Luciana Yoshie Tsuchiya

Um estudo de reticulados q-ários com a métrica da soma

Campinas
2012

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e
Computação Científica - IMECC
Departamento de Matemática

Luciana Yoshie Tsuchiya

Um estudo de reticulados q-ários com a métrica da soma

Dissertação de mestrado apresentada ao Instituto de Matemática, Estatística e Computação Científica da UNICAMP para obtenção do título de Mestre em Matemática.

Orientadora: Sueli Irene Rodrigues Costa

Este exemplar corresponde à versão final da dissertação defendida por Luciana Yoshie Tsuchiya e orientada pela Profa. Dr.a Sueli Irene Rodrigues Costa.

Profa. Dra. Sueli Irene Rodrigues Costa

Campinas, 2012

FICHA CATALOGRÁFICA ELABORADA POR
ANA REGINA MACHADO - CRB8/5467
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

Tsuchiya, Luciana Yoshie, 1977 -
T789e Um estudo de reticulados q-ários com a métrica da soma / Luciana Yoshie Tsuchiya. - Campinas, SP : [s.n.], 2012.

Orientador: Sueli Irene Rodrigues Costa.
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Métrica de Lee. 2. Geometria discreta. 3. Teoria dos reticulados. I. Costa, Sueli Irene Rodrigues, 1949-. II Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para a Biblioteca Digital

Título em inglês: A study of q-ary lattices with the sum metric
Palavras-chave em inglês:
Lee metric
Discrete geometry
Lattice theory
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
Edson Agustini
Marinês Guerreiro
Data da defesa: 11-05-2012
Programa de Pós Graduação: Matemática

Dissertação de Mestrado defendida em 11 de maio de 2012 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof.(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof. (a). Dr (a). EDSON AGUSTINI

Prof. (a). Dr (a). MARINES GUERREIRO

À minha família
Dedico

"Sua tarefa é descobrir o seu trabalho e então, com todo o coração, dedicar-se a ele."
(*Buda*)

Agradecimentos

Agradeço primeiramente a Deus e a Jesus, por iluminarem sempre os meus caminhos.

À professora Sueli Costa, pela orientação, conselhos e a disposição em sempre me ajudar.

À minha amiga Grasiele Cristiane Jorge, pela sua amizade e por toda sua ajuda imprescindíveis para a realização deste trabalho.

Aos professores Edson Agustini e Marinês Guerreiro, pela leitura atenta do trabalho e pelas sugestões e comentários que contribuíram para melhorar a versão final.

Aos amigos do mestrado, que compartilharam comigo os bons e maus momentos desta caminhada.

A todos os meus amigos (novos e antigos), pela torcida, apoio e por proporcionar momentos alegres.

Às minhas queridas amigas Ana Camila, Letícia, Isadora, Francielle, Fernanda, Juliana, Lilian, Gislene, Laís e Cíntia, que foram a minha família em Campinas e fizeram da nossa casa um lar.

Ao meu namorado Valter, por todo apoio, carinho e compreensão.

Aos meus pais Maria José e Mário, pelo amor incondicional.

À minha irmã Adriana, por sempre cuidar de mim.

E ao meu irmão Eduardo, pela disposição em sempre me ajudar.

Resumo

Reticulados no $\mathbb{R}^n$ são conjuntos discretos de pontos gerados como combinações inteiras de vetores linearmente independentes. A estrutura e as propriedades de reticulados vêm sendo exploradas em diversas áreas, dentre elas a Teoria da Informação. Neste trabalho fizemos um estudo de reticulados q-ários na métrica da soma, os quais estão relacionados aos códigos q-ários. Iniciamos com o estudo de reticulados gerais abordando questões como, densidade de empacotamento, determinação da região de Voronoi, equivalência de reticulados e processos de decodificação, fazendo um paralelo destas questões na métrica euclidiana e na métrica da soma. Em seguida, no Capítulo 2, tratamos brevemente os conceitos de códigos corretores de erros, onde os códigos q-ários estão inseridos e códigos lineares definidos sobre corpos finitos. No estudo dos códigos q-ários consideramos a distância de Lee que é uma alternativa à usual métrica de Hamming. Por fim, no Capítulo 3, abordamos os reticulados q-ários que são obtidos a partir de códigos q-ários pelo processo conhecido como Construção A. Estudamos uma forma de se decodificar um reticulado q-ário via a Construção A, usando a decodificação do código e vice-versa e discutimos um algoritmo de decodificação (Lee Sphere Decoding) para reticulados q-ários que possuem matriz geradora de formato especial.

Abstract

Lattices in $\mathbb{R}^n$ are discrete sets of points generated as integer combinations of linearly independent vectors. The structure and properties of lattices have been explored in several areas, including Information Theory. In this work, we study q-ary lattices which are obtained from q-ary codes in the sum metric. We begin the study of general lattices, approaching topics as packing density, Voronoi regions, lattice equivalence and decoding processes, considering both the Euclidean and sum metric. In Chapter 2, we introduce some error correcting codes concepts focusing on q-ary codes and the more general class of linear codes defined over finite fields. In the study of q-ary codes, we consider the Lee distance, as an extension and alternative to the usual Hamming metric. Finally, in Chapter 3, we approach the q-ary lattices, which are obtained from q-ary codes via the so called Construction A. We study a q-ary lattice decoding process, relate it to the associate code decoding and discuss a decoding algorithm for lattices which have special generator matrices.

Sumário

Lista de Símbolos

$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Q}$	conjunto dos números racionais
$\mathbb{R}$	conjunto dos números reais
$\mathbb{Z}_q$	conjunto dos números inteiros reduzidos módulo q
$\|B\|$	cardinalidade do conjunto B
$A = (a_{ij})$	matriz
$\det(A)$	determinante da matriz A
$<,>$	produto interno
$\|.\|$	norma
$\|.\|_2$	norma euclidiana
$\|.\|_1$	norma da soma
d	métrica
$B[x, r]$	bola fechada centrada em x com raio r
Λ	reticulado
$\Lambda^{\perp}$	reticulado dual de Λ
$\Lambda_A(C)$	reticulado q-ário associado ao código C via a Construção A
C	código
$C^{\perp}$	código dual
ρ	raio de empacotamento do reticulado
$\Delta(\Lambda)$	densidade de empacotamento do reticulado Λ
δ	densidade de centro do reticulado
$\det(\Lambda)$	determinante do reticulado Λ
$C^{\perp}$	código dual
ρ	raio de empacotamento do reticulado
$\lfloor a \rfloor$	maior inteiro menor ou igual a a

$\lceil a \rceil$	menor inteiro maior ou igual a a
$[a]$	inteiro mais próximo de a
$R(v)$	região de Voronoi de v
$V_{n_{eucl}}$	volume da esfera euclidiana unitária n dimensional
$V_{n_{soma}}$	volume da esfera da soma unitária n dimensional
η	norma mínima do reticulado
μ_{Lee}	norma mínima de Lee do código
ζ	raio de cobertura do reticulado
d_{Lee}	métrica de Lee
d_{soma}	métrica da soma
d_{eucl}	métrica euclidiana
d_h	métrica de Hamming
$d(C)$	distância mínima do código C

Introdução

Encontramos na literatura um vasto estudo sobre reticulados com a métrica euclidiana, mas muito pouco é conhecido sobre as propriedades de reticulados com a métrica da soma. O objetivo deste trabalho é realizar um estudo de reticulados q-ários com a métrica da soma, os quais estão relacionados aos códigos q-ários com a métrica de Lee.

Dado $q \in \mathbb{N}$, um código linear q-ário C é um subgrupo aditivo próprio do $\mathbb{Z}_q$-módulo $\mathbb{Z}_q^n$. Assim, considerando a aplicação $\phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}_q^n$ dada por $\phi(x_1, ..., x_n) = (\overline{x_1}, ..., \overline{x_n})$, podemos caracterizar um reticulado q-ário da seguinte forma: C é um código linear q-ário se, e somente se, $\Lambda_A(C) := \phi^{-1}(C)$ é um reticulado em $\mathbb{R}^n$. Neste caso, a aplicação ϕ é chamada de Construção A [16].

Via a Construção A, podemos obter vários resultados relacionados a um reticulado q-ário a partir do código q-ário C associado [12]. Podemos encontrar, por exemplo, a dimensão do reticulado q-ário, matrizes geradoras especiais para $\Lambda_A(C)$, sua norma mínima da soma, seu raio de empacotamento da soma, o reticulado dual de $\Lambda_A(C)$, bem como sua matriz geradora e processos de decodificação na métrica da soma derivados da decodificação do código.

A teoria de reticulados, tem sido bastante utilizada na resolução de problemas da teoria da informação. Os códigos com a métrica de Lee foram introduzidos em [7] e desde então são objetos de vários estudos teóricos e práticos. Para $q = 2$ e $q = 3$, a usual distância de Hamming [3] para códigos lineares é igual a distância de Lee. Via Construção A, podemos obter também alguns resultados relacionados aos códigos q-ários, como um conjunto de geradores, a cardinalidade do código e processos de decodificação derivados da decodificação do reticulado associado.

Todas as questões citadas acima são abordadas nesta dissertação. No Capítulo 1, introduzimos definições básicas e propriedades relacionadas a reticulados em geral. Alguns dos conceitos estudados envolvem a noção de distância, como a região de Voronoi de um reticulado, a densidade de empacotamento, o raio de cobertura, equivalência de reticulados e decodificação de reticulados. Procuramos fazer uma comparação destes conceitos com a métrica euclidiana e com a métrica da soma. Ainda neste capítulo, exibimos alguns exem-

plos de reticulados mais conhecidos e ao final estudamos dois algoritmos de decodificação para reticulados, o primeiro, chamado de *Sphere decoding*, que faz uso de uma fatoração QR na matriz geradora do reticulado para decodificá-lo com a métrica euclidiana e o segundo, como uma adaptação do primeiro, faz uso de uma matriz geradora do reticulado na forma Normal de Hermite para reticulados com a métrica d_p, $0 < p < \infty$, definida por $d_p(x,y) = (|x_1-y_1|^p+\cdots+|x_n-y_n|^p)^{\frac{1}{p}}$, sendo $x, y \in \mathbb{R}^n$, com $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n)$.

O segundo capítulo é dedicado ao estudo dos códigos lineares q-ários. Iniciamos com os códigos corretores de erros definidos sobre um conjunto A finito qualquer. Em seguida, fizemos uma breve introdução aos códigos lineares definidos sobre corpos finitos e por fim estudamos os códigos lineares q-ários, já introduzindo a distância de Lee. Os códigos q-ários estão inseridos no primeiro conjunto de códigos citados e em particular, quando q é primo, $\mathbb{Z}_q$ é um corpo e então o código q-ário possui todas as propriedades dos códigos definidos sobre corpos. Por outro lado, quando q não é um número primo, algumas destas propriedades podem ser perdidas, como por exemplo, um conjunto de geradores linearmente independentes.

Finalmente no terceiro capítulo, estudamos os reticulados q-ários que são obtidos de códigos q-ários pela Construção A. Diversas propriedades destes reticulados obtidas via Construção A foram abordadas, como por exemplo, no caso em que q é primo, conseguimos obter uma matriz de um reticulado q-ário na forma Normal de Hermite, derivada de uma matriz na forma padrão do código q-ário associado. Esta matriz ajuda a simplificar o algoritmo de decodificação para a métrica d_p no caso em que $p = 1$, apresentado no Capítulo 2, dando origem ao algoritmo *Lee Sphere Decoding*. Estudamos ainda uma forma de se decodificar um código q-ário na métrica de Lee usando um processo de decodificação do reticulado q-ário associado e vice-versa. Exemplificamos esta última abordagem com a decodificação de um código de Goppa clássico.

Capítulo 1

Reticulados

Neste capítulo, da Seção 1.1 à Seção 1.7 introduziremos definições básicas e propriedades relacionadas a reticulados. Algumas delas usam a noção de distância e têm sido amplamente estudadas com a métrica euclidiana. Muito pouco é conhecido na literatura sobre propriedades de reticulados estudadas na métrica da soma. Assim, procuramos fazer uma comparação destas definições e propriedades na métrica euclidiana e da soma. Na Seção 1.8 exibiremos alguns exemplos de reticulados e na Seção 1.9 dois algoritmos de decodificação de reticulados. As principais referências utilizadas neste capítulo foram [1], [5],[12], [16] e [11].

1.1 Conceitos Fundamentais

Definição 1.1. *Um subconjunto Λ de $\mathbb{R}^n$ é um* **reticulado**, *se existe um conjunto $\beta = \{u_1, u_2, ..., u_m\}$ de vetores linearmente independentes de $\mathbb{R}^n$, com $m \leq n$, tal que $x \in \Lambda$ se, e somente se, $x = a_1u_1 + \cdots + a_mu_m$, com $a_i \in \mathbb{Z}$ para $i = 1, ..., m$.*

Chamamos β de **base** de Λ e ela não é única.

Definição 1.2. *Seja $\Lambda \in \mathbb{R}^n$ um reticulado. Definimos a dimensão de Λ e denotamos por $dim(\Lambda)$, o número de vetores de uma base β de Λ.*

Exemplo 1.3. *A Figura 1.1 mostra alguns pontos do reticulado Λ com uma base dada por $\{(1,1),(1,3)\}$. Uma outra base para o reticulado Λ é $\{(1,1),(2,0)\}$.*

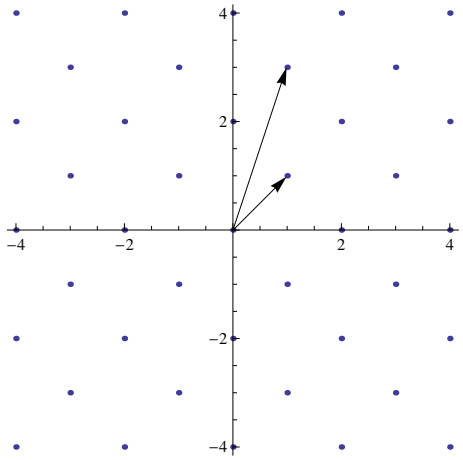


Figura 1.1: Exemplo 1.3

Proposição 1.4. *[16] Se Λ é um reticulado de dimensão n gerado por uma base β, uma base α do $\mathbb{R}^n$ é uma base deste reticulado se, e somente se, $\alpha \subset \Lambda$ e a matriz mudança de base $[T]_\alpha^\beta$ de β para α é uma matriz unimodular, isto é, tem entradas inteiras e determinante ± 1.*

Demonstração. Seja $[T]_\beta^\alpha$ a matriz mudança de base de α para β. Como cada elemento da base β pode ser escrito como combinação inteira dos elementos de α e vice-versa, as matrizes $[T]_\alpha^\beta$ e $[T]_\beta^\alpha$ só possuem entradas inteiras e, por conseguinte, os respectivos determinantes também são inteiros. Como $[T]_\alpha^\beta \cdot [T]_\beta^\alpha = I$, onde I é a matriz identidade, temos $det([T]_\alpha^\beta) \cdot det([T]_\beta^\alpha) = 1$ e daí $det([T]_\alpha^\beta) = det([T]_\beta^\alpha) = \pm 1$.
Reciprocamente, como α é uma base de $\mathbb{R}^n$ e a matriz mudança de base β para α possui somente entradas inteiras, então todo elemento da base β pode ser escrito como combinação inteira dos elementos da base α e, portanto, todo elemento do reticulado gerado por β pertence ao reticulado gerado por α e vice-versa. □

Corolário 1.5. *Se Λ é um reticulado de dimensão $m \leq n$ e α e β são bases do reticulado, então a matriz mudança de base $[T]_\alpha^\beta$ de β para α tem entradas inteiras e determinante ± 1.*

Demonstração. Se $m = n$ já demonstramos. Se $m < n$, para as matrizes mudança de base $[T]_\alpha^\beta$ e $[T]_\beta^\alpha$ das bases do reticulado, também vale $[T]_\alpha^\beta \cdot [T]_\beta^\alpha = I$, então a demonstração do corolário é análoga a primeira parte da demonstração da Proposição 1.4. □

Observação 1.6. *Note que um reticulado Λ é um subgrupo aditivo do $\mathbb{R}^n$. Em particular, se $u, v \in \Lambda$, então $u + v$ e $u - v$ são vetores do reticulado.*

Teorema 1.7. *[14] Se Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$, então Λ é um reticulado.*

Demonstração. Seja Λ um subgrupo aditivo discreto de $\mathbb{R}^n$. Provemos por indução sobre n que Λ é um reticulado. Sejam $\{v\}$ um subconjunto maximal linearmente independente de Λ e $r \in \mathbb{R}$, tal que $B[0,r] \cap \Lambda \neq \{0\}$, em que $B[0,r]$ denota a bola fechada centrada em 0 e raio r. Como Λ é um subgrupo discreto, toda bola fechada centrada em zero, possui finitos elementos de Λ. Podemos escolher assim, $z \in B[0,r] \cap \Lambda$, $z \neq 0$, tal que a norma de z seja mínima e substituir v por z. Logo, dado qualquer $w \in \Lambda$ temos $w = \lambda z$. Agora, suponha que exista $w_1 = \lambda_1 z \in \Lambda$, tal que λ_1 não seja um número inteiro. Como Λ é subgrupo aditivo, $\lfloor \lambda_1 \rfloor z \in \Lambda$, em que $\lfloor \lambda_1 \rfloor$ denota o maior inteiro menor ou igual a λ_1, e temos também

$$w_1' = \lambda_1 z - \lfloor \lambda_1 \rfloor z = (\lambda_1 - \lfloor \lambda_1 \rfloor) z \in \Lambda.$$

Daí

$$\|w_1'\| = \|(\lambda_1 - \lfloor \lambda_1 \rfloor) z\| = |\lambda_1 - \lfloor \lambda_1 \rfloor| \|z\| \leq \|z\|.$$

Mas isto contradiz a minimalidade de $\|z\|$. Portanto, qualquer $w \in \Lambda$ é uma combinação inteira de z. Logo Λ é um reticulado.

Agora, seja $\{v_1, ..., v_m\}$ um subconjunto maximal linearmente independente de Λ, $m \leq n$. Seja V o subespaço gerado por $\{v_1, ..., v_{m-1}\}$ e seja $\Lambda_0 = \Lambda \cap V$. Então Λ_0 é subgrupo aditivo discreto, assim por indução é um reticulado. Logo existe uma base $\{u_1, ..., u_{m'}\}$ de Λ_0. Como os elementos $v_1, ..., v_{m-1} \in \Lambda_0$ temos que $m' = m - 1$, e podemos substituir $\{u_1, ..., u_{m'}\}$ por $\{v_1, ..., v_{m-1}\}$, ou equivalentemente assumir que todo elemento de Λ_0 é uma combinação linear com coeficientes inteiros de $v_1, ..., v_{m-1}$. Seja T o subconjunto de todos os $x \in \Lambda$ da forma

$$x = a_1 v_1 + \cdots + a_m v_m$$

com $a_i \in \mathbb{R}$, tais que $0 \leq a_i < 1$ para $i = 1, ..., m-1$ e $0 \leq a_m \leq 1$. Então, T é limitado, logo finito já que Λ é discreto. Assim, podemos escolher um $x' \in T$ com o menor m-ésimo coeficiente não-nulo, digamos que

$$x' = b_1 v_1 + \cdots + b_m v_m.$$

Certamente $\{v_1, ..., v_{m-1}, x'\}$ é linearmente independente. Seja $z \in \Lambda$, podemos escolher coeficientes inteiros c_i tais que

$$z' = z - c_m x' - c_1 v_1 - \cdots - c_{m-1} v_{m-1}$$

esteja em T e o coeficiente de v_m em z' seja menor do que b_m, mas não negativo. Pela escolha de x' este coeficiente deve ser zero, então $z' \in \Lambda_0$. Logo $\{v_1, ..., v_{m-1}, x'\}$ geram Λ e Λ é um reticulado. □

Proposição 1.8. *[5] Um reticulado Λ é geometricamente uniforme, isto é, dados dois vetores quaisquer $x, y \in \Lambda$, existe uma isometria $\phi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ tal que:*
(i) $\phi(\Lambda) = \Lambda$, ou seja, ϕ é uma simetria de Λ,
(ii)$\phi(x) = y$, ou seja, ϕ age transitivamente em Λ.

Demonstração. Dados $x, y \in \Lambda$, tome a translação dada por $\phi(v) = v + (y - x)$. É claro que ϕ é uma isometria e a condição (ii) é trivialmente satisfeita. Agora seja $\beta = \{u_1, ..., u_n\}$ uma base de Λ. Como $y - x \in \Lambda$, existem $b_1, ..., b_n \in \mathbb{Z}$ tais que $y - x = b_1u_1 + \cdots + b_nu_n$. Dado $w \in \phi(\Lambda)$, existe um $v \in \Lambda$ tal que $\phi(v) = w$, assim existem $a_1, ..., a_n$ inteiros tais que $v = a_1u_1 + \cdots + a_nu_n$. Logo, $\phi(v) = v + (y - x) = (a_1 + b_1)u_1 + \cdots + (a_n + b_n)u_n \in \Lambda$. Portanto $\phi(\Lambda) \subseteq \Lambda$.
Seja $r \in \Lambda$, tome $z = r - (y - x) \in \Lambda$, então $\phi(z) = r - (y - x) + (y + x) = r$. Portanto $\Lambda \subseteq \phi(\Lambda)$ e a condição (i) também é satisfeita. □

Corolário 1.9. *Seja Λ um reticulado e $v \in \Lambda$, então a translação $T(u) = u + v$, é uma isometria que leva Λ em Λ.*

Demonstração. A prova deste corolário é análoga a prova da condição (ii) da proposição anterior, bastando substituir $x - y$ por v na demonstração. □

Observamos que a translação é isometria para todas as métricas d_p, $1 \leq p < \infty$.

Definição 1.10. *Seja $\{u_1, ..., u_m\}$, uma base de vetores do reticulado Λ, onde $u_i = (u_{i1}, ..., u_{in})$, para $i = 1, ..., m$ e $m \leq n$ e seja $x \in \Lambda$. Podemos escrever x da forma*

$$x = k_1 \begin{pmatrix} u_{11} \\ \vdots \\ u_{1n} \end{pmatrix} + \cdots + k_m \begin{pmatrix} u_{m1} \\ \vdots \\ u_{mn} \end{pmatrix} = \begin{pmatrix} u_{11} & \cdots & u_{m1} \\ \vdots & & \vdots \\ u_{1n} & \cdots & u_{mn} \end{pmatrix} \begin{pmatrix} k_1 \\ \vdots \\ k_m \end{pmatrix}$$

onde $k_i \in \mathbb{Z}$, para $i = 1, ..., m$. Isso mostra que todo $x \in \Lambda$ é da forma Mv^T, onde M é a matriz cuja as colunas são os vetores de uma base de Λ e $v = (k_1, ..., k_m)$ é um vetor com entradas inteiras. A matriz M descrita acima é chamada uma **matriz geradora** *do reticulado Λ.*

Se um reticulado Λ possui uma base cujos vetores possuem apenas entradas inteiras, podemos obter uma matriz geradora para o reticulado em um formato especial que é muito útil.

Definição 1.11. *[18] Seja $H = (h_{ij})$ uma matriz $n \times m$, com $n \leq m$, com coeficientes inteiros. Se $m = n$ e H é não singular, dizemos que H é uma matriz na* ***forma Normal de Hermite*** *(HNF) se:*
(i) H é triangular superior;
(ii) $h_{ii} > 0$, para todo $i = 1, ..., n$;
(iii) $h_{ij} < h_{jj}$, para todo $i < j$.

Se $n \leq m$ a matriz H na forma Normal de Hermite é da forma

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & * & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & * \end{pmatrix} \tag{1.1}$$

onde as últimas n colunas formam uma matriz HNF de ordem n.

Se $A = (a_{ij})$ é uma matriz $n \times m$, com $m \geq n$ e coeficientes em $\mathbb{Z}$, é possível encontrar, fazendo operações elementares nas colunas de A, uma matriz B da forma 1.1. A matriz H formada pelas últimas n colunas de B será chamada de matriz HNF de A. O seguinte algoritmo ensina como encontrar a matriz H. Denotaremos por h_{ij} os coeficientes de H e por A_i e H_i as colunas de A e H, respectivamente, e dado um número real z denotaremos por $[z]$ e $\lfloor z \rfloor$ o inteiro mais próximo de z e o maior inteiro menor ou igual a z, respectivamente.

