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

Grasiele Cristiane Jorge

Reticulados q-ários e algébricos

Tese de Doutorado apresentada ao Instituto de Matemática, Estatística e Computação Científica da UNICAMP para obtenção do título de Doutor em Matemática.

Orientadora: Sueli Irene Rodrigues Costa

Este exemplar corresponde à versão final da tese defendida por Grasiele Cristiane Jorge e orientada pela Profa. Dr.a Sueli Irene Rodrigues Costa.

Profa. Dra. Sueli Irene Rodrigues Costa

Campinas, 2012

[1]Este trabalho contou com apoio financeiro da Capes e do CNPq - processo n^o 140239/2009 − 0

FICHA CATALOGRÁFICA ELABORADA POR
MARIA FABIANA BEZERRA MULHER - CRB8/6162
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

Jorge, Grasiele Cristiane, 1983 -
J768r Reticulados q-ários e algébricos / Grasiele Cristiane Jorge. - Campinas, SP : [s.n.], 2012.

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

1. Geometria discreta. 2. Teoria de reticulados. 3. Teoria dos números algébricos. 4. Empacotamento de esferas. 5. Distância mínima. I. Costa, Sueli Irene Rodrigues, 1949-. II. Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: q-ary and algebraic lattices

Palavras-chave em inglês (Keywords):

1. Discrete geometry
2. Lattice theory
3. Algebraic number theory
4. Sphere packing
5. Minimum distance

Área de concentração: Matemática

Titulação: Doutor em Matemática

Banca examinadora: Profa. Dra. Sueli Irene Rodrigues Costa [Orientador]
Prof. Dr. Marcelo Firer
Prof. Dr. Reginaldo Palazzo Junior
Prof. Dr. Marcelo Muniz Silva Alves
Prof. Dr. Antonio Aparecido de Andrade

Data da defesa: 27-02-2012

Programa de Pós Graduação: Matemática

Tese de Doutorado defendida em 27 de fevereiro de 2012 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). REGINALDO PALAZZO JUNIOR

Prof(a). Dr(a). MARCELO FIRER

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES

Prof(a). Dr(a). ANTONIO APARECIDO DE ANDRADE

"O que sabemos é uma gota e
o que ignoramos é um oceano."

Isaac Newton

Aos meus pais, Claudio Donizetti Jorge (in memorian)
e Maria de Lourdes Faioto Jorge
dedico.

AGRADECIMENTOS

- Agradeço primeiramente à Deus por ter me dado saúde, força e esperança.
- À Profa. Sueli I.R. Costa pelos 4 anos de orientação e de agradável convívio, pela amizade e pela força nos momentos de insegurança.
- À banca examinadora pelos comentários e sugestões que contribuíram para melhorar a versão final.
- Aos professores do Departamento de Matemática do IMECC-Unicamp pela minha formação durante o Doutorado.
- Aos professores do IBILCE-UNESP pela formação durante a graduação e o Mestrado. Em especial ao Toninho pela orientação durante a Iniciação Científica e o Mestrado e pelo incentivo durante toda a caminhada.
- Ao Antonio e Agnaldo pelas parcerias durante o doutorado e valiosas discussões. Ao Cristiano e João também por discussões relativas a tese.
- Aos meu pais Claudio Donizetti Jorge (in memorian) e Maria de Lourdes Faioto Jorge por sempre me apoiarem em meio a tantas dificuldades. E ao meu irmão Gustavo que, junto comigo, sempre acreditou nos sonhos.
- Ao meu namorado Cleber pelo companherismo, pelo carinho e pela paciência. Agradeço também pela leitura da tese.

- Aos amigos do Doutorado: Luiz, Nelson, Ivan, Thiago, Eduardo e Alisson, obrigada por compartilharem o primeiro semestre de 2008 sempre transmitindo palavras positivas e pela amizade que só aumentou a partir de então. Aos amigos Durval, Luís e tantos outros que fiz no IMECC.

- As amizades novas que fiz durante esse período e as amizades antigas que se fortaleceram, em especial Cintya, Carina, Fernanda, Bruna, Marcinha, Ju, Ana Camila, Nati, Mari, Lu, Cecília e Rosi. Muito obrigada pelos momentos de descontração, pelas conversas e pelo companheirismo.

- Aos inúmeros amigos que fiz nestes 10 anos de estudos. Aos meus amigos de Olímpia, amigos da graduação e amigos do mestrado. A distância nunca vai apagar o carinho especial que tenho por cada um de vocês.

- A todos os integrantes do laboratório 227-228 IMECC-UNICAMP.

- À CAPES e ao CNPq pelo auxílio financeiro.

Meu muito obrigada a todos vocês. Vocês tornaram minha caminhada mais feliz.

RESUMO

O uso de códigos e reticulados em teoria da informação e na "chamada criptografia pós-quântica" vem sendo cada vez mais explorado. Neste trabalho estudamos temas relacionados a estas duas vertentes. A análise de reticulados foi feita via as métricas euclidiana e da soma. Para a métrica euclidiana, estudamos um algoritmo que procura pela treliça mínima de um reticulado com sub-reticulado ortogonal. No caso bidimensional foi possível caracterizar todos os sub-reticulados ortogonais de um reticulado racional qualquer. No estudo de reticulados via métrica da soma, trabalhamos com duas relações entre códigos e reticulados, conhecidas como "Construção A" e "Construção B". Generalizamos a Construção B para uma classe de códigos q-ários, $q \in \mathbb{N}$, e estudamos relações entre os processos de decodificação de um reticulado q-ário na métrica da soma e seu código associado na métrica de Lee via Construção A. Baseados no algoritmo "Sphere decoding" para a métrica euclidiana, construímos um algoritmo "Lee sphere decoding" para decodificação na métrica da soma. Tal algoritmo apresenta algumas simplificações para algumas classes de reticulados obtidos via as construções A e B. Por fim, utilizando técnicas algébricas para gerar reticulados no $\mathbb{R}^n$, construímos reticulados que podem ser utilizados simultaneamente nos canais de transmissão dos tipos gaussiano e de Rayleigh com desvanecimento, os quais constituem famílias de reticulados D_n-rotacionados para $n = \frac{p-1}{2}$ com p primo, $p \geq 7$ e $n = 2^{r-2}$ para $r \geq 5$. Considerando o "trade-off" entre densidade de empacotamento e distância produto mínima, os reticulados D_n-rotacionados assim construídos podem ser mais eficientes do que outras construções conhecidas de reticulados $\mathbb{Z}^n$-rotacionados.

ABSTRACT

The use of codes and lattices in Information Theory and in the so-called "Post-quantum Cryptography" has been increasingly explored. In this work we have studied topics related to these two aspects. The analysis of lattices was made via Euclidean and sum metrics. For the Euclidean metric we studied an algorithm that searches for a minimum trellis of a lattice with orthogonal sublattice. In the two-dimensional case it has been possible to characterize all orthogonal sublattices of any rational lattice. In the study of lattices via sum metric, we worked with two relations between codes and lattices, the so-called "Construction A " and "Construction B". We generalized Construction B for the class of q-ary codes, $q \in \mathbb{N}$, and studied the relationship between the decoding processes of a q-ary lattice in the sum metric and its associated code in the Lee metric via Construction A. Based on the algorithm "Sphere decoding" for the Euclidean metric we derive an algorithm, the "Lee sphere decoding", to decode in the sum metric. This algorithm has some simplifications for some classes of lattices obtained via Constructions A and B. Finally, using algebraic techniques to generate lattices in $\mathbb{R}^n$, we have constructed lattices that can be used simultaneously for the Gaussian and Rayleigh fading channels, which are families of D_n-rotated lattices for $n = \frac{p-1}{2}$, with p prime, $p \geq 7$ and $n = 2^{r-2}$ for $r \geq 5$. Considering the "trade-off" between the packing density and the minimum product distance, the D_n-rotated lattices constructed this way may be more efficient than others known constructions of $\mathbb{Z}^n$-rotated lattices.

CONTEÚDO

LISTA DE SÍMBOLOS

$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Q}$	conjunto dos números racionais
$\mathbb{C}$	conjunto dos números complexos
$\mathbb{R}$	conjunto dos números reais
$\mathbb{Z}_q$	conjunto dos números inteiros reduzidos módulo q
$\prod$	produtório
$\sum$	somatório
$\|B\|$	cardinalidade do conjunto B
$A = (a_{ij})$	matriz
$\det(A)$	determinante da matriz A
$<,>$	produto interno
$\|.\|_p$	norma p
d	métrica
Λ	reticulado
ρ	distância mínima no reticulado
$\Delta(\Lambda)$	densidade de empacotamento do reticulado Λ
$\delta(\Lambda)$	densidade de centro do reticulado Λ
$\det(\Lambda)$	determinante do reticulado Λ

$div(\Lambda)$	diversidade do reticulado Λ
$d_{p,min}$	distância produto mínima
$d_{p,rel}$	distância produto mínima relativa
d_{Lee}	métrica de Lee
d_1, d_{soma}	métrica da soma
$\mathcal{A}$	anel
$I, J, P, Q, ...$	ideais
$\mathcal{A}/I$	anel quociente
$\mathcal{A}[x]$	anel de polinômios com coeficientes em $\mathcal{A}$
$grau(f)$	grau do polinômio f
$Ker(f)$	núcleo da aplicação f
$Im(f)$	imagem da aplicação f
$f^{'}$	derivada de f
$\mathbb{K}$, $\mathbb{L}$, $\mathbb{M}$, $\mathbb{F}$, $\mathbb{E}$	corpos
$[\mathbb{L} : \mathbb{K}]$	grau da extensão $\mathbb{L}\|\mathbb{K}$
$Gal(\mathbb{L}\|\mathbb{K})$	grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$N_{\mathbb{L}\|\mathbb{K}}(\alpha)$	norma do elemento $\alpha \in \mathbb{L}$
$min_{\mathbb{K}}(\theta)$	polinômio minimal de θ sobre $\mathbb{K}$
$T_{\mathbb{L}\|\mathbb{K}}(\alpha)$	traço do elemento $\alpha \in \mathbb{L}$
$\mathcal{O}_{\mathbb{L}}$	anel de inteiros de $\mathbb{L}$ sobre $\mathcal{A}$
$d(\mathbb{L}\|\mathbb{K})$	discriminante da extensão $\mathbb{L}$ sobre $\mathbb{K}$
$N(I)$	norma do $\mathbb{Z}$-módulo I
$\varphi(n)$	função de Euler aplicada a n
$\phi_n(x)$	n-ésimo polinômio ciclotômico
$\Delta(\mathbb{L}\|\mathbb{K})^{-1}$	codiferente da extensão $\mathbb{L}$ sobre $\mathbb{K}$
$\Delta(\mathbb{L}\|\mathbb{K})$	diferente da extensão $\mathbb{L}$ sobre $\mathbb{K}$

INTRODUÇÃO

É cada vez maior a necessidade de transmitir e receber informações através de sistemas de comunicações digitais (telefones celulares, satélites, computadores, etc). Além disso, busca-se por meios seguros de guardar as informações a serem enviadas de forma que somente o receptor tenha acesso às informações corretas. A crescente demanda por sistemas mais eficientes e seguros de transmissão de dados tem estimulado a pesquisa sobre reticulados e códigos corretores de erros e inclusive o uso destes na proposição de esquemas criptográficos.

A teoria de códigos corretores de erros tem como um marco inicial o trabalho de Shannon [59] onde foi demonstrado o Teorema da Capacidade do Canal. Diferentes técnicas e abordagens, as quais objetivam otimizar a eficiência da transmissão dentro de características específicas do canal de transmissão de sinais vêm se desenvolvendo desde então.

A seguir descreveremos brevemente o modelo de um típico sistema de transmissão digital.

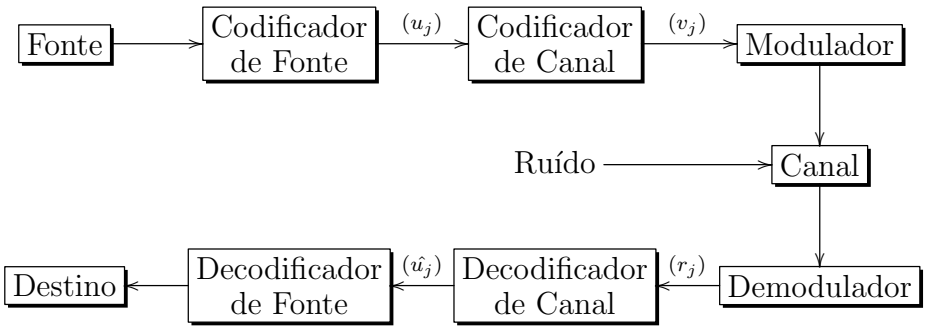


Figura 1: **Modelo do sistema**

- **Fonte** (de informação): pode ser uma pessoa ou uma máquina que gera uma onda sonora contínua ou uma sequência de símbolos discretos.

- **Codificador de fonte:** associa as saídas da fonte às sequências $(u_j) = (u_1, \cdots, u_k)$ de dígitos (geralmente binários) chamadas de sequências de informação ou palavras-código de fonte. Tendo em vista a eliminação de redundâncias, nesta etapa deve-se utilizar o menor número possível de dígitos por unidade de tempo para representar a saída da fonte. Além disso, a saída da fonte deve ser reconstruída a partir da sequência de informação associada sem ambiguidades.

- **Codificador de canal:** transforma a palavra código fonte (u_j) em uma outra sequência $(v_j) = (v_1, \cdots, v_n)$ chamada de palavra-código de canal. Este estágio tem por objetivo inserir redundância na sequência (u_j) com vistas a minimizar a interferência de ruídos no canal.

- **Modulador:** gera formas de ondas que são apropriadas para a transmissão através do canal. O modulador digital transforma símbolos discretos da saída do codificador de canal em um sinal contínuo com duração de T segundos, de tal forma que a amplitude e/ou frequência e/ou fase seja(m) alterada(s) de acordo com a necessidade.

- **Canal:** é o meio físico por onde a informação é transmitida/armazenada.

- **Demodulador, decodificador de canal e decodificador de fonte:** fazem o inverso do modulador, codificador de canal e codificador de fonte, respectivamente.

A informação a ser transmitida através de um sistema de comunicação está sujeita a um conjunto de interferências que no processo de modelagem serão alocadas ao canal de transmissão. Essa coletânea de interferências é denominada *ruído*. Devido à natureza do ruído, sua modelagem é probabilística. Dessa forma, a caracterização estatística do mesmo se realiza-se através do estabelecimento da função densidade de probabilidade.

O que se busca então, é determinar características geométricas e algébricas de tal forma que se consiga determinar o desempenho do sistema de comunicação sob a menor probabilidade de erro, maior taxa e menor potência de transmissão, etc.

Um reticulado $\Lambda = \Lambda^n \subseteq \mathbb{R}^n$ é um conjunto discreto de pontos do $\mathbb{R}^n$ gerado por combinações lineares inteiras de n vetores linearmente independentes sobre $\mathbb{R}$, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$. Um empacotamento de esferas em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio de forma que estas esferas tenham no máximo um ponto em comum. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas forma um reticulado $\Lambda \subseteq \mathbb{R}^n$. A densidade de empacotamento de um reticulado Λ, denotada por $\Delta(\Lambda)$, é a proporção do espaço coberta pelo empacotamento associado a este reticulado. Problemas associados a empacotamentos vêm tendo aplicações em diversas áreas, como por exemplo, em telecomunicações [68]. Um reticulado Λ tem diversidade $m \leq n$ se m é o número máximo tal que para todo $\boldsymbol{y} = (y_1, \cdots, y_n) \in \Lambda$ com $\boldsymbol{y} \neq \mathbf{0}$ existem no mínimo m coordenadas não nulas em $\boldsymbol{y}$. Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$ com diversidade máxima ($m = n$), a distância produto mínima de Λ é definida como $d_{min}(\Lambda) = \min\{\prod_{i=1}^{n} |y_i| \text{ para todo } \boldsymbol{y} = (y_1, \cdots, y_n) \in \Lambda, \boldsymbol{y} \neq \mathbf{0}\}$ [51]. Para estabelecer uma comparação entre reticulados de normas mínimas diferentes, a distância produto mínima relativa é definida multiplicando-se a distância produto mínima do reticulado por $\frac{1}{\lambda^n}$ onde λ é a distância mínima do reticulado.

Constelações de sinais tendo estrutura de reticulados apresentam alta eficiência espectral na transmissão [17]. O problema de encontrar boas constelações de sinais para o canal gaussiano está associado à densidade de empacotamento do reticulado na métrica euclidiana [23]: quanto maior for a densidade de empacotamento, menor é a probabilidade de erros na transmissão. Para um canal do tipo Rayleigh com desvanecimento, uma probabilidade de erro mais baixa está associada à alta diversidade e a uma distância produto mínima relativa grande [17].

Dado um reticulado qualquer, em geral é difícil calcular a densidade de empacotamento em relação à métrica euclidiana e a distância produto mínima. Para a densidade de empacotamento é necessário determinar o vetor de norma mínima, o que para reticulados gerais é um problema difícil (a conjectura é que seja NP-Hard [49]) e o mesmo ocorre para a distância produto mínima. Usando teoria algébrica dos números, podemos obter reticulados como a imagem de um homomorfismo torcido aplicado a certos $\mathbb{Z}$-módulos contidos em extensões finitas de $\mathbb{Q}$ [10]. Através de certas propriedades específicas dos corpos de números utilizados na construção de cada reticulado, podemos calcular a densidade, a diversidade e a distância produto mínima do reticulado em questão [6, 17, 51]. Tendo em vista construir reticulados

que sejam simultaneamente eficientes para ambos os canais, gaussiano e do tipo Rayleigh com desvanecimento, construímos famílias de reticulados D_n-rotacionados com diversidade máxima para $n = 2^{r-2}$ com $r \geq 5$ e $n = (p-1)/2$ com $p \geq 7$ primo [38]. Nos trabalhos [4, 13, 14] são construídos reticulados $\mathbb{Z}^n$-rotacionados com diversidade máxima para $n = 2^{r-2}$ com $r \geq 4$ e $n = (p-1)/2$ com $p \geq 5$ primo, que são bons apenas para o canal do tipo Rayleigh com desvanecimento. Considerando o "trade-off" densidade versus distância produto mínima relativa, os reticulados que construímos em [38] podem ser considerados como mais eficientes para transmissão simultânea nos dois canais quando a dimensão do reticulado aumenta.

O uso de códigos corretores de erros e reticulados em criptografia ganhou atenção especial com a possibilidade do surgimento do computador quântico. Na década de 90 ficou demonstrado que alguns dos métodos atuais de criptografia terão sua segurança ameaçada em computadores quânticos, [60]. Esquemas criptográficos baseados em códigos e reticulados vêm sendo bastante pesquisados também como alternativa para computadores clássicos, incluída na chamada "criptografia pós-quântica" [48]. Em [47], códigos de Goppa foram propostos para serem utilizados num criptossistema de chave pública (sistema Mc-Eliece) que permanece seguro até os dias atuais. A segurança dos criptossistemas que utilizam códigos corretores de erros e reticulados está baseada no fato de que até o momento não se conhecem algoritmos de decodificação para códigos lineares e reticulados arbitrários capazes de operar em tempo polinomial, mesmo em computadores quânticos [48].

Em geral, reticulados são estudados na métrica euclidiana [23] e o problema de decodificação para reticulados gerais é provado ser NP-Hard [48]. Um processo de decodificação na métrica euclidiana para ser utilizado em reticulados que possuem um sub-reticulado ortogonal é dado pelo Algoritmo de Viterbi, aplicado a uma treliça associada ao quociente do reticulado Λ por um sub-reticulado ortogonal $\Lambda^\star$ [8, 9]. A complexidade de decodificar Λ via treliças está associada à cardinalidade do grupo quociente $\Lambda/\Lambda^\star$. Tendo em vista estudar tal método de decodificação, procuramos encontrar sub-reticulados ortogonais de Λ que minimizam $|\Lambda/\Lambda^\star|$. Este algoritmo tem alta complexidade como é inerente ao problema de decodificação de reticulados.

Uma classe de reticulados muito utilizada na proposição de métodos criptográficos é a dos reticulados q-ários, que podem ser obtidos através da Construção A aplicada a um código

linear q-ário $C \subseteq \mathbb{Z}_q^n$, $q \in \mathbb{N}$ [23, 56, 18, 19].

Tendo em vista construir reticulados que possam ser utilizados na transmissão de sinais em outros tipos de canais, por exemplo, canais com distribuição de Laplace [33], e que além disso, possam ser utilizados em sistemas criptográficos, estudamos a decodificação de reticulados q-ários na métrica de soma. Devido a associação entre códigos e reticulados através da Construção A, relacionamos a decodificação de um código q-ário na métrica de Lee à decodificação do reticulado q-ário associado pela Construção A na métrica da soma (distância de Mannhatan ou l_1-métrica) [18, 19]. Se o código possuir um algoritmo eficiente de decodificação na métrica de Lee, o reticulado associado pode ser decodificado eficientemente na métrica da soma. Continuando o trabalho feito para a Construção A, estendemos a Construção B de [23] para códigos binários e ternários para uma classe de códigos q-ários.

A fim de encontrar algoritmos de decodificação eficientes para reticulados obtidos pelas Construções A e B na métrica da soma, estudamos o algoritmo clássico "Sphere decoding" [65, 66, 34] e o modificamos para esta métrica. Como as rotações em reticulados em geral não são isometrias na métrica da soma, não podemos aplicar uma fatoração QR na matriz geradora de tais reticulados. Em nosso trabalho utilizamos uma forma especial para a matriz geradora do reticulado, a qual permitiu simplificar e adaptar o algoritmo que chamamos de "Lee sphere decoding" [18].

Mais especificamente, este trabalho está organizado como se segue:

No Capítulo 1, apresentamos as definições básicas envolvendo reticulados e propriedades dos reticulados na métrica euclidiana e na métrica da soma. Apresentamos também uma modificação no algoritmo "Sphere Decoding" para a métrica d_p, $1 \leq p < \infty$.

No Capítulo 2, descrevemos uma maneira para procurar sub-reticulados ortogonais $\Lambda^\star$ de um reticulado Λ que minimizam $|\Lambda/\Lambda^\star|$. Fixado um sub-reticulado ortogonal $\Lambda^\star$, construímos o diagrama de treliças para representar o grupo quociente $\Lambda/\Lambda^\star$ a partir de um base do sub-reticulado ortogonal. Por fim, caracterizamos todos os sub-reticulados ortogonais de um reticulado bidimensional racional qualquer.

No Capítulo 3, trabalhamos com duas associações entre códigos e reticulados, a "Construção A" e a "Construção B". Estudamos propriedades de ambas contruções, generalizamos a Construção B para uma classe de códigos q-ários, $q \in \mathbb{N}$, e estudamos relações entre os processos de decodificação de um reticulado q-ário na métrica da soma e seu código associado na

métrica de Lee via Construção A. Por fim, apresentamos o algoritmo "Lee sphere decoding" com algumas simplificações para classes especiais de reticulados obtidos via Construções A e B.

No Capítulo 4, utilizando técnicas algébricas para gerar reticulados no $\mathbb{R}^n$ (o homomorfismo de Minkowski e o homomorfismo torcido) e tendo em vista construir reticulados que possam ser utilizados simultaneamente nos canais gaussiano e do tipo Rayleigh com desvanecimento, reproduzimos algumas famílias de reticulados D_n-rotacionados para $n = \frac{p-1}{2}$ com $p \geq 7$ primo e $n = 2^{r-2}$ para $r \geq 5$. Essas construções foram feitas a partir de construções de alguns reticulados $\mathbb{Z}^n$-rotacionados [4, 13, 14]. Provamos que não é possível construir os reticulados D_3 e D_5 via ideais de certos subcorpos de corpos ciclotômicos.

Descrevemos as perspectivas futuras de continuidade deste trabalho em uma última seção.

CAPÍTULO 1

RETICULADOS

Reticulados têm se mostrado bastante úteis em aplicações em telecomunicações e em criptografia "pós-quântica". Além disso, do ponto de vista teórico, eles despertam o interesse de muitos pesquisadores.

Nos estudos envolvendo reticulados, o que se busca em geral é, fixada uma dimensão, qual é o melhor reticulado nesta dimensão em relação à uma certa propriedade. Como veremos no decorrer do capítulo, um reticulado que é "bom" em algum aspecto não é necessariamente "bom" em outros aspectos. Por isso, para cada propriedade estudada, existem classes de reticulados interessantes.

Neste capítulo, vamos estudar reticulados nas métricas euclidiana e da soma. Existe uma vasta literatura sobre reticulados na métrica euclidiana, como por exemplo [23]. A pesquisa sobre reticulados na métrica da soma não é extensa, algumas referências que discutem o assunto são [29, 56, 32]. Apresentamos neste capítulo as definições básicas envolvendo reticulados e também alguns de seus parâmetros nas métricas euclidiana e da soma. A métrica da soma também é conhecida como métrica de Manhattan, métrica do taxi ou até mesmo métrica de Lee. Enfatizamos aqui o estudo dos reticulados com esta métrica, que tem sido ainda pouco explorada, observando propriedades, conexões e diferenças com a métrica euclidiana, a serem utilizadas nos resultados dos próximos capítulos. Na última seção, propomos uma modificação do algoritmo "Sphere decoding" clássico na métrica euclidiana para

a métrica d_p, $1 \leq p < \infty$.

1.1 Conceitos e resultados básicos

Intuitivamente, um reticulado em $\mathbb{R}^n$ é um conjunto infinito e discreto de pontos do $\mathbb{R}^n$ dispostos de forma regular.

Definição 1.1.1. *Seja $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$ tal que $m \leq n$. O conjunto de pontos*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i \boldsymbol{v}_i, \ \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, \cdots, m \right\}$$

é chamado de **reticulado** *e $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ é chamada uma* **base** *do reticulado.*

Definição 1.1.2. *Chamamos de* **posto** *de um reticulado Λ o número de vetores de uma base de Λ, isto é, a dimensão do subespaço gerado por Λ em $\mathbb{R}^n$.*

Exemplo 1.1.1. *Considere os vetores $\{(1,2),(1,0)\}$. A Figura 1.1 mostra alguns pontos do reticulado Λ que possui estes vetores como base.*

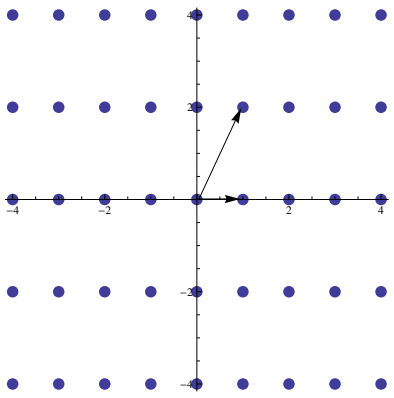


Figura 1.1: Reticulado Λ

Uma outra forma de se definir reticulado é dada pelo resultado a seguir.

Teorema 1.1.1. *[57] Se $\Lambda \subset \mathbb{R}^n$ é um subgrupo aditivo discreto, então Λ é gerado como $\mathbb{Z}$-módulo por $\boldsymbol{m}$ vetores, $\boldsymbol{m} \leq \boldsymbol{n}$, que são linearmente independentes sobre $\mathbb{R}$, isto é, Λ é um reticulado.* □

Definição 1.1.3. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ uma base para Λ tal que $\boldsymbol{v}_i = (v_{i1}, \cdots, v_{in})$ para $i = 1, \cdots, m$. Chamamos de* **matriz geradora** *para Λ a matriz $\boldsymbol{M}$ que é definida pelos vetores da base dispostos em suas linhas, isto é,*

$$\boldsymbol{M} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix},$$

e de **matriz de Gram** *a matriz $\boldsymbol{G} = \boldsymbol{M}\boldsymbol{M}^t$, cujas entradas são dadas pelo produto interno $g_{ij} = \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle$ para $1 \leq i, j \leq m$, e $\boldsymbol{M}^t$ denota a transposta de $\boldsymbol{M}$.*

Observação 1.1.1. *Um reticulado pode ser gerado por mais de uma base e consequentemente apresenta mais de uma matriz geradora e mais de uma matriz de Gram. Temos que duas matrizes geradoras $\boldsymbol{M}_1$ e $\boldsymbol{M}_2$ geram o mesmo reticulado se, e somente se, existe uma matriz unimodular $\boldsymbol{U}$ (com entradas inteiras e $det(\boldsymbol{U}) = \pm 1$) tal que $\boldsymbol{M}_2 = \boldsymbol{U}\boldsymbol{M}_1$. As respectivas matrizes de Gram estão relacionadas por*

$$\boldsymbol{G}_2 = \boldsymbol{M}_2\boldsymbol{M}_2^t = \boldsymbol{U}\boldsymbol{M}_1\boldsymbol{M}_1^t\boldsymbol{U}^t = \boldsymbol{U}\boldsymbol{G}_1\boldsymbol{U}^t.$$

Como a matriz $\boldsymbol{U}$ é unimodular, temos que o determinante de qualquer matriz de Gram de um mesmo reticulado não varia.

Definição 1.1.4. *Chamamos de* **determinante** *de um reticulado Λ e denotamos por* $\det(\Lambda)$ *o determinante de uma matriz de Gram de Λ.*

Definição 1.1.5. *Dizemos que um reticulado $\Lambda \subset \mathbb{R}^n$ é* **racional (integral)** *se uma (portanto todas) de suas matrizes de Gram possuir todas as entradas racionais (inteiras).*

Observação 1.1.2. *[8] Dado um reticulado racional Λ, sempre existe um reticulado integral $\Lambda^\star$ tal que $\Lambda^\star = k\Lambda$ para algum $k \in \mathbb{N}$.*

Definição 1.1.6. *Dizemos que um reticulado $\Lambda \subseteq \mathbb{R}^n$ é* **inteiro** *se $\Lambda \subseteq \mathbb{Z}^n$.*

Os reticulados inteiros possuem uma matriz geradora com características especiais, a matriz HNF.

Definição 1.1.7. *[27] Dizemos que uma matriz $\boldsymbol{H}$ está na forma normal de Hermite* **HNF** *se satisfaz as seguintes condições:*

- $\boldsymbol{H}$ *é triangular superior, isto é,* $h_{ij} = 0$ *para* $i > j$, $j = 1, \cdots, n-1$,
- $h_{ii} > 0$ *para* $i = 1, \cdots, n$,
- $h_{i,j} < h_{jj}$ *para* $i < j$.

Definição 1.1.8. *Dizemos que um reticulado* Λ *é* **ortogonal** *se* Λ *possui uma base* $\boldsymbol{B}$ *com os vetores de* $\boldsymbol{B}$ *dois a dois ortogonais.*

Exemplo 1.1.2. *Considere o reticulado* Λ *com base* $\{(-1,-3),(1,1)\}$ *dado pela Figura 1.2. Temos que tal base não é ortogonal, mas se tomarmos o conjunto* $\{(1,1),(1,-1)\}$ *temos uma base ortogonal para o reticulado.*

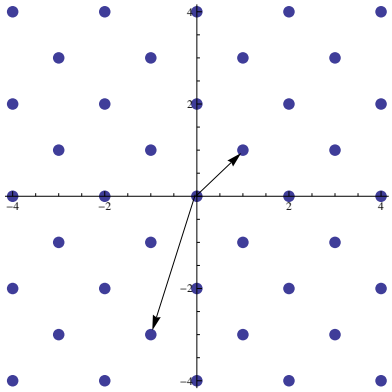


Figura 1.2: Reticulado Λ

Uma questão natural é saber quando um reticulado é ortogonal. O próximo resultado relaciona a ortogonalidade de um reticulado com a base de Minkowski. Esta é uma base especial $\{\boldsymbol{w}_1, \cdots, \boldsymbol{w}_n\}$ tal que $\boldsymbol{w}_j$ é um vetor de norma mínima do sub-reticulado gerado por $\{\boldsymbol{w}_j, \cdots, \boldsymbol{w}_n\}$ [20]. Encontrar a base de Minkowski de um reticulado é um problema difícil de ser resolvido computacionalmente para dimensões altas.

Teorema 1.1.2. *[20] Seja* Λ *um reticulado que admite uma base ortogonal ordenada* $\boldsymbol{B} = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ *na norma euclidiana, isto é,* $||\boldsymbol{b}_i||_2 \leq ||\boldsymbol{b}_{i+1}||_2$ *para* $1 \leq i \leq n-1$ *e* $\{\boldsymbol{w}_1, \cdots, \boldsymbol{w}_n\}$ *uma base de Minkowski de* Λ. *Então* $\boldsymbol{w}_i = \pm\boldsymbol{b}_i$ *para todo* $i = 1, \cdots, n$ *a menos de uma possível reordenação entre os vetores de mesma norma em* $\boldsymbol{B}$. □

Definição 1.1.9. *Dizemos que $\Lambda^\star \subset \Lambda$ é um* **sub-reticulado** *de Λ se $\Lambda^\star$ for um reticulado.*

Definição 1.1.10. *Dizemos que um $\mathbb{Z}$-módulo $\boldsymbol{M}$ é livre de posto $\boldsymbol{r}$ se existem $\boldsymbol{r}$ vetores $v_1, \cdots, v_r \in \boldsymbol{M}$ que são linearmente independentes sobre $\mathbb{Z}$ e tal que para todo $m \in \boldsymbol{M}$ tem-se $m = \sum_{i=1}^{r} a_i v_i$ com $a_i \in \mathbb{Z}$ para todo $i = 1, \cdots, r$.*

Definição 1.1.11. *Dizemos que um grupo abeliano $\boldsymbol{G}$ é livre de posto $\boldsymbol{r}$ se $\boldsymbol{G}$ é um $\mathbb{Z}$-módulo livre de posto $\boldsymbol{r}$.*

Note que um reticulado Λ é um grupo aditivo abeliano livre e um sub-reticulado $\Lambda^\star \subseteq \Lambda$ é um subgrupo de Λ. A próxima proposição apresenta uma relação para a cardinalidade do grupo quociente $\Lambda/\Lambda^\star$.

Proposição 1.1.1. *[61] Sejam $\boldsymbol{G}$ um grupo abeliano livre de posto $\boldsymbol{r}$ e $\boldsymbol{H}$ um subgrupo de $\boldsymbol{G}$. Temos que $\boldsymbol{G}/\boldsymbol{H}$ é finito se, e somente se, posto$(\boldsymbol{G})$ = posto$(\boldsymbol{H})$. Se $\{\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n\}$ é uma $\mathbb{Z}$-base para $\boldsymbol{G}$ e $\{\boldsymbol{y}_1, \cdots, \boldsymbol{y}_n\}$ é uma $\mathbb{Z}$-base para $\boldsymbol{H}$ tal que $\boldsymbol{y}_i = \sum_{j=1}^{n} a_{ij}\boldsymbol{x}_j$ com $a_{ij} \in \mathbb{Z}$ para todo $i = 1, \cdots, n$, então $|\boldsymbol{G}/\boldsymbol{H}| = |\det(a_{ij})|$.* □

Observação 1.1.3. *A Proposição 1.1.1 no caso de $\boldsymbol{G} = \Lambda$ e $\boldsymbol{H} = \Lambda^\star$, onde $\Lambda^\star \subseteq \Lambda$ são reticulados, afirma que $|\Lambda/\Lambda^\star| < \infty$ se, e somente se, posto(Λ) = posto$(\Lambda^\star)$. Além disso, se $\boldsymbol{M}$ é uma matriz geradora para Λ e $\boldsymbol{N}$ uma matriz geradora para $\Lambda^\star$, existe uma matriz com entradas inteiras $\boldsymbol{A}$ tal que $\boldsymbol{N} = \boldsymbol{A}\boldsymbol{M}$. Assim, pela mesma proposição, temos que*

$$|\Lambda/\Lambda^\star| = |\det(\boldsymbol{A})| = |\det(\boldsymbol{N})|/|\det(\boldsymbol{M})| = \det(\Lambda^\star)^{1/2}/\det(\Lambda)^{1/2}.$$

Definição 1.1.12. *A cardinalidade do grupo quociente $\Lambda/\Lambda^\star$ é chamada de* **índice** *de $\Lambda/\Lambda^\star$.*

Exemplo 1.1.3. *Considere o reticulado $\Lambda = \mathbb{Z}^3 = \{(a, b, c);\ a, b, c \in \mathbb{Z}\}$, os sub-reticulados $\Lambda^\star = \{a(1,0,0)+b(0,1,0);\ a, b \in \mathbb{Z}\}$ e $\Lambda^{\Phi} = \{a(2,0,5)+b(1,2,3)+c(0,0,1);\ (a, b, c) \in \mathbb{Z}^3\}$. Temos que posto$(\Lambda) = 3$, posto$(\Lambda^\star) = 2$ e posto$(\Lambda^{\Phi}) = 3$. Mostremos que $|\Lambda/\Lambda^\star| = \infty$. Dados $c_1, c_2 \in \mathbb{Z}$ com $c_1 \neq c_2$, temos que $(0, 0, c_1) - (0, 0, c_2) = (0, 0, c_1 - c_2) \notin \Lambda^\star$, ou seja, estes vetores pertencem a classes distintas no quociente $\Lambda/\Lambda^\star$. Portanto, existem infinitas classes em $\Lambda/\Lambda^\star$. Agora, como posto(Λ) = posto(Λ^{Φ}), temos que $|\Lambda/\Lambda^{\Phi}| = \det(\Lambda^{\Phi})^{1/2}/\det(\Lambda)^{1/2} = 4$.*

Definição 1.1.13. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto n. Dizemos que o reticulado Λ^* é o* **reticulado dual** *de Λ se*

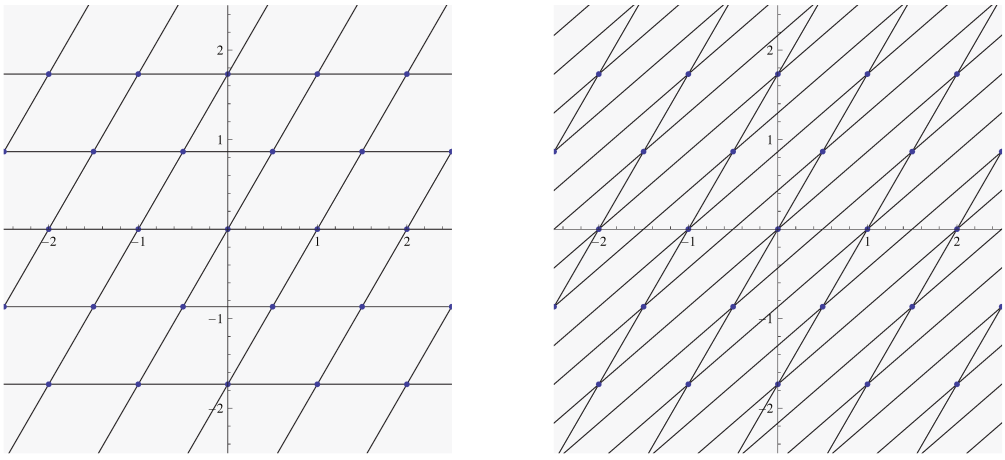
$$\Lambda^* = \{\boldsymbol{x} \in \mathbb{R}^n;\ \langle \boldsymbol{x}, \boldsymbol{z} \rangle \in \mathbb{Z},\ \forall \boldsymbol{z} \in \Lambda\}.$$

Proposição 1.1.2. *[23] Se $\boldsymbol{M}$ é uma matriz geradora para o reticulado Λ de posto n, então $(\boldsymbol{M}^{-1})^t$ é uma matriz geradora para o reticulado dual Λ^*.* □

Consideramos a seguir apenas reticulados $\Lambda \subseteq \mathbb{R}^n$ de posto n.

Definição 1.1.14. *Uma* **região fundamental** $\boldsymbol{F}$ *de um reticulado Λ é um subconjunto de $\mathbb{R}^n$ que ladrilha $\mathbb{R}^n$ por translações $\boldsymbol{v} + \boldsymbol{F}$ com $\boldsymbol{v} \in \Lambda$ tais que $\bigcup_{\boldsymbol{v} \in \Lambda} \boldsymbol{v} + \boldsymbol{F} = \mathbb{R}^n$ e dois ladrilhos ou são disjuntos ou se interceptam apenas nos bordos.*

Exemplo 1.1.4. *Considere o reticulado Λ com base $\{(1,0), (1/2, \sqrt{3}/2)\}$. Na Figura 1.3 temos dois ladrilhamentos do $\mathbb{R}^2$, obtidos por translações pelos vetores de Λ. O ladrilhamento (a) é obtido pela região fundamental $\boldsymbol{F}_1 = \{a_1(1,0) + a_2(1/2, \sqrt{3}/2),\ 0 \leq a_1, a_2 < 1\}$ e o ladrilhamento (b) é obtido pela região fundamental $\boldsymbol{F}_2 = \{a_1(2, \sqrt{3}) + a_2(-1/2, -\sqrt{3}/2),\ 0 \leq a_1, a_2 < 1\}$.*



(a) Ladrilhamento por $\boldsymbol{F}_1$ (b) Ladrilhamento por $\boldsymbol{F}_2$

Figura 1.3: Ladrilhamentos de Λ

Proposição 1.1.3. *[15] O volume de qualquer região fundamental de um reticulado $\Lambda \subseteq \mathbb{R}^n$ é o mesmo.* □

Definição 1.1.15. *Chamamos de* **volume** *de um reticulado* Λ*, denotado por* $\mathrm{vol}(\Lambda)$*, o volume de uma das regiões fundamentais de* Λ*.*

Definição 1.1.16. *Dado um reticulado* Λ *com base* $\boldsymbol{B} = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$*, chamamos de* **politopo fundamental** *a região do* $\mathbb{R}^n$ *definida por*

$$\boldsymbol{P_B} = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i;\ \ 0 \leq a_i < 1 \right\}.$$

Proposição 1.1.4. *[40] O politopo fundamental de* Λ *é uma região fundamental e seu volume é dado por* $\det(\Lambda)^{1/2}$*. Assim,* $\mathrm{vol}(\Lambda) = \det(\Lambda)^{1/2}$*.* □

Observação 1.1.4. *Seja* $\Lambda^\star$ *um sub-reticulado de um reticulado* Λ*. Na intersecção de cada politopo fundamental de* $\Lambda^\star$ *com* Λ *está um conjunto de representantes para o grupo quociente* $\Lambda/\Lambda^\star$*. De fato, seja* $\{\boldsymbol{b}_1^*, \cdots, \boldsymbol{b}_n^*\}$ *uma base para* $\Lambda^\star$*. O politopo fundamental de* $\Lambda^\star$ *dado por esta base é* $\boldsymbol{F} = \{\sum_{i=1}^n a_i \boldsymbol{b}_i^*;\ \ 0 \leq a_i < 1\}$*. Se* $\boldsymbol{a}, \boldsymbol{b} \in \Lambda \cap \boldsymbol{F}$ *com* $\boldsymbol{a} \neq \boldsymbol{b}$*, então* $\boldsymbol{a} = \sum_{i=1}^n \alpha_i \boldsymbol{b}_i^*$*,* $\boldsymbol{b} = \sum_{i=1}^n \beta_i \boldsymbol{b}_i^*$*,* $0 \leq \alpha_i, \beta_i < 1$*. Então,* $\boldsymbol{a} - \boldsymbol{b} = \sum_{i=1}^n (\alpha_i - \beta_i)\boldsymbol{b}_i^* \notin \Lambda^\star$*, pois* $0 \leq \alpha_i - \beta_i < 1$ *e pelo menos um destes coeficientes é não nulo pois* $\boldsymbol{a} \neq \boldsymbol{b}$*. Portanto,* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *estão em classes distintas no grupo quociente* $\Lambda/\Lambda^\star$*. Assim, já que todos os elementos de* $\Lambda \cap \boldsymbol{F}$ *estão em classes distintas em* $\Lambda/\Lambda^\star$*. Agora, dado* $\boldsymbol{x} \in \Lambda$*, temos que existem* $\boldsymbol{f} \in \boldsymbol{F}$ *e* $\boldsymbol{w} \in \Lambda^\star$ *tais que* $\boldsymbol{x} = \boldsymbol{f} + \boldsymbol{w}$*, pois* $\boldsymbol{F}$ *é uma região fundamental de* $\Lambda^\star$*. Agora, note que* $\boldsymbol{f} = \boldsymbol{x} - \boldsymbol{w} \in \Lambda \cap \boldsymbol{F}$ *e que* $\boldsymbol{x} - \boldsymbol{f} = \boldsymbol{w} \in \Lambda^\star$*. Portanto,* $\overline{\boldsymbol{x}} = \overline{\boldsymbol{f}}$*. Logo, um conjunto de representantes para* $\Lambda/\Lambda^\star$ *está em* $\Lambda \cap \boldsymbol{F}$*.*

Exemplo 1.1.5. *Considere o reticulado hexagonal* Λ *com base* $\{(1,0), (1/2, \sqrt{3}/2)\}$ *e o sub-reticulado* $\Lambda^\star$ *com base* $\{(1,0), (0, 2\sqrt{3})\}$*. Temos que* $|\Lambda/\Lambda^\star| = 4$*. Na Figura 1.4 podemos ver que existem 4 pontos de* Λ *na região fundamental* $\boldsymbol{F} = \{a(1,0) + b(0, 2\sqrt{3});\ \ 0 \leq a, b < 1\}$ *de* $\Lambda^\star$*.*

1.2 Reticulados equivalentes

Nesta seção, vamos estudar reticulados equivalentes nas métricas euclidiana e da soma.

Definição 1.2.1. *Fixada uma métrica* d *em* $\mathbb{R}^n$*, uma isometria* $\sigma_d : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ *é uma aplicação que satisfaz* $d(\boldsymbol{x}, \boldsymbol{y}) = d(\sigma_d(\boldsymbol{x}), \sigma_d(\boldsymbol{y}))$ *para todo* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$*.*

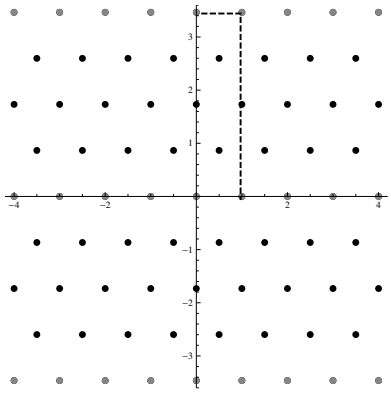


Figura 1.4: Reticulado Λ e sub-reticulado Λ^*

Definição 1.2.2. *Fixada uma métrica d em $\mathbb{R}^n$, dizemos que dois reticulados Λ_1 e Λ_2 são* **d-equivalentes** *se existirem uma isometria $\sigma_d : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ e um número real positivo λ tais que $(\lambda\sigma_d)(\Lambda_1) = \Lambda_2$. Chamamos λ de* **fator de dilatação**. *Quando $\lambda = 1$, dizemos que os reticulados Λ_1 e Λ_2 são* **congruentes**.

Definição 1.2.3. *Um parâmetro de um reticulado Λ é chamado de* **invariante geométrico** *de Λ se ele permanece constante na classe de reticulados equivalentes.*

1.2.1 Reticulados equivalentes na métrica euclidiana

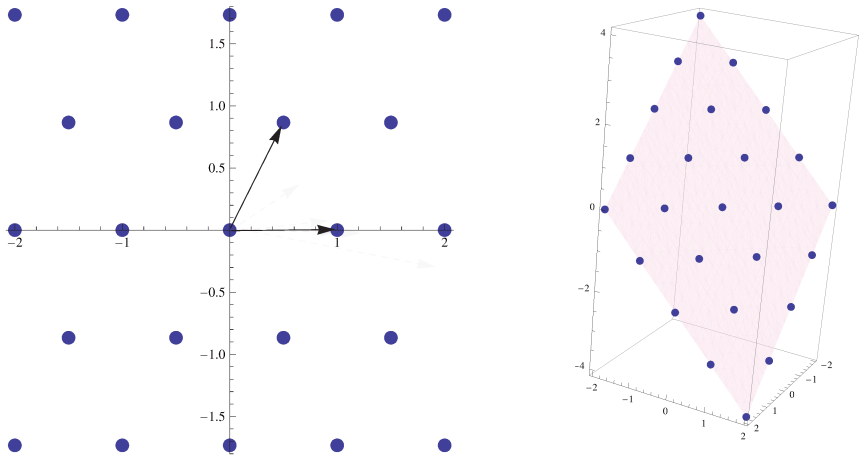
Considerando a métrica euclidiana, temos que isometrias em reticulados são dadas por rotações e reflexões compostas com translações por vetores do reticulado [23].

Sejam Λ_1 e Λ_2 reticulados equivalentes na métrica euclidiana, com matrizes geradoras M_1 e M_2, respectivamente. Temos que existem $\lambda \in \mathbb{R}$, uma matriz unimodular U e uma matriz ortogonal R tais que $M_2 = \lambda U M_1 R$. As respectivas matrizes de Gram estão associadas por

$$G_2 = M_2 M_2^t = \lambda^2 U M_1 M_1^t U^t = \lambda^2 U G_1 U^t.$$

Proposição 1.2.1. *[40] Dados dois reticulados Λ_1 e Λ_2 com a métrica euclidiana com matrizes de Gram G_1 e G_2, respectivamente, se existe um número real positivo λ tal que $G_1 = \lambda^2 G_2$, então os reticulados Λ_1 e Λ_2 são equivalentes.* □

Exemplo 1.2.1. *A Figura 1.5 mostra o reticulado hexagonal com base $\{(1,0),(1/2,\sqrt{3}/2\}$ definido no $\mathbb{R}^2$ e o reticulado A_2 com base $\{(-1,1,0),(0,-1,1)\}$ definido no $\mathbb{R}^3$.*



(a) Reticulado hexagonal (b) Reticulado A_2

Figura 1.5: Reticulados equivalentes na métrica euclidiana

Temos que tais reticulados são equivalentes pois suas matrizes de Gram estão associadas por

$$\begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} = \sqrt{2}^2 \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix},$$

onde a matriz da esquerda é uma matriz de Gram do reticulado hexagonal e a da direita é uma matriz de Gram do reticulado A_2.

Uma outra forma de ver a equivalência é considerar o reticulado hexagonal imerso no $\mathbb{R}^3$ *com base*

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 1/2 & \sqrt{3}/2 & 0 \end{pmatrix}.$$

Primeiro fazemos uma dilatação por $\sqrt{2}$ *em tal reticulado e depois aplicamos a transformação ortogonal dada por*

$$R = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{6} & 1/\sqrt{3} \\ -1/\sqrt{2} & 1/\sqrt{6} & 1/\sqrt{3} \\ 0 & \sqrt{2}/\sqrt{3} & 1/\sqrt{3} \end{pmatrix}$$

donde obtemos o reticulado A_2.

Considerando a métrica euclidiana, temos que o mesmo reticulado pode ser representado

de diferentes maneiras e algumas de suas propriedades como a densidade não variam, já a diversidade, como veremos a seguir, pode mudar consideravelmente com uma rotação.

1.2.2 Reticulados equivalentes na métrica da soma

Proposição 1.2.2. *[2] As isometrias $\phi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ com a métrica da soma que fixam a origem são dadas por permutações de coordenadas compostas com trocas de sinais em algumas entradas e o grupo de isometrias é isomorfo a $\mathbb{Z}_2^n \rtimes S_n$, onde S_n é o grupo de permutações.* □

Pela proposição acima, temos que as isometrias entre reticulados no $\mathbb{R}^n$ com relação à métrica da soma são composições de translações por vetores do reticulado com permutações de coordenadas e mudanças de sinal em algumas entradas. Aplicar essas isometrias em um reticulado com a métrica da soma equivale a multiplicar sua matriz geradora à direita por uma matriz ortogonal que possui em cada coluna somente uma entrada não nula sendo ± 1 esta entrada.

Observação 1.2.1. *É fácil ver que toda isometria com a métrica da soma é uma isometria com a métrica euclidiana. Portanto, reticulados equivalentes na métrica da soma são equivalentes na métrica euclidiana. É interessante observar que não vale o contrário.*

Observação 1.2.2. *Não é verdade que dois reticulados Λ_1 e Λ_2 que possuem matrizes de Gram associadas por $G_1 = \lambda G_2$ sejam equivalentes, como vale no caso euclidiano. Considere o reticulado $\mathbb{Z}^2$ e uma versão rotacionada deste reticulado por 45 graus. Neste exemplo, os reticulados possuem matrizes de Gram idênticas e não são equivalentes, pois a rotação por 45 graus não é isometria na métrica da soma. De fato, o vetor $(1,0) \in \mathbb{Z}^2$ é levado pela rotação no vetor $(\sqrt{2}/2, -\sqrt{2}/2)$ e $d_{soma}((1,0),(0,0)) = 1$ enquanto que $d_{soma}((\sqrt{2}/2, -\sqrt{2}/2),(0,0)) = \sqrt{2}$.*

1.3 Problemas envolvendo reticulados

1.3.1 Número de vizinhos

Um problema bastante estudado envolvendo reticulados é o problema do número de vizinhos, (*kissing number*).

