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

Um Estudo sobre o Problema do Vetor mais Próximo nos Reticulados Raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$: Algoritmos e Simulações Numéricas

Drielson Dávison Silva Gouvêa

drielsondsg@gmail.com

Dissertação de Mestrado

Orientador(a): **Prof. Dr.Cristiano Torezzan**

Agosto de 2011
Campinas - SP

Um Estudo sobre o Problema do Vetor mais Próximo nos Reticulados Raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$: Algoritmos e simulações numéricas.

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Drielson Dávison Silva Gouvêa** e aprovada pela comissão julgadora.

Campinas, 15 de agosto de 2011.

Banca Examinadora:

Prof°. Dr. Cristiano Torezzan (UNICAMP - FCA)

Prof°. Dr. João Eloir Strapasson (UNICAMP - FCA)

Profª. Drª. Carina Alves (UNESP-RIO CLARO)

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, **UNICAMP**, como requisito parcial para obtenção de Título de **Mestre em Matemática Universitária**.

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

G745e	Gouvêa, Drielson Dávison Silva, 1976- Um estudo sobre o problema do vetor mais próximo nos reticulados raízes Z^n, An e Dn : algoritmos e simulações numéricas / Drielson Dávison Silva Gouvêa. - Campinas, SP: [s.n.], 2011. Orientador: Cristiano Torezzan. Dissertação (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica. 1. Teoria dos reticulados. 2. Algoritmos – Métodos de simulação. 3. Geometria discreta. 4. Teoria da informação em matemática. I. Torezzan, Cristiano, 1976-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em Inglês: A study of the closest vector problem in roots lattices Z^n, An and Dn : algorithms and numerical simulations
Palavras-chave em Inglês:
Lattice theory
Algorithms – Simulation methods
Discrete geometry
Information theory in mathematics
Área de concentração: Matemática Universitária
Titulação: Mestre em Matemática Universitária
Banca examinadora:
Cristiano Torezzan [Orientador]
João Eloir Strapasson
Carina Alves
Data da defesa: 15-08-2011
Programa de Pós-Graduação: Matemática Universitária

Dissertação de Mestrado Profissional defendida em 15 de agosto de 2011 e aprovada pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). CRISTIANO TOREZZAN

Prof. (a). Dr (a). JOÃO ELOIR STRAPASSON

Prof. (a). Dr (a). CARINA ALVES

À minha esposa Joise e aos meus filhos Adryan e Hannah.

Dedico.

Agradecimentos

Embora uma dissertação seja, pela sua finalidade acadêmica, um trabalho individual, há contributos de natureza diversa que não podem nem devem deixar de ser realçados. Por essa razão, desejo expressar os meus sinceros agradecimentos.

Antes de tudo, quero agradecer a DEUS por ter me concedido esta oportunidade e ter me abençoado em todos os dias da minha vida.

Aos meus queridos pais Ritacínio e Maria Galiléia, vocês são os tesouros da minha vida, tento aqui recompensá-los por todo o incentivo, carinho e esforço dado na construção da minha educação.

A Minha esposa Joise, que foi a primeira a me incentivar neste projeto, você é a base da nossa família, não teria chegado aqui sem o seu apoio, sem sua compreensão e principalmente sem seu carinho.

Aos meus lindos filhos, Adryan Lucas e Hannah Yasmim, pela compreensão nos momentos ausentes e aos meus queridos irmãos pelo incentivo diário.

Agradeço ao meu orientador e amigo Prof°.Cristiano Torezzan pelo seu incetivo, seu apoio, sua paciência, pela partilha do saber e das valiosas contribuições para o trabalho. Sempre o terei como exemplo durante a minha carreira docente.

A Professora Sueli Costa pelo incentivo, aos professores do Mestrado pelo ensino e aos monitores João Paulo, Agnaldo Ferrari e Lívia Minami pela dedicação e amizade.

A Dona Neide, da pousada Nova Barão, pela amizade e pelas constantes orações durante minha estada em Campinas.

Ao Sistema de Ensino Universo pela oportunidade de me liberar para realizar este mestrado, tenho um grande orgulho de fazer parte desta familia. Em especial, quero agradecer aos diretores Manoel Lisboa, Heraldo Cañizo, Jurueno Sampaio e Júlio Reis pelo grande apoio dado durante este mestrado.

Resumo

Neste trabalho estuda-se o problema do vetor mais próximo em reticulados. Este problema consiste em encontrar um vetor de um reticulado mais próximo de um ponto dado do $\mathbb{R}^n$ e é conhecido também como problema da decodificação em reticulados. Estuda-se de forma específica algoritmos para o problema do vetor mais próximo para os reticulados raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$. Além de uma breve revisão da literatura, os algoritmos para decodificação nesses reticulados são apresentados em detalhes, incluindo exemplos e também os códigos utilizados para implementação desses métodos na linguagem do software livre Scilab. Algumas simulações numéricas foram feitas utilizando esses códigos para investigar o tempo gasto na decodificação em função da dimensão do reticulado.

Palavras-chave: Reticulados, Problema do vetor mais próximo, algoritmos e decodificação.

Abstract

In this paper we study the nearest vector problem in lattices. This problem consists in finding a vector of a lattice closest to a given point of $\mathbb{R}^n$ and is also known as the decoding problem in lattices. It is studied in a specific algorithms for the nearest vector problem for lattices roots $\mathbb{Z}^n$, $\mathbb{A}_n$ and $\mathbb{D}_n$. Besides a brief review of the literature, algorithms for decoding these lattices are presented in detail, including examples and also the codes used to implement these methods in the language of the free software Scilab. Some numerical simulations were done using these codes to investigate the time spent in decoding according to the size of the lattice.

Keywords: Lattices, closest vector problem, algorithms and decoding .

Sumário

Introdução

O estudo de reticulados tem apresentado conexões com muitas áreas da matemática e da engenharia. Além de sua conhecida relação com problemas empacotamentos e coberturas esféricas, novas aplicações têm surgido, dentre as quais o processo de decodificação em reticulados que consiste no fato de, dados um reticulado e um vetor no espaço euclidiano n-dimensional, deve-se encontrar o ponto do reticulado mais próximo de tal vetor com respeito a distância euclidiana. Este é um problema NP-Completo para o caso geral mas pode ser eficientemente resolvido em alguns casos, como nos reticulados raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$, i.e.,

- $\mathbb{Z}^n = \{x \in \mathbb{R}^n : x_i \in \mathbb{Z}\}$.
- $\mathbb{A}_n = \left\{ x \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0 \right\}$.
- $\mathbb{D}_n = \left\{ x \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \in 2 \cdot \mathbb{Z} \right\}$.

O objetivo deste trabalho é mostrar algumas simulações numéricas (algoritmos) eficientes para decodificar nos reticulados raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$ utilizando a linguagem do software livre Scilab. Essas simulações decorrem de propriedades especiais destes reticulados. No entanto, ainda não se conhece algoritmo capaz de decodificar reticulados n-dimensionais quaisquer em tempo polinomial.

Esta dissertação é constituída de quatro capítulos. O Capítulo 1 é dedicado aos conceitos básicos necessários ao desenvolvimento do trabalho, começando por um estudo detalhado sobre reticulados, que vem sendo muito utilizados na Teoria das Comunicações.

No Capítulo 2 daremos ênfase aos reticulados raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$ e seus duais, onde estudaremos em detalhes suas matrizes geradoras e de Gram, além de outras propriedades como vetor de norma mínima, densidade de empacotamento e de centro.

O Capítulo 3 aborda alguns dos principais problemas em reticulados começando com a explanação do problema da redução de base em reticulados, incluindo o método de Gauss para a redução de bases em reticulados de duas dimensões e o algoritmo LLL (Lenstra, Lenstra e Lovász). Em seguida introduzimos a definição do Problema do Vetor mais Curto (PVMC) que consiste em "dado um reticulado $\Lambda \in \mathbb{R}^n$, determinar o vetor não nulo de norma mínima de Λ". Este problema é NP - completo [15]. A última parte do capítulo 3 é dedicada ao Problema do Vetor mais Próximo (PVMP) que consiste em "dado $b \in \mathbb{R}^n$, determinar o vetor u pertencente a um reticulado Λ cuja distância a b é mínima". O Problema do Vetor mais Próximo também é NP - completo [15]. Daremos uma ênfase maior a este problema, já que a idéia central desta dissertação diz respeito ao mesmo.