Algoritmo 1.12. *[18]*

- ***Passo 1:*** *Atribua valor n para i e valor m para k e coloque $l = 1$.*
- ***Passo 2:*** *Se todos os a_{ij}, para $j < k$, são nulos, verifique se $a_{ik} < 0$. Neste caso substitua a coluna A_k, por $-A_k$ e então vá para o passo 5.*
  Se algum a_{ij}, para $j < k$ é não nulo, vá para o passo 3.
- ***Passo 3:*** *Escolha um a_{ij} não nulo para $j \leq k$ que possua o menor valor absoluto. Denote-o por a_{ij_0}. Então, se $j_0 < k$, permute as colunas A_k e A_{j_0}. Se $a_{ik} < 0$, substitua a coluna A_k, por $-A_k$ e coloque $b := a_{ik}$, então vá para o passo 4.*

- ***Passo 4:*** *Para $j = 1, ..., k-1$, coloque $q := [a_{ij}/b]$ e $A_j = A_j - qA_k$ e então vá para o passo 2.*

- ***Passo 5:*** *Coloque $b := a_{ik}$. Se $b = 0$, então atribua o valor $k+1$ para k e vá para o passo 6. Caso contrário, para $j > k$ coloque $q := \lfloor a_{ij}/b \rfloor$ e $A_j = A_j - qA_k$ e então vá para o passo 6.*

- ***Passo 6:*** *Se $i = l$, então para $j = 1, ..., m-k+1$ coloque $H_j = A_{j+k-1}$ e o algoritmo termina. Caso contrário atribua valor $i-1$ para i, $k-1$ para k e vá para o passo 2.*

Observação 1.13. *[18] Para encontrar a matriz HNF da matriz A fizemos apenas operações inteiras sobre as colunas de A. É possível mostrar também que a matriz HNF de A é única. Então, se A for uma matriz com coeficientes inteiros, cujas colunas são um conjunto de geradores de um reticulado Λ, as colunas da matriz HNF de A nos fornecem a única base de Λ cuja a matriz geradora associada H é HNF. No caso em que a dimensão do reticulado é n, a matriz H será triangular superior. Podemos também modificar facilmente o algoritmo 1.12 e encontrar, para este caso, uma matriz HNF de A triangular inferior.*

Definição 1.14. *Dizemos que $\Lambda^* \subset \Lambda$ é um* **sub-reticulado** *de Λ, se Λ^* ainda for um reticulado.*

Definição 1.15. *Dizemos que um $\mathbb{Z}$-módulo M é livre de posto r se existem r vetores $v_1, ..., v_r \in M$ que são linearmente independentes sobre $\mathbb{Z}$ e tais que para todo $v \in M$ tem-se $v = \sum_{i=1}^{r} a_i v_i \in M$, com $a_i \in \mathbb{Z}$, para $i = 1, ..., r$.*

Definição 1.16. *Dizemos que um grupo abeliano G é livre de posto r se G é um $\mathbb{Z}$-módulo livre de posto r.*

Proposição 1.17. *[14] Sejam G um grupo abeliano livre de posto r e H um subgrupo de G. Então G/H é finito se, e somente se, $posto(G) = posto(H)$. Se $\{x_1, ..., x_n\}$ é uma $\mathbb{Z}$-base para G e $\{y_1, ..., y_n\}$ é uma $\mathbb{Z}$-base para H tais que $y_i = \sum_{i=1}^{n} a_{ij} x_j$, para $a_{ij} \in \mathbb{Z}$, $i = 1, ..., n$, então $|G/H| = |det(a_{ij})|$.*

Observação 1.18. *[12] Um reticulado Λ é um grupo abeliano livre e um sub-reticulado $\Lambda^* \subseteq \Lambda$ é um subgrupo de Λ. Então, pela Proposição 1.17, temos que $|\Lambda/\Lambda^*| < \infty$ se, e somente se, $dim(\Lambda) = dim(\Lambda^*)$. Além disso, se M é uma matriz geradora para Λ e N uma matriz geradora para Λ^*, existe uma matriz com entradas inteiras A tal que $N = AM$. Assim temos que*

$$|\Lambda/\Lambda^*| = |det(A)| = |det(N)|/|det(M)|$$

Proposição 1.19. *[16] Sejam Λ um reticulado n-dimensional e M uma matriz geradora de Λ. Definamos o conjunto*

$$D_\Lambda = \{x \in \mathbb{R}^n : \langle x, z\rangle \in \mathbb{Z}, \forall z \in \Lambda\}.$$

Temos que D_Λ é um reticulado n-dimensional com uma matriz geradora dada por $(M^{-1})^t$.

Demonstração. Primeiramente notamos que se $u = (M^{-1})^t w$, com $w \in \mathbb{Z}^n$, então dado um $z \in \Lambda$, podemos escrever z da forma $z = Mv$, com $v \in \mathbb{Z}^n$ e assim

$$\langle u, z\rangle = \langle (M^{-1})^t w, Mv\rangle = v^t M^t (M^{-1})^t w = v^t w \in \mathbb{Z}.$$

Logo $u \in D_\Lambda$.
Agora, as colunas da matriz $(M^{-1})^t$ são linearmente independentes, pois M é uma matriz não singular. Logo, estas colunas formam uma base de $\mathbb{R}^n$. A i-ésima coluna de $(M^{-1})^t$ é dada por $C_i := (M^{-1})^t e_i$, $i = 1, ..., n$ e pelo que mostramos acima ela pertence a D_Λ. Então seja $y \in D_\Lambda$, como $y \in \mathbb{R}^n$ e $\{C_1, ..., C_n\}$ é uma base de $\mathbb{R}^n$, temos $y = k_1 C_1 + \cdots + k_n C_n = (M^{-1})^t k$, onde $k = (k_1, ..., k_n) \in \mathbb{R}^n$. Queremos mostrar que k é um vetor com entradas inteiras. Como $y \in D_\Lambda$, então $\langle y, z\rangle \in \mathbb{Z}$, para todo $z \in \Lambda$. Assim, tome os vetores de Λ da forma Me_i, $i = 1, ..., n$. Logo, para cada $i = 1, ..., n$ temos

$$\langle y, Me_i\rangle = \langle (M^{-1})^t k, Me_i\rangle = e_i^t M^t (M^{-1})^t k = e_i^t (M^{-1}M)^t k = e_i^t k = \langle e_i, k\rangle = k_i \in \mathbb{Z}.$$

Portanto $D_\Lambda = \{y \in \mathbb{R}^n : y = (M^{-1})^t k, k \in \mathbb{Z}^n\}$, ou seja, D_Λ é um reticulado n-dimensional com matriz geradora $(M^{-1})^t$. □

Definição 1.20. *O conjunto D_Λ definido na Proposição 1.19, é chamado de **reticulado dual** do reticulado Λ e o denotamos por $\Lambda^\perp$.*

Definição 1.21. *Dizemos que um reticulado Λ é **auto dual** se $\Lambda = \Lambda^\perp$.*

Exemplo 1.22. *Considere o reticulado $\Lambda = \mathbb{Z}^2$, com base $\{(1, 0), (0, 1)\}$. O reticulado dual de Λ é $\Lambda^\perp = \mathbb{Z}^2$, ou seja, $\mathbb{Z}^2$ é um reticulado auto dual.*

1.2 Matriz de Gram e determinante do reticulado

Definição 1.23. *Sejam Λ um reticulado e M uma matriz geradora de Λ, a matriz $M^tM =: G$ é chamada* **matriz de Gram** *do reticulado Λ.*

Observação 1.24. *Note que as ij-ésimas entradas de G são dadas pelo produto interno (usual) $\langle v_i, v_j \rangle$, onde v_i, para $i = 1, ..., m$ são os vetores da base do reticulado, e que G é uma matriz simétrica, assim G guarda informações métricas importantes sobre a base escolhida.*

Como um reticulado possui infinitas bases diferentes, possui também matrizes geradoras diferentes e consequentemente matrizes de Gram diferentes, entretanto o determinante de cada uma delas só depende do reticulado. É o que mostra o seguinte resultado.

Proposição 1.25. *[5] Sejam A e B duas matrizes geradoras de um reticulado Λ, então $G := A^TA$ e $G' := B^TB$ possuem o mesmo determinante.*

Demonstração. Como A e B são matrizes geradoras para o reticulado Λ, existe uma matriz U tal que $B = AU$ e pelo Colorário 1.5 $det(U) = \pm 1$. Assim

$$det(B^tB) = det(A^tU^tAU) = det(A^t)det(U^t)det(A)det(U) = det(A^tA).$$

□

Definição 1.26. *Definimos o* **determinante** *de Λ e denotamos por* $\det(\Lambda)$ *como o determinante de uma matriz de Gram qualquer de Λ.*

Definição 1.27. *Dizemos que um reticulado Λ é ortogonal se possuir uma base β com vetores dois a dois ortogonais.*

Observação 1.28. *Se Λ é um reticulado ortogonal, ele possui uma matriz de Gram diagonal e o determinante do reticulado será o produto dos elementos da diagonal desta matriz.*

De agora em diante trabalharemos com reticulados de dimensão n no $\mathbb{R}^n$.

1.3 Região fundamental

Definição 1.29. *Uma* **região fundamental** *F de um reticulado Λ é um subconjunto fechado do $\mathbb{R}^n$ que ladrilha $\mathbb{R}^n$, isto é, tomando cópias de F transladadas pelos vetores $v \in \Lambda$, conseguimos cobrir todo $\mathbb{R}^n$ de forma que dois ladrilhos ou não têm intersecção ou se intersectam apenas no bordo.*

Definição 1.30. *Um* **paralelotopo fundamental** *é o conjunto*

$$P = \{\theta_1 u_1 + \cdots + \theta_n u_n : 0 \leq \theta_i \leq 1, \text{ para todo } i = 1, ..., n\},$$

sendo $\beta = \{u_1, u_2, ..., u_n\}$ *é uma base de um reticulado* Λ*, ou seja, é o paralelepípedo n-dimensional gerado pelo vetores da base do reticulado* Λ*.*

Observação 1.31. *O volume de um paralelotopo fundamental* $vol(P)$ *é dado pelo determinante da matriz geradora* M *do reticulado [5]. Assim,* $det(\Lambda) = det(G) = det(M^t M) = det^2(M) = (vol(P))^2$*.*

Proposição 1.32. *[16] O paralelotopo fundamental é uma região fundamental.*

Demonstração. É claro que P é fechado, então basta provar que tomando os traslados $P+v = \{x + v : x \in P\}$, onde $v \in \Lambda$, cobrimos todo o $\mathbb{R}^n$ de forma que dois ladrilhos ou não têm intersecção ou se intersectam apenas no bordo.
Seja $\lfloor a \rfloor$ a parte inteira do número real a, isto é, $\lfloor a \rfloor \in \mathbb{Z}$ e $0 \leq a - \lfloor a \rfloor < 1$, então para cada vetor $v = \sum_{i=1}^n a_i u_i$ de $\mathbb{R}^n$, onde u_i para $i = 1, ..., n$ são os elementos da base do reticulado, temos

$$\sum_{i=1}^n a_i u_i = \sum_{i=1}^n \lfloor a_i \rfloor u_i + \sum_{i=1}^n (a_i - \lfloor a_i \rfloor) u_i.$$

Como $\sum_{i=1}^n \lfloor a_i \rfloor u_i \in \Lambda$ e $\sum_{i=1}^n (a_i - \lfloor a_i \rfloor) u_i \in P$, segue que $\mathbb{R}^n = \bigcup_{v \in \Lambda} v + P$.
O interior de $v + P$ é o conjunto

$$int(v + P) = \{v + \sum_{i=1}^n b_i u_i : 0 < b_i < 1\}.$$

Sejam $x \in \mathbb{R}^n$ e $v_1, v_2 \in \Lambda$ tais que $x \in int(v_1 + P) \cap int(v_2 + P)$. Assim existem $a_i, ..., a_n, b_i, ..., b_n \in \mathbb{Z}$ e $\alpha_i, ..., \alpha_n, \beta_1, ..., \beta_n$, com $0 \leq \alpha_i, \beta_i < 1$, $i = 1, ..., n$, tal que

$$x = \sum_{i=1}^n a_i u_i + \sum_{i=1}^n \alpha_i u_i \text{ e } x = \sum_{i=1}^n b_i u_i + \sum_{i=1}^n \beta_i u_i.$$

Como $\{u_1, ..., u_n\}$ é base de $\mathbb{R}^n$, temos $a_i - b_i + \alpha_i - \beta_i = 0$ para $i = 1, ..., n$. Assim, como $a_i - b_i \in \mathbb{Z}$ e $0 \leq |\alpha_i - \beta_i| < 1$, temos $a_i = b_i$ e $\alpha_i = \beta_i$, ou seja, $v_1 = v_2$.
Portanto, nenhum ponto do interior de $v + P$ pode estar no interior de outro traslado $u + P$. □

Exemplo 1.33. *Considere o reticulado* Λ *com base* $\{(0, 1), (2, 1)\}$*. Na Figura 1.2, temos o paralelotopo fundamental* P *apoiado sobre os vetores da base do reticulado* Λ *e o ladrilhamento dado pelas translações de* P *por vetores do reticulado.*

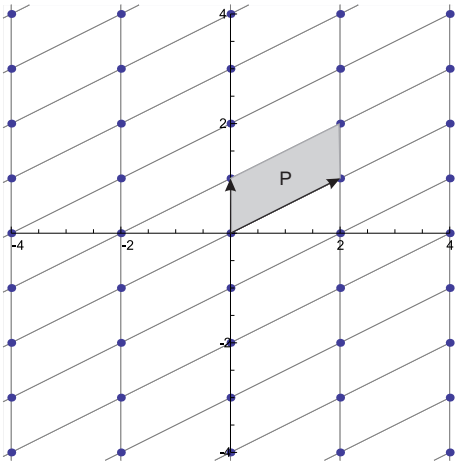


Figura 1.2: Paralelotopo fundamental do reticulado Λ.

Proposição 1.34. *[5] O volume de qualquer região fundamental de um reticulado Λ é sempre o mesmo.*

Não faremos a demonstração deste resultado, que pode ser encontrada em [2].

Definição 1.35. *Dados $x, y \in \mathbb{R}^n$, a distância da soma entre x e y é definida como $d(x,y) = \sum_{i=1}^{n} |x_i - y_i|$, sendo $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n)$.*

No que segue, continuaremos a introduzir conceitos e resultados relacionados a reticulados e quando envolverem a noção de distância, sempre que possível, faremos uma comparação nas métricas euclidiana e da soma.

1.4 Região de Voronoi

Definição 1.36. *A* **região de Voronoi** *de um ponto $v \in \Lambda$ é o conjunto*

$$R(v) = \{x \in \mathbb{R}^n : d(x,v) \leq d(x,u), \text{ para todo } u \in \Lambda\}.$$

Para uma métrica induzida por uma norma $\|\cdot\|$ em $\mathbb{R}^n$, podemos reescrever a definição acima da seguinte maneira:

$$R(v) = \{x \in \mathbb{R}^n : \|v - x\| \leq \|u - x\|, \text{ para todo } u \in \Lambda\}.$$

Este é o caso das métricas euclidiana e da soma. No que segue consideraremos apenas as métricas induzidas por normas em $\mathbb{R}^n$.

Proposição 1.37. *[5] Seja $v \in \Lambda$, temos que*

$$R(v) = v + R(0) = \{v + x \in \mathbb{R}^n : x \in R(0)\}.$$

Demonstração. Temos

$$R(0) = \{y \in \mathbb{R}^n : \|y\| \leq \|w - y\|, \forall w \in \Lambda\}$$

Seja $T_v : \mathbb{R}^n \to \mathbb{R}^n$ a translação dada por $T_v(k) = k + v$. Tomando um $x \in \mathbb{R}(0)$, temos $\|v - T_v(x)\| = \|v - (x + v)\| = \|x\| \leq \|w - x\| = \|w - T_v(x) + v\| = \|u - T_v(x)\|$, para todo $u \in \Lambda$. Logo $T_v(x) = x + v \in \mathbb{R}(v)$, ou seja, $v + R(0) \subseteq R(v)$.
Agora seja $y \in \mathbb{R}(v)$. Podemos escrever y da forma $y = v + k$, onde $k = y - v \in \mathbb{R}^n$. Mostremos que $k \in \mathbb{R}(0)$. De fato,

$$\|k\| = \|v - (k + v)\| = \|v - y\| \leq \|w - y\|, \text{ para todo } w \in \Lambda.$$

Assim

$$\|k\| \leq \|w - y\| = \|w - v + k\| = \|r + k\|, \text{ para todo } r \in \Lambda.$$

Logo $k \in \mathbb{R}(0)$ e, portanto, $R(v) = v + R(0)$. □

A proposição acima nos diz que $R(0)$ é uma região fundamental do reticulado Λ, já que pela definição ela é fechada e dado qualquer ponto $u \in \mathbb{R}^n$ ou esse ponto está mais próximo de algum vetor $v \in \Lambda$ e, neste caso, $u \in R(v) = v + R(0)$, ou este ponto está à mesma distância de diferentes pontos do reticulado e neste caso pertence ao bordo comum das regiões de Voronoi destes pontos. Assim, as regiões de Voronoi dos pontos do reticulado ladrilham todo $\mathbb{R}^n$.

No espaço n-dimensional euclidiano as regiões de Voronoi de um ponto $v \in \Lambda$ são poliedros n-dimensionais fechados e convexos determinados pela intersecção de semiespaços determinados por hiperplanos cujos pontos equidistam de v e dos demais pontos do reticulado. Na métrica da soma as regiões de Voronoi de um reticulado podem não ser poliedros n-dimensionais convexos.

Exemplo 1.38. *Dados dois pontos $x = (0, 0)$ e $y = (2, 3)$, o conjunto dos pontos que estão à mesma distância de x e y nas métricas euclidiana e da soma são dados pelas figuras da direita e da esquerda, respectivamente.*

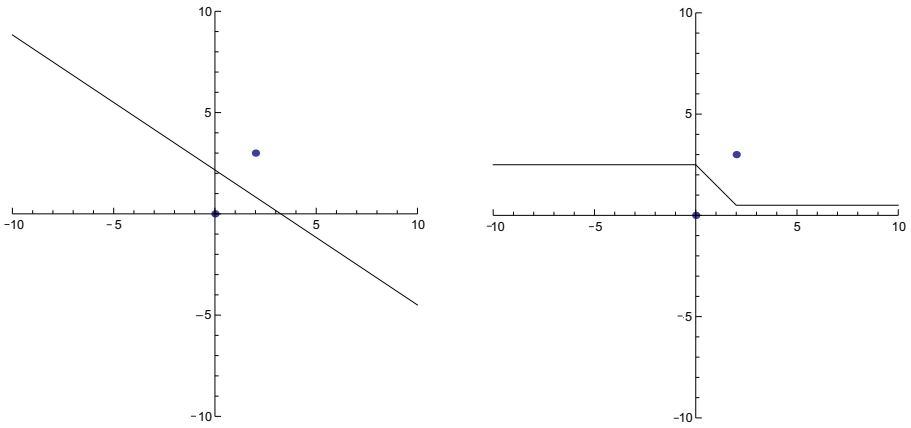


Figura 1.3: Conjunto dos pontos que estão à mesma distância dos pontos x e y nas métricas euclidiana e da soma.

Exemplo 1.39. *Na Figura 1.4, à esquerda temos, as regiões de Voronoi em relação a métrica euclidiana e à direita, as regiões de Voronoi na métrica da soma do reticulado hexagonal dado pela base* $\{(1,0),(1/2,\sqrt{3}/2)\}$.

Exemplo 1.40. *Nas Figuras 1.5, à esquerd,a temos as regiões de Voronoi na métrica euclidiana e à direita, as regiões de Voronoi na métrica da soma do reticulado* Λ *que tem por base* $\{(1,4),(0,3)\}$.

Observação 1.41. *Embora as regiões de Voronoi de um reticulado na métrica euclidiana e na métrica da soma sejam diferentes, pela Proposição 1.34, elas possuem o mesmo volume, pois ambas são regiões fundamentais.*

1.5 Densidade de empacotamento de um reticulado

A densidade de empacotamento de um reticulado Λ é a proporção do espaço coberto pela união de esferas e mesmo raio disjuntas centradas em pontos de Λ com o maior raio possível. Esse conceito está diretamente relacionado ao clássico problema do empacotamento esférico que consiste em descobrir a melhor forma de distribuir esferas de raio r em $\mathbb{R}^n$ de modo que:
(i) duas esferas quaisquer deste arranjo apenas se toquem em um ponto da "casca" ou não possuam interseção alguma,
(ii) este arranjo de esferas seja o mais denso possível, isto é, ocupe o maior espaço possível.

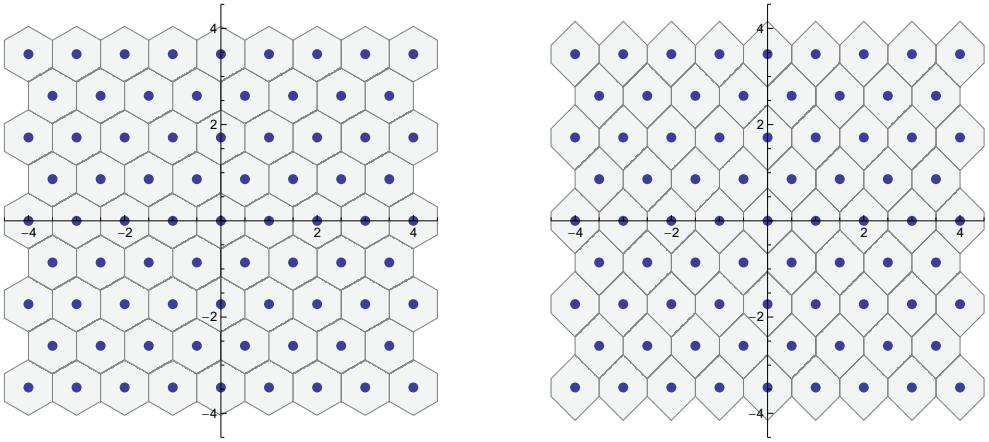


Figura 1.4: Regiões de Voronoi do reticulado hexagonal consideradas na métrica euclidiana e da soma.

Podemos descrever um empacotamento de esferas em $\mathbb{R}^n$ especificando apenas os seus centros e o raio das esferas. Quando os centros das esferas formam um reticulado dizemos que o empacotamento é um empacotamento reticulado.
Existem várias motivações para se encontrar os empacotamentos reticulados n-dimensionais com alta densidade. Até a oitava dimensão ele ocorre nas famílias de reticulados A_n, D_n e E_n que abordaremos brevemente mais adiante e têm correspondência com os diagramas de *Coxeter-Dynkin*. Em dimensão 24 o empacotamento do reticulado *Leech* Λ_{24} tem uma misteriosa conexão com a geometria hiperbólica e com a álgebra de Lie. Empacotamentos reticulados têm aplicações diretas na Teoria dos Números, resolução de equações Diofantinas, na Geometria dos Números e nos problemas decorrentes de comunicação digital. Empacotamentos tridimensionais têm aplicações na Química, na Física e na Biologia [16]. De forma geral, à medida que a dimensão cresce a densidade de empacotamento do reticulado decresce.

Exemplo 1.42. *A Figura 1.6 mostra, à esquerda e à direita o empacotamento de esferas na métrica euclidiana e da soma, respectivamente, do reticulado* $\{(2,5),(0,4)\}$

Podemos avaliar o quão denso é um reticulado, comparando o volume de uma região de Voronoi $R(v)$ de um ponto $v \in \Lambda$ com o volume da maior bola fechada centrada em v que ela contém.

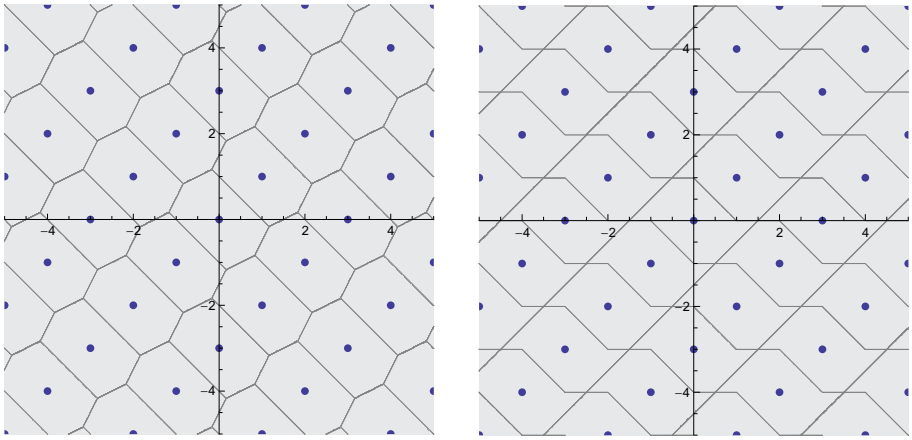


Figura 1.5: Regiões de Voronoi do reticulado Λ consideradas na métrica euclidiana e da soma.

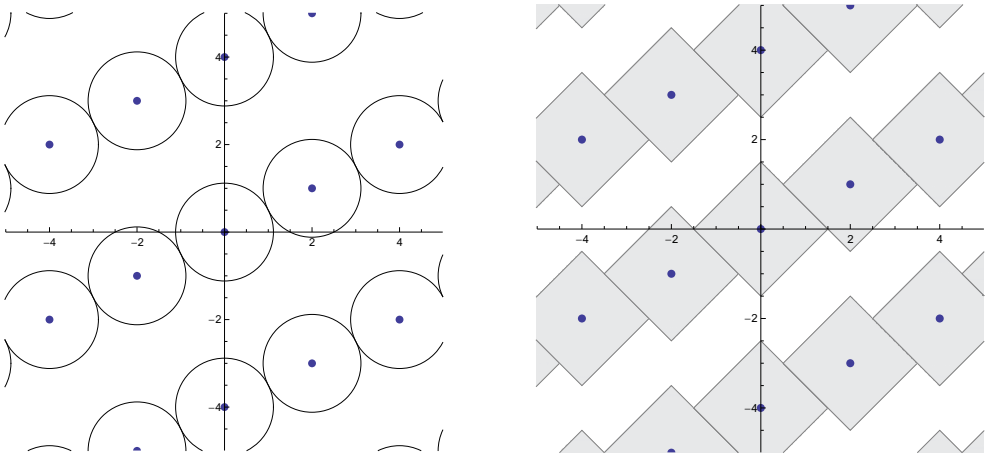


Figura 1.6: Empacotamento reticulado nas métricas euclidiana e da soma

Definição 1.43. *Seja d uma métrica em $\mathbb{R}^n$. Chamamos de* **raio de empacotamento** *de um reticulado Λ o valor:*

$$\rho = max\{r : B_d[0,r] \subset R(0)\},$$

onde $B_d[0,r]$ denota a bola fechada na métrica d de centro 0 e raio r.

