclasses laterais e, assim, cada S_g tem a mesma lista ordenada de distâncias Euclidianas interclasses laterais, pois todas as constelações S_g são formadas de d-cadeias fechadas. Portanto, $\mu : G \longrightarrow P(S)$, dada por $\mu(g) = S_g$, é um mapeamento casado. ■

Pelo Teorema 3.3.2, observamos que a constelação de sinais S casada com o grupo G tem a seguinte propriedade: o perfil de distância de qualquer ponto de sinal independe do ponto de sinal. Portanto, G tem uma medida de distância invariante por translação. Assim, um código linear C projetado sobre este grupo tem a propriedade de distância independente da palavra-código e também, para um canal Gaussiano, a probabilidade de erro independente da palavra-código.

Lema 3.3.1 *Seja* G *um grupo que é uma extensão de* H *por* K. *Então,*

(1) *Se S é uma constelação de sinais casada com H, então S é casada com G.*

(2) *Se S é uma constelação de sinais casada com K, então S é casada com G.*

Prova. (2) Seja $\underline{\mu} : G \longrightarrow S$ definida por $\underline{\mu}(g) = \mu(aH)$, se $g \in aH$, para todo $g \in G$, onde μ é o rotulamento casado de $K \simeq G/H$ sobre S. É claro que $\underline{\mu}$ está bem definida e é sobrejetiva. Dados $g_1, g_2 \in G$, existem únicos $a_1, a_2 \in [G/H]$ e $h_1, h_2 \in H$ tais que $g_1 = a_1h_1$ e $g_2 = a_2h_2$. Como $g_1^{-1}g_2 = h_1^{-1}a_1^{-1}a_2h_2$ e

$$h_1^{-1}a_1^{-1}a_2h_2 = a_1^{-1}(a_1h_1^{-1}a_1^{-1})a_2h_2 = a_1^{-1}h_3a_2h_2,\ h_3 = a_1h_1^{-1}a_1^{-1} \in H,$$
$$h_3a_2h_2 = a_2(a_2^{-1}h_3a_2h_2) = a_2h_4,\ h_4 = a_2^{-1}h_3a_2h_2 \in H$$

temos que $g_1^{-1}g_2 = a_1^{-1}a_2h_4$, isto é, $g_1^{-1}g_2 \in a_1^{-1}a_2H$. Portanto

$$d(\underline{\mu}(g_1), \underline{\mu}(g_2)) = d(\mu(a_1H), \mu(a_2H)) =$$
$$d(\mu(H), \mu(a_1^{-1}a_2H)) = d(\underline{\mu}(e), \underline{\mu}(g_1^{-1}g_2)).$$

Logo, $\underline{\mu}$ é um mapeamento casado. ■

Note que o mapeamento casado $\underline{\mu}$ do Lema 3.3.1 não é um rotulamento casado, pois $\underline{\mu}$ não é injetivo.

3.4 Construindo constelações de sinais casadas com grupos

Em geral, o Teorema 3.3.2, não diz explicitamente nada sobre a natureza geométrica da constelação de sinais. De fato, ele diz que uma constelação de sinais deve ser encontrada como uma união de constelações de sinais. Assim, a chave para transformar o Teorema 3.3.2 em um algoritmo construtivo é proporcionado pela definição da d-cadeia, Teorema 3.3.1 e do Lema 3.3.1.

Algoritmo A: Dado um grupo finito G.

Passo 1. Associe a G um conjunto qualquer de rótulos A.

Passo 2. Construa a tabela de Cayley para A.

Passo 3. Para cada linha da tabela de Cayley do Passo 2 associe uma permutação σ_i, $i \in A$.

Passo 4. Dado $\mathbf{x} = \mathbf{x}_0 = (x_0, \ldots, x_{|A|-1}) \in \mathbb{R}^{|A|}$ encontre $\mathbf{x}_i = (x_{\sigma_i(0)}, \ldots, x_{\sigma_i(|A|-1)})$, $1 \leq i \leq |A| - 1$.

Passo 5. Selecione em cada conjunto A_j os elementos do grupo associados aos vetores $\mathbf{x}_j$ que estão a mesma distância Euclidiana quadrática d_j de $\mathbf{x}_0$.

Passo 6. Para cada conjunto A_j do Passo 5 associe uma d_j-cadeia.

Passo 7. Associe a cada d_j-cadeia do Passo 6 um subgrupo H_j de G.

Passo 8. Faça $S_j = \bigcup_{i \in \mathbb{I}} S_{ji}$, onde S_{ji} são as constelações de sinais casadas com as classes laterais de H_j em G.

Exemplo 3.4.1 *Encontre as constelações de sinais casada com o grupo* $\mathbb{Z}_6$.

Passo 1. *Seja* $A = \{0,1,2,3,4,5\}$ *um conjunto de rótulos para* $\mathbb{Z}_6$.

Passo 2. *Ver Tabela* 3.1.

Passo 3. *Sejam*

$$\sigma_0 = (0),\ \sigma_1 = (012345),\ \sigma_2 = (024)(135),$$
$$\sigma_3 = (03)(14)(25),\ \sigma_4 = (042)(153)\ \ e\ \ \sigma_5 = (054321)$$

as permutações associadas ao Passo 2.

Passo 4. *Dado* $\mathbf{x}_0 = (x_0, x_1, x_2, x_3, x_4, x_5) \in \mathbb{R}^6$. *Então*

$$\mathbf{x}_1 = (x_1, x_2, x_3, x_4, x_5, x_0),$$
$$\mathbf{x}_2 = (x_2, x_3, x_4, x_5, x_0, x_1),$$
$$\mathbf{x}_3 = (x_3, x_4, x_5, x_0, x_1, x_2),$$
$$\mathbf{x}_4 = (x_4, x_5, x_0, x_1, x_2, x_3),$$
$$\mathbf{x}_5 = (x_5, x_0, x_1, x_2, x_3, x_4).$$

Passo 5. *Sejam* $A_1 = \{1,5\}$, $A_2 = \{2,4\}$ *e* $A_3 = \{3\}$ *os conjuntos com distâncias Euclidianas quadráticas* d_1, d_2 *e* d_3, *respectivamente.*

Passo 6.

	0	1	5
0	0	1	5
1	1	2	0
2	2	3	1
3	3	4	2
4	4	5	3
5	5	0	4

	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

	0	3
0	0	3
3	3	0

Passo 7. *Sejam* $H_1 = \mathbb{Z}_6$, $H_2 = \{0,2,4\}$ *e* $H_3 = \{0,3\}$ *os subgrupos de* $\mathbb{Z}_6$ *associados as* d_j*-cadeias* $j = 1,2,3$ *do Passo* 6.

Passo 8. *Sejam* $S_1 = S_{11}$, *onde* $S_{11} = \{0,1,2,3,4,5\}$, $S_2 = S_{21} \cup S_{22}$, *onde* $S_{21} = \{0,2,4\}$ *e* $S_{22} = \{1,3,5\}$, *e* $S_3 = S_{31} \cup S_{32} \cup S_{33}$, *onde* $S_{31} = \{0,3\}$, $S_{32} = \{1,4\}$ *e* $S_{33} = \{2,5\}$.
Os gráficos associados a S_1, S_2 *e* S_3 *são o hexágono da Figura* 3.1, *o antiprisma da Figura* 3.2 *e o prisma da Figura* 3.3, *respectivamente. Pelo Lema 3.3.1 as constelações de sinais* $2PSK$ *e* $3PSK$ *são também casadas com o grupo* $\mathbb{Z}_6$.

Exemplo 3.4.2 *Encontre as constelações de sinais casada com o grupo* $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Passo 1. *Seja* $A = \{0,1,2,3,4,5,6,7\}$ *um conjunto de rótulos para* $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Passo 2. *Ver Tabela* 3.2.

Passo 3. *Sejam*

$$\sigma_0 = (0),\ \sigma_1 = (0123)(4567),\ \sigma_2 = (02)(13)(46)(57),$$
$$\sigma_3 = (0321)(4765),\ \sigma_4 = (04)(15)(26)(37),\ \sigma_5 = (0527)(1634)$$
$$\sigma_6 = (06)(17)(24)(35)\ e\ \sigma_7 = (0725)(1436)$$

as permutações associadas ao Passo 2.

Passo 4. *Dado* $\mathbf{x}_0 = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{R}^8$. *Então*

$$\mathbf{x}_1 = (x_1, x_2, x_3, x_0, x_5, x_6, x_7, x_4),$$
$$\mathbf{x}_2 = (x_2, x_3, x_0, x_1, x_6, x_7, x_4, x_5),$$
$$\mathbf{x}_3 = (x_3, x_0, x_1, x_2, x_7, x_4, x_5, x_6),$$
$$\mathbf{x}_4 = (x_4, x_5, x_6, x_7, x_0, x_1, x_2, x_3),$$
$$\mathbf{x}_5 = (x_5, x_6, x_7, x_4, x_1, x_2, x_3, x_0),$$
$$\mathbf{x}_6 = (x_6, x_7, x_4, x_5, x_2, x_3, x_0, x_1),$$
$$\mathbf{x}_7 = (x_7, x_4, x_5, x_6, x_3, x_0, x_1, x_2).$$

Passo 5. *Sejam* $A_1 = \{1,3\}, A_2 = \{2\}, A_3 = \{4\}, A_4 = \{5,7\}$ *e* $A_5 = \{6\}$ *os conjuntos com distâncias Euclidianas quadráticas* d_1, d_2, d_3, d_4 *e* d_5, *respectivamente.*

Passo 6.

	0	1	3
0	0	1	3
1	1	2	0
2	2	3	1
3	3	0	2

	0	2
0	0	2
2	2	0

	0	4
0	0	4
4	4	0

	0	5	7
0	0	5	7
5	5	2	0
2	2	7	5
7	7	0	2

	0	6
0	0	6
6	6	0

Passo 7. *Sejam* $H_1 = \{0,1,2,3\}$, $H_2 = \{0,2\}$, $H_3 = \{0,4\}$, $H_4 = \{0,2,5,7\}$ *e* $H_5 = \{0,6\}$ *os subgrupos de* $\mathbb{Z}_4 \times \mathbb{Z}_2$ *associados as* d_j*-cadeias* $j = 1,2,3,4,5$ *do Passo* 6.

Passo 8. *Sejam* $S_1 = S_{11} \cup S_{12}$, *onde* $S_{11} = \{0,1,2,3\}$, $S_{11} = \{4,5,6,7\ \}$, $S_3 = S_{31} \cup S_{32} \cup S_{33} \cup S_{34}$, *onde* $S_{31} = \{0,4\}$, $S_{32} = \{1,5\}$, $S_{33} = \{2,6\}$ *e* $S_{34} = \{3,7\}$. *As outras constelações de sinais são, a menos de permutações de rótulos, similares a estas.*

Os gráficos associados a S_1 *e* S_3 *são o antiprisma da Figura* 3.4 *e o prisma da Figura* 3.5, *respectivamente. Pelo Lema 3.3.1 as constelações de sinais* $2PSK$ *e* $4PSK$ *são também casadas com o grupo* $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Exemplo 3.4.3 *Encontre as constelações de sinais casada com o grupo diedral* D_3.

Passo 1. *Seja* $A = \{0,1,2,3,4,5\}$ *um conjunto de rótulos para* D_3.

Passo 2. *Ver Tabela* 3.3.

Passo 3. *Sejam*

$$\sigma_0 = (0),\ \sigma_1 = (012)(345),\ \sigma_2 = (021)(354),$$
$$\sigma_3 = (03)(15)(24),\ \sigma_4 = (04)(13)(25)\ \ e\ \ \sigma_5 = (05)(14)(23)$$

as permutações associadas ao Passo 2.

Passo 4. *Dado* $\mathbf{x}_0 = (x_0, x_1, x_2, x_3, x_4, x_5) \in \mathbb{R}^6$. *Então*

$$\mathbf{x}_1 = (x_1, x_2, x_0, x_4, x_5, x_3),$$
$$\mathbf{x}_2 = (x_2, x_0, x_1, x_5, x_3, x_4),$$
$$\mathbf{x}_3 = (x_3, x_5, x_4, x_0, x_2, x_1),$$
$$\mathbf{x}_4 = (x_4, x_3, x_5, x_1, x_0, x_2),$$
$$\mathbf{x}_5 = (x_5, x_4, x_3, x_2, x_1, x_0).$$

Passo 5. *Sejam* $A_1 = \{1,2\}$, $A_2 = \{3\}$, $A_3 = \{4\}$ *e* $A_4 = \{5\}$ *os conjuntos com distâncias Euclidianas quadráticas* d_1, d_2, d_3 *e* d_4, *respectivamente.*

Passo 6.

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

	0	3
0	0	3
3	3	0

	0	4
0	0	4
4	4	0

	0	5
0	0	5
5	5	0

Passo 7. *Sejam* $H_1 = \{0,1,2\}$, $H_2 = \{0,3\}$, $H_3 = \{0,4\}$ *e* $H_4 = \{0,5\}$ *os subgrupos de* D_3 *associados as* d_j*-cadeias* $j = 1,2,3,4$ *do Passo* 6.

Passo 8. *Sejam* $S_1 = S_{11} \cup S_{12}$, *onde* $S_{11} = \{0,1,2\}$ *e* $S_{12} = \{3,5,4\}$, $S_2 = S_{21} \cup S_{22} \cup S_{23}$, *onde* $S_{21} = \{0,3\}$, $S_{22} = \{1,4\}$ *e* $S_{23} = \{2,5\}$. *As outras constelações de sinais são, a menos de permutações dos rótulos, similares a estas.*

Os gráficos associados a S_1 *e* S_2 *são o prisma da Figura* 3.7 *e o antiprisma da Figura* 3.6, *respectivamente. Pelo Lema 3.3.1 as constelações de sinais* $2PSK$ *e* $3PSK$ *são também casadas com o grupo* D_3.

Exemplo 3.4.4 *Encontre as constelações de sinais casada com o grupo diedral* D_4.

Passo 1. *Seja* $A = \{0,1,2,3,4,5,6,7\}$ *um conjunto de rótulos para* D_4.

Passo 2. *Ver Tabela* 3.4.

Passo 3. *Sejam*

$$\sigma_0 = (0),\ \sigma_1 = (0123)(4567),\ \sigma_2 = (02)(13)(46)(57),$$
$$\sigma_3 = (0321)(4765),\ \sigma_4 = (04)(17)(26)(35),\ \sigma_5 = (05)(14)(27)(36)$$
$$\sigma_6 = (06)(15)(24)(37) \text{ e } \sigma_7 = (07)(16)(25)(34)$$

as permutações associadas ao Passo 2.

Passo 4. *Dado* $\mathbf{x}_0 = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{R}^8$. *Então*

$$\mathbf{x}_1 = (x_1, x_2, x_3, x_0, x_5, x_6, x_7, x_4),$$
$$\mathbf{x}_2 = (x_2, x_3, x_0, x_1, x_6, x_7, x_4, x_5),$$
$$\mathbf{x}_3 = (x_3, x_0, x_1, x_2, x_7, x_4, x_5, x_6),$$
$$\mathbf{x}_4 = (x_4, x_7, x_6, x_5, x_0, x_3, x_2, x_1),$$
$$\mathbf{x}_5 = (x_5, x_4, x_7, x_6, x_1, x_0, x_3, x_2),$$
$$\mathbf{x}_6 = (x_6, x_5, x_4, x_7, x_2, x_1, x_0, x_3),$$
$$\mathbf{x}_7 = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0).$$

Passo 5. *Sejam* $A_1 = \{1,3\}$, $A_2 = \{2\}$, $A_3 = \{4\}$, $A_4 = \{5\}$, $A_5 = \{6\}$ *e* $A_6 = \{7\}$ *os conjuntos com distâncias Euclidianas quadráticas* d_1, d_2, d_3, d_4, d_5 *e* d_6, *respectivamente.*

Passo 6.

	0	1	3
0	0	1	3
1	1	2	0
2	2	3	1
3	3	0	2

	0	2
0	0	2
2	2	0

	0	4
0	0	4
4	4	0

	0	5
0	0	5
5	5	0

	0	6
0	0	6
6	6	0

	0	7
0	0	7
7	7	0

Passo 7. *Sejam* $H_1 = \{0,1,2,3\}$, $H_2 = \{0,2\}$, $H_3 = \{0,4\}$, $H_4 = \{0,5\}$, $H_5 = \{0,6\}$ *e* $H_6 = \{0,7\}$ *os subgrupos de* D_4 *associados as* d_j*-cadeias* $j = 1,2,3,4,5,6$ *do Passo* 6.

Passo 8. *Sejam* $S_1 = S_{11} \cup S_{12}$, *onde* $S_{11} = \{0,1,2,3\}$, $S_{11} = \{4,7,6,5\}$, $S_3 = S_{31} \cup S_{32} \cup S_{33} \cup S_{34}$, *onde* $S_{31} = \{0,4\}$, $S_{32} = \{1,5\}$, $S_{33} = \{2,6\}$ *e* $S_{34} = \{3,7\}$. *As outras constelações são, a menos de permutações de rótulos, similares a estas.*

Os gráficos associados a S_1 *e* S_3 *são o antiprisma da Figura* 3.8 *e o prisma da Figura* 3.9, *respectivamente. Pelo Lema 3.3.1 as constelações de sinais* $2PSK$ *e* $4PSK$ *são também casadas com o grupo* D_4.