Definição 1.3.1. *Seja d um métrica em $\mathbb{R}^n$. Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, chamamos de* **vetor de distância mínima***, os vetores não nulos $\boldsymbol{x} \in \Lambda$ que minimizam $d(\boldsymbol{x}, \mathbf{0}) = min\{d(\boldsymbol{y}, \mathbf{0});\ \boldsymbol{y} \in \Lambda,\ \boldsymbol{y} \neq \mathbf{0}\}$ e de* **distância mínima***, o valor $\lambda = d(\boldsymbol{x}, \mathbf{0})$ para $\boldsymbol{x}$ vetor de distância mínima.*

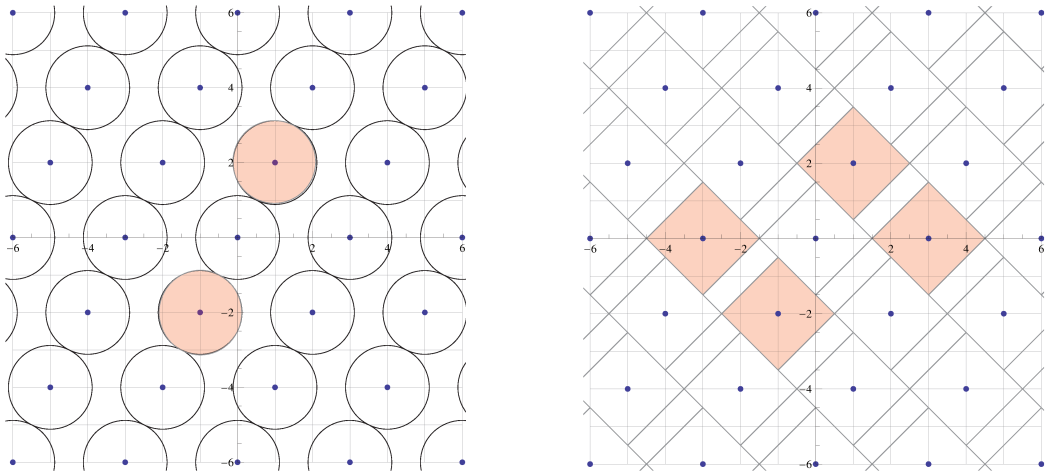
Definição 1.3.2. *Dado um reticulado Λ e uma métrica d em $\mathbb{R}^n$, chamamos de kissing number a quantidade de vetores de distância mínima do reticulado.*

Dados um reticulado Λ em uma métrica d em $\mathbb{R}^n$, se traçarmos esferas de raio $\lambda/2$ ao redor de cada ponto do reticulado de forma que estas esferas no máximo tangenciam umas as outras, o *kissing number* mede quantas esferas tocam uma esfera central. Uma questão interessante é saber para cada dimensão qual o reticulado que apresenta o maior número de vizinhos. Com a métrica euclidiana, nas dimensões 2, 3, 8 e 24 são conhecidos os maiores *kissing numbers* possíveis, que correspondem à 6, 12, 240 e 196560, respectivamente [23].

Exemplo 1.3.1. *Considere o reticulado Λ com base $\{(-3, 0), (-2, 2)\}$ na Figura 1.6. Temos que os vetores de distância mínima na métrica euclidiana são $\{(1, 2), (-1, -2)\}$ (figura (a)) e na métrica da soma são $\{(1, 2), (-1, -2), (-3, 0), (3, 0)\}$ (figura (b)). Portanto, o reticulado Λ possui kissing number 2 na métrica euclidiana e kissing number 4 na métrica da soma.*

1.3.2 Densidade de Empacotamento

A densidade de empacotamento é um dos principais tópicos estudados envolvendo reticulados. Dado uma métrica d em $\mathbb{R}^n$, a densidade de empacotamento fornece uma medida de quanto do espaço pode ser coberto por esferas de mesmo raio na métrica d, de forma que estas esferas ou não se interceptam ou se interceptam apenas no bordo. Em cada dimensão busca-se pelo reticulado com a maior densidade de empacotamento possível e são poucas as



(a) Métrica euclidiana (b) Métrica da soma

Figura 1.6: Número de vizinhos

dimensões em que tais reticulados são conhecidos. A densidade é amplamente estudada para a métrica euclidiana e existem poucas referências de seu estudo na métrica da soma.

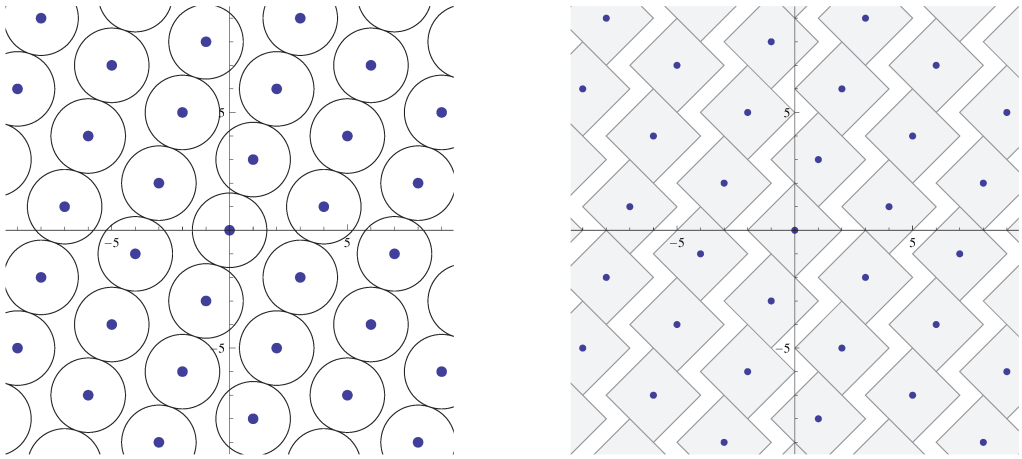
Definição 1.3.3. *Seja d uma métrica em $\mathbb{R}^n$. Um* **empacotamento de esferas**, *ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que quaisquer duas esferas ou não se interceptam ou se interceptam no bordo. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio. Um* **empacotamento reticulado** *é um empacotamento em que o conjunto dos centros das esferas forma um reticulado Λ em $\mathbb{R}^n$.*

Exemplo 1.3.2. *A Figura 1.7 mostra um empacotamento do reticulado com base $\boldsymbol{B} = \{(1,3),(0,11)\}$ tendo raio máximo com a distância euclidiana (figura (a)) e com a distância da soma (figura (b)).*

No Exemplo 1.3.2, as esferas possuem o maior raio no qual duas a duas se interceptam no máximo no bordo. A seguir, vamos descrever empacotamentos reticulados em que as esferas tenham raio máximo.

Definição 1.3.4. *Chamamos de* **raio de empacotamento** *de um reticulado Λ em relação a uma métrica d o valor*

$$\boldsymbol{\rho} = max\{r \in \mathbb{R};\ \Lambda + B_d[0,r] \text{ é um empacotamento reticulado}\},$$



(a) Métrica euclidiana (b) Métrica da soma

Figura 1.7: Empacotamento de esferas

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

Observação 1.3.1. *É fácil ver que* $\boldsymbol{\rho} = \lambda/2$*, onde* λ *é o valor da distância mínima de* Λ *na métrica* d*.*

Dado um reticulado Λ*, encontrar a distância mínima é um problema difícil de ser resolvido computacionalmente (a conjectura é que seja NP-hard [49]). Na métrica euclidiana é conjecturado que não existe algoritmo em tempo polinomial capaz de resolver tal problema [49].*

Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ, a **densidade de empacotamento** $\Delta(\Lambda)$ é a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas de raio ρ centradas nos pontos de Λ.

Denotando por $B_d[0, \boldsymbol{\rho}]$ a esfera na métrica d com centro na origem e raio $\boldsymbol{\rho}$, temos que, em virtude da homogeneidade, a **densidade de empacotamento** de um reticulado $\Lambda \subseteq \mathbb{R}^n$ de posto n é igual a

$$\begin{aligned}\Delta(\Lambda) &= \frac{\text{Volume de uma esfera de raio } \boldsymbol{\rho}}{\text{Volume da região fundamental de } \Lambda} = \frac{\text{vol}(B_d[\mathbf{0}, \boldsymbol{\rho}])}{\text{vol}(\Lambda)} \\ &= \frac{\text{vol}(B_d[\mathbf{0}, 1])\boldsymbol{\rho}^n}{\text{vol}(\Lambda)} = \frac{\text{vol}(B_d[\mathbf{0}, 1])\boldsymbol{\rho}^n}{\det(\Lambda)^{1/2}}.\end{aligned}$$

Para a métrica euclidiana, temos que o volume da bola unitária n-dimensional é dado em [23] por:

$$\mathrm{vol}(B_{eucl}[\mathbf{0},1]) = \begin{cases} \dfrac{\pi^{n/2}}{(\frac{n}{2})!}, \text{ se } n \text{ é par,} \\ \\ \dfrac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!}, \text{ se } n \text{ é ímpar.} \end{cases}$$

Para a métrica da soma, temos que o volume euclidiano da bola unitária é dado em [56] por:

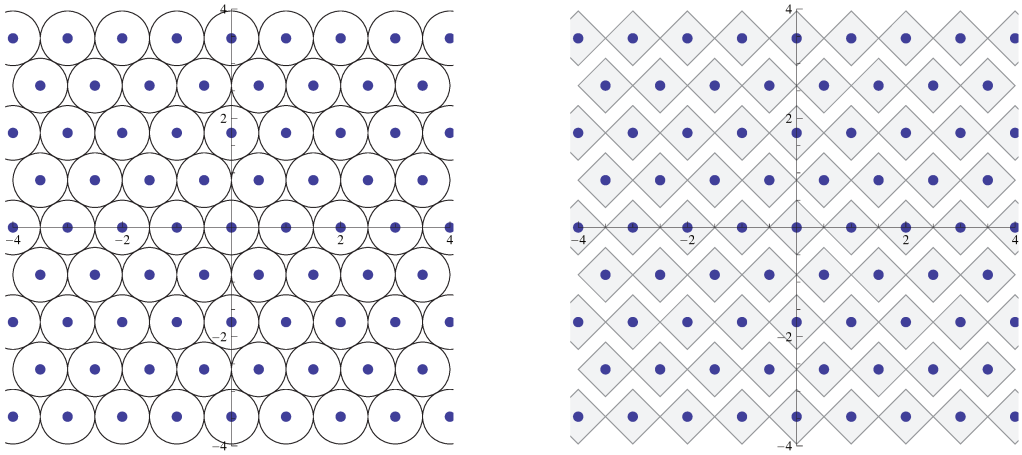
$$\mathrm{vol}(B_{soma}[\mathbf{0},1]) = \frac{2^n}{n!}.$$

Fixada a dimensão, o problema do empacotamento máximo se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por

$$\delta(\Lambda) = \frac{\boldsymbol{\rho}^n}{\mathrm{vol}(\Lambda)},$$

o qual depende do reticulado Λ e do raio $\boldsymbol{\rho}$.

Exemplo 1.3.3. *Considere o reticulado hexagonal com base* $\{(1,0),(1/2,\sqrt{3}/2)\}$ *dado pela Figura 1.8.*



(a) Métrica euclidiana (b) Métrica da soma

Figura 1.8: Empacotamento de esferas

Temos que sua densidade nas métricas euclidiana e da soma são dadas por

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

Este é o empacotamento mais denso em $\mathbb{R}^2$ com a distância euclidiana, até mesmo se comparado com empacotamentos não reticulados.

Observação 1.3.2. *Para a distância euclidiana e da soma temos:*

- *Para a métrica euclidiana já foram demonstrados quais são os empacotamentos reticulados mais densos nas dimensões de 1 a 8 [23] e na dimensão 24 [22]. Foi provado que nas dimensões de 1 a 3 os empacotamentos mais densos são empacotamentos reticulados. Em algumas outras dimensões são conhecidos reticulados mais densos, mas nada foi provado.*

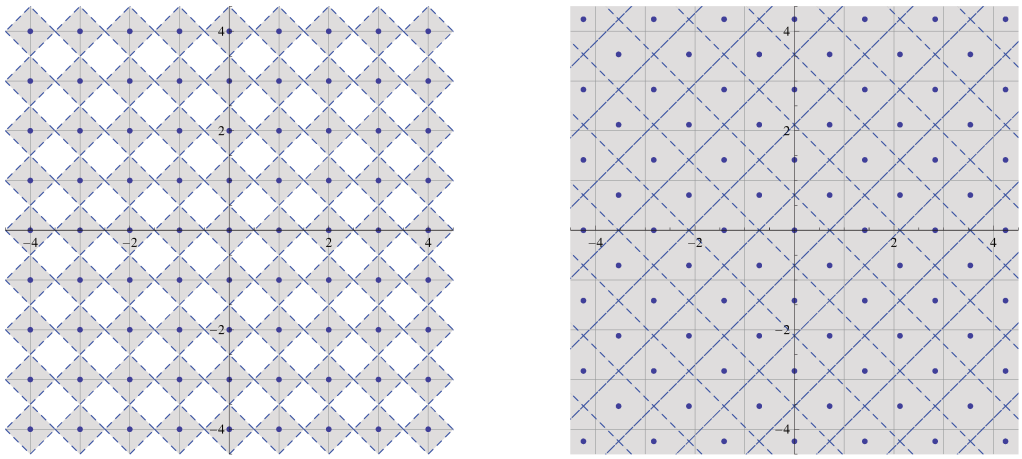
- *Para a métrica da soma foi provado quais são os empacotamentos reticulados mais densos nas dimensões de 1 a 3 [29]. Nas demais dimensões somente poucos limitantes são conhecidos para a densidade de empacotamento.*

Exemplo 1.3.4. *Considere o reticulado $\Lambda \subseteq \mathbb{R}^3$ com base $\{(1,-2,3),(-2,3,1),(3,1,-2)\}$. Temos que a densidade da soma de tal reticulado é $18/19$ e foi demonstrado por Minkowski [29] que essa é a densidade da soma máxima em $\mathbb{R}^3$.*

Proposição 1.3.1. *[40] A densidade de empacotamento na métrica euclidiana é um invariante geométrico, isto é, reticulados equivalentes têm a mesma densidade.* □

Exemplo 1.3.5. *Considere o reticulado $\mathbb{Z}^2$ com a métrica da soma, dado pela Figura 1.9. Temos que sua densidade na métrica da soma é $\Delta_{soma}(\mathbb{Z}^2) = \frac{2^2(1/2)^2}{2!} = 1/2 = 0,5$. Agora, aplicando uma rotação de 45 graus em tal reticulado obtemos a densidade na métrica da soma $\Delta_{soma}(Rot(\mathbb{Z}^2)) = \frac{2^2(\sqrt{2}/2)^2}{2!} = 1$, que é máxima.*

Observação 1.3.3. *A densidade de empacotamento é um invariante geométrico para reticulados na métrica da soma. De fato, basta notar que se Λ_1 e Λ_2 são dois reticulados equivalentes na métrica da soma por um fator de dilatação α e uma permutação nas coordenadas composta com trocas de sinais. Seus determinantes estão associados por $\det(\Lambda_1) = \alpha^n \det(\Lambda_2)$. Assim, se ρ é o raio de empacotamento de Λ_1, então $\Delta_{soma}(\Lambda_1) = \frac{\mathrm{vol}(B_{soma}(\alpha\rho))}{\det(\Lambda_2)^{1/2}} = \frac{\alpha^n \mathrm{vol}(B_{soma}(\rho))}{\alpha^n \det(\Lambda_1)^{1/2}} = \Delta_{soma}(\Lambda_1)$.*



(a) Reticulado $\mathbb{Z}^2$ (b) Reticulado $\mathbb{Z}^2$-rotacionado

Figura 1.9: Diversidade

Observação 1.3.4. *Existem reticulados em que a densidade euclidiana é maior que a densidade da soma e vice-versa. Por exemplo, o reticulado $\mathbb{Z}^2$ possui densidade euclidiana maior que sua densidade da soma. Aplicando uma rotação de 45 graus, sua densidade da soma é maior que sua densidade euclidiana.*

1.3.3 Raio de cobertura

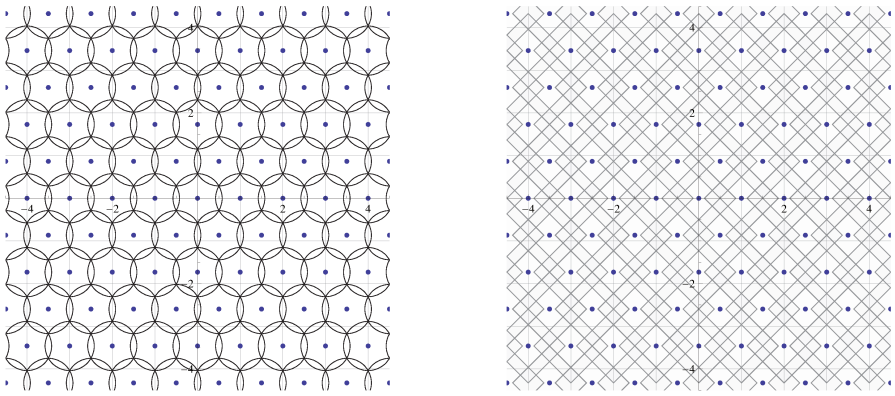
O problema do raio de cobertura é de certa forma dual ao problema do raio de empacotamento. Dado um reticulado, o objetivo é encontrar o menor raio tal que a reunião de esferas de mesmo raio cobrem o $\mathbb{R}^n$.

Definição 1.3.5. *Dados um reticulado Λ e uma métrica d em $\mathbb{R}^n$, o conjunto $\Lambda + B_d[0, r]$ é dito uma* **cobertura** *de $\mathbb{R}^n$ se $\mathbb{R}^n \subseteq \Lambda + B_d[0, r]$.*

Definição 1.3.6. *Dados um reticulado Λ e uma métrica d em $\mathbb{R}^n$, chamamos de* **raio de cobertura** *do reticulado o valor*

$$\tau = min\{r;\ \Lambda + B_d[\mathbf{0}, r] \ \text{ é uma cobertura do } \mathbb{R}^n\}.$$

Exemplo 1.3.6. *Considere o reticulado hexagonal Λ. A Figura 1.10 mostra o raio de cobertura de Λ em relação à métrica euclidiana e à métrica da soma.*



(a) Métrica euclidiana (b) Métrica da soma

Figura 1.10: Raio de cobertura

Observação 1.3.5. *Note que se τ é o raio de cobertura de um reticulado Λ na métrica euclidiana e χ é o raio de cobertura de Λ na métrica da soma temos que $\tau \leq \chi \leq \tau\sqrt{n}$.*

1.3.4 Região de Voronoi

A região de Voronói de um ponto $\boldsymbol{x} \in \Lambda$ é o conjunto dos pontos de $\mathbb{R}^n$ que estão mais próximos de $\boldsymbol{x}$, segundo uma métrica d, do que qualquer outro ponto de Λ.

Definição 1.3.7. *Se $\boldsymbol{v} \in \Lambda$, a* **região de Voronoi** *de $\boldsymbol{v}$ é o conjunto*

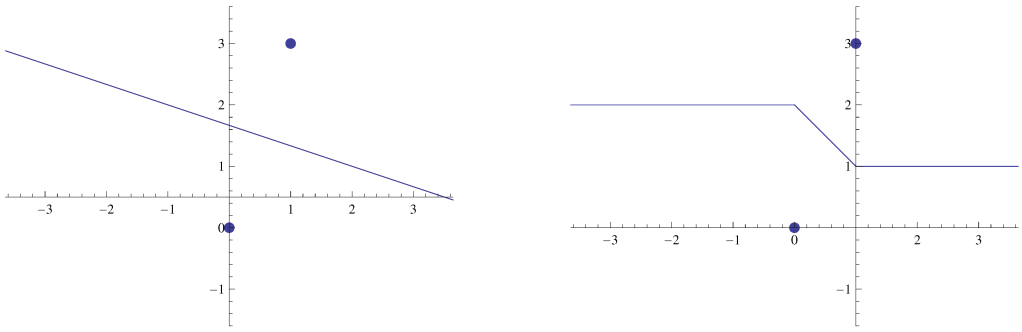
$$R(\boldsymbol{v}) = \{\boldsymbol{x} \in \mathbb{R}^n;\ d(\boldsymbol{v}, \boldsymbol{x}) \leq d(\boldsymbol{u}, \boldsymbol{x});\ \boldsymbol{u} \in \Lambda\}.$$

Observação 1.3.6. *Como translação por um vetor do reticulado é uma isometria tanto na métrica da soma como na euclidiana, toda região de Voronoi ao redor de um ponto $\boldsymbol{v} \in \Lambda$ pode ser obtida por uma translação da região de Voronoi do ponto zero, isto é,*

$$R(\boldsymbol{v}) = \boldsymbol{v} + R(\boldsymbol{0}).$$

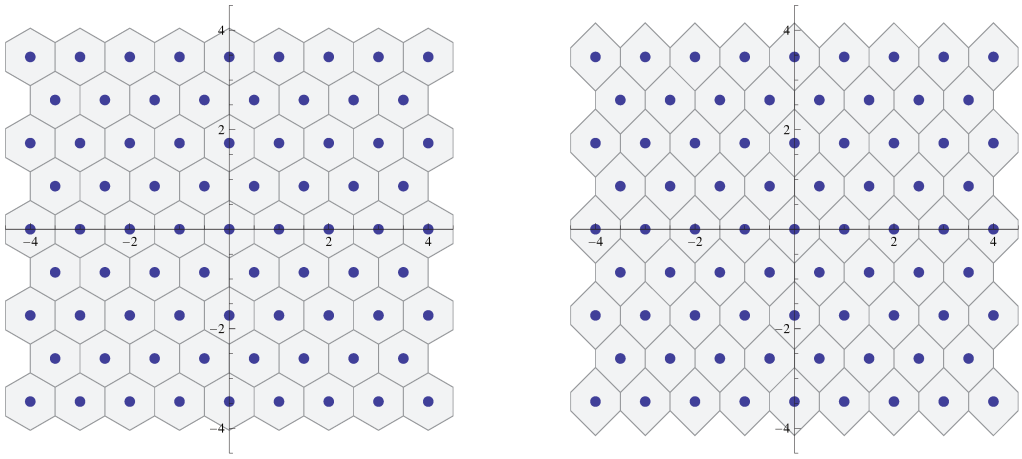
Exemplo 1.3.7. *Dados os pontos $\boldsymbol{x} = (0,0), \boldsymbol{y} = (1,3) \in \mathbb{R}^2$, o conjunto dos pontos $\boldsymbol{z}$ que satisfazem $d_{eucl}(\boldsymbol{z}, \boldsymbol{x}) = d_{eucl}(\boldsymbol{z}, \boldsymbol{y})$ e $d_{soma}(\boldsymbol{z}, \boldsymbol{x}) = d_{soma}(\boldsymbol{z}, \boldsymbol{y})$ são dados pela Figura 1.11.*

Exemplo 1.3.8. *Considere o reticulado hexagonal Λ com base $\{(1,0), (1/2, \sqrt{3}/2)\}$. A Figura 1.12 mostra as regiões de Voronoi de Λ segundo a distância euclidiana e a distância da soma.*



(a) Métrica euclidiana (b) Métrica da soma

Figura 1.11: $\boldsymbol{x} = (0,0), \boldsymbol{y} = (1,3)$



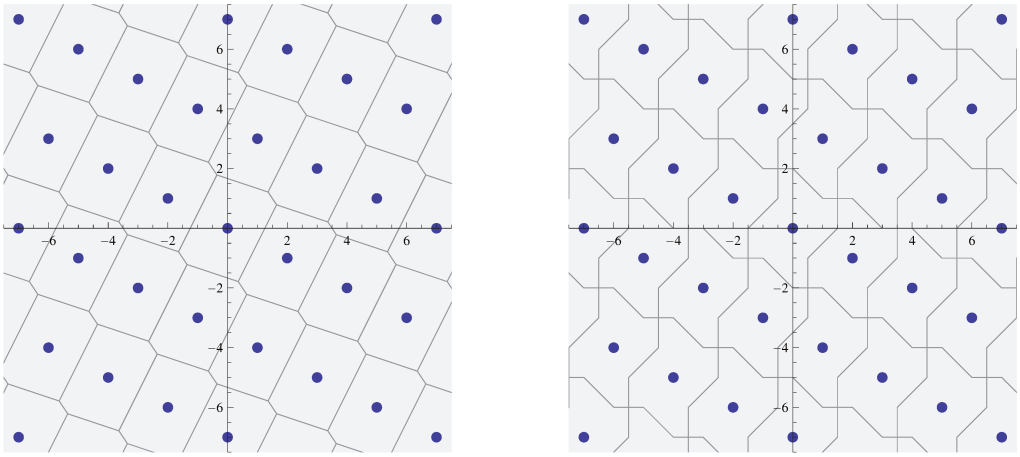
(a) Métrica euclidiana (b) Métrica da soma

Figura 1.12: Região de Voronoi

Exemplo 1.3.9. *Considere o reticulado com base* $\{(1,3),(0,7)\}$. *A Figura 1.13 representa a região de Voronoi de* Λ *em relação à distância euclidiana e em relação à distância da soma.*

Observação 1.3.7. *Embora as regiões de Voronoi obtidas com a métrica euclidiana e da soma sejam diferentes, elas possuem o mesmo volume euclidiano, pois ladrilham* $\mathbb{R}^n$ *por translações dos pontos do reticulado e seu volume, dado por* $\det(\Lambda)^{1/2}$, *é o mesmo que de qualquer politopo fundamental de* Λ.

Os vértices das regiões de Voronoi são especialmente interessantes. Eles incluem os pontos do $\mathbb{R}^n$ cuja distância a Λ é um máximo absoluto.



(a) Métrica euclidiana (b) Métrica da soma

Figura 1.13: Região de Voronoi

1.3.5 Diversidade e Distância Produto Mínima

A diversidade e a distância produto mínima são parâmetros estudados nos reticulados para serem utilizados em canais do tipo Rayleigh com desvanecimento. Para este canal o problema de minimizar a probabilidade de erros na transmissão de sinais ligados a reticulados está associado à reticulados com diversidade máxima e a maior distância produto mínima possível [17].

Definição 1.3.8. *Dados dois vetores* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$*, definimos a* **diversidade** *ou a distância de Hamming de* $\boldsymbol{x}$ *e* $\boldsymbol{y}$ *como*

$$div(\boldsymbol{x}, \boldsymbol{y}) = \#\{i,\ x_i \neq y_i,\ i = 1, \ldots, n\}.$$

Definição 1.3.9. *Dado um subconjunto* $S \subseteq \mathbb{R}^n$*, a* **diversidade** *ou a distância mínima de Hamming de* S *é definida por*

$$div(S) = min\{div(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \neq \boldsymbol{y}, \boldsymbol{x},\ \boldsymbol{y} \in S\}.$$

Todo reticulado Λ é um subconjunto do $\mathbb{R}^n$. Desta forma, podemos estender as Definições (1.3.8) e (4.6.9) para reticulados. Como reticulados têm estrutura de grupo, isto é, a soma de quaisquer dois elementos de Λ pertence à Λ, podemos reformular as definições.

Definição 1.3.10. *Seja* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado e* $\boldsymbol{x} = (x_1, \ldots, x_n) \in \Lambda$.

- *A* **diversidade** *de* $\boldsymbol{x}$ *é definida como o número de* x_i*'s não nulos;*
- *A* **diversidade** *de* Λ *é definida como* $div(\Lambda) = min\{div(\boldsymbol{x});\ \boldsymbol{x} \in \Lambda,\ \boldsymbol{x} \neq \boldsymbol{0}\}$.

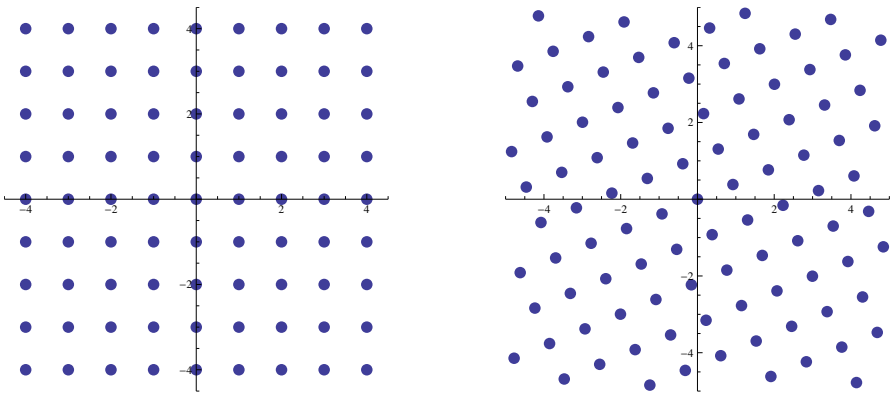
Exemplo 1.3.10. *Para o reticulado* $\mathbb{Z}^2$*, temos que*

$$div(\mathbb{Z}^2) = min\{div(\boldsymbol{x});\ \boldsymbol{x} \in \mathbb{Z}^2,\ \boldsymbol{x} \neq \boldsymbol{0}\} = 1.$$

Um reticulado $\mathbb{Z}^2$*-rotacionado* Λ_θ *com base* $\{(cos(\theta), sen(\theta)), (-sen(\theta), cos(\theta))\}$ *terá diversidade máxima se* $\tan(\theta) \notin \mathbb{Q}$*. Por exemplo, reticulado* Λ *com base*

$$\left\{\left(-\sqrt{2-\sqrt{2}}, -\sqrt{2+\sqrt{2}}\right), \left(-\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}\right)\right\}$$

dado pela Figura 1.14, possui diversidade máxima.



(a) Reticulado $\mathbb{Z}^2$ (b) Reticulado $\mathbb{Z}^2$-rotacionado

Figura 1.14: Diversidade

O reticulado da direita que possui diversidade máxima não possui nenhum ponto interceptando os eixos coordenados. Além disso, como o reticulado é um grupo aditivo, dados quaisquer dois pontos do reticulado eles diferem em todas as entradas.

Observação 1.3.8. *A diversidade é um invariante geométrico para reticulados com a métrica da soma. Já para a métrica euclidiana a diversidade varia com rotações, portanto, não é um invariante geométrico.*

Definição 1.3.11. *Sejam* Λ *um reticulado em* $\mathbb{R}^n$ *com diversidade* $l \leq n$ *e* $\boldsymbol{x} = (x_1, \cdots, x_n) \in \Lambda$*. Definimos:*

- *A* **distância l-produto** *de* $\boldsymbol{x}$ *por* $d_p^l(\boldsymbol{x}) = \prod_{x_i \neq 0} |x_i|$;
- *A* **distância l-produto mínima** *de* Λ *por* $d_{p,min}^l(\Lambda) = min\{d_p^l(\boldsymbol{x}) \mid \boldsymbol{x} \neq \boldsymbol{0}, \boldsymbol{x} \in \Lambda\}$.

Definição 1.3.12. *Sejam* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado com diversidade* n *e* $\boldsymbol{x} = (x_1, \cdots, x_n) \in \Lambda$.

- *A* **distância produto** *de* $\boldsymbol{x}$ *é definida como* $d_p(\boldsymbol{x}) = \prod_{i=1}^{n} |x_i|$.
- *A* **distância produto mínima** *de* Λ *é definida como*

$$d_{p,min}(\Lambda) = min\{d_p(\boldsymbol{x}) \mid \boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0}\}.$$

Definição 1.3.13. *Chamamos de* **distância produto mínima relativa** *de um reticulado* Λ *e denotamos por* $d_{p,rel}(\Lambda)$*, a distância produto mínima da versão escalonada de* Λ *que possui vetor de distância mínima unitário.*

Para calcular a distância produto mínima relativa de um reticulado Λ com distância mínima ρ, devemos dividir a distância produto mínima de Λ por ρ^n.

1.3.6 Decodificação em reticulados

A decodificação é um problema muito estudado envolvendo reticulados (SVP - shortest vector problem) no que se refere a aplicações. Dados um reticulado Λ, uma métrica d em $\mathbb{R}^n$ e um vetor recebido $\boldsymbol{y}$, procura-se pelo vetor $\boldsymbol{x} \in \Lambda$ mais próximo de $\boldsymbol{y}$, isto é, queremos encontrar $\boldsymbol{x} \in \Lambda$ tal que

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

Decodificação na métrica euclidiana

Para a métrica euclidiana é conjecturado que não existe algoritmo em tempo polinomial capaz de resolver o SVP para reticulados gerais e este fato é utilizado em criptossistemas pós-quânticos [49].

Alguns reticulados, como por exemplo os reticulados $\mathbb{Z}^n$, D_n, A_n e E_8, apresentam algoritmos próprios de decodificação para a métrica euclidiana [23]. Isto se deve à algumas características especiais que eles apresentam e que não são encontradas em reticulados gerais.

Alguns dos algoritmos mais estudados para tentar resolver o SVP são os algoritmos de redução de base [42, 62, 8], o *Sphere decoding* [65, 66, 34] e a decodificação por treliças [8].

Os principais métodos de redução de base são a redução de Minkowski, o LLL e a base K-Z reduzida. Tais métodos procuram por uma base do reticulado que tenha os vetores "mais ortogonais possível" e de tamanho "razoavelmente pequeno". A decodificação é feita através de projeções do vetor recebido nessa base. Os métodos de Minkowski e K-Z são reduções ótimas, no sentido que a base contém um vetor de norma mínima do reticulado. A desvantagem é que não existe algoritmo em tempo polinomial conhecido capaz de calcular a base de Minkowski ou a base K-Z-reduzida de um reticulado qualquer. Já o método LLL possui um algoritmo em tempo polinomial que calcula sua base reduzida, porém tal base pode não ser a melhor possível e a decodificação usando esta base pode falhar.

A decodificação por treliças será abordada no próximo capítulo. O método *Sphere decoding* apresenta alto custo computacional também, mas pode ser especialmente útil, por exemplo, em situações onde a mudança de base não pode ser utilizada.

Decodificação na métrica d_p

Para cada $1 \leq p < \infty$, a *norma* $\|.\|_p : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow [0, +\infty)$ definida por

$$\|\boldsymbol{x}\|_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}$$

induz a métrica d_p em $\mathbb{R}^n$ pondo $d_p(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|_p$ para todo $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$.

Neste seção, propomos uma modificação no algoritmo *Sphere decoding* clássico para a métrica d_p. O algoritmo foi desenvolvido em conjunto com Antonio Campello. Para a métrica da soma, no caso de reticulados q-ários, q primo um estudo detalhado será feito no Capítulo 3. Dado um vetor $\boldsymbol{y} \in \mathbb{R}^n$, o objetivo é encontrar o ponto do reticulado Λ que está mais próximo de $\boldsymbol{y}$ na métrica d_p. O algoritmo procura o ponto do reticulado mais próximo entre os pontos que se encontram dentro de uma esfera centrada em $\boldsymbol{y}$ com um certo raio R pré-definido.

A Figura 1.15 mostra um exemplo da esfera da soma ($p = 1$) centralizada em um vetor recebido $\boldsymbol{y}$.

A dificuldade do algoritmo é como determinar o raio R de forma que dentro da esfera

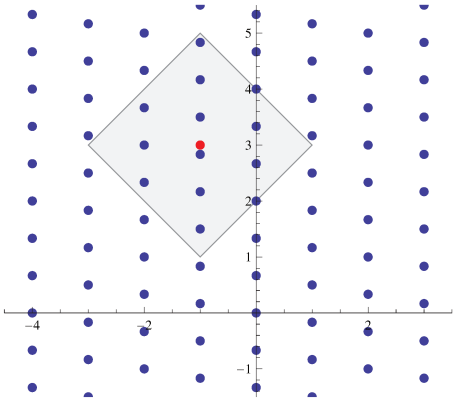


Figura 1.15: *Esfera centrada em* $\boldsymbol{y} = (-1, 2.8)$ *com a métrica da soma*

centralizada em $\boldsymbol{y}$ exista pelo menos um ponto do reticulado e que esse raio não seja muito grande, pois existiriam muitos pontos do reticulado dentro desta esfera a serem testados. O raio natural a ser escolhido é o raio de cobertura, mas que é difícil de ser encontrado em um reticulado geral.

O estudo do método *Sphere decoding* clássico é abordado por exemplo nos artigos [65, 66, 34]. Nestes artigos o algoritmo é estudado para a distância euclidiana e uma estratégia utilizada para melhor gerar os pontos do reticulado dentro da esfera foi usar fatoração de matrizes. Em [65, 66] é feita uma fatoração de Cholesky em uma matriz de Gram do reticulado. Em [34], é feita uma fatoração QR na matriz geradora do reticulado. Tais decomposições não podem ser aplicadas a outras métricas, pois no decorrer do algoritmo elas estão relacionadas com rotações no reticulado, as quais são isometrias na métrica euclidiana.

Vamos trabalhar com uma matriz geradora do reticulado na forma normal de Hermite, por isso restringiremos nosso estudo a reticulados inteiros.

Sejam $\boldsymbol{y} \in \mathbb{R}^n$ e $\boldsymbol{H}$ a matriz geradora do reticulado $\Lambda \subseteq \mathbb{Z}^n$ na forma normal de Hermite. Cada ponto do reticulado Λ pode ser descrito como $\boldsymbol{sH}$ para algum $\boldsymbol{s} \in \mathbb{Z}^n$. Vamos procurar os pontos de Λ que se encontram na esfera centralizada em $\boldsymbol{y}$ com raio R na métrica d_p, isto é, queremos encontrar os vetores $\boldsymbol{s} \in \mathbb{Z}^n$ que satisfazem

$$d_p(\boldsymbol{sH}, \boldsymbol{y}) = \|\boldsymbol{sH} - \boldsymbol{y}\|_p \leq R.$$

Sejam $\lceil a \rceil$ e $\lfloor a \rfloor$ denotando o maior e o menor inteiro mais próximo de a, respectivamente.

Temos que

$$\boldsymbol{sH} = (s_1, \cdots, s_n) \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ 0 & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_{nn} \end{pmatrix} = (s_1 h_{11}, s_1 h_{12} + s_2 h_{22}, \cdots, \sum_{i=1}^{n} s_i h_{in}) \text{ e}$$

$$\|\boldsymbol{sH} - \boldsymbol{y}\|_p^p = |s_1 h_{11} - y_1|^p + |s_1 h_{12} + s_2 h_{22} - y_2|^p + \cdots + \left| \sum_{i=1}^{n} s_i h_{in} - y_n \right|^p . \tag{1.1}$$

Vamos encontrar as soluções de $\|\boldsymbol{sH} - \boldsymbol{y}\|_p^p \leq R^p$, formando uma árvore de possibilidades para $s_1, \cdots, s_n$.

Primeiro, vamos analisar os possíveis valores para s_1. Como cada parcela de (1.1) é não negativa, temos que s_1 satisfaz $|s_1 h_{11} - y_1|^p \leq R^p$. Mas, isto acontece se, e somente se,

$$\left\lceil \frac{-R + y_1}{h_{11}} \right\rceil \leq s_1 \leq \left\lfloor \frac{R + y_1}{h_{11}} \right\rfloor .$$

Agora para cada valor de s_1 obtido no intervalo acima vamos calcular as possibilidades para s_2. Fazendo $R_2 = R_1^p - |s_1 h_{11} - y_1|^p \geq 0$ temos

$$\left\lceil \frac{-\sqrt[p]{R_2} + y_2 - s_1 h_{12}}{h_{22}} \right\rceil \leq s_2 \leq \left\lfloor \frac{\sqrt[p]{R_2} + y_2 - s_1 h_{12}}{h_{22}} \right\rfloor .$$

Fixando s_1 e s_2 (com s_2 dependendo de s_1), obtemos os valores possíveis para s_3 e assim por diante até s_n. Para o nível $k > 1$ temos que

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

onde $R_k = R_{k-1} - |\sum_{i=1}^{k-1} s_i h_{i,k-1} - y_{k-1}|^p$.

Com isso, encontramos os vetores $\boldsymbol{s} \in \mathbb{Z}^n$ tais que $||\boldsymbol{sH} - \boldsymbol{y}||_p \leq R$ e podemos enunciar esse resultado na proposição seguinte.

Proposição 1.3.2. *Sejam $\boldsymbol{y} = (y_1, \cdots, y_n)$ um vetor, $\boldsymbol{H} = (h_{ij})_{i,j=1}^n$ uma matriz geradora do reticulado Λ na forma normal de Hermite e $R > 0$ um raio. Os vetores $\boldsymbol{s} = (s_1, \cdots, s_n) \in \mathbb{Z}^n$ tais que $||\boldsymbol{sH} - \boldsymbol{y}||_p \leq R$ são obtidos (com s_k dependendo de $s_1, \cdots, s_{k-1}$ para $k = 2, \cdots, n$) construindo todos os vetores inteiros nas seguintes variações:*

$$\left\lceil \frac{-R + y_1}{h_{11}} \right\rceil \leq s_1 \leq \left\lfloor \frac{R + y_1}{h_{11}} \right\rfloor$$

e para $k = 2, \cdots, n$

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

com $R_k = R_{k-1} - |\sum_{i=1}^{k-1} s_i h_{i,k-1} - y_{k-1}|^p$. □

A Figura 1.16 esquematiza a relação entre as coordenadas s_i's do vetor $\boldsymbol{s}$. A árvore começa a ser montada a partir de s_1, donde vamos obtendo caminhos. Os pontos do reticulado que estão dentro da esfera centralizada em $\boldsymbol{y}$ são aqueles gerados pelos caminhos que vão até o nível n. No caso da figura seguinte, só é gerado um ponto.

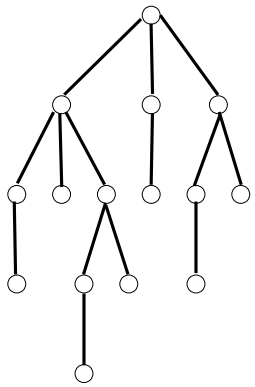


Figura 1.16: Árvore gerada pelos vetores $\boldsymbol{s}$

Definição 1.3.14. *Chamamos de* **ponto factível** *um ponto formado por um caminho da árvore que atinge o nível* n*, ou seja, o vetor* $(s_1, \cdots, s_n)$ *é formado.*

Para cada ponto factível $\boldsymbol{s}$, obtemos o vetor $\boldsymbol{s}H \in \Lambda$ e calculamos sua distância a $\boldsymbol{y}$. No *Sphere decoding* clássico, a medida em que vamos gerando cada nó da árvore vamos calculando distâncias parciais. Isso economiza passos para caminhos com partes em comum e o mesmo pode ser feito para o distância d_p.

Nem todo caminho da árvore gera um ponto factível. A complexidade do algoritmo está relacionada com os nós visitados e não somente com os pontos factíveis. A complexidade também está relacionada com a escolha do raio R. O melhor raio a ser escolhido é o raio de cobertura, que não é conhecido para um reticulado geral. Podemos utilizar a estimativa de

Babai, como é feito em [34]. A estimativa de Babai é obtida da seguinte forma: primeiro encontramos $\boldsymbol{x} \in \mathbb{R}^n$ tal que $\boldsymbol{x}H = \boldsymbol{y}$. Se $\boldsymbol{x}$ possuir todas as entradas inteiras, então $\boldsymbol{y} \in \Lambda$, caso contrário, fazemos o arredondamento ao inteiro mais próximo nas entradas de $\boldsymbol{x}$ de forma que $[\boldsymbol{x}]H \in \Lambda$. Tomando

$$R = \|[\boldsymbol{x}]H - \boldsymbol{y}\|_p$$

temos que existe pelo menos um ponto do reticulado Λ na esfera centralizada em $\boldsymbol{y}$ com raio R.

Observação 1.3.9. *Considere a transformação $\phi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ dada por $\phi(\boldsymbol{x}) = \boldsymbol{x}H$, onde H é uma matriz geradora para Λ. Podemos ver Λ como imagem desta transformação em $\mathbb{Z}^n$, isto é, $\Lambda = \phi(\mathbb{Z}^n)$.*

- *Para $p = 2$ (métrica euclidiana) [65], temos que os pontos do reticulado Λ que estão dentro de uma esfera de raio R são obtidos como imagem de pontos de $\boldsymbol{s} \in \mathbb{Z}^n$ que estão contidos no elipsóide*

$$\|\boldsymbol{s}H - \boldsymbol{y}\|^2 = |s_1h_{11} - y_1|^2 + |s_1h_{12} + s_2h_{22} - y_2|^2 + \cdots + |\sum_{i=1}^{n} s_ih_{in} - y_n|^2 \leq R^2.$$

  O que o algoritmo busca são os pontos deste elipsóide.

- *Para $p = 1$ (métrica da soma), temos que os pontos do reticulado Λ que estão dentro de uma esfera da soma de raio R são obtidos como a imagem de pontos de $\mathbb{Z}^n$ que estão dentro de uma certa esfera rotacionada e dilatada em algumas direções. De fato, para $p = 1$, temos que*

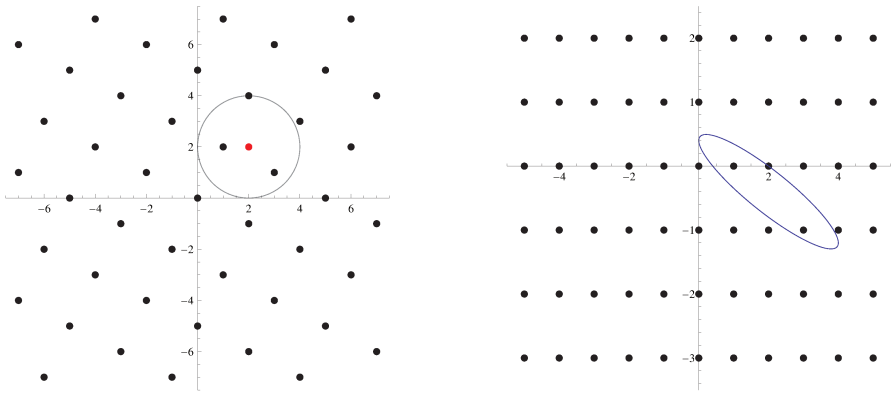
$$\|\boldsymbol{s}H - \boldsymbol{y}\| = |s_1h_{11} - y_1| + |s_1h_{12} + s_2h_{22} - y_2| + \cdots + |\sum_{i=1}^{n} s_ih_{in} - y_n| \leq R.$$

  Fazendo a mudança de variáveis $X_i = \sum_{j=1}^{i} s_jh_{ji}$ para $i = 1, \cdots, n$, temos que

$$|X_1 - y_1| + \cdots + |X_n - y_n| \leq R.$$

  Esta é a equação de uma bola de raio R na métrica da soma.

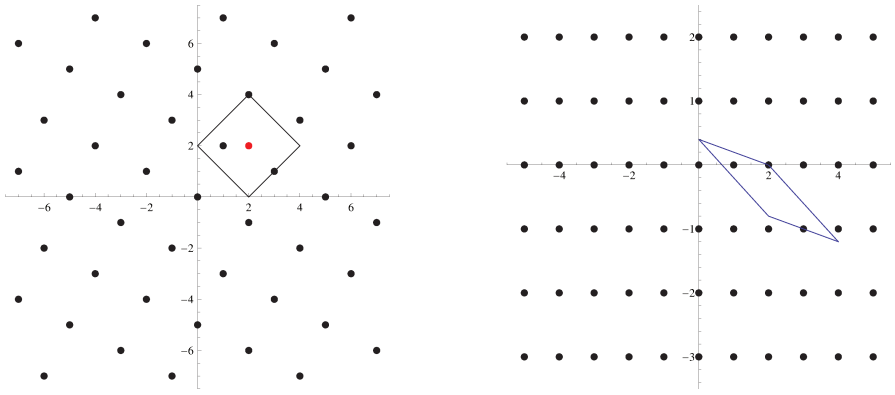
Exemplo 1.3.11. *Considere o reticulado* Λ *com base* $\{(1,2),(0,5)\}$ *e o vetor* $\boldsymbol{y} = (2,2)$. *Para a métrica euclidiana, temos pela estimativa de Babai que* $R = 2$. *A Figura 1.17 mostra a esfera de raio* 2 *centrada em* $\boldsymbol{y}$ *contendo os pontos do reticulado* Λ *(figura (a)) e a elipse* $(s_1 - 2)^2 + (2s_1 + 5s_2 - 2)^2 = 4$ *(figura (b)) contendo os pontos de* $\mathbb{Z}^2$.



(a) (b)

Figura 1.17: Sphere decoding na métrica euclidiana

Para a métrica da soma, temos pela estimativa de Babai que $R = 2$. *A Figura 1.18 mostra a bola de raio* 2 *centrada em* $\boldsymbol{y}$ *contendo os pontos do reticulado* Λ *(figura (a)) e a bola torcida* $|s_1 - 2| + |2s_1 + 5s_2 - 2| = 2$ *(figura (b)) contendo os pontos de* $\mathbb{Z}^2$.



(a) (b)

Figura 1.18: Sphere decoding na métrica da soma

Observação 1.3.10. *Fixado um reticulado* Λ *e um raio* R, *é mais fácil decodificar na métrica da soma do que na métrica euclidiana. Isto se deve ao fato de que na métrica euclidiana*

precisamos extrair raízes quadradas, o que não acontece na métrica da soma. Além disso, na métrica euclidiana podemos gerar mais pontos do que na métrica da soma, pois a bola da soma está contida na bola euclidiana de mesmo raio. Pela estimativa de Babai,

$$R_{eucl} = \|[\boldsymbol{x}]H - \boldsymbol{y}\|_2 \leq \|[\boldsymbol{x}]H - \boldsymbol{y}\|_1 = R_{soma}.$$

1.4 Alguns reticulados importantes e suas propriedades

Nesta seção apresentaremos alguns reticulados que são amplamente estudados na literatura, como por exemplo, em [23].

- O **reticulado** $\mathbb{Z}^n$ definido por

$$\mathbb{Z}^n = \{(x_1, \ldots, x_n); \quad x_i \in \mathbb{Z}, \ \forall i = 1, \cdots, n\} \tag{1.2}$$

  é muito estudado para canais do tipo Rayleigh com desvanecimento, onde versões rotacionadas apresentam diversidade máxima e alta distância produto mínima. Em dimensão 2, sua versão rotacionada por 45 graus apresenta a maior densidade da soma possível na dimensão.

- O **reticulado** A_n**,** $n \geq 1$ definido por

$$A_n = \{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} : \ x_1 + \cdots + x_{n+1} = 0\} \tag{1.3}$$

  apresenta as melhores densidades euclidianas possíveis nas dimensões 2 e 3. Já foi provado inclusive que nas dimensões 2 e 3 sua densidade é máxima considerando empacotamentos reticulados e não reticulados. O reticulado A_2 é equivalente ao reticulado hexagonal na métrica euclidiana.

- O **reticulado** D_n definido por

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \text{ é par}\} \tag{1.4}$$

  possui as melhores densidades euclidianas possíveis nas dimensões 4 e 5.

- O **reticulado** E_8 definido por

$$E_8 = \{(x_1, \ldots, x_8) : \text{todo } x_i \in \mathbb{Z} \text{ ou todo } x_i \in \mathbb{Z} + 1/2, \text{ e } \sum x_i \text{ é par}\} \tag{1.5}$$

  é o reticulado com maior densidade euclidiana na dimensão 8.

- O **reticulado** E_6 definido por

$$E_6 = \{(x_1, \ldots, x_8) \in E_8 : x_1 + x_8 = x_2 + \cdots + x_7 = 0\} \tag{1.6}$$

  apresenta a maior densidade euclidiana em sua dimensão.

- O **reticulado** E_7 definido por

$$E_7 = \{(x_1, \ldots, x_8) \in E_8 : x_1 + \cdots + x_8 = 0\} \tag{1.7}$$

  apresenta a maior densidade euclidiana em sua dimensão.

- O **reticulado MCC - Mean-centered cuboidal** que possui como uma base

$$\left\{ \left(\sqrt{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}, 0 \right), \left(\sqrt{\frac{1}{2}}, 0, \sqrt[4]{\frac{1}{2}} \right), \left(0, \sqrt[4]{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}} \right) \right\}. \tag{1.8}$$

  é um ótimo quantizador.

Os reticulados A_n, D_n, E_8, E_6, E_7 e $\mathbb{Z}^n$ são chamados de **reticulados raízes** devido a uma associação com o sistema de raízes de certas álgebras de Lie e vale o seguinte resultado:

Teorema 1.4.1. *[46] Um reticulado integral que é gerado por vetores de normas euclidiana* 1 *e* 2 *é uma soma ortogonal de reticulados equivalentes aos reticulados raízes.*

CAPÍTULO 2

TRELIÇAS

O método de decodificação por treliças foi introduzido para códigos lineares em [31] e depois para reticulados que possuem um sub-reticulado ortogonal na métrica euclidiana em [8]. Dado um reticulado Λ, a complexidade de decodificar Λ por treliças está associada à cardinalidade do grupo quociente $\Lambda/\Lambda^\star$, onde $\Lambda^\star$ é o sub-reticulado ortogonal de Λ utilizado no processo de decodificação. Neste capítulo, estudamos um método para procurar um sub-reticulado ortogonal de Λ de forma a minimizar $|\Lambda/\Lambda^\star|$. Este método tem alta complexidade como é inerente ao problema de decodificação de reticulados. Além disso, dado o sub-reticulado ortogonal $\Lambda^\star$, construímos o diagrama de treliças para representar o grupo quociente $\Lambda/\Lambda^\star$ de uma forma um pouco diferente do que foi apresentado em [8], onde o diagrama de treliça foi construído a partir de uma base do reticulado Λ. Neste trabalho contruímos tal diagrama a partir de uma base do sub-reticulado ortogonal. Em [30] apresentamos um trabalho sobre a decodificação de códigos de grupo comutativo em dimensões $2n$ via o algoritmo de Viterbi no reticulado associado na dimensão n. No final do capítulo, caracterizamos todos os sub-reticulados ortogonais de um reticulado bidimensional racional [39].