O Capítulo 4 destina-se a apresentar em detalhes alguns algoritmos para decodificação nos reticulados raízes $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$ que solucionam o Problema do Vetor mais Próximo. Neste capítulo foram feitas algumas simulações numéricas utilizando os códigos correspondentes na linguagem do software livre Scilab. O objetivo principal destas simulações é investigar o tempo gasto na decodificação em função da dimensão do reticulado.

Capítulo 1

Teoria dos Reticulados

Este capítulo será dedicado a Teoria de Reticulados. As principais referências para este capítulo são: [1, 4, 15, 23, 24, 25].

O estudo dos reticulados têm encontrado inúmeras aplicações na matemática e na ciência da computação, que vão desde a teoria dos números e da aproximação diofantina até a otimização combinatória e a criptografia. Apesar da sua aparente simplicidade, os reticulados escondem uma rica estrutura combinatorial. Seu estudo detalhado têm atraído a atenção de grandes matemáticos devido aos enormes avanços nos últimos dois séculos.

Neste capítulo, tentaremos ver um panorama geral dos reticulados no $\mathbb{R}^m$ e de alguns dos problemas mais importantes relacionados com eles, como: empacotamento de esferas, cobertura com esferas e o kissing number (número de contato). Para isto, começaremos com as definições básicas de tópicos importantes e propriedades fundamentais sobre este assunto.

1.1 Reticulados

Definição 1.1 *Seja $\mathbb{R}^m$ um espaço Euclidiano m-dimensional. Um reticulado Λ em $\mathbb{R}^m$ é um subgrupo aditivo, em relação a operação usual de adição, formado por todas as combinações lineares, à coeficientes inteiros, de $\boldsymbol{n}$ vetores linearmente independentes $b_1, b_2, ..., b_n \in \mathbb{R}^m$ $(m \geq n)$, i. e.,*

$$\Lambda(b_1, ..., b_n) = \left\{ \sum_{i=1}^{n} \alpha_i b_i : \alpha_i \in \mathbb{Z} \right\}$$

Os inteiros n e m são chamados de *posto* e *dimensão* de um reticulado, respectivamente [15]. Os vetores $b_1, b_2, ..., b_n$ são chamados de vetores da base de Λ e o conjunto $\beta = \{ b_1, ..., b_n\}$ é chamado de *base do reticulado* Λ e é convenientemente representada pela matriz

$$B = (b_1, ..., b_n) \in \mathbb{R}^{n \times m}$$

denominada *matriz geradora*, que possui os vetores da base como colunas. Qualquer reticulado está bem determinado se conhecermos uma matriz geradora. Em outras palavras, um reticulado n - dimensional é a imagem de $\mathbb{Z}^n$ por uma tranformação linear $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$, $(m \geq n)$, de posto completo.

Usando esta notação, podemos redefinir um reticulado Λ da seguinte maneira

$$\Lambda(B) = B \cdot \mathbb{Z}^n \triangleq \{B\alpha : \alpha \in \mathbb{Z}^n\}$$

onde $B\alpha$ é a multiplicação usual entre um vetor e uma matriz.

Como qualquer subgrupo do grupo aditivo do $\mathbb{R}^n$, um reticulado Λ é um conjunto infinito de vetores do $\mathbb{R}^n$, tal que a soma de dois vetores de Λ também é um vetor de Λ. A origem é o vetor identidade de Λ, e se $v \in \Lambda$, então $(-v) \in \Lambda$; é claro, então, que todos os múltiplos inteiros de um vetor de Λ são vetores distintos de Λ, e que a diferença entre dois vetores de Λ também é um vetor de Λ. A restrição de existir, para um reticulado, um conjunto gerador de vetores linearmente independentes do $\mathbb{R}^n$ é exatamente o que o diferencia dos demais subgrupos aditivos do $\mathbb{R}^n$.

Exemplo 1.1 *O conjunto $\mathbb{Z}^n$ de todas a n-uplas de inteiros é um reticulado do $\mathbb{R}^n$, tendo a base vetorial canônica $\{ e_1, ..., e_n\}$ do $\mathbb{R}^n$ (onde $e_i, i = 1, ..., n$, é o vetor com **1** na i-ésima coordenada e **0** nas demais coordenadas) como um conjunto gerador ou base.*

Este reticulado será chamado *reticulado canônico* ou *padrão*, seu estudo detalhado será visto mais adiante na secção que fala sobre reticulados raízes.

Graficamente, um reticulado pode ser descrito como um conjunto de pontos que estão na intersecção de uma infinita malha regular n- dimensional.

Nas figuras 1.1 e 1.2 a seguir, temos alguns exemplos de reticulados no plano. Destacamos aqui um reticulado que será constantemente citado ao longo desta dissertação, e que representaremos por $\bar{\Lambda}$.

Exemplo 1.2 *Reticulado padrão bidimensional $\mathbb{Z}^2 \subset \mathbb{R}^2$.*

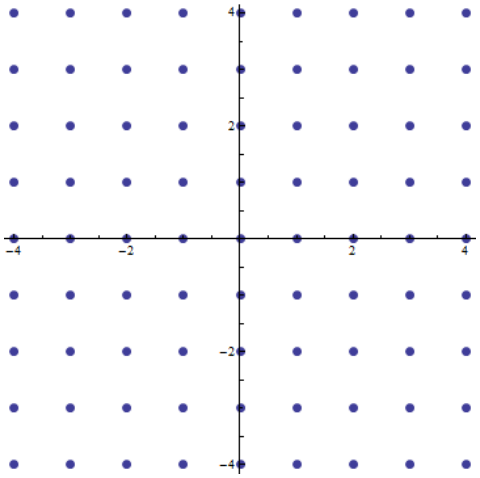


Figura 1.1: Reticulado $\mathbb{Z}^2 \subset \mathbb{R}^2$.

Exemplo 1.3 *$\bar{\Lambda} \subset \mathbb{R}^2$ é um reticulado gerado pela base de vetores $b_1 = (1, 2)^T$ e $b_2 = (-3, 1)^T$, ou seja, sua matriz geradora A dada por*

$$A = \begin{pmatrix} 1 & -3 \\ 2 & 1 \end{pmatrix},$$

Alguns pontos de $\bar{\Lambda}$ estão representado na figura 1.2.

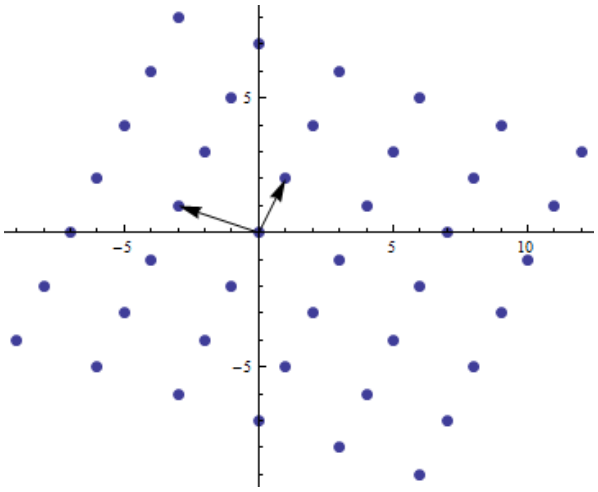


Figura 1.2: Reticulado $\bar{\Lambda} \subset \mathbb{R}^2$. Destaque para os vetores da base b_1 e b_1.

A dimensão é uma propriedade importante de qualquer reticulado. A dimensão de um reticulado Λ é igual ao número de vetores que compõem a base sendo denotado por $dim\,(\Lambda)$. Um reticulado é dito *dimensionalmente completo* (ou *ordenadamente completo*) quando $dim\,(\Lambda) = n$, [10].

Quando $dim\,(\Lambda) \geq 2$, o reticulado admite infinitamente muitas bases (todas com o mesmo número de vetores) e todas as bases estão relacionadas por uma matriz unimodular.

Mais especificadamente, dadas duas matrizes A e B associadas a duas bases de um reticulado, existe uma matriz U unimodular(matriz de coordenadas inteiras e determinante ± 1), tal que $B = A \cdot U$, [15].

A título de exemplo, vamos considerar a matriz

$$A = \begin{pmatrix} 1 & -3 \\ 2 & 1 \end{pmatrix}$$

geradora do reticulado $\bar{\Lambda}$ apresentado no exemplo 1.3.

Para qualquer matriz unimodular U, a matriz $B = A \cdot U$ é também uma base para $\bar{\Lambda}$. Por exemplo, se considerarmos $U = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ (U tem coordenadas inteiras e

determinante igual a 1), temos $B = A \cdot U = \begin{pmatrix} -5 & -8 \\ 4 & 5 \end{pmatrix}$ que gera o mesmo reticulado gerado por A.