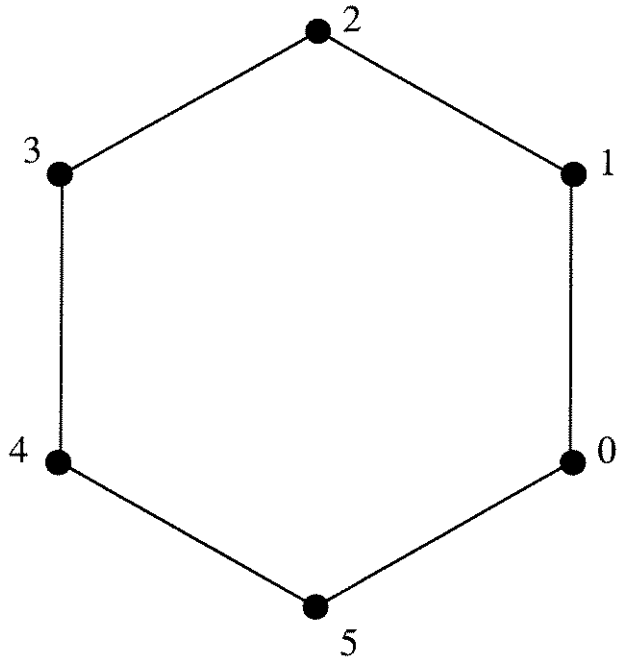


Figura 3.1: Hexágono casado com $\mathbb{Z}_6$.

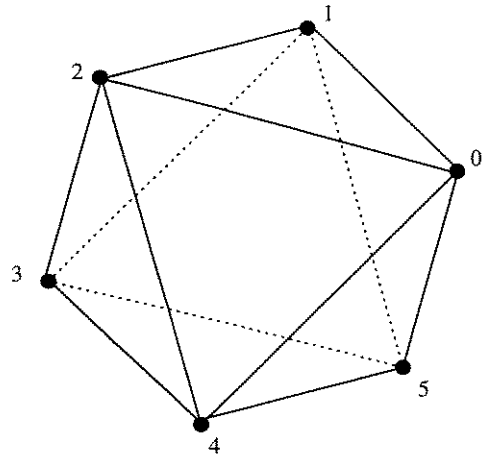


Figura 3.2: Antiprisma casado com $\mathbb{Z}_6$.

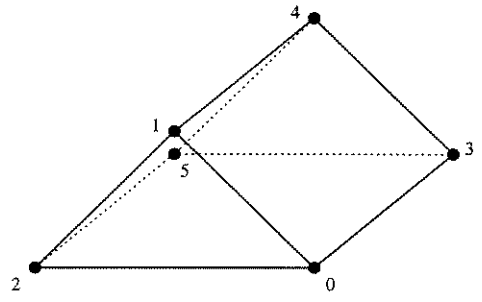


Figura 3.3: Prisma casado com $\mathbb{Z}_6$.

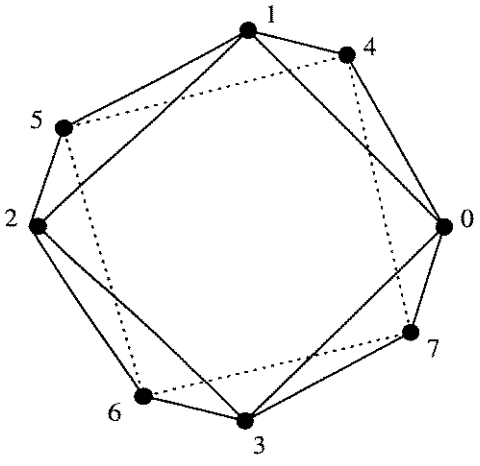


Figura 3.4: Antiprisma casado com $\mathbb{Z}_4 \times \mathbb{Z}_2$.

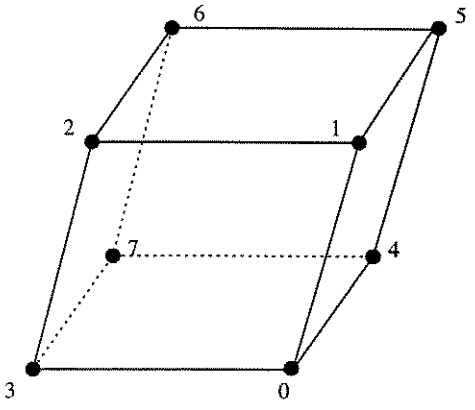


Figura 3.5: Prisma casado com $\mathbb{Z}_4 \times \mathbb{Z}_2$.

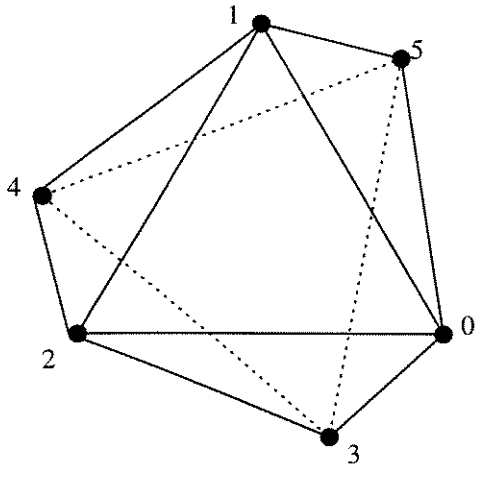


Figura 3.6: Antiprisma casado com D_3.

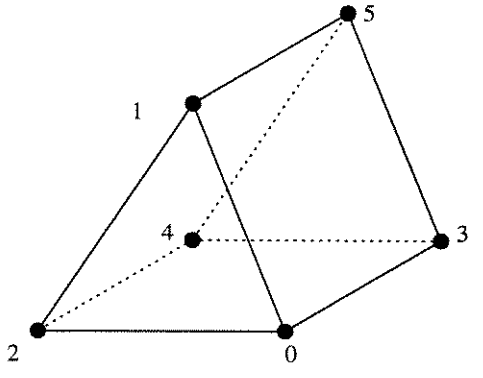


Figura 3.7: Prisma casado com D_3.

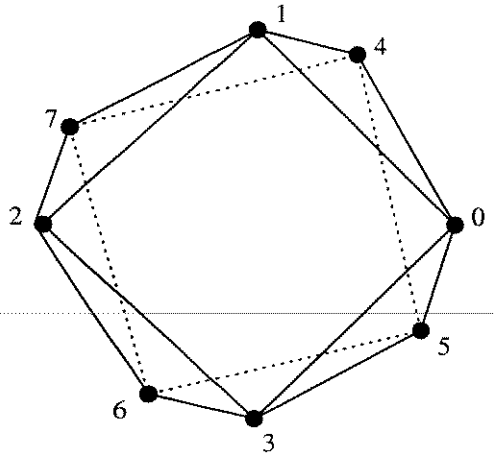


Figura 3.8: Antiprisma casado com D_4.

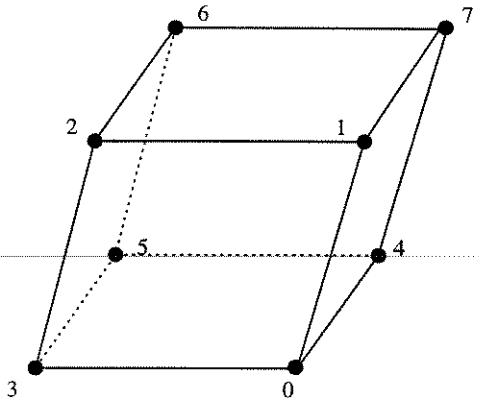


Figura 3.9: Prisma casado com D_4.

Capítulo 4

Construção de Códigos de Classes Laterais sobre Grupos

4.1 Introdução

Existem muitas maneiras de construir códigos novos usando códigos conhecidos. Uma referência excelente sobre construções de códigos é [26]. Como motivação exibiremos nesta seção algumas destas construções. Neste e no próximo capítulo usamos a notação $[n, k, d]_q$ para representar um código linear sobre $\mathbb{F}_q$ de comprimento n, dimensão k e distância mínima d.

(1) Sejam $C_1 = [n, k, d]_q$ e $C_2 = [N, K, D]_q$ dois códigos lineares. Então,

$$C = C_1 \oplus C_2 = \{(\mathbf{c}_1, \mathbf{c}_2) : \mathbf{c}_1 \in C_1,\ \mathbf{c}_2 \in C_2\}$$

é um $[N + n, K + k, \min\{D, d\}]_q$ código linear. Note que esta *soma direta externa* de códigos lineares pode ser estendida para qualquer número finito de códigos lineares.

(2) Sejam $C_1 = [n, k, d]_q$ e $C_2 = [N, K, D]_q$ códigos lineares. Então,

$$C = C_1 \otimes C_2$$

é um $[Nn, Kk, Dd]_q$ código linear, onde suas palavras-código são matrizes tais que todas suas linhas pertencem a C_1 e todas suas colunas pertencem a C_2, isto é, C pode ser identificado com um subespaço do espaço vetorial das $N \times n$ matrizes com entradas em $\mathbb{F}_q$. Note que este *produto Kroneckeriano* de códigos lineares pode ser estendido para qualquer número finito de códigos lineares.

(3) A concatenação é um método específico de construção de códigos longos através de códigos menores. Este método foi primeiramente proposto por Forney em [13] como um meio de construir códigos de bloco longos, os quais podem ser decodificados sem a complexidade usualmente requerida no uso de códigos longos. Este resultado foi generalizado por Blokh e Zyablov em [2]. Agora vamos considerar um esquema de codificação concatenada proposta por Zinoviev [34] que generaliza as proposta de [2, 13].

Sejam $B_i = [n, k_i, d_i]_{q_i}$, $i = 0, \ldots, m-1$, códigos lineares. Seja $M = M(B_0, \ldots, B_{m-1})$ uma $m \times n$ matriz cuja i-ésima linha contém uma palavra-código arbitrária $\mathbf{b}_i = (b_{i1}, \ldots, b_{in}) \in B_i$. Então,

$$M = \begin{bmatrix} b_{01} & b_{02} & \cdots & b_{0n} \\ b_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(m-1)1} & b_{(m-1)2} & \cdots & b_{(m-1)n} \end{bmatrix}.$$

Quando as palavras-código $\mathbf{b}_i \in B_i$, $i = 0, \ldots, m-1$, percorrem todos os possíveis valores, obtemos um conjunto $\{M(B_0, \ldots, B_{m-1})\}$ constituído de $\prod_{i=0}^{m-1} q_i^{k_i}$ tais matrizes.

Suponhamos que temos um $A = [N, |A|, D_0]$ código linear sobre $\mathbb{F}_q$, onde $|A| = \prod_{i=0}^{m-1} q_i$ é a cardinalidade do código. Seja

$$A_0 / \cdots / A_m,$$

uma cadeia de partições, com m-níveis e q_i-maneiras, onde

$$A_0 = A, \ A_m = \{\mathbf{0}\} \text{ e } A_s = [N, |A_s|, D_s], \ |A_s| = \prod_{i=s}^{m-1} q_i, \ s = 1, \ldots, m-1.$$

Este particionamento estabelece uma correspondência biunívoca de $\mathbb{F}_{q_0} \times \cdots \times \mathbb{F}_{q_{m-1}}$ sobre A_0. Assim, substituindo na matriz M cada coluna $(b_{0j}, \ldots, b_{(m-1)j})^t$, $j = 1, \ldots, n$, por uma palavra-código $\mathbf{a}_j$ de A_0 obtemos uma $N \times n$ matriz com entradas em $\mathbb{F}_q$. O conjunto $C = \{M(B_0, \ldots, B_{m-1})\}$ de todas as possíveis matrizes cujas colunas são transformadas como acima é um *código concatenado generalizado* ou, simplesmente um *código GC* linear sobre $\mathbb{F}_q$, com os seguintes parâmetros

$$[Nn, |C|, d]_q \text{ com } |C| = \prod_{i=0}^{m-1} q_i^{k_i} \text{ e } d \geq \min_{0 \leq i \leq m-1} \{D_i d_i\}.$$

Os códigos componentes $A_0, \ldots, A_m$ e $B_0, \ldots, B_{m-1}$ são chamados de *códigos internos e externos*, respectivamente. Quando os códigos componentes $A_0, \ldots, A_m$ e/ou $B_0, \ldots, B_{m-1}$ são não lineares o código C é não linear.

Os principais métodos de construções de códigos novos usando códigos conhecidos como acima, consistem na união de um número finito de elementos de uma partição de grupos. Mais precisamente, sejam G um grupo finito e H um subgrupo normal de G. Então H induz uma partição G/H em G de $[G : H]$ classes laterais de H. Seja $[G/H]$ um sistema de representantes de classes laterais fixo de H em G. Dado $K \subset [G/H]^N$, $C = KH^N$ é um código sobre G e é um código "linear" se, e somente se, K é um subgrupo de $[G/H]^N$ com a operação de multiplicação módulo H^N.

Por exemplo, sejam $G = \mathbb{F}_2^2$ e $H = \{(g_1, g_2) \in G : g_1 + g_2 = 0\}$ um subgrupo normal de G. Seja $[G/H] = \{(00), (10)\}$ um sistema de representantes de classes laterais fixo de H em G. Então $C = K + H^2$ é um código sobre G que tem H^2 como subcódigo e por sua vez é um subcódigo de G^2, onde $K = \{(0000), (1010)\} \subset [G/H]^2$.

Chamamos a atenção para o fato de que a construção de códigos da forma $C = KH^N$, torna-se impraticável quando a ordem da partição G/H for muito grande. Infelizmente, não se conhece nenhum método sistemático de selecionar o subconjunto K de $[G/H]$ de modo que o código $C = KH^N$ seja ótimo.

Como a ordem da partição G/H é finita, existe um refinamento de G/H em uma cadeia de partições de m-níveis

$$G_0/\cdots/G_m,$$

onde

$$G_0 = G,\ G_m = H,\ G_i = [G_i/G_{i+1}]G_{i+1},\ 0 \leq i \leq m-1.$$

Assim, um método alternativo de construir códigos da forma $C = KH^N$ é considerar o subconjunto K de $[G_0/G_m]^N$ definido por $K = \prod_{i=0}^{m-1} K_i$, onde $K_i \subset [G_i/G_{i+1}]^N$, $0 \leq i \leq m-1$. Assim, fixados os K_i, toda palavra-código de C pode ser escrita de modo único na forma kh, onde $k = \prod_{i=0}^{m-1} k_i$, $h \in G_m^N$, com $k_i \in K_i$. Portanto, C é a união de todas as classes laterais de G_m^N.

Na Seção 4.2 apresentamos uma construção de códigos de classes laterais generalizados sobre o grupo $\mathbb{Z}_q$, que segue esta forma geral de construção. A vantagem de construir códigos multicamadas reside no fato de que, para o mesmo comprimento e mesma taxa de informação, muitos destes códigos apresentam um ganho de codificação maior do que o dos códigos com somente uma camada. Na Seção 4.3 apresentamos, como resultados novos, duas tabelas de códigos de classes laterais sobre os grupos D_3 e Q_8, respectivamente.

4.2 Construção de códigos de classes laterais generalizados

Nesta seção apresentamos uma construção de códigos de classes laterais generalizados sobre o grupo $\mathbb{Z}_q$. De forma indutiva, temos a generalização para $G = \mathbb{Z}_{q_0} \times \cdots \times \mathbb{Z}_{q_{m-1}}$, onde $A_0 = [N, |A_0|, D_0]$ é um código linear sobre G com $|A_0| = \prod_{i=0}^{m-1} q_i$. Em [29] Portugheis apresenta uma condição necessária e suficiente para a linearidade destes códigos de classes laterais generalizados. Esta construção é similar a construção proposta para empacotamentos esféricos apresentada no próximo capítulo. Assim, para decodificar os códigos obtidos com esta construção podemos utilizar o algoritmo a ser proposto para reticulados ou o algoritmo proposto em [29].

Sejam A e A' códigos lineares sobre $\mathbb{Z}_q$ de comprimento N tal que $A' \subset A$. Então A' induz uma partição A/A' em A com $|A/A'| = q^m$, $1 \leq m \leq \log_q |A|$, classes laterais de A'. Se

$$[A/A'] = \left\{ \sum_{i=0}^{m-1} \alpha_i \mathbf{a}_i : \alpha_i \in \mathbb{N}_q,\ 0 \leq i \leq m-1 \right\},$$

onde $\mathbf{a}_i \in A$, $\mathbf{a}_i \notin A'$ e $\mathbb{N}_q = \{0, \ldots, q-1\}$, é um sistema de representantes de classes laterais fixo de A' em A, então uma cadeia de partições, com m-níveis e q-maneiras,

$$A_0/A_1/\cdots/A_m$$

pode ser definida como um refinamento de A/A', fazendo

$$A_0 = A,\ A_m = A',\ A_i = [A_i/A_{i+1}] + A_{i+1},\ \text{e}\ \ |A_i/A_{i+1}| = q,$$

onde

$$[A_i/A_{i+1}] = \{\alpha_i \mathbf{a}_i : \alpha_i \in \mathbb{N}_q\}\ \ \text{e}\ \mathbf{a}_i \in A_i,\ \mathbf{a}_i \notin A_{i+1},\ 0 \leq i \leq m-1.$$

Como

$$A_i = \bigcup_{\alpha_i \in \mathbb{N}_q} (\alpha_i \mathbf{a}_i + A_{i+1}),\ 0 \leq i \leq m-1$$

temos que toda classe lateral à esquerda de A_m em A_0 é determinada de modo único pelo conjunto de seqüências $(\alpha_0, \ldots, \alpha_{m-1})$, isto é, existe uma correspondência biunívoca de $\mathbb{Z}_q^m$ em A_0/A_m, a qual não é necessariamente um isomorfismo de $\mathbb{Z}_q^m$ em A_0/A_m. Note que $\mathbb{Z}_q$ é um grupo de rótulos para cada nível A_i/A_{i+1} da cadeia de partições.

Definição 4.2.1 *Sejam $A_0/\cdots/A_m$ uma cadeia de partições de códigos lineares sobre $\mathbb{Z}_q$ cada um de comprimentos N, com m-níveis e q-maneiras, e $B_0,\ldots,B_{m-1}$ códigos sobre $\mathbb{Z}_q$ cada um de comprimento n. Fixado $\beta_i \in [A_i/A_{i+1}] - \{\mathbf{0}\}$, $0 \leq i \leq m-1$, define-se um código $\mathbf{C}$ sobre $\mathbb{Z}_q$ como o conjunto*

$$\mathbf{C} \triangleq \left\{ \sum_{i=0}^{m-1} (\mathbf{b}_i \otimes \beta_i) : \mathbf{b}_i \in B_i, 0 \leq i \leq m-1 \right\} + A_m^n = \bigcup_{\mathbf{b}_i \in B_i} \left(\sum_{i=0}^{m-1} (\mathbf{b}_i \otimes \beta_i) + A_m^n \right),$$

onde para cada $\mathbf{b}_i \in B_i$, $\mathbf{b}_i \otimes \beta_i \triangleq (b_{i1}\beta_i,\ldots,b_{in}\beta_i)$, $0 \leq i \leq m-1$, a soma é sobre $\mathbb{Z}_q$ e a união é sobre todos os códigos $B_0,\ldots,B_{m-1}$.