2.1 Decodificação em reticulados via classes

Dado um reticulado Λ, podemos decodificar Λ utilizando a decodificação em qualquer sub-reticulado $\Lambda^\star$ de Λ como descreveremos a seguir [23].

Seja $\Lambda/\Lambda^\star = \{\overline{\boldsymbol{g_i}},\ i = 1, \ldots, |\Lambda/\Lambda^\star|\}$. Temos que

$$\Lambda = \bigcup_{i=1}^{|\Lambda/\Lambda^\star|} \boldsymbol{g}_i + \Lambda^\star, \quad \text{onde} \quad (\boldsymbol{g}_i + \Lambda^\star) \cap (\boldsymbol{g}_j + \Lambda^*) = \emptyset \quad \text{se} \quad i \neq j.$$

Note que os elementos de cada classe $\boldsymbol{g}_i + \Lambda^*$ para $i = 1, \cdots, |\Lambda/\Lambda^\star|$, são obtidos por uma translação do sub-reticulado $\Lambda^\star$ por $\boldsymbol{g}_i$. Seja $\boldsymbol{y} \in \mathbb{R}^n$ um vetor recebido, o processo de decodificação em Λ é feito da seguinte forma:

- Para cada classe $\boldsymbol{g}_i + \Lambda^\star$, faça $\boldsymbol{y}_i = \boldsymbol{y} - \boldsymbol{g}_i$ e decodifique $\boldsymbol{y}_i$ no sub-reticulado $\Lambda^\star$, encontrando o ponto $\boldsymbol{x}_i \in \Lambda^\star$ mais próximo de $\boldsymbol{y}_i$.
- Tomando $\boldsymbol{x}_i^* = \boldsymbol{x}_i + \boldsymbol{g}_i$, este é um ponto da classe $\boldsymbol{g}_i + \Lambda^\star$ mais próximo de $\boldsymbol{y}$.
- Calcule $min\ \{d(\boldsymbol{y}, \boldsymbol{x}_i^*),\ i = 1, \cdots, |\Lambda/\Lambda^\star|\}$ e encontre o vetor do reticulado Λ mais próximo de $\boldsymbol{y}$.

Observação 2.1.1. *Nas condições anteriores, dada uma classe $\boldsymbol{g}_i + \Lambda^*$ e um vetor $\boldsymbol{y}$, se existem $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \Lambda^*$ tais que $d(\boldsymbol{x}_1, \boldsymbol{y} - \boldsymbol{g}_i) = d(\boldsymbol{x}_2, \boldsymbol{y} - \boldsymbol{g}_i)$, então $d(\boldsymbol{x}_1 + \boldsymbol{g}_i, \boldsymbol{y}) = d(\boldsymbol{x}_2 + \boldsymbol{g}_i, \boldsymbol{y})$. Portanto, no caso de existir mais de um vetor no reticulado Λ^* mais próximo de $\boldsymbol{y} - \boldsymbol{g}_i$, então existe mais de um vetor em $\boldsymbol{g}_i + \Lambda^*$ mais próximo de $\boldsymbol{y}$.*

Exemplo 2.1.1. *O reticulado E_8 contém D_8 como sub-reticulado de índice 2. Como D_8 possui um algoritmo conhecido de decodificação, podemos utilizar esse algoritmo para decodificar o reticulado E_8.*

Se o reticulado Λ for ortogonal, o processo de decodificação fica mais simples. De fato, seja Λ um reticulado que possui uma base ortogonal $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$. Dado um vetor recebido $\boldsymbol{y} \in \mathbb{R}^n$, temos que

$$\boldsymbol{y} = \sum_{i=1}^{n} P_{\boldsymbol{v}_i}(\boldsymbol{y})\boldsymbol{v}_i \ \text{ onde } \ P_{\boldsymbol{v}_i}(\boldsymbol{y}) = \frac{\langle \boldsymbol{y}, \boldsymbol{v}_i \rangle}{\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle}.$$

Dado um vetor $\boldsymbol{x} \in \Lambda$, temos que $\boldsymbol{x} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i$ com $a_i \in \mathbb{Z}$ para todo $i = 1, \cdots, n$. Como $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ é ortogonal, temos que

$$d^2(\boldsymbol{y}, \boldsymbol{x}) = \sum_{i=1}^{n} \left| \frac{\langle \boldsymbol{y}, \boldsymbol{v}_i \rangle}{\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle} - a_i \right|^2 \|\boldsymbol{v}_i\|^2,$$

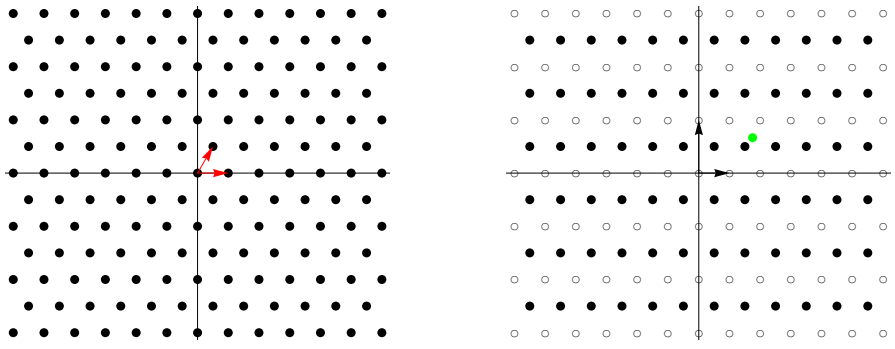
é mínimo quando $a_i = \left[\frac{\langle \boldsymbol{y}, \boldsymbol{v}_i \rangle}{\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle} \right]$, onde $[z]$ denota o inteiro mais próximo de z. Portanto,

$$\boldsymbol{x} = \left[\frac{\langle \boldsymbol{y}, \boldsymbol{v}_1 \rangle}{\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle} \right] \boldsymbol{v}_1 + \cdots + \left[\frac{\langle \boldsymbol{y}, \boldsymbol{v}_n \rangle}{\langle \boldsymbol{v}_n, \boldsymbol{v}_n \rangle} \right] \boldsymbol{v}_n$$

é o ponto de Λ mais próximo de $\boldsymbol{y}$. Note que neste processo de decodificação, só é necessário o uso de projeções e arredondamentos.

Exemplo 2.1.2. *Neste exemplo, mostraremos como decodificar o reticulado hexagonal com base* $\{(1,0), (1/2, \sqrt{3}/2)\}$ *através da decodificação do sub-reticulado ortogonal* $\Lambda^\star$ *com base* $\{(1,0), (0, \sqrt{3})\}$. *Temos que* $\Lambda/\Lambda^\star = \left\{ \overline{(0,0)}, \overline{(1/2, \sqrt{3}/2)} \right\}$.

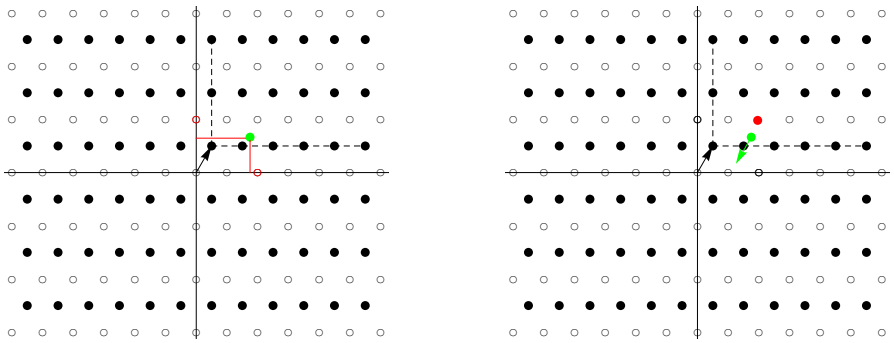
A Figura 2.1 mostra o reticulado hexagonal (figura (a)) e o reticulado hexagonal particionado como duas cópias do sub-reticulado ortogonal $\Lambda^\star$ *(figura (b)). Seja* $\boldsymbol{y}$ *um vetor recebido.*



(a) (b)

Figura 2.1: Reticulado hexagonal

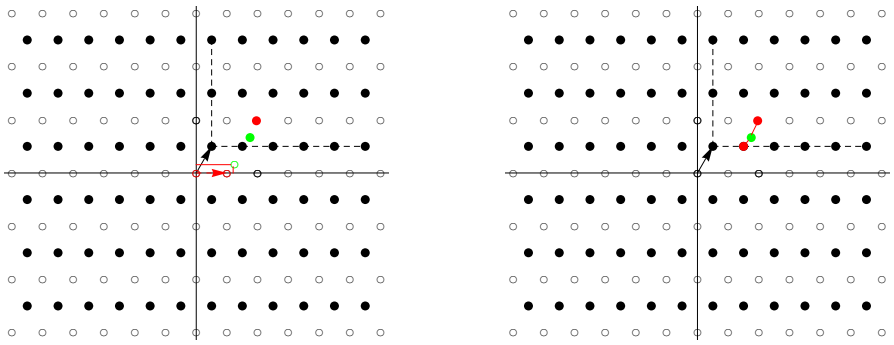
Como na Figura 2.2, o primeiro passo é decodificar $\boldsymbol{y}$ *em* $(0,0) + \Lambda^\star = \Lambda^\star$ *(figura (a)). Em seguida, vamos subtrair de y o vetor* $\boldsymbol{g}_2 = (1/2, \sqrt{3}/2)$ *e decodificar o ponto* $\boldsymbol{y} - \boldsymbol{g}_2$ *em* $\Lambda^\star$ *(figura (b)).*



(a) (b)

Figura 2.2: Reticulado hexagonal

Na Figura 2.3, após encontrar o ponto $\boldsymbol{x}_2$ *de* $\Lambda^\star$ *mais próximo de* $\boldsymbol{y}-\boldsymbol{g}_2$*, fazemos* $\boldsymbol{x}_2+\boldsymbol{g}_2$ *e otemos o ponto da malha preta mais próximo de* $\boldsymbol{y}$*. Finalizamos comparando as distâncias euclidianas entre os dois candidatos (figura (b)).*



(a) (b)

Figura 2.3: Reticulado hexagonal

O algoritmo de Viterbi é utilizado na decodificação de um reticulado usando a decodificação de um sub-reticulado ortogonal. Ele segue a idéia acima, economizando alguns passos como veremos a seguir.

2.2 Diagrama de Treliça

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado e $\Lambda^\star$ um sub-reticulado ortogonal de Λ. O **diagrama de treliça** de Λ em relação à $\Lambda^\star$ é um grafo que tem por objetivo representar o grupo quociente

$\Lambda/\Lambda^\star$.

Observação 2.2.1. *Se Λ é um reticulado de posto n com base $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ e matriz de Gram correspondente $\boldsymbol{G} = (\langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle)_{i,j=1}^n$ com entradas racionais, então Λ possui um sub-reticulado ortogonal $\Lambda^\star$ dado por múltiplos dos vetores de Gram-Schmidt da base. De fato, considere*

$$\hat{\boldsymbol{b}}_{\boldsymbol{1}} = \boldsymbol{b}_1 \quad e \quad \hat{\boldsymbol{b}}_{\boldsymbol{i}} = \boldsymbol{b}_i - \sum_{j=1}^{i-1} \frac{\left\langle \boldsymbol{b}_i, \hat{\boldsymbol{b}}_{\boldsymbol{j}} \right\rangle}{\left\langle \hat{\boldsymbol{b}}_{\boldsymbol{j}}, \hat{\boldsymbol{b}}_{\boldsymbol{j}} \right\rangle} \hat{\boldsymbol{b}}_{\boldsymbol{j}} \quad para \quad i = 2, \cdots, n.$$

Temos que $\left\{\hat{\boldsymbol{b}}_{\boldsymbol{1}}, \cdots, \hat{\boldsymbol{b}}_{\boldsymbol{n}}\right\}$ são ortogonais. Além disso, são obtidos por combinações lineares racionais dos vetores da base do reticulado, pois a matriz de Gram possui todas as entradas racionais. Logo, para cada $\hat{\boldsymbol{b}}_{\boldsymbol{i}}$ existe um número inteiro $\alpha_i \in \mathbb{Z}$ tal que $\alpha_i \hat{\boldsymbol{b}}_{\boldsymbol{i}}$ é escrito como combinação linear inteira dos vetores da base. Como a ortogonalidade é preservada no conjunto $\{\hat{\boldsymbol{b}}_{\boldsymbol{1}}, \alpha_2 \hat{\boldsymbol{b}}_{\boldsymbol{2}}, \cdots, \alpha_n \hat{\boldsymbol{b}}_{\boldsymbol{n}}\}$ e estes vetores pertencem ao reticulado Λ, temos que eles geram um sub-reticulado ortogonal de Λ.

Em [31] o diagrama de treliça foi construído a partir de uma sequência de espaços vetoriais encaixados. Em [8], o diagrama de treliça foi construído partindo de uma base para o reticulado Λ e representando o grupo quociente do reticulado Λ pelo sub-reticulado ortogonal $\Lambda^\star$, onde $\Lambda^\star$ é definido por múltiplos do vetores de Gram-Schmidt da base como na Observação (2.2.1). Foi mostrado em [8], que construir um diagrama de treliça partindo das bases é equivalente à construir diagramas de treliça partindo dos espaços vetoriais. Neste capítulo, a fim de simplificar os cálculos, vamos construir o diagrama de treliça partindo da base do sub-reticulado ortogonal que queremos representar.

O próximo exemplo mostra um reticulado que não possui sub-reticulado ortogonal de mesmo posto.

Exemplo 2.2.1. *Este exemplo mostra um reticulado que não possui sub-reticulado ortogonal. Seja Λ o reticulado com base $\left\{(\sqrt{2}, 0), (\sqrt{3}, 1)\right\}$. Temos que uma matriz de Gram para Λ em relação à esta base é dada por*

$$G = \begin{pmatrix} 2 & \sqrt{6} \\ \sqrt{6} & 4 \end{pmatrix}.$$

Mostremos que este reticulado não possui sub-reticulado ortogonal. Sejam $\boldsymbol{v}_1 = a_1(\sqrt{2}, 0) + a_2(\sqrt{3}, 1)$, $\boldsymbol{v}_2 = b_1(\sqrt{2}, 0) + b_2(\sqrt{3}, 1) \in \Lambda$, com $a_i, b_i \in \mathbb{Z}$ para $i = 1, 2$. Se $\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = 0$,

então teremos $2a_1b_1 + \sqrt{6}a_2b_1 + \sqrt{6}a_1b_2 + 4a_2b_2 = 0$ *e isto implica que* $a_2b_1 + a_1b_2 = 0$ *e* $a_1b_1 + 2a_2b_2 = 0$. *Da primeira equação segue que* $\langle (a_2, a_1), (b_1, b_2) \rangle = 0$, *ou seja, existe* $\lambda \in \mathbb{R}$ *tal que* $(b_1, b_2) = \lambda(-a_1, a_2)$. *Substituindo tais valores na segunda equação temos que* $\lambda(a_1^2 + 2a_2^2) = 0$ *e segue que* $\boldsymbol{v}_1 = \mathbf{0}$ *ou* $\boldsymbol{v}_2 = \mathbf{0}$.

Portanto, temos que não existem dois vetores não nulos ortogonais neste reticulado. Portanto, não existe sub-reticulado ortogonal.

Exemplo 2.2.2. *O reticulado MCC tem matriz de Gram dada por*

$$\frac{1}{2}\begin{pmatrix} 1+\sqrt{2} & -1 & -1 \\ -1 & 1+\sqrt{2} & 1-\sqrt{2} \\ -1 & 1-\sqrt{2} & 1+\sqrt{2} \end{pmatrix}.$$

Um sub-reticulado ortogonal é dado pela base

$$\left\{ \left(2\sqrt{\frac{1}{2}}, 0, 0\right), \left(0, 2\sqrt[4]{\frac{1}{2}}, 0\right), \left(0, 0, -2\sqrt[4]{\frac{1}{2}}\right) \right\}.$$

Portanto, não são apenas reticulados racionais que possuem sub-reticulado ortogonal.

A seguir, vamos trabalhar apenas com reticulados que possuem sub-reticulado ortogonal com o mesmo posto do reticulado, para que a cardinalidade do grupo quociente seja finita. Neste capítulo, estamos interessados em encontrar um sub-reticulado ortogonal $\Lambda^\star$ com base ortogonal $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ que minimiza a cardinalidade do grupo quociente $\Lambda/\Lambda^\star$, que é dada por

$$\left|\frac{\Lambda}{\Lambda^\star}\right| = \frac{det(\Lambda^\star)^{\frac{1}{2}}}{det(\Lambda)^{\frac{1}{2}}} = \frac{\left(\prod_{i=1}^{n} ||\boldsymbol{b}_i||^2\right)^{\frac{1}{2}}}{det(\Lambda)^{\frac{1}{2}}} = \frac{\left(\prod_{i=1}^{n} ||\boldsymbol{b}_i||\right)}{det(\Lambda)^{\frac{1}{2}}},$$

onde $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ é uma base ortogonal do sub-reticulado ortogonal $\Lambda^\star$. Minimizar $|\Lambda/\Lambda^\star|$ é equivalente a minimizar $\prod_{i=1}^{n} ||\boldsymbol{b}_i||$.

Definição 2.2.1. *Dado um reticulado* Λ, *dizemos que um sub-reticulado* $\Lambda^\star$ *é* **mínimo** *em relação à uma base* $\boldsymbol{B} = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ *se os vetores* $\boldsymbol{b}_i$ *são os vetores de menor norma no conjunto* $\Lambda \cap span(\boldsymbol{b}_i)$, *para todo* $i = 1, \cdots, n$, *onde* $span(\boldsymbol{b}_i) = \boldsymbol{b}_i\mathbb{R}$. *Chamamos a base* $\boldsymbol{B}$ *de* **base mínima**.

Dado um sub-reticulado ortogonal mínimo em relação à uma base ortogonal mínima $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$, não estamos interessados nos sub-reticulados ortogonais com base $\{a_1\boldsymbol{b}_1, \cdots, a_n\boldsymbol{b}_n\}$, onde $a_i \in \mathbb{Z}$ e tal que $|a_i| > 1$ para todo $i = 1, \cdots, n$, pois queremos minimizar o produto da norma dos elementos da base. Assim, para cada conjunto de vetores ortogonais do reticulado Λ, queremos os vetores de menor norma possível em cada uma dessas direções.

Observação 2.2.2. *Notemos que dado um reticulado Λ, todas as suas bases são mínimas. De fato, seja $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ uma base de Λ. Sem perda de generalidade, suponhamos que existe um vetor em $\boldsymbol{w}_1$ tal que $\boldsymbol{w}_1 \in \Lambda \cap span(\boldsymbol{v}_1)$ e $||\boldsymbol{w}_1|| < ||\boldsymbol{v}_1||$. Como $\boldsymbol{w}_1 \in \Lambda$, podemos escrever $\boldsymbol{w}_1 = \sum_{i=1}^{n} a_i\boldsymbol{v}_i$ onde $a_i \in \mathbb{Z}$. Agora, temos que $\boldsymbol{w}_1 = \alpha\boldsymbol{v}_1$ para algum $\alpha \in \mathbb{R}$. Assim, temos que $\alpha\boldsymbol{v}_1 = \sum_{i=1}^{n} a_i\boldsymbol{v}_i$, o que implica que existe uma combinação linear não nula dos vetores da base, contradizendo o fato da base ser formada por vetores linearmente independentes sobre $\mathbb{R}$.*

Pelo que foi feito em [8], variando todas as bases do reticulado, consequentemente variamos todos os sub-reticulados ortogonais mínimos, mas só sabemos qual sub-reticulado será representado após calcular o Gram-Schmidt dos vetores da base. A fim de simplificar os cálculos e deixar mais claro o processo de decodificação, neste trabalho, iremos construir o diagrama de treliça partindo de uma base do sub-reticulado ortogonal.

Sejam $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ uma base para Λ e $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ uma base ortogonal mínima para $\Lambda^\star$. Considere os seguintes espaços vetoriais unidimensionais

$$W_i = span\{\boldsymbol{b}_i\} \quad \text{onde} \quad i = 1, \cdots, n.$$

Dados $\boldsymbol{y} \in \mathbb{R}^n$ e $\boldsymbol{x} \in \Lambda$, temos que

$$\boldsymbol{y} = \sum_{i=1}^{n} P_{\boldsymbol{b}_i}(\boldsymbol{y})\boldsymbol{b}_i, \text{ onde } P_{\boldsymbol{b}_i}(\boldsymbol{y}) = \frac{\langle \boldsymbol{y}, \boldsymbol{b}_i \rangle}{\langle \boldsymbol{b}_i, \boldsymbol{b}_i \rangle} \text{ e}$$

$$\boldsymbol{x} = \sum_{i=1}^{n} P_{\boldsymbol{b}_i}(\boldsymbol{x})\boldsymbol{b}_i, \text{ onde } P_{\boldsymbol{b}_i}(\boldsymbol{x}) = \frac{\langle \boldsymbol{x}, \boldsymbol{b}_i \rangle}{\langle \boldsymbol{b}_i, \boldsymbol{b}_i \rangle}.$$

Assim, como $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ é um conjunto ortogonal, segue que

$$d^2(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} |P_{\boldsymbol{b}_i}(\boldsymbol{x}) - P_{\boldsymbol{b}_i}(\boldsymbol{y})|^2 ||\boldsymbol{b}_i||^2.$$

Para cada classe do grupo quociente $\Lambda/\Lambda^\star$, iremos procurar pelo elemento $\boldsymbol{x}$ que minimiza $d(\boldsymbol{x}, \boldsymbol{y})$. Para isto, devemos estudar as projeções nas direções dos vetores da base do sub-reticulado ortogonal.

O exemplo seguinte, mostra que quando projetamos duas classes distintas do quociente $\Lambda/\Lambda^\star$ na mesma direção, a projeção pode ser igual e isso será considerado na construção do diagrama de treliça.

Exemplo 2.2.3. *Considere o reticulado hexagonal com o sub-reticulado* $\Lambda^\star$ *dado pela base* $\left\{(1,0),(0,2\sqrt{3})\right\}$ *e representado pela malha preta na figura abaixo. Temos uma partição do reticulado* Λ *em* 4 *cópias do sub-reticulado* $\Lambda^\star$.

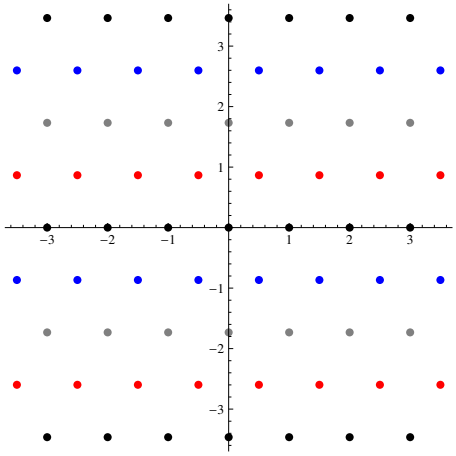


Figura 2.4: Reticulado hexagonal

Note que quando fazemos projeções das malhas vermelha e azul na direção do vetor $(1,0)$, *obtemos o mesmo resultado. O mesmo vale para as malhas cinza e preta.*

Para saber quando a projeção de duas classes numa mesma direção coincide, considere os seguintes reticulados

$$\Lambda_{W_i} = \Lambda \cap W_i = \boldsymbol{b}_i\mathbb{Z} \quad \text{para} \quad i = 1, \cdots, n$$

e as projeções

$$P_{\boldsymbol{b}_i}(\Lambda) \quad \text{para} \quad i = 1, \cdots, n$$

na direção dos vetores da base de $\Lambda^\star$.

Como $\Lambda_{W_i} \subset P_{\boldsymbol{b}_i}(\Lambda)$ para todo $i = 1, \cdots, n$, definimos os grupos quocientes

$$G_i = \frac{P_{\boldsymbol{b}_i}(\Lambda)}{\Lambda_{W_i}},\ i = 1, \cdots, n.$$

A cardinalidade de G_i representa o número de diferentes projeções na direção de $\boldsymbol{b}_i$ para $i = 1, \cdots, n$.

Observação 2.2.3. *Sejam $\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}} \in \Lambda/\Lambda^\star$. Se $\overline{\boldsymbol{x}} = \overline{\boldsymbol{y}}$, então $P_{\boldsymbol{b}_i}(\boldsymbol{x}) + \Lambda_{W_i} = P_{\boldsymbol{b}_i}(\boldsymbol{y}) + \Lambda_{W_i}$ para todo $i = 1, \cdots, n$. De fato, se $\overline{\boldsymbol{x}} = \overline{\boldsymbol{y}}$, então $\boldsymbol{x} - \boldsymbol{y} \in \Lambda^\star = \Lambda_{W_1} \oplus \cdots \oplus \Lambda_{W_n}$, o que implica que $P_{\boldsymbol{b}_i}(\boldsymbol{x} - \boldsymbol{y}) \in \Lambda_{W_i}$ e, assim, $\overline{P_{\boldsymbol{b}_i}(\boldsymbol{x})} = \overline{P_{\boldsymbol{b}_i}(\boldsymbol{y})}$ para $i = 1, \cdots, n$. Com isso, temos que cada classe de $\Lambda/\Lambda^\star$ gera um único elemento em G_i. Mas, como veremos depois, duas classes distintas em $\Lambda/\Lambda^\star$ podem gerar o mesmo elemento em G_i para alguns valores de i.*

Fixada uma classe $\overline{\boldsymbol{x}} \in \Lambda/\Lambda^\star$, temos que as projeções de tal classe na direção dos vetores $\boldsymbol{b}_i$ são representadas pela sequência

$$g(\boldsymbol{x}) = (g_1(\boldsymbol{x}), \cdots, g_n(\boldsymbol{x})),\ \text{onde } g_i(\boldsymbol{x}) = P_{\boldsymbol{b}_i}(\boldsymbol{x}) + \Lambda_{W_i},\ i = 1, \cdots, n,\ \boldsymbol{x} \in \Lambda.$$

O conjunto das possíveis projeções dentre todas as classes é dado por $G = \{g(\boldsymbol{x}), \boldsymbol{x} \in \Lambda\}$.

Para cada classe $\overline{\boldsymbol{x}}$ do quociente $\Lambda/\Lambda^\star$, calculamos a sequência $g(\boldsymbol{x})$ e através das relações entre todas as possíveis sequências obtidas variando as classes, construímos o diagrama de treliça. Note que cada entrada i de uma sequência $g(\boldsymbol{x})$ equivale a um elemento de G_i. O diagrama de treliça é construído da seguinte forma [8]:

- Inicie com um ponto S_0 ligando a ele $|G_1|$ arestas.
- Rotule cada uma destas arestas por um elemento de G_1.
- No final de cada uma destas arestas coloque um nó S_{1i}, para $i = 1, \cdots, |G_1|$ e vá para o nível 2.
- Passando ao nível 2, para cada uma dessas arestas identificadas com um elemento de G_1, procure no conjunto G as sequências com esse elemento na primeira entrada. A cada sequência encontrada trace uma aresta ligada à primeira por um nó e identifique-a pelo elemento de G_2 que aparece na segunda entrada da sequência. Finalize o nível 2 colocando em cada aresta um nó S_{2i}.

- Repita o mesmo procedimento no nível 3 procurando por sequências em G cujos dois primeiros elementos sejam os elementos rotulados nas duas sequências anteriores. Se existirem duas sequências com o terceiro elemento igual, ligue os dois nós da segunda aresta em um único nó, entrelaçando os caminhos.

- Continue a preencher os caminhos até o nível n e junte todas as arestas em um único nó S_n.

O exemplo seguinte, mostra passo a passo como construir um diagrama de treliça para o reticulado hexagonal.

Exemplo 2.2.4. *Vamos construir o diagrama de treliça do reticulado hexagonal em relação ao sub-reticulado ortogonal com base* $\{\boldsymbol{b}_1 = (1,0), \boldsymbol{b}_2 = (0,\sqrt{3})\}$ *dado pela Figura 2.5. Temos que tal sub-reticulado, representado pelos pontos vermelhos, particiona o reticulado hexagonal em duas classes distintas. Considere* $W_1 = span(\boldsymbol{b}_1)$ *e* $W_2 = span(\boldsymbol{b}_2)$. *Temos que* $\Lambda_{W_1} = (1,0)\mathbb{Z}$ *e* $\Lambda_{W_2} = (0,\sqrt{3})\mathbb{Z}$. *Para as projeções temos que* $P_{\boldsymbol{b}_1}(\Lambda) = (1/2,0)\mathbb{Z}$ *e* $P_{\boldsymbol{b}_2}(\Lambda) = (0,\sqrt{3}/2)\mathbb{Z}$.

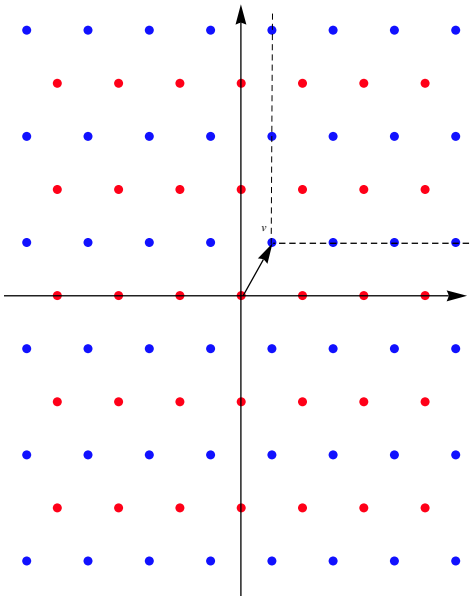


Figura 2.5: Reticulado hexagonal

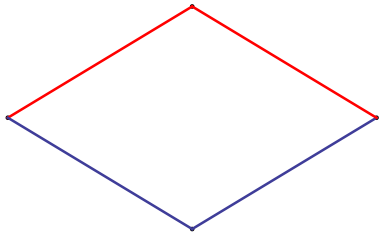
Com isso, segue que

$$G_1 = \frac{(1/2,0)\mathbb{Z}}{(1,0)\mathbb{Z}} = \left\{\overline{(0,0)}, \overline{(1/2,0)}\right\} \simeq \mathbb{Z}_2 \quad e \quad G_2 = \frac{(0,\sqrt{3}/2)\mathbb{Z}}{(0,\sqrt{3})\mathbb{Z}} = \left\{\overline{(0,0)}, \overline{(0,\sqrt{3}/2)}\right\} \simeq \mathbb{Z}_2.$$

Agora vamos calcular o conjunto de sequências G. Temos duas classes no grupo quociente $\Lambda/\Lambda^\star$ dadas por $\left\{\overline{(0,0)}, \overline{(1/2,\sqrt{3}/2)}\right\}$. Então

$$g(0,0) = ((0,0)+\Lambda_{w_1}, (0,0)+\Lambda_{w_2}) \text{ e } g(1/2,\sqrt{3}/2) = ((1/2,0)+\Lambda_{W_1}, (0,\sqrt{3}/2)+\Lambda_{W_2}).$$

Assim, temos $G = \left\{g(0,0), g(1/2,\sqrt{3}/2)\right\}$ e vamos construir o diagrama de treliça. Partindo de um nó inicial S_0, devemos colocar 2 arestas, cada uma representando um elemento de G_1. A primeira aresta vamos rotular pelo elemento $(0,0)+\Lambda_{W_1}$ e esta será ligada à aresta $(0,0)+\Lambda_{W_2}$ que representam a sequência $g(0,0)$. A aresta rotulada por $(1/2,0)+\Lambda_{W_1}$ será ligada à aresta $(0,\sqrt{3}/2)+\Lambda_{W_2}$ representando a sequência $g(1/2,\sqrt{3}/2)$. Por fim, tais arestas são ligadas em um único nó, como mostra o seguinte diagrama, onde o caminho vermelho representa a sequência $g(0,0)$ e, o azul, a sequência $g(1/2,\sqrt{3}/2)$.



É possível explicitar as projeções $P_{\boldsymbol{b}_i}(\Lambda)$. Seja $\boldsymbol{M}$ a matriz geradora para o reticulado Λ em relação à base $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ e $\boldsymbol{N}$ a matriz geradora do sub-reticulado ortogonal $\Lambda^\star$ em relação à base ortogonal $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$. Temos que existe uma matriz $\boldsymbol{A} = (a_{ij})$ com entradas inteiras tal que $\boldsymbol{N} = \boldsymbol{A}\boldsymbol{M}$, ou seja, $\boldsymbol{M} = \boldsymbol{A}^{-1}\boldsymbol{N}$. Assim, segue que

$$\boldsymbol{v}_i = c_{i1}\boldsymbol{b}_1 + \cdots + c_{in}\boldsymbol{b}_n \text{ para todo } i = 1, \cdots, n$$

com c_{ij} elementos da matriz $\boldsymbol{A}^{-1}$ para todo $1 \leq i, j \leq n$.

Dado um elemento $\boldsymbol{v} \in \Lambda$, existem $\alpha_i \in \mathbb{Z}$ para $i = 1, \cdots, n$ tais que

$$\boldsymbol{v} = \alpha_1\boldsymbol{v}_1 + \cdots + \alpha_n\boldsymbol{v}_n = (\alpha_1 c_{11} + \cdots + \alpha_n c_{n1})\boldsymbol{b}_1 + \cdots + (\alpha_1 c_{1n} + \cdots + \alpha_n c_{nn})\boldsymbol{b}_n.$$

Assim, segue que $P_{\boldsymbol{b}_i}(\boldsymbol{v}) = (\alpha_1 c_{1i} + \cdots + \alpha_n c_{ni})\boldsymbol{b}_i$ para todo $i = 1, \cdots, n$ e

$$P_{\boldsymbol{b}_i}(\Lambda) = (c_{1i}\mathbb{Z} + \cdots + c_{ni}\mathbb{Z})\boldsymbol{b}_i.$$

Agora, se $\eta_i = min\{|c_{1i}z_1 + \cdots + c_{ni}z_n|; \quad 0 \neq (z_1, \cdots, z_n) \in \mathbb{Z}^n\}$, temos que

$$P_{\boldsymbol{b}_i}(\Lambda) = \eta_i \boldsymbol{b}_i \mathbb{Z}.$$

Lema 2.2.1. *[8] Se $f(\boldsymbol{x}) = a_1x_1 + \cdots + a_nx_n$ com $a_i, x_i \in \mathbb{Z}$ para todo $i = 1, \cdots, n$, então o mínimo de $|f(\boldsymbol{x})|$ sobre todo $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$ não nulo é igual a $mdc(a_1, \cdots, a_n)$.* □

Proposição 2.2.1. *Temos que*

$$\eta_i = \frac{mdc(M_i c_{1i}, \cdots, M_i c_{ni})}{M_i},$$

onde M_i é o mínimo múltiplo comum dos denominadores de c_{ij}, onde $j = 1, \cdots, n$.

Demonstração: Basta notar que $M_i c_{ij} \in \mathbb{Z}$ para todo i, j. Além disso, temos $min\{|c_{1i}z_1 + \cdots + c_{ni}z_n|, \ 0 \neq (z_1, \cdots, z_n) \in \mathbb{Z}^n\} = \frac{1}{M_i} min\{|M_i c_{1i}z_1 + \cdots + M_i c_{ni}z_n|, \ 0 \neq (z_1, \cdots, z_n) \in \mathbb{Z}^n\}$. Usando o Lema 2.2.1, chegamos ao resultado. □

Com isso, temos que

$$G_i(\Lambda) = \frac{P_{\boldsymbol{b}_i}(\Lambda)}{\Lambda_{W_i}} = \frac{\eta_i \boldsymbol{b}_i \mathbb{Z}}{\boldsymbol{b}_i \mathbb{Z}} \quad \text{para} \quad i = 1, \cdots, n \quad \text{e} \quad |G_i| = \frac{1}{\eta_i}.$$

Para construir o diagrama de treliça, precisamos saber quais são os elementos do grupo quociente $\Lambda/\Lambda^\star$. Para isso, usaremos o resultado provado em [1] que usando a forma normal de Smith caracteriza um conjunto de geradores para o grupo quociente $\Lambda/\Lambda^\star$.

Definição 2.2.2. *Dizemos que uma matriz $\boldsymbol{B}$ de ordem $n \times n$ está na* **forma normal de Smith** *se $\boldsymbol{B}$ é uma matriz diagonal com coeficientes inteiros não negativos tal que $b_{i,i}|b_{i+1,i+1}$ para todo $i < n$.*

Teorema 2.2.1. *[21] Se $\boldsymbol{A}$ é uma matriz $n \times n$, com coeficientes em um domínio de ideais principais R e determinante não nulo, então existe uma única matriz $\boldsymbol{D}$ na forma normal de Smith tal que $\boldsymbol{D} = \boldsymbol{PAQ}$, com $\boldsymbol{P}$ e $\boldsymbol{Q}$ matrizes unimodulares em R.*

Teorema 2.2.2. *[1] Sejam Λ um reticulado com matriz geradora $\boldsymbol{M}$ e $\Lambda^\star$ um sub-reticulado com matriz geradora $\boldsymbol{N}$. Se $\boldsymbol{A} = (a_{ij})$, $a_{i,j} \in \mathbb{Z}$, é a matriz tal que $\boldsymbol{N} = \boldsymbol{AM}$, então os geradores do grupo quociente $\Lambda/\Lambda^\star$ são as linhas $\boldsymbol{h}_j$ da matriz $\boldsymbol{Q}^{-1}\boldsymbol{M}$ para $d_j \neq 1$ onde $\boldsymbol{A} = \boldsymbol{P}^{-1}\boldsymbol{D}\boldsymbol{Q}^{-1}$ é a decomposição de Smith da matriz $\boldsymbol{A}$ e d_j são elementos da diagonal da matriz $\boldsymbol{D}$.* □

Exemplo 2.2.5. *Considere o reticulado com base $\boldsymbol{v}_1 = (1, 0, -1)$, $\boldsymbol{v}_2 = (2, 1, 0)$ e $\boldsymbol{v}_3 = (0, 1, 1)$ e o sub-reticulado ortogonal com base $\boldsymbol{b}_1 = (1, 0, -1)$, $\boldsymbol{b}_2 = (1, 1, 1)$ e $\boldsymbol{b}_3 = (-1, 2, -1)$. Temos que as bases estão relacionadas por*

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & 1 \\ -1 & 2 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 7 & -4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Fazendo a decomposição de Smith em $\boldsymbol{A}$, temos que

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 7 & -4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Assim, temos $\boldsymbol{Q}^{-1}\boldsymbol{M} = \boldsymbol{M}$ e os elementos do grupo quociente $\Lambda/\Lambda^\star$ são dados por

$$\Lambda/\Lambda^\star = \left\{ a\overline{(0,1,1)}, a = 0, 1, \cdots, 5 \right\} = \left\{ \overline{(0,0,0)}, \overline{(0,1,1)}, \overline{(0,2,2)}, \overline{(0,3,3)}, \overline{(0,4,4)}, \overline{(0,5,5)} \right\}.$$

Dessa forma, obtemos

$$\Lambda_{W_1} = (1, 0, -1)\mathbb{Z}, \;\; \Lambda_{W_2} = (1, 1, 1)\mathbb{Z} \quad e \quad \Lambda_{W_3} = (-1, 2, -1)\mathbb{Z}.$$

Para as projeções, temos

$$\boldsymbol{A}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -1/2 & 2/3 & 1/6 \end{pmatrix},$$

$$P_{\boldsymbol{b}_1}(\Lambda) = 1/2(1, 0, 1)\mathbb{Z}, \;\; P_{\boldsymbol{b}_2}(\Lambda) = 1/3(1, 1, 1)\mathbb{Z} \quad e \quad P_{\boldsymbol{b}_3}(\Lambda) = 1/6(-1, 2, -1)\mathbb{Z}.$$

Vamos calcular o conjunto G :

$$1 \Longrightarrow g(0,0,0) = ((0,0,0) + \Lambda_{W_1}, (0,0,0) + \Lambda_{W_2}, (0,0,0) + \Lambda_{W_3})$$

$$2 \Longrightarrow g(0,1,1) = ((-1/2,0,1/2) + \Lambda_{W_1}, (2/3,2/3,2/3) + \Lambda_{W_2}, (-1/6,2/6,-1/6) + \Lambda_{W_3})$$
$$= ((-1/2,0,1/2) + \Lambda_{W_1}, (0,0,0) + \Lambda_{W_2}, (-1/6,2/6,1/6) + \Lambda_{W_3})$$

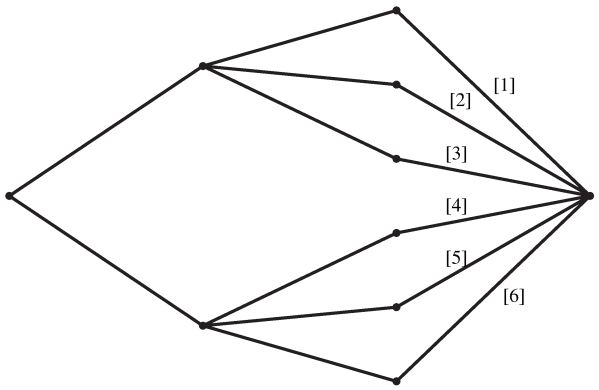
$$3 \Longrightarrow g(0,2,2) = ((-1,0,1) + \Lambda_{W_1}, (4/3,4/3,4/3) + \Lambda_{W_2}, (-2/6,4/6,-1/6) + \Lambda_{W_3})$$
$$= ((0,0,0) + \Lambda_{W_1}, (4/3,4/3,4/3) + \Lambda_{W_2}, (-2/6,4/5,-2/6) + \Lambda_{W_3})$$

$$4 \Longrightarrow g(0,3,3) = ((-3/2,0,3/2) + \Lambda_{W_1}, (2,2,2) + \Lambda_{W_2}, (-3/6,1,-3/6) + \Lambda_{W_3})$$
$$= ((-1/2,0,1/2) + \Lambda_{W_1}, (0,0,0) + \Lambda_{W_2}, (-3/6,1,-3/6) + \Lambda_{W_3})$$

$$5 \Longrightarrow g(0,4,4) = ((-2,0,2) + \Lambda_{W_1}, (8/3,8/3,8/3) + \Lambda_{W_2}, (-4/6,8/6,-4/6) + \Lambda_{W_3})$$
$$= ((0,0,0) + \Lambda_{W_1}, (2/3,2/3,2/3) + \Lambda_{W_2}, (-4/6,8/6,-4/6) + \Lambda_{W_3})$$

$$6 \Longrightarrow g(0,5,5) = ((-5/2,0,5/2) + \Lambda_{W_1}, (10/3,10/3,10/3) + \Lambda_{W_2}, (-5/6,10/6,-5/6) + \Lambda_{W_3})$$
$$= ((-1/2,0,1/2) + \Lambda_{W_1}, (4/3,4/3,4/3) + \Lambda_{W_2}, (-5/6,10/6,-5/6) + \Lambda_{W_3})$$

O diagrama de treliça representando o grupo quociente $\Lambda/\Lambda^\star$ *é dado por*



Exemplo 2.2.6. *O reticulado MCC tem como base* $\boldsymbol{v}_1 = \left(\sqrt{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}, 0\right)$, $\boldsymbol{v}_2 = \left(\sqrt{\frac{1}{2}}, 0, \sqrt[4]{\frac{1}{2}}\right)$ *e* $\boldsymbol{v}_3 = \left(0, \sqrt[4]{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}\right)$. *Considere o sub-reticulado ortogonal com base* $\boldsymbol{b}_1 = \left(2\sqrt{\frac{1}{2}}, 0, 0\right)$, $\boldsymbol{b}_2 = \left(0, 2\sqrt[4]{\frac{1}{2}}, 0\right)$ *e* $\boldsymbol{b}_3 = \left(0, 0, -2\sqrt[4]{\frac{1}{2}}\right)$, *temos que*

$$\begin{pmatrix} 2\sqrt{\frac{1}{2}} & 0 & 0 \\ 0 & 2\sqrt[4]{\frac{1}{2}} & 0 \\ 0 & 0 & -2\sqrt[4]{\frac{1}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} \sqrt{\frac{1}{2}} & \sqrt[4]{\frac{1}{2}} & 0 \\ \sqrt{\frac{1}{2}} & 0 & \sqrt[4]{\frac{1}{2}} \\ 0 & \sqrt[4]{\frac{1}{2}} & \sqrt[4]{\frac{1}{2}} \end{pmatrix}.$$

Fazendo a decomposição de Smith em $\boldsymbol{A}$ *obtemos*

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

que implica que

$$\boldsymbol{Q}^{-1}\boldsymbol{M} = \begin{pmatrix} \sqrt{2} & \sqrt[4]{2^3} & \sqrt[4]{2^3} \\ \sqrt{\frac{1}{2}} & 0 & \sqrt[4]{\frac{1}{2}} \\ 0 & \sqrt[4]{\frac{1}{2}} & \sqrt[4]{\frac{1}{2}} \end{pmatrix}.$$

Os elementos do grupo quociente $\Lambda/\Lambda^\star$ *são dados por*

$$\left\{ \overline{(0,0,0)}, \overline{\left(0, \sqrt[4]{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}\right)}, \overline{\left(\sqrt{\frac{1}{2}}, 0, \sqrt[4]{\frac{1}{2}}\right)}, \overline{\left(\sqrt{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}, 2\sqrt[4]{\frac{1}{2}}\right)} \right\}.$$

Temos que

$$\Lambda_{W_1} = \left(2\sqrt{\frac{1}{2}}, 0, 0\right)\mathbb{Z},\ \Lambda_{W_2} = \left(0, 2\sqrt[4]{\frac{1}{2}}, 0\right)\mathbb{Z} \text{ e } \Lambda_{W_3} = \left(0, 0, -2\sqrt[4]{\frac{1}{2}}\right)\mathbb{Z}.$$

Como

$$\boldsymbol{A}^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix},$$

temos para as projeções

$$P_{\boldsymbol{b}_1}(\Lambda) = 1/2\left(2\sqrt{\frac{1}{2}}, 0, 0\right)\mathbb{Z},\ P_{\boldsymbol{b}_2}(\Lambda) = \frac{1}{2}\left(0, 2\sqrt[4]{\frac{1}{2}}, 0\right)\mathbb{Z} \text{ e } P_{\boldsymbol{b}_3}(\Lambda) = \frac{1}{2}\left(0, 0, -2\sqrt[4]{\frac{1}{2}}\right)\mathbb{Z}.$$

Assim, segue que G é dado por

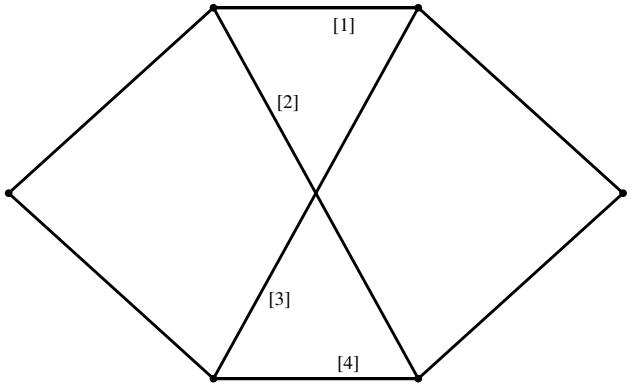
$$1 \Longrightarrow (\mathbf{0} + \boldsymbol{b}_1\mathbb{Z}, \mathbf{0} + \boldsymbol{b}_2\mathbb{Z}, \mathbf{0} + \boldsymbol{b}_3\mathbb{Z})$$

$$2 \Longrightarrow (\mathbf{0} + \boldsymbol{b}_1\mathbb{Z}, 1/2\boldsymbol{b}_2 + \boldsymbol{b}_2\mathbb{Z}, 1/2\boldsymbol{b}_3 + \boldsymbol{b}_3\mathbb{Z})$$

$$3 \Longrightarrow (1/2\boldsymbol{b}_1 + \boldsymbol{b}_1\mathbb{Z}, 1/2\boldsymbol{b}_2 + \boldsymbol{b}_2\mathbb{Z}, \mathbf{0} + \boldsymbol{b}_3\mathbb{Z})$$

$$4 \Longrightarrow (1/2\boldsymbol{b}_1 + \boldsymbol{b}_1\mathbb{Z}, \mathbf{0} + \boldsymbol{b}_2\mathbb{Z}, 1/2\boldsymbol{b}_3 + \boldsymbol{b}_3\mathbb{Z})$$

A treliça associada ao quociente $\Lambda/\Lambda^\star$ é dada por



Observação 2.2.4. *[8] Considere os espaços vetoriais i-dimensionais*

$$V_0 = \{0\}, \;\; V_i = span\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i\},$$

os reticulados

$$\Lambda_{V_i} = \Lambda \cap V_i \; para \;\; i = 0, 1, \cdots, n$$

e as projeções $P_{V_i}(\Lambda)$ para $i = 0, 1, \cdots, n$.

Os nós em cada nível i representam elementos do grupo quociente

$$\Sigma_i = \frac{P_{V_i}(\Lambda)}{\Lambda_{V_i}}, \;\; i = 0, 1, \cdots, n.$$

Isto se deve ao fato que

$$\Sigma_i = \frac{P_{V_i}(\Lambda)}{\Lambda_{V_i}} = \frac{P_{W_1}(\Lambda) \oplus \cdots \oplus P_{W_i}(\Lambda)}{\Lambda_{W_1} \oplus \cdots \oplus \Lambda_{W_i}}.$$

O conjunto de sequências

$$\Sigma = \{(\sigma_0(\boldsymbol{x}), \sigma_1(\boldsymbol{x}), \cdots, \sigma_n(\boldsymbol{x})),\ \textit{onde}\ \sigma_i(\boldsymbol{x}) = P_{V_i}(\boldsymbol{x}) + \Lambda_{V_i},\ \boldsymbol{x} \in \Lambda/\Lambda^\star\}$$

é o conjunto dos caminhos na treliça que passa pelos nós.

Observação 2.2.5. *É importante lembrar que cada caminho na treliça representa uma classe do grupo quociente* $\Lambda/\Lambda^\star$.

Estamos considerando como medida de complexidade de uma treliça o número de caminhos na treliça, ou seja, a cardinalidade do grupo quociente $|\Lambda/\Lambda^\star|$. Notemos que se para dois sub-reticulados distintos $\Lambda^\star, \Lambda^\diamond$ tivermos $|\Lambda/\Lambda^\star| = |\Lambda/\Lambda^\diamond|$, então a treliça menos complexa é aquela que possui o menor número de nós, pois com isso os caminhos têm partes em comum e como veremos depois, isso será útil na aplicação do algoritmo de Viterbi. No nosso estudo, apenas consideramos a cardinalidade do quociente $|\Lambda/\Lambda^\star|$ como uma medida de complexidade.

2.3 Algoritmo de Viterbi

Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto n, $\Lambda^\star$ um sub-reticulado ortogonal com treliça T associada ao grupo quociente $\Lambda/\Lambda^\star$ e $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ uma base ortogonal mínima para $\Lambda^\star$. Seja $\boldsymbol{y} \in \mathbb{R}^n$ com $\boldsymbol{y} = \sum_{i=1}^n y_i \boldsymbol{b}_i$ onde $y_i \in \mathbb{R}$.

Lembrando que $\Lambda_{W_i} = \boldsymbol{b}_i\mathbb{Z}$, note que podemos escrever

$$G_i = \left\{ z_j \eta_i \boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z},\ \ z_j \in \mathbb{Z}\ \ 1 \leq z_j \leq \frac{1}{\eta_i} \right\}.$$

Para cada classe em G_i encontramos o representante da classe com a menor distância euclidiana de $y_i\boldsymbol{b}_i$. Isto é, fixados i, j e tomando $a_{ij} = \eta_i z_j$, encontramos na classe $a_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z} \in G_i$ um representante $c_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z}$ tal que $||c_{ij}\boldsymbol{b}_i - y_i\boldsymbol{b}_i||^2$ seja a menor possível.

Temos que $a_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z} = b\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z}$ se, e somente se, $(b - a_{ij})\boldsymbol{b}_i \in \boldsymbol{b}_i\mathbb{Z}$, o que equivale a $b = a_{ij} + z$ para algum $z \in \mathbb{Z}$. Agora, $||y_i\boldsymbol{b}_i - b\boldsymbol{b}_i||^2 = ||y_i\boldsymbol{b}_i - (a_{ij}+z)\boldsymbol{b}_i||^2 = |(y_i - a_{ij}) - z|^2||\boldsymbol{b}_i||^2$. Este valor será mínimo se $z = [y_i - a_{ij}]$. Assim, $c_{ij} = a_{ij} + [y_i - a_{ij}]$ é tal que $a_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z} = c_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z}$ e $||c_{ij}\boldsymbol{b}_i - y_i\boldsymbol{b}_i||^2$ é a menor possível.