Exemplo 1.44. *Considere o reticulado do Exemplo 1.40. Na Figura 1.7, à esquerda temos a maior bola euclidiana possível, dentro da região de Voronoi na métrica euclidiana do ponto $(0,0)$ e à direita a maior bola da soma possível dentro da região de Voronoi do ponto $(0,0)$ na métrica da soma.*

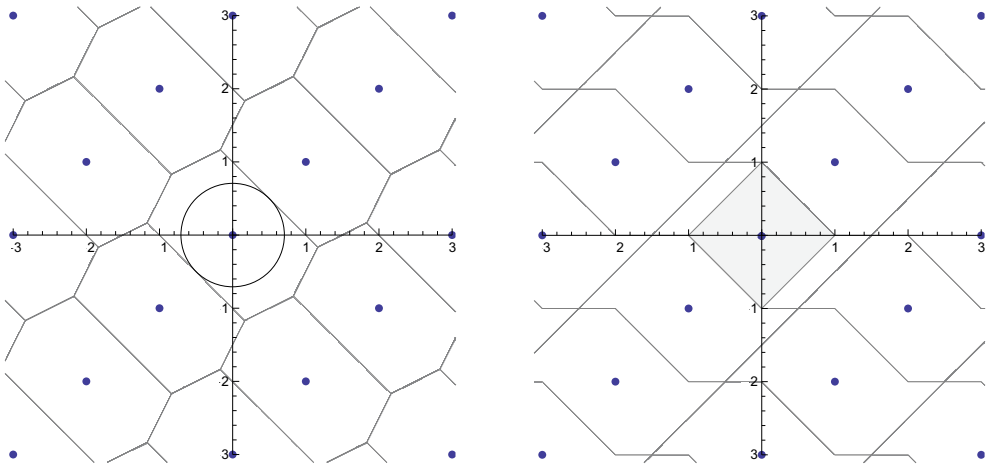


Figura 1.7: Maior bola euclidiana e da soma possíveis dentro de uma região de Voronoi do reticulado Λ do exemplo 1.40

Definição 1.45. *Seja d uma métrica em $\mathbb{R}^n$. A* ***norma mínima*** *η na métrica d de um reticulado $\Lambda \subseteq \mathbb{R}^n$ é definida por*

$$\eta = min\{d(x,0) : x \in \Lambda,\ x \neq 0\}.$$

Os vetores do reticulado Λ que satisfazem a norma mínima são chamados de ***vetores de norma mínima****.*

Lema 1.46. *Seja d uma métrica em $\mathbb{R}^n$ e Λ um reticulado. Definamos*

$$\overline{\rho} = máx\{r : B_d(u,r) \cap B_d(v,r) = \varnothing, u, v \in \Lambda\}.$$

Temos $\overline{\rho} = \rho$, onde ρ é o raio de empacotamento do reticulado.

Demonstração. Considere a bola fechada $B_d[0,\overline{\rho}]$. Afirmamos que $B_d[0,\overline{\rho}] \subset R(0)$. De fato, suponha que $B_d[0,\overline{\rho}] \nsubseteq R(0)$, logo existe $x \in B_d[0,\overline{\rho}]$ tal que $\|x\| \geq \|x-v\|$, para algum $v \in \Lambda$. Então, $x \in B_d(0,\overline{\rho}) \cap B_d(v,\overline{\rho})$, pois $\|x-v\| \leq \|x\| \leq \overline{\rho}$. Mas isso contradiz a definição de $\overline{\rho}$. Assim, $B_d[0,\overline{\rho}] \subset R(0)$ e pela maximalidade de ρ segue que $\rho \geq \overline{\rho}$.

Agora como a região de Voronoi de um ponto v do reticulado pode ser dada por $R(0)+v$, podemos considerar $\rho = \text{máx}\{r : B_d[v,r] \subset R(v), v \in \Lambda\}$. Suponha que existam $u, v \in \Lambda$ e um $x \in \mathbb{R}^n$ tais que $x \in B_d(u,\rho) \cap B_d(v,\rho)$. Daí temos $x \in B_d(u,\rho) \subset R(u)$ e $x \in B_d(v,\rho) \subset R(v)$, logo $x \in R(u) \cap R(v)$. Como as regiões de Voronoi se intercectam apenas em sua fronteira, x pertence à fronteira de $R(u)$, logo qualquer bola aberta centrada em u possui pontos de $R(u)$ e pontos de $\mathbb{R}^n - R(u)$. Em particular, a bola $B_d(u,\rho)$ possui

pontos de $\mathbb{R}^n - R(u)$, mas isso contradiz a definição de ρ. Logo $B_d(u,\rho) \cap B_d(v,\rho) = \varnothing$ e da maximalidade de $\overline{\rho}$ temos $\overline{\rho} \geq \rho$. Portanto, $\overline{\rho} = \rho$. □

Proposição 1.47. *[19] Seja d uma métrica em $\mathbb{R}^n$ e $\Lambda \in \mathbb{R}^n$. O raio de empacotamento ρ é metade da norma mínima η de Λ na métrica d.*

Demonstração. Sejam $u, v \in \Lambda$, $u \neq v$ e $r = \dfrac{\eta}{2}$. Suponhamos que $x \in B_d(u,r) \cap B_d(v,r)$. Por um lado temos $d(u,x) + d(x,v) \geq d(u,v) = d(u-v,0) \geq \eta$. Por outro lado temos $d(u,x) + d(x,v) < r + r = \eta$, o que é uma contradição. Logo, temos $B_d(u,r) \cap B_d(v,r) = \varnothing$. Mostremos que $r = \dfrac{\eta}{2}$ é o maior raio possível para um empacotamento reticulado. Se $r > \dfrac{\eta}{2}$, seja $u \in \Lambda$ tal que $d(u,0) = \eta$, então para $w = u/2 \in \mathbb{R}^n$ temos $d(w,u) = d(w,0) = \dfrac{\eta}{2} < r$, mas isto é uma contradição, pois teríamos que $w \in B_d(u,r) \cap B_d(0,r)$. Portanto, $r = \rho$. □

Definição 1.48. *Definimos a* **densidade** *de um reticulado Λ em $\mathbb{R}^n$ por*

$$\Delta(\Lambda) = \frac{vol(B_d[0,r])}{vol(R(0))}.$$

Pela Proposição 1.34 e a Observação 1.31, temos $vol(R(0)) = vol(P) = (det(\Lambda))^{1/2}$, sendo P o paralelotopo fundamental de Λ, logo

$$\Delta(\Lambda) = \frac{vol(B_d[0,r])}{(det(\Lambda))^{1/2}}.$$

Assim, a densidade depende apenas de uma base e da norma mínima de Λ. Isso facilita bastante o cálculo da densidade do reticulado, já que na prática determinar a região de Voronoi de um reticulado é um problema nada trivial.

O volume de uma bola $n-$dimensional de raio r é dado por $V_n r^n$, onde V_n é o volume da bola unitária. [16].

Para a distância euclidiana o volume da esfera unitária é dado por [16]:

$$V_{n_{eucl}} = \begin{cases} \dfrac{\pi^{n/2}}{\frac{n}{2}!}, & \text{se } n \text{ é par,} \\ \dfrac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!}, & \text{se } n \text{ é ímpar.} \end{cases} \tag{1.2}$$

Para a distância da soma o volume da esfera unitária é dado por [15]:

$$V_{n_{soma}} = \frac{2^n}{n!}$$

Exemplo 1.49. *Considere o reticulado hexagonal com a base* $\{(1,0),(1/2,\sqrt{3}/2)\}$. *Temos que a sua densidade na métrica euclidiana e da soma são dadas por*

$$\Delta_{eucl}(\Lambda) = \frac{\pi/4}{\sqrt{3}/2} \simeq 0,9069 \text{ e } \Delta_{soma}(\Lambda) = \frac{1/2}{\sqrt{3}/2} \simeq 0,5773.$$

Definição 1.50. *Definimos a* ***densidade de centro*** *de um empacotamento reticulado* Λ *por*

$$\delta = \frac{\Delta}{(det(\Lambda))^{1/2}} = \frac{\rho^n}{(det(\Lambda))^{1/2}},$$

sendo ρ *o raio de empacotamento.*

Como o volume da bola unitária n-dimensional é conhecido, o estudo de empacotamentos reticulados pode ser reduzido ao cálculo da densidade de centro.

Veremos na Seção 1.7.1 que, se considerarmos a métrica euclidiana, ao rotacionarmos um reticulado, o novo reticulado possuirá a mesma densidade do anterior, mas o mesmo pode não acontecer se considerarmos a métrica da soma.

1.6 O raio de cobertura

Podemos considerar o problema do raio de cobertura como o dual do problema do raio de empacotamento. O que se deseja é, dado um reticulado, encontrar um raio tal que a união de esferas de mesmo raio centradas nos pontos do reticulado cubra todo o $\mathbb{R}^n$ e a proporção de áreas sobrepostas das esferas seja a menor possível.

Definição 1.51. *Dados um reticulado* Λ *em* $\mathbb{R}^n$ *e uma métrica* d, *chamamos de* **raio de cobertura** *do reticulado o valor*

$$\zeta = min\{r : \mathbb{R}^n \subseteq \Lambda + B_d[0,r]\}.$$

Para um bom empacotamento procuramos um reticulado que maximize a área da região de $\mathbb{R}^n$ coberta por esferas, por outro lado, para uma boa cobertura procuramos um reticulado que minimize a área das regiões justapostas da cobertura. Para medir o quanto uma cobertura é melhor do que a outra neste sentido, temos uma taxa análoga a densidade de empacotamento, chamada de *densidade de cobertura.*

Definição 1.52. *Seja* d *uma métrica,* Λ *um reticulado no* $\mathbb{R}^n$ *e* ζ *o seu raio de cobertura na métrica* d, *a* **densidade de cobertura** θ *do reticulado* Λ *é dada por*

$$\theta = \frac{vol(B_d[0,\zeta])}{(det(\Lambda))^{1/2}} = \frac{V_n \zeta^n}{(det(\Lambda))^{1/2}},$$

sendo V_n é o volume da bola n-dimensional unitária.

Exemplo 1.53. *Considere o reticulado $\mathbb{Z}^2$. Na Figura 1.8 à esquerda temos o raio de cobertura em relação à distância euclidiana. Este raio é igual a $\sqrt{2}/2$. A figura da direita mostra o raio de cobertura deste reticulado em relação à distância da soma. Este raio é igual a 1. A densidade de cobertura deste reticulado nas métricas euclidiana e da soma são dadas respectivamente, por*

$$\theta_{eucl}(\Lambda) = \frac{\pi}{2} \text{ e } \theta_{soma}(\Lambda) = 2$$

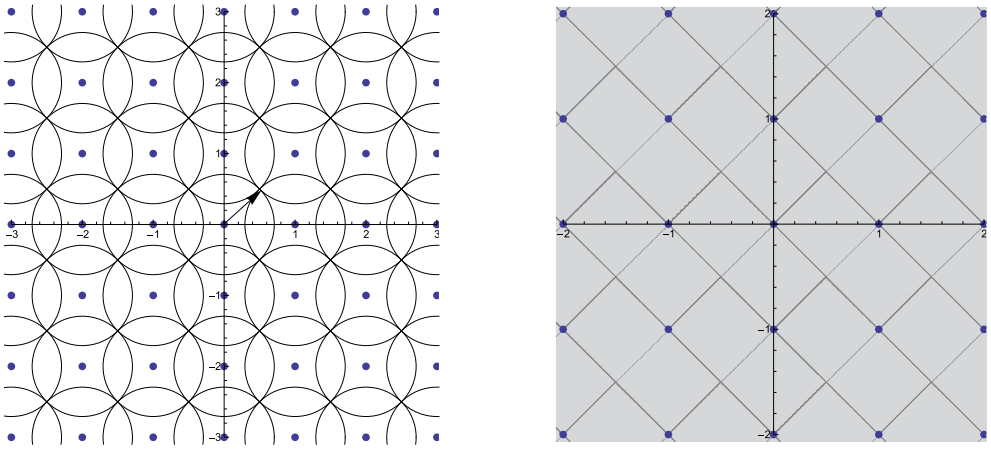


Figura 1.8: Raio de cobertura no reticulado $\mathbb{Z}^2$

Observação 1.54. *[12] Se ζ e τ são os raios de cobertura de um reticulado Λ nas métricas euclidiana e da soma, respectivamente, então temos $\zeta \leq \tau \leq \sqrt{n}\zeta$.*

1.7 Reticulados equivalentes

Definição 1.55. *Seja d uma métrica em $\mathbb{R}^n$. Uma aplicação φ em $\mathbb{R}^n$ é uma isometria na métrica d se, dados $x, y \in \mathbb{R}^n$, temos $d(x,y) = d(\varphi(x), \varphi(y))$.*

Definição 1.56. *Dois reticulados Λ_1 e Λ_2 são ditos* **equivalentes** *na métrica d se existe uma isometria $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ e um número real positivo λ tais que $(\lambda\varphi)(\Lambda_1) = \Lambda_2$. Dizemos que λ é a* **razão de semelhança** *de Λ_1 para Λ_2. Quando $\lambda = 1$ dizemos que os reticulados são congruentes.*

1.7.1 Reticulados equivalentes na métrica Euclidiana

As isometrias no espaço euclidiano $\mathbb{R}^n$ são dadas por rotações em torno de "retas" $n-2$ dimensionais, reflexões em torno de "planos"$n-1$ dimensionais, translações e composições destas [21]. A matriz de uma rotação ou de uma reflexão é uma matriz ortogonal, ou seja, é uma matriz não singular O, tal que $O^TO = OO^T = I$. É fácil verificar que composições de matrizes ortogonais também são matrizes ortogonais, assim, toda isometria euclidiana φ pode ser escrita como

$$\varphi(x) = O\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

onde O é uma matriz ortogonal e $x^t = (x_1, ..., x_n), c^t = (c_1, ..., c_n) \in \mathbb{R}^n$.
Como transformações ortogonais levam base em base, rotações e reflexões levam um reticulado em um reticulado e, se c é um vetor do reticulado, pelo Corolário 1.9 o reticulado $\Lambda' := \Lambda + c$, trasladado por c, é um reticulado. Mais precisamente Λ' é o próprio reticulado Λ. Agora, se c não é um vetor do reticulado não é verdade que o conjunto

$$S = \{v + c, v \in \Lambda\}$$

é um reticulado.
De fato, se S fosse um reticulado, S seria um subgrupo discreto do $\mathbb{R}^n$, assim dados $u, v \in \Lambda$, os vetores $u + c$ e $v + c$ pertenceriam a S ,e portanto, $(u + c) - (v + c) = u - v \in S$. Logo, $u - v = z + c$ para algum $z \in \Lambda$. Daí teríamos que $c = u - v - z \in \Lambda$, o que é uma contradição.

Decorre que na métrica euclidiana as isometrias em reticulados são dadas por rotações, reflexões, translações por vetores do reticulado e a composição destas três. Como as translações por vetores do reticulado levam o reticulado no próprio reticulado, podemos considerar no estudo de reticulados equivalentes na métrica euclidiana apenas as rotações e as reflexões.

Proposição 1.57. *[5] Se Λ_1 e Λ_2 são reticulados equivalentes na métrica euclidiana, então existem matrizes de Gram G_1 e G_2 de Λ_1 e Λ_2 respectivamente e um número real positivo λ tais que*
i) $G_2 = \lambda^2 U^T G_1 U$, onde U é uma matriz unimodular;
ii)$\rho_2 = \lambda\rho_1$, sendo ρ_1 e ρ_2 raios de empacotamento de Λ_1 e Λ_2, respectivamente.
iii)$\Delta(\Lambda_1) = \Delta(\Lambda_2)$.

Demonstração. i) Se A é uma matriz geradora do reticulado Λ_1, como Λ_1 e Λ_2 são equivalentes, existem um $\lambda \in \mathbb{R}$ positivo e matrizes U unimodular e M ortogonal, tais que a matriz λMAU é a matriz geradora de Λ_2. Assim,

$$G_2 = (\lambda MAU)^T(\lambda MAU) = \lambda^2 U^T A^T M^T MAU = \lambda^2 U^T A^T AU = \lambda^2 U^T G_1 U.$$

ii) Sejam φ uma aplicação ortogonal e $\lambda \in \mathbb{R}$ positivo, tais que $(\lambda\varphi)(\Lambda_1) = \Lambda_2$. Dado $v \in \Lambda_1$, temos que $\|\lambda\varphi(v)\|_2 = \lambda\|v\|_2$. Por outro lado, existe um $x \in \Lambda_2$ tal que $\|\lambda\varphi(v)\|_2 = \|x\|_2$, logo $\|x\|_2 = \lambda\|v\|_2$. Assim, se ρ_1 e ρ_2 são o raio de empacotamento e Δ_1 e Δ_2 são as densidades de Λ_1 e Λ_2 respectivamente, temos

$$\frac{min\{\|x\|_2 : x \in \Lambda_2\}}{2} = \frac{min\{\lambda\|v\|_2 : v \in \Lambda_1\}}{2} = \frac{\lambda min\{\|v\|_2 : v \in \Lambda_1\}}{2}$$

e daí o raio de empacotamento de λ_2 é $\rho_2 = \lambda\rho_1$.

iii) Com as mesmas notações da demonstração do item (i) e recordando que matrizes unimodulares têm o determinante igual a ± 1, temos

$$det(\Lambda_2) = det(\lambda^2 U^T G_1 U) = \lambda^{2n} det(U^T U) det(G_1) = \lambda^{2n} det(\Lambda_1).$$

Daí

$$\Delta_2 = \frac{V_{n_{eucl}}\rho_2^n}{(det(\Lambda_2)^{1/2}} = \frac{V_{n_{eucl}}(\lambda\rho_1)^n}{\lambda^n(det(\Lambda_2)^{1/2}} = \Delta_2.$$

□

Temos uma recíproca do item i da Proposição 1.57, na proposição abaixo.

Proposição 1.58. *[16] Sejam Λ_1 e Λ_2 reticulados, se existem matrizes de Gram G_1 e G_2 dos reticulados Λ_1 e Λ_2 respectivamente, tais que $G_2 = \lambda G_1$, então os reticulados são equivalentes na métrica euclidiana.*

Demonstração. Sejam $\beta_1 = \{u_1, ..., u_n\}$ e $\beta_2 = \{v_1, ..., v_n\}$ bases dos reticulados Λ_1 e Λ_2 as quais as matrizes de Gram G_1 e G_2, tais que $G_2 = \lambda G_1$, estão associadas. Então, a aplicação linear $T : \mathbb{R}^n \to \mathbb{R}^n$, definida por $T(u_i) = \frac{1}{\lambda}v_i$ é uma isometria tal que $(\lambda T)(\Lambda_1) = \Lambda_2$.
De fato, como $G_2 = \lambda^2 G_1$, temos $\lambda^2\langle u_i, u_j\rangle = \langle v_i, v_j\rangle$, para $i, j = 1, ..., n$. Assim, dado $u = a_1u_1 + \cdots + a_nu_n \in \Lambda_1$, temos

$$\begin{aligned}\|T(u)\|_2^2 = \ & \langle T(u), T(u)\rangle \\ & = \langle a_1T(u_1) + \cdots + a_nT(u_n), a_1T(u_1) + \cdots + a_nT(u_n)\rangle \\ & = \langle a_1\frac{1}{\lambda}v_1 + \cdots + a_n\frac{1}{\lambda}v_n, a_1\frac{1}{\lambda}v_1 + \cdots + a_n\frac{1}{\lambda}v_n\rangle \\ & = \sum_{i,j=1}^{n} a_ia_j\frac{1}{\lambda^2}\langle v_i, v_j\rangle \\ & = \sum_{i,j=1}^{n} a_ia_j\frac{1}{\lambda^2}.\lambda^2\langle u_i, u_j\rangle \\ & = \langle u, u\rangle \\ & = \|u\|^2.\end{aligned}$$

Logo, dados $u, v \in \Lambda_1$ temos

$$d(T(u), T(v)) = d(T(u) - T(v), 0) = d(T(u - v), 0) = \|T(u - v)\|_2 = \|u - v\|_2 = d(u - v, 0) = d(u, v).$$

Portanto, T é uma isometria.
Agora, para $x = a_1u_1 + \cdots + a_nu_n \in \Lambda_1$, temos que

$$(\lambda T)(x) = \lambda[(1/\lambda)a_1v_1 + \cdots + (1/\lambda)a_nv_n] = a_1v_1 + \cdots + a_nv_n \in \Lambda_2.$$

Logo $(\lambda T)(\Lambda_1) \subseteq \Lambda_2$.
E dado $y = b_1v_1 + \cdots + b_nv_n \in \Lambda_2$, tomando $w = b_1u_1 + \cdots + b_nu_n \in \Lambda_1$, obtemos $(\lambda T)(w) = y$.
Assim, concluímos a igualdade $(\lambda T)(\Lambda_1) = \Lambda_2$. □

Seja Λ é um reticulado com base $\{u_1, ..., u_n\}$. Como uma rotação R é uma transformação ortogonal ela leva base em base e assim considerando a métrica euclidiana, $R(\Lambda)$ também é um reticulado com base $\{T(u_1), ..., T(u_n)\}$. Sendo R uma isometria, os reticulados Λ e $\Lambda' = R(\Lambda)$ são equivalentes, logo possuem a mesma densidade, isto é, uma rotação preserva a densidade de um reticulado na métrica euclidiana, mas o mesmo não acontece se considerarmos a métrica da soma.

1.7.2 Reticulados equivalentes na métrica da soma

Desejamos saber quais são as isometrias possíveis no $\mathbb{R}^n$ em relação à métrica da soma.

Proposição 1.59. *[12] Se $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é uma isometria com a métrica da soma, então $f = a + \phi$, onde $a \in \mathbb{R}^n$ e ϕ é uma isometria na métrica da soma tal que $\phi(0) = 0$.*

Demonstração. Tomemos $a = f(0)$ e $\phi(x) = f(x) - a$. Temos que

$$d(\phi(x), \phi(y)) = d(f(x) - a, f(y) - a) = d(f(x), f(y))$$

e $\phi(0) = f(0) - a = 0$.

□

Proposição 1.60. *Se $\phi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é uma isometria linear com a métrica da soma, então $\phi(e_i) = \pm e_j$ e se $i \neq j$ temos que $\phi(e_i) \neq \phi(e_j)$, para todo $1 \leq i, j \leq n$.*

Demonstração. Como $\phi : \mathbb{R}^n \to \mathbb{R}^n$ é isometria linear, $d(\phi(e_i), 0) = d(\phi(e_i), \phi(0)) = d(e_i, 0) = 1$, $i = 1, ..., n$, logo $\phi(e_i)$ pertence ao bordo de $B_{soma}[0, 1]$. Suponha $\phi(e_1) \neq e_j$, para todo $j = 1, ..., n$. Assim existem pelo menos duas entradas não nulas no vetor $\phi(e_1)$. Seja $\phi(e_j) = (a_{j1}, ..., a_{jn})$, para todo $j = 1, ..., n$. Mostremos que existem $k, j \in \{1, ..., n\}$, $k \neq j$, tais que $\phi(e_k)$ e $\phi(e_j)$ possuem uma entrada não nula na mesma posição.
Se algum $\phi(e_j)$, $j \neq i$, tiver uma entrada não nula na mesma posição de $\phi(e_1)$ está feito. Agora, se isto não acontece, temos $n-2$ posições para verificar se dentre $n-1$ vetores existem dois com uma entrada não nula em comum. Como estes vetores não podem ser nulos, isto acontece. Assim, sejam $k, j \in \{1, ..., n\}$, $k \neq j$, tais que $\phi(e_k)$ e $\phi(e_j)$ possuem uma entrada não nula em comum, isto é, existe i tal que $a_{ki} = a_{ji} \neq 0$. Pela desigualdade triangular temos $|a+b| \leq |a|+|b|$ e a igualdade vale se, e somente se, $ab \geq 0$. Temos dois casos a analisar.

- Se $a_{ki}(-a_{ji}) < 0$, temos $|a_{ki} + (-a_{ji})| < |a_{ki}| + |-(a_{ji})|$ e assim

$$\begin{aligned} 2 &= d(e_k, e_j) \\ &= d(\phi(e_k), \phi(e_j)) \\ &\sum_{l=1, l\neq i}^{n} |a_{kl} + (-a_{jl})| + |a_{ki} + (-a_{ji})| \\ &\sum_{l=1, l\neq i}^{n} |a_{kl}| + |(-a_{jl})| + |a_{ki}| + |(-a_{ji})| \\ &< 2, \end{aligned}$$

  o que é uma contradição.

- Se $a_{ki}(-a_{ji}) > 0$, então $a_{ki}a_{ji} < 0$, daí temos $|a_{ki} + a_{ji}| < |a_{ki}| + |a_{ji}|$ e assim

$$\begin{aligned} 2 &= d(e_k, -e_j) \\ &= d(\phi(e_k), \phi(-e_j)) \\ &= \sum_{l=1, l\neq i}^{n} |a_{kl} + a_{jl}| + |a_{ki} + a_{ji}| \\ &< \sum_{l=1, l\neq i}^{n} |a_{kl}| + |a_{jl}| + |a_{ki}| + |a_{ji}| \\ &< 2, \end{aligned}$$

  o que é uma contradição. Logo não podemos ter duas entradas em comum, o que implica que $\phi(e_i)$ só pode ter uma entrada não nula, $\phi(e_i) = \pm e_k$ e $\phi(e_i) \neq \phi(e_j)$, se $i \neq j$, para todo $1 \leq i, j \leq n$.

□

As isometrias descritas na Proposição 1.60 são aplicações ortogonais, cujas matrizes possuem em cada coluna somente uma entrada não nula igual a ± 1. Assim as aplicações ortogonais cujas matrizes possuem a forma que acabamos de descrever compostas com uma translação são isometrias de $\mathbb{R}^n$ com a métrica da soma. De fato, é possível mostrar que estas são as únicas isometrias de $\mathbb{R}^n$ na métrica da soma [20]. Com as mesmas observações que fizemos para as isometrias euclidianas em reticulados com respeito às translações, no estudo de reticulados equivalentes com a métrica da soma, nos restringiremos apenas às isometrias dadas pela Proposição 1.60.