Chamaremos o código $\mathbf{C}$ de *código de classe lateral generalizado*, (cf. [14]), o denotaremos por

$$\mathbf{C} = \sum_{i=0}^{m-1} (B_i \otimes [A_i/A_{i+1}]) + A_m^n.$$

Isso exibe explicitamente $\mathbf{C}$ como a união de $\prod_{i=0}^{m-1} |B_i|$ classes laterais à esquerda de A_m^n, onde $|B_i|$ é a cardinalidade do código B_i, $0 \leq i \leq m-1$.

Dado $\mathbf{c} \in \mathbf{C}$, $\mathbf{c} = \sum_{i=0}^{m-1}(\mathbf{b}_i \otimes \beta_i) + \mathbf{a}_m$, com $\mathbf{b}_i \in B_i$, $\mathbf{a}_m \in A_m^n$ e $\beta_i \in [A_i/A_{i+1}] - \{\mathbf{0}\}$, $0 \leq i \leq m-1$. Então,

$$\begin{aligned} \mathbf{c} &= \sum_{i=0}^{m-1} (b_{i1}\beta_i,\ldots,b_{in}\beta_i) + (\mathbf{a}_{m1},\ldots,\mathbf{a}_{mn}) \\ &= \left(\sum_{i=0}^{m-1} (b_{i1}\beta_i),\ldots, \sum_{i=0}^{m-1} (b_{in}\beta_i) \right) + (\mathbf{v}_1 M_m,\ldots,\mathbf{v}_n M_m). \end{aligned}$$

Portanto, $\mathbf{c} = (\mathbf{u}_1 M,\ldots,\mathbf{u}_n M) + VM_m$, onde $\mathbf{u}_k = (b_{0k},\ldots,b_{(m-1)k})$, $1 \leq k \leq n$, é uma m-upla formada da k-ésima componente de cada palavra-código $\mathbf{b}_i \in B_i$, $0 \leq i \leq m-1$, isto é, $\mathbf{u}_k$ é um rótulo de alguma classe lateral à esquerda de A_m em A_0, M é uma $m \times N$ matriz cujas linhas são os vetores β_k, $0 \leq i \leq m-1$, isto é, $M = \{\mathbf{a}_i : 0 \leq i \leq m-1\}$, pois $\beta_i = \alpha\mathbf{a}_i$, $\alpha \in \mathbb{N}_q - \{0\}$, $0 \leq i \leq m-1$, $V = \{\mathbf{v}_k : 1 \leq k \leq n\}$ é uma $n \times K_m$ matriz com linhas $\mathbf{v}_k \in \mathbb{Z}_q^{K_m}$ e M_m é uma matriz geradora do código A_m. Assim,

$$\mathbf{c} = UM + VM_m,$$

onde $U = \{\mathbf{u}_k : 1 \leq k \leq n\}$ é uma $n \times m$ matriz com linhas $\mathbf{u}_k \in \mathbb{Z}_q^m$. Isto significa que a i-ésima linha do produto UM é uma combinação linear das linhas de M com escalares da i-ésima linha de U. Por essa razão vamos considerar

$$\mathbf{C} = \left\{ \sum_{i=0}^{m-1} (\mathbf{b}_i \otimes \mathbf{a}_i) : \mathbf{b}_i \in B_i, 0 \leq i \leq m-1 \right\} + A_m^n.$$

Por simplicidade tomamos, em geral, o código $A_m = \{\mathbf{0}\}$. Note que os códigos B_i podem ser somente códigos de bloco, ou somente códigos convolucionais, ou uma composição de códigos de bloco e convolucionais e, em geral, não necessitam ser lineares. Todavia se os códigos B_i são lineares, então temos o seguinte resultado.

Teorema 4.2.1 *Se os códigos B_i são lineares, então $\mathbf{C}$ é um código linear sobre $\mathbb{Z}_q$.*

Prova. É claro que $\mathbf{0} \in \mathbf{C}$. Dados $\mathbf{c}, \mathbf{c}' \in \mathbf{C}$, $\mathbf{c} = UM + \mathbf{a}_m$ e $\mathbf{c}' = U'M + \mathbf{a}'_m$. Então $\mathbf{c} - \mathbf{c}' = UM + \mathbf{a}_m - (U'M + \mathbf{a}'_m) = (U - U')M + (\mathbf{a}_m - \mathbf{a}'_m) \in \mathbf{C}$. Portanto, $\mathbf{C}$ é um subgrupo de $\mathbb{Z}_q^{Nn}$. ■

A seguir apresetamos algumas observações.

(1) Se M_i são matrizes geradoras dos códigos lineares B_i, $0 \leq i \leq m-1$, com $A_m = \{\mathbf{0}\}$, então

$$M = [M_0 \otimes \mathbf{a}_0, M_1 \otimes \mathbf{a}_1, \ldots, M_{m-1} \otimes \mathbf{a}_{m-1}],$$

é uma matriz geradora para $\mathbf{C}$, onde $M_i \otimes \mathbf{a}_i = [\mathbf{r}_{i1} \otimes \mathbf{a}_i, \ldots, \mathbf{r}_{ik_i} \otimes \mathbf{a}_i]$ e $\mathbf{r}_{ij}$, $1 \leq j \leq k_i$, são as linhas de M_i. A notação $[X, Y, \ldots]$ significa uma matriz coluna, cujos elementos das "colunas" são as matrizes $X, Y, \ldots$

(2) Se os códigos lineares B_i, $0 \leq i \leq m-1$, são todos de bloco de comprimento n e dimensão k_i, $0 \leq i \leq m-1$, sobre $\mathbb{Z}_q$, então $\mathbf{C}$ é um $[Nn, k]$-código linear sobre $\mathbb{Z}_q$, onde

$$k = \begin{cases} (\sum_{i=0}^{m-2} k_i) + nk_{m-1}, & \text{se } A_m \neq \{\mathbf{0}\} \\ \sum_{i=0}^{m-1} k_i, & \text{se } A_m = \{\mathbf{0}\}. \end{cases}$$

(3) Se os códigos B_i, $0 \leq i \leq m-1$, são somente códigos convolucionais, ou a composição de códigos de bloco e convolucionais, então $\mathbf{C}$ é um código de treliça com taxa

$$R = \frac{1}{m} \sum_{i=0}^{m-1} R_i,$$

onde R_i são as taxas dos códigos B_i, $0 \leq i \leq m-1$, (cf. [37]). Embora códigos de treliça sejam essenciais em muitas aplicações práticas, não iremos considerá-los.

(4) Se $A_0 = S$ é uma constelação de sinais casada com um grupo G_0, então $\mathbf{C} = [n, |\mathbf{C}|, d(\mathbf{C})]$ é um código de classe lateral (pode ser linear ou não) sobre G_0 com taxa e ganho de codificação dados, respectivamente, por

$$R = \frac{1}{n} \log_2 |\mathbf{C}| \ \ [bits/T] \text{ e } \gamma(\mathbf{C}) = \frac{d(\mathbf{C})}{d(A_0)} \frac{R}{\log_2 |A_0|},$$

onde $d(\mathbf{C})$ é a mínima distância de $\mathbf{C}$ dada pelo Teorema 4.2.2, com a substituição de $d_H(A_i)$ pela distância Euclidiana quadrática interclasses laterais $d_{\min}(A_i)$, $0 \leq i \leq m-1$, e $d(A_0)$ é a mínima distância Euclidiana quadrática da modulação não codificada S casada com G_0, isto é, A_0 é um $[1, |A_0|, d(A_0)]$ código. Neste caso a definição $\mathbf{b}_i \otimes \mathbf{a}_i$ significa que o código B_i é sobre o alfabeto $[A_i/A_{i+1}]$.

Teorema 4.2.2 $\min_{0\leq i\leq m-1}\{d_H(B_i)d_H(A_i), d_H(A_m)\} \leq d_H(\mathbf{C}) \leq d_H(A_m)$. *Em particular, se* $B_0 \subset \cdots \subset B_m$, *então*

$$d_H(\mathbf{C}) = \min_{0\leq i\leq m-1}\{d_H(B_i)d_H(A_i), d_H(A_m)\}.$$

Prova. Dados $\mathbf{c}, \bar{\mathbf{c}} \in \mathbf{C}$, $\mathbf{c} = UM + \mathbf{a}_m$, $\bar{\mathbf{c}} = \bar{U}M + \bar{\mathbf{a}}_m$. Há dois casos a serem considerados:

(1) Se $A_m \neq \{\mathbf{0}\}$ e $U = \bar{U} = \mathbf{0}$, então $d_H(\mathbf{c}, \bar{\mathbf{c}}) = d_H(\mathbf{a}_m, \bar{\mathbf{a}}_m)$. Logo, $d_H(\mathbf{c}, \bar{\mathbf{c}}) \geq d_H(A_m)$, onde a igualdade pode ser alcançada escolhendo $(\mathbf{a}_m - \bar{\mathbf{a}}_m)$ com uma única componente não nula e igual a uma palavra-código em A_m com distância de Hamming $d_H(A_m)$;

(2) Se U e $\bar{U} \neq 0$, então existe um primeiro índice, digamos $r \geq 1$, tal que $U \neq \bar{U}$, isto é, $\mathbf{u}_r \neq \bar{\mathbf{u}}_r$. Logo, $\mathbf{b}_{i_r} \neq \bar{\mathbf{b}}_{i_r}$, para algum i_r, $0 \leq i_r \leq m-1$. Assim, pelo menos $d_H(B_{i_r})$ componentes da palavra $(\mathbf{c} - \bar{\mathbf{c}})$ pertencem a $\mathbf{a}_{i_r} + A_{i_r+1}$, isto implica que $d_H(\mathbf{c}, \bar{\mathbf{c}}) \geq d_H(B_{i_r})d_H(A_{i_r})$, $0 \leq i_r \leq m-1$. Uma vez que A_m^n é um subcódigo de $\mathbf{C}$ temos que $d_H(A_m) \geq d_H(\mathbf{C})$. Portanto, $\min_{0\leq i\leq m-1}\{d_H(B_i)d_H(A_i), d_H(A_m)\} \leq d_H(\mathbf{C}) \leq d_H(A_m)$.

Em particular, se $B_0 \subset \cdots \subset B_m$, então a igualdade pode ser alcançada escolhendo $\mathbf{c} = \mathbf{b}_{i_r} \otimes \mathbf{a}_{i_r}$ e $\bar{\mathbf{c}} = \bar{\mathbf{b}}_{i_r} \otimes \mathbf{a}_{i_r}$, onde $(\mathbf{b}_{i_r} - \bar{\mathbf{b}}_{i_r})$ e $\mathbf{a}_{i_r}$ são palavras-código de B_{i_r} e A_{i_r}, respectivamente, com mínima distância de Hamming. Portanto, $d_H(\mathbf{C}) = \min_{0\leq i\leq m-1}\{d_H(B_i)d_H(A_i), d_H(A_m)\}$. ■

4.3 Exemplos

Nesta seção apresentamos alguns exemplos de códigos novos, Exemplos 4.3.2, 4.3.3, e códigos conhecidos tão bons quanto os da literatura, que foram encontrados usando a Definição 4.2.1.

Exemplo 4.3.1 *Seja* $A_0/A_1/A_2/A_3/A_4$ *uma cadeia de partições, com* 4*-níveis e* 4*-maneiras, onde* $A_i = RS(4, i+1)_4$, $i = 0, 1, 2, 3$ *e* $A_4 = RS(4, \infty)_4$ *são códigos Reed-Solomon.*

(1) *Para os códigos* $B_0 = [5, 0, \infty]_4$, $B_1 = [5, 2, 4]_4$, $B_2 = [5, 3, 3]_4$ *e* $B_3 = [5, 4, 2]_4$ *dados na Tabela-VI de* [23] *obtemos, pelo Teorema* 4.2.2,

$$d_H(\mathbf{C}) = \min_{0 \le i \le 3} \{d_H(B_i) d_H(A_i), d_H(A_4)\} = \min\{\infty, 4.2, 3.3, 2.4, \infty\} = 8.$$

Assim, pelo Teorema 4.2.1, *o código* $\mathbf{C} = [20, 9, 8]_4$ *é linear.*

(2) *Para os códigos* $B_0 = [11, 5, 6]_4$, $B_1 = [11, 8, 3]_4$, $B_2 = [11, 10, 2]_4$ *e* $B_3 = [11, 10, 2]_4$ *dados na Tabela-VI de* [23], *obtemos o código linear* $\mathbf{C} = [44, 33, 6]_4$.

(3) *Para os códigos* $B_0 = [12, 6, 6]_4$, $B_1 = [12, 9, 3]_4$, $B_2 = [12, 11, 2]_4$ *e* $B_3 = [12, 11, 2]_4$ *dados na Tabela-VI de* [23], *obtemos o código linear* $\mathbf{C} = [48, 37, 6]_4$. ■

Exemplo 4.3.2 *Neste exemplo construímos uma classe de códigos sobre a constelação de sinais normalizada casada com o grupo diedral* D_3 *do Exemplo* 3.2.3. *Seja* $A_0/A_1/A_2$ *uma cadeia de partições, com* 2*-níveis, onde* $A_0 = D_3$, $A_1 = \langle 1 \rangle$, $A_2 = \{0\}$ *e mínimas distâncias Euclidianas quadráticas* $1.5/1.5/\infty$, *isto é, os* A_i *são códigos de espaço Euclidiano de comprimento unitário. Então, obtemos os códigos* $\mathbf{C} = \{\mathbf{b}_0 \otimes 3 +_\theta \mathbf{b}_1 \otimes 1 : \mathbf{c}_i \in B_i, i = 0, 1\}$ *sobre* D_3 *mostrados na Tabela* 4.1, *onde os códigos* $B_0 = [n, k_0, d_0]_2$ *na primeira coluna da tabela são da Tabela-I de* [3]. *Os códigos* $B_1 = [n, k_1, d_1]_3$ *na segunda coluna da Tabela* 4.1 *são da Tabela-V de* [23]. *Na terceira coluna da Tabela* 4.1 *encontra-se os códigos novos* $\mathbf{C}$ *com parâmetros* $[n, |\mathbf{C}|, d(\mathbf{C})]$, *onde* $|\mathbf{C}|$ *e* $d(\mathbf{C})$ *representam o número de palavras-código e a mínima distância Euclidiana quadrática do código. Finalmente, na quarta e quinta coluna da Tabela* 4.1 *encontra-se a taxa e o ganho de codificação dos códigos* $\mathbf{C}$ *definidos na observação* (4) *acima.* ■

Exemplo 4.3.3 *Neste exemplo construímos uma classe de códigos sobre a constelação de sinais normalizada casada com o grupo dos quatênios* Q_8 *do Exemplo* 3.2.5. *Seja* $A_0/A_1/A_2$ *uma cadeia de partições, com* 3*-níveis e* 2*-maneiras, onde* $A_0 = Q_8$, $A_1 = \langle 1 \rangle$, $A_2 = \langle 2 \rangle$, $A_3 = \{0\}$ *e mínimas distâncias Euclidianas quadráticas* $1/1/2/\infty$, *isto é, os* A_i *são códigos de espaço Euclidiano de comprimento unitário. Então obtemos os códigos* $\mathbf{C} = \{\mathbf{b}_0 \otimes 4 +_\theta \mathbf{b}_1 \otimes 1 +_\theta \mathbf{b}_2 \otimes 2 : \mathbf{b}_i \in B_i, i = 0, 1, 2\}$ *sobre* Q_8 *mostrados na Tabela* 4.2, *onde os códigos* $B_i = [n, k_i, d_i]_2$ *nas três colunas da Tabela* 4.2 *são da Tabela-I de* [3]. *Na quarta coluna da Tabela* 4.2 *encontra-se os códigos novos* $\mathbf{C}$ *com parâmetros* $[n, |\mathbf{C}|, d(\mathbf{C})]$, *onde* $|\mathbf{C}|$ *e* $d(\mathbf{C})$ *representam o número de palavras-código e a mínima distância Euclidiana quadrática do código. Finalmente, na quinta e sexta coluna da Tabela* 4.2 *encontra-se a taxa e o ganho de codificação dos códigos* $\mathbf{C}$ *definidos na observação* (4) *acima.* ■

B_0	B_1	$\mathbf{C}$	$R\,[bits/T]$	$\gamma(\mathbf{C})[dB]$
$[8,7,2]$	$[8,7,2]$	$[8,2^7 3^7,3]$	2.26	2.43
$[8,4,4]$	$[8,4,4]$	$[8,2^4 3^4,6]$	1.29	3.01
$[12,8,3]$	$[12,9,3]$	$[12,2^8 3^9,4.5]$	1.86	3.33
$[12,7,4]$	$[12,7,4]$	$[12,2^7 3^7,6]$	1.51	3.68
$[12,4,6]$	$[12,6,6]$	$[12,2^4 3^6,9]$	1.13	4.18
$[16,15,2]$	$[16,15,2]$	$[16,2^{15} 3^{15},3]$	2.42	2.72
$[16,11,4]$	$[16,11,4]$	$[16,2^{11} 3^{11},6]$	1.78	4.40
$[16,7,6]$	$[16,8,6]$	$[16,2^7 3^8,9]$	1.23	4.55
$[24,19,3]$	$[24,20,3]$	$[24,2^{19} 3^{20},4.5]$	2.11	3.90
$[24,15,4]$	$[24,18,4]$	$[24,2^{15} 3^{18},6]$	1.81	4.46
$[24,14,6]$	$[24,16,6]$	$[24,2^{14} 3^{16},9]$	1.64	5.80
$[24,12,8]$	$[24,12,9]$	$[24,2^{12} 3^{12},12]$	1.29	6.00

Tabela 4.1: Códigos sobre D_3.