Para cada classe $a_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z} = c_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z}$, associamos o valor

$$d_{ij} = ||y_i\boldsymbol{b}_i - c_{ij}\boldsymbol{b}_i||^2 = |(y_i - a_{ij}) - [y_i - a_{ij}]|^2||\boldsymbol{b}_i||^2$$

que corresponde a menor distância da projeção da classe $a_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z}$ à projeção de $\boldsymbol{y}$ na direção de $\boldsymbol{b}_i$.

Algoritmo de Viterbi

- **Passo 1**: Calcule d_{ij} para todo i e todo j e identifique no segmento da treliça representando por $a_{ij}\boldsymbol{b}_i + \boldsymbol{b}_i\mathbb{Z} \in G_i$ o valor d_{ij}.

- **Passo 2**: Rotule os nós no nível 2 por $S_{2t} \in \Sigma_2(\Lambda)$. Fixado um deste nós S_{2t}, selecione todos os caminhos que saem de S_0 e chegam até S_{2t}. Para cada um destes caminhos some as distâncias associadas. Calcule o mínimo entre todas as somas obtidas para caminhos diferentes. Guarde apenas o caminho cuja soma das distâncias é mínima e descarte os demais caminhos. Faça isso para todo $t = 1, \cdots, |\sum_2|$, ficando com apenas um caminho ligando S_0 a S_{2t} para cada t.

- **Passo 3**: Para cada nó $S_{3t} \in \sum_3$ selecione todos os caminhos que partem de S_0 e chegam a S_{3t}. Nesta seleção devem ser excluídos os caminhos que foram desconsiderados no nível 2. Calcule o mínimo entre todas as somas obtidas. Guarde apenas o caminho cuja soma das distâncias é mínima e descarte os demais.

- **Passo 4**: Repita o mesmo procedimento em cada nível até encontrar um único caminho que sai de S_0 e vai até S_n.

O caminho final resultante representa a classe do grupo quociente $\Lambda/\Lambda^\star$ que tem o representante mais próximo de $\boldsymbol{y}$. Tal elemento é dado por

$$\boldsymbol{x}^* = c_{1j_1}\boldsymbol{b}_1 + \cdots + c_{nj_n}\boldsymbol{b}_n.$$

Exemplo 2.3.1. *Considere reticulado MCC do Exemplo 2.2.6 e seu sub-reticulado ortogonal com base* $\boldsymbol{b}_1 = \left(2\sqrt{\frac{1}{2}}, 0, 0\right)$, $\boldsymbol{b}_2 = \left(0, 2\sqrt[4]{\frac{1}{2}}, 0\right)$ *e* $\boldsymbol{b}_3 = \left(0, 0, -2\sqrt[4]{\frac{1}{2}}\right)$. *Dado* $\boldsymbol{y} = (1, 1, 0)$ *um*

vetor, temos que

$$\boldsymbol{y} = \sqrt{\frac{1}{2}}\boldsymbol{b}_1 + \frac{\sqrt[4]{\frac{1}{2}}}{2\sqrt{2}}\boldsymbol{b}_2 + 0\boldsymbol{b}_3.$$

Como

$$G_1 = \{0 + \boldsymbol{b}_1\mathbb{Z}, 1/2\boldsymbol{b}_1 + \boldsymbol{b}_1\mathbb{Z}\}$$

$$G_2 = \{0 + \boldsymbol{b}_2\mathbb{Z}, 1/2\boldsymbol{b}_2 + \boldsymbol{b}_2\mathbb{Z}\}$$

$$G_3 = \{0 + \boldsymbol{b}_3\mathbb{Z}, 1/2\boldsymbol{b}_3 + \boldsymbol{b}_3\mathbb{Z}\}$$

segue que

$$d_{11} = 0.1715, d_{12} = 0.0857, d_{21} = 0.4648, d_{22} = 0.0253, d_{31} = 0, d_{32} = 0.7071$$

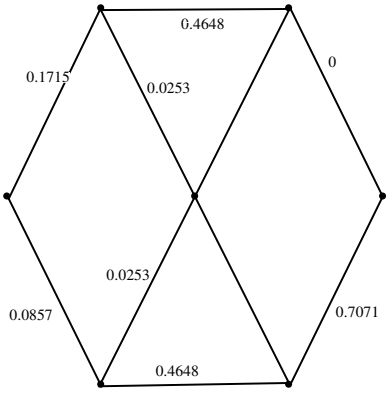
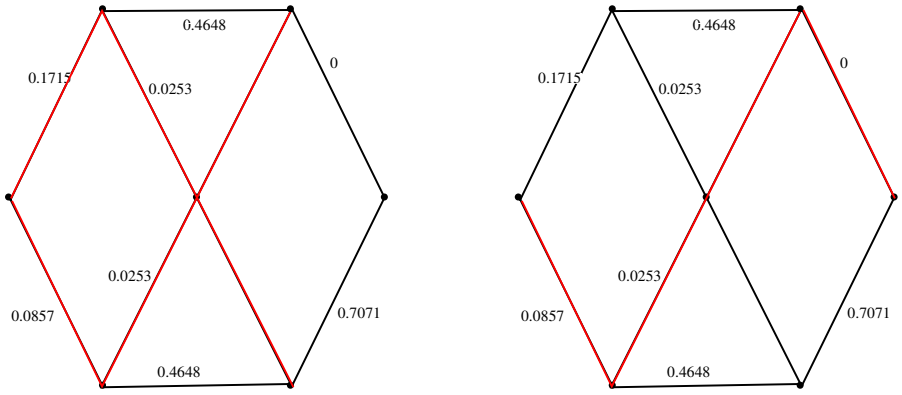


Figura 2.6: $\boldsymbol{y} = (1, 1, 0)$

Olhando para cada nó no nível 2, escolhemos os caminhos com a menor soma de distâncias
Entre os dois caminhos restantes, no nível 3 resta apenas 1 caminho.
O ponto do reticulado MCC mais próximo de $\boldsymbol{y}$ *é* $\boldsymbol{x} = \left(\sqrt{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}, 0\right)$.



(a) (b)

Figura 2.7: $\boldsymbol{y} = (1, 1, 0)$

2.4 Busca de sub-reticulado ortogonal

Nesta seção, descreveremos o método que derivamos para procurar um sub-reticulado ortogonal $\Lambda^\star$ de um reticulado Λ a fim de minimizar a cardinalidade do grupo quociente $\Lambda/\Lambda^\star$. Tal método pode ser utilizado na decodificação de códigos de grupo comutativo, pois estes sempre possuem sub-reticulado ortogonal [30].

Para iniciar o algoritmo é necessário conhecer um sub-reticulado ortogonal $\Lambda^\diamond \subseteq \Lambda$ tal que $|\Lambda/\Lambda^\diamond| = \boldsymbol{M} < \infty$. Usaremos $\boldsymbol{M}$ como limitante superior para a busca. É interessante partir do menor $\boldsymbol{M}$ possível. Se a matriz de Gram do reticulado possui todas as entradas racionais, é fácil encontrar um sub-reticulado ortogonal através do Gram-Schmidt da base como vimos na Observação (2.2.1).

Estamos em busca de um sub-reticulado ortogonal $\Lambda^\star$ tal que $|\Lambda/\Lambda^\star| = \frac{det(\Lambda^\star)^{\frac{1}{2}}}{det(\Lambda)^{\frac{1}{2}}}$ seja mínima. Isto é equivalente a encontrar n vetores linearmente independentes $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ no reticulado Λ tal que

$$\prod_{i=1}^{n} \|\boldsymbol{b}_i\| \leq (M-1)det(\Lambda)^{\frac{1}{2}}$$

seja mínimo.

Seja λ_1 a distância mínima do reticulado Λ. No pior caso, suponha que $\|\boldsymbol{b}_i\| = \lambda_1$ para $i = 1, \cdots, n-1$. Para compensar o fato que $\prod_{i=1}^{n} \|\boldsymbol{b}_i\| \leq (M-1)det(\Lambda)^{\frac{1}{2}}$, devemos ter $\|\boldsymbol{b}_n\| \leq \frac{(M-1)det(\Lambda)^{\frac{1}{2}}}{{\lambda_1}^{n-1}}$.

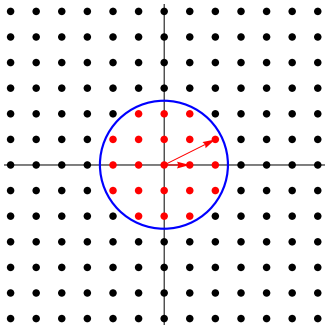


Figura 2.8: $B[\mathbf{0}, \boldsymbol{R}] \cap \Lambda$

Portanto, para percorrermos todas as possibilidades é necessário que $\boldsymbol{b}_i \in B[\mathbf{0}, \boldsymbol{R}]$, onde $B[\mathbf{0}, \boldsymbol{R}]$ denota a bola euclidiana de centro na origem e raio

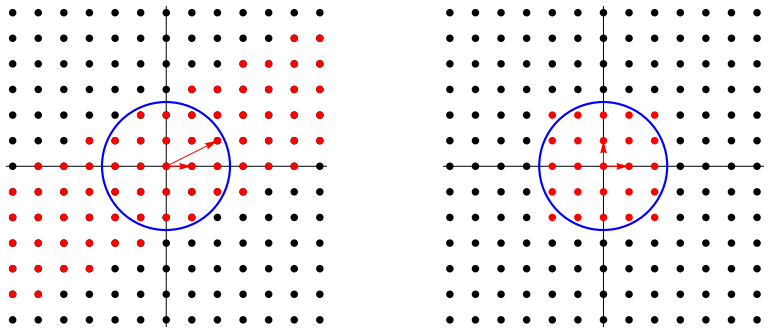
$$\boldsymbol{R} = \frac{(\boldsymbol{M}-1)|det(\Lambda)|^{\frac{1}{2}}}{{\lambda_1}^{n-1}}.$$

Observação 2.4.1. *Para encontrar o vetor de norma mínima, vamos utilizar o algoritmo da redução da base de Minkowski proposta por Strapasson [62], que é eficiente para dimensões baixas.*

O primeiro problema que encontramos é como gerar os pontos do reticulado Λ que estão contidos em $B[\mathbf{0}, \boldsymbol{R}]$. A Figura 2.8 mostra um reticulado Λ e sua intersecção com a bola $B[\mathbf{0}, \boldsymbol{R}]$.

Observação 2.4.2. *Note que se tomarmos uma base para tal reticulado e procurarmos gerar os pontos do reticulado variando os coeficientes nessa base, podemos gerar bem mais pontos que os pontos contidos na bola. Para eliminar esses pontos devemos calcular a norma de cada um destes vetores. Isso se torna difícil a medida em que a dimensão aumenta. Uma observação interessante é que para uma base do reticulado com vetores pequenos, quanto "mais ortogonais" estes forem, menos pontos extras serão gerados. Isso acontece porque o paralelogramo gerado pelos vetores da base se aproxima da esfera como podemos observar na Figura 2.9.*

Tendo em vista não gerar pontos extras, para gerar os pontos do reticulado Λ que pertencem a $B[\mathbf{0}, \boldsymbol{R}]$, utilizaremos as idéias do algoritmo "Sphere decoding".



(a) (b)

Figura 2.9: $B[\mathbf{0}, \boldsymbol{R}]$

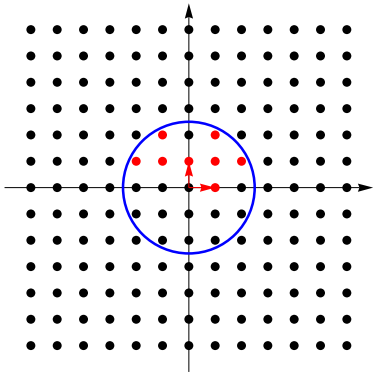


Figura 2.10: $B[\mathbf{0}, \boldsymbol{R}]$

Como buscamos por uma base ortogonal mínima, não é necessário gerar todos os pontos do reticulado dentro da esfera $B[\mathbf{0}, \boldsymbol{R}]$. É necessário apenas gerar os pontos do reticulado com norma mínima em cada direção em que houver pontos do reticulado. A Figura 2.10 exemplifica isto.

Cada ponto $\boldsymbol{x} \in \Lambda$ pode ser descrito como $\boldsymbol{x} = \boldsymbol{s}\boldsymbol{M}$, onde $\boldsymbol{M}$ é uma matriz geradora para Λ e $\boldsymbol{s} \in \mathbb{Z}^n$. O método "Sphere decoding", primeiro gera o vetor $\boldsymbol{s}$ para depois encontrar o vetor $\boldsymbol{x} \in \Lambda$. Antes de gerar $\boldsymbol{x}$, vamos estabelecer condições sobre $\boldsymbol{s}$ para gerar só o menor vetor em cada direção:

- Para obter o menor vetor em cada direção devemos exigir $mdc(s_1, \cdots, s_n) = 1$.
- Se $\boldsymbol{x} = \boldsymbol{s}\boldsymbol{M} \in \Lambda \cap B[\mathbf{0}, \boldsymbol{R}]$, então $-\boldsymbol{x} = -s\boldsymbol{M} \in \Lambda \cap B[\mathbf{0}, \boldsymbol{R}]$. Agora, $mdc(s_1, \cdots, s_n) = mdc(-s_1, \cdots, -s_n)$. Portanto, devemos gerar apenas um desses dois pontos.

A medida em que geramos tais pontos, procuramos pelos conjuntos ortogonais. Note que se $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, então $\boldsymbol{x} = \boldsymbol{s}\boldsymbol{M}$ e $\boldsymbol{y} = \boldsymbol{s}^*\boldsymbol{M}$ com $\boldsymbol{s}, \boldsymbol{s}^* \in \mathbb{Z}^n$, donde $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{s}\boldsymbol{M}\boldsymbol{M}^t\boldsymbol{s}^{*t}$. Para cada vetor gerado $\boldsymbol{s}^*$, podemos guardar o vetor $\boldsymbol{M}\boldsymbol{M}^t\boldsymbol{s}^*$ e usa-lo para calcular o produto interno de $\boldsymbol{s}^*\boldsymbol{M}$ com os vetores $\boldsymbol{s}\boldsymbol{M}$, onde $\boldsymbol{s} \in \mathbb{Z}^n$.

Para cada vetor gerado $\boldsymbol{s}_i \in \mathbb{Z}^n$ vamos chamar o ponto do reticulado correspondente de $\boldsymbol{x}_i = \boldsymbol{s}_i\boldsymbol{M}$. A medida em que vamos calculando o produto interno de $\boldsymbol{x}_i$ com outros vetores gerados, construimos uma matriz $\boldsymbol{K} = (k_{ij})$ onde $k_{ij} = 1$ se $\left\langle \boldsymbol{x}_i, \boldsymbol{x}_j^t \right\rangle = 0$ e $k_{ij} = 0$ se $\left\langle \boldsymbol{x}_i, \boldsymbol{x}_j^t \right\rangle \neq 0$.

Após calcular todos os produtos internos, dois a dois, vamos procurar por n vetores linearmente independentes usando as entradas da matriz $\boldsymbol{K}$. Por exemplo, no caso de três vetores, devemos procurar por i, j, l tais que $k_{ij}k_{jl}k_{il} = 1$. Após obter um conjunto de n vetores ortogonais $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n$, calculamos $Prod = \prod_{i=1}^{n} ||\boldsymbol{x}_i||$ e guardamos apenas o conjunto com o menor valor para $Prod$.

Exemplo 2.4.1. *Seja Λ o reticulado com base $\boldsymbol{v}_1 = (4, 25, 28)$, $\boldsymbol{v}_2 = (0, 50, 0)$ e $\boldsymbol{v}_3 = (0, 0, 200)$. Temos que $200I_3$ gera um sub-reticulado ortogonal $\Lambda^\star$. Temos que $|\Lambda/\Lambda^\star| = 200$, portanto podemos construir uma treliça com 200 caminhos. Aplicando o algoritmo de busca pelo sub-reticulado ortogonal que minimize $|\Lambda/\Lambda^\star|$ encontramos o sub-reticulado Λ^* com base $\boldsymbol{b}_1 = (-32, 0, -24)$, $\boldsymbol{b}_2 = (-24, 0, 32)$ e $\boldsymbol{b}_3 = (0, 50, 0)$. Temos que $|\Lambda/\Lambda^*| = 2$ e este é o menor quociente possível.*

Em [8], foi calculada a treliça mínima dos reticulados D_n para $n \geq 3$, E_6, E_7, E_8 e A_n para $n \leq 9$. No que segue, calculamos a treliça mínima para o reticulado MCC, que não havia sido calculada.

Exemplo 2.4.2. *Considere o reticulado MCC dado pelo Exemplo 2.2.6. Naquele exemplo, temos que uma treliça associada ao quociente do reticulado pelo sub-reticulado ortogonal possui 4 caminhos. Partindo de tal informação e utilizando o algoritmo que busca pela treliça mínima, encontramos o sub-reticulado ortogonal com base*

$$\left\{ \left(0, \left(-\frac{1}{2}\right)^{1/4}, \left(-\frac{1}{2}\right)^{1/4}\right), \left(0, \left(-\frac{1}{2}\right)^{1/4}, \left(\frac{1}{2}\right)^{1/4}\right), \left(-\sqrt{2}, 0, 0\right) \right\}$$

que gera uma treliça com dois caminhos. Portanto, a treliça encontrada com dois caminhos é mínima.

2.5 Sub-reticulados ortogonais em reticulados bidimensionais

Neste seção, trabalhamos com reticulados $\Lambda \subseteq \mathbb{R}^2$ de posto 2 que possuem matriz de Gram com entradas inteiras. Procuramos por sub-reticulados ortogonais utilizando as características da forma normal de Smith da matriz de Gram [21]. A forma normal de Smith pode ser aplicada apenas em matrizes com determinante não nulo e cujas entradas pertençam a um domínio de ideais principais, portanto, analisaremos apenas reticulados inteiros. Como para cada reticulado com matriz de Gram com entradas racionais sempre existe um reticulado equivalente obtido por uma dilatação cuja matriz de Gram possui todas as entradas inteiras, podemos estender o resultado para estes reticulados.

Teorema 2.5.1. *Sejam $\Lambda \subset \mathbb{R}^2$ um reticulado, $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ uma base para Λ, $\boldsymbol{G}$ a matriz de Gram associada a esta base com entradas inteiras e com decomposição de Smith $\boldsymbol{G} = \boldsymbol{P}^{-1}\boldsymbol{D}\boldsymbol{Q}^{-1}$, onde $\boldsymbol{D}$ é uma matriz diagonal com $d_{11}|d_{22}$ e $\boldsymbol{P}, \boldsymbol{Q}$ são matrizes unimodulares. Os sub-reticulados ortogonais de Λ que possuem os menores vetores em cada direção são caracterizados pela base $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$, onde $\boldsymbol{w}_1 = a\boldsymbol{v}_1 + b\boldsymbol{v}_2$ e $\boldsymbol{w}_2 = c^*\boldsymbol{v}_1 + d^*\boldsymbol{v}_2$ com a, b, c, d inteiros satisfazendo:*

- $mdc(a, b) = 1$;
- $c^* = \frac{c}{t}$, $d^* = \frac{d}{t}$, *onde*

$$c = -q_{11}w(ap^*_{12} + bp^*_{22}) + q_{12}(ap^*_{11} + bp^*_{21}),$$

$$d = -q_{21}w(ap^*_{12} + bp^*_{22}) + q_{22}(ap^*_{11} + bp^*_{21})$$

com $d_{22} = d_{11}w$, q_{ij} elementos da matriz $\boldsymbol{Q}$, p^*_{ij} elementos da matriz $\boldsymbol{P}^{-1}$ e $t = mdc(c, d)$.

Demonstração: Seja $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$ uma base ortogonal para um sub-reticulado ortogonal bidimensional de Λ tal que $\boldsymbol{w}_1 = a\boldsymbol{v}_1 + b\boldsymbol{v}_2$ e $\boldsymbol{w}_2 = c\boldsymbol{v}_1 + d\boldsymbol{v}_2$. Como queremos encontrar o menor sub-reticulado ortogonal em cada direção tomemos $\boldsymbol{w}_1$ tal que a, b não sejam simultaneamente nulos e $mdc(a, b) = 1$. Seja $\boldsymbol{M}$ a matriz geradora com $\boldsymbol{v}_1, \boldsymbol{v}_2$ suas linhas. Temos que

$$\langle \boldsymbol{w}_1, \boldsymbol{w}_2 \rangle = (a, b)(\boldsymbol{M}\boldsymbol{M}^t)(c, d)^t = (a, b)\boldsymbol{G}(c, d)^t,$$

onde $\boldsymbol{M}\boldsymbol{M}^t = \boldsymbol{G}$. Como as entradas de $\boldsymbol{G}$ são números inteiros, utilizando a decomposição de Smith em $\boldsymbol{G}$ temos

$$\langle \boldsymbol{w}_1, \boldsymbol{w}_2 \rangle = (a,b)\boldsymbol{P}^{-1} \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \boldsymbol{Q}^{-1}(c,d)^t.$$

Como d_1 divide d_2, segue que $d_2 = d_1 w$ para algum $w \in \mathbb{Z}$. Com isso, obtemos

$$\begin{aligned} \langle \boldsymbol{w}_1, \boldsymbol{w}_2 \rangle &= (a,b)\boldsymbol{P}^{-1} d_1 \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix} \boldsymbol{Q}^{-1}(c,d)^t \\ &= d_1(a,b) \begin{pmatrix} p_{11}^* & p_{12}^* \\ p_{21}^* & p_{22}^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix} \boldsymbol{Q}^{-1}(c,d)^t \\ &= (\tilde{a}, \tilde{b}) \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix} (\tilde{c}, \tilde{d})^t \\ &= \left\langle (\tilde{a}, \tilde{b}), (\tilde{c}, w\tilde{d}) \right\rangle \end{aligned}$$

onde $(\tilde{a}, \tilde{b}) = d_1(a,b) \begin{pmatrix} p_{11}^* & p_{12}^* \\ p_{21}^* & p_{22}^* \end{pmatrix}$ e $(\tilde{c}, \tilde{d}) = \boldsymbol{Q}^{-1}(c,d)^t$. Então, $0 = \langle \boldsymbol{w}_1, \boldsymbol{w}_2 \rangle = \left\langle (\tilde{a}, \tilde{b}), (\tilde{c}, w\tilde{d}) \right\rangle$.
Em $\mathbb{R}^2$ vale que $\left\langle (\tilde{a}, \tilde{b}), (\tilde{c}, w\tilde{d}) \right\rangle = 0$ se, e somente se, existe $\lambda \in \mathbb{R}^*$ tal que

$$\begin{cases} \tilde{c} = -\lambda \tilde{b} \\ w\tilde{d} = \lambda \tilde{a} \end{cases}$$

donde

$$\begin{cases} \tilde{c} = -\lambda \tilde{b} \\ \tilde{d} = \frac{\lambda}{w} \tilde{a} \end{cases}$$

O fato de $\tilde{a}, \tilde{b}, \tilde{c}$ e $\tilde{d}$ serem inteiros implica que $\lambda \in \mathbb{Q}$. Agora, como $\boldsymbol{Q}^{-1}(c,d)^t = (\tilde{c}, \tilde{d})^t$, segue que

$$\begin{pmatrix} c \\ d \end{pmatrix} = \boldsymbol{Q} \begin{pmatrix} \tilde{c} \\ \tilde{d} \end{pmatrix} = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix} \begin{pmatrix} \tilde{c} \\ \tilde{d} \end{pmatrix} =$$

$$\begin{pmatrix} q_{11}\tilde{c} + q_{12}\tilde{d} \\ q_{21}\tilde{c} + q_{22}\tilde{d} \end{pmatrix} = \begin{pmatrix} q_{11}(-\lambda\tilde{b}) + q_{12}(\frac{\lambda}{w}\tilde{a}) \\ q_{21}(-\lambda\tilde{b}) + q_{22}(\frac{\lambda}{w}\tilde{a}) \end{pmatrix}.$$

De

$$(\tilde{a},\tilde{b}) = d_1(a,b)\begin{pmatrix} p_{11}^* & p_{12}^* \\ p_{21}^* & p_{22}^* \end{pmatrix} = d_1\begin{pmatrix} ap_{11}^* + bp_{21}^* \\ ap_{12}^* + bp_{22}^* \end{pmatrix}^t,$$

segue que

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -\lambda q_{11} d_1(ap_{12}^* + bp_{22}^*) + \frac{q_{12}\lambda}{w} d_1(ap_{11}^* + bp_{21}^*) \\ -\lambda q_{21} d_1(ap_{12}^* + bp_{22}^*) + \frac{q_{22}\lambda}{w} d_1(ap_{11}^* + bp_{21}^*) \end{pmatrix}.$$

Como $\lambda \in \mathbb{Q}^*$, então $\lambda = \frac{m}{n}$ para $m, n \in \mathbb{Z}$ com $n \neq 0$. Assim, temos que

$$w\,n\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -q_{11} d_1 mw(ap_{12}^* + bp_{22}^*) + q_{12} md_1(ap_{11}^* + bp_{21}^*) \\ -q_{21} d_1 mw(ap_{12}^* + bp_{22}^*) + q_{22} m(ap_{11}^* + bp_{21}^*) \end{pmatrix}.$$

Agora, note que o vetor $\boldsymbol{w}_2^* = p\,n\,c\,\boldsymbol{v}_1 + p\,n\,d\,\boldsymbol{v}_2$ é múltiplo do vetor $\boldsymbol{w}_2$. Como queremos o menor mútiplo em cada direção basta tomarmos

$$c^* = \frac{-q_{11} w(ap_{12}^* + bp_{22}^*) + q_{12}(ap_{11}^* + bp_{21}^*)}{t} \quad \text{e}$$

$$d^* = \frac{-q_{21} w(ap_{12}^* + bp_{22}^*) + q_{22}(ap_{11}^* + bp_{21}^*)}{t},$$

onde $t = mdc(-q_{11}w(ap_{12}^* + bp_{22}^*) + q_{12}(ap_{11}^* + bp_{21}^*, -q_{21}w(ap_{12}^* + bp_{22}^*) + q_{22}(ap_{11}^* + bp_{21}^*))$. Tomando $\boldsymbol{w}_1 = a\boldsymbol{v}_1 + b\boldsymbol{v}_2$ e $\boldsymbol{w}_2 = c^*\boldsymbol{v}_1 + d^*\boldsymbol{v}_2$, obtemos o menor sub-reticulado ortogonal nesta direção. Os demais sub-reticulados são obtidos multiplicando tais vetores por números inteiros. □

Exemplo 2.5.1. *Considere a versão escalonada do reticulado hexagonal com base* $\boldsymbol{v}_1 = (\sqrt{2}, 0)$ *e* $\boldsymbol{v}_2 = (\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2})$ *e com matriz de Gram com decomposição de Smith dada por*

$$\boldsymbol{G} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -4 & 5 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1}.$$

Os sub-reticulados ortogonais com menores vetores em cada direção são dados pela base $\boldsymbol{w}_1 = a\boldsymbol{v}_1 + b\boldsymbol{v}_2$ *e* $\boldsymbol{w}_2 = \frac{-a-2b}{mdc(-a-2b,2a+b)}\boldsymbol{v}_1 + \frac{2a+b}{mdc(-a-2b,2a+b)}\boldsymbol{v}_2$.

Observação 2.5.1. *Um observação interessante é que no* $\mathbb{R}^2$, *dado qualquer vetor* $\boldsymbol{w}$ *em um reticulado racional* Λ *sempre existe um sub-reticulado ortogonal de* Λ *com uma base ortogonal que possui* $\boldsymbol{w}$ *como um de seus vetores. Isto segue do fato de que dados* $\boldsymbol{w} \in \Lambda$ *e um outro vetor qualquer* $\boldsymbol{z} \in \Lambda$ *tal que* $\boldsymbol{w}$ *e* $\boldsymbol{z}$ *sejam linearmente independentes, basta aplicar o processo de ortogonalização de Gram-Schmidt considerando* $\boldsymbol{w}$ *fixo.*

CAPÍTULO 3

RETICULADOS Q-ÁRIOS

Neste capítulo, iremos trabalhar com duas relações entre códigos e reticulados, a "Construção A" e a "Construção B". A Construção A é apresentada em [23, 56] para códigos q-ários, enquanto que a Construção B é definida em [23] para uma classe de códigos binários e ternários. Neste capítulo estudamos propriedades de ambas contruções, generalizamos a Construção B para uma classe de códigos q-ários, $q \in \mathbb{N}$, e estudamos relações entre os processos de decodificação de um reticulado q-ário na métrica da soma e seu código associado na métrica de Lee via Construção A. Alguns resultados deste capítulo foram apresentados no 2011 IEEE Information Theory Workshop [18].

Nas seções 3.1 e 3.2, estudamos códigos e reticulados q-ários para $q \in \mathbb{N}$, verificando suas propriedades e como caracterizar a matriz geradora de um reticulado q-ário em função da matriz geradora do código q-ário associado. Na Seção 3.3, estendemos a Construção B para uma classe de códigos q-ários e derivamos algumas propriedades dos reticulados obtidos por essa construção. Na seção 3.4, obtemos via Construção A uma relação entre a decodificação de um reticulado q-ário na métrica da soma e seu código associado na métrica de Lee. Na seção 3.5, apresentamos o algoritmo "Lee sphere decoding" com algumas simplificações para uma classe de reticulados obtidos via Construções A e B. Na seção 3.6, introduziremos os reticulados do tipo $(q_1, \cdots, q_n)-$ários que podem ser interessantes em algumas aplicações e generalizam o caso anterior.

3.1 Códigos q-ários, $q \in \mathbb{N}$, na métrica de Lee

Em [52] são definidos códigos lineares sobre qualquer anel comutativo finito. Neste trabalho, estudaremos códigos sobre o anel $\mathbb{Z}_q$ dos inteiros módulo q. Em [35], é apresentado um estudo de códigos lineares sobre corpos finitos $\mathbb{Z}_q$, q primo.

Definição 3.1.1. *Seja $q \in \mathbb{N}$. Um* **código linear q-ário $\boldsymbol{C}$** *é um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$, ou seja, é um subgrupo aditivo de $\mathbb{Z}_q^n$.*

Exemplo 3.1.1. *Temos que $\boldsymbol{C} = \langle(\overline{1},\overline{3},\overline{5})\rangle = \{(\overline{0},\overline{0},\overline{0}),(\overline{1},\overline{3},\overline{5}),(\overline{2},\overline{0},\overline{4}),(\overline{3},\overline{3},\overline{3}),(\overline{4},\overline{0},\overline{2}),(\overline{5},\overline{3},\overline{1})\} \subseteq \mathbb{Z}_6^3$ é um código linear 6-ário.*

Algumas das propriedades presentes em códigos lineares definidos sobre corpos $\mathbb{Z}_q$, q primo, não são válidas em códigos lineares definidos sobre o anel $\mathbb{Z}_q$, $q \in \mathbb{N}$, por exemplo, a existência de uma base. Para q primo, temos a propriedade que todo código linear $C \subseteq \mathbb{Z}_q^n$ possui uma base com cardinalidade menor ou igual a n. A existência da base segue do fato de $\mathbb{Z}_q$ ser corpo para q primo, o que não acontece quando q não é um número primo.

Exemplo 3.1.2. *Considere o código $\boldsymbol{C} = \langle(\overline{2},\overline{4},\overline{6})\rangle = \{(\overline{0},\overline{0},\overline{0}),(\overline{2},\overline{4},\overline{6}),(\overline{4},\overline{8},\overline{0}),(\overline{6},\overline{0},\overline{6}),(\overline{8},\overline{4},\overline{0}),(\overline{10},\overline{8},\overline{6})\} \subseteq \mathbb{Z}_{12}^3$. Temos que $\boldsymbol{C}$ é gerado por $(\overline{2},\overline{4},\overline{6})$, mas $(\overline{2},\overline{4},\overline{6})$ é linearmente dependente sobre $\mathbb{Z}_{12}$, pois $\overline{6}(\overline{2},\overline{4},\overline{6}) = (\overline{0},\overline{0},\overline{0})$. Além disso, para qualquer outro elemento $(\overline{a},\overline{b},\overline{c}) \in \boldsymbol{C}$ temos que $\overline{6}(\overline{a},\overline{b},\overline{c}) = (\overline{0},\overline{0},\overline{0})$. Portanto, $\boldsymbol{C}$ não possui uma base.*

Podemos caracterizar um código linear q-ário $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ por um conjunto minimal de geradores.

Definição 3.1.2. *Chamamos de* **matriz geradora** *para um código linear q-ário $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$, $q \in \mathbb{N}$, uma matriz cujas linhas apresentam o menor número de geradores para o código $\boldsymbol{C}$.*

Proposição 3.1.1. *Sejam $q \in \mathbb{N}$, $\mathbb{Z}_q$ o anel de inteiros módulo q e $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário. Qualquer conjunto de geradores de $\boldsymbol{C}$ pode ser reduzido a um conjuntos de geradores com $k \leq n$ elementos.*

Demonstração: Seja $\{\overline{\boldsymbol{x}_1},\cdots,\overline{\boldsymbol{x}_m}\}$ um conjunto de geradores para $\boldsymbol{C}$. Dado $\overline{\boldsymbol{x}} \in \boldsymbol{C}$ temos que $\overline{\boldsymbol{x}} = \sum_{i=1}^m \overline{a}_i\overline{\boldsymbol{x}_i}$ com $\overline{a}_i \in \mathbb{Z}_q$. Assim, $x - \sum_{i=1}^m a_i\boldsymbol{x}_i = q\boldsymbol{w}$ para algum $\boldsymbol{w} \in \mathbb{Z}^n$, o que implica

que $x = \sum_{i=1}^{m} a_i \boldsymbol{x}_i + q\boldsymbol{w}$. Notamos que $\boldsymbol{w} = \sum_{i=1}^{n} w_i e_i$, onde $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ para todo $i = 1, \cdots, n$. Seja A o conjunto gerado por combinações lineares inteiras de $\{\boldsymbol{x}_1, \cdots, \boldsymbol{x}_m\} \bigcup \{qe_1, \cdots, qe_n\}$. Temos que $\boldsymbol{C} = \{\overline{x} \in \mathbb{Z}_q^n; \boldsymbol{x} \in A\}$. Como A é um $\mathbb{Z}$-submódulo de $\mathbb{Z}^n$ e $\mathbb{Z}$ é anel principal, decorre que A pode ser gerado por um conjunto de no máximo n vetores $\{\boldsymbol{y}_1, \cdots, \boldsymbol{y}_n\}$ e assim $\overline{\boldsymbol{x}}$ é gerado como combinação de $\{\overline{\boldsymbol{y}_1}, \cdots, \overline{\boldsymbol{y}_n}\}$. □

Observação 3.1.1. *[50] Sejam $q \in \mathbb{N}$, $\mathbb{Z}_q$ o anel de inteiros módulo q e $\boldsymbol{M}$ um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$. Se $\boldsymbol{M}$ possui uma base sobre $\mathbb{Z}_q$ com $\boldsymbol{k}$ elementos, então qualquer outra base de $\boldsymbol{M}$ possui exatamente $\boldsymbol{k}$ elementos.*

Em geral, códigos lineares sobre $\mathbb{Z}_q^n$ são estudados na métrica de Hamming [35]. Uma métrica mais natural em $\mathbb{Z}_q^n$ é a métrica de Lee [41], que pode ser vista como a métrica induzida da métrica da soma em $\mathbb{R}^n$.

Dado $q \in \mathbb{N}$, um conjunto de representantes para $\mathbb{R}/q\mathbb{Z}$ é dado por $[0, q)$. Identificaremos $\mathbb{R}/q\mathbb{Z}$ com $[\overline{0}, \overline{q})$, onde para cada $x \in \mathbb{R}$, $\overline{x}$ é definido como o único número real não negativo tal que $x - \overline{x} \in q\mathbb{Z}$.

Definição 3.1.3. *Dados $\overline{a}, \overline{b} \in [\overline{0}, \overline{q})$ com $0 \leq a, b < q$, definimos a métrica de Lee por*

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

Geometricamente, identificando as classes do anel $\mathbb{Z}_q$ com os vértices de um polígono regular de q lados, a distância de Lee entre duas classes será o menor número de arestas entre os vértices.

Exemplo 3.1.3. *Em $\mathbb{Z}_8$, temos que $d_{Lee}(\overline{5}, \overline{0}) = min\{|5 - 0|, 8 - |5 - 0|\} = 3$ (ver Figura 3.1). Agora, para $q = 7$ temos que $d_{Lee}(\overline{3.5}, \overline{13.2}) = min\{|3.5 - 6.2|, 7 - |3.5 - 6.2|\} = 2.7$.*

Definição 3.1.4. *Dado $n \in \mathbb{N}$, definimos a métrica de Lee em $[\overline{0}, \overline{q})^n$ por*

$$d_{Lee}(\boldsymbol{a}, \boldsymbol{b}) = \sum_{i=1}^{n} d_{Lee}(\overline{a_i}, \overline{b_i}),$$

onde $\boldsymbol{a} = (\overline{a_1}, \cdots, \overline{a_n}), \boldsymbol{b} = (\overline{b_1}, \cdots, \overline{b_n}) \in [\overline{0}, \overline{q})^n$.

Geometricamente, se identificarmos os elementos de $\mathbb{Z}_q^n$ com os pontos de uma malha quadriculada $[0, q) \times \cdots \times [0, q)$ e identificarmos os lados opostos desta malha, temos que a distância de Lee entre dois pontos é o menor número de arestas ligando esses pontos.

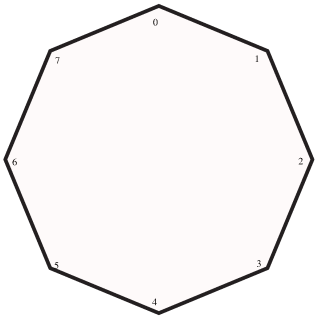


Figura 3.1: Métrica de Lee em $\mathbb{Z}_8$

Exemplo 3.1.4. *Em $\mathbb{Z}_5^2$ a distância de Lee entre os elementos $\boldsymbol{a} = (\overline{1}, \overline{1})$ e $\boldsymbol{b} = (\overline{4}, \overline{4})$ é $d_{Lee}(\boldsymbol{a}, \boldsymbol{b}) = min\{|1-4|, 5-|1-4|\} + min\{|1-4|, 5-|1-4|\} = 2+2 = 4$. A Figura 3.2, com os lados opostos identificados representa $\mathbb{Z}_5^2$ e podemos ver que o menor número de arestas ligando $\boldsymbol{a}$ e $\boldsymbol{b}$ é 4.*

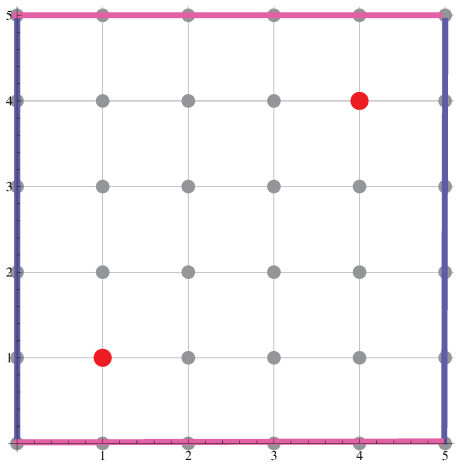


Figura 3.2: Métrica de Lee em $\mathbb{Z}_5^2$

Definição 3.1.5. *Dado um código linear q-ário $\boldsymbol{C}$ chamamos de* **distância mínima de Lee** *o valor $\boldsymbol{d}_{Lee} = min\{d_{Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{0}});\ \overline{\boldsymbol{0}} \neq \overline{\boldsymbol{x}} \in \boldsymbol{C}\}$.*

Proposição 3.1.2. *Se $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ é um código linear com distância mínima de Lee d_{Lee}, então a capacidade de correção de erros de Lee de $\boldsymbol{C}$ é $t = \left\lfloor \frac{d_{Lee}-1}{2} \right\rfloor$.*

Demonstração: Mostremos que as bolas de Lee centralizadas em palavras-código com raio t não se interceptam. De fato, suponha que existe $\boldsymbol{x} \in B[\boldsymbol{a}_1, t] \cap B[\boldsymbol{a}_2, t]$ para $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \boldsymbol{C}$.

Então $d(\boldsymbol{a}_1, \boldsymbol{a}_2) \leq d(\boldsymbol{a}_1, \boldsymbol{x}) + d(\boldsymbol{x}, \boldsymbol{a}_2) \leq 2t \leq 2(\frac{d_{Lee}-1}{2}) < d_{Lee}$, o que é uma contradição. Mostremos agora que t é o maior raio inteiro tal que as esferas de Lee ao redor de cada palavra-código não se tocam. Seja $t^* = t + 1$ e suponha que as bolas de Lee centralizadas em palavras-código com raio t^* não se interceptam. Desta forma, para todo $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{C}$, temos que

$$d(\boldsymbol{a}, \boldsymbol{b}) > 2(t+1) = 2t + 2 = \begin{cases} d_{Lee} + 1 \text{ se } d_{Lee} \text{ for par} \\ d_{Lee} + 2 \text{ se } d_{Lee} \text{ for ímpar} \end{cases}$$

o que contradiz o fato de $d_{Lee} = min\{d_{Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{0}});\ \overline{\boldsymbol{0}} \neq \overline{\boldsymbol{x}} \in \boldsymbol{C}\}$. □

Observação 3.1.2. *Um fato conhecido [26] é que dois códigos são equivalentes na métrica de Lee se um pode ser obtido de outro por uma permutação de coordenadas composta com troca de sinais em algumas posições. Sejam $q \in \mathbb{N}$ um número primo e $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário com matriz geradora $\boldsymbol{A}$. Fazendo operações elementares nas linhas de $\boldsymbol{A}$ e considerando a permutação de colunas, obtemos uma matriz na forma $\boldsymbol{G} = (\boldsymbol{I}_{m\times m} : \boldsymbol{B}_{m\times n-m})$, que gera um código q-ário equivalente a $\boldsymbol{C}$ na métrica de Lee [35].*

3.2 Construção A

A Construção A é uma forma de se obter reticulados através de códigos linerares $C \subseteq \mathbb{Z}_q^n$ [23], [56]. Alguns reticulados bem conhecidos como E_8 e D_n, $n \geq 3$, podem ser vistos via Construção A aplicada em alguns códigos lineares binários.

Proposição 3.2.1. *[23] Considere a aplicação sobrejetora*

$$\begin{aligned} \phi :\ \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, \cdots, x_n) &\longmapsto (\overline{x_1}, \cdots, \overline{x_n}), \end{aligned} \tag{3.1}$$

onde $\overline{x_i}$ é obtido de x_i por redução módulo q para todo $i = 1, \cdots, n$. Temos que $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(\boldsymbol{C}) \subseteq \mathbb{Z}^n$ é um reticulado em $\mathbb{R}^n$. Além disso, $q\mathbb{Z}^n \subseteq \phi^{-1}(\boldsymbol{C})$.

Demonstração: Seja $\boldsymbol{C}$ um código linear q-ário. Como $\phi^{-1}(\boldsymbol{C}) \subseteq \mathbb{Z}^n$ é um conjunto discreto, basta mostrar que $\phi^{-1}(\boldsymbol{C})$ é um grupo aditivo e assim, por [61] temos que $\phi^{-1}(\boldsymbol{C})$ é um reticulado. Mostremos então que $\phi^{-1}(\boldsymbol{C})$ é grupo aditivo.

- $\mathbf{0} \in \phi^{-1}(\boldsymbol{C})$, pois $\phi(\mathbf{0}) = \overline{\mathbf{0}} \in \boldsymbol{C}$,

- Se $\boldsymbol{a}, \boldsymbol{b} \in \phi^{-1}(\boldsymbol{C})$, então $\phi(\boldsymbol{a}) = \overline{\boldsymbol{a}} \in \boldsymbol{C}$ e $\phi(\boldsymbol{b}) = \overline{\boldsymbol{b}} \in \boldsymbol{C}$. Assim, $\phi(\boldsymbol{a} - \boldsymbol{b}) = \overline{\boldsymbol{a} - \boldsymbol{b}} = \overline{\boldsymbol{a}} - \overline{\boldsymbol{b}} \in \boldsymbol{C}$. Portanto, $\boldsymbol{a} - \boldsymbol{b} \in \phi^{-1}(\boldsymbol{C})$, o que mostra que $\phi^{-1}(\boldsymbol{C})$ é subgrupo aditivo em $\mathbb{R}^n$.

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

Definição 3.2.1. *Chamamos de* **Construção A** *a aplicação ϕ que relaciona um código linear $q-$ário $\boldsymbol{C}$ a um reticulado $\phi^{-1}(\boldsymbol{C})$ e chamamos o reticulado $\Lambda_A(C) = \phi^{-1}(\boldsymbol{C})$ de* **reticulado q-ário.**

Observação 3.2.1. *Em [48] define-se reticulado q-ário como um reticulado Λ que satisfaz $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$ para algum $q \in \mathbb{N}$. Note que tal definição é equivalente à anterior. De fato, se Λ é um reticulado q-ário segundo a Definição 3.2.1, temos que $\phi^{-1}(\{\overline{\mathbf{0}}\}) = q\mathbb{Z}^n$, donde segue que $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$. Agora, seja Λ um reticulado que satisfaz $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$ para algum $q \in \mathbb{N}$. Seja $\boldsymbol{C} = \phi(\Lambda)$. Se $\boldsymbol{x} \in \phi^{-1}(\boldsymbol{C})$, então $\phi(\boldsymbol{x}) \in \boldsymbol{C}$, o que implica que existe $\boldsymbol{y} \in \Lambda$ tal que $\phi(\boldsymbol{x}) = \phi(\boldsymbol{y})$ e, assim, $\boldsymbol{x} - \boldsymbol{y} \in Ker(\phi) = q\mathbb{Z}^n \subseteq \Lambda$. Como $\boldsymbol{y} \in \Lambda$ e $\boldsymbol{x} - \boldsymbol{y} \in \Lambda$, segue que $\boldsymbol{x} \in \Lambda$ e, desta forma, $\phi^{-1}(\boldsymbol{C}) \subseteq \Lambda$. Como $\phi^{-1}(\boldsymbol{C}) = \phi^{-1}(\phi(\Lambda)) \supset \Lambda$, segue que $\Lambda = \phi^{-1}(\boldsymbol{C})$.*

Para demonstrar a Proposição 3.2.2, que é enunciada em [23], deduzimos inicialmente o seguinte lema.

Lema 3.2.1. *Sejam $\boldsymbol{v}_i = (v_{i1}, \cdots, v_{in}) \in \mathbb{Z}^n$ para $i = 1, \cdots, m$, com $m \leq n$. Se $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ é linearmente independente sobre $\mathbb{Z}$, então $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ é linearmente independente sobre $\mathbb{R}$.*

Demonstração: Suponhamos que $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ seja linearmente dependente sobre $\mathbb{R}$. Sem perda de generalidade, assumimos que $\boldsymbol{v}_1$ seja escrito como combinação linear de um conjunto maximal linearmente independente sobre $\mathbb{R}$ dado por $\{\boldsymbol{v}_{k_1}, \cdots, \boldsymbol{v}_{k_s}\}$, $k_j \in \{2, \cdots, m\}$. Logo,

existem $\lambda_{k_j} \in \mathbb{R}$ tais que $\boldsymbol{v}_1 = \lambda_{k_1}\boldsymbol{v}_{k_1} + \cdots + \lambda_{k_s}\boldsymbol{v}_{k_s}$, donde:

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

Como os vetores $\{\boldsymbol{v}_{k_1}, \cdots, \boldsymbol{v}_{k_s}\}$ são linearmente independentes sobre $\mathbb{R}$, a matriz $\boldsymbol{G} = (v_{k_j,i})$ tem posto s. Logo, existe uma submatriz $\boldsymbol{G}_1$ formanda por s colunas de $\boldsymbol{G}$ que possui determinante não nulo. Sem perda de generalidade, suponhamos que $\boldsymbol{G}_1$ seja composta pelas s primeiras colunas de $\boldsymbol{G}$. Então

$$(v_{11}, \cdots, v_{1s}) = (\lambda_{k_1}, \cdots, \lambda_{k_s}) \begin{pmatrix} v_{k_1,1} & v_{k_1,2} & \cdots & v_{k_1,s} \\ v_{k_2,1} & v_{k_2,2} & \cdots & v_{k_2,s} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k_s,1} & v_{k_s,2} & \cdots & v_{k_s,s} \end{pmatrix}.$$

Como $det(\boldsymbol{G}_1) \neq 0$, então $\boldsymbol{G}_1$ é inversível e sua inversa é dada por $\boldsymbol{G}_1^{-1} = \frac{1}{det(\boldsymbol{G}_1)}\boldsymbol{G}_2$, onde $\boldsymbol{G}_2$ é a matriz transposta da matriz de cofatores de $\boldsymbol{G}_1$. Então, $\boldsymbol{G}_1^{-1} \in M_{s\times s}(\mathbb{Q})$. Desta forma,

$$(v_{11}, \cdots, v_{1s}) = (\lambda_{k_1}, \cdots, \lambda_{k_s})\, G_1 \Longrightarrow (v_{11}, \cdots, v_{1s})\, G_1^{-1} = (\lambda_{k_1}, \cdots, \lambda_{k_s})\,,$$

donde segue que $\lambda_{k_j} \in \mathbb{Q}$ para todo j. Logo, o conjunto $\{v_1, v_{k_1}, \cdots, v_{k_s}\}$ é linearmente dependente sobre $\mathbb{Q}$ e, consequentemente, linearmente dependente sobre $\mathbb{Z}$, o que contraria a hipótese. Portanto, o conjunto $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ é linearmente independente sobre $\mathbb{R}$. □

Proposição 3.2.2. *[23] Se $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ é um código linear q-ário, então o posto de $\Lambda_A(\boldsymbol{C})$ é n.*

Demonstração: Temos que $q\mathbb{Z}^n \subset \Lambda_A(C) \subset \mathbb{Z}^n$ são $\mathbb{Z}$-módulos. Como $\mathbb{Z}$ é um domínio principal, segue que $n = \text{posto}(q\mathbb{Z}^n) \leq \text{posto}(\Lambda_A(\boldsymbol{C})) \leq \text{posto}(\mathbb{Z}^n) = n$. Logo, $\text{posto}(\Lambda) = n$. Assim, existem n vetores linearmente independentes sobre $\mathbb{Z}$ que geram Λ. Como esses vetores têm entradas inteiras, pelo Lema 3.2.1, temos que eles são linearmente independentes sobre $\mathbb{R}$. Portanto, formam uma base para o reticulado $\Lambda_A(C)$. □

Observação 3.2.2. *Os reticulados q-ários possuem como um sub-reticulado ortogonal* $q\mathbb{Z}^n$. *Desta forma, podemos notar que uma maneira de decodificar tais reticulados é usar o algoritmo de Viterbi para a treliça obtida do quociente do reticulado pelo sub-reticulado ortogonal* $q\mathbb{Z}^n$. *O número de caminhos na treliça é dado por* $\frac{det(q\mathbb{Z}^n)^{1/2}}{det(\Lambda_A(C))^{1/2}} = \frac{q^n}{det(\Lambda_A(C))^{1/2}}$.

Seja $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário. Do fato de $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n \simeq \boldsymbol{C}$, geometricamente um reticulado q-ário pode ser visto como o conjunto de pontos obtidos através das translações dos pontos presentes na hipercubo $[0,q)^n$ por vetores inteiros múltiplos de q. Os pontos do reticulado dentro da hipercubo $[0,q)^n$ são identificados com os pontos do código $\boldsymbol{C}$.

Exemplo 3.2.1. *A Figura 3.3 mostra o reticulado gerado pelo código* $7-$*ário*

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

Os pontos de mesma cor representam cópias da caixa $[0,7)^2$.

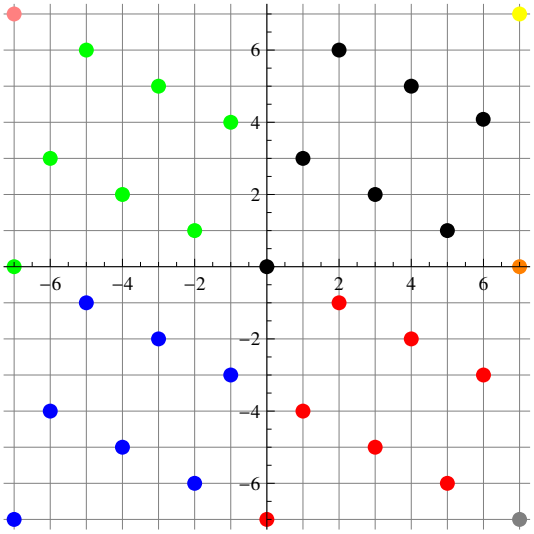


Figura 3.3: $\Lambda_A(\boldsymbol{C})$

Observação 3.2.3. *Vale observar que todo reticulado de posto* n, $\Lambda \subseteq \mathbb{Z}^n$, *possui como sub-reticulado ortogonal* $det(\Lambda)\mathbb{Z}^n$. *De fato, seja* $\boldsymbol{B}$ *uma matriz geradora para* Λ. *Temos que* $\boldsymbol{B}^{-1}\boldsymbol{B} = \frac{1}{det(\boldsymbol{B})}\overline{\boldsymbol{B}}^t\boldsymbol{B} = \boldsymbol{I}_n$, *onde* $\overline{\boldsymbol{B}}$ *é a matriz cofatora de* $\boldsymbol{B}$. *Assim,* $\overline{\boldsymbol{B}}^t\boldsymbol{B} = det(\boldsymbol{B})\boldsymbol{I}_n$.