Observação 1.61. *A Proposição 1.57 continua sendo válida para reticulados equivalentes na métrica da soma. A demonstração da proposição para a métrica da soma é análoga à feita para a métrica euclidiana, sendo necessário apenas mudar as normas, já que as transformações ortogonais descritas na Proposição 1.60 também preservam a norma da soma. De fato, se $x \in \mathbb{R}^n$, podemos escrever x da forma $x = x_1e_1 + \cdots + x_ne_n$ e então $\phi(x) = x_1\phi(e_1) + \cdots + x_n\phi(e_n)$. Fazendo uma reordenação nas coordenadas de $\phi(x)$ temos*

$$\phi(x) = (\pm x_{k1})e_1 + (\pm x_{k2})e_2 + \cdots + (\pm x_{kn})e_n,$$

onde $k_i \in \{1, 2, ..., n\}$ e se $i \neq j$, então $x_{ki} \neq x_{kj}$. Tomando as normas da soma de x e $\phi(x)$, obtemos

$$\|x\|_1 = \sum_{i=1}^{n} |x_i| = \sum_{i=1}^{n} |\pm x_{ki}| = \|\phi(x)\|_1 .$$

Proposição 1.62. *Reticulados equivalentes na métrica da soma são equivalentes na métrica euclidiana.*

Demonstração. Seja $\phi : \mathbb{R}^n \to \mathbb{R}^n$ uma isometria na métrica da soma, assim $e_i \neq e_j$ se, e somente se $\Phi(e_i) \neq \Phi(e_j)$, logo

$$d_{euclid}(\phi(e_i), \phi(e_j)) = \sqrt{2} = d_{euclid}(e_i, e_j).$$

É claro que se $e_i = e_j$, então $d_{euclid}(\phi(e_i), \phi(e_j)) = d_{euclid}(e_i, e_j)$. Decorre que ϕ é uma isometria linear na métrica euclidiana. □

Exemplo 1.63. *[12] Considere o reticulado $\mathbb{Z}^2$ com a métrica da soma. Temos que sua densidade de empacotamento na métrica da soma é $\triangle_{soma}(\mathbb{Z}^2) = \dfrac{2^2(1/2)^2}{2!} = \dfrac{1}{2} = 0,5$. Agora seja R uma rotação de 45 graus em torno da origem. A densidade de $R(\mathbb{Z}^2)$ na métrica da soma é $\triangle_{soma}(R(\mathbb{Z}^2)) = \dfrac{2^2(\sqrt{2}/2)^2}{2!} = 1$ que é máxima em sua dimensão.*

Na Figura 1.9 temos à esquerda e à direita respectivamente, os empacotamentos na métrica da soma do reticulado $\mathbb{Z}^2$ e do reticulado $R(\mathbb{Z}^2)$.

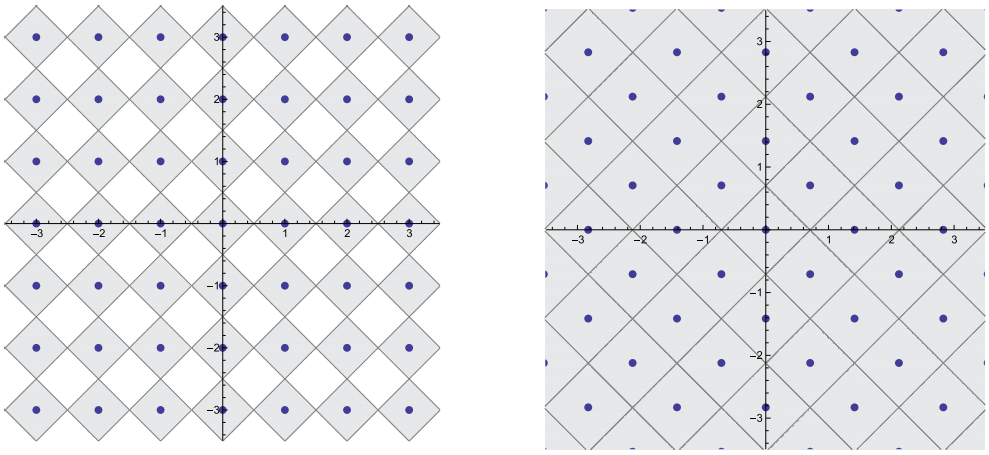


Figura 1.9: Empacotamento dos reticulados $\mathbb{Z}^2$ e $R(\mathbb{Z}^2)$

Observação 1.64. *O Exemplo 1.63, mostra que a recíproca da Proposição 1.62 não vale. De fato, o reticulado $\mathbb{Z}^2$ e o reticulado $\mathbb{Z}^2$ rotacionado por 45 graus, são equivalentes na métrica euclidiana, mas não são equivalentes na métrica da soma, pois se fossem a densidade de empacotamento na métrica da soma dos dois reticulados seria a mesma.*

Observação 1.65. *A Proposição 1.58 também não é válida para reticulados na métrica da soma. De fato, é fácil verificar que os reticulados do Exemplo 1.63 possuem a mesma matriz*

de Gram, mas o mesmo argumento usado na observação acima mostra que estes reticulados não são equivalentes na métrica da soma.

1.8 Exemplos de reticulados

Nesta seção descreveremos alguns reticulados importantes e suas propriedades. A principal referência é [16].

1.8.1 Os reticulados cúbicos $\mathbb{Z}^n$

O reticulado cúbico $\mathbb{Z}^n$ é o conjunto

$$\mathbb{Z}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{Z},\ i = 1, ..., n\}$$

A matriz geradora deste reticulado é a matriz identidade de ordem n, logo seu determinante é igual a 1. Na métrica euclidiana e da soma a norma mínima é 1 e os vetores de norma mínima são $(0, ..., \pm 1, ..., 0)$. O raio de empacotamento é $\rho = \frac{1}{2}$. Na métrica euclidiana o raio de cobertura é $\frac{\sqrt{n}}{2} = \rho.\sqrt{n}$. A densidade nas métricas euclidianas e da soma é dada por $\Delta = V_n 2^{-n}$, onde devemos considerar V_n como o volume da bola unitária $n-$dimensional em cada métrica. E a densidade de centro em ambas as métricas é $\delta = 2^{-n}$. As regiões de Voronoi na métrica euclidiana e da soma são iguais e têm a forma de hipercubos. O reticulado $\mathbb{Z}^n$ é auto dual.
Na dimensão 2 sua versão rotacionada por 45 graus apresenta a maior densidade de empacotamento e a menor densidade de cobertura possíveis na dimensão e ambas são iguais a 1. Isso porque a região de Voronoi do reticulado e as bolas de raio ρ e ζ coincidem.

1.8.2 Os reticulados A_n

O reticulado A_n é o conjunto

$$A_n = \{(x_0, x_1, ..., x_n) \in \mathbb{Z}^{n+1} : x_0 + \cdots + x_n = 0\}.$$

Observe que são usadas $n+1$ coordenadas, para definir o reticulado A_n que está no hiperplano $\sum x_i = 0$.
Uma matriz geradora é dada por

$$\begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & -1 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

O seu determinante é $n+1$. Na métrica euclidiana e da soma, as normas mínimas são $\sqrt{2}$ e 2, respectivamente, e os vetores de norma mínima são todas as permutações de $(1,-1,0,...,0)$. Os raios de empacotamento na métrica euclidiana e da soma são $\rho = \dfrac{1}{\sqrt{2}}$ e 1, respectivamente. O raio de cobertura na métrica euclidiana é $\zeta = \rho(2a(n+1-a)/(n+1))^{1/2}$, onde a é a parte inteira de $\dfrac{n+1}{2}$ [16].

O reticulado hexagonal, mostrado nos Exemplos 1.39 e 1.49 é equivalente na métrica euclidiana ao reticulado A_2. De fato, o reticulado hexagonal pode ser gerado pelos vetores $(1,0)$ e $\left(\dfrac{-1}{2}, \dfrac{\sqrt{3}}{2}\right)$, enquanto que o reticulado A_2 é gerado pelos vetores $(-1,1,0)$ e $(0,-1,1)$, assim suas matrizes de Gram nestas bases estão associadas por

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} = (\sqrt{2})^2 \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

onde a matriz da esquerda é a matriz de Gram do reticulado hexagonal e a da direita é a matriz de Gram do reticulado A_2. Assim, pela Proposição 1.58, estes reticulados são equivalentes na métrica euclidiana.

O determinante do reticulado hexagonal é igual a $\dfrac{3}{4}$. Na métrica euclidiana sua norma mínima é $\eta = 1$, os vetores de norma mínima são $(\pm 1, 0)$ e $\left(\pm\dfrac{1}{2}, \pm\dfrac{\sqrt{3}}{2}\right)$, o raio de empacotamento é $\rho = \dfrac{1}{2}$, a densidade de empacotamento é $\Delta = \dfrac{\pi}{\sqrt{12}}$ e o raio de cobertura é $\zeta = \dfrac{2\rho}{\sqrt{3}}$. O reticulado hexagonal possui a maior densidade de empacotamento na dimensão 2.

1.8.3 Os reticulados D_n

O reticulado D_n, para $n \geq 3$ é definido por

$$D_n = \{(x_1, ..., x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \text{ é par}\},$$

ou, dito de outro modo, D_n é obtido colorindo os pontos de $\mathbb{Z}^n$ alternadamente de vermelho e branco, como em um tabuleiro de xadrez e pegando apenas os pontos vermelhos, por isso D_n as vezes é chamado de reticulado *checkboard*.
Uma matriz geradora de D_n é dada por

$$\begin{pmatrix} -1 & 1 & 0 & \cdots & 0 \\ -1 & -1 & 1 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & -1 \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}$$

O determinante de D_n é 4. Na métrica euclidiana e da soma as normas mínimas são $\eta = \sqrt{2}$ e 2, respectivamente, os vetores de norma mínima são todas as permutações de $(\pm 1, \pm 1, 0..., 0)$, o raio de empacotamento na métrica euclidiana e da soma são $\rho = \dfrac{1}{\sqrt{2}}$ e 1, respectivamente. Na métrica euclidiana a densidade de centro é $\delta = 2^{-(n+2)/2}$, e o raio de cobertura é $\zeta = \rho\sqrt{2}$.

O reticulado D_3 é equivalente a A_3 na métrica euclidiana e é conhecido também por reticulado *face-centered cubic*. Na métrica euclidiana, D_3, D_4 e D_5 são os empacotamentos reticulados mais densos possíveis em dimensão $3, 4$ e 5.

1.8.4 Os reticulados E_6, E_7 e E_8

O reticulado E_8 é o conjunto

$$E_8 = \{(x_1, ..., x_8) : \text{todo } x_i \in \mathbb{Z} \text{ ou todo } x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \text{ é par}\}$$

Uma matriz geradora para E_8 é

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}$$

O determinante de E_8 é 1. Na métrica euclidiana e da soma, as normas mínimas são $\eta = \sqrt{2}$ e 2, respectivamente, os raios de empacotamento são $\rho = \frac{1}{\sqrt{2}}$ e 1, respectivamente. Na métrica euclidiana a densidade é $\Delta = \frac{\pi^4}{384} \simeq 0,2537$, a densidade de centro é $\delta = \frac{1}{16}$, o raio de cobertura é $\zeta = \rho\sqrt{2} = 1$ e a densidade de cobertura é $\theta = \frac{\pi^4}{24} \simeq 4,0584$. O reticulado E_8 é auto dual e possui a maior densidade na métrica euclidiana na dimensão 8.

Obtemos os reticulados E_7 e E_6 a partir do reticulado E_8 da seguinte forma:

$$E_7 = \{(x_1, ..., x_8) \in E_8 : x_1 + ... + x_8 = 0\} \text{ e}$$

$$E_6 = \{(x_1, ..., x_8) \in E_8 : x_1 + x_8 = x_2 + \cdots + x_7 = 0\}$$

O determinante de E_7 é 2. Na métrica euclidiana a norma mínima é $\eta = \sqrt{2}$, o raio de empacotamento é $\rho = \frac{1}{\sqrt{2}}$, a densidade de empacotamento é $\Delta = \frac{\pi^3}{105} \simeq 0,2953$, a densidade de centro é $\delta = \frac{1}{16}$ e o raio de cobertura é $\zeta = \rho\sqrt{3} = \frac{\sqrt{3}}{2}$.

Já o reticulado E_6 possui determinante igual a 3. Na métrica euclidiana este reticulado possui norma mínima $\eta = \sqrt{2}$, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade de empacotamento $\Delta = \frac{\pi^3}{48\sqrt{3}} \simeq 0,03729$, densidade de centro $\delta = \frac{1}{8\sqrt{3}}$ e raio de cobertura $\zeta = \rho\sqrt{8/3}$. Estes reticulados apresentam a maior densidade de empacotamento na métrica euclidiana em suas dimensões 7 e 6 respectivamente.

1.9 Decodificação em reticulados

Dado um reticulado n-dimensional Λ, uma métrica d em $\mathbb{R}^n$ e um ponto $z \in \mathbb{R}^n$, decodificar o reticulado Λ corresponde a encontrar o ponto de Λ mais próximo de z, ou seja, encontrar $x \in \Lambda$ tal que

$$d(x,z) = min\{d(y,z) : z \in \Lambda\}.$$

Este problema é conhecido como *Closest Vector* (CVP). A dificuldade em resolver este problema é encontrar este vetor mais próximo sem ter que recorrer a complexidade de uma busca exaustiva. Alguns reticulados conhecidos que apresentam características especiais possuem algoritmos próprios de decodificação para a métrica euclidiana, como, por exemplo, os reticulados $\mathbb{Z}^n$, D_n e E_8. Para reticulados gerais, a maioria dos algoritmos de decodificação são estudados na métrica euclidiana, mas muito poucos algoritmos de decodificação na métrica da soma são conhecidos. Em [4] e [11] é apresentado o algoritmo **Sphere decoding** para decodificação de reticulados na métrica euclidiana que usa a fatoração QR e de *Cholesky*, respectivamente, na matriz geradora do reticulado. Estas fatorações não podem ser aplicadas à métrica da soma, pois no decorrer do algoritmo elas estão associadas à propriedades específicas da métrica euclidiana. Em [12] e [1] é apresentado uma adaptação do *Sphere Decoding* como um método de decodificação de reticulados para a métrica da soma. Nesta seção apresentaremos o *Sphere Decoding* usando a fatoração QR [4] e a adaptação do *Sphere Decoding* para a métrica d_p, $1 \leq p < \infty$ [12].

1.9.1 *Sphere decoding* na métrica euclidiana

A ideia básica do algoritmo *Sphere Decoding* é bastante simples: seja Λ um reticulado m-dimensional, com $m \leq n$ e $z \in \mathbb{R}^n$. O algoritmo consiste em procurar os pontos do reticulado Λ que estão em uma esfera euclidiana de raio $\mathcal{R}$ em torno do vetor dado z. Desta forma, o espaço de busca fica reduzido e por conseguinte, as computações necessárias. Claramente o ponto do reticulado Λ mais próximo de z dentro desta esfera, será o ponto mais próximo de todo o reticulado. Para aplicar o método, temos duas questões a resolver:

1) *A escolha do raio* $\mathcal{R}$.

Se $\mathcal{R}$ for muito grande, obtêm-se muitos pontos do reticulado dentro da esfera. Por outro lado, se $\mathcal{R}$ for muito pequeno, não é garantida a existência de um ponto do reticulado dentro da esfera. Um candidato natural é o raio de cobertura do reticulado, mas que para reticulados gerais não é muito fácil de ser encontrado. Uma outra escolha para $\mathcal{R}$ pode ser feita usando a estimativa de Babai. Se A é uma matriz geradora para o reticulado Λ e $\widehat{r} \in \mathbb{R}^m$ é a solução para o sistema

$$Ar = z,$$

então, a estimativa de Babai é dada por $[\widehat{r}]$, em que $[a]$ denota o vetor cujas as entradas são os números inteiros mais próximos das respectivas entradas de $a \in \mathbb{R}^m$. Assim, tomando o raio $\mathcal{R} = \|A[\widehat{r}] - z\|_2$, garantimos a existência de pelo menos um ponto do reticulado dentro da esfera centrada em z com este raio, a saber, $A[\widehat{r}]$, [4].

2) *Encontrar os pontos do reticulado dentro da esfera*

O *Sphere Decoding* não resolve a primeira questão, mas ele propõe um algoritmo eficiente para resolver a segunda.

Dado um ponto $x \in \Lambda$, temos $x = As$, onde A é a matriz geradora do reticulado e $s \in \mathbb{Z}^m$, então os pontos do reticulado que estão em uma esfera n-dimensional de raio $\mathcal{R}$ e centro z na métrica euclidiana são dados por $x = As$ tal que $s \in \mathbb{Z}^m$ e

$$\|z - As\|_2^2 \leq \mathcal{R}^2. \tag{1.3}$$

Para desmembrar o problema em subproblemas, é muito útil considerar a fatoração QR da matriz A, isto é, considerar

$$A = Q \begin{bmatrix} R \\ 0_{(n-m)\times m} \end{bmatrix} \tag{1.4}$$

onde R é uma matriz $m \times m$ triangular superior e $Q = [Q_1 \quad Q_2]$ é uma $n \times n$ matriz ortogonal, com Q_1 e Q_2 representando as primeiras m e $m - n$ colunas ortogonais de Q, respectivamente. Sempre que uma matriz $n \times m$ tem posto igual a m, é possível fatorá-la da forma descrita [13].

Recordemos que, como Q é ortogonal, temos $Q^tQ = I$ e $Q^t = \begin{bmatrix} Q_1^t \\ Q_2^t \end{bmatrix}$ também é uma matriz ortogonal. Portanto, Q^t preserva a norma euclidiana. Assim, a condição (1.3) pode ser escrita como

$$\|z - As\|_2^2 = \left\| z - [Q_1 \quad Q_2] \begin{bmatrix} R \\ 0 \end{bmatrix} s \right\|^2 = \left\| \begin{bmatrix} Q_1^t \\ Q_2^t \end{bmatrix} z - \begin{bmatrix} R \\ 0 \end{bmatrix} s \right\|_2^2 = \|Q_1^t z - Rs\|_2^2 + \|Q_2^t z\|_2^2 \leq \mathcal{R}^2$$

Desta forma, passamos a buscar $s \in \mathbb{Z}^n$ tal que

$$\left\|Q_1^t z - Rs\right\|_2^2 \leq \mathcal{R}^2 - \left\|Q_2^t z\right\|_2^2. \tag{1.5}$$

Colocando $y = Q_1^t z$ e $(\mathcal{R}')^2 = \mathcal{R}^2 - \|Q_2^t z\|_2^2$, podemos reescrever a desigualdade como

$$\sum_{i=1}^{m} \left(y_i - \sum_{j=i}^{n} r_{i,j} s_j \right)^2 \leq (\mathcal{R}')^2 \tag{1.6}$$

onde $r_{i,j}$ é a ij-ésima entrada de R. Expandindo o lado direito da desigualdade acima obtemos

$$(y_m - r_{m,m}s_m)^2 + (y_{m-1} - r_{m-1,m-1}s_{m-1} - r_{m-1,m}s_m)^2 +$$

$$\cdots + (y_1 - r_{1,1}s_1 - r_{1,2}s_2 - \cdots - r_{1,m}s_m)^2 \leq (R')^2 \tag{1.7}$$

onde o primeiro termo depende apenas de s_m, o segundo de s_m e s_{m-1} e assim por diante. Portanto, uma condição necessária para que As esteja na esfera é que

$$(y_m - r_{m,m}s_m)^2 \leq (\mathcal{R}'^2)$$

e esta condição só vale se s_m estiver no seguinte intervalo

$$\left\lceil \frac{-\mathcal{R}' + y_m}{r_{m,m}} \right\rceil \leq s_m \leq \left\lfloor \frac{\mathcal{R}' + y_m}{r_{m,m}} \right\rfloor \tag{1.8}$$

onde $\lceil a \rceil$ e $\lfloor a \rfloor$ denotam o menor inteiro maior ou igual a a e o maior inteiro menor ou igual a a, respectivamente, para $a \in \mathbb{R}$.

Agora, para cada s_m satisfazendo 1.7, definimos $(\mathcal{R}')^2_{m-1} = (\mathcal{R}')^2 - (y_m - r_{m,m}s_m)^2$ e $y_{m-1|m} = y_{m-1} - r_{m-1,m}s_m$, assim $(y_{m-1} - r_{m-1,m-1}s_{m-1} - r_{m-1,m}s_m)^2 \leq (\mathcal{R}')^2_{m-1}$ se, e somente se, s_{m-1} está no intervalo

$$\left\lceil \frac{-\mathcal{R}'_{m-1} + y_{m-1|m}}{r_{m-1,m-1}} \right\rceil \leq s_{m-1} \leq \left\lfloor \frac{\mathcal{R}'_{m-1} + y_{m-1|m}}{r_{m-1,m-1}} \right\rfloor. \tag{1.9}$$

Procedemos de forma análoga para s_{m-2} e assim por diante até obtermos s_1 e, por conseguinte, todos os pontos do reticulado da forma As que satisfazem (1.3).

1.9.2 *Sphere decoding* na métrica d_p, $1 \leq p < \infty$

Fazendo uma modificação no *Sphere decoding* clássico, podemos obter uma espécie de generalização do algoritmo para a métrica d_p, $1 \leq p < \infty$, para o caso em que o reticulado Λ é um reticulado n-dimensional inteiro. Dados dois vetores $x, y \in \mathbb{R}^n$ a métrica d_p é dada por

$$d_p(x, y) = (|x_1 - y_1|^p + \cdots + |x_n - y_n|^p)^{\frac{1}{p}}.$$

A ideia central do algoritmo para encontrar o ponto de um reticulado Λ mais próximo de um vetor dado $z \in \mathbb{R}^n$, continua sendo encontrar os pontos do reticulado dentro de uma bola na métrica d_p centrada em z com um certo raio R. A dificuldade de se encontrar o raio R ideal ainda permanece e, para o caso geral, não podemos mais aplicar a fatoração QR na matriz

do reticulado, já que a norma p, $1 \leq p < \infty$ e $p \neq 2$, nem sempre é preservada por uma matriz ortogonal qualquer.

Sejam Λ um reticulado inteiro n-dimensional, H uma matriz geradora para Λ na forma Normal de Hermite e $y \in \mathbb{R}^n$ um vetor dado. Escolhido um raio R, queremos encontrar os pontos do reticulado $x = Hs$, $s \in \mathbb{Z}^n$, que estão na bola na métrica d_p de centro y e raio R, ou seja, queremos encontrar os pontos $s \in \mathbb{Z}^n$ que satisfazem

$$d_p(Hs, y) = \|Hs - y\|_p \leq R. \tag{1.10}$$

Temos

$$\begin{pmatrix} h_{11} & h_{21} & \cdots & h_{n1} \\ 0 & h_{22} & \cdots & h_{n2} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & h_{nn} \end{pmatrix} (s_1, ..., s_n) = \left(\sum_{i=1}^{n} h_{i1}s_i, ..., h_{n-1,n-1}s_{n-1} + h_{n,n-1}s_n, h_{n,n}s_n \right).$$

Assim,

$$\|Hs-y\|_p^p = |\sum_{i=1}^{n} h_{i1}s_i - y_1|^p + \cdots + |h_{n-1,n-1}s_{n-1} + h_{n,n-1}s_n - y_{n-1}|^p + |h_{n,n}s_n - y_1|^p. \tag{1.11}$$

Encontraremos as soluções de $\|Hs-y\|_p^p \leq R^p$, formando uma árvore de possibilidades para $s_1, ..., s_n$.

Analisemos os possíveis valores para s_n. Temos que s_n satisfaz $|h_{n,n}s_n - y_n|^p \leq R$, se e somente se,

$$\left\lceil \frac{-R + y_n}{h_{n,n}} \right\rceil \leq s_n \leq \left\lfloor \frac{R + y_n}{h_{n,n}} \right\rfloor.$$

Para cada valor inteiro de s_n obtido no itervalo acima calculamos as possibilidades de s_{n-1}. Colocando $R_{n-1} = R^p - |h_{n,n}s_n - y_1|^p$ temos que s_{n-1} satisfaz

$$|h_{n-1,n-1}s_{n-1} + h_{n,n-1}s_n - y_{n-1}|^p \leq R_{n-1}$$

se, e somente se

$$\left\lceil \frac{-\sqrt[p]{R_{n-1}} + y_n - h_{n,n-1}s_n}{h_{n-1,n-1}} \right\rceil \leq s_{n-1} \leq \left\lfloor \frac{\sqrt[p]{R_{n-1}} + y_n - h_{n,n-1}s_n}{h_{n-1,n-1}} \right\rfloor.$$

Fixando s_n e s_{n-1} (com s_{n-1} dependendo de s_n), procedemos da mesma forma e obtemos os valores possíveis para s_{n-2} e assim por diante até obtermos s_1. Para $k < n$ colocando $R_k = R_{k+1} - |\sum_{i=1}^{k-1} h_{k+1,i}s_i - y_{k+1}|^p$ obtemos s_k no seguinte intervalo

$$\left\lceil \frac{-\sqrt[p]{R_k} + y_k - \sum_{i=1}^{k-1} h_{ki}s_i}{h_{k,k}} \right\rceil \leq s_k \leq \left\lfloor \frac{\sqrt[p]{R_k} + y_k - \sum_{i=1}^{k-1} h_{ki}s_i}{h_{k,k}} \right\rfloor .$$

Na busca dos pontos $s \in \mathbb{Z}^n$ que satisfazem a desigualdade 1.10, o algoritmo vai formando uma árvore com as relações entre as coordenadas s_i dos pontos s (Figura 1.10). A árvore começa a ser montada a partir de s_n e vai bifurcando, obtendo assim todos os caminhos. Os pontos do reticulado que estão dentro da esfera de centro y são os que são gerados pelos caminhos que vão do nível 1 até o nível n. Na árvore da figura são gerados dois pontos, que são os que vão do nível 1 até o nível 4. Estes pontos são chamados de **pontos factíveis**.

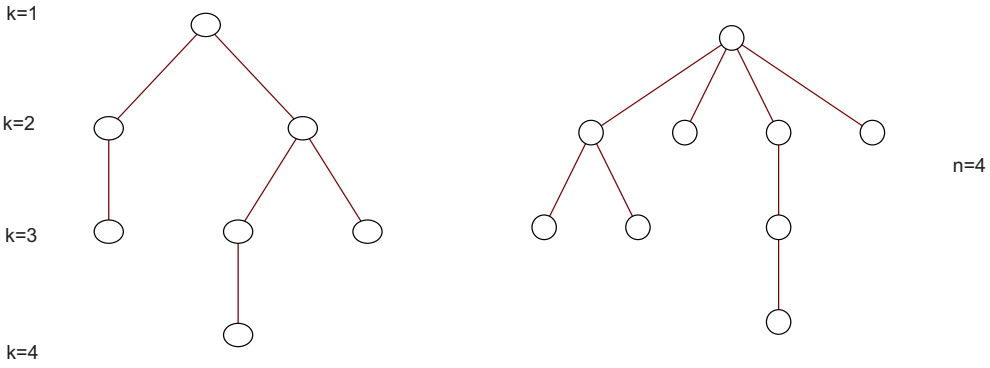


Figura 1.10: Árvore de coordenadas

Para cada ponto factível s obtemos o vetor $Hs \in \Lambda$. Devemos calcular a sua distância até y para encontrar o ponto mais próximo.