Exemplo 4.3.4 *Seja* $A_0/A_1/A_2/A_3$ *uma cadeia de partições da constelação de sinais* $8PSK$, *com* 3-*níveis e* 2-*maneiras, onde* $A_i = 2^i\mathbb{Z}_8$, $i = 0,1,2,3$.

(1) *Para os códigos* $B_0 = [6,0,\infty]_2$, $B_1 = [6,2,4]_2$ *e* $B_2 = [6,5,2]_2$ *dados na Tabela-I de* [3], *obtemos o código* $\mathbf{C} = [6,|\mathbf{C}|,8]$ *sobre* $\mathbb{Z}_8$, *onde* $|\mathbf{C}| = 2^7$.

(2) *Para os códigos* $B_0 = [7,0,\infty]_2$, $B_1 = [7,3,4]_2$ *e* $B_2 = [7,6,2]_2$ *dados na Tabela-I de* [3], *obtemos o código* $\mathbf{C} = [7,|\mathbf{C}|,8]$ *sobre* $\mathbb{Z}_8$, *onde* $|\mathbf{C}| = 2^9$.

(3) *Para os códigos* $B_0 = [8,0,\infty]_2$, $B_1 = [8,4,4]_2$ *e* $B_2 = [8,7,2]_2$ *dados na Tabela-I de* [3], *obtemos o código* $\mathbf{C} = [8,|\mathbf{C}|,8]$ *sobre* $\mathbb{Z}_8$, *onde* $|\mathbf{C}| = 2^{11}$.

Note que estes códigos são tão bons quanto os códigos cíclicos de [28] *e semelhantes aos de* [22].

■

B_0	B_1	B_2	$\mathbf{C}$	$R\,[bits/T]$	$\gamma(\mathbf{C})[dB]$
$[8,7,2]$	$[8,7,2]$	$[8,8,1]$	$[8,2^{22},2]$	2.75	2.63
$[8,4,4]$	$[8,4,4]$	$[8,7,2]$	$[8,2^{15},4]$	1.88	4.00
$[8,2,5]$	$[8,2,5]$	$[8,4,4]$	$[8,2^{8},5]$	1.00	2.22
$[12,11,2]$	$[12,11,2]$	$[12,12,1]$	$[12,2^{34},2]$	2.83	2.80
$[12,5,4]$	$[12,5,4]$	$[12,11,2]$	$[12,2^{21},4]$	1.75	3.68
$[12,2,8]$	$[12,2,8]$	$[12,5,4]$	$[12,2^{9},8]$	0.75	3.01
$[16,11,4]$	$[16,11,4]$	$[16,15,2]$	$[16,2^{37},4]$	2.31	5.00
$[16,5,8]$	$[16,5,8]$	$[16,11,4]$	$[16,2^{21},8]$	1.31	5.43
$[16,2,10]$	$[16,2,10]$	$[16,8,5]$	$[16,2^{12},10]$	0.75	4.00
$[24,15,4]$	$[24,15,4]$	$[24,23,2]$	$[24,2^{43},4]$	2.20	4.67
$[24,14,6]$	$[24,14,6]$	$[24,19,3]$	$[24,2^{47},6]$	1.96	5.93
$[24,12,8]$	$[24,12,8]$	$[24,15,4]$	$[24,2^{39},8]$	1.63	6.38
$[24,5,12]$	$[24,5,12]$	$[24,14,6]$	$[24,2^{24},12]$	1.00	6.02

Tabela 4.2: Códigos sobre Q_8.

Capítulo 5

Construção de Empacotamentos Esféricos via Códigos de Classes Laterais Generalizados

5.1 Introdução

A primeira construção de um reticulado Λ em $\mathbb{R}^N$ utilizando um código linear foi proposta em [24]. Seja $C = [N, k, d]_p$ um código linear, onde p é um número primo. Se identificarmos $\mathbb{Z}_p$ com o subconjunto $\mathbb{N}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}$, então

$$\Lambda = \bigcup_{\mathbf{c} \in C} (l(\mathbf{c}) + p\mathbb{Z}^N)$$

é um reticulado em $\mathbb{R}^N$, onde $\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$ é um grupo de rótulos e $l : \mathbb{Z}_p^N \longrightarrow [\mathbb{Z}/p\mathbb{Z}]^N$. Isto exibe explicitamente Λ como a união de p^k classes laterais à esquerda de $p\mathbb{Z}^N$

Os principais métodos de construções de novos empacotamentos esféricos usando-se reticulados conhecidos como acima, consistem na união de um número finito de elementos de uma partição. Mais precisamente, sejam Γ e Λ reticulados em $\mathbb{R}^N$ tal que Λ é um sub-reticulado de Γ. Então Λ induz uma partição Γ/Λ de Γ em $[\Gamma : \Lambda]$ classes laterais de Λ. Seja $[\Gamma/\Lambda]$ um sistema de representantes de classes laterais de Λ em Γ. Dado $H \subset [\Gamma/\Lambda]$, $\mathbf{L}_N = H + \Lambda$ é um empacotamento esférico em $\mathbb{R}^N$ e é um reticulado se, e somente se, H é um subgrupo de $[\Gamma/\Lambda]$ com a operação de adição módulo Λ. De um modo geral, $\mathbf{L}_{Nn} = H + \Lambda^n$ é um empacotamento esférico em $\mathbb{R}^{Nn}$ e é um reticulado se, e somente se,

H é um subgrupo de $[\Gamma^n/\Lambda^n]$ com a operação de adição módulo Λ^n, onde Γ^n/Λ^n é isomorfo a $(\Gamma/\Lambda)^n$.

Por exemplo, sejam $\Gamma = \mathbb{Z}$ e $\Lambda = 2\mathbb{Z}$ reticulados em $\mathbb{R}$ tal que Λ é um sub-reticulado de Γ e $[\Gamma/\Lambda] = \{0, 1\}$ um sistema de representantes de classes laterais de Λ em Γ. Então $\mathbf{L}_4 = H + \Lambda^4$ é um reticulado em $\mathbb{R}^4$ que tem Λ^4 como um sub-reticulado e por sua vez é um sub-reticulado de Γ^4, onde o subgrupo selecionado é dado por $H = \{(0,0,0,0),(1,1,0,0)\} \subset [\Gamma/\Lambda]^4$. Note que $\mathbf{L}_4$ tem um ganho de codificação fundamental de $1.51[dB]$, portanto mais denso do que Γ ou Γ^4.

Chamamos a atenção para o fato de que a construção de empacotamentos esféricos da forma $\mathbf{L}_{Nn}$ que seja mais denso do que Γ para a utilização em esquemas de quantização e/ou codificação de canais com Ruído Gaussiano Branco Aditivo em faixa limitada, torna-se impraticável quando a ordem da partição Γ/Λ for muito grande. Infelizmente, não se conhece nenhum método sistemático de selecionar o subgrupo H de $[\Gamma/\Lambda]^n$ de modo que o empacotamento esférico $\mathbf{L}_{Nn} = H + \Lambda^n$ seja mais denso do que Γ^n.

Seja r a ordem da partição Γ/Λ, (cf. Lema 2.3.3), e $r = \prod_{i=0}^{m-1} q_i$, onde $q_i = p_i^{n_i}$, com p_i números primos distintos, $0 \leq i \leq m-1$ e $n_0 + \cdots + n_{m-1} \leq N$. Como Γ/Λ é um grupo comutativo finito, existe um refinamento da partição Γ/Λ em uma cadeia de partições de m-níveis e q_i-maneiras

$$\Lambda_0/\Lambda_1/\cdots/\Lambda_{m-1}/\Lambda_m,$$

onde

$$\Lambda_0 = \Gamma,\ \Lambda_m = \Lambda,\ \Lambda_i = [\Lambda_i/\Lambda_{i+1}] + \Lambda_{i+1} \text{ e } |\Lambda_i/\Lambda_{i+1}| = q_i,\ 0 \leq i \leq m-1.$$

Assim, um método alternativo de construir empacotamentos esféricos da forma $\mathbf{L}_{Nn} = H + \Lambda_m^n$ é considerar o subconjunto H de $[\Lambda_0/\Lambda_m]^n$ definido por $H = \sum_{i=0}^{m-1} H_i$, onde H_i são subconjuntos de $[\Lambda_i/\Lambda_{i+1}]^n, 0 \leq i \leq m-1$. É claro que $\mathbf{L}_{Nn}$ é um reticulado se, e somente se, cada H_i é um subgrupo de $[\Lambda_i/\Lambda_{i+1}]^n, 0 \leq i \leq m-1$. Uma vez que Λ_i/Λ_{i+1} é isomorfo ao grupo rótulos $\mathbb{Z}_{q_i}$, $0 \leq i \leq m-1$, os conjuntos H_i podem ser identificados com códigos C_i sobre $\mathbb{Z}_{q_i}$, assim, cada palavra-código $\mathbf{c}_i \in C_i$ será identificada com um elemento $h_i \in H_i$ e $\sum_{i=0}^{m-1} h_i$ é o representante de alguma classe lateral de Λ_m^n em Λ_0^n. Portanto, $\mathbf{L}_{Nn}$ é a união de todas as classes laterais de Λ_m^n.

Na Seção 5.2 apresentamos uma construção multicamada, que estende a proposta de [10], para a obtenção de empacotamentos esféricos com o maior ganho de codificação fundamental possível em $\mathbb{R}^{Nn}$. Na Seção 5.3, com o propósito de completude, um algoritmo de decodificação com distância limitada é exibido para a decodificação dos reticulados obtidos através desta construção. Finalmente,

na Seção 5.3 apresentamos, como resultado desta construção, empacotamentos esféricos conhecidos e novos. Em dimensões 68 e 72, um novo recorde de densidades parece ter sido alcançado.

5.2 Construção de empacotamentos esféricos

Os resultados desta seção estendem a proposta de [10], para qualquer número r, onde $r = \prod_{i=0}^{m-1} q_i$ é a decomposição de r em fatores primos distintos. Com o propósito de completude, apresentamos as provas de todos os resultados que foram estendidos. Para maiores detalhes, (cf. [9]).

Sejam Γ e Λ reticulados em $\mathbb{R}^N$ tal que Λ é um sub-reticulado de Γ. Então Λ induz uma partição Γ/Λ de ordem r e $r\Gamma \subseteq \Lambda$. Se

$$[\Gamma/\Lambda] = \left\{ \sum_{i=0}^{m-1} a_i \mathbf{g}_i : a_i \in \mathbb{N}_{q_i} \right\},$$

onde $\mathbf{g}_i \in \Gamma$, $\mathbf{g}_i \notin \Lambda$ e $\mathbb{N}_{q_i} = \{0, \ldots, q_i - 1\}$, é um sistema de representantes de classes laterais fixo de Λ em Γ, então uma cadeia de partições

$$\Lambda_0/\Lambda_1/\cdots/\Lambda_{m-1}/\Lambda_m,$$

com m-níveis e q_i-maneiras, pode ser definida como um refinamento de Γ/Λ, fazendo

$$\Lambda_0 = \Gamma,\ \Lambda_m = \Lambda \text{ e } \Lambda_i = [\Lambda_i/\Lambda_{i+1}] + \Lambda_{i+1},$$

onde

$$[\Lambda_i/\Lambda_{i+1}] = \{a_i \mathbf{g}_i : a_i \in \mathbb{N}_{q_i}\},\ \mathbf{g}_i \in \Lambda_i,\ \mathbf{g}_i \notin \Lambda_{i+1} \text{ e } |\Lambda_i/\Lambda_{i+1}| = q_i,\ 0 \leq i \leq m-1,$$

com $\mathbb{Z}_{q_i} \simeq \Lambda_i/\Lambda_{i+1}$, $0 \leq i \leq m-1$ um grupo de rótulos.

Definição 5.2.1 *Sejam $\Lambda_0/\Lambda_1/\cdots/\Lambda_{m-1}/\Lambda_m$ uma cadeia de partições de reticulados em $\mathbb{R}^N$, com m-níveis e q_i-maneiras, e $C_0, \ldots, C_{m-1}$ códigos de bloco sobre $\mathbb{Z}_{q_i}$ cada um de comprimento n. Fixado $\alpha_i \in [\Lambda_i/\Lambda_{i+1}] - \{\mathbf{0}\}$, $0 \leq i \leq m-1$, define-se um empacotamento esférico $\mathbf{L}_{Nn}$ em $\mathbb{R}^{Nn}$ como o conjunto*

$$\mathbf{L}_{Nn} \triangleq \left\{ \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \alpha_i) : \mathbf{c}_i \in C_i, 0 \leq i \leq m-1 \right\} + \Lambda_m^n = \bigcup_{\mathbf{c}_i \in C_i} \left(\sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \alpha_i) + \Lambda_m^n \right),$$

onde para cada $\mathbf{c}_i = (c_{i1}, \ldots, c_{in}) \in C_i$, $\mathbf{c}_i \otimes \alpha_i \triangleq (c_{i1}\alpha_i, \ldots, c_{in}\alpha_i)$, com as palavras-código $\mathbf{c}_i$ vista como um vetor real de componentes $c_{ij} \in \mathbb{N}_{q_i}$, $0 \leq i \leq m-1$, $1 \leq j \leq n$ e a união é sobre todos os códigos $C_0, \ldots, C_{m-1}$.

Chamamos a atenção de que, o empacotamento esférico $\mathbf{L}_{Nn}$ é periódico, no sentido de que ele é invariante sob deslocamento de múltiplos inteiros dos vetores básicos de Λ_m^n. O arranjo periódico $\mathbf{L}_{Nn}$ é chamado de *código de classe lateral generalizado*, (cf. [14]), o denotaremos por

$$\mathbf{L}_{Nn} = \sum_{i=0}^{m-1} (C_i \otimes [\Lambda_i/\Lambda_{i+1}]) + \Lambda_m^n.$$

Dado $\mathbf{l} \in \mathbf{L}_{Nn}$, $\mathbf{l} = \sum_{i=0}^{m-1}(\mathbf{c}_i \otimes \alpha_i) + \lambda_m$, com $\mathbf{c}_i \in C_i, \lambda_m \in \Lambda_m^n$ e $\alpha_i \in [\Lambda_i/\Lambda_{i+1}] - \{0\}$. Então,

$$\begin{aligned} \mathbf{l} &= \sum_{i=0}^{m-1}(c_{i1}\alpha_i, \ldots, c_{in}\alpha_i) + (\lambda_{m1}, \ldots, \lambda_{mn}) \\ &= \left(\sum_{i=0}^{m-1}(c_{i1}\alpha_i), \ldots, \sum_{i=0}^{m-1}(c_{in}\alpha_i)\right) + (\mathbf{v}_1 D, \ldots, \mathbf{v}_n D)\,. \end{aligned}$$

Portanto, $\mathbf{l} = (\mathbf{u}_1 B, \ldots, \mathbf{u}_n B) + VD$, onde $\mathbf{u}_k = (c_{0k}, \ldots, c_{(m-1)k})$, $1 \leq k \leq n$, é a m-upla formada da k-ésima componente de cada palavra-código $\mathbf{c}_i \in C_i$, $0 \leq i \leq m-1$, isto é, $\mathbf{u}_k$ é um rótulo de alguma classe lateral à esquerda de Λ_m em Λ_0, B é uma $m \times N$ matriz cujas linhas são os vetores $\alpha_0, \ldots, \alpha_{m-1}$, isto é, $B = \{\mathbf{g}_i : 0 \leq i \leq m-1\}$, pois $\alpha_i = a\mathbf{g}_i$, $a \in \mathbb{N}_{q_i} - \{0\}$, $V = \{\mathbf{v}_k : 1 \leq k \leq n\}$ é uma $n \times N$ matriz cujas linhas são os vetores $\mathbf{v}_k \in \mathbb{Z}^N$, $1 \leq k \leq n$, e $D = M_m^t$, onde M_m é uma matriz geradora para o reticulado Λ_m. Assim,

$$\mathbf{l} = UB + VD,$$

onde $U = \{\mathbf{u}_k : 1 \leq k \leq n\}$ é uma $n \times m$ matriz cujas linhas são os vetores $\mathbf{u}_k \in \mathbb{N}_{q_i}^m$. Isto significa que a i-ésima linha do produto UB é uma combinação linear das linhas de B com escalares da i-ésima linha de U. Por essa razão vamos considerar

$$\mathbf{L}_{Nn} = \left\{ \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \mathbf{g}_i) : \mathbf{c}_i \in C_i,\ 0 \leq i \leq m-1 \right\} + \Lambda_m^n.$$

Isso exibe explicitamente $\mathbf{L}_{Nn}$ como a união de $\prod_{i=0}^{m-1} |C_i|$ classes laterais de Λ_m^n, onde $|C_i|$ é a cardinalidade do código C_i. Em particular, se $q_i = q$ e os códigos C_i, $0 \leq i \leq m-1$, são lineares, isto é, subgrupos de $\mathbb{Z}_q^n$, então o empacotamento esférico $\mathbf{L}_{Nn}$ é um reticulado em $\mathbb{R}^{Nn}$, (cf. Teorema 5.2.1 a seguir). Neste caso,

$$\mathbf{c}_i + \mathbf{c}_j = \mathbf{c}_i \oplus \mathbf{c}_j + q(\mathbf{c}_i \circ \mathbf{c}_j),$$

onde "+" é a soma ordinária em $\mathbb{R}^N$, "$\oplus$" é soma em $\mathbb{Z}_q$ e "$\circ$" é definida por

$$\mathbf{c}_i \circ \mathbf{c}_j \triangleq \left(\lfloor \frac{1}{q}(c_{i1} + c_{j1}) \rfloor, \ldots, \lfloor \frac{1}{q}(c_{in} + c_{jn}) \rfloor \right),$$

sendo $\lfloor x \rfloor$ o maior inteiro menor ou igual a x. No caso em que $q = 2$, temos

$$\lfloor \frac{1}{q}(c_{ik} + c_{jk}) \rfloor = c_{ik}c_{jk},\ 1 \leq k \leq n.$$

Note que, quando $\mathbb{Z}_q$ é substituído pelo corpo de Galois $\mathbb{F}_q$ a soma acima tem restrições, pois neste caso a soma depende da característica do corpo. Uma alternativa, é considerar os códigos C_i como sendo quasilineares. Se $q_i = q$ e os códigos C_i, $0 \leq i \leq m-1$, são lineares, então temos o seguinte resultado.