Para garantirmos que matriz $B = \begin{pmatrix} -5 & -8 \\ 4 & 5 \end{pmatrix}$ gera o mesmo reticulado $\bar{\Lambda}$ é suficiente mostrarmos que os vetores da base $\left\{(1,2)^T, (-3,1)^T\right\}$ podem ser escritos na forma $B\alpha, \alpha \in \mathbb{Z}^2$. De fato, se considerarmos o sistema linear

$$\begin{pmatrix} -5 & -8 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

teremos como solução os valores $x = 3$ e $y = -2$.

Além disso,

$$\begin{pmatrix} -5 & -8 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -3 \\ 1 \end{pmatrix}$$

de onde teremos $x = -1$ e $y = 1$.

A matriz $U' = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$ é exatamante inversa da matriz $U = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$, assim

$$\begin{pmatrix} -5 & -8 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 2 & 1 \end{pmatrix}$$

A matriz unimodular U é denominada matriz de mudança de base do reticulado.

É interessante observarmos que, embora as duas malhas sejam diferentes, os pontos do conjunto intersecção são exatamente os mesmos, ou seja, $\{ b_1, b_2\}$ e $\{ b'_1, b'_2\}$ são duas bases diferentes para o mesmo reticulado $\bar{\Lambda}(b_1, b_2) = \bar{\Lambda}(b'_1, b'_2)$.

Definição 1.2 *Se B é uma matriz geradora do reticulado Λ, a matriz definida por $G = B^T \cdot B$, onde T denota a transposta de B, é chamada* ***matriz de Gram*** *associada ao reticulado Λ.*

Definição 1.3 *O determinante de um reticulado Λ, denotado por $det(\Lambda)$, é definido como sendo o determinante da matriz $\boldsymbol{G}$, ou seja,*

$$det(\Lambda) = det(G).$$

Observação 1.1 *Para um reticulado dimensionalmente completo, ou seja, com $dim(\Lambda) = n$ e sendo B uma matriz quadrada. Então,*

$$det(\Lambda) = det\left(B^T \cdot B\right) = det\left(B^T\right) \cdot det(B) = (det(B))^2.$$

É claro que um reticulado possui várias bases diferentes e consequentemente várias matrizes de Gram diferentes, assim, a notação G_A ou G_B sera utilizada quando for necessária uma referência específica. No entanto, o determinante de cada uma delas é o mesmo e só depende do reticulado.

Para verificar isso, considere A e B duas matrizes geradoras de Λ de forma que $B = A \cdot U$, com U sendo a matriz unimodular.

Assim,

$det(G_B) = det\left(B^T \cdot B\right) = det\left(U^T \cdot A^T \cdot A \cdot U\right) = det\left(U^T\right) \cdot det\left(A^T \cdot A\right) \cdot det(U) = 1 \cdot det\left(A^T \cdot A\right) \cdot 1 = det\left(A^T \cdot A\right) = det(G_A)$.

■

Exemplo 1.4 *Considere o reticulado Λ gerado por $A = \{u_1, u_2\}$, com $u_1 = (1,1)^T$ e $u_2 = (2,0)^T$, e por $B = \{v_1, v_2\}$ com $v_1 = (1,-3)^T$ e $v_2 = (0,-2)^T$.Sejam G_A e G_B as respectivas matrizes de Gram , então, podemos dizer que*

$$G_A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}^T \cdot \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 4 \end{pmatrix}$$

$$G_B = \begin{pmatrix} 1 & 0 \\ -3 & -2 \end{pmatrix}^T \cdot \begin{pmatrix} 1 & 0 \\ -3 & -2 \end{pmatrix} = \begin{pmatrix} 10 & 6 \\ 6 & 4 \end{pmatrix}$$

onde,

$$det(\Lambda) = det(G_A) = det(G_B) = 4.$$

1.1.1 Empacotamento Reticulado no Plano

Um empacotamento esférico ou simplesmente empacotamento, é um conjunto enumerável de bolas abertas, de mesmo raio, mutuamente disjuntas.

Definição 1.4 *Denomina-se empacotamento reticulado quando o centro das bolas são os pontos de um reticulado. A todo reticulado Λ tem-se um empacotamento esférico associado, que é dado por bolas cujo raio é igual a metade da distância mínima os entre pontos de Λ.*

Um exemplo de empacotamento reticulado é apresentado na figura 1.3

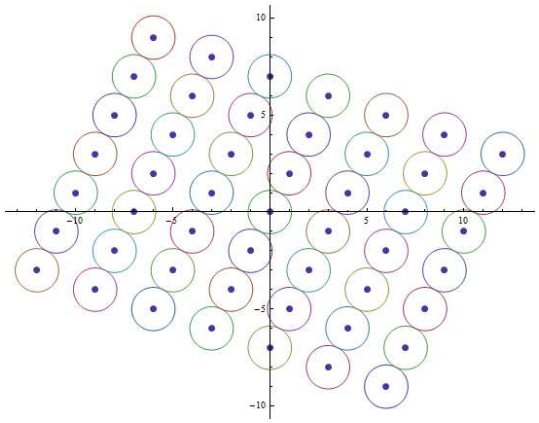


Figura 1.3: Empacotamento associado ao reticulado $\bar{\Lambda}$ apresentado no exemplo 1.3

Definição 1.5 *Seja $x = (x_1, ..., x_n) \in \Lambda$, onde Λ é um reticulado. A norma de x é dada por:*

$$||x|| = x \cdot x = \sum x^2$$

Chamamos de norma minimal ou distância mínima d_Λ de um reticulado Λ à menor distância euclidiana entre dois pontos distintos quaisquer de Λ.

$$d_\Lambda \triangleq min\,\{||x - y|| : x, y \in \Lambda; x \neq y\}$$

Uma importante característica de um empacotamento reticulado é o *raio de empacotamento*, isto é, o maior raio possível tal que as bolas centradas nos pontos do reticulado sejam mutuamente disjuntas.

Proposição 1.1 *O raio de um empacotamento reticulado, é dado por* $\rho = \frac{d_\Lambda}{2}$.

Demonstração: Basta provarmos que se tomarmos $r = \frac{d_\Lambda}{2}$ entao r satisfaz que $B_\rho(u) \cap B_\rho(v) = \emptyset$, onde $B_\rho(u)$ representa a bola aberta de raio ρ centrada em u e depois provarmos que $r = \frac{d_\Lambda}{2}$ é o maior possível.

Considere $r = \frac{d_\Lambda}{2}$. Se tomarmos qualquer $x \in \mathbb{R}^n$ tal que $x \in B_r(u)$, sabemos que $d(u,x) + d(x,v) \geq d(u,v) \geq d_\Lambda$ e que $d(u,x) < r = \frac{d_\Lambda}{2}$. Vamos supor que $x \in B_r(v)$, logo $d(x,v) < r = \frac{d_\Lambda}{2}$. Assim, temos $d(u,x) + d(x,v) < \frac{d_\Lambda}{2} + \frac{d_\Lambda}{2} = d_\Lambda$, o que é uma contradição. Portanto, tomando $r = \frac{d_\Lambda}{2}$ temos que $B_\rho(u) \cap B_\rho(v) = \emptyset$.

Agora provaremos que $r = \frac{d_\Lambda}{2}$ é o maior raio possível. Caso $r = \frac{d_\Lambda}{2}$, sejam $u, v \in \Lambda$ tais que $d(u,v) = d_\Lambda$. Para $\frac{u+v}{2} \in \mathbb{R}^n$ temos que $d(h,u) = d(h,v) = \frac{d_\Lambda}{2} < r$.

Portanto, existiria $h \in \mathbb{R}^n$ tal que $h \in B_r(u) \cap B_r(v)$, logo $r = \frac{d_\Lambda}{2} = \rho$ é o maior raio possível.

■

1.1.2 Regiões Fundamentais e Densidade

Definição 1.6 *Seja* Λ *um reticulado em* $\mathbb{R}^m$. *Uma região fundamental* F *de* Λ *é um subconjunto fechado de* $\mathbb{R}^m$ *que ladrilha* $\mathbb{R}^m$, *isto é, tomando as translações* $F + v$, *com* $v \in \Lambda$, *conseguimos cobrir todo o* $\mathbb{R}^m$ *de modo que dois ladrilhos ou não têm intersecção ou se intersectam apenas nos bordos.*

Outra importante característica de um empacotamento é a proporção do espaço $\mathbb{R}^m$ que é ocupada pelas bolas do empacotamento, que é denominada densidade do empacotamento. Afim de estudarmos a densidade de um empacotamento reticulado, vamos definir inicialmente a região de Voronoi de um reticulado.