Nem todo caminho da árvore gera um ponto factível. A complexidade do algoritmo está relacionada com o número de nós visitados e com o raio R escolhido. A estimativa de Babai também pode ser usada para a escolha do raio na métrica d_p.

Observação 1.66. *[11] Para $p = 2$, d_2 é a métrica euclidiana, então os pontos do reticulado Λ que estão dentro de uma esfera euclidiana de raio R centradas em y, são obtidos como a imagem pela transformação $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ dada por $T(x) = Hx$, dos pontos $s \in \mathbb{Z}^n$ que estão dentro do elipsoide*

$$\|Hs - y\|_2^2 = |\sum_{i=1}^{n} h_{i1}s_i - y_1|^2 + \cdots + |h_{n-1,n-1}s_{n-1} + h_{n,n-1}s_n - y_{n-1}|^2 + |h_{n,n}s_n - y_1|^2 = R^2.$$

O algoritmo busca então, pelos pontos deste elipsoide.

Para $p = 1$, d_1 é a métrica da soma, então os pontos do reticulado Λ que estão dentro de uma esfera da soma de raio R centrada em y, são obtidos pela imagem da transformação T, dos pontos $s \in \mathbb{Z}^n$ que estão dentro de uma certa esfera da soma rotacionada e dilatada em algumas direções dada por

$$\|Hs - y\| = |\sum_{i=1}^{n} h_{i1}s_i - y_1| + \cdots + |h_{n-1,n-1}s_{n-1} + h_{n,n-1}s_n - y_{n-1}| + |h_{n,n}s_n - y_1| = R.$$

Exemplo 1.67. *Considere o reticulado Λ com base $\{(2,0),(1,3)\}$ e o vetor $z = (2,3)$. Na métrica euclidiana, usando a estimativa de Babai obtemos $R = \sqrt{10}$. Na Figura 1.11, à esquerda temos a esfera euclidiana de raio $\sqrt{10}$ centrada em z contendo os pontos do reticulado Λ e à direita temos a elipse $(2s_1 + s_2 - 2)^2 + (3s_2 - 3)^2 = 10$ contendo os pontos de $\mathbb{Z}^2$. Na métrica da soma, usando a estimativa de Babai, obtemos $R = 4$. Na Figura 1.12, à esquerda temos a esfera da soma de raio 4 centrada em z contendo os pontos do reticulado Λ e à direita, a bola torcida $|2s_1 + s_2 - 2| + |3s_2 - 3| = 4$ contendo os pontos de $\mathbb{Z}^2$.*

Observação 1.68. *No caso $p = 1$ não precisamos extrair raízes quadradas no decorrer do algoritmo. Além disto a bola da soma de raio R é menor que a bola euclidiana com mesmo raio e por conseguinte a primeira pode conter menos pontos do reticulado do que a segunda. Por estas razões é mais fácil decodificar usando o algoritmo na métrica da soma do que na métrica euclidiana.*

Exemplo 1.69. *Considere o reticulado Λ com base $\{(2,3),(3,2)\}$ e o vetor $z = (2,2)$. Na métrica euclidiana, usando a estimativa de Babai obtemos $R = \sqrt{8}$. Na Figura 1.13, à esquerda temos a esfera euclidiana de raio $\sqrt{8}$ centrada em z contendo os pontos do reticulado Λ e à direita temos a elipse $(2s_1 + 3s_2 - 2)^2 + (3s_1 + 2s_2 - 2)^2 = 8$ contendo os pontos de $\mathbb{Z}^2$. Na Figura 1.14, à esquerda temos a esfera da soma de raio $\sqrt{8}$ centrada em z contendo os pontos do reticulado Λ e à direita, a bola torcida $|2s_1 + 3s_2 - 2| + |3s_1 + 2s_2 - 2| = \sqrt{8}$ contendo os pontos de $\mathbb{Z}^2$.*

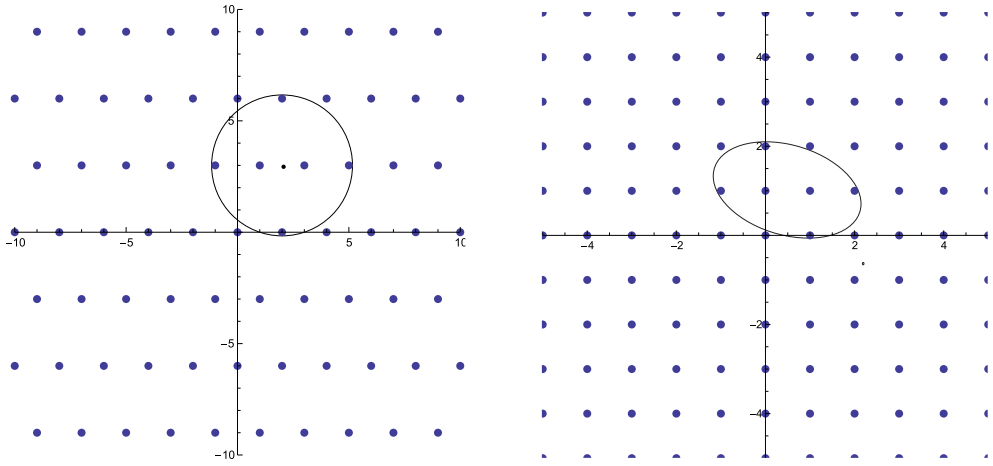


Figura 1.11: Bola contendo pontos do reticulado Λ e elipse contendo pontos de $\mathbb{Z}^2$.

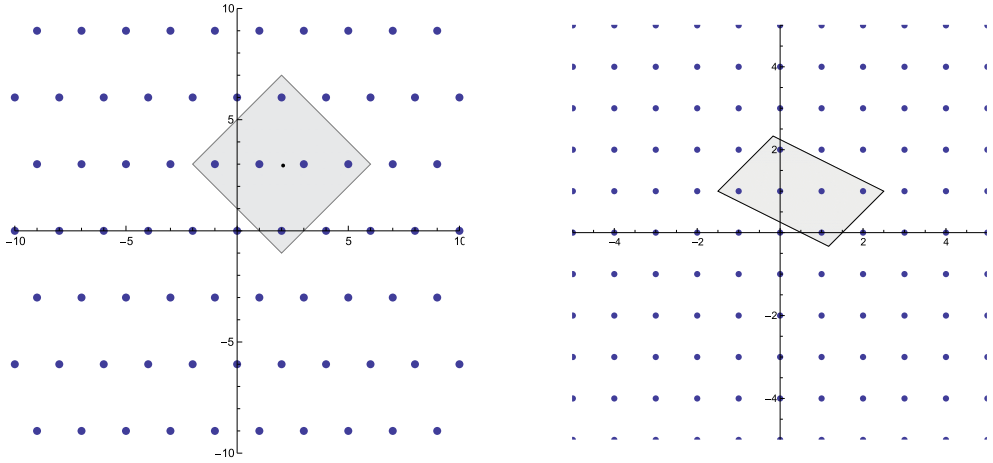


Figura 1.12: Bola da soma contendo pontos do reticulado Λ e bola torcida contendo pontos de $\mathbb{Z}^2$.

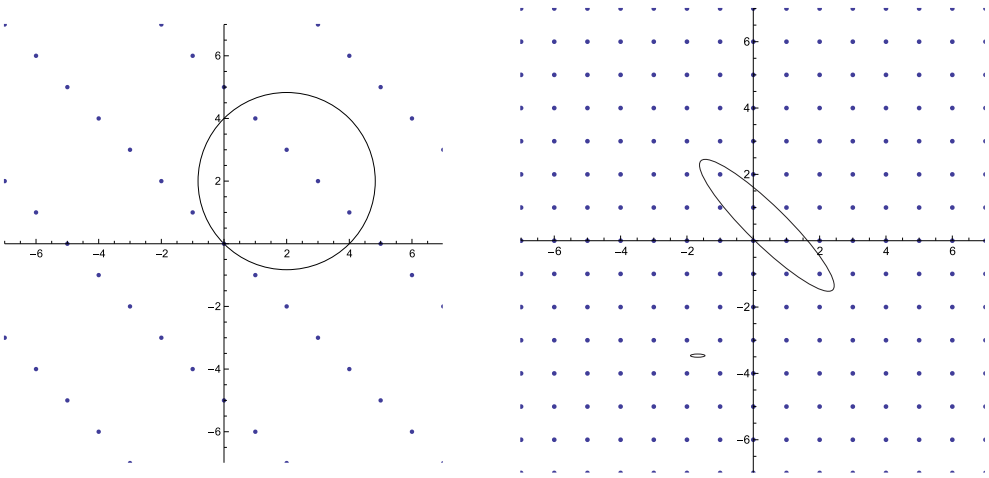


Figura 1.13: Bola contendo pontos do reticulado Λ e elipse contendo pontos de $\mathbb{Z}^2$.

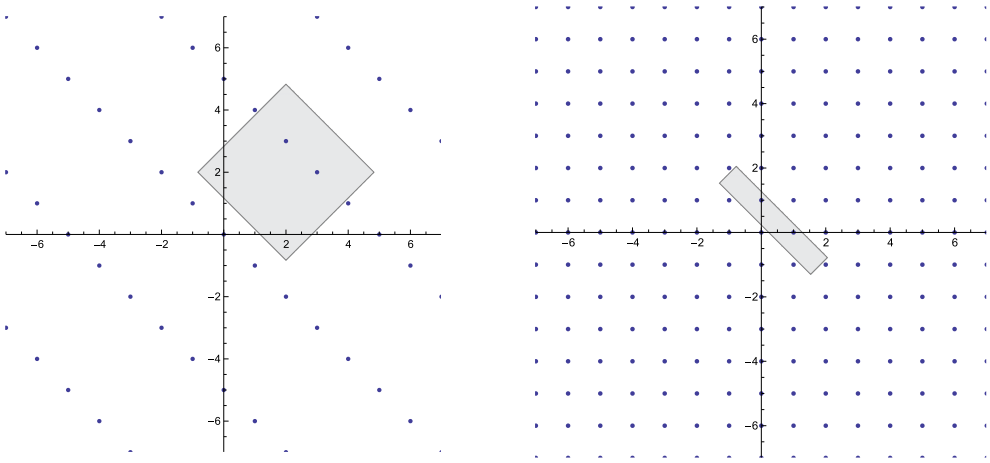
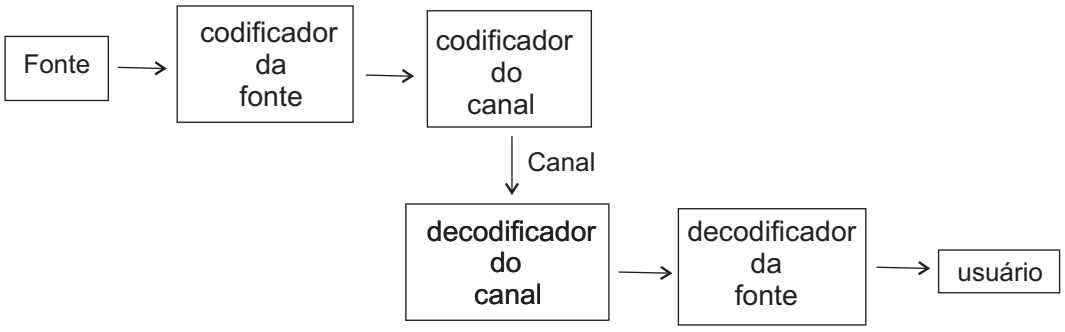


Figura 1.14: Bola da soma contendo pontos do reticulado Λ e bola torcida contendo pontos de $\mathbb{Z}^2$.

Capítulo 2

Códigos q-ários

Sistemas de comunicação são onipresentes em nossa sociedade hoje. Com o advento dos computadores e sua utilização nos mais variados setores a busca por bons sistemas onde a informação seja transmitida e processada de forma digital fez-se necessária. A Teoria da Informação é uma área que trata de aspectos quantitativos de armazenamento e transmissão de mensagens e tem como um de seus principais objetivos garantir a integridade dos dados enviados através de algum tipo de canal. Uma parte integrante desta área é a Teoria dos Códigos Corretores de Erros. Um código corretor de erros é, essencialmente, uma maneira organizada de acrescentar algum dado adicional a cada informação que precise ser transmitida ou armazenada, de modo que permita, ao recuperar a informação, detectar e corrigir os erros cometidos no processo de transmissão da informação.
Todo sistema de envio de mensagens pode ser esquematizado da forma apresentada na figura abaixo [3].



As pesquisas em Teoria da Informação tem como marco inicial o trabalho *A Mathematical Theory of Communication*, de Claude E. Shannon em 1948 [6]. Desde então diferentes subá-

reas da matemática têm sido utilizadas na resolução de problemas de Teoria de Informações e, dentre elas, a Teoria de Reticulados.

Neste capítulo apresentaremos os códigos q-ários. O motivo de os estudarmos é que estes códigos estão relacionados a uma classe especial de reticulados que abordaremos no próximo capítulo.

Começaremos com uma breve introdução aos códigos corretores de erros definidos sobre um conjunto finito A qualquer, depois passaremos ao estudo de códigos lineares definidos sobre um corpo finito K e por fim estudaremos os códigos q-ários. As principais referências são [3], [5] e [12].

2.1 Códigos Corretores de Erros

Seja A um conjunto finito com q elementos, um **código corretor de erros C**, de comprimento n é um subconjunto próprio de A^n. O conjunto A é chamado de **alfabeto** e cada elemento de C é chamado de palavra docódigo.

Se todas as palavras do código são equiprováveis, podemos decodificar um vetor recebido pelo **princípio da máxima verossimilhança**, isto é, se no receptor chega uma palavra com distorção, vamos interpretá-la como a palavra do código que está mais próxima desta e para isto utilizaremos uma função distância d definida no conjunto A^n.

Definição 2.1. *Dados dois pontos $x = (x_1, x_2, ..., x_n)$ e $y = (y_1, y_2, ..., y_n)$ de A^n, definimos a **distância de Hamming** entre x e y como*

$$d_h = |\{i : x_i \neq y_i \, 1 \leq i \leq n\}|$$

A distância de *Hamming* é uma função distância muito utilizada nos processos de decodificação. É fácil ver que ela satisfaz todas as propriedades de uma métrica e por isso ela é também chamada de métrica de *Hamming*.

Definição 2.2. *Seja $C \subset A^n$ um código e d uma métrica, a* **distância mínima** *de C na métrica d é definida por*

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

Lema 2.3. *Seja C um código, $d(C)$ sua distância mínima em uma métrica d e $k = \left\lfloor \frac{d(C)-1}{2} \right\rfloor$. Se c e c' são palavras distintas de C, então*

$$B[c,k] \cap B[c',k] = \varnothing,$$

onde $B[c,t] = \{u \in A^n : d(u,a) \leq t\}$.

Demonstração. Suponha que exista um $x \in B[c,k] \cap B[c',k]$, então temos $d(x,c) \leq k$ e $d(x,c') \leq k$. Daí

$$d(c,c') \leq d(c,x) + d(x,c') \leq 2k \leq d-1.$$

Isto contradiz o fato de d ser a distância mínima do código.

□

Proposição 2.4. *[3] Seja C um código e $d(C)$ a sua distância mínima em uma métrica d, então o código C pode corrigir até $k = \left\lfloor \frac{d(C)-1}{2} \right\rfloor$ erros e detectar até $d(C)-1$ erros.*

Demonstração. Seja c uma palavra do código transmitida com t erros, $t \leq k$, de forma que o vetor recebido tenha sido r. Então $d(r,c) \leq t \leq k$. Logo, r está na bola de centro c e raio k. Pelo Lema 2.3, r não está em nenhuma outra bola centrada em uma palavra do código, com raio k. Isto determina c univocamente a partir de r. Por outro lado, dada uma palavra do código, podemos introduzir nela até $d(C)-1$ erros sem encontrarmos outra palavra do código e, assim, a detecção do erro será possível. □

Definição 2.5. *Seja $C \in A^n$ um código com distância mínima $d(C)$ e seja $k = \left\lfloor \frac{d(C)-1}{2} \right\rfloor$. O código C será dito **perfeito** se*

$$\bigcup_{c \in C} B[c,k] = A^n$$

Observação 2.6. *Pela Proposição 2.4, um código terá maior capacidade de correção de erros quanto maior for a sua distância mínima.*

Observação 2.7. *[3] A Proposição 2.4 também permite traçarmos uma estratégia para a detecção e correção de erros. Seja C um código com a métrica d e distância mínima $d(C)$. Considere k como definido na Proposição 2.4. Quando o receptor recebe um vetor $r \in A^n$, umas das seguintes situações acontece:*

(i) O vetor r se encontra em uma bola fechada de raio k centrada em uma palavra c do código.

Neste caso, pela demonstração da Proposição 2.4, essa palavra é única e então substituímos r por c.
(ii) O vetor r não se encontra em alguma bola fechada de raio k centrada em uma palavra do código. Neste caso, não é possível decodificar r com uma boa margem de segurança.

Por (i) não podemos ter certeza absoluta de que c tenha sido a palavra transmitida, pois mais de k erros poderiam ter sido cometidos na transmissão, afastando assim r da palavra transmitida e aproximando-o de outra palavra do código. Em códigos perfeitos (ii) não ocorre.

Um código C sobre um alfabeto A possui três parâmetros fundamentais $[n, M, d(C)]$, que são respectivamente, o seu comprimento, o seu número de elementos e a sua distância mínima. Estes parâmetros são interdependentes. Interessam-nos códigos para os quais M e d são grandes relativamente a n.

Definição 2.8. *Seja A um alfabeto e d uma métrica. Diremos que uma função $\phi : A^n \longrightarrow A^n$ é uma isometria de A^n na métrica d, quando dados $x, y \in A^n$, temos*

$$d(\phi(x), \phi(y)) = d(x, y).$$

Definição 2.9. *Dados dois códigos C e C' em A^n, diremos que C' é equivalente a C na métrica d, se existir uma isometria ϕ de A^n tal que $\phi(C) = C'$.*

Observação 2.10. *[3] É fácil verificar que a relação de equivalência de códigos é, de fato, uma relação de equivalência, isto é, satisfaz as propriedades reflexiva, simétrica e transitiva.*

Decorre imediatamente da definição que dois códigos equivalentes possuem os mesmos parâmetros. Então no que diz respeito aos parâmetros tanto faz estudar um código ou um equivalente a ele.

2.1.1 Códigos lineares definidos sobre corpos

Na prática, a classe de códigos mais utilizada é a classe dos códigos lineares definidos sobre corpos.

Definição 2.11. *Se A for um corpo finito com q elementos e se C for um subespaço vetorial de dimensão s de A^n, diremos que o código C é linear definido sobre o corpo A e teremos $|C| = q^t$.*

Definição 2.12. *Seja $\beta = \{v_1, ..., v_s\}$ uma base de $C \subset K^n$, sendo K um corpo finito e considere a matriz M, cujas colunas são os vetores $v_i = (v_{i1}, ..., v_{in})$, $i = 1, ..., t$, isto é*

$$M = \begin{pmatrix} v_{11} & \cdots & v_{s1} \\ \vdots & & \vdots \\ v_{1n} & \cdots & v_{sn} \end{pmatrix}$$

A matriz M é chamada de ***matriz geradora*** *de C associada à base β.*

Considerando a transformação linear definida por

$$\begin{array}{rccc} T: & K^s & \longrightarrow & K^n \\ & x & \mapsto & Mx^t \end{array},$$

onde $x = (x_1, ..., x_s)$, temos que $T(x) = Mx^t = x_1v_1 + \cdots + x_sv_s$, logo $T(K^s) = C$. Podemos então considerar K^s o código da fonte, C o código de canal e a transformação T uma codificação.

Observação 2.13. *A matriz M não é única, pois ela depende da escolha da base β. Como uma base de um subespaço vetorial pode ser obtida de uma outra qualquer através de operações do tipo:*

- *Permutação de dois elementos da base;*
- *Multiplicação de um elemento da base por um escalar não nulo;*
- *Substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.*

decorre que duas matrizes geradoras de um código C podem ser obtidas uma da outra por uma sequencia de operações do tipo:
($C1$) *Permutação de duas colunas;*
($C2$) *Multiplicação de uma coluna por um escalar não nulo;*
($C3$) *Adição de um múltiplo escalar de uma coluna a outra.*

Definição 2.14. *Dizemos que uma matriz geradora G de um código linear C definido sobre um corpo está na forma padrão se tivermos*

$$G = \begin{pmatrix} Id_k \\ A \end{pmatrix}$$

onde Id_s é a matriz identidade de ordem s e A uma matriz $(n-s)\times s$.

Observação 2.15. *Se dois códigos lineares C e C', definidos sobre um corpo K, são equivalentes em uma métrica d, então uma isometria $T : K^n \longrightarrow K^n$ na métrica d, tal que $T(C) = C'$, deve ser linear.*

2.1.2 Códigos q-ários

Definição 2.16. *Seja $q \in \mathbb{N}$. Considere o $\mathbb{Z}_q$-módulo $\mathbb{Z}_q^n$. Um* **código linear q-ário** *C é um subgrupo aditivo próprio de $\mathbb{Z}_q^n$.*

Exemplo 2.17. *Em $\mathbb{Z}_7^2$, temos que*

$$C = \langle(\overline{3},\overline{5})\rangle = \{(\overline{0},\overline{0}),(\overline{3},\overline{5}),(\overline{6},\overline{3}),(\overline{2},\overline{1}),(\overline{5},\overline{6}),(\overline{1},\overline{4}),(\overline{4},\overline{2})\}$$

é um código linear 7-ário.

Em particular, para q primo, o anel $\mathbb{Z}_q$ é um corpo finito e assim todas as propriedades presentes em códigos lineares (sobre corpos) continuam válidas para os códigos definidos sobre este anel. Quando q não é primo, algumas das propriedades de códigos lineares definidos sobre corpos deixam de ser verdadeiras, por exemplo, a existência de uma base, uma vez que $\mathbb{Z}_q$ deixa de ser um domínio de integridade e assim já não podemos mais garantir um conjunto minimal de geradores linearmente independentes para o código.

Exemplo 2.18. *Considere o código 16-ário definido em $\mathbb{Z}_{16}^3$*

$$C = \langle(\overline{2},\overline{4},\overline{8})\rangle = \{(\overline{0},\overline{0},\overline{0}),(\overline{2},\overline{4},\overline{8}),(\overline{0},\overline{4},\overline{8}),(\overline{0},\overline{6},\overline{12}),(\overline{0},\overline{8},\overline{0}),(\overline{10},\overline{4},\overline{8}),(\overline{12},\overline{8},\overline{0}),(\overline{14},\overline{12},\overline{8})\},$$

Temos que C é gerado por $(\overline{2},\overline{4},\overline{8})$ que não é linearmente independente sobre $\mathbb{Z}_{16}^3$, pois $\overline{8}(\overline{2},\overline{4},\overline{8}) = (\overline{0},\overline{0},\overline{0})$ e para qualquer outro elemento $(\overline{a},\overline{b},\overline{c}) \in C$ temos que $\overline{8}(\overline{a},\overline{b},\overline{c}) = (\overline{0},\overline{0},\overline{0})$. Portanto, C não possui uma base.

Proposição 2.19. *[10] Seja $q \in \mathbb{N}$, $\mathbb{Z}_q$ o anel de inteiros módulo q e M um subgrupo aditivo próprio de $\mathbb{Z}_q^n$. Se M possui uma base sobre $\mathbb{Z}_q$ com k elementos, então qualquer outra base de M possui exatamente k elementos.*

A não existência de uma base para códigos definidos sobre anéis que não são corpos acarreta em algumas alterações na definição de matriz geradora para o código. A Proposição 2.19 garante que se o código possui uma base, todas as outras têm a mesma cardinalidade

e, nestes casos, a definição de matriz geradora coincide com a dada para códigos lineares definidos sobre corpos. Para os casos em que o código não possui uma base, definiremos da seguinte forma:

Definição 2.20. *Uma* **matriz geradora** *para um código q-ário C é uma matriz cujas as colunas apresentam o menor número de geradores para o código.*

Proposição 2.21. *Seja $C \subset \mathbb{Z}_q^n$, $C \neq \{0\}$, um código linear q-ário com matriz geradora M. Definamos o conjunto*

$$D_c = \{x \in \mathbb{Z}_q^n : \langle x, y\rangle = 0, \forall y \in C\},$$

onde $\langle x, y\rangle$ é o produto interno dado por $\langle v, u\rangle = x_1y_1 + \cdots + x_ny_n$, para $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n)$ em $\mathbb{Z}_q^n$. Então
(i) D_c é um subgrupo aditivo próprio de $\mathbb{Z}_q^n$, isto é, D_c é um código linear q-ário;
(ii) $x \in D_c$ se, e somente se, $xM = 0$.

Demonstração. (i) Sejam $u, v \in D_c$. Temos para todo $w \in \mathbb{C}$,

$$\langle u - v, w\rangle = \langle u, w\rangle - \langle v, w\rangle = 0$$

e, portanto, $u - v \in D_c$, provando que D_c é um subgrupo aditivo de $\mathbb{Z}_q^n$. Agora suponha que $D_c = \mathbb{Z}_q^n$, então os vetores $e_i \in \mathbb{Z}_q^n$, com $i = 1, ..., n$, cuja i-ésima coordenada é 1 e as demais são zero, pertencem a D_c. Assim se $y \in C$, sendo $y = (y_1, ..., y_n)$, então $\langle e_i, y\rangle = y_i = 0$ para todo $i = 1, ..., n$. Logo $C = \{0\}$, o que é uma contradição. Portanto, D_c é um subgrupo próprio de $\mathbb{Z}_q^n$.
(ii) $x \in D_c$ se, e somente se, x é ortogonal a todos os elementos de C se, e somente se, w é ortogonal a todos os elementos geradores de C, o que é equivalente a dizer que $xM = 0$, pois as colunas de M são os geradores de C. □

Definição 2.22. *O conjunto D_c definido na Proposição 2.21 e chamado de* **código dual** *do código C e o denotamos por $C^\perp$.*

Em particular, quando q é primo, de forma análoga mostramos que $C^\perp$ é um subespaço de $\mathbb{Z}_q^n$. De forma geral, isto vale para qualquer código linear definido sobre um corpo.