Teorema 5.2.1 *Se $q_i = q$ e os códigos C_i, $0 \leq i \leq m-1$, são lineares, então $\mathbf{L}_{Nn}$ é um reticulado em $\mathbb{R}^{Nn}$.*

Prova. É claro que $\mathbf{0} \in \mathbf{L}_{Nn}$. Dado $\mathbf{l} = UB + \lambda_m \in \mathbf{L}_{Nn}$. Então,

$$\mathbf{l} = ((1-q)U)B + (qU)B + \lambda_m.$$

Assim, existe $\mathbf{l}' = ((q-1)U)B - \lambda'_m \in \mathbf{L}_{Nn}$, onde $\lambda'_m = (qU)B + \lambda_m \in \Lambda_m^n$, pois $q\Lambda_0 \subseteq \Lambda_m$, tal que $\mathbf{l} + \mathbf{l}' = \mathbf{0}$. Dados $\mathbf{l}, \mathbf{l}' \in \mathbf{L}_{Nn}$, $\mathbf{l} = UB + \lambda_m$ e $\mathbf{l}' = U'B + \lambda'_m$. Então,

$$\begin{aligned} \mathbf{l} + \mathbf{l}' &= UB + \lambda_m + U'B + \lambda'_m \\ &= (U + U')B + \lambda_m + \lambda'_m. \end{aligned}$$

Como $U + U' = U \oplus U' + q(U \circ U')$ e $\mathbf{c}_i \oplus \mathbf{c}'_i = \overline{\mathbf{c}}_i \in C_i$ temos que

$$\mathbf{l} + \mathbf{l}' = \overline{U}B + \overline{\lambda}_m \in \mathbf{L}_{Nn},$$

pois, $\overline{U} = U \oplus U'$ e $\overline{\lambda}_m = q(U \circ U')B + \lambda_m + \lambda'_m \in \Lambda_m^n$. Portanto, $\mathbf{L}_{Nn}$ é um subgrupo de $\mathbb{R}^{Nn}$. ■

O teorema seguinte determina uma cota da mínima distância Euclidiana quatrática dos empacotamentos esféricos da Definição 5.2.1.

Teorema 5.2.2 $\min_{0 \leq i \leq m-1}\{d_H(C_i)d^2_{\min}(\Lambda_i), d^2_{\min}(\Lambda_m)\} \leq d^2_{\min}(\mathbf{L}_{Nn}) \leq d^2_{\min}(\Lambda_m)$. *Em particular, se $C_0 \subseteq \cdots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então*

$$d^2_{\min}(L_{Nn}) = \min_{0 \leq i \leq m-1}\{d_H(C_i)N(\Lambda_i), d^2_{\min}(\Lambda_m)\}.$$

Prova. Dados $\mathbf{l}, \mathbf{l}' \in \mathbf{L}_{Nn} - \{\mathbf{0}\}$. Então $\mathbf{l} = UB + \lambda_m$ e $\mathbf{l}' = U'B + \lambda'_m$. Há dois casos a serem considerados:

(1) Se $U = U' = \mathbf{0}$, então $\mathbf{l} = \lambda_m$, $\mathbf{l}' = \lambda'_m \in \Lambda_m^n$. Logo, $d^2(\mathbf{l}, \mathbf{l}') \geq d^2_{\min}(\Lambda_m)$, onde a igualdade pode ser alcançada escolhendo $(\mathbf{l} - \mathbf{l}')$ com uma única componente não nula e igual a um vetor em Λ_m com norma $d^2_{\min}(\Lambda_m)$;

(2) Se $U \neq U'$, então existe um primeiro índice, digamos k_0, $1 \leq k_0 \leq n$, tal que $\mathbf{u}_{k_0} = (c_{0k_0}, \ldots, c_{(m-1)k_0}) \neq \mathbf{u}'_{k_0} = (c'_{0k_0}, \ldots, c'_{(m-1)k_0})$, isto é, $\mathbf{c}_{i_0} \neq \mathbf{c}'_{i_0}$ para algum i_0, $0 \leq i_0 \leq m-1$. Assim, pelo menos $d_H(C_{i_0})$ componentes de $(\mathbf{l} - \mathbf{l}')$ pertencem a $\mathbf{g}_{i_0} + \Lambda_{i_0+1}$. Logo, $d^2(\mathbf{l}, \mathbf{l}') \geq d_H(C_{i_0}) d^2_{\min}(\Lambda_{i_0})$, $0 \leq i_0 \leq m-1$.

Em particular, se $C_0 \subseteq \cdots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então a igualdade pode ser alcançada escolhedo-se $\mathbf{l} = \mathbf{c}_{i_0} \otimes \lambda_{i_0}$ e $\mathbf{l}' = \mathbf{c}'_{i_0} \otimes \lambda'_{i_0}$, onde $(\mathbf{c}_{i_0} - \mathbf{c}'_{i_0})$ é uma palavra-código de peso mínimo em C_{i_0} e $(\lambda_{i_0} - \lambda'_{i_0})$ é vetor de norma mínima em Λ_{i_0}. ■

Corolário 5.2.1 *Se $C_0 \subseteq \cdots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então dado $\mathbf{l} \in \mathbf{L}_{Nn}$, $\mathbf{l} = UB + \lambda_m$ e $\mathbf{u}_k \neq 0$, para algum k, $1 \leq k \leq n$, temos que $\mathbf{N}(\mathbf{l}) = d^2_{\min}(\mathbf{L}_{Nn})$ se, e somente se, $w_H(\mathbf{c}_i) = d_H(C_i)$ e $d^2_{\min}(\mathbf{L}_{Nn}) = d_H(C_i) d^2_{\min}(\Lambda_i)$, $0 \leq i \leq m-1$, onde $\mathbf{u}_k = (c_{0k}, \ldots, c_{m-1k}) \neq \mathbf{0}$ implica que $\mathbf{c}_i \neq \mathbf{0}$ para algum i, $0 \leq i \leq m-1$.* ■

Com o objetivo de determinar os coeficientes de erros dos empacotamentos esféricos da Definição 5.2.1, para o caso em que os empacotamentos esféricos são reticulados e $C_0 \subseteq \cdots \subseteq C_{m-1}$, é que apresentamos no próximo teorema, (cf. [10]), uma fórmula fechada para a contagem do número de vizinhos. Esse resultado é relevante para o processo de decodificação uma vez que o mesmo está baseado no método de construção sendo proposto. Com o propósito de completute apresentamos a sua demonstração, embora seja mais geral. Para várias aplicações deste resultado, (cf. [10]).

Teorema 5.2.3 *[10] Se $C_0 \subseteq \cdots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então o número de vizinhos $E(\mathbf{L}_{Nn})$ é dado por*

$$E(\mathbf{L}_{Nn}) = \sum_{\substack{i=0 \\ d^2_{\min}(\mathbf{L}_{Nn}) = d_H(C_i) d^2_{\min}(\Lambda_i)}}^{m-1} \left(\sum_{\substack{i=0 \\ w_H(\mathbf{c}_i) = d_H(C_i)}}^{m-1} M^{(i)}(\mathbf{c}_i) \right) + E_m,$$

onde

$$M^{(i)}(\mathbf{c}_i) = \begin{cases} E(\Lambda_i)^{d_H(C_i)}, & \text{se } i = m-1 \\ \displaystyle\sum_{\substack{\mathbf{c}_j \in C_j \\ w_H(\mathbf{c}_j * \mathbf{c}_i) = w_H(\mathbf{c}_j) \\ i < j \leq m-1}} \left[\prod_{\substack{k=1 \\ c_{ik} \neq 0}}^{n} E^{(i)}\left(\sum_{s=i}^{m-1} (c_{sk} g_s) + \Lambda_m \right) \right], & \text{se } 0 \leq i < m-1. \end{cases}$$

sendo $E^{(i)}(X)$ *o número de pontos de* X *com norma igual a* $d^2_{\min}(\Lambda_i)$, $c_j * c_i$ *é o produto componente a componente em* $\mathbb{Z}_q$ *e*

$$E_m = \begin{cases} nE(\Lambda_m), & \text{se } d^2_{\min}(\Lambda_m) = d^2_{\min}(L_{Nn}) \\ 0, & \text{se } d^2_{\min}(\Lambda_m) > d^2_{\min}(L_{Nn}) \end{cases}$$

Prova. Basta determinar o número de vizinhos mais próximos da origem, pois nesse caso $\mathbf{L}_{Nn}$ é um reticulado em $\mathbb{R}^{Nn}$. Dado $\mathbf{l} \in \mathbf{L}_{Nn} - \{\mathbf{0}\}$. Então $\mathbf{l} = UB + \lambda_m$. Há dois casos a serem considerados:

(1) Se $U = \mathbf{0}$, então $\mathbf{l} = \lambda_m \in \Lambda_m^n$ e $\mathbf{N}(\mathbf{l}) \geq d^2_{\min}(\Lambda_m)$. Como $d^2_{\min}(\Lambda_m) \geq d^2_{\min}(\mathbf{L}_{Nn})$ temos duas possibilidades:

(i) Se $d^2_{\min}(\Lambda_m) = d^2_{\min}(\mathbf{L}_{Nn})$, então $\mathbf{l} = (0, \ldots, 0, \lambda_{mk}, 0, \ldots 0)$ com $\lambda_{mk} \in \Lambda_m - \{\mathbf{0}\}$. Assim, o número de vetores $\mathbf{l} \in \mathbf{L}_{Nn}$ tal que $\mathbf{N}(\mathbf{l}) = d^2_{\min}(\Lambda_m)$ é dado por

$$E_m = \begin{pmatrix} n \\ 1 \end{pmatrix} E(\Lambda_m) = nE(\Lambda_m).$$

(ii) Se $d^2_{\min}(\Lambda_m) > d^2_{\min}(\mathbf{L}_{Nn})$, então $\mathbf{N}(\mathbf{l}) > d^2_{\min}(\Lambda_m)$. Assim, $E_m = 0$. Portanto,

$$E_m = \begin{cases} nE(\Lambda_m), & \text{se } d^2_{\min}(\Lambda_m) = d^2_{\min}(L_{Nn}) \\ 0, & \text{se } d^2_{\min}(\Lambda_m) > d^2_{\min}(L_{Nn}) \end{cases};$$

(2) Se $U \neq \mathbf{0}$, então existe um primeiro índice, digamos k_0, $1 \leq k_0 \leq n$, tal que $\mathbf{u}_{k_0} = (c_{0k_0}, \ldots, c_{(m-1)k_0}) \neq \mathbf{0}$, isto é, $\mathbf{c}_{i_0} \neq \mathbf{0}$ para algum i_0, $0 \leq i_0 \leq m-1$. Assim, pelo Corolário 5.2.1, o número de vetores $\mathbf{l} \in \mathbf{L}_{Nn}$ tal que $\mathbf{N}(\mathbf{l}) = d^2_{\min}(\mathbf{L}_{Nn})$ é dado por

$$\sum_{d^2_{\min}(\mathbf{L}_{Nn}) = d_H(C_{i_0}) d^2_{\min}(\Lambda_{i_0})} \left(\sum_{w_H(\mathbf{c}_{i_0}) = d_H(C_{i_0})} M^{(i_0)}(\mathbf{c}_{i_0}) \right),$$

onde $M^{(i_0)}(\mathbf{c}_{i_0})$ é o número de vetores em $\mathbf{l} \in \mathbf{L}_{Nn}$ tal que $\mathrm{N}(\mathbf{l}) = d^2_{\min}(\mathbf{L}_{Nn})$ para cada i_0 e $\mathbf{c}_{i_0}$ fixados com $w_H(\mathbf{c}_{i_0}) = d_H(C_{i_0})$ e $d^2_{\min}(L_{Nn}) = d_H(C_{i_0})d^2_{\min}(\Lambda_{i_0}), 0 \leq i_0 \leq m-1$. Como as $w_H(\mathbf{c}_{i_0}) = d_H(C_{i_0})$ componentes não nulas l_{k_0} de $\mathbf{l}$, comtribui com pelo menos $d^2_{\min}(L_{Nn}) = d_H(C_{i_0})d^2_{\min}(\Lambda_{i_0})$ para $\mathrm{N}(\mathbf{l})$, assim, as outras componentes de $\mathbf{l}$ tal que $\mathrm{N}(\mathbf{l}) = d^2_{\min}(\mathbf{L}_{Nn})$ são não nulas e $c_{i_0 k_0} = 0$. Logo, as palavras-código $\mathbf{c}_j \in C_j$, com $i_0 < j \leq m-1$, em $\mathbf{l} \in \mathbf{L}_{Nn}$ podem ser não nulas, pois $C_{i_0} \subseteq C_j$ implica que $\{k_0 \in \{1,\ldots,n\} : c_{i_0 k_0} = 0\} \subseteq \{k_0 \in \{1,\ldots,n\} : c_{j k_0} = 0\}$, em outras palavras, $w_H(\mathbf{c}_{i_0} * \mathbf{c}_j) = w_H(\mathbf{c}_j), i_0 < j \leq m-1$, onde $\mathbf{c}_{i_0} * \mathbf{c}_j$ é o produto componente a componente em $\mathbb{Z}_q$. Finalmente, como $l_{k_0} = \mathbf{u}_{k_0} B \in (0,\ldots 0, \mathbf{u}_{k_0} B, \ldots, \mathbf{u}_n B) + \Lambda^n_m, \mathbf{u}_{k_0} \neq \mathbf{0}$, e $\mathrm{N}(l_{k_0}) = d^2_{\min}(\Lambda_{i_0})$ implica que $N(\mathbf{l}) = d_H(C_{i_0})d^2_{\min}(\Lambda_{i_0})$. Com isso, obtemos

$$M^{(i_0)}(\mathbf{c}_{i_0}) = \sum_{\substack{\mathbf{c}_j \in C_j \\ w_H(\mathbf{c}_j * \mathbf{c}_{i_0}) = w_H(\mathbf{c}_j) \\ i_0 < j \leq m-1}} \left[\prod_{\substack{k_0 = 1 \\ c_{i_0 k_0} \neq 0}}^{n} E^{(i_0)} \left(\sum_{s=i_0}^{m-1} (c_{s k_0} g_s) + \Lambda_m \right) \right],$$

se $0 \leq i_0 < m-1$, onde $E^{(i_0)}(X)$ é o número de vetores em X com norma igual a $d^2_{\min}(\Lambda_{i_0})$. Quando $i_0 = m-1$, a expressão acima reduz-se a

$$M^{(m-1)}(\mathbf{c}_{m-1}) = \prod_{\substack{k_0 = 1 \\ c_{(m-1)k_0} \neq 0}}^{n} E^{(m-1)} \left(c_{(m-1)k_0} g_{m-1} + \Lambda_m \right) = E(\Lambda_{m-1})^{d_H(C_{m-1})}.$$

Portanto, em qualquer caso chegaremos ao resultado. ∎

Note que, no caso geral, o cálculo do coeficiente de erro $E(\mathbf{L}_{Nn})$ do reticulado $\mathbf{L}_{Nn}$ em $\mathbb{R}^{Nn}$ é feito através de sua função $\theta_{\mathbf{L}_{Nn}}(z)$, isto é,

$$\theta_{\mathbf{L}_{Nn}}(z) = \sum_{j=1}^{K} \sum_{\lambda \in \Lambda^n_m} q^{\mathrm{N}(\lambda + \mathbf{h}_j - \mathbf{h}_1)},$$

onde $q = e^{i\pi z}$, $\mathbf{h}_j \in \left\{ \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \mathbf{g}_i) : \mathbf{c}_i \in C_i \right\}$ e $K = \prod_{i=0}^{m-1} |C_i|$, pois $\mathbf{L}_{Nn}$ é um empacotamento periódico.

Com o propósito de comparação, será conveniente normalizar o coeficiente de erro para duas dimensões, isto é,

$$\tilde{E}(\mathbf{L}_{Nn}) \triangleq \frac{2}{Nn} E(\mathbf{L}_{Nn}).$$

Como o empacotamento esférico $\mathbf{L}_{Nn}$ em $\mathbb{R}^{Nn}$ é periódico, a densidade $\mathbf{L}_{Nn}$ é dada por

$$\Delta(\mathbf{L}_{Nn}) \triangleq \prod_{i=0}^{m-1} |C_i| \, \frac{V(\mathbf{E}_\rho(0))}{V(\Lambda_m)^n},$$

onde $\rho = \frac{1}{2} d_{\min}(\mathbf{L}_{Nn})$ e, consequentemente, a densidade de centro de $\mathbf{L}_{Nn}$ é dada por

$$\delta(\mathbf{L}_{Nn}) \triangleq \prod_{i=0}^{m-1} |C_i| \, \frac{\rho^{Nn}}{V(\Lambda_m)^n},$$

O ganho de codificação fundamental do empacotamento esférico $\mathbf{L}_{Nn}$ em $\mathbb{R}^{Nn}$ é dado, (cf. [14]), por

$$\gamma(\mathbf{L}_{Nn}) \triangleq \frac{d^2_{\min}(\mathbf{L}_{Nn})}{[V(\mathbf{L}_{Nn})]^{\frac{2}{Nn}}},$$

onde $V(\mathbf{L}_{Nn})$ é o volume da região de Voronoi em $\mathbf{L}_{Nn}$. Para calcular o ganho de codificação fundamental devemos encontrar o volume de uma região de Voronoi de $\mathbf{L}_{Nn}$. Como $\mathbf{L}_{Nn}$ é periódico, basta considerar apenas um período, o qual corresponde a uma região congruente à região fundamental básica de Λ_m^{Nn}, pois $\mathbf{L}_{Nn}$ é a união de $\prod_{i=0}^{m-1} |C_i|$ classes laterais à esquerda de Λ_m^{Nn}. Assim, esta região contém $\prod_{i=0}^{m-1} |C_i|$ centros de esferas, uma vez que as regiões de Voronoi destes centros cobrem esta região. Desse modo, temos que

$$V(\mathbf{L}_{Nn}) = \frac{V(\Lambda_m^n)}{\prod_{i=0}^{m-1} |C_i|} = \frac{V(\Lambda_m)^n}{\prod_{i=0}^{m-1} |C_i|}.$$

Portanto, o ganho de codificação fundamental de $\mathbf{L}_{Nn}$ é dado por

$$\gamma(\mathbf{L}_{Nn}) = \left(\prod_{i=0}^{m-1} |C_i| \right)^{\frac{2}{Nn}} \frac{d^2_{\min}(\mathbf{L}_{Nn})}{V(\Lambda_m)^{\frac{2}{N}}}.$$

Neste caso, temos a seguinte relação

$$\delta(\mathbf{L}_{Nn}) = \left(\frac{\gamma(\mathbf{L}_{Nn}}{4} \right)^{\frac{Nn}{2}}.$$

Note que, o ganho de codificação fundamental $\gamma(\mathbf{L}_{Nn})$ mede uma componente do ganho de potência que pode ser alcançado usando uma constelação de sinal S baseada no reticulado $\mathbf{L}_{Nn}$ relativo a uma constelação de sinal baseada em $\mathbb{Z}^{Nn}$. A outra componente, o ganho de fórmula, que depende da forma da constelação, não é considerada bem como o ganho não assintótico.