Definição 1.7 *Sejam* $\Lambda \subset \mathbb{R}^m$ *um reticulado,* B *uma base para* Λ *e* $\mathbb{R}^n$ *o espaço vetorial gerado por esta base e* $v \in \Lambda$. *Definimos a região de Voronoi de* v, *denotada*

por $(vor\,(v))$*, como sendo a região que contém todos os pontos de* $\mathbb{R}^n$ *que estão mais próximos de* v *do que qualquer outro ponto* u *do reticulado, ou seja,*

$$vor\,(v)_\Lambda = \{x \in \mathbb{R}^n : ||v - x|| \leq ||u - x||, \forall u \in \Lambda\}$$

Um exemplo para a região de Voronoi do reticulado $\mathbb{Z}^2$ é apresentado na figura 1.4 e um exemplo da região de Voronoi para o reticulado $\bar{\Lambda}$ na figura 1.5.

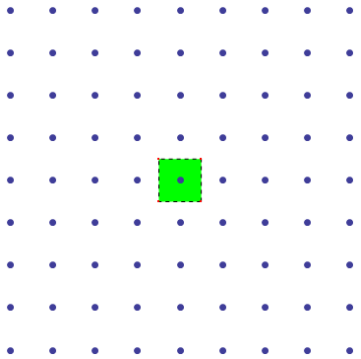


Figura 1.4: Regiões de Voronoi do ponto $v \in \mathbb{Z}^2$.

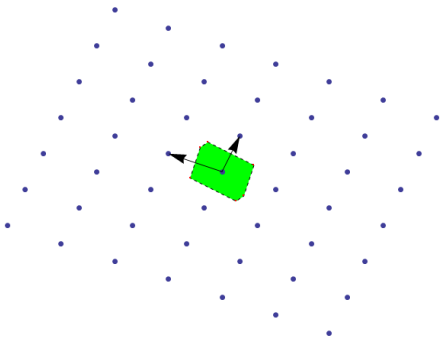


Figura 1.5: Região de Voronoi de um ponto do reticulado $\bar{\Lambda}$.

Tendo construído uma destas regiões, todas as outras são obtidas por translações. Se começarmos de $vor\,(0)$, por exemplo, teremos para todo $v \in \Lambda$,

$$vor\,(v)_\Lambda = v + vor\,(0) = \{x + v \in \mathbb{R}^n; x \in vor\,(0)\}$$

O importante é que estas regiões constituem um ladrilhamento perfeito no plano. As regiões $vor\,(v)_{\Lambda}$ cobrem o plano inteiro e se sobrepõem apenas ao longo de pontos da fronteira (vértices ou arestas).

As figuras 1.6 e 1.7 a seguir ilustram o ladrilhamento por regiões de Voronoi de reticulados no plano. Em uma breve análise nas figuras observa-se dois tipos ou formas de regiões de Voronoi associada com reticulados bi - dimensionais. Uma delas é hexagonal e a outra retangular [7]. Geralmente, um reticulado no plano possui região de Voronoi hexagonal. No plano, a forma hexagonal é chamada de primitiva porque corresponde ao caso geral. Pode ser caracterizada também pela propriedade relacionada a colocação de azulejos correspondentes, o número mínimo possível de polígonos em cada vértice, são três neste caso.

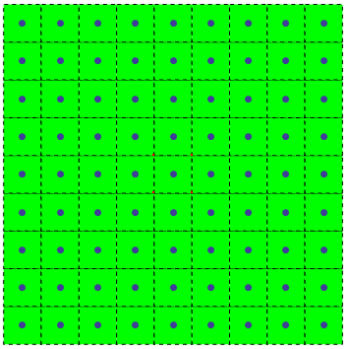


Figura 1.6: Ladrilhamento do plano por regiões de Voronoi do reticulado $\mathbb{Z}^2$.

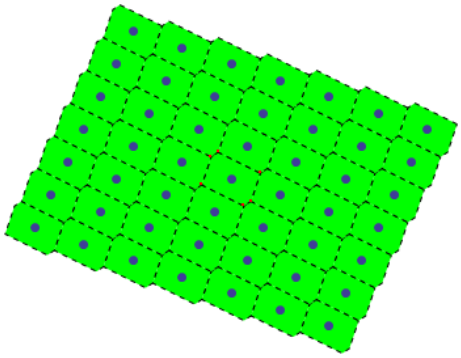


Figura 1.7: Ladrilhamento do plano por regiões de Voronoi gerado pela base do reticulado $\bar{\Lambda}$.

Na dimensão 3, existem cinco tipos de regiões de Voronoi conhecidas como cinco *parallelohedros de Fedorov*[7], de onde temos que apenas uma região é primitiva. As regiões estão mostradas na figura 1.8.

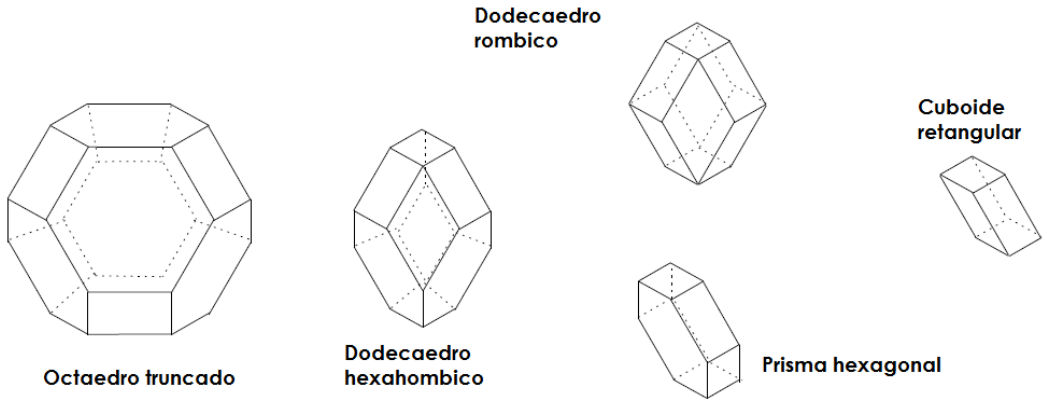


Figura 1.8: Os cinco parallelohedros de Fedorov, são eles próprios as cinco regiões de voronoi de reticulados de dimensão 3. Somente o octaedro truncado é primitivo.

Na dimensão 4 o problema foi resolvido por Delone (ligeiramente editado por Stogrin) com uma lista de 52 tipos de reticulados. O número de formas primitivas ainda não é um, mas três. Para um estudo detalhado da região de Voronoi consultar [3, 13].

Como as regiões de Voronoi ladrilham o espaço em que se encontram, podemos destacar uma bola do empacotamento reticulado conforme mostra a figura 1.9 e então calcular uma propriedade muito importante de um reticulado chamada densidade de empacotamento.

Definição 1.8 *A densidade do empacotamento de um reticulado $\Lambda \in \mathbb{R}^2$, é a razão entre a área do disco de empacotamento (A_D) e a e a área da região de Voronoi $(A_{vor(0)})$. Assim,*

$$\Delta = \frac{A_D}{A_{vor(0)}},$$

onde D é o disco de raio $\rho = \frac{d_\Lambda}{2}$ e $vor\,(0)$ é a região de Voronoi de 0.

A densidade do reticulado $\Lambda \in \mathbb{R}^2$ fornece então uma medida de quanto do plano foi preenchido pela união discos de raio ρ.

Exemplo 1.5 *Observe a região de Voronoi do nosso reticulado* $\bar{\Lambda}$*. Vamos calcular sua densidade.*

Analisando de forma detalhada a região de Voronoi da origem, temos a seguinte situação:

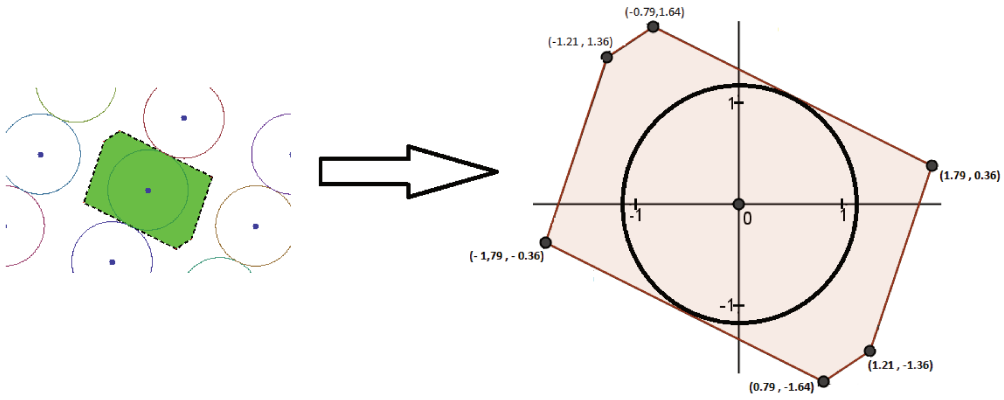


Figura 1.9: Detalhamento da região de Voronoi do ponto $(0,0) \subset \bar{\Lambda}$

Inicialmente, devemos encontrar o raio de empacotamento $\rho_{\bar{\Lambda}}$ *do disco* D *inserido na região de Voronoi, ou seja, devemos encontrar a norma* $||u||$, $u \in \bar{\Lambda}$.