Logo, $det(\Lambda) = det(\boldsymbol{B})^2 = [\overline{\boldsymbol{B}}^t \boldsymbol{B} \overline{\boldsymbol{B}}^t]\boldsymbol{B}$. *Como* $[\overline{\boldsymbol{B}}\boldsymbol{B}\overline{\boldsymbol{B}}^t]$ *tem todas as entradas inteiras, então* $det(\Lambda)\boldsymbol{I}_n$ *é sub-reticulado de* Λ. *Como todo reticulado* $\Lambda \subset \mathbb{Q}^n$ *pode ser transformado em um reticulado* $c\Lambda \subset \mathbb{Z}^n$ *por uma dilatação* c, *temos que todo reticulado com entradas racionais é equivalente a um reticulado* q*-ário para* $q = c\,det(\Lambda)$. *Portanto, quando estudamos as propriedade de reticulados* q*-ários estamos estudando as propriedades de reticulados com entradas racionais a menos de uma dilatação.*

A seguir, baseados na matriz geradora de um código linear q-ário $\boldsymbol{C}$ para $q \in \mathbb{N}$, caracterizaremos um conjunto de geradores para um reticulado q-ário $\Lambda_A(\boldsymbol{C})$. Quando q é um número primo, o fato de $\mathbb{Z}_q$ ser um corpo permite encontrar uma forma geral para uma matriz geradora do reticulado q-ário.

Proposição 3.2.3. *Dado um código linear* q*-ário* $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ *com conjunto de geradores* $\{\overline{\boldsymbol{v}_1}, \cdots, \overline{\boldsymbol{v}_m}\}$, *temos que o conjunto* $\boldsymbol{R} = \{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m, q\boldsymbol{e}_1, \cdots, q\boldsymbol{e}_n\}$, *onde* $\{\boldsymbol{e}_i, i = 1, \cdots, n\}$ *é a base canônica em* $\mathbb{R}^n$, *gera o reticulado* $\Lambda_A(\boldsymbol{C})$.

Demonstração: De fato, se $\boldsymbol{y} \in \phi^{-1}(\boldsymbol{C})$, então existe $\overline{\boldsymbol{c}} \in C$ tal que $\boldsymbol{y} = \boldsymbol{c} + q\boldsymbol{z}$ para algum $\boldsymbol{z} \in \mathbb{Z}^n$. Agora, existem $\overline{a_i} \in \mathbb{Z}_q$ para $i = 1, \cdots, m$, tais que $\overline{\boldsymbol{c}} = \overline{a_1}\overline{\boldsymbol{v}_1} + \cdots + \overline{a_m}\overline{\boldsymbol{v}_m}$, o que é equivalente a $\boldsymbol{c} - a_1\boldsymbol{v}_1 - \cdots - a_m\boldsymbol{v}_m \in q\mathbb{Z}^n$, ou seja, $\boldsymbol{c} - a_1\boldsymbol{v}_1 - \cdots - a_m\boldsymbol{v}_m = q\boldsymbol{w}$ para algum $\boldsymbol{w} \in \mathbb{Z}^n$. Com isso, temos que $\boldsymbol{c} = a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m + q\boldsymbol{w}$ e $\boldsymbol{y} = a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m + q[(w_1, \cdots, w_n) + (z_1, \cdots, z_n)] = a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m + (w_1 + z_1)q\boldsymbol{e}_1 + \cdots + (w_n + z_n)q\boldsymbol{e}_n$. Portanto, o conjunto $\boldsymbol{R}$ gera tal reticulado. □

Após obter um conjunto de geradores para o reticulado q-ário pela Proposição 3.2.3, calculamos a Forma Normal de Hermite (HNF) da matriz formada pelos geradores para obter uma base para o reticulado.

Exemplo 3.2.2. *Considere o código linear* 6*-ário* $\boldsymbol{C}$ *com matriz geradora dada por*

$$\boldsymbol{M} = \begin{pmatrix} \overline{2} & \overline{2} & \overline{2} & \overline{0} & \overline{4} & \overline{5} \\ \overline{0} & \overline{2} & \overline{4} & \overline{1} & \overline{0} & \overline{5} \\ \overline{2} & \overline{1} & \overline{3} & \overline{0} & \overline{1} & \overline{1} \end{pmatrix}.$$

Temos que uma base para o reticulado $\Lambda_A(\boldsymbol{C})$ *é obtida calculando a HNF da matriz de geradores*

$$\begin{pmatrix} 2 & 2 & 2 & 0 & 4 & 5 \\ 0 & 2 & 4 & 1 & 0 & 5 \\ 2 & 1 & 3 & 0 & 1 & 1 \\ 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix} \overset{HNF}{\Longrightarrow} \begin{pmatrix} 2 & 0 & 4 & 0 & 4 & 0 \\ 0 & 1 & 5 & 0 & 3 & 1 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

Observação 3.2.4. *As linhas da matriz geradora de um reticulado q-ário $\Lambda_A(\boldsymbol{C})$ reduzidas módulo q geram o código q-ário $\boldsymbol{C}$ associado.*

Proposição 3.2.4. *Sejam $q \in \mathbb{N}$ um número primo e $\boldsymbol{G} = \begin{pmatrix} \boldsymbol{I}_{m\times m} & \boldsymbol{B}_{m\times n-m} \end{pmatrix}$ uma matriz geradora do código q-ário $\boldsymbol{C} \subset \mathbb{Z}_q^n$ na forma sistemática. Uma matriz geradora do reticulado q-ário $\Lambda_A(\boldsymbol{C})$ é dada por*

$$\boldsymbol{G}_1 = \begin{pmatrix} \boldsymbol{I}_{m\times m} & \boldsymbol{B}_{m\times n-m} \\ \boldsymbol{0}_{n-m\times m} & q\boldsymbol{I}_{n-m\times n-m} \end{pmatrix}. \tag{3.2}$$

Demonstração: Já vimos na Proposição (3.2.3) que as linhas da matriz $\boldsymbol{G}$ juntamente com $q\boldsymbol{e}_i$, para $i = 1, \cdots, n$, geram $\Lambda_A(\boldsymbol{C})$. Vamos chamar de $\boldsymbol{b}_i$, $i = 1, \cdots, m$, as linhas de $\boldsymbol{G}$. Para $j = 1, \cdots, m$, temos que

$$q\boldsymbol{e}_j = q(0, \cdots, 1, \cdots, 0, b_{j,m+1}, \cdots, b_{j,n}) - b_{j,m+1}q\boldsymbol{e}_{m+1} - \cdots - b_{j,n}q\boldsymbol{e}_n.$$

Logo, $q\boldsymbol{e}_j$ para $j = 1, \cdots, m$, pode ser obtido como combinação linear inteira dos vetores $\boldsymbol{b}_i$ para $i = 1, \cdots, m$, com os vetores $q\boldsymbol{e}_i$ para $i = m+1, \cdots, n$. Agora note que a matriz $\boldsymbol{G}_{1n\times n}$ tem determinante $det(\boldsymbol{G}_1) = q^{n-m} \neq 0$. Portanto $\boldsymbol{G}_1$ é invertível em $M_n(\mathbb{R})$ e suas linhas são linearmente independentes sobre $\mathbb{R}$. □

Exemplo 3.2.3. *Considere o código* 13*-ário com matriz geradora dada por*

$$\begin{pmatrix} \overline{1} & \overline{0} & \overline{7} & \overline{5} & \overline{4} \\ \overline{0} & \overline{1} & \overline{8} & \overline{6} & \overline{1} \end{pmatrix}.$$

Temos que uma matriz geradora de $\Lambda_A(\boldsymbol{C})$ é dada por

$$\begin{pmatrix} 1 & 0 & 7 & 5 & 4 \\ 0 & 1 & 8 & 6 & 1 \\ 0 & 0 & 13 & 0 & 0 \\ 0 & 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 & 13 \end{pmatrix}.$$

Observação 3.2.5. *Como dois códigos lineares em $\mathbb{Z}_q^n$ são equivalentes na métrica de Lee se, e somente se, um pode ser obtido de outro por uma troca de coordenadas composta com troca de sinais em algumas posições, temos pela Construção A, que códigos equivalentes na métrica de Lee geram reticulados equivalentes na métrica da soma.*

Por abuso de notação, na proposição seguinte, não faremos distinção entre os elementos de $\boldsymbol{C}$ e os elementos da cópia de $\boldsymbol{C}$ em $[0,q)^n \cap \Lambda_A(\boldsymbol{C})$.

Proposição 3.2.5. *[48] Sejam $\boldsymbol{C}$ um código q-ário com uma matriz geradora $\boldsymbol{N}$, $\Lambda = \Lambda_A(\boldsymbol{C})$, Λ^* o reticulado dual de Λ e $\Lambda^\perp = \{\boldsymbol{y} \in \mathbb{Z}^n;\ \boldsymbol{y}\boldsymbol{N}^t = q\boldsymbol{s};\ \boldsymbol{s} \in \mathbb{Z}^n\}$. Temos que $\Lambda^\perp = q\ \Lambda^*$.*

Demonstração: Seja $\boldsymbol{y} \in \Lambda^\perp$. Dado $\boldsymbol{x} \in \Lambda$, temos que $\boldsymbol{x} = \boldsymbol{c} + q\boldsymbol{t}$ com $\boldsymbol{t} \in \mathbb{Z}^n$ e $\boldsymbol{c} \in \boldsymbol{C}$. Desta forma, $\langle 1/q\ \boldsymbol{y}, \boldsymbol{x}\rangle \in \mathbb{Z}$ implica $\frac{1}{q}\ \boldsymbol{y} \in \Lambda^*$, donde $\boldsymbol{y} \in q\Lambda^*$. Por outro lado, se $\boldsymbol{y} \in q\Lambda^*$, então $\boldsymbol{y} = q\boldsymbol{z}$ com $\boldsymbol{z} \in \Lambda^*$. Se $\boldsymbol{N}$ é uma matriz geradora para $\boldsymbol{C}$, como uma cópia de $\boldsymbol{C}$ está contida em $[0,q)^n \cap \Lambda_A(\boldsymbol{C})$, então $\boldsymbol{z}\boldsymbol{N}^t \in \mathbb{Z}^n$, pois $\boldsymbol{z} \in \Lambda^*$. Finalmente, $q\boldsymbol{z}\boldsymbol{N}^t = q\boldsymbol{s}$ onde $\boldsymbol{s} \in \mathbb{Z}^n$ implica que $q\boldsymbol{z} \in \Lambda^\perp$. □

Observação 3.2.6. *Note que $\Lambda^\perp$ é o reticulado obtido pela Construção A no código definido pelos vetores que são ortogonais a $\boldsymbol{C}$, isto é, $\boldsymbol{C}^* = \{x \in \mathbb{Z}_q^n; \langle x, c\rangle = 0$ para todo $x \in \boldsymbol{C}\}$.*

Através de uma matriz geradora $\boldsymbol{M}$ para $\Lambda^\perp$, pela Proposição 3.2.5, temos que uma matriz geradora para Λ^* é dada por $1/q\ \boldsymbol{M}$. Pela Proposição 1.1.2, temos que uma matriz para Λ é dada por $1/q\ (\boldsymbol{M}^t)^{-1}$.

Exemplo 3.2.4. *Seja $\boldsymbol{C}$ o código 9-ário BCH com matriz verificação de paridade*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 7 & 8 & 0 \\ 8 & 2 & 0 & 7 & 1 & 7 & 0 & 1 \\ 8 & 0 & 1 & 0 & 8 & 0 & 1 & 0 \\ 0 & 8 & 0 & 1 & 0 & 8 & 0 & 1 \\ 0 & 2 & 1 & 2 & 0 & 7 & 8 & 7 \\ 1 & 7 & 0 & 2 & 8 & 2 & 0 & 7 \end{pmatrix}.$$

Neste caso, temos uma matriz geradora para $\boldsymbol{C}^*$ e através desta matriz obtemos uma matriz geradora para $\Lambda^\perp$. Temos que matrizes geradoras para Λ^* e Λ são dadas respectivamente por

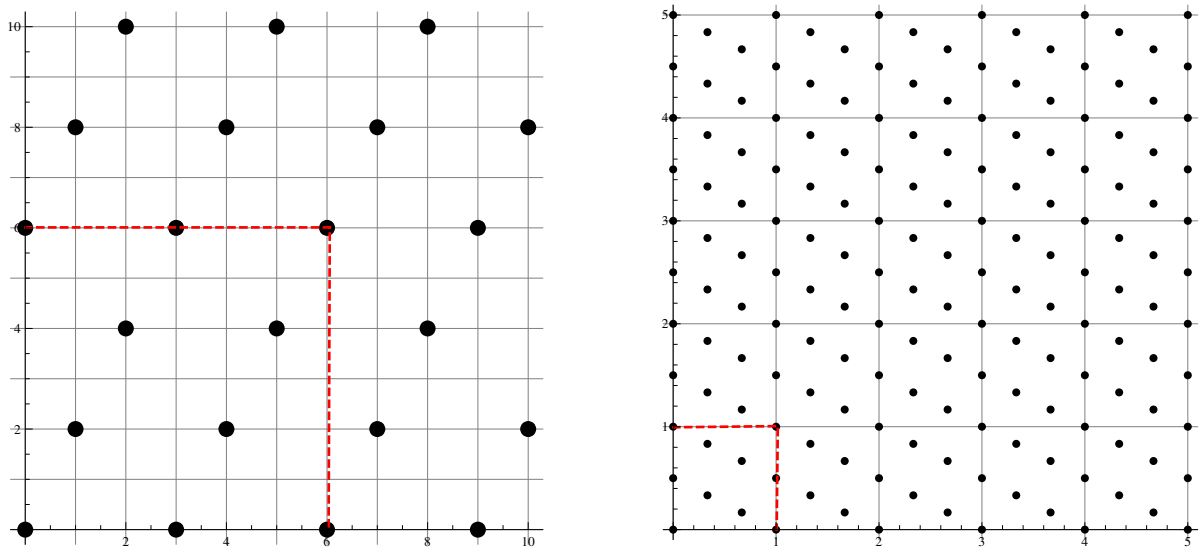
$$1/9 \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 & 6 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad e \quad \begin{pmatrix} 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 & 0 & 0 & 0 \\ -6 & -6 & -3 & -6 & 3 & 0 & 0 & 0 \\ 4 & 4 & 2 & -2 & -2 & 3 & 0 & 0 \\ -1 & -6 & -2 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 \end{pmatrix}.$$

Uma matriz geradora para Λ na forma de Hermite é

$$\begin{pmatrix} 1 & 0 & 2 & 5 & 3 & 5 & 2 & 0 \\ 0 & 1 & 3 & 8 & 1 & 7 & 7 & 0 \\ 0 & 0 & 9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 \end{pmatrix}.$$

Como $(\Lambda_A(\boldsymbol{C}))^* = \frac{1}{q}\Lambda^\perp$ e $\Lambda^\perp$ é um reticulado q-ário, o reticulado dual de $\Lambda_A(\boldsymbol{C})$ contém $\mathbb{Z}^n$ como sub-reticulado e é obtido como cópias dos pontos $\frac{1}{q}\phi^{-1}(C^*)$ presentes na da caixa $[0,1)^n$.

Exemplo 3.2.5. *Seja* $\boldsymbol{C} = \langle(\overline{1},\overline{2})\rangle \subseteq \mathbb{Z}_6^2$ *um código linear 6-ário. Temos que* $\boldsymbol{C}^* = \langle(\overline{2},\overline{2}),(\overline{0},\overline{3})\rangle$. *As figuras seguintes mostram o reticulado* $\Lambda_A(C)$ *e seu dual* $(\Lambda_A(C))^*$.



(a) (b)

Figura 3.4: $\Lambda_A(\boldsymbol{C})$ e seu dual

Se q for um número primo, existe uma matriz geradora para o código $\boldsymbol{C}$ na forma sistemática $\boldsymbol{G} = (\boldsymbol{I}_{k\times k} : \boldsymbol{B}_{k\times n-k})$ e para o código $\boldsymbol{C}^*$ na forma $\boldsymbol{H} = (-\boldsymbol{B^t}_{n-k\times k} : \boldsymbol{I}_{n-k\times n-k})$. Uma matriz geradora para $\Lambda^* = \frac{1}{q}\Lambda_A(\boldsymbol{C}^*)$ é

$$\begin{pmatrix} \frac{-1}{q}\boldsymbol{B}^t_{n-k\times k} & \frac{1}{q}\boldsymbol{I}_{n-k\times n-k} \\ \boldsymbol{I}_{k\times k} & \boldsymbol{0}_{k\times n-k} \end{pmatrix}.$$

Proposição 3.2.6. *Sejam* $q \in \mathbb{N}$ *e* $\Lambda = \phi^{-1}(\boldsymbol{C})$ *um reticulado* q*-ário para algum código linear* $\boldsymbol{C} \subset \mathbb{Z}_q^n$. *Temos que* $det(\Lambda)^{\frac{1}{2}} \geq q^{(n-m)}$, *onde* m *é o número mínimo de geradores do código* $\boldsymbol{C}$. *Se* q *for um número primo, vale a igualdade.*

Demonstração: Temos que $q^m \geq |\boldsymbol{C}| = \left|\frac{\Lambda}{q\mathbb{Z}^n}\right| = \frac{q^n}{det(\Lambda)^{\frac{1}{2}}}$. Assim, $det(\Lambda)^{\frac{1}{2}} \geq q^{n-m}$. Quando q é primo, temos $|\boldsymbol{C}| = q^m$, onde m é a dimensão do código e assim segue a igualdade. □

Exemplo 3.2.6. *Considere o código* 6*-ário com matriz geradora da forma*

$$\boldsymbol{M}_1 = \begin{pmatrix} \overline{2} & \overline{0} & \overline{2} \\ \overline{1} & \overline{1} & \overline{1} \end{pmatrix}.$$

A matriz HNF para o reticulado 6*-ário* $\Lambda = \phi^{-1}(\boldsymbol{C})$ *é dada por*

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

Temos que seu determinante é $det(\Lambda)^{\frac{1}{2}} = 12 \geq 6^{3-2}$*. Além disso,* $|\boldsymbol{C}| = \frac{6^3}{12} = 18$*.*

Observação 3.2.7. *É interessante observar que os elementos da diagonal da matriz HNF dividem* q^n*. Isto acontece pois* $det(q\mathbb{Z}^n) = q^n$ *e* $det(\Lambda) = \prod_{i=1}^{n} h_{ii}$ *que é dado pelo produto dos elementos da diagonal da matriz HNF divide* $det(q\mathbb{Z}^n)$*.*

Encontrar os vetores de distância mínima em um reticulado com a distância da soma é um problema muito difícil de ser resolvido para um reticulado qualquer [48] (assim como na distância euclidiana). Da mesma forma, encontrar a distância de Lee mínima em código também é um problema difícil de ser resolvido no caso geral (assim como na distância de Hamming).

Em [23], é apresentada uma relação entre a distância de Hamming mínima de um código binário $\boldsymbol{C}$ e a distância euclidiana mínima no reticulado 2-ário associado $\Lambda_A(\boldsymbol{C})$. A proposição seguinte, que pode ser encontrada enunciada em [56] apresenta uma relação entre a distância mínima de Lee do código q-ário $\boldsymbol{C}$ e a distância mínima da soma do reticulado q-ário $\Lambda_A(\boldsymbol{C})$. Faremos aqui uma demonstração de tal resultado.

Proposição 3.2.7. *Sejam* $\boldsymbol{C} \subset \mathbb{Z}_q^n$ *um código linear* q*-ário e* $\Lambda = \Lambda_A(\boldsymbol{C})$*. Se* $\boldsymbol{d}_{Lee}$ *é a distância mínima de Lee do código* $\boldsymbol{C}$*, então*

$$\mu = min\{q, \boldsymbol{d}_{Lee}\}$$

é a distância mínima da soma em Λ*.*

Demonstração: Considere o quociente $\Lambda/q\mathbb{Z}^n$ e o conjunto $A = B_{max}[0, q/2] \cap \Lambda$. Para cada classe $\overline{\mathbf{0}} \neq \overline{\boldsymbol{c}} \in C$, existe $\boldsymbol{c}^* \in A$ tal que $\overline{\boldsymbol{c}} = \overline{\boldsymbol{c}^*}$. De fato, basta tomar $c_i^* = c_i$ se $0 \leq c_i \leq q/2$

e $c_i^* = c_i - q$ se $q/2 < c_i < q$. Mostremos que para cada classe não nula $\overline{\boldsymbol{c}} \in \Lambda/q\mathbb{Z}^n$, o representante com a menor distância da soma está em A. Temos que os elementos da classe definida por $\overline{\boldsymbol{c}}$ são da forma $\boldsymbol{x} = \boldsymbol{c}^* + q\boldsymbol{t}$ para algum $\boldsymbol{t} \in \mathbb{Z}^n$. Como $-q/2 \leq c_i^* \leq q/2$ para todo $i = 1, \cdots, n$, segue que

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

Mostremos agora que $d_{Lee}(\overline{\boldsymbol{c}}, \overline{\boldsymbol{0}}) = d_{soma}(\boldsymbol{c}^*, \boldsymbol{0})$. Se $min\{|c_i|, q - |c_i|\} = |c_i|$, então $0 \leq c_i \leq q/2$, o que implica que $c_i^* = c_i$ 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 que $c_i^* = c_i - q$ e, assim, $min\{|c_i|, q - |c_i|\} = q - c_i = |c_i - q| = |c_i^*|$. Portanto,

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

Para a classe nula, os representantes de menor distância na métrica da soma são do tipo $\pm q\boldsymbol{e}_j$ para $j = 1, \cdots, n$. Então, se $\overline{\boldsymbol{c}} = \overline{\boldsymbol{0}}$, temos que $\boldsymbol{x} = q\boldsymbol{e}_1 + q\boldsymbol{t}$ para $\boldsymbol{t} \in \mathbb{Z}^n$ definem os pontos dessa classe. Agora, de

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

temos que

$$\begin{aligned}
\mu &= min\{d_{soma}(\boldsymbol{x}, \boldsymbol{0}); \boldsymbol{0} \neq \boldsymbol{x} \in \Lambda\} \\
&= min\{d_{soma}(\boldsymbol{x}, \boldsymbol{0}) \text{ tal que } \boldsymbol{0} \neq \boldsymbol{x} \in A \text{ ou } \boldsymbol{x} = \pm q\boldsymbol{e}_j, j = 1, \cdots, n\} \\
&= min\{d_{Lee}(\overline{\boldsymbol{c}}, \overline{\boldsymbol{0}}) \text{ tal que } \boldsymbol{0} \neq \overline{\boldsymbol{x}} \in \boldsymbol{C}, q\} = min\{\boldsymbol{d}_{Lee}, q\}.
\end{aligned}$$

□

Exemplo 3.2.7. *A Figura 3.5 esquematiza os dois conjuntos de representantes utilizados na demonstração acima para o quociente $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$ quando $q = 11$ e $\boldsymbol{C}$ é o código gerado por $(\overline{1}, \overline{3})$.*

Temos que $d_{Lee} = 3$ e assim $\mu = min\{3, 11\} = 3$.

Exemplo 3.2.8. *Considere em $\mathbb{Z}_7^5$ o código dado por*

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

Temos que $d_{Lee} = 9 > 7$. Portanto, $\mu = 7 = min\{9, 7\}$.

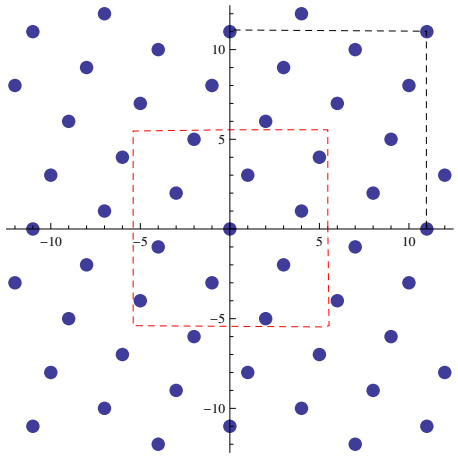


Figura 3.5: $\Lambda_A(\boldsymbol{C})$

Observação 3.2.8. *Em $\mathbb{Z}_q^2$ temos que $d_{Lee} \leq q$ para quaisquer $q \in \mathbb{N}$ e $\boldsymbol{C} \subset \mathbb{Z}_q^2$. De fato, se $(\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}}) \in \boldsymbol{C}$, então $d_{Lee}((\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}}), (\overline{\mathbf{0}}, \overline{\mathbf{0}})) = min\{|a|, q - |a|\} + min\{|b|, q - |b|\} \leq q/2 + q/2 = q$.*

Segue da Proposição (3.2.7) que o **raio de empacotamento de Lee** de um reticulado q-ário $\Lambda_A(\boldsymbol{C})$ é dado por

$$\rho = \frac{\mu}{2} = \frac{min\{\boldsymbol{d}_{Lee}, q\}}{2},$$

onde $\boldsymbol{d}_{Lee}$ é a distância mínima de Lee do código $\boldsymbol{C}$.

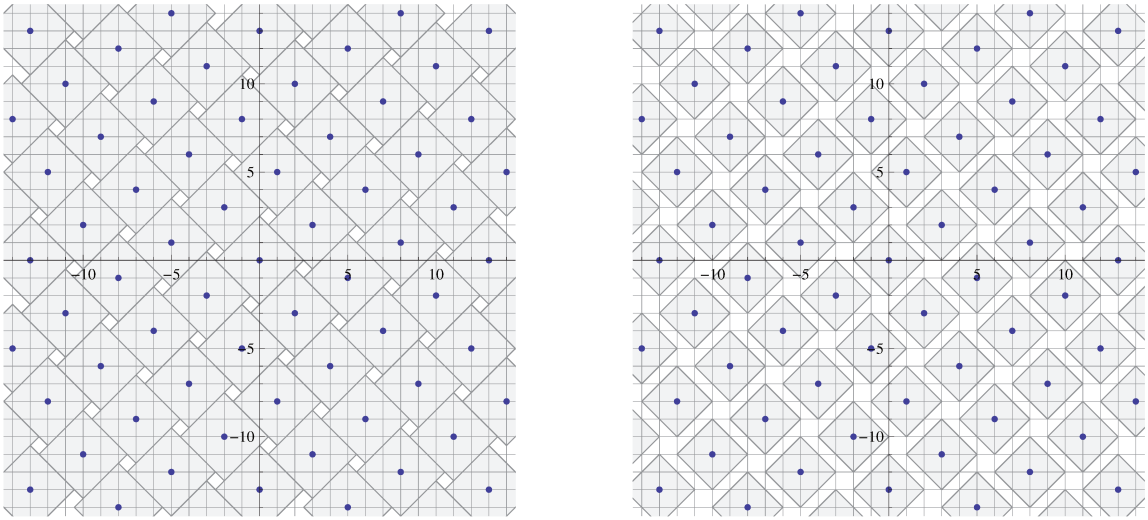
O maior raio inteiro no qual as esferas com a distância da soma centradas nos pontos de $\Lambda_A(\boldsymbol{C})$ não se interceptam é dado por

$$t = \left\lfloor \frac{min\{\boldsymbol{d}_{Lee}, q\} - 1}{2} \right\rfloor$$

o qual denotamos por **raio de correção de erros.**

Exemplo 3.2.9. *Considere o reticulado 13-ário com base $\{(1, 5), (0, 13)\}$ dado pela Figura 3.6. Temos que a distância mínima de Lee de $\boldsymbol{C} = \langle(\overline{1}, \overline{5})\rangle$ é 5 e a distância mínima da soma de $\Lambda_A(\boldsymbol{C})$ é $\mu = min\{5, 13\} = 5$. Assim, o raio de empacotamento de Lee do reticulado é $2,5$ (figura (a)). O raio de correção de erros é 2 (figura (b)). É interessante observar que códigos perfeitos podem não gerar reticulados com densidade de empacotamento máxima.*

Corolário 3.2.1. *Sejam $\boldsymbol{C}$ um código linear q-ário e $\Lambda_A(\boldsymbol{C})$ o reticulado q-ário associado. Os vetores de distância mínima com relação à métrica da soma em $\Lambda_A(\boldsymbol{C})$ são caracterizados por:*



(a) (b)

Figura 3.6: $\Lambda_A(\boldsymbol{C})$

- *Se* $\boldsymbol{d}_{Lee} > q$, *a distância mínima da soma se realiza nos vetores*

$$\{\pm q\boldsymbol{e}_i, i = 1, \cdots, n\};$$

- *Se* $\boldsymbol{d}_{Lee} < q$, *a distância mínima da soma se realiza nos vetores*

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

- *Se* $\boldsymbol{d}_{Lee} = q$, *a distância mínima da soma se realiza nos conjuntos dos itens anteriores.*

Demonstração: Segue da demonstração da Proposição (3.2.7). □

Exemplo 3.2.10. *Considere o reticulado* 6*-ário com base* $\{(1, 4), (0, 6)\}$. *Temos que* $\boldsymbol{d}_{Lee} = 3 < 6$. *Assim, os vetores de distância mínima na métrica da soma em* $\Lambda_A(\boldsymbol{C})$ *são*

$$\{\boldsymbol{c} \in B_{max}[0, 3] \cap \Lambda; \overline{\boldsymbol{c}} \in \boldsymbol{C} \text{ } e \text{ } d_{Lee}(\overline{\boldsymbol{c}}, \overline{\boldsymbol{0}}) = 3\} = \{(-3, 0), (3, 0), (1, -2), (-1, 2)\}.$$

Note que $\overline{(-3, 0)} = \overline{(3, 0)}$, $\overline{(1, -2)} = \overline{(1, 4)}$ *e* $\overline{(-1, 2)} = \overline{(5, 2)}$ *em* $\boldsymbol{C}$. *Na Figura 3.7 estão destacados os pontos do código* $\boldsymbol{C}$ *com* $\boldsymbol{d}_{Lee} = 3$.

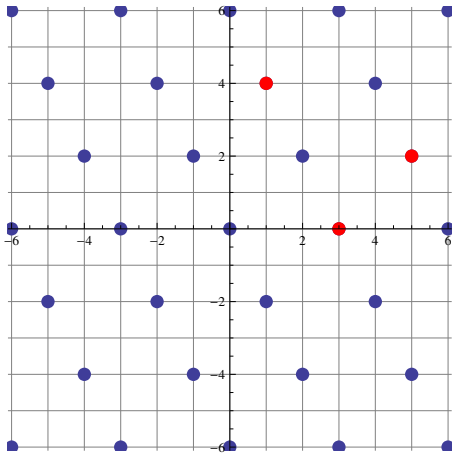


Figura 3.7: $\Lambda_A(\boldsymbol{C})$

3.3 Construção B

A Construção B é apresentada em [23] para códigos binários e ternários. Nesta seção, estendemos tal construção para uma classe de códigos lineares $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$, $q \in \mathbb{N}$. Assim como na Construção A, alguns reticulados bem conhecidos, por exemplo, o reticulado E_8, podem ser obtidos via tal construção [23].

Definição 3.3.1. *Sejam $q = 2^r b$, $r \geq 0$, $b \in \mathbb{N}$ ímpar e $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário tal que*

$$2^r \text{ divide } \sum_{i=1}^{n} c_i \text{ para todo } \overline{\boldsymbol{c}} = (\overline{c_1}, \cdots, \overline{c_n}) \in \boldsymbol{C}. \tag{3.3}$$

Definimos a **Construção B estendida** *para o código $\boldsymbol{C}$ definido acima como*

$$\Lambda_B(\boldsymbol{C}) = \{\boldsymbol{z} = \boldsymbol{c} + q\boldsymbol{w};\ \boldsymbol{w} \in \mathbb{Z}^n,\ \overline{\boldsymbol{c}} \in C \ e\ \ 2^{r+1} \text{ divide } \sum_{i=1}^{n} z_i\}. \tag{3.4}$$

Observação 3.3.1. *Para q ímpar, o código $\boldsymbol{C}$ não possui nenhuma restrição dada por (3.3). Quando q é par, se não colocarmos restrição no código, poderão existir elementos que não originam nenhum ponto do reticulado $\Lambda_B(\boldsymbol{C})$. De fato, se $q = 2^r b$ com $r > 0$, b é ímpar e existe $\overline{\boldsymbol{c}} \in C$ tal que 2^r não divide $\sum_{i=1}^n c_i$, temos que $\sum_{i=1}^n c_i = 2^a t$ com $a < r$ e t ímpar. Desta forma, para todo $\boldsymbol{w} \in \mathbb{Z}^n$, temos que se $\boldsymbol{z} = \boldsymbol{c} + q\boldsymbol{w}$ então $\sum_{i=1}^n z_i = \sum_{i=1}^n c_i + 2^r b \sum_{i=1}^n w_i = 2^a(t + 2^{r-a} b \sum_{i=1}^n w_i)$ não é divisível por 2^{r+1}.*

Exemplo 3.3.1. *Seja* $\boldsymbol{C} = \langle(\overline{1}, \overline{3})\rangle \subseteq \mathbb{Z}_6^2$ *um código linear* 6*-ário nas condições acima. Os pontos em preto na Figura 3.8 representam o reticulado* $\Lambda_B(\boldsymbol{C})$.

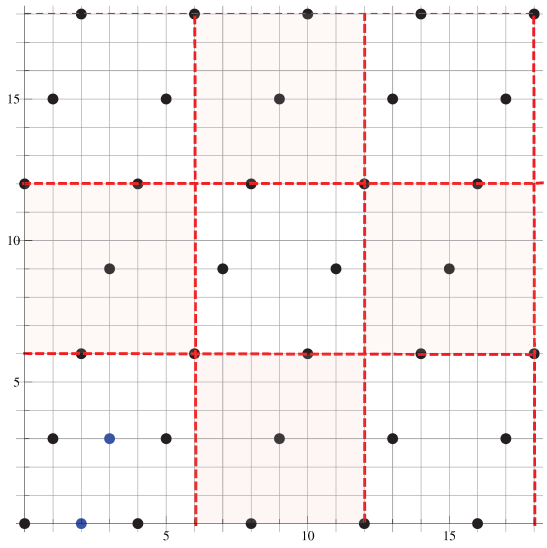


Figura 3.8: $\Lambda_B(\boldsymbol{C})$

$\Lambda_B(\boldsymbol{C})$ *não é um reticulado* 6*-ário e sim um reticulado* 12*-ário. Os pontos pretos e azuis na caixa* $[0, 6)^2$ *equivalem aos pontos do código* $\boldsymbol{C}$*. Os pontos pretos em* $[6, 12) \times [0, 6)$ *são obtidos dos pontos azuis transladados pelo vetor* $(6, 0)$.

Geometricamente, o reticulado $\Lambda_B(\boldsymbol{C})$ pode ser visto como se segue: particionamos o espaço $\mathbb{R}^n$ como cópias do hipercubo $[0, q)^n$ e pintamos alternadamente os hipercubos como em um tabuleiro de xadrez. No hipercubo $[0, q)^n$, marcamos os pontos de $\boldsymbol{C}$ que estão no reticulado. No hipercubo vizinho $[6, 12) \times [0, 6)^{n-1}$, marcamos os pontos de $\boldsymbol{C}$ que não estão no reticulado transladados pelo vetor $(6, 0, \cdots, 0)$. Repetimos os pontos destes dois hipercubos em cada hipercubo de cor equivalente. A união destes pontos é o reticulado $\Lambda_B(\boldsymbol{C})$.

Como pode ser observado, $([0, 2q) \times [0, q)^{n-1}) \cap \Lambda_B(\boldsymbol{C})$ contém uma cópia do código q-ário $\boldsymbol{C}$.

No que se segue, consideraremos apenas códigos $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ satisfazendo as restrições da Equação (3.3).

Proposição 3.3.1. *Nas condições acima,* $\Lambda_B(\boldsymbol{C})$ *é um reticulado se, e somente se,* $\boldsymbol{C}$ *é um código linear* q*-ário.*

Demonstração: Seja $\boldsymbol{C}$ um código linear. Pela demonstração da Proposição 3.2.1, temos que $\phi^{-1}(\boldsymbol{C})$ é um grupo aditivo, onde ϕ é dada pela Eq. (3.1). É claro que $\Lambda_B(\boldsymbol{C})$ é um subgrupo aditivo de $\phi^{-1}(\boldsymbol{C})$. Logo, $\Lambda_B(\boldsymbol{C})$ é um reticulado em $\mathbb{R}^n$. Agora, se $\Lambda_B(\boldsymbol{C})$ é um reticulado, mostremos que $\boldsymbol{C}$ é um código linear. Sejam $\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}} \in \boldsymbol{C}$. Existem alguns casos a analisar, porém, faremos apenas um deles, já que os demais são análogos. Suponha $\boldsymbol{a} \in \Lambda_B(\boldsymbol{C})$ e $\boldsymbol{b} \notin \Lambda_B(\boldsymbol{C})$. Temos $\boldsymbol{b} + q\boldsymbol{e}_1 \in \Lambda_B(\boldsymbol{C})$ e, do fato de $\Lambda_B(\boldsymbol{C})$ ser reticulado, segue que $\boldsymbol{a} - \boldsymbol{b} - q\boldsymbol{e}_1 \in \Lambda_B(\boldsymbol{C})$, ou seja, existe $\overline{\boldsymbol{c}} \in \boldsymbol{C}$ tal que $\boldsymbol{a} - \boldsymbol{b} - q\boldsymbol{e}_1 = \boldsymbol{c} + q\boldsymbol{t}$ para algum $\boldsymbol{t} \in \mathbb{Z}^n$. Assim, $\overline{\boldsymbol{a}} - \overline{\boldsymbol{b}} = \overline{\boldsymbol{c}} \in \boldsymbol{C}$. Portanto, $\boldsymbol{C}$ é um código linear. □

Proposição 3.3.2. *Seja $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário, $q = 2^r b$, b ímpar. Então $\Lambda_B(\boldsymbol{C}) \subseteq \Lambda_A(\boldsymbol{C})$ e $|\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})| = 2$*

Demonstração: É fácil ver que $\Lambda_B(\boldsymbol{C}) \subseteq \Lambda_A(\boldsymbol{C})$. Seja $\overline{\boldsymbol{x}} \in \Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})$. Temos que $\boldsymbol{x} = \boldsymbol{c} + q\boldsymbol{t}$ para $\overline{\boldsymbol{c}} \in \boldsymbol{C}$ e $\boldsymbol{t} \in \mathbb{Z}^n$. Se $\boldsymbol{x} \in \Lambda_B(\boldsymbol{C})$, então $\overline{\boldsymbol{x}} = \overline{\boldsymbol{0}}$ em $\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})$. Agora, se $\boldsymbol{x} \notin \Lambda_B(\boldsymbol{C})$, então $\overline{\boldsymbol{x}} \not\equiv \overline{\boldsymbol{0}}$. Mostremos que para todo $\boldsymbol{y} = \boldsymbol{c}_1 + q\boldsymbol{s} \in \Lambda_A(\boldsymbol{C}) - \Lambda_B(\boldsymbol{C})$ com $\overline{\boldsymbol{c}_1} \in C$ e $\boldsymbol{s} \in \mathbb{Z}^n$, temos que $\overline{\boldsymbol{y}} = \overline{\boldsymbol{x}}$. De fato, primeiro notemos que como $\overline{\boldsymbol{c}}, \overline{\boldsymbol{c}_1} \in \boldsymbol{C}$, então $\sum_{i=1}^n c_i = 2^r a$ e $\sum_{i=1}^n c_{1_i} = 2^r d$ para $a, d \in \mathbb{Z}$. Como $\boldsymbol{x}, \boldsymbol{y} \notin \Lambda_B(C)$, então 2^{r+1} não divide $\sum_{i=1}^n x_i = \sum_{i=1}^n c_i + q\sum_{i=1}^n t_i = 2^r(a + b\sum_{i=1}^n t_i)$ e 2^{r+1} não divide $\sum_{i=1}^n y_i = \sum_{i=1}^n c_{1_i} + q\sum_{i=1}^n s_i = 2^r(d + b\sum_{i=1}^n s_i)$. Segue então que $(a + b\sum_{i=1}^n t_i)$ e $(d + b\sum_{i=1}^n s_i)$ são números ímpares e então 2^{r+1} divide $2^r(a + b\sum_{i=1}^n t_i - d - b\sum_{i=1}^n s_i) = \sum_{i=1}^n x_i - \sum_{i=1}^n y_i$, o que implica que $\boldsymbol{x} - \boldsymbol{y} \in \Lambda_B(\boldsymbol{C})$. Portanto, $\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C}) = \{\overline{0}, \overline{x}\}$. □

Exemplo 3.3.2. *Seja $\boldsymbol{C} = \langle(\overline{1}, \overline{7})\rangle \subseteq \mathbb{Z}_9^2$. Os pontos em preto representam os pontos do reticulado $\Lambda_B(\boldsymbol{C})$ e a união dos pontos pretos e cinzas representa os pontos do reticulado $\Lambda_A(\boldsymbol{C})$. Como pode ser observado na Figura 3.9, $|\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})| = 2$.*

Proposição 3.3.3. *Sejam $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código q-ário e D_n o reticulado definido em (1.4). Então $qD_n \subseteq \Lambda_B(\boldsymbol{C})$ e $|\Lambda_B(\boldsymbol{C})/qD_n| = |\boldsymbol{C}|$.*

Demonstração: É fácil ver que $qD_n \subseteq \phi^{-1}(\boldsymbol{0})$, onde ϕ é dada pela Eq. (3.1) e 2^{r+1} divide $\sum_{i=1}^n qd_i$, pois $\boldsymbol{d} = (d_1, \ldots, d_n) \in D_n$. Então $qD_n \subseteq \Lambda_B(\boldsymbol{C})$. Consideremos o grupo quociente $\Lambda_B(\boldsymbol{C})/qD_n$. Provaremos que cada elemento de $\boldsymbol{C}$ define uma classe diferente neste quociente. Primeiro, notemos que se $\boldsymbol{x}_1 = \boldsymbol{c}_1 + q\boldsymbol{w}_1, \boldsymbol{x}_2 = \boldsymbol{c}_1 + q\boldsymbol{w}_2 \in \Lambda_B(\boldsymbol{C})$, então $\boldsymbol{x}_1 - \boldsymbol{x}_2 = q(\boldsymbol{w}_1 - \boldsymbol{w}_2)$. Assim, $\sum_{i=1}^n w_{1i}$, $\sum_{i=1}^n w_{2i}$ têm a mesma paridade, donde

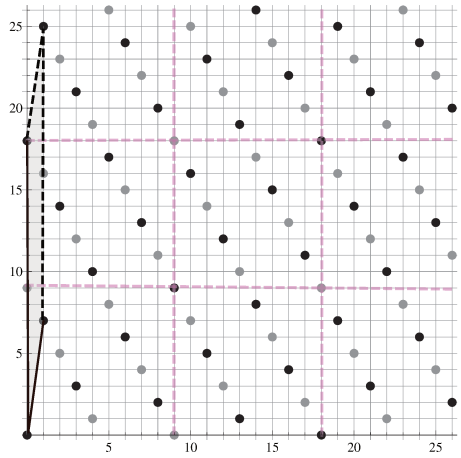


Figura 3.9: $\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})$

$\boldsymbol{w}_1 - \boldsymbol{w}_2 \in D_n$ e $\overline{\boldsymbol{x}_1} = \overline{\boldsymbol{x}_2}$ em $\Lambda_B(\boldsymbol{C})/qD_n$. Agora, se $\boldsymbol{x}_1 = \boldsymbol{c}_1 + q\boldsymbol{w}_1,\ \boldsymbol{x}_2 = \boldsymbol{c}_2 + q\boldsymbol{w}_2 \in \Lambda_B(\boldsymbol{C})$ com $\boldsymbol{c}_1 \neq \boldsymbol{c}_2$ então $\overline{\boldsymbol{x}_1} \not\equiv \overline{\boldsymbol{x}_2}$ em $\Lambda_B(\boldsymbol{C})/qD_n$. De fato, suponhamos $\boldsymbol{x}_1 - \boldsymbol{x}_2 \in qD_n$. Temos que $\boldsymbol{c}_1 - \boldsymbol{c}_2 = \boldsymbol{c} + q\boldsymbol{k}$ para algum $\boldsymbol{k} \in \mathbb{Z}^n$ e $\boldsymbol{c} \in [0, q)^n$ com $\boldsymbol{c} \neq \boldsymbol{0}$. Então $\boldsymbol{x}_1 - \boldsymbol{x}_2 = \boldsymbol{c} + q(\boldsymbol{k} + \boldsymbol{w}_1 - \boldsymbol{w}_2) \in qD_n$ implica $\boldsymbol{c} = q(\boldsymbol{t} - \boldsymbol{k} - \boldsymbol{w}_1 + \boldsymbol{w}_2)$ para algum $\boldsymbol{t} \in D_n$. Como $\boldsymbol{c} \notin q\mathbb{Z}^n$, então $\boldsymbol{x}_1 - \boldsymbol{x}_2 \notin qD_n$. □

Observação 3.3.2. *Em [64], é apresentado um algoritmo para encontrar o ponto mais próximo no reticulado D_n na métrica d_p, $(p \geq 1)$. Usando este algoritmo e a proposição acima, podemos decodificar o reticulado $\Lambda_B(\boldsymbol{C})$ na métrica da soma decompondo-o como soma de $|\boldsymbol{C}|$ classes distintas de D_n.*

Sejam $q \in \mathbb{N}$ um número primo e $[\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}_{k\times n-k}]$ uma matriz geradora para o código q-ário $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ na forma sistemática, onde $\boldsymbol{B} = (b_{i,j})$ e

$$\boldsymbol{D}^* = \begin{pmatrix} q & -q & 0 & \cdots & 0 & 0 \\ 0 & q & -q & \cdots & 0 & 0 \\ 0 & 0 & q & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q & -q \\ 0 & 0 & 0 & \cdots & & 2q \end{pmatrix}. \tag{3.5}$$

Definimos a matriz $\boldsymbol{B}^* = (b^*_{i,j})$ da seguinte forma: As primeiras $n - k - 1$ colunas de $\boldsymbol{B}$ e $\boldsymbol{B}^*$ são iguais. Para a última coluna consideramos:

$$b^*_{n-k,j} = \begin{cases} b_{n-k,j} & \text{se} \quad \sum_{i=1}^{n-k} b_{i,j} \text{ é ímpar;} \\ b_{n-k,j} + q & \text{se} \quad \sum_{i=1}^{n-k} b_{i,j} \text{ é par.} \end{cases}$$

Proposição 3.3.4. *Seja q um número primo. Uma matriz geradora para $\Lambda_B(\boldsymbol{C})$ é dada por*

$$\boldsymbol{N} = \begin{pmatrix} \boldsymbol{I}_{k\times k} & \boldsymbol{B^*}_{n\times(n-k)} \\ \boldsymbol{0}_{(n-k)\times k} & \boldsymbol{D^*}_{(n-k)\times(n-k)} \end{pmatrix}, \tag{3.6}$$

onde $\boldsymbol{B}^*$ e $\boldsymbol{D}^*$ são definidas acima.

Demonstração: Seja $\boldsymbol{x} = \boldsymbol{c} + q\boldsymbol{w} \in \Lambda_B(\boldsymbol{C})$, $\overline{\boldsymbol{c}} \in \boldsymbol{C}$ e $\boldsymbol{w} \in \mathbb{Z}^n$. Como $\overline{\boldsymbol{c}} = \sum_{i=1}^{k} \overline{a}_i \overline{\boldsymbol{c}_i}$, onde $\overline{\boldsymbol{c}_i}$ são as linhas de $[\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}_{k\times n-k}]$ e $\overline{a}_i \in \mathbb{Z}_q$, segue que $\boldsymbol{c} = \sum_{i=1}^{k} a_i \boldsymbol{c}_i + q\boldsymbol{s}$ para algum $\boldsymbol{s} \in \mathbb{Z}^n$. Cada $\boldsymbol{c}_i$ pode ser escrito como $\boldsymbol{c}_i = \boldsymbol{c}_i^* + q\boldsymbol{t}_i$, onde $\boldsymbol{c}_i^*$ é uma linha de $\boldsymbol{B}^*$ e ou $\boldsymbol{t}_i$ é $\boldsymbol{0}$ ou $(0, 0, \cdots, 0, -1)$. Então $\boldsymbol{x} = \sum_{i=1}^{k} a_i \boldsymbol{c}_i^* + q(\boldsymbol{s} + \boldsymbol{w} + \sum_{i=1}^{k} \boldsymbol{t}_i)$. Como $\sum_{i=1}^{n} a_i c_i^*$ é par, segue que $(\boldsymbol{s} + \boldsymbol{w} + \sum_{i=1}^{k} \boldsymbol{t}_i) \in D_n$. Notemos que a matriz

$$\boldsymbol{D}^{**} = \begin{pmatrix} q\boldsymbol{I}_{k\times k} & q\boldsymbol{B}^*_{k\times(n-k)} \\ \boldsymbol{0}_{(n-k)\times k} & \boldsymbol{D^*}_{(n-k)\times(n-k)} \end{pmatrix}$$

é uma matriz geradora para o reticulado qD_n. De fato, seja Λ o reticulado gerador por $\boldsymbol{D}^{**}$. É fácil ver que $\Lambda \subseteq qD_n$. Como $2q^n = \det(\Lambda) = q^n \det(D_n)$, então $\Lambda = qD_n$. Logo, $\boldsymbol{x}$ pode ser escrito como $\boldsymbol{x} = \boldsymbol{k}_1[\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}^*_{k\times n-k}] + (\boldsymbol{k}_2{}^{(1)}, \boldsymbol{k}_2{}^{(2)})\boldsymbol{D}^* = (\boldsymbol{k}_1 + q\boldsymbol{k}_2^{(1)}, \boldsymbol{0} + \boldsymbol{k}_2^{(2)})\boldsymbol{N}$. □

Um reticulado obtido pela Construção B em um código q-ário nunca é q-ário pois $q\boldsymbol{e}_i \notin \Lambda_B(\boldsymbol{C})$ para todo $i = 1, \cdots, n$. A proposição seguinte mostra que estes reticulados podem ser vistos como a Construção A de um código $2q$-ário. Estes reticulados são $2q$-ários.

Proposição 3.3.5. *Se $\boldsymbol{C}_1 \subseteq \mathbb{Z}_q^n$ é um código q-ário, então $\Lambda_B(\boldsymbol{C}_1) = \Lambda_A(\boldsymbol{C}_2)$, onde $\boldsymbol{C}_2 \subseteq \mathbb{Z}_{2q}^n$ é o código $2q$-ário associado ao quociente $\Lambda_B(\boldsymbol{C}_1)/2q\mathbb{Z}^n$. Mais ainda, $\boldsymbol{C}_2$ é gerado pelas linhas de uma matriz geradora de $\Lambda_B(\boldsymbol{C}_1)$ reduzindo as entradas módulo $2q$.*

Demonstração: Temos que $2q\mathbb{Z}^n \subseteq \Lambda_B(\boldsymbol{C}_1)$. Note que $\Lambda_B(\boldsymbol{C}_1)/2q\mathbb{Z}^n$ é um grupo e um conjunto de representantes é dado pelos pontos de $\Lambda_B(\boldsymbol{C}_1)$ dentro do hipercubo $[0, 2q)^n$. Este conjunto pode ser identificado com um código $\boldsymbol{C}_2 \subseteq \mathbb{Z}_{2q}^n$. Então $\Lambda_A(\boldsymbol{C}_2) = \Lambda_B(\boldsymbol{C}_1)$. Agora, se $\{\boldsymbol{y}_i,\ i = 1, \cdots, n\}$ é uma base para $\Lambda_B(\boldsymbol{C}_1)$, um conjunto de geradores para $\Lambda_B(\boldsymbol{C}_1)/2q\mathbb{Z}^n$ é dado por $\{\overline{\boldsymbol{y}}_{\boldsymbol{i}},\ i = 1, \cdots, n\}$, onde $\overline{\boldsymbol{y}}_{\boldsymbol{i}}$ é obtido de $\boldsymbol{y}_i$ por reduções módulo $2q$ em cada entrada. □

Observação 3.3.3. *Como $\Lambda_B(\boldsymbol{C})$ é um reticulado inteiro, então ele é um reticulado q^*-ário para $q^* = \det(\Lambda_B(\boldsymbol{C})) = \frac{2q^n}{|\boldsymbol{C}|}$. Se $|\boldsymbol{C}| \leq q^{n-1}$, então a Proposição 3.3.5 descreve um modo econômico de representar $\Lambda_B(\boldsymbol{C})$ como um reticulado q^*-ário. Mais ainda, para $q = 2^r$ temos que $q^* = 2q$ é o q^* mais econômico tal que $\Lambda_B(\boldsymbol{C})$ é um reticulado q^*-ário. De fato, se $\Lambda_B(\boldsymbol{C})$ é q^*-ário, então $q\boldsymbol{e}_i\mathbb{Z}^n \subseteq \Lambda_B(\boldsymbol{C})$ e 2^{r+1} divide $q^*\boldsymbol{e}_i$ para todo $i = 1, \cdots, n$, isto é, $2^{r+1}|q^*$. Então $q^* = 2^{r+1} = 2q$ é o q^* mais econômico.*

3.4 Decodificação de reticulados q-ários via Construção A

Em [23] é apresentada uma relação entre a decodificação dos códigos binários e dos reticulados 2-ários associados pela Construção A na métrica euclidiana. Nesta seção, obtemos uma relação no caso q-ário. Para $\Lambda_A(\boldsymbol{C})$, onde $\boldsymbol{C}$ é um código linear q-ário, mostraremos que decodificar em $\Lambda_A(\boldsymbol{C})$ com a métrica da soma é equivalente a decodificar em $\boldsymbol{C}$ com a métrica de Lee. Os resultados aqui obtidos foram apresentados em [36, 18].