Proposição 2.23. *[3] Sejam q um número primo e $C \in \mathbb{Z}_q^n$ um código linear q-ário de dimensão k com matriz geradora*

$$G = \begin{pmatrix} Id_k \\ A \end{pmatrix}$$

na forma padrão. Então
(i) $dim C^{\perp} = n - k$,
(ii) $H = \begin{pmatrix} -A^T \\ Id_{n-k} \end{pmatrix}$ *é uma matriz geradora de* $C^{\perp}$.

Demonstração. (i) Pela Proposição 2.21, $x \in C^{\perp}$ se, e somente se, $xG = 0$. Como G está na forma padrão, isto equivale a

$$(x_1, ..., x_k) = (x_{k+1}, ..., x_n)(-A).$$

Portanto, $C^{\perp}$ possui q^{n-k} elementos, que são justamente as possíveis escolhas arbitrárias de $x_{k+1}, ..., x_n$. Logo $C^{\perp}$ tem dimensão $n - k$.
(ii) Por causa do bloco I_{n-k} na matriz H, vemos claramente que as colunas de H são linearmente independentes e, portanto, geram um subespaço de dimensão $n - k$. Como as colunas de H são ortogonais às colunas de G, o espaço gerado pelas colunas de H está contido em $C^{\perp}$ e como estes dois subespaços têm a mesma dimensão, eles coincidem, provando assim que a matriz

$$H = \begin{pmatrix} -A^T \\ Id_{n-k} \end{pmatrix}$$

é uma matriz geradora de $C^{\perp}$. □

Em geral, os códigos são estudados com a métrica de Hamming, mas podemos estudar os códigos $q-$ários, utilizando outra noção de distância definida em $\mathbb{Z}_q$ e $\mathbb{Z}_q^n$, conhecida como distância ou **métrica de Lee**. Códigos na métrica de Lee foram introduzidos em [7] e desde então vêm sendo objetos de diversos estudos teóricos e práticos.

Definição 2.24. *Dados* $\overline{x}, \overline{y} \in \mathbb{Z}_q$ *definimos a distância de Lee em* $\mathbb{Z}_q$ *como*

$$d_{Lee}(\overline{x}, \overline{y}) = min\{|x - y|, q - |x - y|\}.$$

Exemplo 2.25. *Em* $\mathbb{Z}_{11}$ *temos que* $d_{Lee}(\overline{3}, \overline{7}) = 4$ *e* $d_{Lee}(\overline{1}, \overline{9}) = 3$.

Se colocarmos as classes de $\mathbb{Z}_q$ *como os vértices de um polígono regular de* q *lados, a* ***distância de Lee*** *entre duas classes será o menor número de arestas que conectam estes vértices. A Figura 2.1 ilustra* $\mathbb{Z}_{11}$.

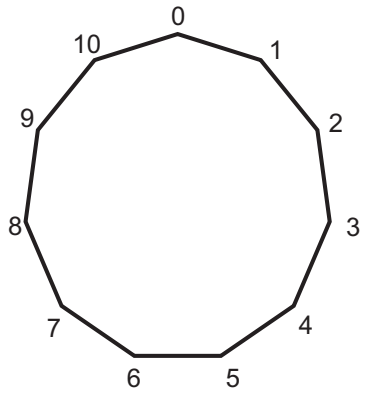


Figura 2.1: $\mathbb{Z}_{11}$

Definição 2.26. *Dados* $\overline{x}, \overline{y} \in \mathbb{Z}_q^n$, *onde* $\overline{x} = (\overline{x_1}, ...\overline{x_n})$ *e* $\overline{y} = (\overline{y_1}, ..., \overline{y_n})$, *definimos a distância de Lee em* $\mathbb{Z}_q^n$ *como*

$$d_{Lee}(\overline{x}, \overline{y}) = \sum_{i=1}^{n} min\{|x_i - y_i|, q - |x_i - y_i|\}.$$

Exemplo 2.27. *Em* $\mathbb{Z}_5^2$, *temos* $d_{Lee}((\overline{1}, \overline{2}), (\overline{4}, \overline{1})) = 3$.
Em particular, para $n = 2$, *os pontos de* $\mathbb{Z}_q^2$ *são correspondentes aos vértices de uma malha quadriculada desenhada em um quadrado de lado q. Os bordos deste quadrado devem ser identificados e, portanto, esta malha estará sobre um toro. A distância de Lee entre dois vértices é a distância do grafo, isto é, o número mínimo de arestas nesta malha para ir de um vértice a outro. A Figura 2.2 representa* $\mathbb{Z}_5^2$.

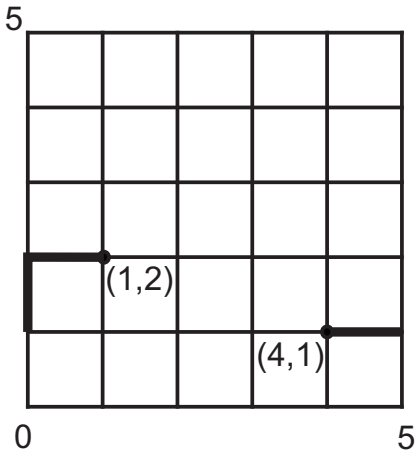


Figura 2.2: $\mathbb{Z}_5^2$

Observação 2.28. *Um fato conhecido é que dois códigos q-ários são equivalentes na métrica de Lee se um pode ser obtido do outro por uma troca de coordenadas composta por uma troca de sinais em algumas posições [23]. De modo mais geral, efetuando também sequências de operações sobre a matriz geradora M de um código q-ário C do tipo:*
$(L1)$ *permutação de duas linhas;*
$(L2)$ *multiplicação de uma linha por* -1,
obtemos uma matriz M' geradora de um código C' equivalente a C na métrica de Lee.

Proposição 2.29. *[3] Se $q \in \mathbb{Z}$ é um número primo e $C \subset \mathbb{Z}_q^n$ é um código q-ário com matriz geradora M, então existe um código equivalente C' na métrica de Lee, com matriz geradora na forma padrão.*

Demonstração. Mostraremos que por meio de uma sequência de operações do tipo $(C1), (C2)$ e $(C3)$ definidas na Observação 2.13 e $(L1)$ podemos colocar M na forma padrão.
Suponhamos que

$$M = \begin{pmatrix} v_{11} & v_{21} & \cdots & v_{k1} \\ v_{12} & v_{22} & \cdots & v_{k2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & \cdots & v_{kn} \end{pmatrix}.$$

Como a primeira coluna de M é não nula, pois os vetores colunas são linearmente independentes, por meio da operação $(L1)$ podemos supor $v_{11} \neq 0$. Agora multiplicando a primeira coluna por v_{11}^{-1}, podemos obter 1 no lugar de v_{11} (operação $(C2)$). Somando à segunda, à terceira, ... e à k-ésima colunas, respectivamente, a primeira coluna multiplicada, respectivamente, por $(-1)v_{21}, (-1)v_{31}, ..., (-1)v_{k1}$ obtemos uma matriz na forma

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{12} & b_{22} & \cdots & b_{k2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1n} & b_{2n} & \cdots & b_{kn} \end{pmatrix}.$$

Agora na segunda coluna desta matriz, temos certamente um elemento não nulo, que por meio de uma operação $(L1)$ pode ser colocado na segunda coluna e segunda linha. Multiplicando a segunda coluna pelo inverso deste elemento, a matriz se transforma em

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ c_{12} & 1 & c_{32} & \cdots & c_{k2} \\ c_{13} & c_{23} & c_{33} & \cdots & c_{k3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{1n} & c_{2n} & c_{3n} & \cdots & c_{kn} \end{pmatrix}.$$

Novamente usando a operação $(C3)$ obtemos a matriz

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ d_{13} & d_{23} & d_{33} & \cdots & d_{k3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{1n} & d_{2n} & d_{3n} & \cdots & d_{kn} \end{pmatrix},$$

e assim sucessivamente, até encontrarmos uma matriz na forma padrão

$$M' = \begin{pmatrix} Id \\ A \end{pmatrix}.$$

□

Proposição 2.30. *Considere o $\mathbb{Z}_q$-módulo $\mathbb{Z}_q^n$, se $q = 2$ ou $q = 3$, então dados $x, y \in \mathbb{Z}_q^n$ temos*

$$d_h(x, y) = d_{Lee}(x, y).$$

Demonstração. Sejam $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{Z}_q^n$. Temos $d_h(x, y) = \sum_{i=1}^{n} d_h(x_i, y_i)$. Se $q = 2$, então $x_i, y_i \in \{0, 1\} = \mathbb{Z}_2$, $i = 1, 2$. Logo, se $x_i \neq y_i$, temos

$$d_h(x_i, y_i) = 1 = d_{Lee}(x_i, y_i).$$

Assim, o i-ésimo termo tanto da distância de Hamming, quanto da distância de Lee, colaboram com uma unidade para as respectivas distâncias. Se, ao contrário, $x_i = y_i$,$i = 1, 2$ então é claro que o i-ésimo termo de ambas as distâncias não colaboram com nenhuma unidade. Portanto, temos que $d_{Lee}(x, y) = d_h(x, y)$. Se $q = 3$, então $x_i, y_i \in \{0, 1, 2\} = \mathbb{Z}_3$. Identificando os elementos de $\mathbb{Z}_3$ com os vértices de um polígono de 3 lados, assim como no Exemplo 2.1, observamos que o número mínimo de arestas conectando dois vértices distintos do polígono é 1. Assim se $x_i \neq y_i$ teremos também

$$d_h(x_i, y_i) = 1 = d_{Lee}(x_i, y_i)$$

e assim podemos chegar às mesmas conclusões que para o caso $q = 2$. □

Capítulo 3

Reticulados q-ários

Existem algumas relações entre reticulados e códigos. Neste capítulo apresentamos a chamada *Construção A*, que associa de modo natural um código q-ário a um reticulado, chamado de reticulado q-ário. Na seção 3.1 obtemos, via Construção A, algumas propriedades destes reticulados, como por exemplo, uma matriz geradora na forma Normal de Hermite para o caso em que q é um número primo. Na seção 3.2 relacionamos a distância mínima de Lee de um código q-ário com a norma mínima da soma do reticulado associado. Na seção 3.3 apresentamos dois resultados que nos fornecem uma forma de decodificar um reticulado q-ário usando a decodificação do código associado e vice-versa. Ao final deste capítulo, na seção 3.4, apresentamos o algoritmo *Lee Sphere decoding*, para decodificação de reticulados q-ários, que é uma simplificação do algoritmo apresentado na Subseção 1.9.2, para o caso em que $p = 1$. As principais referências para os tópicos aqui abordados são [16], [12] e [1].

3.1 Construção A

Nesta seção apresentaremos a Construção A e algumas propriedades de reticulados q-ários, obtidas a via Construção A.

Proposição 3.1. *[16] Considere a aplicação sobrejetora*

$$\begin{array}{rccc} \phi: & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}_q^n \\ & (x_1, ..., x_n) & \mapsto & (\overline{x}_1, ..., \overline{x}_n) \end{array}$$

Temos que $C \in \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(C)$ é um reticulado em $\mathbb{R}^n$.

Demonstração. Seja C um código linear q-ário, como $\phi^{-1}(C) \subseteq \mathbb{Z}^n$ é um conjunto discreto de $\mathbb{R}^n$, basta mostrar que ele é um grupo aditivo e assim, pelo Teorema 1.7 seguirá que $\phi^{-1}(C)$ é um reticulado. Temos $0 \in \phi^{-1}(C)$, pois $\phi(0) = \overline{0} \in C$. E se $a, b \in \phi^{-1}(C)$, então $\phi(a) = \overline{a} \in C$ e $\phi(b) = \overline{b} \in C$. Daí $\phi(a-b) = \overline{a-b} = \overline{a} - \overline{b} \in C$. Portanto, $a - b \in \phi^{-1}(C)$ provando que $\phi^{-1}(C)$ é subgrupo aditivo de $\mathbb{R}^n$.

Reciprocamente, seja $C \in \mathbb{Z}_q^n$ tal que $\phi^{-1}(C)$ é um reticulado. Temos que $\phi(\phi^{-1}(C))$ é um subgrupo de $\mathbb{Z}_q^n$, pois é a imagem de um subgrupo de $\mathbb{Z}^n$, via um homormofismo de grupos. Portanto, C é um código linear q-ário. □

Definição 3.2. *Chamamos de* **Construção A** *a aplicação ϕ que relaciona um código linear q-ário C a um reticulado $\phi^{-1}(C)$ e chamamos $\Lambda_A(C) := \phi^{-1}(C)$ de* **reticulado q-ário**.

Exemplo 3.3. *Seja C_3 o código*

$$C_3 = \{(x_1, x_2, x_3) \in \mathbb{Z}_2^3 : x_1 + x_2 + x_3 = 0\},$$

então o reticulado D_3 é igual a $\Lambda_A(C_3) = \phi^{-1}(C_3)$.
A matriz de Gram de D_3 é dada por

$$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix},$$

então precisamos encontrar uma base $\beta = \{e_1, e_2, e_3\}$ de $\Lambda_A(C_3) = \phi^{-1}(C_3)$ que satisfaça as equações

$$\langle e_1, e_3 \rangle = -1, \langle e_2, e_3 \rangle = -1, \langle e_1, e_2 \rangle = 0.$$

Seja $u = (x, y, z) \in \Lambda_A(C_3)$, como $x + y + z \equiv 0 (mod\, 2)$, segue que $x + y + z = 2m$, para algum $m \in \mathbb{Z}$, logo

$$u = (x, -x - z, z) + (0, 2m, 0) = x(1, -1, 0) + z(0, -1, 1) + 2(0, m, 0),$$

e assim, já que o conjunto de vetores $\{(1, -1, 0), (0, -1, 1), (0, 2, 0)\}$ é linearmente independente, ele é uma base de $\Lambda_A(C_3)$. Observando a matriz de Gram de D_3, vemos que precisamos tentar substituir o vetor $(0, 2, 0)$ por um vetor de norma quadrada 2. Como

$$(0, 2, 0) = (1, -1, 0) + (-1, -1, 0),$$

a norma de $(-1,-1,0)$ *é* 2 *e ele forma um conjunto linearmente independente com* $(1,-1,0)$ *e* $(0,-1,1)$*, podemos trocar* $(0,2,0)$ *por* $(-1,-1,0)$ *e obter uma nova base. Verificando os produtos internos dois a dois da nova base, vemos que basta multiplicarmos o vetor* $(0,-1,1)$ *por* -1 *e trocar a ordem dos elementos da última base para chegar a uma outra base, que é*

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

cuja a matriz de Gram coincide com a de D_3*.*

Proposição 3.4. *[12] Um reticulado* Λ *é um reticulado* q*-ário se, e somente* $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$ *para algum* $q \in \mathbb{N}$*.*

Demonstração. Seja Λ um reticulado q-ário, então $\phi^{-1}(\{\overline{0}\}) = q\mathbb{Z}^n$ e portanto assim $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$. Agora seja Λ um reticulado satisfazendo $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$, para algum $q \in \mathbb{N}$. Temos que $\Lambda/q\mathbb{Z}^n$ é um subgrupo aditivo e podemos escolher seus representantes em $[0,q)^n$, com $[0,q) \subset \mathbb{R}$, pois se $\overline{x} \in \Lambda/q\mathbb{Z}^n$, então $x = y + qk$, com $y \in [0,q)^n$ e $k \in \mathbb{Z}^n$. Daí $x - y = qk \in q\mathbb{Z}^n \subseteq \Lambda$ e segue que $y = x - qk \in \Lambda$ e $\overline{x} = \overline{y} \in \Lambda/q\mathbb{Z}^n$. Identificando os representantes de $\overline{x}$ de $\Lambda/q\mathbb{Z}^n$ com os elementos $\overline{x}$ de $\mathbb{Z}_q^n$, temos que $\Lambda/q\mathbb{Z}^n$ é um subgrupo aditivo e, portanto, um código linear q-ário C. Mostremos que $\Lambda = \phi^{-1}(C)$. Veja que se $x \in \Lambda$, então $x = y + qk$, para algum $y \in [0,q)^n$ e $k \in \mathbb{Z}^n$, daí $\phi(x) = \overline{\overline{y}} \subset \mathbb{C}$ e $x \in \phi^{-1}(\overline{\overline{y}}) \subset \phi^{-1}(C)$. Por outro lado, dado $w \in \phi^{-1}(C)$, existe um $\overline{\overline{r}}$, tal que $\phi(w) = \overline{\overline{r}}$, daí $w = r + qt$, para algum $r \in [0,q)^n$ e $t \in \mathbb{Z}^n$, assim $w - r = qt \in q\mathbb{Z}^n \in \Lambda$ e daí $\overline{w} = \overline{r} \in \Lambda/q\mathbb{Z}^n$. Portanto, $w \in \Lambda$ e concluímos o que queríamos. □

Iremos agora encontrar a dimensão de um reticulado q-ário $\Lambda_A = \phi^{-1}(C) \in \mathbb{Z}^n$.

Lema 3.5. *[12] Sejam* $v_i = (v_{i1},...,v_{in}) \subset \mathbb{Z}^n$ *para* $i = 1,...,m$*, com* $m \leq n$*. Se* $S = \{v_1,...,v_m\}$ *é um conjunto de vetores linearmente independentes sobre* $\mathbb{Z}$*, então* S *é linearmente independente sobre* $\mathbb{R}$*.*

Demonstração. Suponha que S seja um conjunto de vetores linearmente dependentes sobre $\mathbb{R}$. Sem perda de generalidade, podemos supor $v_1 = \alpha_{k_1}v_{k_1} + \cdots + \alpha_{k_s}v_{k_s}$, onde $\alpha_{k_j} \in \mathbb{R}$ e $\{v_{k_1},...,v_{k_s}\}$ é um subconjunto maximal de S de vetores linearmente independentes sobre $\mathbb{R}$, com $k_j \in \{2,...,m\}$ para $j = 1,...,s$. Assim temos o seguinte sistema linear

$$\begin{pmatrix} v_{11} \\ \vdots \\ v_{1n} \end{pmatrix} = \begin{pmatrix} v_{k_1 1} & v_{k_2 1} & \cdots & v_{k_s 1} \\ v_{k_1 2} & v_{k_2 2} & \cdots & v_{k_s 2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k_1 n} & v_{k_2 n} & \cdots & v_{k_s n} \end{pmatrix} \begin{pmatrix} \alpha_{k_1} \\ \vdots \\ \alpha_{k_s} \end{pmatrix}.$$

Como os vetores $\{v_{k_1}, ..., v_{k_s}\}$ são linearmente independentes sobre $\mathbb{R}$, a matriz $M = (v_{k_j i})$ tem posto s. Portanto, existe uma submatriz M' formada por s colunas de M com determinante não-nulo. Sem perda de generalidade podemos supor que M' seja composta pelas s primeiras colunas de M. Assim, como o determinante de M' é diferente de zero, ela é inversível, com inversa dada por $(M')^{-1} = \frac{1}{detM} B$ onde B é a matriz transposta da cofatora de M'. Portanto, as entradas de $(M')^{-1}$ são todas compostas por números racionais. Logo, $(M')^{-1}(v_{11}, ..., v_{1s})^t = (\alpha_{k_1}, ..., \alpha_{k_s})^t \in \mathbb{Q}^n$, isto é, $\alpha_{k_j} = \frac{a_{k_j}}{b_{k_j}}$, com $a_{k_j}, b_{k_j} \in \mathbb{Z}$, $j = 1, ..., s$. Tomando então $\beta = mmc(b_{k_1}, ..., b_{k_s})$, temos a seguinte combinação linear nula

$$\beta v_1 - \beta \frac{a_{k_1}}{b_{k_1}} v_{k_1} - \cdots - \beta \frac{a_{k_s}}{b_{k_s}} v_{k_s} = 0$$

com os coeficientes em $\mathbb{Z}$ e não todos nulos. Mas isto é uma contradição, pois o conjunto S é linearmente independente sobre $\mathbb{Z}$. □

Proposição 3.6. *[12] Se $C \subset \mathbb{Z}_q^n$ é um código linear q-ário, então a dimensão de $\Lambda_A(C)$ é n.*

Demonstração. Temos que $q\mathbb{Z}^n$, $\Lambda_A(C)$ e $\mathbb{Z}^n$ são $\mathbb{Z}$-módulos e $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$. Como $\mathbb{Z}$ é um domínio principal, temos $n = \text{posto}(q\mathbb{Z}^n) \leq \text{posto}(\Lambda_A(C)) \leq \text{posto}(\mathbb{Z}^n) = n$ e, portanto, a dimensão de $\Lambda_A(C)$ é n. Assim existem n vetores linearmente independentes sobre $\mathbb{Z}$ com entradas inteiras que geram $\Lambda_A(C)$. Pelo Lema 3.5, estes vetores são linearmente independentes sobre $\mathbb{R}$, formando então uma base para o reticulado $\Lambda_A(C)$. □

Observação 3.7. *Seja $C \subset \mathbb{Z}_q^n$ um código linear q-ário e $\Lambda_A(C) = \phi^{-1}(C)$ o reticulado q-ário associado. Como $\Lambda_A(C)/q\mathbb{Z}^n \simeq C$, podemos visualizar um reticulado q-ário no $\mathbb{R}^n$ como cópias dos pontos do código C presentes na hiperbloco $[0, q)^n$. Pela Observação 1.18 a cardinalidade do código C associado, isto é, a quantidade de pontos dentro de cada hipercubo é*

$$|C| = |\Lambda(C)/q\mathbb{Z}^n| = \frac{q^n}{det(\Lambda_A(C))^{1/2}}.$$

Se $B \in M_{m \times n}(\mathbb{Z}_q)$ é uma matriz geradora para o código linear q-ário C, podemos descrever o reticulado q-ário $\Lambda_A(C)$ como

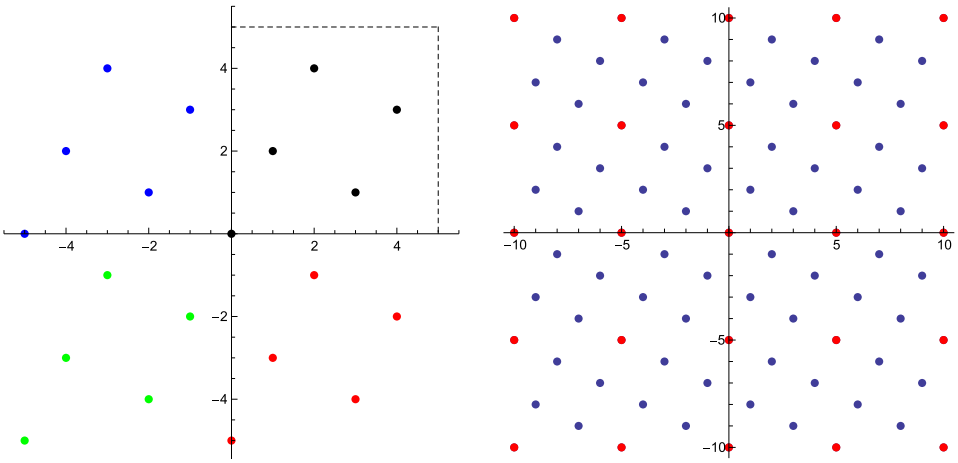


Figura 3.1: Reticulado $\Lambda_A(C)$ e sub-reticulado ortogonal $5\mathbb{Z}^2$

$$\Lambda_A(C) = \{y \in \mathbb{Z}^n : y = c + qr, c \in C, r \in \mathbb{Z}^n\} = \{y \in \mathbb{Z}^n : y = Bs + qr, s \in \mathbb{Z}^m, r \in \mathbb{Z}^n\}.$$

Como $c = (0, ..., 0)$ é uma palavra do código, vemos claramente que $\Lambda_A(C)$ possui $q\mathbb{Z}^n$ como sub-reticulado ortogonal.

Exemplo 3.8. *Considere o código 5-ário*

$$C = \langle(\overline{3}, \overline{1})\rangle = \{(\overline{0}, \overline{0}), (\overline{3}, \overline{1}), (\overline{1}, \overline{2}), (\overline{4}, \overline{3}), (\overline{2}, \overline{4})\}.$$

Sua matriz geradora é $B = (\overline{3}\ \overline{1})$. Assim o reticulado q-ário $\Lambda_A(C)$ é dado por

$$\phi^{-1}(C) = \{y \in \mathbb{Z}^2 : y = Bs + 5r, s \in \mathbb{Z}, r \in \mathbb{Z}^2\}$$

Na Figura 3.1 temos o reticulado $\Lambda_A(C)$ à esquerda. Cada cor representa uma cópia da caixa $[0, 5)^2$ e à direita temos este mesmo reticulado com os pontos em vermelho representando o sub-reticulado ortogonal $5\mathbb{Z}^2$.

Encontraremos agora uma matriz geradora para um reticulado $\Lambda_A(C)$ na forma Normal de Hermite.