5.3 Decodificação de reticulados

Com o propósito de completude, apresentamos nesta seção o algoritmo de decodificação, (cf. [10]), para os empacotamentos esféricos $\mathbf{L}_{Nn}$ de $\mathbb{R}^{Nn}$ obtidos com a construção multicamada da Seção 5.2. Este algoritmo pode ser usado para a quantização de vetores e/ou para a decodificação de códigos reticulados, isto é, um subconjunto finito de pontos de um reticulado, para um canal Gaussiano. Para maiores detalhes sobre codificações e algoritmos de decodificações de reticulados, (cf. [8] ou [9]).

Um *algoritmo de decodificação por máxima verossimilhança* ou *simplesmente algoritmo ML* para um reticulado Γ em $\mathbb{R}^N$ é um algoritmo que, dado $\mathbf{x} \in \mathbb{R}^N$, encontra um ponto de Γ mais próximo de $\mathbf{x}$ do que qualquer outro ponto de Γ, isto é, dado $\mathbf{x} \in \mathbb{R}^N$ existe $\lambda \in \Gamma$ tal que $\mathbf{N}(\mathbf{x}-\lambda) \leq \mathbf{N}(\mathbf{x}-\lambda')$ para todo $\lambda' \in \Gamma$, $\lambda \neq \lambda'$. Assim, uma região de decisão de um algoritmo de decodificação por ML para Γ é essencialmente uma região de Voronoi para Γ, salvo ambiguidade envolvida em resolver empate na fronteira. Note que, se $\Phi(\lambda)$ é o ponto mais próximo de Γ para $\mathbf{x} \in \mathbb{R}^N$, então $\mathbf{r} + \Phi(\lambda - \mathbf{r})$ é o ponto mais próximo de $\mathbf{r} + \Gamma$ para $\mathbf{x} \in \mathbb{R}^N$. Portanto, um algoritmo de decodificação por ML de um reticulado Γ pode ser usado como um algoritmo de decodificação por ML de uma translação de Γ. Como a medida de distância de um reticulado Γ em $\mathbb{R}^N$ é invariante por translação temos que o algoritmo por ML para Γ em $\mathbb{R}^N$ é invariante por translação.

Exemplo 5.3.1 [8] *Sejam Λ e Γ reticulados em $\mathbb{R}^N$ tais que*

$$\Gamma = \bigcup_{i=0}^{m-1} \{\mathbf{g}_i + \Lambda\},$$

onde $m = [\Gamma : \Lambda]$ e $g_i \in [\Gamma/\Lambda], 0 \leq i \leq m-1$.

Seja Φ um decodificador para Λ. Para decodificar Γ procedemos como segue: dado $\mathbf{r} \in \mathbb{R}^N$, calcule $\mathbf{r}_i = \mathbf{r} - \mathbf{g}_i$, $\mathbf{s}_i = \Phi(\mathbf{r}_i)$ e $d_i = \mathbf{N}(\mathbf{s}_i - \mathbf{r}_i)$, $0 \leq i \leq m-1$. Seja $i = i_0$ o índice tal que d_{i_0} é minimizada. Então a saída decodificada é $\widehat{\lambda} = \mathbf{s}_{i_0} + \mathbf{g}_{i_0} \in \Gamma$. Neste caso, a complexidade de decodificação do algoritmo para Γ, $N_D(C)$, (o número de operações binárias ou comparações de dois números) é dada aproximadamente por $(m-1)N$ etapas para calcular $\mathbf{r}_i$, mais $m\mathbf{N}_D(\Lambda)$, onde $\mathbf{N}_D(\Lambda)$ é a complexidade de Λ, e mais $2mN$ para calcular d_i, isto é,

$$\mathbf{N}_D(\Gamma) = m\mathbf{N}_D(\Lambda) + (m-1)N + 2mN.$$

■

Seja C um *codificador reticulado*, formado pelos pontos de um reticulado Γ ou de uma translação $\mathbf{r}+\Gamma$ (onde $\mathbf{r} \in \mathbb{R}^N$ é escolhido de modo que $\mathbf{r}+\Gamma$ seja simétrico com relação a origem $\mathbf{0} \in \mathbb{R}^N$) dentro de um politopo $\mathbf{P}$ (um *politopo* é uma região convexa, compacta e simétrica em relação a $\mathbf{0} \in \mathbb{R}^N$ que é uma interseção finita de hiperplanos). Assim, quando $V(\mathbf{P}) \gg V(\Gamma)$, isto é, quando o número $V(\mathbf{P})/V(\Gamma)$ de pontos da constelação de sinais é bastante grande, o *ganho nominal* de C é dado, (cf. [10]), em $[dB]$ por

$$\gamma(C) \triangleq \gamma(\Gamma) + \gamma(\mathbf{P}),$$

onde $\gamma(\mathbf{P})$ é o *ganho de forma* de $\mathbf{P}$ que é dado por

$$\gamma(\mathbf{P}) \triangleq \frac{1}{12G(\mathbf{P})},$$

onde

$$G(\mathbf{P}) \triangleq \frac{E}{2V(\mathbf{P})^{\frac{2}{N}}}$$

é o *segundo momento normalizado* de $\mathbf{P}$ e E é a enérgia média em $\mathbf{P}$.

Para uma dada probabilidade de erro P_e, digamos $P_e = 10^{-6}$, tal que

$$E(\Gamma) \ll \frac{1}{P_e}, \quad N \ll \frac{1}{P_e}$$

a *perda pelo coeficiente de erro* de um reticulado Γ em $\mathbb{R}^N$ é dada, (cf. [10]), em $[dB]$ por

$$\eta(\Gamma) \triangleq -\frac{3.01}{\ln(P_e)} \log_2 \left(\frac{E(\Gamma)}{2N} \right).$$

consequentemente, o *ganho efetivo de codificação* do reticulado Γ em $\mathbb{R}^N$ é dado em $[dB]$ por

$$\gamma_e(\Gamma) \triangleq \gamma(\Gamma) - \eta(\Gamma).$$

Note que, $E(C) \approx E(\Gamma)$ para $V(\mathbf{P}) \gg V(\Gamma)$ e $P_e = 10^{-6}$ e, neste caso, $\eta(C) \approx \eta(\Gamma)$. Portanto, em $[dB]$

$$\gamma_e(C) \approx \gamma_e(\Gamma) + \gamma(\mathbf{P}).$$

Um *algoritmo de decodificação com distância limitada* para um empacotamento esférico Γ em $\mathbb{R}^N$ é um algoritmo com a seguinte propriedade: dado $\mathbf{x} \in \mathbb{R}^N$ se existe $\lambda \in \Gamma$ tal que $\mathbf{N}(x-\lambda) < d^2_{\min}(\Gamma)/4$, então $\mathbf{x}$ será decodificado como λ. A seguir apresentamos um algoritmo de decodificação com distância limitada ou algoritmo de decodificação por estágio, (cf. [10]), para os empacotamentos esféricos $\mathbf{L}_{Nn}$ em $\mathbb{R}^{Nn}$ obtidos através da construção proposta na Seção 5.2.

Algoritmo A^a: Dado $\mathbf{r} \in \mathbb{R}^{nN}$.

Passo 0. Faça $\mathbf{r}_0 = \mathbf{r}$ e decodifique $\mathbf{r}_0$ no ponto $(\widehat{c}_0 \otimes \mathbf{g}_0) + \widehat{\lambda}_1$ mais próximo do reticulado $\Gamma_0 = (C_0 \otimes [\Lambda_0/\Lambda_1]) + \Lambda_1^n$ em $\mathbb{R}^{nN}$;

Passo 1. Faça $\mathbf{r}_1 = \mathbf{r}_0 - (\widehat{c}_0 \otimes \mathbf{g}_0)$ e decodifique $\mathbf{r}_1$ no ponto $(\widehat{c}_1 \otimes \mathbf{g}_1) + \widehat{\lambda}_2$ mais próximo do reticulado $\Gamma_1 = (C_1 \otimes [\Lambda_1/\Lambda_2]) + \Lambda_2^n$ em $\mathbb{R}^{nN}$;

$\vdots$

Passo (m-1). Faça $\mathbf{r}_{m-1} = \mathbf{r}_{m-2} - (\widehat{c}_{m-2} \otimes \mathbf{g}_{m-2})$ e decodifique $\mathbf{r}_{m-1}$ no ponto $(\widehat{c}_{m-1} \otimes \mathbf{g}_{m-1}) + \widehat{\lambda}_m$ mais próximo do reticulado $\Gamma_{m-1} = (C_{m-1} \otimes [\Lambda_{m-1}/\Lambda_m]) + \Lambda_m^n$ em $\mathbb{R}^{nN}$.

Portanto, $\mathbf{r}$ será decodificado como $\widehat{l} = \widehat{U}B + \widehat{\lambda}_m \in \mathbf{L}_{Nn}$, pois $\mathbf{r}_{m-1} = \mathbf{r}_0 - \sum_{i=0}^{m-2}(\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i)$.

O próximo resultado é uma extensão para o empacotamento esférico $\mathbf{L}_{Nn}$ de um resultado semelhante para reticulados em [10].

Lema 5.3.1 *Se $q_i = q$ e os códigos C_i, $0 \leq i \leq m-1$, são lineares, então o algoritmo A^a é invariante por translação.*

Prova. Seja $\widehat{\mathbf{l}} = \sum_{i=0}^{m-1}(\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i) + \widehat{\lambda}_m \in \mathbf{L}_{Nn}$ o resultado da decodificação de $\mathbf{r} \in \mathbb{R}^{nN}$ pelo algoritmo A^a. Dado $\mathbf{l} \in \mathbf{L}_{Nn}$, devemos mostrar que o algoritmo A^a decodifica $\mathbf{r}' = \mathbf{r} + \mathbf{l}$ em $\widehat{\mathbf{l}}' = \widehat{\mathbf{l}} + \mathbf{l}$, para todo $\mathbf{l} \in \mathbf{L}_{Nn}$.

Seja $\mathbf{l} = \sum_{i=0}^{m-1}(\mathbf{c}_i \otimes \mathbf{g}_i) + \lambda_m \in \mathbf{L}_{Nn}$. Então, fazendo

$$\mathbf{l}_{i+1} = \sum_{j=0}^{i-1}[(\widehat{\mathbf{c}}_j \circ \mathbf{c}_j) \otimes (q\mathbf{g}_j)] + \sum_{j=i+1}^{m-1}(\mathbf{c}_j \otimes \mathbf{g}_j) + \lambda_m, \quad 0 < i \leq m-1,$$

$\mathbf{l}_1 = \sum_{i=1}^{m-1}(\mathbf{c}_i \otimes \mathbf{g}_i) + \lambda_m$ e $\mathbf{l}_i = (\mathbf{c}_i \otimes \mathbf{g}_i) + \mathbf{l}_{i+1}$, obtemos

$$\mathbf{l}_i \in \Gamma_i = (C_i \otimes [\Lambda_i/\Lambda_{i+1}]) + \Lambda_{i+1}^n,$$

pois $\mathbf{l}_{i+1} \in \Lambda_{i+1}^n$, desde que $q\Lambda_0 \subseteq \Lambda_{j+1}$, $0 \leq j \leq i-1$.

Agora mostraremos, por indução sobre i, que na aplicação do algoritmo A^a, a decodificação de $\mathbf{r}' = \mathbf{r} + \mathbf{l}$ é dada por $\mathbf{r}'_i = \mathbf{r}_i + \mathbf{l}_i$. De fato,

(1) se $i = 0$, então $\mathbf{r}'_0 = \mathbf{r}$, $\mathbf{r}_0 = \mathbf{r}$ e $\mathbf{l}_0 = \mathbf{l}$, $\mathbf{l}_1 = \sum_{i=1}^{m-1}(\mathbf{c}_i \otimes \mathbf{g}_i) + \lambda_m$;

(2) suponhamos que o resultado seja válido para todos i e k tal que $0 \leq k \leq i$ implica que $\mathbf{r}'_k = \mathbf{r}_k + \mathbf{l}_k$. Se $\mathbf{r}_i$ é decodificado por ML no ponto mais próximo $(\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i) + \widehat{\lambda}_{i+1}$ do reticulado Γ_i, então

$\mathbf{r}'_i = \mathbf{r}_i + \mathbf{l}_i$ será decodificado por ML no ponto mais próximo $(\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i) + \widehat{\lambda}_{i+1} + \mathbf{l}_i$ de Γ_i, pois o algoritmo ML é sempre invariante por translação. Como

$$\begin{aligned}(\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i) + \widehat{\lambda}_{i+1} + \mathbf{l}_i &= [(\widehat{\mathbf{c}}_i + \mathbf{c}_i) \otimes \mathbf{g}_i] + \widehat{\lambda}_{i+1} + \mathbf{l}_{i+1} \\ &= (\widehat{\mathbf{c}}'_i \otimes \mathbf{g}_i) + \widehat{\lambda}'_{i+1},\end{aligned}$$

onde $\widehat{\mathbf{c}}'_i = \widehat{\mathbf{c}}_i \oplus c_i \in C_i$ e $\widehat{\lambda}'_{i+1} = \widehat{\lambda}_{i+1} + \mathbf{l}_{i+1} + ((\widehat{\mathbf{c}}_i \circ \mathbf{c}_i) \otimes (q\mathbf{g}_i)) \in \Lambda^n_{i+1}$, temos que

$$\mathbf{r}'_{i+1} = \mathbf{r}'_i - (\widehat{\mathbf{c}}'_i \otimes \mathbf{g}_i).$$

Assim, pela hipotése de indução

$$\begin{aligned}\mathbf{r}'_{i+1} &= \mathbf{r}_i + \mathbf{l}_i - (\widehat{\mathbf{c}}'_i \otimes \mathbf{g}_i) \\ &= \mathbf{r}_{i+1} + [\mathbf{l}_{i+1} + ((\widehat{\mathbf{c}}_i \circ \mathbf{c}_i) \otimes (q\mathbf{g}_i))] \\ &= \mathbf{r}_{i+1} + [\mathbf{l}_{i+2} + (\mathbf{c}_{i+1} \otimes \mathbf{g}_{i+1}) \\ &= \mathbf{r}_{i+1} + \mathbf{l}_{i+1}.\end{aligned}$$

Logo, $\mathbf{r}'$ fica decodificado no ponto $\widehat{\mathbf{l}}' = \sum_{i=0}^{m-1}(\widehat{\mathbf{c}}'_i \otimes \mathbf{g}_i) + \widehat{\lambda}'_m$.

Portanto, $\widehat{\mathbf{l}}' = \widehat{\mathbf{l}} + \mathbf{l}$, uma vez que $\widehat{\mathbf{c}}'_i = \widehat{\mathbf{c}}_i \oplus c_i - q(\widehat{\mathbf{c}}_i \circ \mathbf{c}_i)$, $0 \leq i \leq m-1$ e $\widehat{\lambda}'_m = \widehat{\lambda}_m + \mathbf{l}_m + ((\widehat{\mathbf{c}}_{m-1} \circ \mathbf{c}_{m-1}) \otimes (q\mathbf{g}_{m-1}))$. ■

Teorema 5.3.1 *Dado* $\mathbf{r} \in \mathbb{R}^{Nn}$, *se* $C_0 \subseteq \cdots \subseteq C_{m-1}$, $q_i = q$, $0 \leq i \leq m-1$, *e existe* $\mathbf{l} \in \mathbf{L}_{Nn}$ *tal que* $\mathrm{N}(\mathbf{r} - \mathbf{l}) < \frac{d^2_{\min}(\mathbf{L}_{Nn})}{4}$, *então* $\mathbf{r}$ *será decodificado corretamente pelo algoritmo* A^a.