Como $u = x\,(1,2) + y\,(-3,1)$, *então* $||u||^2 = 5x^2 - 2xy + 10y^2$. *Daí, temos alguns casos para analisar:*

- *Se* $x \cdot y = 0$ *isto implica* $x = 0$ *ou* $y = 0$, *logo o menor valor que* $||u||^2$ *assume é 5, e isto ocorre nos vetores* $\pm\,(1,2)$*;*
- *Se* $x \cdot y < 0$, *então* $5x^2 - 2xy + 10y^2 \geq 5x^2 - 2xy + 5y^2 \geq 4x^2 + 4y^2 + (x-y)^2 \geq 8$, *pois* $x, y \in \mathbb{Z}$ *e* $x \cdot y \neq 0$*;*
- *e é lógico que se* $x \cdot y > 0$, *então* $||u||^2 > 5$.

Portanto, os vetores de menor norma são os dois vetores $(1,2)$ *e* $(-1,-2)$*; logo, o raio de empacotamento é igual a* $\rho_{\bar{\Lambda}} = \frac{\sqrt{5}}{2}$.

Para calcular a densidade de empacotamento, temos que determinar a área de uma região de Voronoi deste reticulado que, neste caso, é um polígono de seis lados. Observe que a segunda figura já nos fornece as coordenadas de cada vértice do polígono, logo,

como a área da região delimitada por um polígono convexo de vértices percorridos no sentido anti-horário é dada por [5]:

$$A = \frac{1}{2}\left(\begin{vmatrix} x_0 & y_0 \\ x_1 & y_1 \end{vmatrix} + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} + ... + \begin{vmatrix} x_{n-1} & y_{n-1} \\ x_n & y_n \end{vmatrix} + \begin{vmatrix} x_n & y_n \\ x_0 & y_0 \end{vmatrix} \right)$$

então,

$$A_{vor(0)} = \frac{1}{2}\left(\begin{vmatrix} -0,79 & 1,64 \\ -1,21 & 1,36 \end{vmatrix} + \begin{vmatrix} -1,21 & 1,36 \\ -1,79 & -0,36 \end{vmatrix} \right) +$$

$$+\frac{1}{2}\left(\begin{vmatrix} -1,79 & -0,36 \\ 0,79 & -1,64 \end{vmatrix} + \begin{vmatrix} 0,79 & -1,64 \\ 1,21 & -1,36 \end{vmatrix} \right) +$$

$$+\frac{1}{2}\left(\begin{vmatrix} 1,21 & -1,36 \\ 1,79 & 0,36 \end{vmatrix} + \begin{vmatrix} 1,79 & 0,36 \\ -0,79 & 1,64 \end{vmatrix} \right)$$

logo,

$$A_{vor(0)} = 7 unidades\ de\ área.$$

Em posse do raio de empacotamento e da área da região de Voronoi já podemos calcular a densidade de empacotamento, uma vez que a área do disco inserido na região de Voronoi já esta definida como $A_D = \pi\rho_\Lambda^2$. *Assim,*

$$\Delta = \frac{A_D}{A_{vor(0)}} = \frac{\pi\left(\frac{\sqrt{5}}{2}\right)^2}{7} = \frac{5\pi}{28} \cong 0,561.$$

É importante sabermos que não apenas a região de Voronoi ladrilha o plano pelas translações por vetores de Λ, mas que também podemos tomar como ladrilhos, relativos a estas mesmas translações, o paralelogramo $\mathcal{P}$ apoiado na base do reticulado,isto é,

$$\mathcal{P} = \{av_1 + bv_2 | 0 \leq a < 1, 0 \leq b < 1\}.$$

A nível de comparação, vamos continuar com a base dada no exemplo 1.5

Observe na figura 1.10 o paralelogramo $\mathcal{P}$ gerado pela base do reticulado $\bar{\Lambda}$.

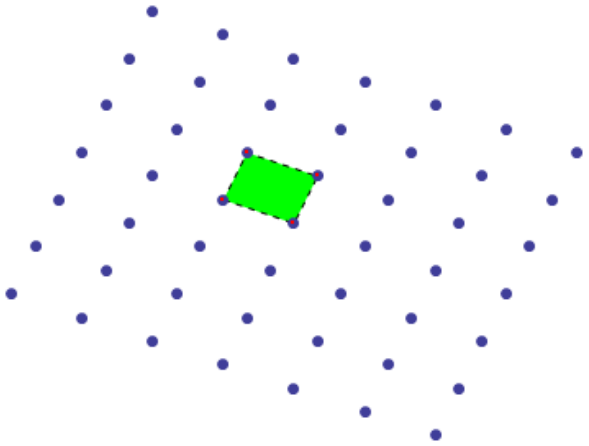


Figura 1.10: Paralelogramo gerado pela base do reticulado $\bar{\Lambda}$.

Para calcularmos a área de um paralelogramo com suporte em $b_1 = (b_{11}, b_{21})$ e $b_2 = (b_{12}, b_{22})$ é muito simples, basta calcularmos o valor absoluto do determinante da matriz formada pelas coordenadas da base, ou seja:

$$A = \frac{1}{2}\left|\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right|$$

Se calcularmos a área do paralelogramo definido pela base dada, teremos:

$$A = \frac{1}{2}\left|\begin{pmatrix} 1 & -3 \\ 2 & 1 \end{pmatrix}\right| = 7 \textit{unidades de área.}$$

Observe que a área do paralelogramo é a mesma da região de Voronoi do exemplo 1.5, logo podemos, também, calcular a densidade de $\bar{\Lambda}$, ou seja,

$$\Delta = \frac{A_D}{A_{\mathcal{P}}} = \frac{\pi\left(\frac{\sqrt{5}}{2}\right)^2}{7} = \frac{5\pi}{28} \cong 0,561.$$

Observação 1.2 *A área da região de Voronoi da origem de um reticulado Λ gerado por qualquer base $\beta \in \Lambda$ é igual à área do paralelogramo apoiado em β, $A_{vor(0)} = A_{\mathcal{P}}$.*

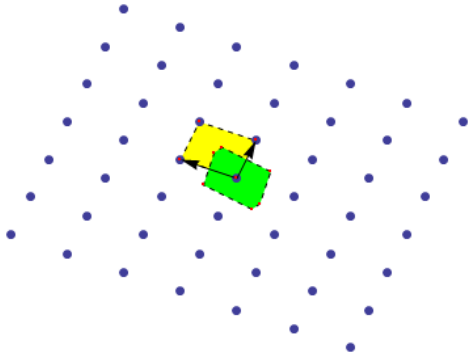


Figura 1.11: A região de Voronoi e o Paralelogramo de mesma área

As idéias de região de Voronoi e paralelogramo fundamental podem ser extendidas de maneira análoga para um reticulado $\Lambda \in \mathbb{R}^m$.

No caso do $\mathbb{R}^m$ uma região fundamental bastante útil para nós é o paralelotopo fundamental gerado por uma base de Λ.