Proposição 3.9. *[12] Se C é um código linear q-ário com matriz geradora*

$$M = \begin{pmatrix} \overline{v_{11}} & \overline{v_{21}} & \cdots & \overline{v_{m1}} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{v_{1n}} & \overline{v_{2n}} & \cdots & \overline{v_{mn}} \end{pmatrix},$$

então um conjunto de geradores para o reticulado $\Lambda_A(C)$ é dado pelas colunas da matriz

$$M_1 = \begin{pmatrix} v_{11} & v_{21} & \cdots & v_{m1} & q & 0 & \cdots & 0 \\ v_{12} & v_{22} & \cdots & \vdots & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & \cdots & v_{mn} & 0 & 0 & \cdots & q \end{pmatrix},$$

Demonstração. Seja $y \in \Lambda_A(C)$, então existe $\overline{c} \in C$ tal que $y = c + qz$ para algum $z \in \mathbb{Z}^n$. Como $\overline{c} \in C$, podemos escrevê-lo como combinação linear das linhas de M, isto é, existem $\overline{a_i} \in \mathbb{Z}_q$ tais que $\overline{c} = \overline{a_1 v_1} + \cdots + \overline{a_m v_m}$. Logo $\overline{c} - \overline{a_1 v_1} - \cdots - \overline{a_m v_m} = \overline{0} \in C$, e daí $c - a_1 v_1 - \cdots - a_m v_m \in \phi^{-1}(\{\overline{0}\}) = q\mathbb{Z}^n$. Assim, existe um $w \in \mathbb{Z}^n$ tal que $c - a_1 v_1 - \cdots - a_m v_m = qw$. Decorre que

$$\begin{aligned} y &= a_1 v_1 + \cdots + a_m v_m + q[(w_1, ..., w_n) + (z_1, ..., z_n)] \\ &= a_1 v_1 + \cdots + a_m v_m + (w_1 + z_1) q e_1 + \cdots + (w_n + z_n) q e_n \end{aligned}$$

e, portanto, as colunas da matriz M_1 geram $\Lambda_A(C)$. □

Depois de obter um conjunto de geradores para o reticulado q-ário podemos calcular a forma Normal de Hermite da matriz geradora associada para obter uma base para o reticulado.

Exemplo 3.10. *[12] Considere o código linear 6-ário C com a matriz geradora dada por*

$$M = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{2} & \overline{2} \\ \overline{3} & \overline{4} \\ \overline{0} & \overline{1} \\ \overline{4} & \overline{0} \end{pmatrix}$$

Pela Proposição 3.9, as colunas da matriz

$$M_1 = \begin{pmatrix} 2 & 0 & 6 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 6 & 0 & 0 & 0 \\ 3 & 4 & 0 & 0 & 6 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 6 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix}$$

geram $\Lambda_A(C)$. Calculando a forma Normal de Hermite da matriz M_1, obtemos uma matriz geradora para $\Lambda_A(C)$ dada por

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 2 & 1 & 3 & 0 & 0 \\ 2 & 1 & 0 & 3 & 0 \\ 4 & 0 & 0 & 0 & 6 \end{pmatrix}$$

Quando q é primo, pela Proposição 2.29, o código $C \in \mathbb{Z}_q^n$ com matriz geradora A é equivalente a um código q-ário C' na métrica de Lee com matriz geradora na forma padrão. Vimos que C' pode ser obtido de C por trocas de coordenadas compostas com trocas de sinais em algumas posições, assim códigos equivalentes na métrica de Lee geram reticulados equivalentes na métrica da soma via a Construção A.

Se um código q-ário C possui uma matriz na forma padrão, então o reticulado $\Lambda_A(C)$ possui uma matriz geradora na forma Normal de Hermite que apresenta as colunas da matriz geradora de C na forma padrão em suas colunas. Mais precisamente temos:

Proposição 3.11. *Se $q \subset \mathbb{N}$ é um número primo e G uma matriz geradora de um código q-ário $C \in \mathbb{Z}_q^n$ na forma padrão*

$$G = \begin{pmatrix} I_{m\times m} \\ B_{n-m\times m} \end{pmatrix},$$

então o reticulado $\Lambda_A(C)$ possui matriz geradora na forma Normal de Hermite dada por

$$\begin{pmatrix} I_{m\times m} & 0_{m\times n-m} \\ B_{n-m\times m} & qI_{n-m\times n-m} \end{pmatrix}$$

Demonstração. Pela Proposição 3.9, as colunas de G juntamente com qe_i, para $i = 1, ..., n$ geram $\Lambda_A(C)$. As colunas de G são vetores da forma $G_i = (0, ..., 0, 1, 0, ..., 0, g_{i,m+1}, ..., g_{i,n})$ para $i = 1, ..., m$, onde o 1 ocupa a i-ésima coordenada. Assim, para $j = 1, ..., m$, temos

$$\begin{aligned} qe_j &= q(0, ..., 1, ..., 0, g_{i,m+1}, ..., g_{i,n}) - g_{i,m+1}qe_{m+1} - \cdots - g_{i,n}qe_n \\ &= qG_i - (g_{i,m+1}q)e_{m+1} - \cdots - (g_{i,n}q)e_n, \end{aligned}$$

ou seja, qe_j, para $j = 1, ..., m$, pode ser escrito como uma combinação linear dos vetores $G_1, ..., G_m, qe_{m+1}, ..., qe_n$. Mostremos que estes vetores são linearmente independentes sobre $\mathbb{R}$. Considere a combinação linear nula

$$\sum_{i=1}^{m} \alpha_i G_i + \sum_{i=m+1}^{n} \alpha_i q e_i = 0,$$

com $\alpha_i \in \mathbb{R}$. É imediato ver que $\alpha_1 = \cdots = \alpha_m = 0$. Substituindo estes valores na combinação acima obtemos $\alpha_{m+1} = \cdots = \alpha_n = 0$. Portanto, $\{G_1, ..., G_m, qe_{m+1}, ..., qe_n\}$ constitui uma base de $\Lambda_A(C)$ e a matriz geradora cujas colunas são os vetores desta base é uma matriz HNF. □

Observação 3.12. *Pelo fato da forma Normal de Hermite de uma matriz ser única, quando q é primo, ao calcularmos a forma normal de Hermite de qualquer matriz geradora do reticulado $\Lambda_A(C)$ iremos obter exatamente a matriz da Proposição 3.9. Desta forma é fácil encontrar uma base para o código via uma matriz geradora para o reticulado.*

Podemos também calcular uma matriz geradora de um reticulado q-ário $\Lambda = \phi^{-1}(C)$ através da matriz geradora do código dual $C^\perp$ de C. Observando que $(C^\perp)^\perp = C$, pela Proposição 2.21, temos que $c \in C$ se, e somente se, $cA = 0$, onde A é a matriz geradora de $C^\perp$. A matriz A é chamada de matriz de controle de paridade de C.

Proposição 3.13. *[9] Sejam $C \subset \mathbb{Z}_q^n$ um código linear q-ário, $C^\perp$ seu código dual e $\Lambda_A(C^\perp) = \phi^{-1}(C^\perp)$. Então $\Lambda_A(C^\perp) = q(\Lambda_A(C))^\perp$, onde $(\Lambda_A(C))^\perp$ é o reticulado dual de $\Lambda_A(C)$.*

Demonstração. Seja $y \in \Lambda_A(C^\perp)$, então $y = c^* + qt$ com $t \in \mathbb{Z}^n$ e $\overline{c^*} \in C^\perp$. Dado $x \in \Lambda_A(C)$, podemos escrever $x = c + qk$, onde $\overline{c} \in C$ e $k \in \mathbb{Z}^n$. Assim,

$$\langle (1/q)y, x\rangle = 1/q\langle c^*, c\rangle + \langle c^*, k\rangle + \langle t, c\rangle + q\langle t, k\rangle.$$

Agora como $\overline{c^*} \in C^\perp$ e $\overline{c} \in C$, temos $\langle \overline{c^*}, \overline{c}\rangle = 0$, logo $\langle c^*, c\rangle = qs$, com $s \in \mathbb{Z}$ e, portanto, $1/q\langle c^*, c\rangle \in \mathbb{Z}$. Assim, $\langle (1/q)y, x\rangle \in \mathbb{Z}$ e daí $(1/q)y \in (\Lambda_A(C))^\perp$. Logo $y \in q(\Lambda_A(C))^\perp$.
Por outro lado, seja $z \in q(\Lambda_A(C))^\perp$, queremos mostrar que $z \in \Lambda_A(C) = \phi^{-1}(C^\perp)$.
Seja

$$\overline{A} = \begin{pmatrix} \overline{v_{11}} & \cdots & \overline{v_{k1}} \\ \vdots & \ddots & \vdots \\ \overline{v_{1n}} & \cdots & \overline{v_{kn}} \end{pmatrix},$$

uma matriz geradora para o código C com entradas em $\mathbb{Z}_q$ e considere a matriz

$$A = \begin{pmatrix} v_{11} & \cdots & v_{k1} \\ \vdots & \ddots & \vdots \\ v_{1n} & \cdots & v_{kn} \end{pmatrix},$$

com entradas em $\mathbb{Z}$. Temos

$$\begin{aligned} \phi^{-1}(C^{\perp}) &= \{y \in \mathbb{Z}^n : \phi(y)\overline{A} = \overline{0}\} \\ &= \{y = (y_1, ..., y_n) \in \mathbb{Z}^n : (\overline{y_1}, ..., \overline{y_n})\overline{A} = \overline{0}\} \\ &= \{y \in \mathbb{Z}^n : yA = qs, s \in \mathbb{Z}^n\} \end{aligned}$$

Agora, se $z \in q(\Lambda_A(C))^{\perp}$, então $z = qw$, com $w \in (\Lambda_A(C))^{\perp}$. Então, $wA \in \mathbb{Z}^n$. Assim, $qwA = qs$, com $s \in \mathbb{Z}^n$ e logo $z = qw \in \phi^{-1}(C^{\perp}) = \Lambda_A(C^{\perp})$.
Portanto, $\Lambda_A(C^{\perp}) = q(\Lambda_A(C))^{\perp}$. □

Observação 3.14. *Dada uma matriz geradora para $C^{\perp}$, isto é, uma matriz controle de paridade de C, podemos calcular uma matriz geradora M para $\Lambda_A^*(C^{\perp}) = \phi^{-1}(C^{\perp})$, então pela Proposição 3.13 a matriz $1/qM$ é uma matriz geradora para $(\Lambda_A(C))^{\perp}$ e pela Proposição 1.19, $((1/qM)^{-1})^t = q(M^{-1})^t$ é uma matriz geradora para $\Lambda_A(C)$.*

Proposição 3.15. *Sejam q um número primo e C um código linear q-ário com matriz geradora na forma padrão $G = (I_{k\times k} : B_{k\times n-k})^t$, então uma matriz geradora para $\Lambda_A(C^{\perp})$ é*

$$\begin{pmatrix} -B^t_{k\times n-k} & qI_{k\times k} \\ I_{n-k\times n-k} & 0_{n-k\times k} \end{pmatrix}$$

Demonstração. Pela Proposição 2.23, a matriz

$$H = \begin{pmatrix} -B^t_{k\times n-k} \\ I_{n-k\times n-k} \end{pmatrix}$$

é uma matriz geradora do código $C^{\perp}$. Pela Proposição 3.9 as colunas de H, juntamente com qe_i, para $i = 1, ..., n$ geram $\Lambda_A(C^{\perp})$. As colunas de H são dadas por $H_i := (-h_{i1}, ..., -h_{ik}, 0, ..., 1, ..., 0)$, para $i = 1, ..., n-k$.
Para $j = n-k+1, ..., n$ temos que

$$qe_j = q(-h_{j1}, ..., -h_{jk}, 0, ..., 1, ..., 0) + h_{j1}qe_1 + \cdots + b_{jk}qe_k.$$

Portanto, qe_j, para $j = n-k+1, ..., n$, pode ser obtido como combinação de $\{H_i,\, i = 1, ..., n-k\} \cup \{qe_i,\, i = 1, ..., k\}$. Mostremos que estes elementos são linearmente independentes. Considerando a combinação nula dada por

$$\sum_{i=1}^{k} \alpha_i q e_i + \sum_{i=1}^{n-k} \beta_i H_i = 0,$$

claramente temos $\beta_i = 0$, para $i = 1, ..., n-k$ e como qe_i, $i = 1, ..., k$ são linearmente independentes, temos que $\alpha_i = 0$, para $i = 1, ..., k$. Portanto, $\{H_i,\ i = 1, ..., n-k\} \cup \{qe_i,\ i = 1, ..., k\}$ constitui uma base para o reticulado. □

3.2 Norma mínima de Lee e norma mínima da soma

Na Seção 2.1 introduzimos a distância de Lee para códigos q-ários. Como uma alternativa à usual métrica de Hamming para códigos e à métrica euclidiana para reticulados, considerar a métrica de Lee e a métrica da soma, respectivamente, quando lidamos com códigos e reticulados q-ários parece ser mais natural. A métrica de Lee tem uma relação estreita com a métrica da soma. Note que se x e y distam menos de $\left\lfloor \frac{q-1}{2} \right\rfloor$ entre si, então $d_{Lee} = \sum_{i=1}^{n} |x_i - y_i|$, o que nos diz que localmente ela é a métrica da soma. Nesta seção estudaremos algumas relações entre a norma mínima de Lee de um código C e a norma mínima da soma do reticulado $\Lambda_A(C)$.

Definição 3.16. *Seja C um código linear q-ário. Definimos a* ***norma mínima de Lee*** *de C como o valor*

$$\mu_{Lee} = min\{d_{Lee}(\overline{x}, \overline{0}) : \overline{0} \neq \overline{x} \in C\}.$$

Encontrar os vetores de norma mínima em um reticulado com a distância da soma, assim como na métrica euclidiana é um problema de difícil solução. Igualmente encontrar a norma mínima de Lee de um código C é um problema difícil de resolver no caso geral.

Proposição 3.17. *[12] Seja $\Lambda_A(C)$ um reticulado q-ário, se μ_{Lee} é a norma mínima de Lee do código C, então*

$$\mu = min\{q, \mu_{Lee}\}$$

é a norma mínima da soma em $\Lambda_A(C)$.

Demonstração. Considere o quociente $\Lambda_A(C)/q\mathbb{Z}^n$. Escolha um conjunto de representantes para este quociente como o conjunto de pontos de $A = B_{max}[0, q/2] \cap \Lambda_A(C)$, onde $B_{max}[x, r]$ denota a bola fechada de centro x e raio r na métrica do máximo. Mostremos primeiramente que, para cada classe não nula de $\Lambda_A(C)/q\mathbb{Z}^n$, o representante com a norma mínima da soma

está em A e que, para a classe nula os representantes de menor norma da soma são do tipo $\pm qe_j$, para $j = 1, ..., n$. Seja $\overline{0} \neq \overline{c} \in A$. Os elementos da classe definida por $\overline{c}$ são da forma $x = c + qt$, para algum $t \in \mathbb{Z}^n$. Como $-q/2 \leq c_i \leq q/2$, para todo $i = 1, ..., n$ temos

$$d_{soma}(x, 0) = \sum_{i=1}^{n} |c_i + qt_i| \geq \sum_{i=1}^{n} |c_i| = d_{soma}(c, 0).$$

Agora, se $\overline{c} = \overline{0}$, temos $x = qe_1 + qt$, para $t \in \mathbb{Z}^n$, definem os pontos desta classe. Então

$$d_{soma}(x, 0) = |q + qt_1| + \sum_{i=2}^{n} |qt_i| \geq |q| = q = d_{soma}(\pm qe_j, 0), \text{ para } j = 1, ..., n.$$

Com isso temos

$$\begin{aligned} \mu &= min\{d_{soma}(x, 0) : 0 \neq x \in \Lambda_A(C)\} \\ &= min\{d_{soma}(x, 0) : 0 \neq x \in A \text{ ou } x = \pm qe_j,\ j = 1, ..., n\}. \end{aligned}$$

Relacionemos μ com a norma mínima de Lee de C e com q. Mostremos que, para cada $\overline{0} \neq \overline{c} \in C$, temos $d_{Lee}(\overline{c}, \overline{0}) = d_{soma}(c^*, 0)$, onde $c^* \in A$ e $\overline{c} = \overline{c^*}$ em $\Lambda/q\mathbb{Z}^n$. Temos $c_i^* = c_i$, se $0 \leq c_i \leq q/2$ e $c_i^* = c_i - q$, se $q/2 < c_i < q$. Assim,

- Se $min\{|c_i|, q - |c_i|\} = |c_i|$, então $0 \leq c_i \leq q/2$, o que implica $c_i^* = c_i$ e $min\{|c_i|, q - |c_i|\} = |c_i| = |c_i^*|$.
- Se $min\{|c_i|, q - |c_i|\} = q - |c_i|$, então $q/2 < c_i < q$, o que implica $c_i^* = c_i - q$ e assim, $min\{|c_i|, q - |c_i|\} = q - c_i = |c_i - q| = |c_i^*|$.

Portanto,

$$d_{Lee}(\overline{c}, \overline{0}) = \sum_{i=1}^{n} min\{|c_i|, q - |c_i|\} = \sum_{i=1}^{n} |c_i^*| = d_{soma}(c^*, 0)$$

e obtemos

$$\mu = min\{d_{Lee}(\overline{c}, \overline{0}) \text{ tal que } \overline{0} \neq \overline{c} \in C, q\} = min\{\mu_{Lee}, q\}.$$

□

Exemplo 3.18. *A Figura 3.2 mostra os dois conjuntos de representantes utilizados na demonstração da proposição acima para o quociente $\Lambda_A(C)/q\mathbb{Z}^n$, quando $q = 7$ e C é o código gerado por $(\overline{2}, \overline{1})$.*

Temos $\mu_{Lee} = 3$ e assim $\mu = min\{3, 7\} = 3$.

Exemplo 3.19. *Dado $q \in \mathbb{N}$, em $\mathbb{Z}_q^2$ a norma mínima de Lee é sempre menor ou igual a q, para qualquer código $C \subseteq \mathbb{Z}_q^2$, pois $d((\overline{a}, \overline{b}), (\overline{0}, \overline{0})) = min\{|a|, q - |a|\} + min\{|b|, q - |b|\} \leq \frac{q}{2} + \frac{q}{2} = q$, para qualquer $(\overline{a}, \overline{b}) \in C$.*

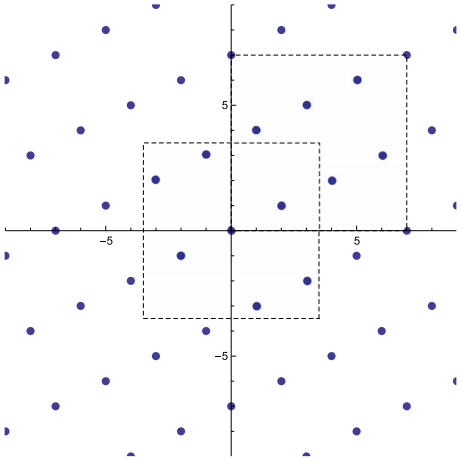


Figura 3.2: Conjunto de representantes do reticulado $\Lambda_A(C)$

Dado um código q-ário C, pelas Proposições 1.47 e 3.17 o raio de empacotamento do reticulado q-ário $\Lambda_A(C)$ na métrica da soma é dado por

$$\rho = \frac{\mu}{2} = \frac{min\{\mu_{Lee}, q\}}{2},$$

onde μ_{Lee} é a norma mínima de Lee do código C.

Observação 3.20. *Para um código q-ário C com distância de Lee mínima d_{Lee}, temos que $d_{Lee} = \mu_{Lee}$. De fato, imediatamente da definição da métrica de Lee temos $d_{Lee}(x, y) = d_{Lee}(x - y, 0)$, para quaisquer $x, y \in C$. Como $z = x - y \in C$, então*

$$min\{d_{Lee}(x, y) : x, y \in C\} = min\{d_{Lee}(z, 0) : z \in C\}.$$

O maior raio inteiro no qual as esferas com a distância da soma centradas nos pontos de $\Lambda_A(C)$ não se intercectam é $k = \left\lfloor \frac{d_{Lee} - 1}{2} \right\rfloor$. Este raio é chamado de **raio de correção de erros** [12].

Exemplo 3.21. *Considere o código 11-ário dado por $C = \langle(\overline{1}, \overline{4})\rangle$, a norma mínima de Lee de C é 4 e a distância mínima da soma de $\Lambda_A(C) = \{(1, 4), (3, 1)\}$ é $\mu = min\{4, 11\} = 4$. Assim o raio de empacotamento do reticulado $\Lambda_A(C)$ é 2 e o raio de correção é 1. A Figura 3.3 mostra à esquerda as bolas da soma de raio 2 e à direita as bolas da soma de raio 1 centradas nos pontos do reticulado $\Lambda_A(C)$*

Como uma consequência da demonstração da Proposição 3.17 temos o seguinte corolário.

Corolário 3.22. *Seja C um código linear q-ário e $\Lambda_A(C)$ o reticulado q-ário associado. Os vetores de norma mínima com a distância da soma em $\Lambda_A(C)$ são caracterizados por:*

- *Se $\mu_{Lee} > q$, a norma mínima da soma se realiza nos vetores*

$$\{\pm qe_i, i = 1, ..., n\};$$

- *Se $\mu_{Lee} < q$, a norma mínima dos vetores da soma se realiza nos vetores*

$$\{c \in B_{max}[0, q/2] \cap \Lambda \text{ tal que } \overline{c} \in C \text{ e } d_{Lee}(\overline{c}, \overline{0}) = \mu_{Lee}\};$$

- *Se $\mu_{Lee} = q$, a distância mínima da soma se realiza nos conjuntos*

$$\{\pm qe_i, i = 1, ..., n\} \text{ e } \{c \in B_{max}[0, q/2] \cap \Lambda \text{ tal que } \overline{c} \in C \text{ e } d_{Lee}(\overline{c}, \overline{0}) = \mu_{Lee}\}.$$

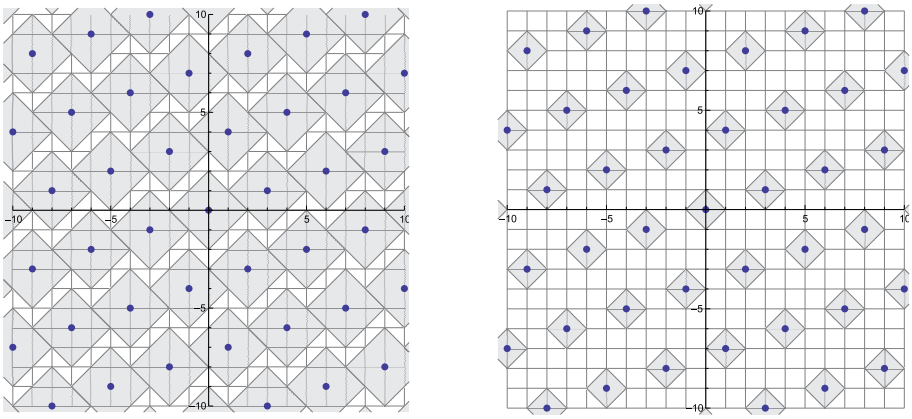


Figura 3.3: Bolas da soma de raio 2 e raio 1. (Exemplo 3.21)

3.3 Decodificação de reticulados q-ários na métrica da soma via Construção A

Um processo de decodificação para reticulados construídos a partir de códigos binários via a Construção A é apresentado em [16]. É mostrado que decodificar um código binário $C \subset \mathbb{Z}_q^n$ corresponde a decodificar o reticulado binário $\Lambda_A(C) \subset \mathbb{R}^n$ na métrica euclidiana. Em [1] é obtido uma relação semelhante para decodificação de códigos na métrica de Lee e reticulados na métrica de soma. Nesta seção apresentaremos esta relação.

A partir de agora denotaremos ambas as métricas, de Lee e da soma, por d e sempre que nos referirmos a um ponto de um código q-ário C e a um vetor do reticulado q-ário $\Lambda_A(C)$ os denotaremos por $\overline{x}$ e x respectivamente. Como $\Lambda_A(C)/q\mathbb{Z}^n$ é isomorfo a C não faremos distinção entre seus elementos. Recordemos que $[a]$ denota o inteiro mais próximo de a.