Prova. Pelo Lema 5.3.1, basta mostrar o caso em que $\mathbf{l} = \mathbf{0}$, isto é, $\mathrm{N}(\mathbf{r}) < \frac{d^2_{\min}(\mathbf{L}_{Nn})}{4}$. Como o primeiro passo do algoritmo A^a decodifica $\mathbf{r} = \mathbf{r}_0$ no ponto mais próximo $(\widehat{\mathbf{c}}_0 \otimes \mathbf{g}_0) + \widehat{\lambda}_1 \in \Gamma_0$ e

$$\mathrm{N}(\mathbf{r}_0 - ((\widehat{\mathbf{c}}_0 \otimes \mathbf{g}_0) + \widehat{\lambda}_1)) \leq \mathrm{N}(\mathbf{r}_0) < \frac{1}{4}d^2_{\min}(\mathbf{L}_{Nn}) \leq \frac{1}{4}d_H(C_0)d^2_{\min}(\Lambda_0)$$

temos que

$$\begin{aligned}\mathrm{N}((\widehat{\mathbf{c}}_0 \otimes \mathbf{g}_0) + \widehat{\lambda}_1) &\leq [\mathrm{N}(\mathbf{r}_0 - ((\widehat{\mathbf{c}}_0 \otimes \mathbf{g}_0) + \widehat{\lambda}_1))^{\frac{1}{2}} + \mathrm{N}(\mathbf{r}_0)^{\frac{1}{2}}]^2 \\ &< d_H(C_0)d^2_{\min}(\Lambda_0) = d^2_{\min}(\Gamma_0).\end{aligned}$$

O único ponto de Γ_0 com norma menor do que $d^2_{\min}(\Gamma_0)$ é o vetor $\mathbf{0}$, logo $\widehat{\mathbf{c}}_0 \otimes \mathbf{g}_0 = \widehat{\lambda_1} = \mathbf{0}$ e $\mathbf{r}_1 = \mathbf{r}_0$.

Como o i-ésimo passo do algoritmo A^a decodifica $\mathbf{r}_i$ no ponto mais próximo $(\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i) + \widehat{\lambda}_{i+1} \in \Gamma_i$. De modo análogo, mostra-se que

$$\mathrm{N}((\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i) + \widehat{\lambda}_{i+1}) < d_H(C_i)d^2_{\min}(\Lambda_i) = d^2_{\min}(\Gamma_i), \ 1 \leq i < m-1.$$

Logo, $\widehat{\mathbf{c}}_i \otimes \mathbf{g}_i = \widehat{\lambda}_i = \mathbf{0}$ e $\mathbf{r}_{i+1} = \mathbf{r}_i$, $1 \leq i < m-1$. Finalmente, como

$$\mathbf{N}(\mathbf{r}_{m-1} - \widehat{\lambda}_m) \leq \mathbf{N}(\mathbf{r}_{m-1}) < \frac{1}{4} d^2_{\min}(\mathbf{L}_{Nn}) \leq \frac{1}{4} d^2_{\min}(\Lambda_m)$$

temos que

$$\mathbf{N}(\widehat{\lambda}_m) < d^2_{\min}(\Lambda_m).$$

Logo, $\widehat{\lambda}_m = \mathbf{0}$. Portanto, $\widehat{\mathbf{l}} = \mathbf{l} = \mathbf{0}$. ■

Note que na prova do Teorema 5.3.1 não usamos que $\mathbf{L}_{Nn}$ é um reticulado. O conjunto de pontos $\mathbf{r} \in \mathbb{R}^{Nn}$ que mapeia para o ponto $\mathbf{0}$ é chamado a *região de decisão*, isto é,

$$R^a(\mathbf{0}) = \{\mathbf{r} \in \mathbb{R}^{Nn} : \mathbf{N}(\mathbf{r}) \leq d^2_{\min}(\mathbf{L}_{Nn})/4\},$$

do algoritmo A^a. Pelo Lema 5.3.1, todas as regiões de decisão $R^a(\mathbf{l})$ são congruentes e, $R^a(\mathbf{l}) = \mathbf{l} + R^a(\mathbf{0})$ para todo $\mathbf{l} \in \mathbf{L}_{Nn}$. Neste caso, $R^a(\mathbf{0})$ é uma região fundamental para $\mathbf{L}_{Nn}$. Como as esferas $E_\rho(\mathbf{0})$ de centro $\mathbf{0} \in \mathbf{L}_{Nn}$ e raio $\rho = d_{\min}(\mathbf{L}_{Nn})/2$, deve tocar-se, temos que existem pontos de norma igual a ρ^2 na fronteira de $R^a(\mathbf{0})$. O número de pontos na fronteira de $R^a(\mathbf{0})$ com norma igual a ρ^2 é o *coeficiente de erro efetivo* de $\mathbf{L}_{Nn}$ e, denotaremos por $E_e(L_{Nn})$, em geral, $E_e(\mathbf{L}_{Nn}) \geq E(\mathbf{L}_{Nn})$. Assim, A^a é um algoritmo sub-ótimo ou decodificação com distância limitada para o empacotamento esférico $\mathbf{L}_{Nn}$ em $\mathbb{R}^{Nn}$.

O próximo resultado é uma extensão para o reticulado $\mathbf{L}_{Nn}$ de um resultado semelhante para reticulados em [10]. Com o propósito de completute apresentamos a sua demonstração, embora seja mais geral.

Teorema 5.3.2 *[10] Se $C_0 \subseteq \cdots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então o coeficiente de erro efetivo $E_e(\mathbf{L}_{Nn})$ é dado por*

$$E_e(\mathbf{L}_{Nn}) = \sum_{d^2_{\min}(\mathbf{L}_{Nn}) = d_H(C_i) d^2_{\min}(\Lambda_i)} (E(C_i)E(\Lambda_{i+1}))^{d_H(C_i)} + E_m,$$

onde

$$E_m = \begin{cases} nE(\Lambda_m), & se\ d^2_{\min}(\Lambda_m) = d^2_{\min}(\mathbf{L}_{Nn}) \\ 0, & se\ d^2_{\min}(\Lambda_m) > d^2_{\min}(\mathbf{L}_{Nn}) \end{cases}.$$

Prova. O coeficiente de erro efetivo é o número de pontos na fronteira da região de decisão $R^a(\mathbf{0})$ com norma igual a ρ^2, os quais é o número de pontos $\mathbf{l}$ em $\mathbf{L}_{Nn}$ com $\mathbf{N}(\mathbf{l}) = \mathbf{d}^2_{\min}(\mathbf{L}_{Nn})$. Assim, como

$d^2_{\min}(\mathbf{L}_{Nn}) = \min_{0\le i\le m-1}\{d_H(C_i)d^2_{\min}(\Lambda_i), d^2_{\min}(\Lambda_m)\}$ e para $\mathbf{l}\in\mathbf{L}_{Nn}$, $\mathbf{l}\neq\mathbf{0}$, $\mathbf{N}(\mathbf{l}) = \mathbf{d}^2_{\min}(\mathbf{L}_{Nn})$ se, e somente se, $w_H(\mathbf{c}_i) = d_H(C_i)$ e $d^2_{\min}(\mathbf{L}_{Nn}) = d_H(C_i)d^2_{\min}(\Lambda_i) = d^2_{\min}(\Gamma_i)$, $0\le i\le m-2$, temos que

$$E_e(\Gamma_i) = \begin{cases} (E(C_i)E(\Lambda_{i+1}))^{d_H(C_i)}, & \text{se } d^2_{\min}(\Gamma_i) = d^2_{\min}(\mathbf{L}_{Nn}) \\ 0, & \text{se } d^2_{\min}(\Gamma_i) > d^2_{\min}(\mathbf{L}_{Nn}) \end{cases}.$$

$$E_e(\Gamma_{m-1}) = \begin{cases} (E(C_{m-1})E(\Lambda_m))^{d_H(C_{m-1})}, & \text{se } d_1 = d_2 < d_3 \\ nE(\Lambda_m), & \text{se } d_1 > d_2 = d_3 \\ (E(C_{m-1})E(\Lambda_m))^{d_H(C_{m-1})} + nE(\Lambda_m), & \text{se } d_1 = d_2 = d_3 \\ 0, & \text{se } d_1 < d_2 < d_3 \end{cases},$$

onde $d_1 = d^2_{\min}(\Gamma_{m-1})$, $d_2 = d^2_{\min}(\mathbf{L}_{Nn})$ e $d_3 = d^2_{\min}(\Lambda_m)$. Portanto, completamos à prova. ■

Agora apresentamos o cálculo aproximado da complexidade de decodificação do algoritmo A^a para $\mathbf{L}_{Nn}$. Para maiores detalhes e exemplos, (cf. [10]).

Primeiro. Dado $\mathbf{r}_i = (\mathbf{r}_{i1},\ldots,\mathbf{r}_{in})$, $\mathbf{r}_{ij}\in\mathbb{R}^N$, $0\le i\le m-1$, $1\le j\le n$, então para cada $i = 0,\ldots,m-1$, o algoritmo escolhe um $c_{ij}\in\mathbb{N}_{q_i}$ que esteja mais próximo de cada uma das componentes $\mathbf{r}_{ij}$ de $\mathbf{r}_i$, $1\le j\le n$, isto é,

$$d_{ij} \triangleq \min\left\{\mathbf{N}(\mathbf{r}_{ij} - ((c_{ij}\mathbf{g}_i) + \lambda_{(i+1)j}))\right\}.$$

Note que d_{ij} é a mínima distância Euclidiana quadrática de cada classe lateral à esquerda de Λ_{i+1} em Λ_i da componente recebida $\mathbf{r}_{ij}$, $1\le j\le n$.

Segundo. Para cada $i = 0,\ldots,m-1$, seja $\tilde{\mathbf{c}}_i = (\tilde{c}_{i1},\ldots,\tilde{c}_{in})$ uma aproximação para a palavra-código $\mathbf{c}_i = (c_{i1},\ldots,c_{in})\in C_i$. Então um algoritmo de decodificação suave para decodificar C_i, (cf. apêndice de [15] ou [35]), é usado para corrigir erros em $\tilde{\mathbf{c}}_i$, e a palavra resultante é uma palavra-código $\hat{\mathbf{c}}_i\in C_i$. isto é,

$$d_i \triangleq \min\left\{\mathbf{N}(\mathbf{r}_i - ((\mathbf{c}_i\otimes\mathbf{g}_i) + \lambda_{i+1}))\right\}.$$

Como a norma é uma medida de distância aditiva e

$$\min(\sum_{i=0}^{m-1} X_i) = \sum_{i=0}^{m-1}(\min X_i),$$

temos que

$$d_i = \sum_{j=1}^{n} d_{ij},\ 0\le i\le m-1.$$

Finalmente, como o algoritmo A^a para $\mathbf{L}_{Nn}$ usa apenas a palavra código $\mathbf{c}_i \in C_i$ para minimizar d_i e

$$\begin{aligned}\Gamma_i &= \{\mathbf{c}_i \otimes \mathbf{g}_i : \mathbf{c}_i \in C_i\} + \Lambda_{i+1}^n = \bigcup_{\mathbf{c}_i \in C_i} (\mathbf{c}_i \otimes \mathbf{g}_i + \Lambda_{i+1}^n) \\ &= \bigcup_{\mathbf{c}_i \in C_i} \{(c_{i1}\mathbf{g}_i + \lambda_{i1}, \ldots, c_{in}\mathbf{g}_i + \lambda_{in}) : \lambda_{ij} \in \Lambda_{i+1}\}, 0 \leq i \leq m-1,\end{aligned}$$

a complexidade para decodificar Γ_i é dada aproximadamente por

$$\mathbf{N}_D(\Gamma_i) = n\left(\mathbf{N}_D(\Lambda_i/\Lambda_{i+1}) + 1\right) + \mathbf{N}_D(C_i),$$

onde $\mathbf{N}_D(\Lambda_i/\Lambda_{i+1})$ é a complexidade do algoritmo por ML usado para decodificar a partição Λ_i/Λ_{i+1}, (cf. apêndice [15]), e $\mathbf{N}_D(C_i)$ é a complexidade do algoritmo com decisão suave por ML usado para decodificar C_i. Portanto, a complexidade para o algoritmo A^a para $\mathbf{L}_{Nn}$ é dada por

$$\mathbf{N}_D^a(\mathbf{L}_{Nn}) \triangleq \sum_{i=0}^{m-1} \mathbf{N}_D(\Gamma_i) + mnN,$$

onde mnN refere-se aos passos do algoritmo A^a que calcula cada $\mathbf{r}_i$ a ser decodificado em relação a Γ_i, no passo subsequente. A complexidade normalizada é dada por

$$\tilde{\mathbf{N}}_D^a(\mathbf{L}_{Nn}) = \frac{2}{nN}\mathbf{N}_D^a(\mathbf{L}_{Nn}).$$

A relação de degradação de desempenho em $[dB]$ por redução de complexidade em [oitavas], (cf. [10]), do reticulado $\mathbf{L}_{Nn}$ é dada por

$$\beta(\mathbf{L}_{Nn}) \triangleq -\frac{\Delta(\mathbf{L}_{Nn})}{\log_2\left(\frac{\mathbf{N}_D^a(\mathbf{L}_{Nn})}{\mathbf{N}_D(\mathbf{L}_{Nn})}\right)} \text{ e } \Delta(\mathbf{L}_{Nn}) \approx 0.22 \log_2\left(\frac{E_e(\mathbf{L}_{Nn})}{E(\mathbf{L}_{Nn})}\right).$$

Note que um algoritmo de decodificação misto pode alcançar o melhor compromisso entre desempenho e complexidade, isto é, no primeiro passo do algoritmo A^a usamos um decodificador com desisão suave por ML e um decodificador com decisão abrupta sub-ótimo nos passos subsequentes. Para comparações do algoritmo A^a com outros algoritmos, (cf. [9]).

5.4 Exemplos

Nesta seção apresentaremos alguns exemplos de empacotamentos esféricos como ilustrações da construção multicamada da Seção 5.2 e obteção de seus principais parâmetros. Em dimensões 68 e 72, novo recorde de densidades parece ter sido alcançado. Para mais exemplos e comparações, (cf. [10]).

Exemplo 5.4.1 *Seja* $\Lambda_0/\Lambda_1/\Lambda_2$ *uma cadeia de partições, com 2-níveis e 2-maneiras, onde* $\Lambda_0 = \mathbb{Z}^2$ *é o reticulado cúbico em* $\mathbb{R}^2$ *com uma matriz geradora*

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e $\Lambda_i = T_2^i(\Lambda_0), i = 1, 2$, *os sub-reticulados de* Λ_0 *induzidos pelo endomorfismo* T_2 *de* Λ_0 *definido pela matriz*

$$[T_2] = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

que escala Λ_0 *por* $\sqrt{2}$ *e rotaciona por* $45°$. *Neste caso,*

$\mathbf{g}_0 = (1,0)$, $\mathbf{g}_1 = (1,1)$, $d^2_{\min}(\mathbf{L}_{2n}) = \min_{0\leq i\leq 1}\{2^i d_H(C_i), 4\}, V(\mathbf{L}_{2n}) = 2^{2n-k}$ *e* $\gamma(\mathbf{L}_{2n}) = 2^{\frac{k-2n}{n}} d^2_{\min}(\mathbf{L}_{2n})$, *onde* $k = k_0 + k_1$.

(1) *Para os códigos* $C_0 = [2,1,2]_2$ *e* $C_1 = [2,2,1]_2$ *dados na Tabela-I de* [3]. *Temos,*

$$d^2_{\min}(\mathbf{L}_4) = 2, V(\mathbf{L}_4) = 2 \text{ e } \gamma(\mathbf{L}_4) = 1,51[dB],$$

$E(\mathbf{L}_4) = \sum_{w_H(\mathbf{c}_0)=d_H(C_0)} M^{(0)}(\mathbf{c}_0) + \sum_{w_H(\mathbf{c}_1)=d_H(C_1)} M^{(1)}(\mathbf{c}_1) = M^{(0)}(\mathbf{c}_0) + 2M^{(1)}(\mathbf{c}_1)$. *Para* $\mathbf{c}_0 =$ (11), *obtemos*

$$\begin{aligned} M^{(0)}(\mathbf{c}_0) &= \sum_{\mathbf{c}_1 \in C_1} \left[\prod_{k=1}^{2} E^{(0)}(c_{ok}\mathbf{g}_0 + c_{1k}\mathbf{g}_1 + \Lambda_2)\right] \\ &\quad w_H(\mathbf{c}_1 * \mathbf{c}_0) = w_H(\mathbf{c}_1) \\ &= E^{(0)}(\mathbf{g}_0 + \Lambda_2)^2 + 2E^{(0)}(\mathbf{g}_0 + \Lambda_2)E^{(0)}(\mathbf{g}_0 + \mathbf{g}_1 + \Lambda_2) + E^{(0)}(\mathbf{g}_0 + \mathbf{g}_1 + \Lambda_2)^2 \\ &= 2^2 + 2.2.2 + 2^2 = 16. \end{aligned}$$

e $M^{(1)}(\mathbf{c}_1) = E^{(1)}(\Lambda_2)^{d_H(C_1)} = 4^1 = 4$. *Logo,*

$$E(\mathbf{L}_4) = 24 \text{ e } \tilde{E}(\mathbf{L}_4) = 12.$$

$E_e(\mathbf{L}_4) = E^{(0)}(C_0)E^{(0)}(\Lambda_1)^{d_H(C_0)} + E^{(1)}(C_1)E^{(1)}(\Lambda_2)^{d_H(C_1)} = 4^2 + 2.4^1 = 24$ *e* $\tilde{E}_e(\mathbf{L}_4) = 12$.

Finalmente,

$$\begin{aligned} \mathbf{N}_D^q(\mathbf{L}_4) &= 2(\mathbf{N}_D(\Lambda_0/\Lambda_1) + 1) + \mathbf{N}_D(C_0) + 2(\mathbf{N}_D(\Lambda_1/\Lambda_2) + 1) + \mathbf{N}_D(C_1) + 8 \\ &= 6 + 4 + 6 + 2 + 8 = 26. \end{aligned}$$

Note que $\mathbf{L}_4$ *é similar ao reticulado do tabuleiro de xadrez* $\mathbf{D}_4$ *em* $\mathbb{R}^4$, (*cf.* [8]).