Definição 1.9 *Dada uma base $\beta = \{b_1, ..., b_n\}$, o paralelotopo fundamental (ou região fundamental) gerado por esta base é o sólido*

$$\mathcal{P} = [0,1)^n \cdot B \triangleq \{\theta_1 b_1 + ... + \theta_m b_m, 0 \leq \theta_i < 1\}$$

Exemplo 1.6 *Para o reticulado $\bar{\Lambda}$ a região fundamental pode ser vista na figura 1.10.*

Exemplo 1.7 *$\Lambda = \mathbb{Z}^3$ é um reticulado gerado pelos vetores $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ e $e_3 = (0,0,1)$, com região fundamental descrita pela figura 1.12.*

Definição 1.10 *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado, $\beta = \{v_1, ..., v_n\}$ uma base de Λ e $\mathcal{P}$ a região fundamental. Se $v_i = (v_{i1}, v_{i2}, ..., v_{in})$, para $i = 1, 2, ..., n$ definimos o volume da região fundamental, $\mathcal{P}$ como o módulo do determinante da matriz*

$$B = \begin{pmatrix} v_{11} & v_{21} & ... & v_{n1} \\ v_{12} & v_{22} & ... & v_{n2} \\ . & . & ... & . \\ . & . & ... & . \\ v_{1n} & v_{2n} & ... & v_{nn} \end{pmatrix}.$$

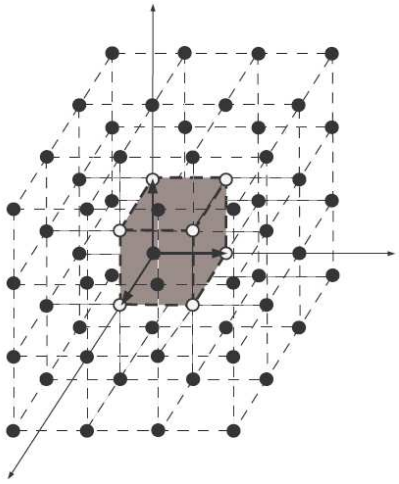


Figura 1.12: Região Fundamental de $\Lambda = \mathbb{Z}^3$

Exemplo 1.8 *Seja* $\Lambda \subseteq \mathbb{R}^3$ *um reticulado,* $\beta = \{(1,1,2),(0,3,1),(1,3,2)\}$ *uma base de* Λ *e* $\mathcal{P}$ *a região fundamental. Assim*

$$vol\,(\mathcal{P}) = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 3 & 3 \\ 2 & 1 & 2 \end{vmatrix} = |-4| = 4.$$

Proposição 1.2 *O volume da região fundamental* $vol\,(\mathcal{P})$ *é independente da base* β *de* Λ *.[21]*

Demonstração: *Se além da base* β *pegarmos uma outra base* α *do reticulado* Λ*, definida por* $\alpha = \{t_1, ..., t_n\}$*, então* $t_i = \sum_{j=1}^{n} \alpha_{ij} v_j$*, com* $\alpha_{ij} \in \mathbb{Z}$*. Assim,* $vol\,(\mathcal{P}_\alpha) = |det(\alpha_{ij})| \cdot vol\,(\mathcal{P}_\beta)$*. Como a matriz mudança de base* (α_{ij}) *é inversível, segue que* $det(\alpha_{ij}) = \pm 1$*. Portanto* $vol\,(\mathcal{P}_\alpha) = vol\,(\mathcal{P}_\beta)$*.*

■

O volume de um reticulado Λ, denotado por $vol\,(\Lambda)$, é o volume m-dimensional do paralelotopo fundamental gerado por qualquer de suas bases. Por definição, é a raiz quadrada do determinante da *matriz de Gram*, por qualquer de suas bases. Assim sendo, quando o reticulado dimensional é completo, segue-se que

$$vol\,(\Lambda) = \sqrt{det\,(G)} = \sqrt{det\,(\Lambda)}$$

para qualquer uma das matrizes da sua base.

No entanto quando mudamos a base de um reticulado o formato do paralelotopo fundamental se altera.

1.1.3 Reticulados Equivalentes e Ortogonais

Definição 1.11 *Seja $\Lambda \subset \mathbb{R}^m$ um reticulado. Um subreticulado é um subconjunto $\Gamma \subset \Lambda$, que é um reticulado.*

Num reticulado Λ de dimensão m em $\mathbb{R}^m$, temos naturalmente uma estrutura de anel induzida por $\mathbb{Z}^n$ e portanto, um grupo aditivo abeliano a ele associado. Assim, um subreticulado Γ é então um subgrupo de Λ e podemos considerar o grupo quociente Λ/Γ.

O índice do subreticulado Γ é a cardinalidade do grupo quociente Λ/Γ e

$$\Lambda/\Gamma = \frac{vol(\Gamma)}{vol(\Lambda)} = \frac{\sqrt{det(\Gamma)}}{\sqrt{det(\Lambda)}} = |det(B)|.$$

É sempre possível encontrar um subreticulado de um dado reticulado considerando sua versão escalonada por um fator inteiro.

Dado um reticulado Λ, um reticulado escalonado Γ pode ser obtido multiplicando os vetores do reticulado por uma constante, isto é, $\Gamma = c \cdot \Lambda$ onde $c \in \mathbb{R}^n$. Assim, Γ é um subreticulado de Λ quando $c \in \mathbb{Z}^n$.

Mais geralmente, temos a seguinte definição.

Definição 1.12 *Se um reticulado pode ser obtido de outro por rotações, reflexões ou multiplicação por um escalar, dizemos que eles são* ***equivalentes****.*

Mais precisamente, duas matrizes geradoras M e M' definem reticulados equivalentes se, e somente se, eles são descritos por $M' = cUMB$, onde:

- c é uma constante diferente de zero;
- U é a matriz unimodular;
- B é uma matriz real ortogonal.

Observação 1.3 *As correspondentes matrizes de Gram são relacionadas por* $G' = c^2UGU^T$.

Exemplo 1.9 *Consideramos em dimensão 2 os dois seguintes reticulados:*

- ***H****, o reticulado hexagonal gerado pelos vetores* $(1,0)$ *e* $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$*, e*
- $\mathbb{A}_2 = \{(x_0, x_1, x_2) \in \mathbb{Z}^3 : x_0 + x_1 + x_2 = 0\}$.

Vale notar que apesar de utilizar três coordenadas para descrevê-lo, $\mathbb{A}_2$ *está contida no espaço euclidiano 2-dimensional* $\{(x_0, x_1, x_2) \in \mathbb{R}^3 : x_0 + x_1 + x_2 = 0\}$.

Uma base para $\mathbb{A}_2$ *é* $\{(1,-1,0);(0,1,-1)\}$. *Logo teremos como matrizes geradoras de* H *e* $\mathbb{A}_2$ *respectivamente*

$$M_H = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \quad e \quad M_{\mathbb{A}_2}^T = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}^T .$$

Logo, suas matrizes de Gram são respectivamente

$$G_H = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \quad e \quad G_{\mathbb{A}_2} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

Assim, calculamos facilmente que $det(H) = \frac{3}{4}$ *e* $det(\mathbb{A}_2) = 3$.

Não é dificil de se ver que estes dois reticulados são equivalentes. Por exemplo, podemos multiplicar H *por* $\sqrt{2}$*, ou seja:*

$$\sqrt{2}M_H = \begin{pmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{pmatrix}.$$

obtendo a seguinte matriz de Gram

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

que é a mesma obtida se tomarmos em $\mathbb{A}_2$ *a base* $\{(1,-1,0);(0,-1,1)\}$.

Como se pode ver, uma vantagem de usar $\mathbb{A}_2$ em lugar de H é que você tem coordenadas inteiras, em vez de se trabalhar com $\frac{\sqrt{3}}{2}$. Além disso, em $\mathbb{A}_2$ se observa de forma imediata a simetria entre as três coordenadas.

Graficamente, podemos visualizar o exemplo acima através da figura 1.13.

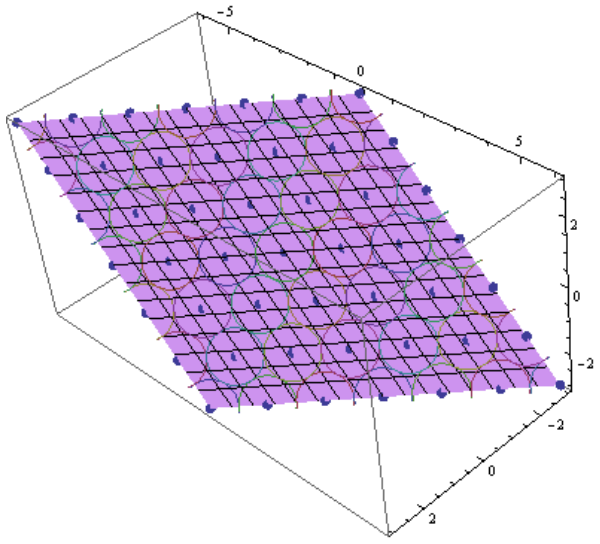


Figura 1.13: Equivalencia entre os reticulados H e $\mathbb{A}_2$

Um outro tipo de reticulado que usaremos é o ortogonal, vamos defini-lo.