Proposição 3.23. *[12] Seja $\Lambda_A(C)$ um reticulado q-ário e $r = (r_1, ..., r_n) \in \mathbb{R}^n$ um vetor dado. Dado um elemento $\overline{x} \in \Lambda_A(C)/q\mathbb{Z}^n$, onde $x = (x_1, ..., x_n)$, o representante $\overline{z}$ da classe $\overline{x}$ que está mais próximo de r em $\Lambda_A(C)$, considerando a métrica da soma, é dado por $z = (z_1, ..., z_n)$, onde $z_i = x_i + qw_i$ e $w_i = \left[\frac{r_i - x_i}{q}\right]$, para cada $1 = 1, ..., n$.*

Demonstração. Um representante da classe de x é dado por $z = x + qw$, onde $w \in \mathbb{Z}^n$. A distância $d_{soma} = \sum_{i=1}^{n} |r_i - x_i - qw_i|$ será mínima quando tivermos $w_i = \left[\frac{r_i - x_i}{q}\right]$. □

Observação 3.24. *Se na proposição acima, ocorrer de $w_i = \left[\frac{r_i - x_i}{q}\right] = a + 1/2$, em que $a \in \mathbb{Z}$, para algum (ou alguns), $i = 1, ..., n$, então teremos dois (ou mais) pontos do reticulado, equidistantes de r, mais próximos de r. Isto significa que r está na fronteira comum das regiões de Voronoi dos dois pontos do reticulado.*

Definição 3.25. *Seja $r \in \mathbb{R}^n$. Fazendo reduções módulo q em cada uma das entradas de r obtemos um vetor cujas entradas são os restos da divisão da respectiva entrada de r por q com coeficiente inteiro. Denotando este vetor por $r(mod\, q)$, temos $r(mod\, q) = r - q\left(\left\lfloor \frac{r_1}{q} \right\rfloor, ..., \left\lfloor \frac{r_n}{q} \right\rfloor\right)$.*

Proposição 3.26. *[12] Seja $\Lambda_A(C)$ um reticulado q-ário e $r = (r_1, ..., r_n) \in \mathbb{R}^n$ um vetor dado. Se $\overline{x} \in C$ é o elemento do código C mais próximo de $r(mod\, q)$ considerando a métrica de Lee, então $z \in \Lambda_A(C)$ dado pela Proposição 3.23 tal que $\overline{z} = \overline{x}$ em $\Lambda_A(C)/q\mathbb{Z}^n$, é o elemento de $\Lambda_A(C)$, mais próximo de r.*

Demonstração. Seja $r = (r_1, ..., r_n) = (r_1^*, ..., r_n^*) + q(t_1, ..., t_n)$, com $0 \leq r_i^* \leq q$ e $t_i \in \mathbb{Z}$, para $i = 1, ..., n$. Temos $r(mod\, q) = (r_1^*, ..., r_n^*) = r^*$. Seja $\overline{x} \in C$ o vetor mais próximo de $r(mod\, q)$ considerando a métrica de Lee. Mostraremos que um ponto mais próximo de r em $\Lambda_A(C)$ está na mesma classe de x em $\Lambda_A(C)/q\mathbb{Z}^n$. Para cada $\overline{a} \in C$, $a = (a_1, ..., a_n)$, usando a Proposição 3.23, encontramos o representante a^* mais próximo de r considerando a métrica da soma, então $d(r, a^*) = d(r(mod\, q), \overline{a})$. De fato, para a distância da soma temos

$$d(r, a^*) = \sum_{i=1}^{n} |r_i^* - a_i - \alpha_i q|,$$

onde $\alpha_i = \left(\left[\frac{r_i^* - a_i}{q} + t_i\right] - t_i\right)$. Agora, $-1 \leq \frac{r_i^* - a_i}{q} \leq 1$, pois $|r_i^* - a_i| \leq q$, $\alpha_i \in \{-1, 0, 1\}$. Logo, podemos observar:

- Se $\alpha_i = 0$, para algum i, então $-q/2 \leq r_i^* - a_i \leq q/2$ e temos

$$\min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = |r_i^* - a_i|;$$

- Se $\alpha_i = 1$, para algum i, então $-q/2 \leq r_i^* - a_i \leq q$ e temos

$$\min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = q - |r_i^* - a_i| \text{ e } |r_i^* - a_i| = r_i^* - a_i;$$

- Se $\alpha_i = -1$, para algum i, então $-q \leq r_i^* - a_i \leq -q/2$ e temos

$$\min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = q - |r_i^* - a_i| \text{ e } |r_i^* - a_i| = -(r_i^* - a_i).$$

Logo, $d(r, a^*) = \sum_{i=1}^n |r_i^* - a_i - \alpha_i q| = \sum_{i=1}^n min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = d(r(mod\, q), a)$. Como z é o ponto mais próximo de r, então $\overline{z}$ minimiza $d(r(mod\, q)$, ou seja, $\overline{z} = \overline{x}$. □

A Proposição 3.26 nos fornece um processo de decodificação para reticulados q-ários com a métrica da soma via seu código gerador C. Para encontrar o ponto de $\Lambda_A(C)$ mais próximo de $r = (r_1, ..., r_n)$ na métrica da soma percorremos os seguintes passos:

- Calcular $r(mod\, q)$.
- Como $r(mod\, q) \in [0, q)^n$, calcular o ponto $\overline{x} = (\overline{x_1}, ..., \overline{x_n})$ do código C mais próximo de $r(mod\, q)$ com a métrica de Lee.
- Para $i = 1, ..., n$, calcular $w_i = \left[\frac{r_i - x_i}{q}\right]$, e obter o vetor $w = (w_1, ..., w_2)$.
- Obter $z = (x_1, ..., x_n) + q(w_1, ..., w_n)$ que é o ponto mais próximo de r com a métrica da soma.

Exemplo 3.27. *Seja C o código 7-ário dado por*

$$C = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{2}), (\overline{2}, \overline{4}), (\overline{3}, \overline{6}), (\overline{4}, \overline{1}), (\overline{5}, \overline{3}), (\overline{6}, \overline{5})\}.$$

Dado $r = (14, 27/5) \in \mathbb{R}^n$, *procuremos o ponto mais próximo de* r *em* $\Lambda_A(C)$, *com relação à distância da soma. Fazendo reduções módulo* q *nas entradas de* r, *obtemos* $r(mod\, q) = (\overline{0}, \overline{5.4})$ *O ponto do código mais próximo de* $r(mod\, q)$ *com a distância de Lee é* $\overline{x} = (\overline{6}, \overline{5})$. *Tomemos* $z = (6, 5) + 7(w_1, w_2)$, *onde* $w_1 = \left[\frac{14-6}{7}\right] = 1$ *e* $w_2 = \left[\frac{5.4-5}{7}\right] = 0$, *temos que* $z = (13, 5)$ *é o ponto de* $\Lambda_A(C)$ *mais próximo de* r *na métrica da soma. A Figura 3.4 mostra o reticulado* $\Lambda_A(C)$, *suas regiões de Voronoi e os pontos* $r, r(mod\, q), \overline{x}$ *e* z.

Podemos obter também, usando a Proposição 3.26 um algoritmo de decodificação para o código associado na métrica de Lee.

Dados $C \subset \mathbb{Z}_q^n$ um código linear q-ário e $\overline{y} \in C$, para decodificar $\overline{y}$ na métrica de Lee podemos percorrer os seguintes passos:

- Utilizar o reticulado q-ário $\Lambda_A(C)$ para decodificar y com a métrica da soma, encontrando $z \in \Lambda_A(C)$ o ponto mais próximo de y.
- Obter o elemento de $\overline{z} \in \Lambda_A(C)/q\mathbb{Z}^n$ fazendo reduções módulo q nas entradas do vetor z.
- O ponto de C mais próximo de y com a distância de Lee é o ponto $\overline{z} \in C$.

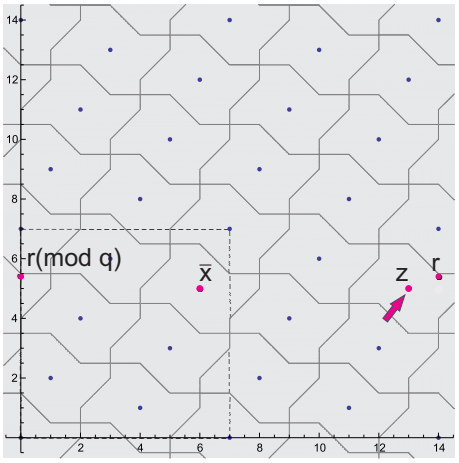


Figura 3.4: Bolas da soma de raio 2 e raio 1

A forma de abordar a decodificação de códigos dada acima é do tipo conhecida como "Soft Decoding"[16]. Nestes casos consideramos o conjunto de vetores recebidos no conjunto $S = [0, q)^n$, isto é, vetores com entradas reais reduzidas módulo q. Na literatura este tipo de

decodificação é muito pouco abordado. Em geral os algoritmos de decodificação consideram os vetores recebidos no conjunto $S = \mathbb{Z}_q^n$, ou seja, vetores com entradas inteiras reduzidas módulo q. Este tipo de decodificação é conhecido como "Hard Decoding".

3.4 Lee Sphere Decoding

No capítulo 1, estudamos um algoritmo de decodificação para reticulados na métrica d_p, $1 \leq p < \infty$. Em [1] é apresentado o algoritmo *Lee Sphere Decoding* para reticulados q-ários, que é semelhante ao algoritmo já estudado, mas com algumas simplificações devido ao formato especial que pode ser obtido da matriz geradora do reticulado. Nesta seção estudaremos tal algoritmo.

Quando q é um número primo, vimos que podemos obter uma matriz geradora para o reticulado q-ário $\Lambda_A(C)$ na Forma Normal de Hermite a partir da matriz geradora na forma padrão do código associado C. Esta matriz é dada por

$$H = \begin{pmatrix} I_{k\times k} & 0_{k\times n-k} \\ B_{n-k\times k} & qI_{n-k\times n-k} \end{pmatrix} \tag{3.1}$$

onde

$$B = \begin{pmatrix} r_{k+1,1} & \cdots & r_{k+1,k} \\ \vdots & \ddots & \vdots \\ r_{n,1} & \cdots & r_{n,k} \end{pmatrix}$$

Para simplificar as notações a partir de agora, consideraremos os vetores de $\mathbb{R}^n$ como sendo vetores colunas. Assim, cada ponto de $x \in \Lambda_A(C)$ pode ser escrito como $x = Hs$, para algum $s \in \mathbb{Z}^n$.
Colocando $s = (s^1, s^2) \in \mathbb{Z}^k \times \mathbb{Z}^{n-k}$ temos que

$$Hs = (s^1, Bs^1 + qs^2)$$

Dado $y \in \mathbb{R}^n$, para decodificar y na métrica da soma, devemos encontrar $x_1 \in \Lambda_A(C)$ tal que

$$d_{soma}(x_1, y) = min\{d_{soma}(x, y) : x \in \Lambda_A(C)\} = min\{\|Hs - y\|_1 : s \in \mathbb{Z}^n\}.$$

Observamos que, devido a forma especial de H, temos

$$\|Hs - y\|_1 = \|s^1 - y^1\|_1 + \|Bs^1 + qs^2 - y^2\|_1 \tag{3.2}$$

e abrindo a expressão acima obtemos

$$\|Hs-y\|_1 = \sum_{i=1}^{k} |s_i - y_i| + \left|\sum_{i=1}^{k} r_{k+1,i}s_i + s_{k+1}q - y_{k+1}\right| + \cdots + \left|\sum_{i=1}^{k} r_{n,i}s_i + s_n q - y_n\right|. \quad (3.3)$$

A ideia geral do algoritmo é primeiro encontrar s^1 e a partir de s^1 encontrar $s^2 = (s_{k+1}, ..., s_n)$, o que é possível devido a forma especial da matriz H. Fixado um raio R, desejamos encontrar todos os vetores inteiros que satisfazem $\|Hs - y\| \leq R$.
As k primeiras parcelas de $\|Hs-y\|$ são da forma $|s_i-y_i|$. Para estas parcelas procederemos da mesma forma que o caso estudado na Seção 1.9.2.
Para $j = 1$, temos o seguinte intervalo de variação para s_1:

$$\lceil -R + y_1 \rceil \leq s_1 \leq \lfloor R + y_1 \rfloor. \quad (3.4)$$

Para $j = 2$, fixado um valor inteiro para s_1 no intervalo dado em 3.4 e tomando $R_2 = R - |s_1 - y_1|$, temos o seguinte intervalo de variação para s_2

$$\lceil -R_2 + y_2 \rceil \leq s_2 \leq \lfloor R_2 + y_2 \rfloor.$$

Procedemos da mesma maneira até $j = k$, $k \leq n$. Para $j \leq k$, fixados valores inteiros para $s_1, ..., s_{j-1}$ dentro dos respectivos intervalos de variação, colocando $R_j = R_{j-1} - |s_{j-1} - y_{j-1}|$, obtemos o seguinte intervalo de variação para s_j

$$\lceil -R_j + y_j \rceil \leq s_j \leq \lfloor R_j + y_j \rfloor.$$

Devido a forma da matriz H, para $j > k$ já não precisamos calcular todas as possibilidades para o vetor $s^2 \in \mathbb{Z}^{n-k}$, o que simplifica o algoritmo. Fixado um vetor $s^1 = (s_1, ..., s_k)$ obtido acima, o vetor s^2 que minimiza 3.2 é o vetor inteiro mais próximo de $1/q(-s^1B + y^2)$. Como para s^1 fixo, as últimas $n - k$ parcelas de 3.3 são independentes entre si, s^2 deve ser o vetor cujas as entradas minimizam as respectivas últimas $n - k$ parcelas de 3.3. As entradas de s_2 são dadas então por

$$s_j = \left\lceil \frac{-\sum_{i=1}^{k} r_{j,i}s_i + y_k}{q} \right\rceil, \; j = k+1, ..., n.$$

Nem todo ponto $x = Hs$ gerado pelo algoritmo satisfaz $\|Hs - y\| \leq R$. Depois de gerarmos s^1, para cada nova entrada s_j de s^2 gerada, podemos testar se

$$t_j = \sum_{i=1}^{k} |s_i - y_i| + \sum_{l=k+1}^{j} \left|\sum_{i=1}^{k} r_{l,i}s_i + s_l q - y_l\right| \leq R.$$

Como este valor de s_j é o valor inteiro que minimiza a parcela, se a desigualdade não for satisfeita por este valor, não será satisfeita por nenhum outro valor e então podemos encerrar este caminho. Se a desigualdade for satisfeita continuamos o processo sempre testando se

$$t_m = t_{m-1} + \left| \sum_{i=1}^{k} r_{m,i} s_i + s_m q - y_m \right| \leq R.$$

Após gerar todos os caminhos da árvore, calculamos qual o ponto mais próximo de y entre as possibilidades encontradas. O cálculo das distâncias é feito em conjunto com a geração da árvore a fim de economizar passos.

No caso de reticulados q-ários que possuem uma matriz geradora como a dada em 3.1 é possível estimar o número de caminhos $v(k, R)$ formados até o índice k, o que não era possível no caso de um reticulado qualquer na métrica da soma. Esta estimativa é dada pela quantidade de pontos de $\mathbb{Z}^k$ contidos numa esfera da soma k-dimensional com raio R, [17], isto é,

$$v(k, R) = \sum_{i=0}^{min\{k,R\}} 2^i \binom{k}{i} \binom{R}{i}. \tag{3.5}$$

A partir do índice k o número de caminhos tendem a reduzir, o que significa que 3.5 é um limitante superior para o número de caminhos visitados pelo algoritmo, assim quando $k << n$, obtemos uma considerável redução no número de pontos visitados pelo algoritmo, uma vez que $v(k, R) << v(n, R)$. Observamos que k é justamente a dimensão do código, assim a complexidade do algoritmo também está relacionada à dimensão do código.

O exemplo seguinte ilustra alguns dos conceitos e resultados estudados.

Exemplo 3.28. *[3] Seja F um corpo finito, extensão de um corpo K. Seja $\varphi(X) \in F[X]$ e, $L = \{\alpha_0, ..., \alpha_{n-1}\} \in F$, onde os α_i são dois a dois distintos e tais que $\varphi(\alpha_i) \neq 0$ para $i = 0, ..., n-1$. Definimos o* ***código de Goppa clássico*** *sobre o corpo K associado ao conjunto L e ao polinômio φ como sendo o conjunto*

$$\Gamma_k(L, \varphi) = \left\{ (c_0, ..., c_{n-1}) \in K^n; \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \frac{\varphi(X) - \varphi(\alpha_i)}{X - \alpha_i} = 0 \right\}.$$

Considere os corpos $K = \mathbb{Z}_3$ e F construído como o anel de classes residuais $K[X]_{P(x)}$, tomando o polinômio irredutível $P(X) = X^2 + X + 2$ em $K[X]$. Seja $C = \Gamma_k(L, \varphi)$ o código de Goppa 3-ário associado a $L = F - \{0\}$ e $\varphi = X^3 + X + 1$. A matriz de paridade de C é dada por

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 & 2 & 2 \\ 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & 2 & 1 & 1 \\ 1 & 1 & 0 & 2 & 2 & 2 \\ 1 & 1 & 2 & 1 & 0 & 2 \end{pmatrix},$$

Como a matriz P tem posto 6 o código C tem dimensão 2. Temos que $c \in C$ se, e somente se, $cP = 0$. Resolvendo este sistema homogêneo obtemos

$$C = \{(2a + b, 2a, a, 2a, a + b, b, a, b)\}; a, b \in \mathbb{Z}_3\}.$$

Assim, a matriz geradora do código é dada por

$$M = \begin{pmatrix} 2 & 1 \\ 2 & 0 \\ 1 & 0 \\ 2 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Fazendo 3 operações elementares sobre as colunas da matriz M, obtemos uma matriz geradora de C na forma padrão dada por

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 2 \\ 0 & 1 \\ 1 & 1 \\ 1 & 2 \\ 0 & 2 \\ 1 & 2 \end{pmatrix}.$$

Este código tem distância de Hamming mínima igual a 4, logo ele é capaz de corrigir 1 *erro. A distância de Lee mínima também é igual a* 4*, uma vez que para* $q = 3$ *as distâncias de Lee e de Hamming são iguais.*
Podemos decodificar o vetor recebido $\overline{w} = (11202020)$*, através do reticulado* $\Lambda_A(C)$ *usando o algoritmo Lee Sphere Decoding.*

Pela Proposição 3.9, a matriz HNF do reticulado $\Lambda_A(C)$ *é dada por*

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 3 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 3 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix},$$

Pela Proposição, 3.17 a distância mínima da soma do reticulado $\Lambda_A(C)$ *é* 3 *e logo o raio de correção do reticulado é* 1*. Assim no algoritmo Lee Sphere decoding podemos usar este raio e encontrar* $s \in \mathbb{Z}^8$ *tal que*

$$\|Hs - w\|_1 \leq 1$$

Expandindo a desigualdade acima temos

$$|s_1-1|+|s_2-1|+|2s_2+3s_3-2|+|s_2+3s_4|+|s_1+s_2+3s_5-2|+|s_1+2s_2+3s_6|+|2s_2+3s_7-2|$$
$$+|s_1+2s_2+3s_8| \leq 1 \tag{3.6}$$

Pelo algoritmo, as possibilidades de s_1 *são os inteiros que estão no intervalo* $0 \leq s_1 \leq 2$*.*

- *Para* $s_1 = 0$*, a única possibilidade para* s_2 *é* 1*.*
- *Para* $s_1 = 1$*, as possibilidades para* s_2 *são os inteiros que estão no intervalo* $0 \leq s_2 \leq 2$*.*
- *Para* $s_1 = 2$*, a única possibilidade para* s_2 *é* 1*.*

Como o código tem dimensão 2, a partir do nível dois os ramos da árvore de coordenadas param de bifurcar, assim fixemos os possíveis valores para s_1 *e* s_2 *e encontremos as demais coordenadas do vetor* s*.*

- *Para* $s_1 = 0$ *e* $s_2 = 1$, *obtemos* $s_3 = 0$. *Como* $t_3 \leq 1$, *podemos continuar e obtemos* $s_4 = 0$. *Como* $t_4 = 2 > 1$ *este ramo da árvore não gera um ponto factível.*

- *Para* $s_1 = 1$ *e* $s_2 = 0$, *obtemos* $s_3 = 1$. *Como* $t_3 = 2 > 1$ *este ramo da árvore não gera um ponto factível.*

- *Para* $s_1 = 1$ *e* $s_2 = 1$, *obtemos* $s_3 = 0, s_4 = 0, s_5 = 0, s_6 = -1, s_7 = 0$ *e* $s_8 = -1$. *Todas estas coordenadas satisfazem a equação 3.6, logo obtemos um ponto factível.*

- *Para* $s_1 = 1$ *e* $s_2 = 2$, *obtemos* $s_3 = -1$. *Como* $t_3 = 2 > 1$ *este ramo da árvore não gera um ponto factível.*

- *Para* $s_1 = 2$ *e* $s_2 = 1$, *obtemos* $s_3 = 0$ *e* $t_3 < 1$. *Continuando obtemos* $s_4 = 0$ *e* $t_4 = 2 > 1$, *logo este ramo não gera um ponto factível.*

Na Figura 3.5 temos a árvore gerada no processo acima. A árvore possui 5 *ramos, o que já era esperado, pois a quantidade de pontos de* $\mathbb{Z}^2$ *contidos numa esfera da soma bidimensional com raio* 1 *é* $\upsilon(2,1) = 5$.

O único ponto factível gerado pelo algoritmo é $s = (1,1,0,0,0,-1,0,-1)$, *assim o ponto do reticulado* $\Lambda_A(C)$ *mais próximo de* w *é* $r = Hs = (1,1,2,1,2,3,2,0)$ *e o ponto do código mais próximo de* $\overline{w}$ *é* $r(mod\, q) = (1,1,2,1,2,0,2,0)$.

Também era esperado a geração de um único ponto factível, já que usamos no algoritmo o raio de correção do reticulado $\Lambda_A(C)$. *Se tivéssemos utilizado um raio maior no algoritmo, provavelmente teríamos obtido mais pontos factíveis, mas o ponto mais próximo de* w *seria gerado pelo vetor* $s = (1,1,0,0,0,-1,0,-1)$.

O código de Goppa C *possui um algoritmo próprio de decodificação que é puramente algébrico. Este algoritmo pode ser encontrado em [3] e por ele obtemos justamente o vetor* $(1,1,2,1,2,0,2,0)$. *Observamos que neste caso, para decodificar o vetor* $\overline{w}$, *o algoritmo algébrico exige uma quantidade de operações muito menor do que a decodificação pelo algoritmo Lee Sphere decoding, aproximadamente 70 operações a menos. Isso se deve a forte estrutura algébrica dos códigos de Goppa. Para códigos com menos estrutura algébrica, o processo acima fortemente baseado na estrutura geométrica dos reticulados pode ser mais vantajoso.*

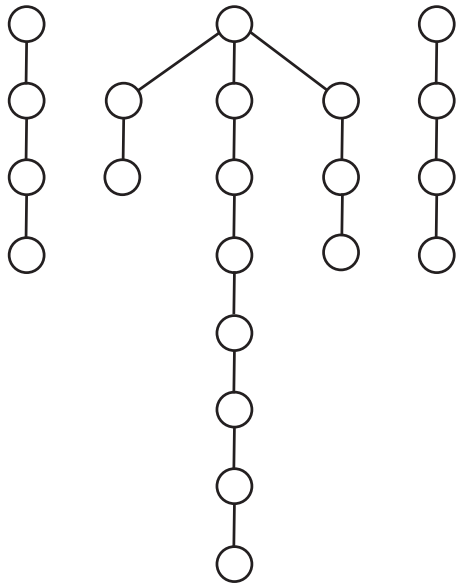


Figura 3.5: Árvore de coordenadas gerada pelo algortimo *Lee Sphere decoding* na busca pelo vetor s.

Capítulo 4

Considerações finais

Via a Construção A é possível decodificar reticulados q-ários na métrica da soma usando o processo de decodificação do código associado na métrica de Lee. Com isso, observamos que é especialmente interessante que o código associado tenha um eficiente algoritmo de decodificação na métrica de Lee. Quanto mais eficiente for este algoritmo de decodificação no código, mais eficiente será o algoritmo de decodificação obtido via a Construção A do reticulado associado na métrica da soma. Reciprocamente, se o reticulado q-ário apresentar um algoritmo eficiente de decodificação na métrica da soma, podemos obter um algoritmo eficiente para o código associado na métrica de Lee.

Reticulados q-ários têm recebido uma atenção especial nos últimos anos devido ao seu uso em sistemas criptográficos. Construções de sistemas criptográficos baseadas em reticulados compões uma das vertentes da chamada criptografia pós-quântica. Acredita-se que estes sejam seguros também, contra computadores quânticos. Por outro lado, criptossistemas baseados em códigos corretores de erros são estudados desde 1978, mas com mais ênfase nos anos recentes. Alguns dos códigos utilizados neste sistemas são os códigos de Goppa e códigos BCH [8].

As conexões entre processos de decodificação de códigos e reticulados podem fornecer ferramentas para se trabalhar simultaneamente com códigos corretores de erros e sistemas criptográficos. Vemos neste campo uma perspectiva para trabalhos futuros.

Referências Bibliográficas

[1] A.C. Campello Jr., G.C. Jorge, S.I.R. Costa, *Decoding q-ary lattices in the Lee metric*, Proceedings of 2011 IEEE Information Theory Workshop, Paraty, Brasil, 2011

[2] A.F.Beardon, *The geometry of discrete groups*, New York, Springer-Verlag, 1995.

[3] A. Hefez, M.L.T. Villela, *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, 2002.

[4] B. Hassib, H. Vikalo, *On the sphere-decoding Algorithm I. Expected Complexity*, IEEE Transactions on Information Theory, vol. 53, no.8, pp. 2806-2818. August, 2005.

[5] C.C. Lavor, M.M. Alvez, R.M. Siqueira, S.I.R. Costa, *Uma introdução à teoria de códigos*, SBMAC, 2006.

[6] C.E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, Vol. 27, pp. 379-423, 623-656, July, October, 1948.

[7] C.Y. Lee, *Some properties of nonbinary error-correcting code*, IEEE Transations on Information Theory, Vol 4. pp 72-78, 1985.

[8] D.J. Bernstein, J. Buchmann, E. Dahmen (eds), *Post Quantum Cryptograph*, Springer, 2009.

[9] D. Miciancio, O. Regev, *Lattice-based Cryptography in Pos-quantum Criptography*, Springer, 2009.

[10] F.C.P Miles, *Anéis e Corpos*, L.P.M, São Paulo, 1972.

[11] E. Viterbo, E. Bigliere, *A Universal Decoding Algorithm for Lattice Codes*, Quatorzieme Colloque Gretsi-Juan-Les-Pins, setembro, 1993.

[12] G.C. Jorge, *Reticulados q-ários e algébricos*, Tese de Doutorado, IMECC-UNICAMP, Campinas, 2012.

[13] G.H. Golub, C.F.V. Loan, *Matrix Computations*, The Johns Hopkins University Press, Baltimore London, 1996.

[14] I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, London, Chapman and Hall, 1987.

[15] J.A. Rush, N.J.A Sloane, *An improvement to Minkowisk-Hlawka bound for packing superball*, Mathematika, v.34, pp.8 18, 1987.

[16] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, New York, Springer-Verlag, 1988.

[17] J. Serra-Sagristá, J. Borrel, *Lattice points enumeration for image coding*, Proceedings of the IEEE Conference of Information Intelligence and Systems, p 482-489, 1999.

[18] H. Cohen, *A Course in Computational Algebraic Number Theory*, New York, Springer-Verlag, 1993.

[19] L.R.B. Naves, *A densidade de empacotamentos esféricos em reticulados*, Dissertação de Mestrado, IMECC-UNICAMP, Campinas, 2009.

[20] M.M.S. Alves, *Códigos geometricamente uniformes em espaços de Lee*, Dissertação de Mestrado, IMECC-UNICAMP, 1998.

[21] H.S.M. Coxeter, *Introduction to Geometry*, New York, Wiley, 1969.

[22] S.I.R. Costa, M.Muniz, E. Agustini, R.Palzzo Jr, *Graphs, Tesselations and Perfect Codes on Flat Tori*, IEEE Transactions on Information Theory, Vol. 50, pp. 2363-2377, (2004)

[23] S.I.R. Costa, J.R. Gerônimo, R. Jr. Palazzo, J.C. Interlando, M.M. Silva, *Applied algebra, algebraic algorithms and error-correcting codes*, Toulosse, 1997, 66-77, Lecture Notes in Comput. Sci., 1255, Springer, Berlim, 1997.

[24] F. Zhao, S. Qiao, *Radius Selection Algorithms for Sphere Decoding*, Canadá.