(2) *Para os códigos* $C_0 = [4,1,4]_2$ *e* $C_1 = [4,3,2]_2$ *dados na Tabela-I de* [3]. *Obtemos*

$$d^2_{\min}(\mathbf{L}_8) = 4,\ V(\mathbf{L}_8) = 2^4,\ \gamma(\mathbf{L}_8) = 3,01[dB],\ \widetilde{E}(\mathbf{L}_8) = 60,\ \widetilde{E}_e(\mathbf{L}_8) = 92\ e\ \mathbf{N}^a_D(\mathbf{L}_8) = 52.$$

Como $\mathbf{N}_D(\mathbf{L}_8) = 72$, (*cf.* [8]), *temos que a relação de degradação de desempenho em* $[dB]$ *por redução de complexidade em* [*oitavas*] *do reticulado* $\mathbf{L}_8$ *é dada por*

$$\beta(\mathbf{L}_8) = 0.29.$$

Note que $\mathbf{L}_8$ *é similar ao reticulado Gosset* $\mathbf{E}_8$ *em* $\mathbb{R}^8$, (*cf.* [8]). ■

Exemplo 5.4.2 *Seja* $\Lambda_0/\Lambda_1\cdots/\Lambda_m$ *uma cadeia de partições, com m-níveis e* 3- *e/ou* 4-*maneiras, onde* $\Lambda_0 = \mathbf{A}_2$ *é o reticulado hexagonal em* $\mathbb{R}^2$ *com uma matriz geradora*

$$M_0 = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

e $\Lambda_i = T_3^i(T_4^j(\Lambda_0))$, $i,j = 0,1,\ldots,m$, *os sub-reticulados de* Λ_0 *induzidos pelos endomorfismos* T_3 *e* T_4 *de* Λ_0 *definidos pelas matrizes*

$$[T_3] = \begin{bmatrix} \frac{3}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{3}{2} \end{bmatrix} \quad e \quad [T_4] = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

■

Usando as cadeias de partições do reticulado hexagonal A_2 geramos todos os empacotamentos esféricos da Tabela-VIII de [23]. Como um exemplo, seja $\Lambda_0/\Lambda_1/\Lambda_2/$ uma cadeia de partições, com 2-níveis, onde $\Lambda_0 = \mathbf{A}_2$, $\Lambda_1 = T_4(\Lambda_0)$ e $\Lambda_2 = T_3(\Lambda_1)$. Então para os códigos $C_0 = [18,9,8]_4$, $C_0' = [30,15,12]_4$ dados na Tabela-VI de [23], e $C_1 = [18,17,2]_3$, $C_1' = [30,26,3]_3$ dados na Tabela-V de [23], obtemos os empacotamento esférico $\mathbf{L}_{36}$ e $\mathbf{L}_{60}$, que são os mais densos conhecidos em suas dimensões.

Seja $\Lambda_0/\Lambda_1\cdots/\Lambda_m$ uma cadeia de partições, com m-níveis e 4-maneiras, onde $\Lambda_0 = \mathbf{D}_4$ é o reticulado do tabuleiro de xadrez em $\mathbb{R}^4$ com uma matriz geradora

$$M_0 = \begin{bmatrix} 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

e $\Lambda_i = T_4^i(\Lambda_0)$, $i = 0, 1, \ldots, m$, os sub-reticulados de Λ_0 induzidos pelo endomorfismo T_4 de Λ_0 definido pela matriz

$$[T_4] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

Usando os melhores códigos quaternários dados na Tabela-VI de [23] e a cadeia de partições do reticulado $\mathbf{D}_4$, obtemos uma variedade de empacotamentos esféricos mostrados na Tabela 5.1, onde os códigos $C_i = [n, k_i, d_i]_4$ nas quatro colunas da tabela são da Tabela-VI de [23]. Na quinta coluna o ganho de codificação fundamental $\gamma(\mathbf{L}_{Nn})$, em $[dB]$, dos nossos empacotamentos e na sexta coluna γc e γk representam o ganho de codificação fundamental, em $[dB]$, dos melhores empacotamentos da Tabela 3.1 de [8] e da Tabela-VIII de [23], respectivamente. Finalmente, na sétima coluna temos a dimensão dos empacotamentos $\mathbf{L}_{Nn}$.

Em dimensões 68 e 72, os empacotamentos esféricos obtidos na Tabela 5.1 são mais densos do que os correspondentes da Tabela VIII de [23]. As densidades de centros destes empacotamentos esféricos são $\delta(\mathbf{L}_{68}) \approx 2^{24.95}$ e $\delta(\mathbf{L}_{72}) \approx 2^{30.73}$, respectivamente. Os empacotamentos esféricos obtidos com esta construção dependem muito dos códigos e do endomorfismo a serem utilizados, uma vez que a utilização de códigos com distâncias de Hamming maiores para os primeiros níveis da partição implica em melhores empacotamento dos subcódigos para um endomorfismo apropriado. Alguns dos resultados deste capítulo foram publicados em [31]

$\mathbf{C}_0$	$\mathbf{C}_1$	$\mathbf{C}_2$	$\mathbf{C}_3$	$\gamma(\mathbf{L}_{Nn})[dB]$	$\gamma[dB]$	Nn
$[2,1,2]$	$[2,2,1]$	$[2,2,1]$	$[2,2,1]$	3.01	3.01c	$\mathbf{L}_8$
$[3,2,2]$	$[3,3,1]$	$[3,3,1]$	$[3,3,1]$	3.51	3.63c	$\mathbf{L}_{12}$
$[4,1,4]$	$[4,3,2]$	$[4,4,1]$	$[4,4,1]$	4.52	4.52c	$\mathbf{L}_{16}$
$[5,2,4]$	$[5,4,2]$	$[5,5,1]$	$[5,5,1]$	5.12	5.12c	$\mathbf{L}_{20}$
$[6,3,4]$	$[6,5,2]$	$[6,6,1]$	$[6,6,1]$	5.52	6.02c	$\mathbf{L}_{24}$
$[7,3,4]$	$[7,6,2]$	$[7,7,1]$	$[7,7,1]$	5.38	5.81c	$\mathbf{L}_{28}$
$[8,1,8]$	$[8,4,4]$	$[8,7,2]$	$[8,8,1]$	6.02	6.28c	$\mathbf{L}_{32}$
$[9,1,9]$	$[9,5,4]$	$[9,8,2]$	$[9,9,1]$	6.19	6.38k	$\mathbf{L}_{36}$
$[10,2,8]$	$[10,6,4]$	$[10,9,2]$	$[10,10,1]$	6.62	6.62c	$\mathbf{L}_{40}$
$[11,2,8]$	$[11,7,4]$	$[11,10,2]$	$[11,11,1]$	6.71	6.98c	$\mathbf{L}_{44}$
$[12,3,8]$	$[12,8,4]$	$[12,11,2]$	$[12,12,1]$	7.02	7.78c	$\mathbf{L}_{48}$
$[13,4,8]$	$[13,9,4]$	$[13,12,2]$	$[13,13,1]$	7.30	7.30k	$\mathbf{L}_{52}$
$[14,5,8]$	$[14,10,4]$	$[14,13,2]$	$[14,14,1]$	7.53	7.52k	$\mathbf{L}_{56}$
$[15,6,8]$	$[15,11,4]$	$[15,14,2]$	$[15,15,1]$	7.73	7.77k	$\mathbf{L}_{60}$
$[16,1,16]$	$[16,7,8]$	$[16,12,4]$	$[16,15,2]$	8.10	8.10c	$\mathbf{L}_{64}$
$[17,1,17]$	$[17,8,8]$	$[17,13,4]$	$[17,16,2]$	8.23	8.01k	$\mathbf{L}_{68}$
$[18,1,18]$	$[18,9,8]$	$[18,13,4]$	$[18,17,2]$	8.59	8.16k	$\mathbf{L}_{72}$
$[19,9,8]$	$[19,14,4]$	$[19,18,2]$	$[19,19,1]$	8.16	8.24k	$\mathbf{L}_{76}$
$[20,2,16]$	$[20,10,8]$	$[20,15,4]$	$[20,19,2]$	8.43	8.73c	$\mathbf{L}_{80}$
$[21,3,16]$	$[21,10,8]$	$[21,16,4]$	$[21,20,2]$	8.53	8.54k	$\mathbf{L}_{84}$
$[22,3,16]$	$[22,11,8]$	$[20,17,4]$	$[22,21,2]$	8.62	8.58k	$\mathbf{L}_{88}$
$[23,3,16]$	$[23,12,8]$	$[23,18,4]$	$[23,22,2]$	8.70	8.72k	$\mathbf{L}_{92}$
$[24,4,16]$	$[24,13,8]$	$[24,19,4]$	$[24,23,2]$	8.91	9.29c	$\mathbf{L}_{96}$
$[25,5,16]$	$[25,14,8]$	$[25,20,4]$	$[25,24,2]$	9.09	9.07k	$\mathbf{L}_{100}$

Tabela 5.1: Empacotamentos esféricos obtidos de partições do reticulado $\mathbf{D}_4$.

Capítulo 6

Conclusões

Neste trabalho foram estudados e apresentados métodos de construção de códigos geometricamente uniformes tanto no espaço Euclidiano quanto no espaço de Hamming.

Basicamente no espaço Euclidiano os grupos considerados foram os não comutativos, devido ao seu potencial de excederem o limitante do MPSK. Com relação ao espaço Euclidiano duas variantes foram analisadas. A primeira variante teve a ver com a construção de códigos, cuja cardinalidade é grande, através da composição de códigos, cujas cardinalidades são menores, baseado na proposta de Zinoviev [34] sobre concatenação generalizada. A segunda variante teve a ver com a construção de empacotamentos esféricos tendo como base a construção de reticulados proposta por Costa e Silva e Palazzo em [10]. As principais contribuições deste trabalho podem ser resumidas como segue:

No Capítulo 3, resolvemos o problema de uma constelação de sinais casada com um grupo não comutativo, o qual é o produto semidireto de um grupo comutativo por um grupo cíclico de ordem par. Também apresentamos, um algoritmo para encontrar a constelação de sinais casada com um grupo que é a extensão de dois grupos menores.

No Capítulo 4, apresentamos uma proposta de construção de uma classe de códigos de classes laterais sobre o grupo $\mathbb{Z}_q$ com expressões explícitas para os principais parâmetros destes códigos. Esta construção inclui as construções de [22, 29, 37]. Duas tabelas de códigos do espaço Euclidiano novos foram fornecidas.

No Capítulo 5, estendemos a proposta de [10] para a construção multicamada de empacotamentos esféricos ou reticulados com expressões explícitas para os principais parâmetros desses reticulados. Vários exemplos de empacotamentos esféricos foram fornecidos, mostrando novas formas de construção

de empacotamentos esféricos conhecidos e em dimensões 68 e 72, um novo recorde de densidades parece ter sido alcançado.

Propostas de novos trabalhos:

O problema de constelações de sinais é equivalente ao problema de empacotamento de uma esfera em $\mathbb{R}^N$. Por exemplo, a constelação de sinais normalizada

$$S = \left\{ \frac{1}{\sqrt{2}}(x_1, x_2, x_3, x_4) : x_i \in \{-1, 0, 1\}, \sum_{i=1}^{4} x_i \equiv 0 \pmod 2 \right\}$$

é obtida do reticulado do tabuleiro de xadrez D_4 em $\mathbb{R}^4$. Nesta direção temos as seguintes propostas:

- O Teorema 3.2.3 pode ser estendido para grupos mais gerais?
- Encontrar uma condição necessária e suficiente para que as constelações de sinais casadas com o grupo diedral D_n sejam similares as do grupo comutativo $\mathbb{Z}_{2n}$?

A relação entre códigos e empacotamentos esféricos é feita como segue: se C é um $[N, K, d]$ código sobre $\mathbb{Z}_q$, então, identificando o grupo $\mathbb{Z}_q$ com o conjunto $\{0, 1, \ldots, q-1\} \subset \mathbb{Z}$, C pode ser considerado como um empacotamento esférico em $\mathbb{R}^N$ com centros nas palavras código e raio $\rho = \lfloor \frac{d-1}{2} \rfloor$, onde a distância usada é a de Hamming. É claro que esse empacotamento é um reticulado quando C é um código linear. Neste caso, as cotas de Hamming, de Gilbert-Varshamov e de McElice-Rodemich-Ramsey-Welch, (cf. [26]), correspondem ao expoente de densidade do empacotamento, a cota de Minkowiski e a cota de Kabatyansky-Levenstein, (cf. [8]), respectivamente. Nesta direção temos as seguintes propostas:

- É possível encontrar uma cota para empacotamento esférico semelhante à de Plotkin, (cf. [26])?
- Códigos de verificação de paridade correspondem ao reticulado $\mathbf{A}_N$ ou a $\mathbf{D}_N$, (cf. [8])?
- A função θ de um reticulado corresponde a função enumeração de peso de um código linear?
- Reticulados auto-duais correspondem a códigos auto-duais?

A proposta apresentada para a construção de empacotamentos esféricos depende tanto do endomorfismo quanto dos códigos. Em Almeida [1] foi mostrado, usando métodos computacionais, como

encontrar os melhores endomorfismos em dimensões um e dois. Por exemplo, os melhores endomorfismos do reticulado cúbico $\mathbb{Z}^3$ em $\mathbb{R}^3$ podem ser obtidos da equação Diofantina:

$$x^2 + y^2 + z^2 = m,\ x, y, z \in \mathbb{Z},$$

a qual tem solução se, e somente se, $m \neq 4^n(8k + 7)$, com $n, k \in \mathbb{Z}$ e $n \geq 0$. Nesta direção temos a seguinte proposta:

- Endomorfismos de reticulados noutras dimensões podem também produzir boas partições e seria interessante investigar os empacotamentos esféricos obtidos a partir destas partições.

Bibliografia

[1] C. Almeida, *Modulação-codificada generalizada via equação de Diofanto*, Tese de Doutorado, FEE-UNICAMP, 1990.

[2] E.L. Blokh and V.V. Zyablov, "Coding of generalized cascade codes," *Probl. Peredachi Inform.*, No 3, pp. 45-50, 1974.

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

[4] A.R. Calderbank and N.J.A. Sloane, "New trellis codes based on lattices and cosets," *IEEE Trans. Inform. Theory*, vol. 33, pp. 177-195, 1987.

[5] C.E. Câmara, *Construção de códigos esféricos via d-cadeia e a geometria de grupos*, Tese de Doutorado, FEE-UNICAMP, 1995.

[6] J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, 1971.

[7] C.J. Chen, T.Y. Chen and H.-A. Loeliger, "Construction of linear ring codes for 6-PSK," *IEEE Trans. Inform. Theory*, vol. 40, pp. 563-566, 1994.

[8] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups*, New York, Springer-Verlag, 1988.

[9] M.A.O. Costa e Silva, "*Reticulados e suas partições aplicados a codificação sobre canais AWGN limitados em faixa*," Tese de Doutorado, FEE-UNICAMP, 1991.

[10] M.A.O. Costa e Silva e R. Palazzo, Jr., "A bounded-distance decoding algorithm for lattices based on generalized code formula," *IEEE Trans. Inform. Theory*, vol. 40, pp. 2075-2082, 1994.

[11] E.L. Cusack, "Error control codes for QAM signaling," *Electron. Lett.*, vol. 20, pp. 62-63, 1984.

[12] D.S. Dummit and R.M. Foote, *Abstract Algebra*, New Jersey, Prentice Hall, 1991.

[13] G.D. Forney, Jr., *Concatenades Codes*, MIT Press, Cambridge, Mass. 1966.

[14] G.D. Forney, Jr., "Coset codes I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123-1151, 1988.

[15] G.D. Forney, Jr., "Coset codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152-1187, 1988.

[16] G.D. Forney, Jr., "Coset codes III: Ternary codes, lattices and trellis codes," in preparation, 1989.

[17] G.D. Forney, Jr., "A bounded-distance decoding algorithm for the Leech lattices, with generalizations," *IEEE Trans. Inform. Theory*, vol. 35, pp. 906-909, 1989.

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

[19] G.D. Forney, Jr., "On the Hamming distance properties of group codes," *IEEE Trans. Inform. Theory*, vol.38, pp. 1797-1801, 1992.

[20] V.V. Ginzburg, "Muldimensional signals for continous Channel," *Problems Inform. Transmission*, vol. 20, pp. 20-34, 1984.

[21] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 23, pp. 371-377, 1977.

[22] F.R.Kschischang, P.G. de Buda and S. Pasupathy, "Blocks Coset codes for M-ary phase shift keying," *IEEE J. Select Area Commun.*, vol. 7, pp. 900-913, 1989.

[23] F.R.Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inform. Theory*, vol. 38, pp. 227-246, 1992.

[24] J. Leech and N.J.A. Sloane, "Sphere packings and error correcting codes," *Canad. J. Math.*, vol. 23, pp. 718-745, 1971.

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

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

[27] R. Palazzo Jr, J. C. Interlando and C. Almeida, "Constructions of signals sets matched to abelian and non-abelian groups", *Proc. IEEE Internat. Symp. on Inform. Theory*, ISIT-94, Trondhein, Norway, p. 488, 1994.

[28] P.M. Piret, "Algebraic construction of cyclic codes over $\mathbb{Z}_8$ with a good Euclidean minimum distance," *IEEE Trans. Inform. Theory*, vol. 41, pp. 815-818, 1995.

[29] J. Portugheis, *Generalized concatenated codes for MPSK modulation*, Doctoral Thesis, TH Darmstadt, 1992.

[30] S.I. Sayegh, "A class of optimum block codes in space signal," *IEEE Trans. Commun.*, vol. 34, pp. 1043-1045, 1986.

[31] A.A. e Silva e R. Palazzo, Jr., "Construção de reticulados via fórmula de códigos p-ários generalizado," $13^{\underline{o}}$ *SBT*, Águas de Lindóia, São Paulo, pp. 66-70, 1995.

[32] D. Slepian, "Group Codes for the Gaussian Channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575-602, 1968.

[33] G. Ungerboeck, "Channel codings with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol. 28, pp. 55-67, 1982.

[34] V.A. Zinoviev, "Generalized cascade codes," *Probl. Peredachi Inform.*, vol. 12, pp. 5-15,1976.

[35] J.K. Wolf, "Efficient maximum likelihood decoding of linear block codes using trellis," *IEEE Trans. Inform. Theory*, vol. 24, pp. 76-80,1978.

[36] J.M. Wozencraft and I.M. Jacobs, *Principles of Communication Engineering.* New York: Wiley, 1965.

[37] J. Wu and D.J. Costello, Jr., "New multilevel codes over $GF(q)$," *IEEE Trans. Inform. Theory*, vol. 38, pp. 933-939,1992.