Definição 1.13 *Um subreticulado $\Gamma \subset \Lambda$ é dito ortogonal (ou retangular) se, e somente se, existe uma base de vetores ortogonais β' para Γ.*

Para qualquer base ordenada $\beta = \{u_1, ..., u_m\}$ de um reticulado Λ, é possível associar um conjunto $GS_\beta = \{b_1, ..., b_m\}$ de vetores ortogonais, aplicando recursivamente o processo de **ortogonalização de Gram-Schmidt**

$$b_1 = u_1$$

$$b_i = b_i - \sum_{j=1}^{i-1} \frac{\langle u_i, b_j \rangle}{\langle b_j, b_j \rangle} u_j, i = 2, ..., m$$

Os vetores b_i podem não pertencer ao reticulado Λ_β. No entanto, se $\langle u_i, u_j \rangle$ for um número racional para todo i e j, é possível encontrar um múltiplo de b_i que pertence a Λ_β, o que permite escrever:

Proposição 1.3 *Se uma matriz de Gram de um reticulado Λ possui somente elementos racionais (se Λ e racional), então Λ possui um subreticulado ortogonal Γ*

Exemplo 1.10 *Considere a matriz de Gram do nosso reticulado $\bar{\Lambda}$, gerado pelos vetores $b_1 = (1,2)^T$ e $b_2 = (-3,1)^T$ no plano,*

$$G_{\bar{\Lambda}} = \begin{pmatrix} 10 & -1 \\ -1 & 5 \end{pmatrix}$$

Como os elementos de $G_{\bar{\Lambda}}$ são todos racionais, $\bar{\Lambda}$ possui um subreticulado ortogonal.

1.1.4 Reticulado Dual

Agora vamos definir o conceito de dual de um reticulado e analisar algumas das suas propriedades [19].

Definição 1.14 *Para um reticulado de posto completo definimos o seu reticulado dual (às vezes conhecido como reticulado recíproco),*

$$\Lambda^* = \{y \in \mathbb{R}^n | \forall x \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\}$$

em geral, definimos

$$\Lambda^* = \{y \in posto(\Lambda) | \forall x \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\}$$

Ou seja, o dual de Λ é o conjunto de todos os pontos (no espaço de Λ), cujo produto interno com qualquer um dos pontos é um inteiro. Como mostraremos mais tarde, Λ^* é realmente um reticulado, como o nome sugere.

Exemplo 1.11 *O reticulado de pontos inteiros satisfaz $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ (e, portanto, pode ser chamado de auto-dual). Da mesma forma, $(2\mathbb{Z}^n)^* = \frac{1}{2}\mathbb{Z}^n$, e isso dá uma justificativa para o nome do reticulado recíproco.*

A partir da definição acima, temos a seguinte interpretação geométrica de um reticulado dual. Para qualquer vetor x, o conjunto de todos os pontos do produto interno

com formas inteiras é um conjunto de hiperplanos perpendiculares à x e separados por uma distância $\frac{1}{||x||}$. Assim, qualquer vetor x em um reticulado Λ impõe a restrição de que todos os pontos do Λ^* estão em um dos hiperplanos definidos por x. Veja a figura 1.14 para uma ilustração.

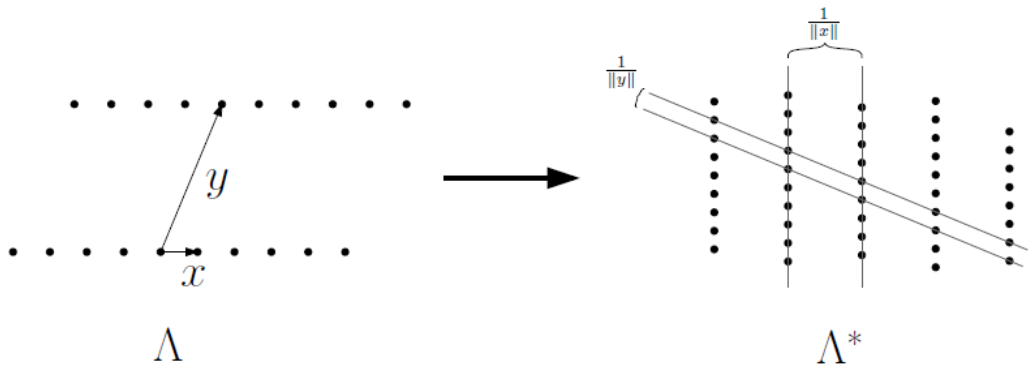


Figura 1.14: O reticulado Λ e seu dual Λ^*

Definição 1.15 *Para uma base $B = (b_1, b_2, ..., b_n) \in \mathbb{R}^{m \times n}$, definimos a base dual $B^* = (b_1^*, b_2^*, ..., b_n^*) \in \mathbb{R}^{m \times n}$ como a única base que satisfaça as seguintes condições:*

- $posto\,(B^*) = posto\,(B)$
- $B^T \cdot B^* = Id$

A segunda condição pode ser interpretada como dizendo que $\langle b_i, b_j \rangle = \delta_{ij}$, onde $\delta_{ij} = 1$ se $i = j$ e 0 em contrário. Não é difícil verificar que B^* é realmente única. De fato, para o caso de um reticulado dimensionalmente completo, B^* é dada por $(B^T)^{-1}$, em geral, temos $B^* = B \cdot (B^T B)^{-1}$ (E podemos usar isso como nossa definição de base dual).

Exemplo 1.12 *Utilizando a segunda condição no reticulado $\bar{\Lambda}$ de base $\{b_1, b_2\}$ onde $b_1 = (1, 2)^T$ e $b_2 = (-3, 1)^T$, obtemos como base dual $\{b_1^*, b_2^*\}$ de onde temos $b_1^* = \left(\frac{1}{7}, \frac{3}{7}\right)^T$ e $b_2^* = \left(\frac{-2}{7}, \frac{1}{7}\right)^T$.*

Proposição 1.4 *Para todo reticulado Λ dimensionalmente completo, $det(\Lambda^*) = \frac{1}{det(\Lambda)}$.*

Demonstração: *Para todo reticulado dimensionalmente completo,*

$$det(\Lambda^*) = \mid det((B^T)^{-1}) \mid = \left|\frac{1}{det(B^T)}\right| = \left|\frac{1}{det(B)}\right| = \frac{1}{det(\Lambda)}.$$

de forma geral temos,

$$det(\Lambda^*) = \sqrt{det((B^*)^T B^*)} = \sqrt{det(((B^T B)^{-1})^T B^T \cdot B.(B^T B)^{-1})} =$$
$$= \sqrt{det(B^T B)^{-1}} = \frac{1}{\sqrt{det(B^T B)}} = \frac{1}{det(\Lambda)}$$

■

Observação 1.4 *Podemos também estabelecer uma relação entre as matrizes de Gram de reticulados n-dimensionais duais. Sejam G e G^* as matrizes de Gram respectivamente de Λ e Λ^*, temos:*

$det(G.G^*) = det(G).det(G^*) =$

$= det(B^T B).det((B^*)^T B^*)$

$= det(B^T).det(B).det((B^*)^T).det(B^*) = 1$

e

$det(G) = det(G^*)^{-1}$

Observação 1.5 *Em particular, quando $\Lambda = \Lambda^*$, dizemos que Λ e um reticulado auto-dual*

1.2 Empacotamento Reticulado no $\mathbb{R}^m$ $(m \geq 3)$

O problema de empacotamento de esferas em espaços euclidianos de dimensões maiores ou igual a 3, segue a o mesmo raciocínio do caso planar onde, dado um número grande de esferas iguais, deseja - se saber qual é o modo mais eficiente (quer dizer, mais denso) de empacotá-las.

Como se pode notar, este problema possui aplicações importantes. Em dimensão igual a 3, o problema tem uma história extremamente rica. Em 1500 Sir Walter Raleigh

levantou a seguinte questão: "*de que forma seria mais eficiente colocar uma pilha de canhões no convés de um navio ?*". O Matemático inglês Thomas Harriot, a quem ele havia explicado a situação, escreveu por sua vez ao astrônomo Johannes Kepler sobre o problema. Kepler conjecturou que a embalagem mais densa era para ser encontrada na maneira usual e que os marinheiros tinham então de fazer um empilhamento de balas de canhão de forma igual as das mercearias para empilhar laranjas (Figura 1.15). Isso ficou conhecido como a *conjectura Kepler*, e manteve-se um importante problema pendente há muitos anos, apesar da grande quantidade de pesquisa matemática que ele inspirou.

Notavelmente, sendo esta a resposta correta foi necessário de cerca de 400 anos de matemática para prová-la. Ao longo do caminho, foram muitas as "evidências"que falharam. Recentemente (1998) Thoma Hales, utilizando as idéias de demostração fundamentadas na resolução de uma série de problemas de otimização usando computadores (método de exaustão), anunciou que teve uma prova da conjectura de Kepler. Os Referees disseram que a prova de Hales está "99% certa". Assim a conjectura de Kepler está agora muito perto de transforma-se em um teorema. Em 2003, T. Hales publicou um artigo detalhado descrevendo a parte não computacional desta prova. Ele trabalha em uma prova formal para remover qualquer resto de incerteza, e estima que tal prova levará cerca de 20 anos de trabalho.