Podemos estudar a decodificação em códigos de formas diferentes. Uma abordagem é considerar o conjunto de vetores recebidos como $S = \mathbb{Z}_q^n$, ou seja, os vetores recebidos têm entradas inteiras reduzidas modulo q. Outra abordagem é definida para $S = [0, q)^n$, ou seja, os vetores recebidos têm entradas reais reduzidas módulo q. Baseados em [23], chamaremos o primeiro tipo de decodificação em códigos de "Hard decoding" e o segundo tipo de "Soft decoding". Nas demonstrações a seguir consideraremos o caso mais geral "Soft decoding".

A fim de melhorar a notação, quando nos referirmos a um vetor $\overline{\boldsymbol{x}}$, estamos considerando-o como ponto do código q-ário $\boldsymbol{C}$, mas quando nos referirmos a $\boldsymbol{x}$, estamos considerando-o como ponto do reticulado q-ário $\Lambda_A(\boldsymbol{C})$. Devido ao isomorfismo $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n \simeq \boldsymbol{C}$, não faremos distinção entre os elementos de $\boldsymbol{C}$ e $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$. Denotaremos por $[a]$ o arredondamento ao inteiro mais próximo de a.

Proposição 3.4.1. *Seja $\Lambda_A(\boldsymbol{C})$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Dado um elemento $\overline{\boldsymbol{x}} \in \Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$ com $\boldsymbol{x} = (x_1, \cdots, x_n)$, o representante $\overline{\boldsymbol{z}}$ da classe $\overline{\boldsymbol{x}}$ que está mais próximo de $\boldsymbol{r}$ em $\Lambda_A(\boldsymbol{C})$, considerando a métrica da soma, é dado por $\boldsymbol{z} = (z_1, \cdots, z_n)$, onde $z_i = x_i + qw_i$ e $w_i = \left[\dfrac{r_i - x_i}{q}\right]$ para cada $i = 1, \cdots, n$.*

Demonstração: Cada representante da classe de $\boldsymbol{x}$ é dado por $\boldsymbol{z} = \boldsymbol{x} + q\boldsymbol{w}$, onde $\boldsymbol{w} \in \mathbb{Z}^n$. Na métrica da soma, $d(\boldsymbol{r}, \boldsymbol{z}) = \sum_{i=1}^{n} |r_i - x_i - qw_i|$ é mínima quando cada parcela do somatório é mínima, isto é, $w_i = \left[\frac{r_i - x_i}{q}\right]$. □

Definição 3.4.1. *Sejam $\Lambda_A(\boldsymbol{C})$ um reticulado q-ário e $\boldsymbol{r} \in \mathbb{R}^n$ um vetor. Chamaremos de $\boldsymbol{r}$ (mod q) o vetor obtido de $\boldsymbol{r}$ por reduções módulo q em cada entrada de $\boldsymbol{r}$. Essas reduções são feitas tomando o resto da divisão de cada entrada de $\boldsymbol{r}$ por q com coeficientes inteiros.*

A próxima proposição relaciona a decodificação no reticulado q-ário $\Lambda_A(\boldsymbol{C})$ na métrica da soma com a decodficação no código q-ário $\boldsymbol{C}$ na métrica de Lee.

Proposição 3.4.2. *Sejam $\Lambda_A(\boldsymbol{C})$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Se $\overline{\boldsymbol{x}} \in \boldsymbol{C}$ é o elemento do código $\boldsymbol{C}$ mais próximo de $\boldsymbol{r}$ (mod q) considerando a métrica de Lee, então $\boldsymbol{z} \in \Lambda_A(\boldsymbol{C})$ dado pela Proposição 3.4.1 tal que $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}}$ em $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$, é um elemento de $\Lambda_A(\boldsymbol{C})$ mais próximo de $\boldsymbol{r}$.*

Demonstração: Seja $\boldsymbol{r}$ (mod q) $= \boldsymbol{r}^*$, isto é, $\boldsymbol{r} = (r_1, \cdots, r_n) = ({r_1}^*, \cdots, {r_n}^*) + q(t_1, \cdots, t_n)$, onde $0 \leq {r_i}^* < q$ e $t_i \in \mathbb{Z}$ para $i = 1, \cdots, n$. Seja $\overline{\boldsymbol{x}} \in \boldsymbol{C}$ com $\boldsymbol{x} = (x_1, \cdots, x_n)$, $0 \leq x_i \leq q-1$ para $i = 1, \cdots, n$, o ponto mais próximo de $\boldsymbol{r}$ (mod q) considerando a métrica de Lee. Mostraremos que o ponto mais próximo de $\boldsymbol{r}$ em $\Lambda_A(\boldsymbol{C})$ está na mesma classe que $\boldsymbol{x}$ em $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$. Para cada classe $\overline{\boldsymbol{a}} \in \boldsymbol{C}$ com $\boldsymbol{a} = (a_1, \cdots, a_n)$, pela Proposição 3.4.1 encontramos o representante $\boldsymbol{a}^*$ mais próximo de $\boldsymbol{r}$ considerando a métrica de Lee. Mostraremos que $\boldsymbol{d}(\boldsymbol{r}, \boldsymbol{a}^*) = d(\boldsymbol{r}$ (mod q), $\overline{\boldsymbol{a}})$. Para a métrica da soma temos

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

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

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

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

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

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

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

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

Assim,

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

Como $\boldsymbol{z}$ é o ponto mais próximo de $\boldsymbol{r}$, então $\overline{\boldsymbol{z}}$ minimiza $d(\boldsymbol{r} \pmod{\text{q}}, \boldsymbol{z})$, isto é, $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}}$. □

Dado $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$, devemos proceder como indicado abaixo para encontrar um ponto de $\Lambda_A(\boldsymbol{C})$ mais próximo de $\boldsymbol{r}$ na métrica da soma:

- Calcular $\boldsymbol{r} \pmod{\text{q}}$ fazendo reduções módulo q em todas as entradas de $\boldsymbol{r}$,
- Como $\boldsymbol{r} \pmod{\text{q}} \in [0, q)^n$, calcular o ponto $\overline{\boldsymbol{x}} = (\overline{x_1}, \cdots, \overline{x_n})$ do código $\boldsymbol{C}$ mais próximo de $\boldsymbol{r} \pmod{\text{q}}$ com a métrica de Lee,
- Para $i = 1, \cdots, n$, calcular $w_i = \left\lceil \frac{r_i - x_i}{q} \right\rceil$ e fazer $\boldsymbol{w} = (w_1, \cdots, w_n)$,
- Tomar $\boldsymbol{z} = (x_1, \cdots, x_n) + q(w_1, \cdots, w_n)$, um ponto mais próximo de $\boldsymbol{r}$ com a métrica da soma.

Exemplo 3.4.1. *Considere o reticulado obtido pela Construção A aplicada no código* 11*-ário*

$$\boldsymbol{C} = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3}), (\overline{2}, \overline{6}), (\overline{3}, \overline{9}), (\overline{4}, \overline{1}), (\overline{5}, \overline{4}), (\overline{6}, \overline{7}), (\overline{7}, \overline{10}), (\overline{8}, \overline{2}), (\overline{9}, \overline{5}), (\overline{10}, \overline{8})\}$$

Dado $\boldsymbol{r} = (0, 8.3) \in \mathbb{Z}^2$, vamos procurar o ponto mais próximo de $\boldsymbol{r}$ em $\Lambda_A(\boldsymbol{C})$ com relação à métrica da soma. A classe de $\boldsymbol{r}$ no quociente $\mathbb{R}/11\mathbb{Z}^2$ é $\boldsymbol{r}$ (mod q) $= (\overline{0}, \overline{8.3})$. O ponto de $\boldsymbol{C}$ mais próximo de $\boldsymbol{r}$ (mod q) com a métrica de Lee é $\overline{\boldsymbol{x}} = (\overline{10}, \overline{8})$. Fazendo $\boldsymbol{z} = (10, 8) + q(w_1, w_2)$, onde $w_1 = \left\lceil \frac{0-10}{11} \right\rceil = -1$ e $w_2 = \left\lceil \frac{8-8}{11} \right\rceil = 0$, temos que $\boldsymbol{z} = (-1, 8)$ é o ponto mais próximo de $\boldsymbol{r}$ com relação à métrica da soma. A Figura 3.10 mostra o reticulado $\Lambda_A(\boldsymbol{C})$ e suas regiões de Voronoi na métrica da soma.

Exemplo 3.4.2. *Considere o código* 13*-ário dado por*

$$\boldsymbol{C} = \{(0,0), (1,5), (2,10), (3,2)(4,7)(5,12), (6,4), (7,9), (8,1), (9,6), (10,11), (11,3), (12,8)\}.$$

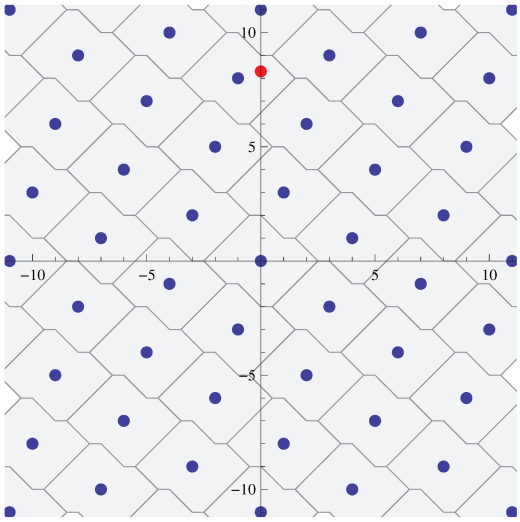


Figura 3.10: $\Lambda_A(\boldsymbol{C})$

Esse código possui distância de Lee mínima $\boldsymbol{d}_{Lee} = 5$. *Dado o ponto* $\boldsymbol{r} = (0, -6)$, *temos que* $\boldsymbol{r}$ *(mod q)* $= (\overline{0}, \overline{7})$ *e o ponto de* $\boldsymbol{C}$ *mais próximo de* $\overline{\boldsymbol{r}}$ *com a métrica de Lee é* $\overline{\boldsymbol{x}} = (\overline{12}, \overline{8})$. *Vamos calcular o vetor* $\boldsymbol{w}$. *Temos que* $w_1 = \left[\frac{0-12}{13}\right] = -1$ *e* $w_2 = \left[\frac{-6-8}{13}\right] = -1$. *Assim,* $\boldsymbol{z} = (12, 8) + 13(-1, -1) = (-1, -5)$. *A Figura 3.11 representa o reticulado* $\Lambda_A(\boldsymbol{C})$, *suas regiões de Voronoi na métrica da soma e o vetor recebido em vermelho.*

Nem todo código q-ário possui um algoritmo eficiente de decodificação com a métrica de Lee. A maioria dos algoritmos conhecidos é do tipo "Hard decoding", ou seja, para decodificar vetores com entradas em $\mathbb{Z}_q^n$. Como exemplo de códigos que posuem algoritmo de decodificação do tipo "Hard decoding" com a métrica de Lee, temos os códigos BCH definidos sobre $\mathbb{Z}_q$, onde q é potência de algum número primo [3, 7] e os códigos negacíclicos [16].

Considerando a decodificação do tipo "Hard decoding" então dentro de cada bola na métrica da soma de raio $t = \lfloor (min\{d_{Lee}, q\} - 1)/2 \rfloor$, centralizada em pontos do reticulado, existem

$$N = \sum_{j=0}^{n} \frac{2^j n! t!}{(n-j)!(t-j)!(j!)^2} \tag{3.7}$$

vetores com entradas inteiras [25]. Assim, o método "Hard decoding" associado a um algoritmo eficiente de decodificação no código $\boldsymbol{C}$ é capaz de recuperar os N pontos da Equação (3.7) decodificando-os como o centro da bola.

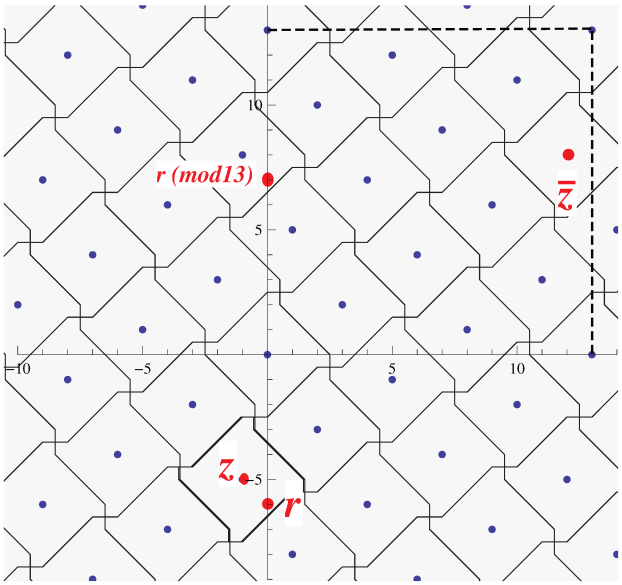


Figura 3.11: $\Lambda_A(\boldsymbol{C})$

Exemplo 3.4.3. *Seja $\boldsymbol{C}$ o código BCH definido em $\frac{\mathbb{Z}_4[x]}{<f(x)>}$, onde $f(x) = x^3 + x + 1$, $\alpha = \beta^2$ com β raiz de $f(x)$ e matriz controle de paridade*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha^5 & \alpha & 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^4 \end{pmatrix}.$$

Uma matriz geradora para tal código em $\mathbb{Z}_4$ é dada por

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

e uma matriz geradora para o reticulado 4-ário $\Lambda = \phi^{-1}(\boldsymbol{C})$ é dada por

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

Seja $\boldsymbol{r} = (0, 7, 4, 8, 0, 12, 0)$ *um vetor recebido. Temos que* $\boldsymbol{r}$ *(mod q)* $= (0, 3, 0, 0, 0, 0, 0)$ *e o ponto de* $\boldsymbol{C}$ *mais próximo de* $\boldsymbol{r}$ *(mod q) segundo a métrica de Lee é* $\overline{\boldsymbol{x}} = (0, 0, 0, 0, 0, 0, 0)$ *[3]. Vamos calcular o vetor* $\boldsymbol{w}$*. Temos que* $w_1 = 0$*,* $w_2 = \left[\frac{7}{4}\right] = 2$*,* $w_3 = \left[\frac{4}{4}\right] = 1$*,* $w_4 = \left[\frac{8}{4}\right] = 2$*,* $w_5 = 0$*,* $w_6 = \left[\frac{12}{4}\right] = 3$ *e* $w_7 = 0$*. Assim,* $\boldsymbol{z} = (0, 0, 0, 0, 0, 0, 0) + 4(0, 2, 1, 2, 0, 3, 0) = (0, 8, 4, 8, 0, 12, 0)$.

A Proposição 3.4.2 pode ser generalizada para a métrica d_p em $\mathbb{R}^n$ com $1 \leq p < \infty$. Para isto, consideremos uma métrica em $[\overline{0}, \overline{q})^n$, induzida da métrica d_p.

Definição 3.4.2. *Dados* $\boldsymbol{a} = (\overline{a_1}, \cdots, \overline{a_n}), \boldsymbol{b} = (\overline{b_1}, \cdots, \overline{b_n}) \in [\overline{0}, \overline{q})^n$*, definimos a métrica*

$$d_{Lee,p}(\boldsymbol{a}, \boldsymbol{b}) = \left(\sum_{i=1}^{n} \left(d_{Lee}(\overline{a_i}, \overline{b_i}) \right)^p \right)^{1/p}.$$

Chamamos $d_{Lee,p}$ *de p-ésima distância de Lee entre* $\boldsymbol{a}$ *e* $\boldsymbol{b}$*.*

Observação 3.4.1. *É fácil ver que* $d_{Lee,p}$ *é uma métrica em* $[\overline{0}, \overline{q})^n$*. A propriedade mais difícil de verificar é a desigualdade triangular. Sejam* $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in [\overline{0}, \overline{q})^n$*. Usando o fato que a métrica de Lee satisfaz a desigualdade triangular, temos que* $d_{Lee}(\overline{a_i}, \overline{b_i}) \leq d_{Lee}(\overline{a_i}, \overline{c_i}) + d_{Lee}(\overline{c_i}, \overline{b_i})$*. Assim, segue que*

$$d_{Lee}(\overline{a_i}, \overline{b_i})^p \leq \left(d_{Lee}(\overline{a_i}, \overline{c_i}) + d_{Lee}(\overline{c_i}, \overline{b_i}) \right)^p.$$

Então

$$d_{Lee,p}(\boldsymbol{a}, \boldsymbol{b}) = \left(\sum_{i=1}^{n} (d_{Lee}(\overline{a_i}, \overline{b_i}))^p \right)^{1/p} \leq \left(\sum_{i=1}^{n} \left(d_{Lee}(\overline{a_i}, \overline{c_i}) + d_{Lee}(\overline{c_i}, \overline{b_i}) \right)^p \right)^{1/p}.$$

Por fim, utilizando a desigualdade de Minkowski, temos que

$$\begin{aligned} d_{Lee,p}(\boldsymbol{a}, \boldsymbol{b}) &= \left(\sum_{i=1}^{n} (d_{Lee}(\overline{a_i}, \overline{b_i}))^p \right)^{1/p} \leq \left(\sum_{i=1}^{n} (d_{Lee}(\overline{a_i}, \overline{c_i}))^p \right)^{1/p} + \left(\sum_{i=1}^{n} (d_{Lee}(\overline{c_i}, \overline{b_i}))^p \right)^{1/p} \\ &= d_{Lee,p}(\boldsymbol{a}, \boldsymbol{c}) + d_{Lee,p}(\boldsymbol{c}, \boldsymbol{b}). \end{aligned}$$

Com isso, podemos enunciar as seguintes proposições cuja demonstração é similar ao caso $p = 1$ estudado acima.

Proposição 3.4.3. *Sejam $\Lambda_A(\boldsymbol{C})$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Dado um elemento $\overline{\boldsymbol{x}} \in \Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$ com $\boldsymbol{x} = (x_1, \cdots, x_n)$, o representante $\overline{\boldsymbol{z}}$ da classe $\overline{\boldsymbol{x}}$ que está mais próximo de $\boldsymbol{r}$ em $\Lambda_A(\boldsymbol{C})$, considerando a métrica d_p, $1 \leq p < \infty$, é dado por $\boldsymbol{z} = (z_1, \cdots, z_n)$, onde $z_i = x_i + qw_i$ e $w_i = \left\lceil \frac{r_i - x_i}{q} \right\rceil$ para cada $i = 1, \cdots, n$.* □

Proposição 3.4.4. *Sejam $\Lambda_A(\boldsymbol{C})$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Se $\overline{\boldsymbol{x}} \in \boldsymbol{C}$ é o elemento do código $\boldsymbol{C}$ mais próximo de $\boldsymbol{r}$ (mod q) considerando a métrica $d_{Lee,p}$, $1 \leq p < \infty$, então $\boldsymbol{z} \in \Lambda_A(\boldsymbol{C})$ dado pela Proposição 3.4.3 tal que $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}}$ em $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$, é um elemento de $\Lambda_A(\boldsymbol{C})$ mais próximo de $\boldsymbol{r}$ na métrica d_p.* □

Pela Proposição (3.4.2), se o reticulado q-ário apresentar um algoritmo eficiente de decodificação na métrica da soma, teremos um algoritmo eficiente de decodificação para o código associado na métrica de Lee. A complexidade de tal algoritmo está relacionada com a complexidade de decodificar o reticulado q-ário com a métrica da soma.

Dado $\boldsymbol{C} \subset \mathbb{Z}_q^n$ um código linear q-ário, podemos proceder da seguinte forma:

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

3.5 Lee Sphere Decoding

No Capítulo 1, apresentamos uma adaptação no algoritmo "Sphere decoding" clássico para ser utilizado na métrica d_p, $1 \leq p < \infty$. Nesta seção, introduzimos algumas simplificações em tal algoritmo no caso de reticulados obtidos de códigos q-ários com q primo via Construções A e B. O que permite tal simplificação é a forma especial das matrizes geradoras de tais reticulados, dadas pelas Equações (3.2) e (3.6). O mesmo resultado pode ser aplicado para outros reticulados que possuem matrizes geradoras semelhantes a estas. Este trabalho

foi desenvolvido em conjunto e consta dos artigos [18, 19]. Estudaremos a decodificação na métrica da soma com $p = 1$. A adaptação do algoritmo para outras métricas d_p é um trabalho em andamento.

3.5.1 Construção A

Quando q é um número primo, pela Equação (3.2), temos que uma matriz geradora do reticulado q-ário $\Lambda_A(\boldsymbol{C})$ na Forma Normal de Hermite é dada por

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{k\times k} & \boldsymbol{B}_{k\times n-k} \\ \boldsymbol{0}_{n-k\times k} & q\boldsymbol{I}_{n-k\times n-k} \end{pmatrix},$$

onde

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

Cada ponto $\boldsymbol{x} \in \Lambda_A(\boldsymbol{C})$ pode ser escrito como $\boldsymbol{x} = \boldsymbol{sH}$ para algum $\boldsymbol{s} \in \mathbb{Z}^n$. Fazendo $\boldsymbol{s} = (\boldsymbol{s}_1, \boldsymbol{s}_2) \in \mathbb{Z}^k \times \mathbb{Z}^{n-k}$, temos que

$$\boldsymbol{sH} = (\boldsymbol{s}_1, \boldsymbol{s}_1\boldsymbol{B} + q\boldsymbol{s}_2).$$

Dado $\boldsymbol{y} \in \mathbb{R}^n$, para decodificar $\boldsymbol{y}$ na métrica da soma, devemos encontrar $\boldsymbol{x}_1 \in \Lambda_A(\boldsymbol{C})$ tal

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

Note que

$$\|\boldsymbol{sH} - \boldsymbol{y}\|_1 = \|\boldsymbol{s}_1 - \boldsymbol{y}_1\|_1 + \|\boldsymbol{s}_1\boldsymbol{B} + q\boldsymbol{s}_2 - \boldsymbol{y}_2\|_1. \tag{3.8}$$

Fixado $\boldsymbol{s}_1 \in \mathbb{Z}^k$, para encontrar $\boldsymbol{s}_2 \in \mathbb{Z}^{n-k}$ que minimiza (3.8), devemos decodificar o vetor $\frac{1}{q}(\boldsymbol{y}_2 - \boldsymbol{s}_1\boldsymbol{B})$ em $\mathbb{Z}^{n-k}$. Essa é a idéia geral do algoritmo: primeiro, vamos encontrar $\boldsymbol{s}_1$ e a partir de $\boldsymbol{s}_1$ encontraremos $\boldsymbol{s}_2$. Essa maneira de resolver o problema só é possível pela forma especial da matriz $\boldsymbol{H}$.

O algoritmo atua de forma similar ao apresentado no Capítulo 1, possuindo algumas simplificações. Dado um raio $\boldsymbol{R}$, encontramos vetores $\boldsymbol{s} \in \mathbb{Z}^n$ satisfazendo $||\boldsymbol{sH} - \boldsymbol{y}||_1 \leq \boldsymbol{R}$,

isto é,

$$\sum_{i=1}^{k} |s_i - y_i| + \left| \sum_{i=1}^{k} b_{i,k+1} s_i + s_{k+1} q - y_{k+1} \right| + \cdots + \left| \sum_{i=1}^{k} b_{i,n} s_i + s_n q - y_n \right| \leq \boldsymbol{R}. \qquad (3.9)$$

Para as k primeiras parcelas da soma em (3.9), procederemos como no caso estudado no Capítulo 1. Para $k = 1$, temos a seguinte variação:

$$\lceil -\boldsymbol{R} + y_1 \rceil \leq s_1 \leq \lfloor \boldsymbol{R} + y_1 \rfloor.$$

Para $j = 2, \cdots, k$, fixados valores para $s_1, \cdots, s_{j-1}$, e fazendo $R_j = R_{j-1} - |s_{j-1} - y_{j-1}|$, temos a seguinte variação:

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

Para $j > k$, não precisamos calcular todas as possibilidades de valores para $\boldsymbol{s}_2 = (s_{k+1}, \cdots, s_n)$ em $\mathbb{Z}^{n-k}$ e é esse fato que introduz as simplificações no algoritmo.

Para cada vetor $\boldsymbol{s}_1$ listado acima, temos que o vetor $\boldsymbol{s}_2$ que minimiza (3.8) é o vetor inteiro mais próximo de $\frac{1}{q}(-\boldsymbol{s}_1\boldsymbol{B} + \boldsymbol{y}_2)$, que é dado por

$$s_j = \left\lceil \frac{-\sum_{i=1}^{k} r_{i,j} s_i + y_j}{q} \right\rfloor \quad \text{onde} \quad j = k+1, \cdots, n.$$

Note que só podemos fazer tal simplicação pois em (3.9) os útimos $n-k$ termos da soma são independentes entre si e fixado $\boldsymbol{s}_1$, minimizar $||\boldsymbol{s}\boldsymbol{H} - \boldsymbol{y}||_1$ é equivalente a minimizar cada parcela do somatório (3.9).

Nem todo ponto $\boldsymbol{x} = \boldsymbol{s}\boldsymbol{H}$ gerado pelo algoritmo satisfaz $||\boldsymbol{s}\boldsymbol{H} - \boldsymbol{y}||_1 \leq \boldsymbol{R}$. Após gerarmos $\boldsymbol{s}_1$, para cada coordenada s_j de $\boldsymbol{s}_2$ gerada, podemos testar se

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

Se a desigualdade não for satisfeita com este valor de s_j, não será satisfeita com nenhum outro valor, pois este é o inteiro que minimiza o valor da parcela em que s_j aparece. Portanto, se a desigualdade for satisfeita, continuamos testando os outros coeficientes. Como $t_{j+1} = t_j + \left| \sum_{i=1}^{k} r_{i,j+1} s_i + s_{j+1} q - y_{j+1} \right|$, podemos guardar este valor para economizar os passos do algoritmo.

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

Para a métrica da soma, chamamos o algoritmo de *Lee sphere decoding*.

O número de caminhos $\upsilon(k, \boldsymbol{R})$ no nível k pode ser estimado pela quantidade de vetores inteiros na esfera k-dimensional centralizada em $\boldsymbol{y}_1$ com raio $\boldsymbol{R}$. Para a métrica da soma, este número pode ser estimado pela quantidade de vetores inteiros na esfera de Lee de raio $\boldsymbol{R}$ centralizada em um vetor com entradas inteiras [58], isto é,

$$\upsilon(k, \boldsymbol{R}) = \sum_{i=0}^{min\{k,\boldsymbol{R}\}} 2^i \binom{k}{i} \binom{\boldsymbol{R}}{i}. \tag{3.10}$$

A partir do índice k, o número de caminhos ou permanece igual ao número de caminhos no índice k ou diminui. Com isso, (3.10) é um limitante superior para o número de caminhos visitados pelo algoritmo na métrica da soma. Para $k << n$, com as simplificações feitas acima, obtemos uma considerável redução no número de pontos gerados, pois $\upsilon(k, \boldsymbol{R}) << \upsilon(n, \boldsymbol{R})$.

O número de nós visitados pelo algoritmo é dado pela soma do número de nós visitados em cada nível.

Proposição 3.5.1. *Se o vetor recebido $\boldsymbol{y}$ é tal que $(r_1, \ldots, r_k) \in \mathbb{Z}^k$, então o número de nós visitados pelo algoritmo na métrica da soma até o nível k é*

$$\sum_{j=1}^{k} \sum_{i=0}^{\min\{j,R\}} 2^i \binom{j}{i} \binom{R}{i}. \tag{3.11}$$

Demonstração: Segue do fato que em cada nível j o número de nós visitados é a quantidade de vetores inteiros na esfera da soma de raio $\boldsymbol{R}$ dada por (3.10). □

Proposição 3.5.2. *[18] Sejam $\boldsymbol{H}$ a matriz geradora $\Lambda_A(C)$ como acima, $\boldsymbol{y}$ um vetor e R a estimativa de Babai para o raio. Temos que*

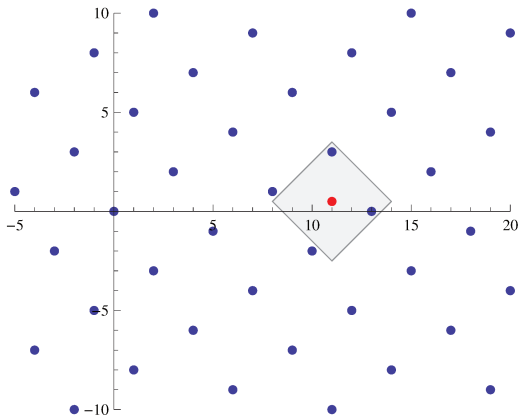
$$R \leq \min\left\{ \frac{n}{2} \max\{q, \|B\|\} + \frac{k}{2},\ \frac{n}{2} \max\{1 + \|B\|, q\} \right\},$$

onde $\|B\| = \max_i \sum_{j=0}^{n} |b_{ij}|$ é a norma usual l_1 para matriz. □

Como é inerente ao problema de decodificação de reticulados, o algoritmo "Lee sphere decoding" tem alta complexidade computacional. Para reticulados q-ários com $k << n$ estabelecemos algumas simplificações a fim de reduzir o número de passos necessários para a decodificação.

O problema de decodificar um reticulado q-ário n-dimensional, q primo, possui sua complexidade ligada a k, que é justamente a dimensão do código q-ário associado ao reticulado pela Construção A.

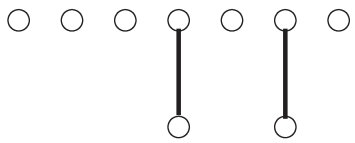
Exemplo 3.5.1. *O reticulado* 13*-ário com base* $\{(1,5),(0,13)\}$ *é ilustrado na figura abaixo.*



Seja $\boldsymbol{y} = (11, 0.5)$ *um vetor recebido. Pela estimativa de Babai, temos que* $\boldsymbol{R} = 3$. *Assim, queremos encontrar* $\boldsymbol{s} = (s_1, s_2) \in \mathbb{Z}^2$ *tal que* $|s_1 - 11| + |5s_1 + 13s_2 - 0.5| \leq 3$. *Para* s_1 *temos como possibilidades os inteiros no intervalo* $8 \leq s_1 \leq 14$. *Para cada* $\boldsymbol{s}_1$ *vamos procurar se existe* $\boldsymbol{s}_2$.

$$\begin{cases} s_1 = 8 \Longrightarrow s_2 = -3 \text{ não satisfaz a desigualdade} \\ s_1 = 9 \Longrightarrow s_2 = -3 \text{ não satisfaz a desigualdade} \\ s_1 = 10 \Longrightarrow s_2 = -4 \text{ não satisfaz a desigualdade} \\ s_1 = 11 \Longrightarrow s_2 = -4 \text{ satisfaz a desigualdade} \\ s_1 = 12 \Longrightarrow s_2 = -5 \text{ não satisfaz a desigualdade} \\ s_1 = 13 \Longrightarrow s_2 = -5 \text{ satisfaz a desigualdade} \\ s_1 = 14 \Longrightarrow s_2 = -5 \text{ não satisfaz a desigualdade} \end{cases}$$

Portanto, a partir dos pontos factíveis, obtemos os pontos $\boldsymbol{sH}$ *na esfera centrada em* $\boldsymbol{y}$ *com raio* 3 *que são:* $(11, 3), (13, 0)$.

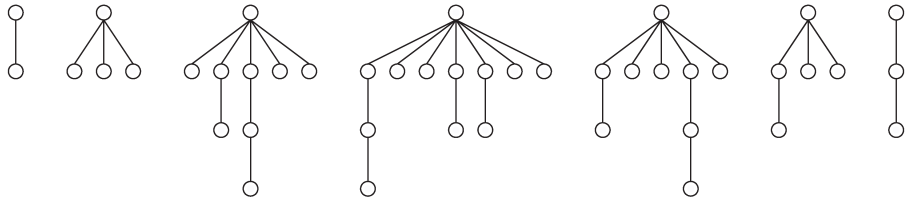


Neste caso, o ponto mais próximo do vetor recebido é o ponto $(13, 0)$ *e como a árvore não possui entrelaçamentos, não economizamos passos no cálculo da distância de cada ponto a* $\boldsymbol{y}$*. Existem dois pontos factíveis e o algoritmo visita* 9 *nós.*

Exemplo 3.5.2. *Sejam o reticulado* 7*-ário com matriz geradora dada por*

$$\begin{pmatrix} 1 & 0 & 5 & 3 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}$$

e $\boldsymbol{y} = (1, 1, 1, 1)$ *um vetor recebido. Por Babai, temos que* $\boldsymbol{R} = 3$*. A figura abaixo mostra a árvore correspondente ao algoritmo para* $\boldsymbol{y} = (1, 1, 1, 1)$ *e* $\boldsymbol{R} = 3$*.*



Os 3 *pontos factíveis são* $(0, 1, 2, 1)$*,* $(1, -2, 1, 1)$ *e* $(2, 2, 0, 1)$*. O ponto mais próximo de* y *é* $(0, 1, 2, 1)$*.*

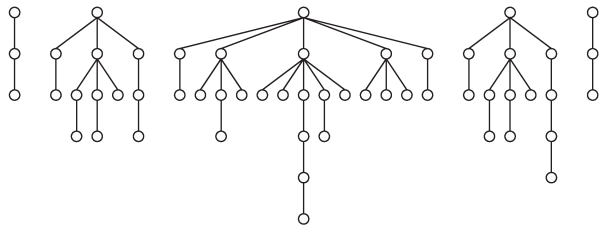
Observação 3.5.1. *Estamos utilizando como raio da esfera na métrica da soma o raio* $\boldsymbol{R}$ *dado pela estimativa de Babai. Como dissemos no Capítulo 1, o raio mais adequado seria o raio de cobertura, que é difícil de ser calculado em um reticulado qualquer. Para reticulados q-ários com a métrica da soma, seria natural pensar num limitante superior para o raio de*

cobertura como $\boldsymbol{R} = q$*. Mas para dimenões maiores que* 2*, este raio pode não funcionar, como veremos no exemplo seguinte.*

Exemplo 3.5.3. *Considere o código* $\boldsymbol{C} = \{\overline{\mathbf{0}}\} \subseteq \mathbb{Z}_q^n$ *para* $n \geq 3$*. Temos que* $\phi^{-1}(\boldsymbol{C}) = q\mathbb{Z}^n$*. Para o ponto* $\boldsymbol{y} = (q/2, \cdots, q/2) \in \mathbb{R}^n$*, temos que* $B[\boldsymbol{y}, q] \cap \Lambda_A(\boldsymbol{C}) = \emptyset$*, pois* $d(\boldsymbol{y}, \boldsymbol{x}) = n\, q/2 > q$ *para todo* $\boldsymbol{x} \in q\mathbb{Z}^n \cap [0, q]^n$ *(os cantos da caixa). Portanto,* q *não pode ser utilizado como raio de cobertura.*

Pelo exemplo acima temos que um limitante superior para o raio de cobertura na métrica de Lee é $\boldsymbol{R} = \dfrac{n\, q}{2}$, o qual aumenta consideravelmente à medida em que n aumenta.

Exemplo 3.5.4. *Seja* $\boldsymbol{C}$ *o código BCH dado no Exemplo 3.4.3. Seja* $\boldsymbol{y} = (1, 1, 1, 5, 2, 3, 5)$ *um vetor recebido. Pela estimativa de Babai,* $\boldsymbol{R} = 2$*. A figura seguinte representa os pontos gerados pelo algoritmo "Lee sphere decoding". O ponto mais próximo de* $\boldsymbol{y}$ *em* $\Lambda_A(C)$ *é* $\boldsymbol{z} = (1, 1, 1, 6, 2, 3, 6)$.



3.5.2 Construção B

Quando q é um número primo, pela Equação (3.6), temos que uma matriz geradora de um reticulado q-ário $\Lambda_B(\boldsymbol{C})$ é dada por

$$\boldsymbol{N} = \begin{pmatrix} \boldsymbol{I}_{k\times k} & \boldsymbol{B}^*{}_{n\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & \boldsymbol{D}^*_{(n-k)\times(n-k)} \end{pmatrix},$$

onde $(\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}_{k\times n-k})$ é uma matriz geradora para o código q-ário $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ e

$$\boldsymbol{D}^* = \begin{pmatrix} q & -q & 0 & \cdots & 0 & 0 \\ 0 & q & -q & \cdots & 0 & 0 \\ 0 & 0 & q & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q & -q \\ 0 & 0 & 0 & \cdots & & 2q \end{pmatrix}.$$

Cada ponto $\boldsymbol{x} \in \Lambda_B(\boldsymbol{C})$ pode ser escrito como $\boldsymbol{x} = \boldsymbol{sN}$ para algum $\boldsymbol{s} \in \mathbb{Z}^n$. Fazendo $\boldsymbol{s} = (\boldsymbol{s}_1, \boldsymbol{s}_2) \in \mathbb{Z}^k \times \mathbb{Z}^{n-k}$, temos que

$$\boldsymbol{sN} = (\boldsymbol{s}_1, \boldsymbol{s}_1\boldsymbol{B}^* + q\boldsymbol{s}_2\boldsymbol{D}),$$

onde

$$\boldsymbol{D} = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & 0 & \cdots & & 2 \end{pmatrix}$$

é uma matriz geradora do reticulado D_{n-k} (1.4).

Dado $\boldsymbol{y} \in \mathbb{R}^n$, note que

$$\|\boldsymbol{sN} - \boldsymbol{y}\|_1 = \|\boldsymbol{s}_1 - \boldsymbol{y}_1\|_1 + \|\boldsymbol{s}_1\boldsymbol{B}^* + q\boldsymbol{s}_2\boldsymbol{D} - \boldsymbol{y}_2\|_1. \tag{3.12}$$

Fixado $\boldsymbol{s}_1 \in \mathbb{Z}^k$, para encontrar $\boldsymbol{s}_2 \in \mathbb{Z}^{n-k}$ que minimiza (3.12), devemos decodificar o vetor $\frac{1}{q}(-\boldsymbol{s}_1\boldsymbol{B}^* + \boldsymbol{y}_2)$ em D_{n-k}. Essa é a idéia geral do algoritmo: primeiro, vamos encontrar $\boldsymbol{s}_1$ e a partir de $\boldsymbol{s}_1$ encontrarmos $\boldsymbol{s}_2$. Essa maneira de resolver o problema só é possível pela forma especial da matriz $\boldsymbol{N}$.

O algoritmo atua de forma similar ao apresentado para Construção A. Dado um raio $\boldsymbol{R}$,

vamos encontrar todos os vetores inteiros $\boldsymbol{s} \in \mathbb{Z}^n$ satisfazendo $||\boldsymbol{sN} - \boldsymbol{y}||_1 \leq \boldsymbol{R}$, isto é,

$$\sum_{i=1}^{k} |s_i - y_i| + \left|\sum_{i=1}^{k} b^*_{i,k+1} s_i + s_{k+1}q - y_{k+1}\right| + \left|\sum_{i=1}^{k} b^*_{i,k+2} s_i - s_{k+1}q + s_{k+2}q - y_{k+2}\right| + \cdots + \left|\sum_{i=1}^{k} b^*_{i,n} s_i - s_{n-1}q + s_n 2q - y_n\right| \leq \boldsymbol{R}. \tag{3.13}$$

Para as k primeiras parcelas da soma em (3.9), procederemos como no caso anterior. Para $k = 1$, temos a seguinte variação:

$$\lceil -\boldsymbol{R} + y_1 \rceil \leq s_1 \leq \lfloor \boldsymbol{R} + y_1 \rfloor.$$

Para $j = 2, \cdots, k$, fixados valores para $s_1, \cdots, s_{j-1}$, e fazendo $R_j = R_{j-1} - |s_{j-1} - y_{j-1}|$, temos a seguinte variação:

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

Para $j > k$, não precisamos calcular todas as possibilidades de valores para $\boldsymbol{s}_2 = (s_{k+1}, \cdots, s_n)$ em $\mathbb{Z}^{n-k}$, sendo esse fato que introduz simplificações no algoritmo.

Para cada vetor $\boldsymbol{s}_1$ listado acima, temos que o vetor $\boldsymbol{s}_2$ que minimiza (3.12) é o vetor de D_{n-k} mais próximo de $\frac{1}{q}(-\boldsymbol{s}_1\boldsymbol{B}^* + \boldsymbol{y}_2)$. Para calcular tal vetor devemos proceder como na decodificação em D_n [23], que é feita da seguinte forma: primeiro decodificamos o vetor $\boldsymbol{s}_2$ em $\mathbb{Z}^{n-k}$ tomando

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

Se $\sum_{j=k+1}^{n} s_j$ for par, então $\boldsymbol{s}_2 \in D_{n-k}$. Caso contrário, calculamos os erros

$$e_j = \frac{-\sum_{i=1}^{k} r_{i,j} s_i + y_j}{q} - \left\lceil \frac{-\sum_{i=1}^{k} r_{i,j} s_i + y_j}{q} \right\rfloor, \ j = k+1, \cdots, n$$

e encontramos o índice i tal que $|e_i| \geq |e_j|$ para todo j. A seguir, substituímos s_i por $s_i + 1$ se $e_i \geq 0$ ou por $s_i - 1$ se $e_i < 0$. O novo vetor $\boldsymbol{s}_2$ está em D_{n-k}.

Nem todo ponto $\boldsymbol{x} = \boldsymbol{sN}$ gerado pelo algoritmo satisfaz $\|\boldsymbol{sN} - \boldsymbol{y}\|_1 \leq \boldsymbol{R}$. Após gerarmos $\boldsymbol{s}_1$ para cada coordenada s_j de $\boldsymbol{s}_2$, gerada podemos testar se

$$t_j = \|(\boldsymbol{s}_1, s_{k+1}, \cdots, s_j)\boldsymbol{N}_{j\times n} - (y_1, \cdots, y_j)\|_1 \leq \boldsymbol{R}.$$

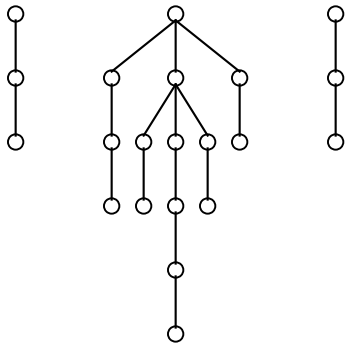


Figura 3.12: $\boldsymbol{y} = (1, 0, 0, 5, 1, 1, 3)$ e $R = 1$

Se a desigualdade não for satisfeita com este valor de s_j, não será satisfeita com nenhum outro valor, pois este é o inteiro que minimiza o valor da parcela em que s_j aparece. Portanto, se a desigualdade for satisfeita continuamos testando os outros coeficientes.

Observação 3.5.2. *Dado um código linear q-ário $\boldsymbol{C}$, o desenho das árvores para um vetor recebido $\boldsymbol{y}$ e um raio $\boldsymbol{R}$ é o mesmo para $\Lambda_A(\boldsymbol{C})$ e $\Lambda_B(\boldsymbol{C})$. A diferença em cada caminho da árvore acontece no máximo em um coeficiente a partir do índice k.*

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

Exemplo 3.5.5. *Seja $\boldsymbol{C}$ o código BCH dado no Exemplo 3.4.3, $\boldsymbol{y} = (1, 0, 0, 5, 1, 1, 3)$ um vetor recebido e $R = 1$. A Figura 3.5.5 representa a árvore de pontos gerados pelo algoritmo para decodificar em $\Lambda_B(\boldsymbol{C})$ na métrica da soma.*

3.6 Uma extensão de reticulados q-ários

Neste seção, definiremos uma classe de reticulados que é uma extensão natural das construções feitas para reticulados q-ários a qual pode ser interessante em algumas aplicações.

Definição 3.6.1. *Sejam $q_1, \ldots, q_m \in \mathbb{N}$ e o anel $\boldsymbol{A} = \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$. Dizemos que $\boldsymbol{C} \subseteq \boldsymbol{A}$ é um código $(q_1, \cdots, q_m)$-ário se $\boldsymbol{C}$ é um subgrupo aditivo de $\boldsymbol{A}$.*

Definição 3.6.2. *Dizemos que* $\boldsymbol{M}$ *é uma matriz geradora para um código* $(q_1, \cdots, q_m)$*-ário* $\boldsymbol{C}$*, se as linhas de* $\boldsymbol{M}$ *constituem um conjunto de geradores para* $\boldsymbol{C}$*.*

Exemplo 3.6.1. *Considere o anel* $\boldsymbol{A} = \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3$*. Temos que* $\boldsymbol{C} = \{(0,0,0), (1,2,0), (0,4,0), (1,1,0), (0,3,0), (1,0,0), (0,2,0), (1,4,0), (0,1,0), (1,3,0), (0,0,0)\}$ *é um código* $(2,5,3)$*-ário com* 11 *vetores. Uma matriz geradora para* $\boldsymbol{C}$ *é dada por*

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

Definição 3.6.3. *Sejam* $q_1, \cdots, q_m \in \mathbb{N}$*. Chamamos de* **Construção A** *a aplicação*

$$\phi : \mathbb{Z}^m \longrightarrow \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$$

$$(a_1, \cdots, a_m) \longmapsto (a_1 \ (mod\ q_1), \cdots, , a_m \ (mod\ q_m))$$

Temos que $\boldsymbol{C} \subset \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$ é um código $(q_1, \cdots, q_m)$-ário se, e somente se, $\Lambda_A(\boldsymbol{C}) = \phi^{-1}(\boldsymbol{C})$ é um reticulado em $\mathbb{R}^m$. Este reticulado será chamado de **reticulado** $(q_1, \cdots, q_m)$**-ário**. Além disso, $q_1\mathbb{Z} \times \cdots \times q_m\mathbb{Z}$ é um sub-reticulado ortogonal de $\Lambda_A(\boldsymbol{C})$.

Geometricamente, um reticulado $(q_1, \cdots, q_m)$-ário é obtido como translações dos pontos do código $\boldsymbol{C}$ dentro do hiper-retângulo $[0, q_1) \times \cdots \times [0, q_m)$ em direções que são combinações lineares inteiras mútiplas de $(0, \cdots, 0, q_i, 0, \cdots, 0)$ para $i = 1, \cdots, m$.

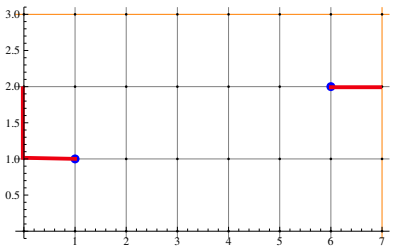
Definição 3.6.4. *Sejam* $q_1, \cdots, q_m \in \mathbb{N}$*. Dados dois vetores* $\boldsymbol{a} = (a_1, \cdots, a_m), \boldsymbol{b} = (b_1, \cdots, b_m) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$*, definimos a* **distância de Lee** *entre* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *por*

$$d_{Lee}(\boldsymbol{a}, \boldsymbol{b}) = d_{Lee}^{q_1}(a_1, b_1) + \cdots + d_{Lee}^{q_m}(a_m, b_m),$$

onde $d_{Lee}^{q_i}(a_i, b_i) = min\{|a_i - b_i|, q_i - |a_i - b_i|\}$*.*

Geometricamente, considere o hiper-retângulo $[0, q_1) \times \cdots \times [0, q_m)$ com lados opostos identificados. A distância de Lee entre dois pontos é o menor números de arestas ligando tais pontos.

Exemplo 3.6.2. *Sejam* $(1,1), (6,2) \in \mathbb{Z}_7 \times \mathbb{Z}_3$*. Temos que* $d_{Lee}((1,1),(6,2)) = min\{5,2\} + min\{1,2\} = 3$*.*



Proposição 3.6.1. *Se $\boldsymbol{d}_{Lee}$ é a distância mínima de Lee em $\boldsymbol{C}$, então a distância mínima da soma em $\Lambda_A(\boldsymbol{C})$ é dada por $\rho = min\{\boldsymbol{d}_{Lee}, q_1, \cdots, q_m\}$.* □

Sejam $\Lambda_A(\boldsymbol{C})$ um reticulado $(q_1, \cdots, q_m)$-ário e $\Lambda^\sharp = q_1\mathbb{Z} \times \cdots \times q_m\mathbb{Z}$ seu sub-reticulado ortogonal. Não faremos distinção entre os elementos de $\boldsymbol{C}$ e $\Lambda_A(\boldsymbol{C})/\Lambda^\sharp$ e denotaremos por $[a]$ o arredondamento ao inteiro mais próximo de a.

Proposição 3.6.2. *Seja $\Lambda_A(\boldsymbol{C})$ um reticulado $(q_1, \cdots, q_m)$-ário e $\boldsymbol{r} = (r_1, \cdots, r_m) \in \mathbb{R}^m$ um vetor recebido. Dado um elemento $\overline{\boldsymbol{x}} \in \Lambda_A(\boldsymbol{C})/\Lambda^\sharp$ com $\boldsymbol{x} = (x_1, \cdots, x_m)$, o representante da classe $\overline{\boldsymbol{x}}$ que está mais próximo de $\boldsymbol{r}$ em $\Lambda_A(\boldsymbol{C})$, considerando a métrica da soma, é dado por $\boldsymbol{z} \in \Lambda$ com $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}}$, onde $\boldsymbol{z} = \boldsymbol{x} + q_1(w_1, 0, \cdots, 0) + \cdots + q_m(0, \cdots, 0, w_m)$ e $w_i = \left[\dfrac{r_i - x_i}{q_i}\right]$ para cada $i = 1, \cdots, m$.*

Demonstração: A demonstração é essencialmente a que foi feita na Proposição 3.4.1, exceto que um representante da classe de $\boldsymbol{x}$ no quociente $\Lambda_A(\boldsymbol{C})/\Lambda^\sharp$ é dado por $\boldsymbol{z} = \boldsymbol{x} + q_1(w_1, 0, \cdots, 0) + \cdots + q_m(0, \cdots, 0, w_m)$, onde $w_i \in \mathbb{Z}$ para todo $i = 1, \cdots, m$. Assim, a métrica da soma satisfaz $d(\boldsymbol{r}, \boldsymbol{z}) = |r_1 - x_1 - q_1w_1| + \cdots + |r_m - x_m - q_mw_m|$, sendo mínima quando $w_i = \left[\frac{r_i - x_i}{q_i}\right]$. □

Definição 3.6.5. *Sejam $\Lambda_A(\boldsymbol{C})$ um reticulado $(q_1, \cdots, q_m)$-ário, $\Lambda^\sharp = q_1\mathbb{Z} \times \cdots \times q_m\mathbb{Z}$ sub-reticulado ortogonal e $\boldsymbol{r} = (r_1, \cdots, r_m) \in \mathbb{R}^m$. Chamaremos de $\boldsymbol{r}$ (mod $\Lambda^\sharp$) o vetor obtido de $\boldsymbol{r}$ por reduções módulo q_i em cada entrada de r_i. Essas reduções são feitas tomando o resto da divisão inteira de cada entrada r_i de $\boldsymbol{r}$ por q_i.*

Proposição 3.6.3. *Sejam $\Lambda_A(C)$ um reticulado $(q_1, \cdots, q_m)$-ário, $\Lambda^\sharp = q_1\mathbb{Z} \times \cdots \times q_m\mathbb{Z}$ e $\boldsymbol{r} = (r_1, \cdots, r_m) \in \mathbb{R}^m$ um vetor recebido. Se $\boldsymbol{x} \in \boldsymbol{C}$ é o elemento do código mais próximo de $\boldsymbol{r}$ (mod $\Lambda^\sharp$) considerando a métrica de Lee, então $\boldsymbol{z} \in \Lambda_A(\boldsymbol{C})$ dado pela Proposição 3.6.2 tal que $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}}$ em $\Lambda_A(\boldsymbol{C})/\Lambda^\sharp$ é um elemento de $\Lambda_A(C)$ mais próximo de $\boldsymbol{r}$.*

Demonstração: A demonstração é similar a da Proposição 3.4.2. □

CAPÍTULO 4

RETICULADOS ALGÉBRICOS

Neste capítulo, vamos utilizar técnicas algébricas para gerar reticulados no $\mathbb{R}^n$, a saber o homomorfismo de Minkowski [57] e o homomorfismo torcido [10]. Estes homomorfismos relacionam $\mathbb{Z}$-módulos de um corpo de números $\mathbb{K}$ de grau n com reticulados no $\mathbb{R}^n$. Com essa identificação, muitas propriedades dos reticulados podem ser estudadas via propriedades dos corpos de números, que possuem uma estrutura algébrica mais rica. Algumas das propriedades mais estudadas em reticulados são a densidade de empacotamento na métrica euclidiana [23], a diversidade e a distância produto mínima [17]. A densidade de empacotamento na métrica euclidiana está relacionada com a eficiência na transmissão de sinais mapeados com pontos do reticulado em canais gaussianos [17]. A diversidade e a distância produto mínima estão associadas a eficiência na transmissão de sinais mapeados com pontos do reticulado em canais do tipo Rayleigh com desvanecimento [17]. Tendo em vista construir reticulados que possam ser utilizados simultaneamente em ambos canais (gaussiano e do tipo Rayleigh com desvanecimento), reproduzimos algumas famílias de reticulados D_n-rotacionados para $n = \frac{p-1}{2}$, com p primo e $p \geq 7$ ou $n = 2^{r-2}$ para $r \geq 5$. Estas construções foram feitas a partir de construções de reticulados $\mathbb{Z}^n$-rotacionados [4, 13, 14]. Para o caso $n = (p-1)/2$ com p primo, os reticulados D_n-rotacionados foram construídos via $\mathbb{Z}$-módulos de posto n que não são ideais. Mostramos que é impossível reproduzir os reticulados D_3 e D_5 via ideais no subcorpo real maximal dos corpos ciclotômicos. Para o caso $n = 2^{r-2}$, os reticulados

D_n-rotacionados foram construídos via ideais.

Um estudo detalhado da teoria aqui utilizada pode ser encontrado em [57, 61, 67, 53, 54, 10, 51].

4.1 Corpo de Números

Esta seção apresenta um resumo de conceitos e resultados necessários para as técnicas aqui abordadas.

Definição 4.1.1. *Sejam* $\mathbb{K}$, $\mathbb{L}$ *corpos. Dizemos que* $\mathbb{L}$ *é uma* **extensão** *de* $\mathbb{K}$ *se* $\mathbb{K} \subset \mathbb{L}$ *e denotamos tal extensão por* $\mathbb{K} \subseteq \mathbb{L}$ *ou* $\mathbb{L}|\mathbb{K}$.

Observação 4.1.1. *Se* $\mathbb{K} \subset \mathbb{L}$ *uma extensão de corpos, é fácil verificar que* $\mathbb{L}$ *é um espaço vetorial sobre* $\mathbb{K}$.

Definição 4.1.2. *Seja* $\mathbb{K} \subset \mathbb{L}$ *uma extensão de corpos. A dimensão do* $\mathbb{K}$*-espaço vetorial* $\mathbb{L}$*, denotada por* $[\mathbb{L} : \mathbb{K}]$*, é chamada de* **grau da extensão**.

Exemplo 4.1.1. *Considere o corpo* $\mathbb{K} = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$. *Temos que* $\mathbb{Q} \subseteq \mathbb{K}$ *é uma extensão de corpos de grau* $[\mathbb{K} : \mathbb{Q}] = 2$, *pois* $\{1, \sqrt{2}\}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$.

Teorema 4.1.1. *[57] Se* $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ *são corpos, então* $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$. □

Definição 4.1.3. *Sejam* $\mathbb{K} \subset \mathbb{L}$ *corpos. Um elemento* $\alpha \in \mathbb{L}$ *é chamado de* **algébrico** *sobre* $\mathbb{K}$ *se existe um polinômio não nulo* $f(x) \in \mathbb{K}[x]$ *tal que* $f(\alpha) = 0$. *O polinômio mônico de menor grau* $f(x)$ *tal que* $f(\alpha) = 0$, *é chamado de* **polinômio minimal** *de* α *sobre* $\mathbb{K}$ *e é denotado por* $min_{\mathbb{K}}\alpha$.

Definição 4.1.4. *Um* **corpo de números** $\mathbb{K}$ *é uma extensão finita de* $\mathbb{Q}$. *Denotamos por* $\mathbb{K}(\theta)$ *o menor corpo contendo o corpo* $\mathbb{Q}$ *e o elemento* θ.

Proposição 4.1.1. *[57] Se* $\mathbb{K}$ *é um corpo de números, existe* $\theta \in \mathbb{L}$ *tal que* $\mathbb{L} = \mathbb{K}(\theta)$ *e* $[\mathbb{L} : \mathbb{K}] =$ *grau* $(min_{\mathbb{K}}\theta)$. □

Definição 4.1.5. *Seja* $\mathbb{K}$ *um corpo de números. Dizemos que um elemento* $\alpha \in \mathbb{K}$ *é um* **inteiro algébrico** *sobre* $\mathbb{Z}$ *se* α *é raiz de um polinômio mônico com coeficientes em* $\mathbb{Z}$.

Exemplo 4.1.2. *Considere a extensão $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. Temos que $\sqrt{2}$ é inteiro algébrico, pois é raiz de $f(x) = x^2 - 2$, já $1/2$ não é inteiro algébrico.*

Proposição 4.1.2. *[57] Seja $\mathbb{K}$ um corpo de números. O conjunto*

$$\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K};\ x \text{ é inteiro algébrico sobre } \mathbb{Z}\}$$

é um anel, chamado de **anel de inteiros** *de $\mathbb{K}|\mathbb{Q}$.* □

Exemplo 4.1.3. *Para o corpo $\mathbb{K} = \mathbb{Q}(i)$, temos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ é seu anel de inteiros.*

Proposição 4.1.3. *[57] Se $\mathbb{K}$ é um corpo de números de grau n, então todo ideal $I \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto $\boldsymbol{n}$. Em particular, quando $I = \mathcal{O}_{\mathbb{K}}$, chamamos a $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ de* **base integral**. □

Definição 4.1.6. *Seja $\mathbb{K}$ um corpo de números. Dizemos que $I \subseteq \mathbb{K}$ é um* **ideal fracionário** *se I é um $\mathcal{O}_{\mathbb{K}}$-módulo e existe $d \in \mathcal{O}_{\mathbb{K}} - \{0\}$ tal que $d\ I \subseteq \mathcal{O}_{\mathbb{K}}$. Em particular, os ideais do anel $\mathcal{O}_{\mathbb{K}}$ são ideais fracionários.*

Proposição 4.1.4. *[57] Todo ideal fracionário I de um corpo de números $\mathbb{K}$ de grau n é um $\mathbb{Z}$-módulo livre de posto n.* □

Lema 4.1.1. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Se $I \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo de posto n, existe $d \in \mathbb{Z} - \{0\}$ tal que $dI \subset \mathcal{O}_{\mathbb{K}}$.*

Demonstração: Como $\mathbb{K}$ é um corpo de números de grau n, temos que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$ e $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Como I é um $\mathbb{Z}$-módulo livre de posto n, seja $\{\gamma_1, \cdots, \gamma_n\}$ uma $\mathbb{Z}$-base de I. Para cada i, temos que $\gamma_i = \sum_{j=0}^{n-1} a_{ij}\alpha^j$ tal que $a_{ij} \in \mathbb{Q}$, para todo $i = 1, \cdots, n$ e $j = 0, 1, \cdots, n-1$. Como $a_{ij} \in \mathbb{Q}$ para todo $i, j = 1, \cdots, n$, segue que $a_{ij} = \dfrac{b_{ij}}{c_{ij}}$ com $b_{ij}, c_{ij} \in \mathbb{Z}$ e $c_{ij} \neq 0$ para todo $i, j = 1, \cdots, n$. Seja $d = mmc\{c_{ij};\ i = 1, \cdots, n,\ j = 0, 1, \cdots, n-1\}$. Temos que $d\gamma_i \in \mathbb{Z}[\alpha]$ para todo $i = 1, \cdots, n$. Como $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, temos que $dI = d\sum_{i=1}^{n} \mathbb{Z}\gamma_i = \sum_{i=1}^{n} \mathbb{Z}d\gamma_i \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, como queríamos. □

Definição 4.1.7. *Se $A \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo de posto n, a* **norma** *de A é dada por $N(A) = |\mathcal{O}_{\mathbb{K}}/A|$. Se $I \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo de posto n tal que $dI = A \subseteq \mathcal{O}_{\mathbb{K}}$, onde $d \in \mathbb{Z} - \{0\}$, a* **norma** *de I é dada por $N(I) = |N(d^{-1})|N(A)$.*

Proposição 4.1.5. *[61] Se $I \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo tal que $\{w_1, \cdots, w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ e $\{e_1w_1, \cdots, e_nw_n\}$ é uma Z-base de I, onde $e_1, \cdots, e_n$ são inteiros não nulos, então $N(I) = |e_1 \cdots e_n|$.* □

Teorema 4.1.2. *[57] Seja $\mathbb{K}$ um corpo de números. Todo ideal fracionário I não nulo de $\mathcal{O}_{\mathbb{K}}$ é escrito de modo único como um produto de ideais primos de $\mathcal{O}_{\mathbb{K}}$, isto é, $I = \prod_{i=1}^{n} P_i^{e_i}$, onde $e_1, \ldots, e_n$ são inteiros e $P_i's$ são ideais primos não nulos de $\mathcal{O}_{\mathbb{K}}$.* □

Teorema 4.1.3. *[57] Seja $\mathbb{K}$ um corpo de números. Se $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita de grau n, existem exatamente n homomorfismos distintos $\{\sigma_1, \cdots, \sigma_n\}$ de $\mathbb{L}$ em $\mathbb{C}$ que fixam $\mathbb{K}$.* □

Definição 4.1.8. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos de grau n e $\{\sigma_1, \cdots, \sigma_n\}$ os n $\mathbb{K}$-homomorfismos distintos de $\mathbb{L}$ em $\mathbb{C}$. Dizemos que um homomorfismo σ_i é* **real** *se $\sigma_i(\mathbb{L}) \subset \mathbb{R}$. Caso contrário, dizemos que σ_i é* **imaginário**. *Além disso, se σ_i for real para todo $i = 1, \cdots, n$, dizemos que a extensão $\mathbb{L}|\mathbb{K}$ é* **totalmente real** *e, se σ_i for imaginário para todo $i = 1, \cdots, n$, dizemos que $\mathbb{L}|\mathbb{K}$ é* **totalmente imaginária**.

Definição 4.1.9. *Um corpo de números $\mathbb{K}$ é chamado de* **CM-corpo** *se existe um subcorpo $\mathbb{F}$ tal que $[\mathbb{K} : \mathbb{F}] = 2$, a extensão $\mathbb{K}|\mathbb{F}$ é totalmente imaginária e a extensão $\mathbb{F}|\mathbb{Q}$ é totalmente real.*

Definição 4.1.10. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão de corpos. Se $\sigma_1, \sigma_2, \ldots, \sigma_n$ são os n homomorfismos distintos de $\mathbb{L}$ em $\mathbb{C}$, então*

$$N(x) = N_{\mathbb{L}|\mathbb{K}}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad Tr(x) = Tr_{\mathbb{L}|\mathbb{K}}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

são chamados a **norma** *e o* **traço** *de x na extensão $\mathbb{L}|\mathbb{K}$, respectivamente.*

Proposição 4.1.6. *[57] Se $\mathbb{K}$ é um corpo de números e $x \in \mathbb{K}$, então $N(x), Tr(x) \in \mathbb{Q}$. Mais ainda, se $x \in \mathcal{O}_{\mathbb{K}}$, então $N(x), Tr(x) \in \mathbb{Z}$.* □

Observação 4.1.2. *[57] Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, onde $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita. Se $\alpha, \alpha^* \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:*
(1)- $Tr_{\mathbb{L}|\mathbb{K}}(\alpha + \alpha^*) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha) + Tr_{\mathbb{L}|\mathbb{K}}(\alpha^*)$;

(2)- $Tr_{\mathbb{L}|\mathbb{K}}(a\alpha)$=$aTr_{\mathbb{L}|\mathbb{K}}(\alpha)$*;*
(3)- $Tr_{\mathbb{L}|\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}]a$*;*
(4)- $N_{\mathbb{L}|\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$*;*
(5)- $N_{\mathbb{L}|\mathbb{K}}(a\alpha) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}|\mathbb{K}}(\alpha)$*;*
(6)- $N_{\mathbb{L}|\mathbb{K}}(\alpha\alpha^*) = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\alpha^*)$.

Proposição 4.1.7. *[45] Sejam* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ *corpos. Temos que*

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = N_{\mathbb{M}|\mathbb{K}}(N_{\mathbb{L}|\mathbb{M}}(\alpha)) \text{ e } T_{\mathbb{L}|\mathbb{K}}(\alpha) = T_{\mathbb{M}|\mathbb{K}}(T_{\mathbb{L}|\mathbb{M}}(\alpha)).$$

Definição 4.1.11. *Seja* I *um ideal fracionário não nulo de* $\mathcal{O}_{\mathbb{K}}$ *tal que* $d\,I = R$*, onde* $d \in \mathcal{O}_{\mathbb{K}} - \{0\}$ *e* R *é ideal de* $\mathcal{O}_{\mathbb{K}}$*. A norma de* I *é definida por* $N(I) = |N_{\mathbb{K}|\mathbb{Q}}(d^{-1})||\mathcal{O}_{\mathbb{K}}/R|$.

Observação 4.1.3. *Se* $I = a\mathcal{O}_{\mathbb{K}}$ *é um ideal principal, então* $N(I) = |N_{\mathbb{K}|\mathbb{Q}}(a)|$.

Definição 4.1.12. *Sejam* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão de corpos de grau* n *e* $\{\omega_1, \ldots, \omega_n\}$ *uma base* $\mathbb{L}$ *sobre* $\mathbb{K}$*. O* **discriminante** *de* $\mathbb{L}|\mathbb{K}$ *é definido como*

$$d(\mathbb{L}|\mathbb{K}) = det[\sigma_j(\omega_i)]^2,$$

onde $\{\sigma_1, \cdots, \sigma_n\}$ *são os homomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$ *que fixam* $\mathbb{K}$.

Observação 4.1.4. *O discriminante independe da escolha da base.*

Definição 4.1.13. *Seja* $\mathbb{K}$ *um corpo de números. O conjunto*

$$\Delta(\mathbb{K}|\mathbb{Q})^{-1} = \{x \in \mathbb{K};\ \forall\, \alpha \in \mathcal{O}_{\mathbb{K}},\, Tr_{\mathbb{K}|\mathbb{Q}}(x\alpha) \in \mathbb{Z}\}$$

é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$*, chamado de* **codiferente**. *O seu ideal inverso* $\Delta(\mathbb{K}|\mathbb{Q})$ *é um ideal inteiro de* $\mathcal{O}_{\mathbb{K}}$*, chamado de* **diferente**.

Observação 4.1.5. *O diferente* $\Delta(\mathbb{K}|\mathbb{Q})$ *pode ser fatorado como um produto de ideais primos. Para corpos ciclotômicos, podemos encontrar em estudo detalhado de como fatorar o diferente como produto de ideais primos em [37].*

4.1.1 Corpos Ciclotômicos

Uma família de corpos muito utilizada na construção de reticulados algébricos devido às suas propriedades é a família dos corpos ciclotômicos. Um estudo desta família pode ser encontrado em [67].

Definição 4.1.14. *Sejam $\zeta \in \mathbb{C}$ e $n \in \mathbb{N}^*$. Dizemos que ζ é uma* **raiz n-ésima da unidade** *se $\zeta^n = 1$.*

Observação 4.1.6. *Existem exatamente n raízes n-ésimas distintas da unidade. O conjunto destas raízes $\{\zeta_{n_k} = cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n}),$ para $k = 0, 1, \cdots, n-1\}$ forma um grupo cíclico em relação à multiplicação, tendo ζ_{n_1} como um gerador.*

Definição 4.1.15. *Dizemos que ζ é uma* **raiz n-ésima primitiva da unidade** *se $\zeta^n = 1$ e $\zeta^m \neq 1$ para $1 < m < n$, ou seja, se ζ gera o grupo da raízes n-ésimas da unidade.*

Definição 4.1.16. *Seja ζ_n uma raiz n-ésima primitiva da unidade. Um* **corpo ciclotômico** *$\mathbb{K}$ é a menor extensão de $\mathbb{Q}$ contendo ζ_n, isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$.*

Definição 4.1.17. *Chamamos de* **n-ésimo polinômio ciclotômico** *o polinômio*

$$\phi_n(x) = \prod_{i=1}^{r}(x - \eta_i),$$

onde η_i é uma raiz n-ésima primitiva da unidade, para $i = 1, \cdots, r$.

Proposição 4.1.8. *[67] Temos que $\phi_n(x) = \dfrac{x^n - 1}{\prod\limits_{d|n, d<n} \phi_d(x)}$ para $n > 1$ e $\phi_1(x) = x - 1$.* □

Teorema 4.1.4. *[67] Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q})] = \varphi(n)$, onde φ é a função de Euler.* □

Teorema 4.1.5. *[67] Se ζ_n é uma raiz n-ésima primitiva da unidade, então o anel dos inteiros de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Z}$ é $\mathbb{Z}[\zeta_n]$ e uma $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_n]$ é $\{1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}\}$.* □

Proposição 4.1.9. *O conjunto dos homomorfismos de um corpo ciclotômico consiste dos homomorfismos σ_j, univocamente determinados por $\sigma_j(\zeta_n) = \zeta_n^j$ com $mdc(j, n) = 1$. Existem exatamente $\phi(n)$ homomorfismos distintos.* □

Teorema 4.1.6. *[67] O discriminante de $\mathbb{L} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

$$d(\mathbb{L}|\mathbb{Q}) = \pm\frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

□

Como consequência do Teorema 4.1.6 segue que:

- se $n = p$, então $d(\mathbb{L}|\mathbb{Q}) = (-1)^{\frac{(p-1)}{2}} p^{p-2}$;
- se $n = p^r$, então $d(\mathbb{L}|\mathbb{Q}) = (-1)^{\frac{(p-1)p^{r-1}}{2}} p^{p^{r-1}\cdot(r(p-1)-1)}$, r inteiro positivo.

Um subcorpo dos corpos ciclotômicos muito utilizado por suas propriedades é o subcorpo real maximal que será definido a seguir.

Proposição 4.1.10. *[67] Se $n \in \mathbb{N}^*$, ζ_n é uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então $\mathbb{K}$ é totalmente real e $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = 2$.* □

Definição 4.1.18. *Nas condições da proposição acima, o corpo $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é chamado de* **subcorpo real maximal** *de $\mathbb{Q}(\zeta_n)$.*

Teorema 4.1.7. *[67] O anel dos inteiros de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ e uma $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é*

$$\left\{1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \cdots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{\frac{\varphi(n)}{2}+1}\right\}.$$

□

Teorema 4.1.8. *[44, 43] O discriminante de $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ sobre $\mathbb{Q}$ é dado por:*

- $d(\mathbb{K}|\mathbb{Q}) = p^{\frac{p-3}{2}}$, *se* $n = p \geq 5$;
- $d(\mathbb{K}|\mathbb{Q}) = 2^{(r-1)2^{r-2}-1}$, *se* $n = 2^r$;
- $d(\mathbb{K}|\mathbb{Q}) = p^{\frac{(r+1)(p-1)p^{r-1}-p^r-1}{2}}$, *se* $n = p^r$, $p \neq 2$, $r > 1$.

□

4.2 Homomorfismo de Minkowski

Seja $\mathbb{K}$ um corpo de números de grau n. Pelo Teorema 4.1.3, temos que existem exatamente n homomorfismos distintos $\sigma_j : \mathbb{K} \longrightarrow \mathbb{C}$ para $j = 1, \cdots, n$, que fixam $\mathbb{Q}$. Se $\bar{\sigma} : \mathbb{C} \longrightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, temos que $\bar{\sigma} \circ \sigma_j = \sigma_k$ para algum $1 \leq k \leq n$ e que $\bar{\sigma} \circ \sigma_j = \sigma_j$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Desta forma, temos que os homomorfismos imaginários aparecem aos pares, isto é, se σ_j é imaginário, existe k tal que $\bar{\sigma} \circ \sigma_j = \sigma_k$.

Assim, usando r_1 para denotar o número de homomorfismos reais e r_2 o número de pares de homomorfismos imaginários, podemos reordenar os homomorfismos $\sigma_1, \ldots, \sigma_n$ de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os homomorfismos reais e que $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ sejam os homomorfismos imaginários com $\sigma_{r_1+r_2+i} = \bar{\sigma} \circ \sigma_{r_1+i}$ para $i = 1, \cdots, r_2$.

Definição 4.2.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Considere o homomorfismo injetivo de grupos*

$$\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$$

$$x \longmapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \cdots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))),$$

onde $\Re$ representa a parte real e $\Im$ representa a parte imaginária, respectivamente, do número complexo. Tal homomorfismo é chamado de **homomorfismo canônico** *ou* **homomorfismo de Minkowski** *de $\mathbb{K}$ em $\mathbb{R}^n$.*

Exemplo 4.2.1. *Sejam $\zeta = \zeta_5$ uma raiz 5-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_5)$ o 5-ésimo corpo ciclotômico. Temos que os $\mathbb{Q}$-homomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são dados por $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, onde $\sigma_i(\zeta) = \zeta^i$, para $i = 1, \cdots, 4$. Agora, $\sigma_i(\mathbb{K}) \nsubseteq \mathbb{R}$ para todo $i = 1, 2, 3, 4$. De fato, basta notar que $\sigma_i(\zeta) \notin \mathbb{R}$ para todo $i = 1, 2, 3, 4$. Neste caso, temos que $\mathbb{K}$ é totalmente imaginário, o que implica $r_1 = 0$ e $r_2 = 2$. Notemos que $\bar{\sigma} \circ \sigma_1 = \sigma_4$ e $\bar{\sigma} \circ \sigma_2 = \sigma_3$. Reorganizando os homomorfismos de maneira conveniente, temos que o homomorfismo de Minkowski é dado por*

$$\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^4$$

$$x \longmapsto (\Re(\sigma_1(x)), \Im(\sigma_1(x)), \Re(\sigma_2(x)), \Im(\sigma_2(x))).$$

Proposição 4.2.1. *[57] Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ o homomorfismo de Minkowski. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_j\}_{1\leq j\leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$ com base $\{\boldsymbol{\sigma}_{\mathbb{K}}(x_1), \cdots, \boldsymbol{\sigma}_{\mathbb{K}}(x_n)\}$ e volume*

$$vol(\sigma_{\mathbb{K}}(M)) = det(\sigma_{\mathbb{K}}(M))^{1/2} = 2^{-r_2} \left|\det(\sigma_j(x_k))_{j,k=1}^{n}\right|,$$

onde r_2 é o número de pares de homomorfismos imaginários. □

Se $\{x_1, \cdots, x_n\}$ é uma $\mathbb{Z}$-base de $M \subset \mathbb{K}$, então uma matriz geradora do reticulado

$$\sigma_{\mathbb{K}}(M) = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{\sigma}_{\mathbb{K}}(x_i);\ a_i \in \mathbb{Z} \right\}$$

é dada por

$$\begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_{r_1}(x_1) & \Re(\sigma_{r_1+1}(x_1)) & \Im(\sigma_{r_1+1}(x_1)) & \dots & \Re(\sigma_{r_1+r_2}(x_1)) & \Im(\sigma_{r_1+r_2}(x_1)) \\ \sigma_1(x_2) & \dots & \sigma_{r_1}(x_2) & \Re(\sigma_{r_1+1}(x_2)) & \Im(\sigma_{r_1+1}(x_2)) & \dots & \Re(\sigma_{r_1+r_2}(x_2)) & \Im(\sigma_{r_1+r_2}(x_2)) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(x_n) & \dots & \sigma_{r_1}(x_n) & \Re(\sigma_{r_1+1}(x_n)) & \Im(\sigma_{r_1+1}(x_n)) & \dots & \Re(\sigma_{r_1+r_2}(x_n)) & \Im(\sigma_{r_1+r_2}(x_n)) \end{pmatrix}.$$

Observação 4.2.1. *Se $\mathbb{K}$ é um corpo de números de grau n, vimos que todo ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Portanto, podemos utilizar ideais fracionários para gerar reticulados no $\mathbb{R}^n$.*

Proposição 4.2.2. *[57] Se $\mathbb{K}$ é um corpo de números de grau n, $d(\mathbb{K}|\mathbb{Q})$ é o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$, $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$ e $I \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(I)$ é um reticulado, com volume*

$$vol(\sigma_{\mathbb{K}}(I)) = det(\sigma_{\mathbb{K}})^{1/2} = 2^{-r_2}|d(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}}N(I),$$

onde r_2 é o número de pares de homomorfismos imaginários. □

Exemplo 4.2.2. *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_8)$, onde $\zeta_8 = e^{\frac{2\pi i}{8}}$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$ seu anel de inteiros com $\mathbb{Z}$-base $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$. Seja $I = 5\mathbb{Z}[\zeta_8]$ um ideal de $\mathbb{Z}[\zeta_8]$. Temos, pela Proposição (4.2.2), que $\sigma_{\mathbb{K}}(I)$ é um reticulado. Além disso, temos que*

$$vol(\sigma_{\mathbb{K}}(I)) = 2^{-r_2}|d(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}}N(I).$$

Agora, como $\mathbb{K}$ é totalmente complexo, segue que $r_2 = 2$. Pelo Teorema (4.1.6), temos que $|d(\mathbb{Q}(\zeta_8)|\mathbb{Q})| = 2^8$ e, como I é um ideal principal, pela Observação (4.1.3), temos que $N(I) = |N_{\mathbb{K}|\mathbb{Q}}(5)| = 5^4$. Assim, $vol(\sigma_{\mathbb{K}}(I)) = 2^{-2}2^{8/2}5^4 = 2^{4-2}5^4 = 2^2 5^4 = 2500$.

4.3 Homomorfismo Torcido

Nesta seção, apresentamos um homomorfismo que é obtido por uma perturbação do homomorfismo de Minkowski multiplicando cada entrada dos vetores do reticulado por um escalar apropriado [10, 11]. Como na seção anterior, dado $\mathbb{K}$ um corpo de números de grau n, os homomorfismos estão organizados como sendo os r_1 primeiros totalmente reais e os $2r_2$ restantes totalmente imaginários.

Definição 4.3.1. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$. Dizemos que α é* **totalmente positivo** *se $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$ e $\alpha_i > 0$ para todo $i = 1, \cdots, n$.*

Definição 4.3.2. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo. Considere o homomorfismo injetivo de grupos*

$$\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$$

$$x \longmapsto (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)),$$
$$\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)))$$

onde $\Re$ e $\Im$ representam a parte real e imaginária, respectivamente, de um número complexo. Tal homomorfismo é chamado de **homomorfismo torcido**.

Proposição 4.3.1. *[51] Se $L \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$, então a imagem $\sigma_\alpha(L)$ em $\mathbb{R}^n$ é um reticulado com base $\{\sigma_\alpha(w_1), \ldots, \sigma_\alpha(w_n)\}$.* □

Se $\{w_1, \ldots, w_n\}$ é uma $\mathbb{Z}$-base de L, então o reticulado $\sigma_\alpha(L)$ tem matriz geradora $\boldsymbol{M}$ dada por

$$\begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_1)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_1)) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_2)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_2)) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_n) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_n)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_n)) \end{pmatrix}. \tag{4.1}$$

Proposição 4.3.2. *[51] Se $\mathbb{K}$ é totalmente real ou um CM-corpo, $\alpha \in \mathbb{K}$ é totalmente positivo, $L \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo com $\mathbb{Z}$-base $\{w_1, \cdots, w_n\}$ e $\boldsymbol{M}$ é como em (4.1), então a matriz de Gram $\boldsymbol{G} = \boldsymbol{M}\boldsymbol{M}^t$ do reticulado $\sigma_\alpha(L)$ é dada por*

$$\boldsymbol{G} = (g_{ij})_{i,j=1}^{n} = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_i \overline{w_j}).$$

□

Motivados pelo estudo de reticulados cuja matriz de Gram apresenta todas as suas entradas inteiras, passaremos ao estudo de reticulados ideais.

Sejam $\mathbb{K}$ um corpo de números totalmente real ou um CM-corpo, de grau n, $I \subseteq \mathbb{K}$ um $\mathbb{Z}$-módulo de posto n e $\alpha \in \mathbb{K}$ totalmente positivo tais que $\alpha I \bar{I} \subset \Delta(\mathbb{K}|\mathbb{Q})^{-1}$, onde $\Delta(\mathbb{K}|\mathbb{Q})^{-1}$ é o codiferente da extensão $\mathbb{K}|\mathbb{Q}$ e $\bar{I}$ é o conjugado complexo de I. Nestas condições, temos que a matriz de Gram $\boldsymbol{G}$ do reticulado $\sigma_\alpha(I)$, como dada na Proposição 4.3.2, apresenta todas as entradas inteiras.

Definição 4.3.3. *Dizemos que $\sigma_\alpha(I)$ é um* **reticulado ideal** *se $\alpha I \bar{I} \subset \Delta(\mathbb{K}|\mathbb{Q})^{-1}$. Quando $\alpha = 1$, dizemos que o reticulado ideal $\sigma(I)$ é do* **tipo traço**.

Observação 4.3.1. *Notemos que quando o corpo $\mathbb{K}$ é totalmente real e $\alpha = 1$, o homomorfismo torcido é exatamente o homomorfismo de Minkowski.*

O Teorema 4.3.1 foi enunciado em [10] para ideais fracionários e relaciona o determinante do reticulado ideal com o discriminante do corpo associado. Estendemos a seguir o resultado para $\mathbb{Z}$-módulos de posto n. A demonstração é essencialmente a que foi feita em [37].

Teorema 4.3.1. *Seja $I \subseteq \mathbb{K}$ um $\mathbb{Z}$-módulo de posto n não nulo. Temos que*

$$det(\sigma_\alpha(I)) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d(\mathbb{K}|\mathbb{Q})|. \tag{4.2}$$

Demonstração: Pelo Lema (4.1.1), temos que existem $d \in \mathbb{Z} - \{0\}$ e $A \subset \mathcal{O}_\mathbb{K}$ um $\mathbb{Z}$-módulo de posto n tal que $dI = A \subset \mathcal{O}_\mathbb{K}$. Como $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e A é um $\mathbb{Z}$-submódulo de $\mathcal{O}_\mathbb{K}$, existem uma $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$ de $\mathcal{O}_\mathbb{K}$ e inteiros $e_1, \ldots, e_n$ tais que $\{e_1 w_1, \ldots, e_n w_n\}$ é uma $\mathbb{Z}$-base de A. Desta forma, como $dI = A$, segue que $I = d^{-1}A$.

Assim, $\{e_1d^{-1}w_1, \ldots, e_nd^{-n}w_n\}$ é uma $\mathbb{Z}$-base de I. Assim, temos que

$$\begin{aligned}\det(\sigma_\alpha(I)) &= \det\begin{pmatrix} Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_1d^{-1}w_1\overline{e_1d^{-1}w_1}) & \cdots & Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_1d^{-1}w_1\overline{e_nd^{-1}w_n}) \\ \vdots & \ddots & \vdots \\ Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_nd^{-1}w_n\overline{e_1d^{-1}w_1}) & \cdots & Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_nd^{-1}w_n\overline{e_nd^{-1}w_n}) \end{pmatrix} \\ &= (e_1e_2\cdots e_n)^2((d^{-1})^2)^n det\begin{pmatrix} Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_1\overline{w_1}) & \cdots & Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_1\overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_n\overline{w_1}) & \cdots & Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_n\overline{w_n}) \end{pmatrix}.\end{aligned}$$

Agora, pela Proposição 4.1.5, temos que $N(A) = |e_1\cdots e_n|$. Logo,

$$det(\sigma_\alpha(I)) = N(A)^2((d^{-1})^2)^n det(H),$$

onde

$$H = \begin{pmatrix} Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_1\overline{w_1}) & \cdots & Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_1\overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_n\overline{w_1}) & \cdots & Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_n\overline{w_n}) \end{pmatrix}.$$

Agora, notamos que $H = MM^\perp$, onde

$$M = TA = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}\begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}$$

e $\perp$ denota a transposta conjugada. Assim, $det(H) = det(M)det(M^\perp) = det(T)det(A)$ $det(A^\perp)det(T^\perp) = (det(A))^2det(T)\overline{det(T)} = (det(A))^2|det(T)|^2$. Mas, temos que $(det(A))^2 = \sigma_1(\alpha)\cdots\sigma_n(\alpha) = N_{\mathbb{K}|\mathbb{Q}}(\alpha)$. Por outro lado, $det(T) = det(\sigma_i(w_j))_{i,j=1}^n = \sqrt{(d(\mathbb{K}|\mathbb{Q}))}$. Desta forma, segue que

$$det(\sigma_\alpha(I)) = N(A)^2((d^{-1})^2)^n N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d(\mathbb{K}|\mathbb{Q})|.$$

Agora, como $d \in \mathbb{Z}$, segue que $N(I) = N(A)N_{\mathbb{K}|\mathbb{Q}}(d^{-1}) = N(A)(d^{-1})^n$. Logo, $N(I)^2 = N(A)^2((d^{-1})^n)^2$. Portanto, $det(\sigma_\alpha(I)) = N(I)^2N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d(\mathbb{K}|\mathbb{Q})|$. □

Em [10, 51, 13] é utilizado o homomorfismo torcido para reproduzir alguns reticulados mais densos em dimensões baixas. Um resultado de [10] é o seguinte:

Proposição 4.3.3. *[10] Se $\mathbb{K}$ é um corpo de números tal que $\mathbb{K}$ é totalmente real ou um CM-corpo, então existe um reticulado ideal do tipo traço com determinante d se, e somente se, existem ideais I, J de $\mathcal{O}_{\mathbb{K}}$ tal que $N(J) = d$ e $\Delta(\mathbb{K}|\mathbb{Q}) = JI\overline{I}$.* □

Com o auxílio da proposição acima, em [10] foram construídas versões algébricas dos reticulados A_{p-1} para p primo, D_4, E_8, E_6, K_{12} e Λ_{24} via corpos ciclotômicos.

4.4 Diversidade e distância produto mínima

Já vimos nos capítulos anteriores que a diversidade e a distância produto mínima estão relacionadas com a probabilidade de erros em canais do tipo Rayleigh com desvanecimento. Vimos que, para se obter reticulados eficientes para serem utilizados neste canal é necessário ter alta diversidade e alta distância produto mínima. A fim de maximizar a diversidade, iremos trabalhar em corpos de números totalmente reais, pois estes possuem diversidade máxima. Já para a distância produto mínima, veremos que quando trabalhamos com ideais principais, seu valor depende somente do discriminante do corpo utilizado na construção do reticulado. Fixada uma dimensão n, afim de obter uma distância produto mínima alta, vamos construir reticulados ideais via corpos de números de grau n com discriminante mínimo.

Proposição 4.4.1. *Sejam $\mathbb{K}$ um corpo de números de grau n totalmente real e $I \subset \mathbb{K}$ um $\mathbb{Z}$-módulo de posto n. Os reticulados $\Lambda_1 = \sigma_\alpha(I)$ e $\Lambda_2 = \sigma_{\mathbb{K}}(I)$ obtidos pelo homomorfismo torcido e de Minkowski, respectivamente, têm diversidade $div(\Lambda_i) = n$, $i = 1, 2$.*

Demonstração: Basta notar que se $\boldsymbol{y} \in \Lambda_i$ e $\boldsymbol{y} \neq \mathbf{0}$, então existe $0 \neq x \in I$ tal que x é levado em $\boldsymbol{y}$ pelo homomorfismo. Agora, como $x \neq 0$, então $\sigma_i(x) \neq 0$ para todo homomorfismo de $\mathbb{K}$ em $\mathbb{C}$. Do fato de $\mathbb{K}$ ser totalmente real segue o resultado. □

As proposições seguintes foram enunciadas em [51] para ideais inteiros $I \subseteq \mathcal{O}_{\mathbb{K}}$.

Proposição 4.4.2. *Seja $I \subset \mathbb{K}$ um ideal fracionário. Os reticulados $\Lambda_1 = \sigma_\alpha(I)$ e $\Lambda_2 = \sigma_{\mathbb{K}}(I)$ obtidos pelo homomorfismo torcido e de Minkowski, respectivamente, têm diversidade $div(\Lambda_i) = r_1 + r_2$, $i = 1, 2$.*

Demonstração: Faremos a demonstração para o homomorfismo torcido. Pelo Lema 4.1.1, temos que existe $d \in \mathbb{Z}$ não nulo tal que $dI \subseteq \mathcal{O}_{\mathbb{K}}$. Note que $dI = R$ é um ideal de $\mathcal{O}_{\mathbb{K}}$. Seja

$\boldsymbol{x} \neq \mathbf{0}$ um ponto do reticulado Λ. Existe $y \in I$ tal que

$$\boldsymbol{x} = \sigma_\alpha(y) = (\sqrt{\alpha_1}\sigma_1(y), \cdots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(y)), \cdots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(y))).$$

Como $\boldsymbol{x} \neq \mathbf{0}$, segue que $y \neq 0$. Sendo $y \neq 0$, temos que $\sigma_i(y) \neq 0$ para todo $i = 1, \cdots, n$. Logo, os primeiros r_1 coeficientes de $\boldsymbol{x}$ são não nulos. Agora, notemos que como $\sigma_{r_1+i}(y) \neq 0$ para todo $i = 1, \cdots, r_2$, segue que $\Re(\sigma_{r_1+i}(y)) \neq 0$ ou $\Im(\sigma_{r_1+i}(y)) \neq 0$. Desta forma, destes $n - r_1$ coeficientes restantes de $\boldsymbol{x}$, pelo menos $\dfrac{n - r_1}{2} = r_2$ são não nulos. Assim, $div(\Lambda) \geq r_1 + r_2$. Seja agora $\beta \in I$ tal que $\beta \neq 0$. Como $dI \subset \mathcal{O}_\mathbb{K}$, segue que $d\beta$ é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$. Assim, existem $a_0, a_1, \cdots, a_{m-1} \in \mathbb{Z}$ tal que $(d\beta)^m + a_{m-1}(d\beta)^{m-1} + \cdots + a_1(d\beta) + a_0 = 0$ e $a_0 \neq 0$. Logo, $-a_0 = (d\beta)^m + a_{m-1}(d\beta)^{m-1} + \cdots + a_1(d\beta) \in R$, pois R é ideal e $d\beta \in R$. Assim, $-a_0 d^{-1} \in I$. Como $-a_0 d^{-1} \in \mathbb{Q}$, pois $d \in \mathbb{Z}$ segue que $\sigma_i(-a_0 d^{-1}) = -a_0 d^{-1}$ para todo $i = 1, \cdots, n$. Logo, $div(-a_0 d^{-1}) = r_1 + r_2$. Portanto, $div(\Lambda) = r_1 + r_2$. □

Proposição 4.4.3. *Seja I um ideal fracionário não nulo de $\mathcal{O}_\mathbb{K}$. Os reticulados $\Lambda_1 = \sigma_\alpha(I)$ e $\Lambda_2 = \sigma_\mathbb{K}(I)$ obtidos pelo homomorfismo torcido e de Minkowski, respectivamente, podem ser imersos no $\mathbb{R}^n$ com*

- *diversidade n se $\mathbb{K}$ é totalmente real.*
- *diversidade $\dfrac{n}{2}$ se $\mathbb{K}$ é totalmente complexo.*

Demonstração: Segue diretamente da Proposição 4.4.2. □

Portanto, vimos que se considerarmos corpos de números totalmente reais na construção de reticulados teremos diversidade máxima. O mesmo resultado vale para $\mathbb{Z}$-módulos de posto n em $\mathbb{K}$.

A próxima proposição apresenta uma expressão para a distância produto mínima de reticulados ideais quando o corpo $\mathbb{K}$ é totalmente real e $I \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo de posto n.

Proposição 4.4.4. *Se $\mathbb{K}$ é um corpo de números totalmente real de grau n, com discriminante $d(\mathbb{K}|\mathbb{Q})$, $I \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo de posto n e $\sigma_\alpha(I)$ tem diversidade n, então a distância produto mínima do reticulado ideal $\Lambda = \sigma_\alpha(I)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{N_{\mathbb{K}|\mathbb{Q}}(\alpha)} min_{0 \neq y \in I} |N_{\mathbb{K}|\mathbb{Q}}(y)| = \frac{\sqrt{det(\sigma_\alpha(I))}}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}} \frac{1}{N(I)} min_{0 \neq y \in I} |N_{\mathbb{K}|\mathbb{Q}}(y)|.$$

Demonstração: Análoga a que foi feita em [51] para ideais fracionários. □

Quando I é um ideal principal, a distância produto mínima do reticulado ideal $\sigma_\alpha(I)$ pode ser calculada conforme o seguinte resultado.

Corolário 4.4.1. *[51] Se $\mathbb{K}$ é um corpo de números totalmente real e I é um ideal principal de $\mathcal{O}_\mathbb{K}$, então a distância produto mínima do reticulado ideal $\sigma_\alpha(I)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\sigma_\alpha(I))}{|d(\mathbb{K}|\mathbb{Q})|}}.$$

□

Observação 4.4.1. *Se o ideal I é principal, temos que $N(I) = min_{0\neq y\in I}|N(y)|$. Quando o ideal I não é ideal principal,*

$$N(I) < min_{0\neq y\in I}|N(y)|.$$

De fato, dado $y \in I$, temos que $N(y) = |\mathcal{O}_\mathbb{K}/y\mathcal{O}_\mathbb{K}| = |\mathcal{O}_\mathbb{K}/I||I/y\mathcal{O}_\mathbb{K}| > N(I)$, pois $|I/y\mathcal{O}_\mathbb{K}| = 1$ se, e somente se, I é um ideal principal. Com isso, temos que a distância produto mínima aumenta quando não trabalhamos com ideais principais. O problema de trabalhar com ideais não principais é a dificuldade para calcular a distância produto mínima. Veremos no decorrer do capítulo que quando trabalhamos com $\mathbb{Z}$-módulos que não são ideais, a distância produto mínima pode diminuir.

Fixada uma dimensão, queremos obter reticulados com diversidade máxima e maior distância produto mínima. Quando consideramos reticulados com vetor de norma mínima euclidiana de tamanhos diferentes, para fazer uma comparação justa entre a distância produto mínima, devemos considerar versões escalonadas desses reticulados, de forma que o vetor de menor norma das versões escalonadas seja unitário.

Neste capítulo, reproduziremos alguns dos reticulados mais densos conhecidos com diversidade máxima. Para os reticulados A_n, D_n, $\mathbb{Z}^n$, E_6, E_7, E_8, caso seja possível reproduzí-los via ideais principais, obteremos os seguintes valores para a distância produto mínima relativa em função do discriminante do corpo de números associado.

- $\mathbb{Z}^n$**:** $d_{p,rel}(\mathbb{Z}^n) = \frac{1}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}}$.
- D_n**:** $d_{p,rel}(D_n) = \frac{1}{\sqrt{2}^n}\frac{\sqrt{4}}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}}$.

- A_n: $d_{p,rel}(A_n) = \frac{1}{\sqrt{2}^n}\frac{\sqrt{n+1}}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}}$.
- E_6: $d_{p,rel}(E_6) = \frac{1}{\sqrt{2}^6}\frac{\sqrt{3}}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}}$.
- E_7: $d_{p,rel}(E_7) = \frac{1}{\sqrt{2}^7}\frac{\sqrt{2}}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}}$.
- E_8: $d_{p,rel}(E_8) = \frac{1}{\sqrt{2}^8}\frac{1}{\sqrt{|d(\mathbb{K}|\mathbb{Q})|}}$.

Pelo que foi visto acima, fixando a dimensão e o corpo utilizado na construção, temos que a família de reticulados $\mathbb{Z}^n$ apresenta a maior distância produto mínima relativa.

Considerando reticulados que são eficientes apenas para o canal do tipo Rayleigh, é interessante utilizar reticulados $\mathbb{Z}^n$-rotacionados, pois além de apresentarem distância produto mínima maior, eles apresentam um algoritmo de decodificação extremamente simples. Para canais gaussianos, esses reticulados são muito ruins para serem utilizados, pois sua densidade de centro euclidiana é 2^{-n}, que é pequena se comparada com a densidade de centro de todos os outros reticulados listados acima.

É interessante construir reticulados que sejam simultaneamente eficientes para os canais gaussiano e do tipo Rayleigh com desvanecimento. Por isso, neste capítulo através de contruções existentes para reticulados $\mathbb{Z}^n$-rotacionados, vamos reproduzir alguns reticulados densos com diversidade alta.

4.5 Reticulados D_n-rotacionados, $n = 2^{r-2}$, $r \geq 5$

Nesta seção, faremos a construção de reticulados D_n-rotacionados via o subcorpo real maximal $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ dos corpos ciclotômicos $\mathbb{Q}(\zeta_{2^r})$ com $r \geq 5$. Desta forma, serão obtidos reticulados D_n-rotacionados para $n = 2^{r-2}$, $r \geq 5$, isto é, n=8,16,32,64,128,256,512,...

Sejam $\zeta = \zeta_{2^r}$ uma raiz 2^r-ésima primitiva da unidade, $\mathbb{L} = \mathbb{Q}(\zeta_{2^r})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}{}^{-1})$. Temos que $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 2^{r-2}$.

$$2^{r-1}\left\{\begin{array}{l}\mathbb{Q}(\zeta)\\ |2\\ \mathbb{Q}(\zeta+\zeta^{-1})\\ |2^{r-2}\\ \mathbb{Q}\end{array}\right.$$

Observação 4.5.1. *Em [4, 14] são construídos reticulados $\mathbb{Z}^n$-rotacionados no subcorpo real maximal de tais corpos ciclotômicos para $\alpha_1 = 2 - e_1$ e $\alpha_2 = 2 + e_1$, respectivamente, e $I = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$. Tais reticulados, além de serem equivalentes na métrica euclidiana, pois ambos são equivalentes ao reticulado $\mathbb{Z}^n$, são equivalentes na métrica da soma. De fato, uma matriz geradora para o reticulado $\frac{1}{\sqrt{2^{r-1}}}\sigma_{\alpha_2}(\mathcal{O}_{\mathbb{K}})$ de [14] é*

$$\boldsymbol{M}_1 = \frac{1}{\sqrt{2^{r-1}}}\boldsymbol{N}\boldsymbol{A},$$

onde $\boldsymbol{N} = (\sigma_j(e_{i-1}))_{i,j=1}^n$ e $\boldsymbol{A} = diag(\sqrt{\sigma_k(\alpha_2)})$. Considere a matriz mudança de base

$$\boldsymbol{M} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix}$$

e a matriz de permutação

$$\boldsymbol{P} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Temos que $\boldsymbol{M}\left(\frac{1}{\sqrt{2^{r-1}}}\boldsymbol{N}\boldsymbol{A}\right)\boldsymbol{P}$ é a matriz geradora para o reticulado $\frac{1}{\sqrt{2^{r-1}}}\sigma_{\alpha_1}(\mathcal{O}_{\mathbb{K}})$ obtido em [4].

Como o reticulado D_n é um sub-reticulado de $\mathbb{Z}^n$, vamos utilizar o reticulado algébrico encontrado em [14] e encontrar um sub-reticulado que seja D_n-rotacionado.

Sejam $e_0 = 1$ e $e_j = \zeta^j + \zeta^{-j}$ para $j = 1, \cdots, 2^{r-2} - 1$. Temos que $\{e_j\}_{j=0}^{2^{r-2}-1}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$.

Uma matriz geradora para o reticulado $\mathbb{Z}^n$-rotacionado $\frac{1}{\sqrt{2^{r-1}}}\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$ de [14] é

$$\boldsymbol{M}_1 = \frac{1}{\sqrt{2^{r-1}}}\boldsymbol{N}\boldsymbol{A},$$

onde $\boldsymbol{N} = (\sigma_j(e_{i-1}))_{i,j=1}^n$ e $\boldsymbol{A} = diag(\sqrt{\sigma_k(\alpha)})$.

Por [14]

$$\boldsymbol{M}_1\boldsymbol{M}_1{}^t = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 2 \end{pmatrix}.$$

Consideremos a matriz mudança de base

$$\boldsymbol{T} = \begin{pmatrix} 1 & -1 & \cdots & 1 & -1 \\ 1 & -1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Para $\boldsymbol{M} = \boldsymbol{T}\boldsymbol{M}_1$, temos que a matriz de Gram $\boldsymbol{G} = \boldsymbol{M}\boldsymbol{M}^t = \boldsymbol{I}_n$ é uma matriz de rotação. Portanto, a matriz $\boldsymbol{M}$ leva a base canônica $\boldsymbol{I}_n$ do $\mathbb{Z}^n$ na base $\boldsymbol{I}_n\boldsymbol{M}$ do reticulado $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$.

Uma matriz geradora para o reticulado D_n (1.4) é dada por

$$\boldsymbol{B} = \begin{pmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}. \tag{4.3}$$

Proposição 4.5.1. *Sejam $I \subseteq \mathcal{O}_\mathbb{K}$ um $\mathbb{Z}$-módulo com $\mathbb{Z}$-base*

$$\{-2e_0 + 2e_1 - 2e_2 + \cdots - 2e_{n-2} + e_{n-1}, -e_{n-1}, e_{n-2}, -e_{n-3}, \ldots, e_2, -e_1\}$$

e $\alpha = 2 + e_1$. O reticulado $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I) \subseteq \mathbb{R}^{2^{r-2}}$ é um reticulado D_n-rotacionado.

Demonstração: Seja $\boldsymbol{B}$ a matriz geradora de D_n dada em (4.3). Usando propriedades do homomorfismo, temos que

$$\boldsymbol{BM} = \frac{1}{\sqrt{2^{r-1}}}\boldsymbol{BTNA} = \frac{1}{\sqrt{2^{r-1}}}\boldsymbol{B}\begin{pmatrix} 1 & -1 & \cdots & 1 & -1 \\ 1 & -1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}\begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}\boldsymbol{A}$$

$$= \frac{1}{\sqrt{2^{r-1}}}\boldsymbol{B}\begin{pmatrix} \sigma_1(e_0 - e_1 + \cdots + e_{n-2} - e_{n-1}) & \cdots & \sigma_n(e_0 - e_1 + \cdots + e_{n-2} - e_{n-1}) \\ \sigma_1(e_0 - e_1 + \cdots + e_{n-2}) & \cdots & \sigma_n(e_0 - e_1 + \cdots + e_{n-2}) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_0) & \cdots & \sigma_n(e_0) \end{pmatrix}\boldsymbol{A}$$

$$= \frac{1}{\sqrt{2^{r-1}}}\begin{pmatrix} \sigma_1(-2e_0 + \cdots - 2e_{n-2} + e_{n-1}) & \cdots & \sigma_n(-2e_0 + \cdots - 2e_{n-2} + e_{n-1}) \\ \sigma_1(-e_{n-1}) & \cdots & \sigma_n(-e_{n-1}) \\ \sigma_1(e_{n-2}) & \cdots & \sigma_n(e_{n-2}) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_2) & \cdots & \sigma_n(e_2) \\ \sigma_1(-e_1) & \cdots & \sigma_n(-e_1) \end{pmatrix}\boldsymbol{A}$$

é uma matriz geradora para $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I)$. Este reticulado é um reticulado D_n-rotacionado, pois $\boldsymbol{BM}(\boldsymbol{BM})^t = \boldsymbol{BB}^t$ é a matriz de Gram padrão do reticulado D_n. □

A seguir, mostraremos que os reticulados D_n-rotacionados obtidos na Proposição 4.5.1 estão associados a um ideal principal de $\mathcal{O}_\mathbb{K}$ e calcularemos sua distância produto mínima relativa.

Proposição 4.5.2. *Seja I o $\mathbb{Z}$-módulo dado na Proposição 4.5.1. I é um ideal principal e $I = e_1\mathcal{O}_\mathbb{K}$.*

Demonstração: É fácil ver que $I = 2e_0\mathbb{Z} + e_1\mathbb{Z} + \cdots + e_{n-1}\mathbb{Z}$. Seja $x \in e_1\mathcal{O}_\mathbb{K}$. Temos que $x = e_1(a_0e_0 + a_1e_1 + a_2e_2 + \cdots + a_{n-1}e_{n-1}) = a_0e_1 + a_1(e_2 + 2e_0) + a_2(e_3 + e_{-1}) + \cdots + a_{n-1}(e_n + e_{-n+2}) = a_1(2e_0) + (a_0 + a_2)(e_1) + (a_1 + a_3)(e_2) + \cdots + (a_{n-2})(e_{n-1}) \in I$. Agora, se $x \in I$, então $x = a_0 2e_0 + a_1e_1 + \cdots + a_{n-1}e_{n-1} = (e_1)[a_0e_1 + a_1e_2 + (a_2 - a_0)e_3 + (a_3 - a_1)e_4 + (a_4 - a_2 - a_0)e_5 + (a_5 - a_3 - a_1)e_6 + \cdots + (a_{n-1})e_{n-2} + (a_{n-2} - a_{n-4} \cdots - a_0)e_{n-1}] \in e_1\mathcal{O}_\mathbb{K}$. Portanto, I é um ideal principal de $\mathcal{O}_\mathbb{K}$. □

Proposição 4.5.3. *Se $\Lambda = \frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I)$ então*

$$d_{p,rel}\left(\frac{1}{2^{r-1}}\sigma_\alpha(I)\right) = \frac{1}{\sqrt{2}^n}\frac{1}{\sqrt{2^{r-1}}^n}\sqrt{8} = 2^{\frac{3-rn}{2}}$$

Demonstração: Primeiro notemos que o valor da norma mínima do reticulado D_n é $\sqrt{2}$. Logo, temos que multiplicar a distância produto mínima por $\frac{1}{\sqrt{2}^n}$. Como o ideal I é principal, utilizando o Corolário 4.4.1, temos que $d_{p,min}(\sigma_\alpha(I)) = \sqrt{N(\alpha)N(I)^2}$. Agora, temos que $N(\alpha) = 2$ e $N(I) = 2$. Portanto,

$$d_{p,rel}\left(\frac{1}{2^{r-1}}\sigma_\alpha(I)\right) = \frac{1}{\sqrt{2}^n}\frac{1}{\sqrt{2^{r-1}}^n}\sqrt{8}.$$

□

Proposição 4.5.4. *Se* $\Lambda = \frac{1}{\sqrt{2^{r-1}}}(\sigma_\alpha(I)) \subseteq \mathbb{R}^{2^{r-2}}$, *então:*

$$\lim_{n\longrightarrow\infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2} \ e \ \lim_{n\longrightarrow\infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0.$$

Demonstração: A demonstração é direta. □

A Tabela 4.1 mostra uma comparação entre a distância produto mínima relativa e a densidade de centro dos reticulados $\mathbb{Z}^n$-rotacionados de [14] e D_n-rotacionados construídos aqui.

r	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(D_n)$
4	4	0.385553	0.324210	0.062500	0.125000
5	8	0.261068	0.201311	0.003906	0.031250
6	16	0.180648	0.133393	0.000015	0.001953
7	32	0.126361	0.091307	2.3×10^{-10}	7.6×10^{-6}
8	64	0.088868	0.063523	5.4×10^{-20}	1.1×10^{-10}
9	128	0.062669	0.044554	2.9×10^{-39}	2.7×10^{-20}

Tabela 4.1: Distância produto relativa versus densidade de centro

Se o objetivo é construir reticulados com boa performance sobre os canais gaussiano e do tipo Rayleigh com desvanecimento, levando em conta o "trade-off" densidade versus distância produto mínima relativa, existem algumas vantagens em considerar os reticulados D_n-rotacionados aqui construídos ao invés dos reticulados $\mathbb{Z}^n$-rotacionados de [14] $n = 2^{r-2}$, $r \geq 5$, de [14], em altas dimensões.

4.6 Reticulados D_n-rotacionados, $n = \frac{p-1}{2}$, p primo

Através da família de reticulados $\mathbb{Z}^n$-rotacionados construída em [51], construímos famílias de reticulados D_n-rotacionados para $n = \frac{p-1}{2}$ com p primo e $p \geq 7$ [38]. Os reticulados D_n-rotacionados foram construídos via $\mathbb{Z}$-módulos de posto n que não são ideais.

Os reticulados D_n-rotacionados serão construídos via o subcorpo real maximal $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ dos corpos ciclotômicos $\mathbb{L} = \mathbb{Q}(\zeta_p)$ com p primo e $p \geq 7$.

Serão obtidos reticulados D_n-rotacionados para $n = \dfrac{p-1}{2}$ com p primo e $p \geq 7$, isto é, $n = 3, 5, 6, 8, 9, 11, 14, 15, , 18, 20, 21, 23, 26, 29, 30, ...$

Sejam p um número primo tal que $p \geq 7$, $\zeta = \zeta_p$ uma raiz p-ésima primitiva da unidade, $\mathbb{L} = \mathbb{Q}(\zeta_p)$ o p-ésimo corpo ciclotômico e $\mathbb{K} = \mathbb{Q}(\zeta_p + {\zeta_p}^{-1})$ seu subcorpo real maximal. Temos que $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{p-1}{2}$.

$$p-1 \left\{ \begin{array}{l} \mathbb{Q}(\zeta_p) \\ |2 \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \\ |\frac{p-1}{2} \\ \mathbb{Q} \end{array} \right.$$

Em [51, 13] são construídos reticulados $\mathbb{Z}^n$-rotacionados através do subcorpo real maximal dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, tomando $\alpha = (1-\zeta)(1-\zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$, $I = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$ e o homomorfismo torcido. Nós derivamos reticulados D_n-rotacionados como sub-reticulados desses reticulados $\mathbb{Z}^n$-rotacionados.

Para p primo, temos que $\left\{e_j = \zeta_p^j + \zeta_p^{-j}\right\}_{j=1}^{\frac{p-1}{2}}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Proposição 4.6.1. *[51] Sejam $e_n^* = e_n$, $e_j^* = \sum_{i=j}^{n} e_i$, para $j = 1, \cdots, n-1$, uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ e $\alpha = 2 - (\zeta + \zeta^{-1})$. Temos que*

$$\frac{1}{p} Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i^* e_j^*) = \delta_{ij},$$

onde δ_{ij} é o delta de Kronecker. □

Segue da Proposição 4.6.1, que o reticulado ideal $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ com $\alpha = 2 - (\zeta + \zeta^{-1})$ é um reticulado $\mathbb{Z}^n$-rotacionado, pois uma matriz de Gram para $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é a matriz identidade e, pela Proposição 1.2.1, temos que reticulados com mesma matriz de Gram são equivalentes na métrica euclidiana.

Uma matriz geradora para o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é dada por

$$\boldsymbol{M} = \frac{1}{\sqrt{p}}\boldsymbol{T}\boldsymbol{N}\boldsymbol{A}, \text{ onde} \tag{4.4}$$

$$\boldsymbol{N} = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}, \ \boldsymbol{T} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \text{ e } \ \boldsymbol{A} = diag(\sqrt{\sigma_k(\alpha)}).$$

Temos que $\boldsymbol{M}\boldsymbol{M}^t = \boldsymbol{I}_n$, ou seja, a matriz $\boldsymbol{M}$ é uma matriz de rotação que leva a base canônica $\boldsymbol{I}_n$ do $\mathbb{Z}^n$ na base $\boldsymbol{I}_n\boldsymbol{M}$ do reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$.

Seja $\boldsymbol{B}$ uma matriz geradora para o reticulado D_n como em (4.3).

Vamos aplicar a matriz de rotação $\boldsymbol{M}$ à matriz geradora $\boldsymbol{B}$ do reticulado D_n e obter um reticulado D_n-rotacionado. A proposição seguinte mostra isso.

Proposição 4.6.2. *Considere o $\mathbb{Z}$-módulo $I \subseteq \mathcal{O}_\mathbb{K}$ com $\mathbb{Z}$-base*

$$\{-e_1 - 2e_2 - \cdots - 2e_n, e_1, e_2, \cdots, e_{n-1}\}$$

e $\alpha = 2 - e_1$. Temos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$ é um reticulado D_n-rotacionado.

Demonstração: Aplicando a matriz de rotação $\boldsymbol{M}$ à matriz $\boldsymbol{B}$, temos que

$$\boldsymbol{BM} = \frac{1}{\sqrt{p}}\boldsymbol{BTNA} = \frac{1}{\sqrt{p}}\boldsymbol{B}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}\begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}\boldsymbol{A}$$

$$= \frac{1}{\sqrt{p}}\boldsymbol{B}\begin{pmatrix} \sigma_1(e_1+\cdots+e_n) & \cdots & \sigma_n(e_1+\cdots+e_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}\boldsymbol{A}$$

$$= \frac{1}{\sqrt{p}}\begin{pmatrix} \sigma_1(-e_1-\cdots-e_n-e_2-\cdots-e_n) & \cdots & \sigma_n(-e_1-\cdots-e_n-e_2-\cdots-e_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}+e_n-e_n) & \cdots & \sigma_n(e_{n-1}+e_n-e_n) \end{pmatrix}\boldsymbol{A}$$

$$= \frac{1}{\sqrt{p}}\begin{pmatrix} \sigma_1(-e_1-2e_2-\cdots-2e_n) & \cdots & \sigma_n(-e_1-2e_2-\cdots-2e_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}\boldsymbol{A}.$$

Assim, note que uma matriz geradora para o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$ é dada por $\boldsymbol{BM}$. Como $\boldsymbol{BM}(\boldsymbol{BM})^t = \boldsymbol{BB}^t$, que é uma matriz de Gram do reticulado D_n, temos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$ é um reticulado D_n-rotacionado. □

Proposição 4.6.3. *O $\mathbb{Z}$-módulo $I \subseteq \mathcal{O}_\mathbb{K}$, dado pela proposição anterior, não é ideal de $\mathcal{O}_\mathbb{K}$.*

Demonstração: É fácil ver que $\{e_1, e_2, \cdots, e_{n-1}, 2e_n\}$ é uma outra $\mathbb{Z}$-base para I. De fato, se $x \in I$, então existem $a_1, \cdots, a_n \in \mathbb{Z}$ tais que $x = a_1(-e_1 - 2e_2 - \cdots - 2e_m) + a_2e_2 + \cdots + a_ne_{n-1} = (a_2 - a_1)e_1 + (a_3 - 2a_1)e_2 + \cdots + (a_n - 2a_1)e_{n-1} - a_1(2e_n) \in \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1} + \mathbb{Z}2e_n$. Agora se $x \in \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1} + \mathbb{Z}2e_n$, então existem $b_1, \cdots, b_n \in \mathbb{Z}$ tais que $x = b_1e_1 + b_2e_2 + \cdots + b_{n-1}e_{n-1} + b_n2e_n = (a_1 - a_n)e_1 + \cdots + (a_{n-1} - 2a_n)e_{m-1} - a_n(-e_1 - 2e_2 - \cdots - 2e_n) \in I$. Agora, temos que e_n não está em I. De fato, se e_n estivesse em I, teríamos $I = \mathcal{O}_\mathbb{K}$, mas, pela Proposição 1.1.1, $\left|\frac{\mathcal{O}_\mathbb{K}}{I}\right| = 1.1.\cdots.1.2 = 2$. Logo, $e_n \notin I$. Mostremos que $e_{n-1}e_1$ não está em I. Temos que $e_{n-1}e_1 = e_n + e_{n-2}$. Como $e_{n-2} \in I$, se $e_{n-1}e_1 \in I$, então $e_n = e_{n-1}e_1 - e_{n-2} \in I$, o que não acontece. Portanto, I não é ideal de $\mathcal{O}_\mathbb{K}$. □

Os reticulados D_n-rotacionados obtidos acima possuem diversidade máxima, pois o corpo $\mathbb{K}$ é totalmente real. Vamos calcular a distância produto mínima de tal família de reticulados.

Lema 4.6.1. $|N_{\mathbb{K}|\mathbb{Q}}(e_1)| = 1$ *para* $e_1 = \zeta_p + \zeta_p^{-1}$.

Demonstração: Temos que $(\zeta + \zeta^{-1})(-\zeta^{p-1} - \zeta^{p-2} - \cdots - \zeta - 1) = 1$. Agora, notemos que $(-\zeta^{p-1} - \zeta^{p-2} - \cdots - \zeta - 1) \in \mathcal{O}_{\mathbb{K}}$ pois $1 \in \mathcal{O}_{\mathbb{K}}$ e $(\zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta) = (\zeta^{p-1} + \zeta) + (\zeta^{p-2} + \zeta^2) + \cdots + (\zeta^{\frac{p+1}{2}} + \zeta^{\frac{p-1}{2}}) \in \mathcal{O}_{\mathbb{K}}$. Assim, $N(\zeta + \zeta^{-1})N(-\zeta^{p-1} - \zeta^{p-2} - \cdots - \zeta - 1) = N(1) = 1$. Como $e_1 \in \mathcal{O}_{\mathbb{K}}$, segue que $N(e_1) \in \mathbb{Z}$, logo $|N(e_1)| = 1$ é a única possibilidade. □

Proposição 4.6.4. *Se* $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(I)$ *com* α *e* I *como na Proposição 4.6.2, então*

$$d_{p,rel}(\Lambda) = 2^{\frac{1-p}{4}} p^{\frac{3-p}{4}}.$$

Demonstração: Primeiro, notamos que como o valor da norma mínima de D_n é $\sqrt{2}$, então devemos dividir a distância produto mínima obtida por $\sqrt{2}^n$. Além disso, como o reticulado D_n-rotacionado obtido é uma versão escalonada de D_n por $1/\sqrt{p}$ devemos dividir a distância produto mínima por $(\sqrt{p})^n$. Pela Proposição 4.4.4, temos que $d_p(\sigma_\alpha(I)) = \sqrt{N(\alpha)} min_{0 \neq y \in I} |N(y)| = \sqrt{p}$, pois $N(\alpha) = p$ e $min_{0 \neq y \in I} |N(y)| = 1$. De fato, temos que $min_{0 \neq y \in I} |N(y)| \geq 1$. Mas $e_1 \in I$ e $|N(e_1)| = 1$. Assim,

$$d_{p,rel}\left(\frac{1}{\sqrt{p}}\sigma_\alpha(I)\right) = \left(\frac{1}{\sqrt{p}^{\frac{p-1}{2}}}\right)\left(\frac{1}{\sqrt{2}^{\frac{p-1}{2}}}\right)\sqrt{p} = 2^{\frac{1-p}{4}} p^{\frac{3-p}{4}}.$$

□

Observação 4.6.1. *A distância produto mínima relativa obtida via o* $\mathbb{Z}$*-módulo* I *equivale a metade da distância produto mínima que obteríamos se fosse possível construir tal família de reticulados via ideais principais. No final da seção, vamos mostrar que não é possível reproduzir alguns reticulados desta família via ideais.*

Proposição 4.6.5. *Se* $\Lambda = \frac{1}{\sqrt{p}}(\sigma_\alpha(I)) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ *e* p *primo, então:*

$$\lim_{n \longrightarrow \infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2} \text{ e } \lim_{n \longrightarrow \infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0.$$

p	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(D_n)$
5	2	$0,66870$	$0,47287$	$0,25$	-
7	3	$0,522757$	$0,36965$	$0,125$	$0,17677$
11	5	$0,383215$	$0,27097$	$0,03125$	$0,08838$
13	6	$0,343444$	$0,24285$	$0,01563$	$0,0625$
17	8	$0,289520$	$0,20472$	$0,0039$	$0,03125$
19	9	$0,27187$	$0,19105$	$0,00195$	$0,02209$
23	11	$0,240454$	$0,17003$	$0,00049$	$0,01105$

Tabela 4.2: Distância produto relativa versus densidade de centro

Demonstração: A demonstração é direta. □

A Tabela 4.2 fornece uma comparação entre a $d_{p,rel}$ e a densidade de centro δ dos reticulados $\mathbb{Z}^n$-rotacionados de [51] e D_n-rotacionados construídos anteriormente.

Considerando o "trade-off" entre densidade de empacotamento e distância produto mínima relativa, podemos dizer que os reticulados apresentados aqui possuem melhor performance do que os reticulados $\mathbb{Z}^n$-rotacionados de [51].

Vamos estudar a possibilidade de construir esta família de reticulados D_n-rotacionados via ideais de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Proposição 4.6.6. *Para p primo e $n = (p-1)/2$, não é possível reproduzir a família de reticulados D_n-rotacionados via o homomorfismo de Minkowski aplicado à ideais de $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.*

Demonstração: Temos que $N(\Delta(\mathbb{Q}(\zeta_p + \zeta_p^{-1})|\mathbb{Q})) = |d(\mathbb{K}|\mathbb{Q})| = p^{\frac{p-3}{2}}$ e $\det(D_n) = 4$. Desta forma, é impossível fatorar o diferente como produto de ideais tal que um destes ideais tenha norma par. Portanto, pela Proposição 4.3.3, temos que é impossível reproduzir tal reticulado via o homomorfismo de Minkowski. □

Para alguns valores de p, veremos que não é possível construir reticulados D_n-rotacionados em $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ via o homomorfismo torcido aplicado à ideais de $\mathbb{Z}(\zeta_p + \zeta_p^{-1})$.

Por (4.2), temos que uma condição necessária para construir um reticulado D_n-rotacionado, escalonado por $\sqrt{c}$ com $c \in \mathbb{Z}$, via ideais de $\mathbb{Z}(\zeta_p + \zeta_p^{-1})$, é a existência de um ideal $I \subseteq \mathcal{O}_{\mathbb{K}}$

e um elemento totalmente positivo α tal que

$$4c^n = N(\alpha)N(I)^2|d(\mathbb{K}|\mathbb{Q})|. \tag{4.5}$$

Como p é primo e $p \geq 7$, temos que $|d(\mathbb{K})|\mathbb{Q}| = p^{\frac{p-3}{2}}$ é ímpar, o que implica que

$$2\text{ou deve dividir a norma de } \alpha \text{ ou a norma de } I. \tag{4.6}$$

Vamos estudar quais os valores possíveis para $N(\alpha)$ e $N(I)$ pares. Como será indicado na Proposição 4.6.9, devemos estudar a fatoração do ideal $2\mathcal{O}_{\mathbb{K}}$.

Proposição 4.6.7. *[37] Sejam $A \subseteq B$ anéis. Se $P \subseteq B$ é um ideal primo, então $P \cap A$ é um ideal primo de A.* □

Proposição 4.6.8. *[57] Seja $P \subseteq \mathbb{Z}$ um ideal primo. Se $P\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{s} Q_i^{e_i}$ com Q_i ideais primos de $\mathcal{O}_{\mathbb{K}}$ e $e_i \geq 1$ para todo $i = 1, \cdots, s$, então $Q_i \cap \mathbb{Z} = P$ para $i = 1, \cdots, s$. Além disso, os Q_i são os únicos ideais primos de $\mathcal{O}_{\mathbb{K}}$ cuja intersecção com $\mathbb{Z}$ resulta no ideal primo P.* □

Proposição 4.6.9. *Se $P \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal primo e $p \in \mathbb{Z}$ é um número primo tal que p divide $N(P)$, então P está na fatoração de $p\mathcal{O}_{\mathbb{K}}$ como produto de ideais primos de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Como P é um ideal primo, temos que $P \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$. Portanto, $P \cap \mathbb{Z} = q\mathbb{Z}$ para algum $q \in \mathbb{N}$, q primo. Como q é primo, pela Proposição 4.6.8, temos que P está na fatoração de $q\mathcal{O}_{\mathbb{K}}$, o que implica que $N(P)$ divide $q^n = N(q\mathcal{O}_{\mathbb{K}})$ e segue que $p = q$ pois p e q são números primos. Portanto, P está na fatoração de $p\mathcal{O}_{\mathbb{K}}$. □

Proposição 4.6.10. *Sejam p um número primo tal que $p\mathcal{O}_{\mathbb{K}}$ é um ideal primo e $B \subseteq \mathcal{O}_{\mathbb{K}}$ um ideal tal que p divide $N(B)$. Temos que $N(B) = (p^n)^a b$ onde $a \geq 1$, b não possui p como fator e $n = [\mathbb{K} : \mathbb{Q}]$.*

Demonstração: Seja $B = \prod_{i=1}^{t} P_i^{r_i}$ onde P_i são ideais primos de $\mathcal{O}_{\mathbb{K}}$ e r_i são inteiros. Como p divide $N(B)$ e p é primo, temos que existe um ideal primo $P \in \{P_i, i = 1, \cdots, t\}$ tal que p divide $N(P)$. Pela Proposição 4.6.9, temos que P aparece na fatoração de $p\mathcal{O}_{\mathbb{K}}$ como produto de ideais primos. Como $p\mathcal{O}_{\mathbb{K}}$ é primo, então $P = p\mathcal{O}_{\mathbb{K}}$ e assim $N(P) = p^n$. Como não existe outro ideal primo que aparece na fatoração de $p\mathcal{O}_{\mathbb{K}}$, temos que $N(B) = (p^n)^a b$ com $p \nmid b$. □

Proposição 4.6.11. *Para $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ com $n = (p-1)/2$, se $2\mathcal{O}_\mathbb{K}$ é ideal primo, então não é possível construir o reticulado D_n-rotacionado via o homomorfismo torcido aplicado a ideais de $\mathcal{O}_\mathbb{K}$.*

Demonstração: Seja $2\mathcal{O}_\mathbb{K}$ é um ideal primo em $\mathcal{O}_\mathbb{K}$. Assim, pela Proposição 4.6.10, qualquer ideal B de $\mathcal{O}_\mathbb{K}$ com norma par é tal que $N(B) = (2^n)^a b$ onde $a \geq 1$ e b é ímpar. Note que $N(\alpha) = N(\alpha\mathcal{O}_\mathbb{K})$. Por (4.6), temos que ou o ideal I ou o elemento α devem ter norma par. Assim $N(I) = (2^n)^{a_1} b_1$ e $N(\alpha) = (2^n)^{a_2} b_2$ com $a_1, a_2 \geq 0$, ($a_1 \neq 0$ ou $a_2 \neq 0$), b_1, b_2 ímpares. Desta forma,

$$N(I)^2 N(\alpha)|d(\mathbb{K}|\mathbb{Q})| = (2^n)^{2a_1+a_2}(b_1^2 b_2)|d(\mathbb{K}|\mathbb{Q})| \neq 4c^n \text{ para todo } c \in \mathbb{Z},$$

pois se $c = 2^a b$ então $4c^n = (2^n)^a 2^2 b^n$ e as potências de 2 nunca serão iguais na igualdade acima. Portanto, não é possível encontrar I e α nas condições necessárias. □

Observação 4.6.2. *Temos que $2\mathcal{O}_\mathbb{K}$ é primo por exemplo para $p = 7$ e $p = 11$. Mas, nem sempre $2\mathcal{O}_\mathbb{K}$ é primo em $\mathcal{O}_\mathbb{K}$:*

- *Para $p = 17$ temos que $2\mathcal{O}_\mathbb{K} = P_1 P_2$ com P_1, P_2 ideais primos.*
- *Para $p = 43$ temos que $2\mathcal{O}_\mathbb{K} = P_1 P_2 P_3$ com P_1, P_2, P_3 ideais primos.*

O fato de $2\mathcal{O}_\mathbb{K}$, não ser primo não garante que a condição necessária seja satisfeita. Devemos estudar as possíveis normas para os ideais primos que aparecem na fatoração de $2\mathcal{O}_\mathbb{K}$.

4.7 Reticulados mais densos com diversidade máxima

Em [10, 6] são reproduzidos alguns dos reticulados mais densos na métrica euclidiana via alguns corpos ciclotômicos, ou seja, com diversidade metade da dimensão. A fim de reproduzir os reticulados mais densos na dimensões 3,4,5,7 e 8 com distância produto mínima relativa alta e diversidade máxima, vamos utilizar o homomorfismo torcido e o subcorpo real maximal dos corpos ciclotômicos. Para cada reticulado rotacionado obtido, vamos descrever uma matriz geradora aproximada, visto que as matrizes são obtidas computacionalmente (Programa Mathematica) e possuem erros de aproximação.

O reticulado D_3-rotacionado

Temos que $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = 3$ se, e somente se, $n = 7, 9, 14, 18$. Para o discriminante, temos que $|d(\mathbb{K}|\mathbb{Q})| = 49$ para $n = 7, 14$ e $|d(\mathbb{K}|\mathbb{Q})| = 81$ para $n = 9, 18$.

Proposição 4.7.1. *Para* $K_1 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $K_2 = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, $K_3 = \mathbb{Q}(\zeta_{14} + \zeta_{14}^{-1})$ *e* $K_4 = \mathbb{Q}(\zeta_{18} + \zeta_{18}^{-1})$ *não é possível construir o reticulado* D_3*-rotacionado via o homomorfismo torcido aplicado a ideais de* $\mathcal{O}_{K_i}$.

Demonstração: Temos que o ideal $2\mathcal{O}_{K_i}$ é ideal primo em $\mathcal{O}_{K_i}$ para $i = 1, \cdots, 4$. Assim, o resultado segue da Proposição 4.6.11. □

Na seção anterior vimos que é possível construir o reticulado D_3-rotacionado via $\mathbb{Z}$-módulo de posto 3 em $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

Proposição 4.7.2. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ *e* $e_i = \zeta_7^i + \zeta_7^{-i}$, $i = 1, 2, 3$. *Considere o* $\mathbb{Z}$*-módulo* I *gerado por* $\{e_1, e_2, -e_1 - 2e_2 - 2e_3\}$ *e o elemento* $\alpha = (1 + \zeta_7)(1 - \zeta_7^{-1})$. *Temos que o reticulado* $\frac{1}{\sqrt{7}}\sigma_\alpha(I)$ *é uma versão rotacionado do reticulado* D_3. *Tal reticulado possui diversidade máxima e distância produto mínima relativa* 0.05051. □

Uma matriz geradora para o reticulado D_3-rotacionado descrito acima é dada por

$$\boldsymbol{A} = \begin{pmatrix} 1.06496 & 0.918994 & 0.145967 \\ 0.40899 & -0.263024 & -1.32799 \\ -0.145967 & -1.06496 & 0.918994 \end{pmatrix}.$$

De forma similar ao que foi feito na seção anterior, utilizando o reticulado $\mathbb{Z}^3$-rotacionado de [5] obtemos:

Proposição 4.7.3. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, $e_0 = 1$ *e* $e_i = \zeta_9^i + \zeta_9^{-i}$, $i = 1, 2$. *Considere o* $\mathbb{Z}$*-módulo* J *gerado por* $\{e_0, -e_0 - 2e_1 - 2e_2, -2e_0 - e_1\}$ *e o elemento* $\alpha = ((1 + \zeta_9)(1 - \zeta_9^{-1}))^2$. *Temos que o reticulado* $\frac{1}{\sqrt{9}}\sigma_\alpha(J)$ *é um reticulado* D_3*-rotacionado com distância produto mínima relativa* 0.03928.

Demonstração: Para a distância produto mínima relativa temos que $d(p, rel)\left(\frac{1}{3}\sigma_\alpha(J)\right) = \frac{1}{\sqrt{2}^3}\frac{1}{3^3}\sqrt{9} = 0.03928$, pois $min\{|N(x)|; x \in J\} = 1$. □

Observação 4.7.1. *Sabemos que quando consideramos apenas ideais principais, a distância produto mínima é maior, quando o discriminante do corpo é menor. Neste caso, as duas construções foram feitas via $\mathbb{Z}$-módulos e a distância produto mínima relativa foi maior no reticulado obtido via o corpo com o menor discriminante.*

O reticulado D_4

Para $n = 15, 16, 20, 24, 30$ e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ tem-se que $[\mathbb{K} : \mathbb{Q}] = 4$. Para $n = 15, 30$ tem-se o menor discriminante $d(\mathbb{K}|\mathbb{Q}) = 3^2 5^3$.

Proposição 4.7.4. *Para os corpos $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ onde $n = 15, 30$ não é possível construir um reticulado D_4-rotacionado via o homomorfismo torcido aplicado a ideais de $\mathcal{O}_\mathbb{K}$.*

Demonstração: A demonstração é similar a da Proposição 4.6.11. Como $d(\mathbb{K}|\mathbb{Q}) = 3^2 5^3$ nestes corpos, uma condição necessária para a construção de tal reticulado é encontrar α e I tal que ou 2 divide $N(\alpha)$ ou 2 divide $N(I)$. Como $2\mathcal{O}_\mathbb{K}$ é um ideal primo em tais extensões, não existem tais candidatos. □

Para $n = 16$ o reticulado D_4-rotacionado é um caso particular da construção feita na seção anterior para reticulados D_n-rotacionados com $n = 2^{r-2}$.

Proposição 4.7.5. *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$, $e_0 = 1$ e $e_i = \zeta_{16}^i + \zeta_{16}^{-i}$, $i = 1, 2, 3$. Considere o ideal $I = e_1\mathcal{O}_\mathbb{K}$ e o elemento $\alpha = 2 + (\zeta + \zeta^{-1})$. Temos que o reticulado $\frac{1}{\sqrt{8}}\sigma_\alpha(I)$ é um reticulado D_4-rotacionado. Tal reticulado possui diversidade máxima e distância produto mínima relativa* 0.011048. □

Uma matriz geradora para o reticulado D_4-rotacionado obtido acima é dada por

$$\boldsymbol{A} = \begin{pmatrix} 1.28146 & -0.449988 & -0.300672 & 0.254898 \\ -0.105582 & 0.725887 & -1.08637 & 0.530797 \\ -0.19509 & 0.55557 & 0.83147 & -0.980785 \\ -0.254898 & -0.300672 & 0.449988 & 1.28146 \end{pmatrix}$$

O reticulado D_5-rotacionado

Temos que $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = 5$ se, e somente se, $n = 11, 22$.

Segue das seções anteriores o seguinte resultado:

Proposição 4.7.6. *Para $K_1 = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ e $K_2 = \mathbb{Q}(\zeta_{22} + \zeta_{22}^{-1})$ não é possível construir o reticulado D_5-rotacionado via o homomorfismo torcido aplicado a ideais de $\mathcal{O}_{\mathbb{K}_i}$, $i = 1, 2$.*

Demonstração: Isso se deve ao fato de $2\mathcal{O}_K$ e $2\mathcal{O}_{K_1}$ serem ideais primos em tais extensões e da Proposição 4.6.11. □

Podemos obter o reticulado D_5 como um caso particular dos reticulados D_n-rotacionados para $n = (p-1)/2$, p primo.

Proposição 4.7.7. *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ e $e_i = \zeta_{11}^i + \zeta_{11}^{-i}$. Considere o $\mathbb{Z}$-módulo I gerado por $\{e_1, e_2, e_3, e_4, -e_1 - 2e_2 - 2e_3 - 2e_4 - 2e_5\}$ e o elemento $\alpha = (1-\zeta_{11})(1-\zeta_{11}^{-1})$. Temos que o reticulado $\frac{1}{\sqrt{11}}\sigma_\alpha(I)$ é equivalente ao reticulado D_5. Tal reticulado tem diversidade máxima e possui distância produto mínima* 0.0014609. □

Uma matriz geradora para D_5-rotacionado obtido acima é dada por

$$\begin{pmatrix} 0.625625 & 0.922903 & 0.781753 & 0.378638 & 0.0483561 \\ 0.285843 & 0.270866 & -0.129715 & -0.71842 & -1.14541 \\ 0.141151 & -0.426994 & -0.874547 & -0.156128 & 1.00426 \\ -0.0483561 & -0.625625 & 0.378638 & 0.922903 & -0.781753 \\ -0.22251 & -0.0927946 & 0.766776 & -1.05262 & 0.49591 \end{pmatrix}$$

Reticulado E_7

O reticulado E_7 pode ser visto como um sub-reticulado do reticulado E_8 [23], ou gerado pelos vetores $(2,0,0,0,0,0,0,0)$, $(0,2,0,0,0,0,0,0)$, $(0,0,2,0,0,0,0,0)$, $(0,0,0,2,0,0,0,0)$, $(1,1,1,0,1,0,0,0)$, $(0,1,1,1,0,1,0,0)$, $(0,0,1,1,1,0,1,0)$, $(0,0,1,1,1,0,1)$.

Temos que não existe corpo $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ tal que $[\mathbb{K} : \mathbb{Q}] = 7$. Em [51] é apresentada uma construção para o reticulado $\mathbb{Z}^7$-rotacionado via um subcorpo $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{29} + \zeta_{29}^{-1})$ tal que $[\mathbb{K} : \mathbb{Q}] = 7$, através da chamada *construção cíclica*. Utilizando o fato de E_7 ser um sub-reticulado de $\mathbb{Z}^7$ podemos rotacionar a matriz geradora do E_7 dada pelos vetores acima pela matriz geradora do reticulado $\mathbb{Z}^7$-rotacionado que tem como matriz de Gram a matriz identidade.

Como este reticulado E_7-rotacionado é um sub-reticulado do reticulado $\mathbb{Z}^7$-rotacionado, temos que sua distância produto mínima é limitada inferiormente pela distância produto

mínima do reticulado $\mathbb{Z}^7$-rotacionado, que é dada por $\sqrt[7]{\boldsymbol{d}_{p,min}(\mathbb{Z}^7)} = 0.23618$. Como a norma mínima de E_7 é $\sqrt{2}$ temos que tirar o fator de correção e com isso temos que $\sqrt[7]{\boldsymbol{d}_{p,rel}(E_7)} \geq 0.16700479$.

Uma matriz geradora para o reticulado E_7-rotacionado é dada por

$$\boldsymbol{A} = \begin{pmatrix} -1.36187 & 0.326205 & -0.897706 & 0.154763 & 0.164643 & 0.55111 & -0.937142 \\ 0.326205 & -0.897706 & 0.154763 & 0.164643 & 0.55111 & -0.937142 & -1.36187 \\ -0.897706 & 0.154763 & 0.164643 & 0.55111 & -0.937142 & -1.36187 & 0.326205 \\ 0.154763 & 0.164643 & 0.55111 & -0.937142 & -1.36187 & 0.326205 & -0.897706 \\ -0.884365 & 0.067186 & -0.757721 & -0.245679 & 0.0524079 & -1.32281 & -0.909024 \\ 0.067186 & -0.757721 & -0.245679 & 0.0524079 & -1.32281 & -0.909024 & -0.884365 \\ -0.757721 & -0.245679 & 0.0524079 & -1.32281 & -0.909024 & -0.884365 & 0.067186 \end{pmatrix}.$$

Reticulado E_8

Para $n = 17, 32, 34, 40, 48, 60$, $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ tem-se $[\mathbb{K} : \mathbb{Q}] = 8$.

Para $n = 17, 32, 34, 40, 48$ utilizamos o software "Mathematica" para procurar por um elemento α e um ideal I satisfazendo as equações (4.2). Através de tal busca não conseguimos reproduzir o reticulado E_8-rotacionado em tais corpos via ideais. Como nossa busca só percorreu uma parte dos ideais de $\mathcal{O}_{\mathbb{K}}$ não podemos garantir que não é possível reproduzir tal reticulado nestes corpos.

Proposição 4.7.8. *Considere o $\mathbb{Z}$-módulo $I \subseteq \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$ com $\mathbb{Z}$-base*

$$\left\{-2, -e_1, -e_2, -e_3, -e_4, -e_5, -e_6, \frac{8}{2}e_8 + \frac{7}{2}e_7 + \cdots + \frac{2}{2}e_2 + \frac{1}{2}e_1\right\}$$

e o elemento $\alpha = (1 - \zeta_{17})(1 - \zeta_{17}^{-1}) = 2 - e_1$. Temos que o reticulado $\frac{1}{\sqrt{17}}\sigma_\alpha(I)$ é um reticulado E_8-rotacionado com distância produto mínima relativa 0.102360784.

Demonstração: Neste caso, para rotacionar o reticulado E_8, utilizamos a matriz geradora para o reticulado $\mathbb{Z}^8$-rotacionado de [51], cuja matriz de Gram é a identidade. Desta forma, obtemos o $\mathbb{Z}$-módulo I. Note que $2I \subseteq \mathcal{O}_{\mathbb{K}}$ e, então, $min\{|N(x)|;\ 0 \neq x \in 2I\} \geq 1$. Como $N(8e_8 + 7e_7 + 6e_6 + 5e_5 + 4e_4 + 3e_3 + 2e_2 + e_1) = 1$, segue que $min\{|N(x)|;\ 0 \neq x \in 2I\} = 1$ e $min\{|N(x)|;\ 0 \neq x \in I\} = 1/2^8$. Assim, $\boldsymbol{d}_{p,rel}\left(\frac{1}{\sqrt{17}}\sigma_\alpha(I)\right) = \frac{1}{\sqrt{17}^8}\frac{1}{\sqrt{2}^8}\sqrt{17}\frac{1}{2^8} = 0.0000000120523$. Portanto, $\sqrt[8]{\boldsymbol{d}_{p,rel}\left(\frac{1}{\sqrt{17}}\sigma_\alpha(I)\right)} = 0.102360784$. □

Uma matriz geradora para o reticulado E_8-rotacionado é dada por

$$\begin{pmatrix} -0.17826 & -0.35046 & -0.51071 & -0.65358 & -0.77419 & -0.86844 & -0.93311 & -0.96600 \\ -0.16623 & -0.2589 & -0.22765 & -0.060305 & 0.21187 & 0.5234 & 0.79334 & 0.94956 \\ -0.13174 & -0.03234 & 0.30777 & 0.64245 & 0.6582 & 0.23766 & -0.41592 & -0.90077 \\ -0.07945 & 0.21119 & 0.50202 & 0.17886 & -0.57213 & -0.80979 & -0.08609 & 0.82131 \\ -0.01645 & 0.34449 & 0.13976 & -0.60945 & -0.34509 & 0.73836 & 0.56232 & -0.71389 \\ 0.04878 & 0.29796 & -0.37742 & -0.29133 & 0.76101 & -0.080129 & -0.87009 & 0.58215 \\ 0.10743 & 0.095907 & -0.47623 & 0.55569 & -0.07143 & -0.64178 & 0.91722 & -0.43059 \\ -1.30869 & -0.02267 & -0.42621 & -0.04698 & -0.24354 & -0.07509 & -0.16059 & -0.11055 \end{pmatrix}$$

Densidade versus distância produto mínima

Existem algumas construções conhecidas de reticulados $\mathbb{Z}^n$-rotacionados nas dimensões estudadas com distância produto mínima maior que as obtidas nas construções acima, porém a densidade de empacotamento do reticulado $\mathbb{Z}^n$ é muito menor que a densidade de empacotamento dos reticulados analisados neste trabalho, esta diferença cresce muito com a dimensão. A tabela abaixo relaciona a distância produto mínima relativa de construções conhecidas do reticulado $\mathbb{Z}^n$-rotacionado com as construções aqui apresentadas, bem como a densidade de centro. Note que quando a dimensão vai aumentando a densidade de centro do reticulado $\mathbb{Z}^n$ vai ficando expressivamente menor que a densidade de centro dos reticulados construídos e a distância produto mínima dos reticulados algébricos construídos diminui em proporçoes menores.

n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(\Lambda)}$	$\delta(\mathbb{Z}^n)$	$\delta(\Lambda)$
3	$0,522757$	$0,36965$	$0,125$	$0,17677$
4	$0,385553$	$0,3242059$	$0,062500$	$0,125000$
5	$0,383215$	$0,2709718$	$0,03125$	$0,08838$
7	$0,23618$	$\geq 0,1670048$	$0,0078125$	$0,0625$
8	$0,289520$	0.1023608	$0,003906$	$0,0625$

Tabela 4.3: Distância produto relativa versus densidade de centro

PERSPECTIVAS FUTURAS

Colocamos aqui algumas perspectivas futuras que são extensões naturais deste trabalho, às quais temos interesse em dar continuidade.

Decodificação em reticulados q-ários na métrica d_p, $1 \leq p < \infty$:

Neste trabalho, obtemos uma relação entre a decodificação de reticulados q-ários na métrica d_1 com a decodificação do código q-ário associado pela Construção A na métrica de Lee (métrica induzida da métrica d_1). Temos interesse em estudar a decodificação na métrica d_p, $p \leq 2$. Além disso, gostaríamos de analisar se a Construção A nos fornece reticulados com características especiais quando o código utilizado na construção é especial, como por exemplo, códigos BCH.

Decodificação de reticulados obtidos via Construção B na métrica de Lee:

Da mesma forma como fizemos para a Construção A, gostaríamos de obter uma relação entre a decodificação de reticulados obtidos via Construção B com a decodificação de um conjunto de representantes do código associado. Já sabemos que o mesmo tipo de relação envolvendo métrica d_1 e a métrica de Lee não é válido, mas temos indícios de que um resultado similar é valido alterando a distância no conjunto de representantes do código associado.

Uso de reticulados q-ários em criptossistemas pós-quânticos:

Um foco de nosso interesse é o da aplicabilidade da pesquisa sobre reticulados e decodificação em diferentes métricas em criptografia. Com uma investigação inicial sobre reticulados q-ários, temos interesse em estudar sistemas criptográficos utilizando tais reticulados e os resultados obtidos envolvendo esta classe.

Estudo de reticulados para processos de codificação dirty-paper:

Códigos dirty-paper são utilizados para transmissão eficiente de dados digitais através de um canal sujeito à alguma interferência conhecida pelo transmissor. Tais códigos foram introduzidos por Max H. Costa em 1983 [24] e têm sido retomados sob novas premissas nos anos recentes. Alguns dos problemas envolvendo dirty-paper têm sido abordados a partir de um par de reticulados encaixados onde um deles seja subjacente a um bom código para o canal e o outro um bom código de fonte [68]. Nosso objetivo é utilizar ferramentas como as Construções A e B na busca por reticulados para serem utilizados em processos de codificação dirty-paper, bem como as técnicas de decodificação propostas em [18] utilizando outras métricas que não a euclidiana.

Construção de reticulados algébricos como suporte para constelação de sinais:

Tendo em vista construir reticulados que apresentam uma constelação de sinais eficiente para a transmissão simultânea sobre os canais gaussiano e do tipo Rayleigh com desvanecimento, neste trabalho, construímos famílias de reticulados D_n-rotacionados com diversidade máxima. Temos interesse em reproduzir outros reticulados mais densos conhecidos em dimensões baixas com diversidade máxima e calcular sua distância produto mínima. Além disso, queremos estudar condições necessárias para quando é possível reproduzir um dado reticulado, por exemplo, no caso do reticulado E_8, queremos saber se é possível reproduzi-lo via ideais no subcorpo real maximal dos corpos ciclotômicos e se não for possível, queremos entender o porquê. Durante nossa pesquisa, conjecturamos que reticulados equivalentes na métrica euclidiana obtidos via ideais principais de um mesmo corpo de números e com

mesma distância produto mínima são equivalentes na métrica de Lee e temos interesse em investigar este fato. Pensando em reticulados que sejam eficientes somente para o canal do tipo Rayleigh com desvanecimento, queremos buscar novas construções de reticulados $\mathbb{Z}^n$-rotacionados que ainda não foram feitas, como por exemplo para os corpos $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ para p primo. Um outro fato que pretendemos investigar é se a construção de reticulados via $\mathbb{Z}$-módulos que não são ideais origina uma distância produto mínima relativa menor do que a construção feita via ideais.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] C. Alves, *Reticulados e Códigos*, Tese de Doutorado, IMECC-UNICAMP, 2008.

[2] M.M.S. Alves, *Códigos Geometricamente Uniformes em Espaços de Lee*, Dissertação de Mestrado, IMECC-UNICAMP, 1998.

[3] A.A. Andrade, *Uma contribuição a construção e decodificação de codigos de bloco lineares sobre aneis finitos,* Tese de Doutorado, FEEC-UNICAMP, 1996.

[4] A.A. Andrade, C. Alves, T.B. Carlos, *Rotated lattices via the cyclotomic field* $\mathbb{Q}(\zeta_{2^r})$, International Journal of Applied Mathematics, v.19, n.3, p.321-331, 2006.

[5] A.A. Andrade, C. Alves, T.B. Carlos, *New constructions of rotated lattices*, International Journal of Applied Mathematics, v.20, p. 1079-1087, 2007.

[6] A.A. Andrade, A.J. Ferrari, C.W.O. Benedito, S.I.R. Costa, *Constructions of algebraic lattices*, Computational & Applied Mathematics, v.29, n.3, p.1-13, 2010.

[7] A. A. Andrade, J. C. Interlando and R. Palazzo Jr., *Alternant and BCH codes over certain rings,* Computational and Applied Mathematics, v.22, p.233-247, 2003.

[8] A.H. Banihashemi, *Decoding Complexity and Trellis Structure of Lattices*, Tese de Doutorado, University of Waterloo, Canada, 1997.

[9] A.H. Banihashemi and I.F. Blake, *Trellis complexity and minimal trellis of lattices*, IEEE Transactions on Information Theory, v.44, n.5, p. 1829-1847, 1998.

[10] E. Bayer-Fluckiger, *Lattices and number fields*, Contemporary Mathematics, v.241, p.69-84, 1999.

[11] E. Bayer-Fluckiger, *Ideal lattices,* Proceedings of the conference Number theory and Diophantine Geometry, Zurich, 1999, Cambridge Univ. Press 2002, p.168-184.

[12] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, *Algebraic lattice constellations bounds on performance*, IEEE Transactions on Information Theory, v.52, n.1, p.319-327, 2006.

[13] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, *New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel*, IEEE Trans. Inform. Theory, v.50, n.4, p.702-714, 2004.

[14] E. Bayer-Fluckiger, G. Nebe, "On the Euclidean minimum of some real number fields", Journal de theorie des nombres de Bordeaux, v.17 n.2, p. 437-454, 2005.

[15] A.F. Beardon, *The geometry of discrete groups,* Springer, 1995.

[16] E. R. Berlekamp. *Algebraic Coding Theory*, revised edition, Laguna Hills, CA Aegean Park Press, 1984.

[17] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiori, *Good lattice constellations for both rayleigh fading and gaussian channels,* IEEE Trans. Inform. Theory, v.42, n.2, p.502-517, 1996.

[18] A.C. Campello, G.C. Jorge, S.I.R. Costa, *Decoding q-ary lattices in the Lee metric*, Proceedings of 2011 IEEE Information Theory Workshop, ISBN 978-4577.0436-9, disponível em IEEE-Xplore, Paraty, Brasil, 2011.

[19] A.C. Campello, G.C. Jorge, S.I.R. Costa, *Decoding integer lattices in the Lee metric*, artigo submetido, arXiv:1105.5557.

[20] T.B. Carlos, *Abordagem Algébrica e Geométrica de Reticulados*, Tese de Doutorado, IMECC-UNICAMP, 2007.

[21] H. Cohen, *A course in Computational Algebraic Number Theory*, Springer, 1993.

[22] H. Cohn, A. Kumar, *Optimality and uniqueness of the Leech lattice among lattices,* Annals of Mathematics, Princeton, v.170, p. 1003-1050, 2009.

[23] J.H. Conway, N.J.A Sloane, *Sphere Packings, Lattices and Groups*, Springer, 1999.

[24] M. Costa, *Writing on dirty paper*, IEEE Transactions on Information Theory, v.29, n.3, p.439-441, 1983.

[25] S.I.R. Costa, J.E. Strapasson, M.M.S. Alves, T.B. Carlos, *Circulant graphs and tesselations on flat tori*, Linear Algebra and its Applications, v. 432, p.369-382, 2010.

[26] S.I.R. Costa, J.R. Gerônimo, R. Palazzo Jr., J.C. Interlando, M.M. Silva, *The symmetry group of $\mathbb{Z}_q^n$ in the Lee space and the $\mathbb{Z}_{q^n}$*-linear codes, Applied algebra, algebraic algorithms and error-correcting codes, Toulouse, 1997, p.66-77, Lecture Notes in Computer Science, 1255, Springer, Berlim, 1997.

[27] P.D. Domich, R. Kannan, L.E. Trotter Jr., *Hermite Normal Form Computation Using Modulo Determinant Arithmetic.* Math. Operations Res. v.12, p. 50-59, 1987.

[28] U. Erez, L. Simon, R. Zamir, *Lattices which are good for (almost) everything*, IEEE Transactions on Information Theory, v. 51, n.10, 2005.

[29] T. Etzion, A. Vardy, E. Yaakobi, *Dense Error-Correcting Codes in the Lee Metric*, IEEE Information Theory Workshop, ITW 2010 Dublin, 2010.

[30] A.J. Ferrari, C. Torezzan, G.C. Jorge, S.I.R. Costa, "Um Algoritmo de Treliça para Decodificação de Códigos de Grupo Comutativo" XXVII Simpósio Brasileiro de Telecomunicações, Blumenau, SC, (29/09-02/10), 2009.

[31] G. D. Forney, Jr and M. D. Trott, "The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders," IEEE Trans. Inform. Theory, vol IT-39, no 9, pp. 1491-1513, Sept. 1993.

[32] W.S. Golomb, L.R. Welch, *Perfect codes in the lee metric and the packing of polyminoes* SIAM J. Appl. Math. v. 18, n.2, January 1970.

[33] D. Guo, S. Shamai and S. Verdú, *Additive Non-Gaussian Noise Channels: Mutual Information and Condition Mean Estimation*, IEEE International Symposium on Information Theory, 2005.

[34] B. Hassibi, H. Vikalo, *On the Sphere Decoding Algorithm I. Expected Complexity,* IEEE Transactions on Signal Processing, v.53, n.8, Augusto 2005.

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

[36] G.C. Jorge, S.I.R.Costa, *Decodificação em reticulados q-ários via Construção A*, 1 Encontro em Teoria de dos Códigos e Criptografia, UFABC, 2010, a ser publicado em ATA do 1 Encontro em Teoria dos Códigos e Criptografia.

[37] G.C. Jorge, *Reticulados Ideais via Corpos Abelianos*, Dissertação de Mestrado, Ibilce - Unesp, São José do Rio Preto, 2008.

[38] G.C. Jorge, A.J. Ferrari, S.I.R. Costa, *Rotated D_n-lattices*, artigo submetido, arXiv:1111.3787v1.

[39] G.C. Jorge, A.J. Ferrari, S.I.R. Costa, *Treliça mínima em reticulados bidimensionais*, Congresso Nacional de Matemática Aplicada e Computacional, 2010.

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

[41] C.Y. Lee, *Some properties of nonbinary error-correcting code*, IRE Transactions on Information Theory, v.4, p.72-82, 1958.

[42] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovaz. *Factoring polynomials with rational coefficients. Math. Ann*, 1982.

[43] J.O.D. Lopes, T.P. da N. Neto, J.C. Interlando, *On computing discriminant of subfields of* $\mathbb{Q}(\zeta_{p^r})$, Journal of Number Theory, v.96, n.2, p.319-325, Outubro, 2002.

[44] J.O.D. Lopes, *Discriminants of subfields of* $\mathbb{Q}(\zeta_{2^r})$, Journal of Algebra Appl, v.2, p.463-469, 2003.

[45] D.A. Marcus, *Numbers Fields,* New York: Springer-Verlag, 1977.

[46] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Springer-Verlag Berlin Heidelberg, 2003.

[47] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory", Jet Propulsion Laboratory DSN Progress Report, 42-44, p.114-116, 1978.

[48] D. Micciancio, O. Regev, *Lattice-Based Cryptography* em *Post Quantum Cryptography,* D.J. Bernstein, J. Buchmann, E. Dahmen (eds), p.147-191, Springer, 2009.

[49] D. Micciancio, S. Goldwasser, Complexity of Lattices Problems; A Cryptographic Perspective, The Kluwer International Series in Engeneering as Computer Science, v. 671, Kluwer Academic Publishers, 2002

[50] F.C.P. Milies, *Anéis e Módulos*, São Paulo: L.P.M, 1972.

[51] F. Oggier, *Algebraic methods for Channel Coding,* Tese de Doutorado, EPFL, Lausane, 2005.

[52] R. Palazzo Jr, J.C. Interlando, J.R. Geronimo, A.A. Andrade, O.M. Favareto, M.C. Araújo, T.P.N. Neto, G.O. Santos, *Fundamentos Algébricos e Geométricos dos Códigos Corretores de Erros*, Departamento de Telemática DT - Unicamp, 2006.

[53] P. Ribenboim, *Algebraic numbers*, Wiley - Interscience, 1972.

[54] P. Ribenboin, *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

[55] R.M. Roth, P.H. Siegel *Lee-Metric BCH Codes and their Application to Constrained and Partial-Response Channels.* IEEE Transactions on Information Theory, v. 40, n.4, Julho, 1994.

[56] J.A. Rush, N.J.A Sloane, *An improvement to the Minkowiski-Hlawka bound for packing superballs*, Mathematika, v. 34, p.8-18, 1987.

[57] P. Samuel, *Algebraic Theory of Numbers*, Paris: Hermann, 1970.

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

[59] C. E. Shannon, *A Mathematical Theory of Communications* BSTJ 27, p.379-423 e 623-656, 1948.

[60] P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Review, v.41, n. 2, pp.303-332, 1999.

[61] I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, London: Chapman & Hall, 1987.

[62] J.E. Strapasson, *Geometria Discreta e Códigos*, Tese de Doutorado, IMEEC-UNICAMP, 2007.

[63] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, Cambridge: University of Cambridge, 2001.

[64] K. Takizawa, H. Yagi, T. Kawabata, *Closest Point Algorithms with l_p Norm for Root Lattices*, Proceedings of IEEE International Symposium on Information Theory, Austin, Texas, p.1042-1046, 2010

[65] E. Viterbo, E. Biglieri, *A universal decoding algorithm for lattices codes*, Quatorzieme Colloque Gretsi - Juan-Les-Pins, 13/09-16/09, 1993.

[66] E. Viterbo, J. Boutros, *A universal Lattice Code Decoder for Fading Channels*, IEEE Transactions on Information Theory, v.45, n.5, Julho, 1999.

[67] L.C. Washington, *Introduction to Cyclotomic Fields*, New York: Springer-Verlag, 1982.

[68] R. Zamir, *Lattices are everywhere*, in Proceedings of the 4th Annual Workshop on Information Theory and its Applications (ITA 2009), (La Jolla, CA), February 2009.

[69] Zhao F., Qiao S. *Radius Selection Algorithms for Sphere Decoding*, Proceedings of the 2nd Canadian Conference on Computer Science and Software Engineering, (2009).

ÍNDICE REMISSIVO