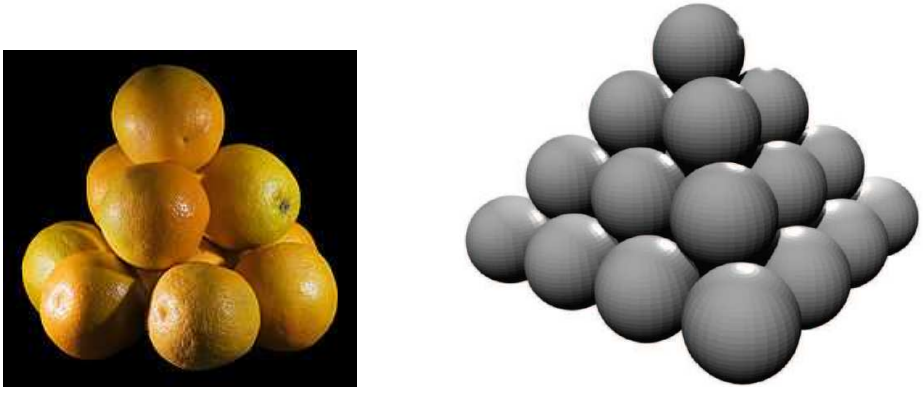


Figura 1.15: Empilhamento de laranjas e de bolas de canhão.

O melhor empacotamento também pode obter colocando esferas de mesmo raio centrado em pontos de um reticulado chamado de face-centrada cúbica (lattice fcc). Veja a Figura 1.16.

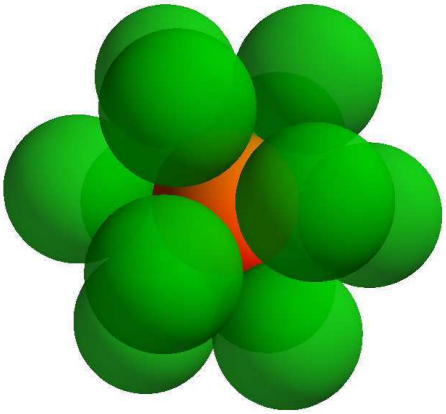


Figura 1.16: Bolas dispostas com seus centros no fcc lattice.

O nome reticulado "fcc"se deve a que se obtêm a partir do reticulado cúbico, juntando os pontos nos centros das faces. Este reticulado pertence a uma família muito importante de reticulados, a família $\mathbb{A}_n, (n \in \mathbb{N})$, de onde $dim\mathbb{A}_n = n$, que por sua vez formam parte dos chamados *reticulados raízes* que veremos melhor mais adiante.

1.2.1 Número de Toques ou Entrechoques ("Kissing Number")

Este problema consiste em determinar, para cada dimensão n, quantas esferas se podem colocar ao redor de uma fixa (todas com o mesmo raio) de modo que todas toquem ou "beijem"a esfera fixa.

Em uma dimensão, o kissing number é 2 , conforme mostra a figura 1.17:

Figura 1.17: Kissing number em dimensão 1

Em dimensão 2 a solução é simples, sendo o kissing number igual a 6, conforme mostra a figura 1.18.

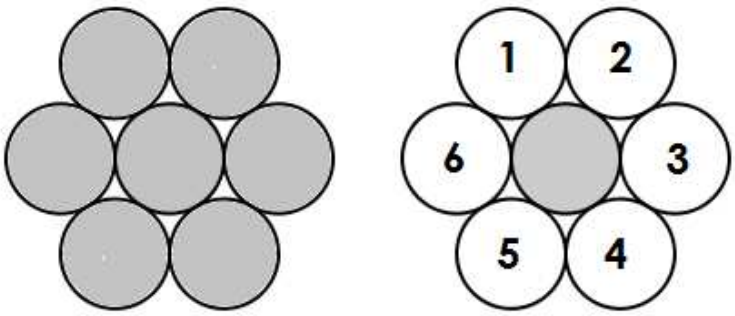


Figura 1.18: Kissing number em dimensão 2

Em dimensão 3 o problema , conhecido como o problema das 13 esferas, possui uma história muito interessante, incluindo uma famosa controvérsia em 1694 entre David Gregory e Sir Isaac Newton. Não é muito difícil reduzir a possibilidade que pode haver no máximo 13 esferas ao redor de uma fixa. Por outra parte, se forem colocadas 13 esferas de mesmo raio, uma no centro, e as outras 12 no que seriam os vértices de um icosaedro, se observam que estas 12 tocam a esfera central, e ainda não se tocam, deixando espaço suficiente até para mudar qualquer uma delas de um lugar para outro, como "em órbita"ao redor da central conforme mostra a figura 1.19.

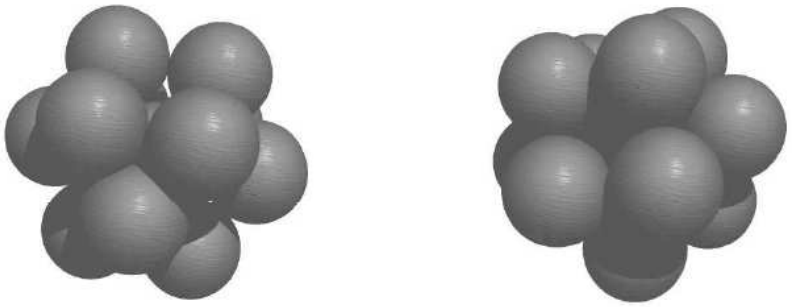


Figura 1.19: Duas formas diferentes mostram que o kissing numbers na dimensão 3 é $n \geq 12$. O segundo, corresponde ao icosaedro.

Dito isto, há ou não espaço suficiente para colocar em órbita uma outra esfera ao redor da central? Se bem que existem muitas provas sobre o número correto, nenhuma delas é verdadeiramente elementar, como a gente gostaria de ver por um problema deste tipo, de natureza finita e muito concreto.

Assim como no $\mathbb{R}^2$, um bom empacotamento é aquele em que a proporção do volume ocupado pelas esferas numa porção do espaço está próxima do maior valor possível. A taxa que nos fornece esta proporção é a densidade do empacotamento. Vamos defini-la para o $\mathbb{R}^m$:

Definição 1.16 *Seja $r = \rho_\Lambda$, o raio do empacotamento de $\Lambda \in \mathbb{R}^m$, então a densidade de Λ é dada por*

$$\Delta(\Lambda) = \frac{vol(B_\rho(0))}{vol(R(0))},$$

onde $vol(B_\rho(0))$ é o volume n - dimensional da esfera de centro O e raio ρ_Λ e sendo $vol(R(0))$ o volume n- dimensional do paralelotopo fundamental de Λ.

É claro que, neste caso, determinar a região de Voronoi de um reticulado não é um problema trivial e, na forma em que foi definida a densidade, esta é de difícil aplicabilidade. Com isso, pela definição 1.12, o volume da região de Voronoi $R(0)$ é igual ao volume de $\mathcal{P}$, assim, o volume de $R(0)$ é igual à raiz quadrada do determinante de Λ.

Portanto, expressamos a densidade de Λ como

$$\Delta(\Lambda) = \frac{vol(B_\rho(0))}{(det\Lambda)^{\frac{1}{2}}},$$

e o problema de calcular Δ fica resolvido se tivermos uma base do reticulado Λ e sua distância mínima.

Para reticulados n-dimensionais em $\mathbb{R}^n$, torna-se necessária a expressão do volume de uma esfera n-dimensional.

O volume V de uma esfera n-dimensional de raio ρ é dado por:

$$V = V_n \rho^n$$

onde V_n é o volume de uma esfera de raio 1, dada por

$$V_n = \frac{\pi^{\frac{n}{2}}}{(\frac{n}{2})!} = \frac{2^n \pi^{\frac{(n-2)}{2}} \left(\frac{(n-2)}{2}\right)!}{n!}.$$

A segunda forma evita o uso de $(\frac{n}{2})!$ quando n é ímpar.

Usando a definição de volume V de uma esfera n-dimensional com a de densidade, podemos redefini-la como

$$\Delta_\Lambda = \frac{V_n \rho^n}{(det\Lambda)^{\frac{1}{2}}}$$

Proposição 1.5 *Reticulados equivalentes têm a mesma densidade.*

Demonstração: *Sejam Λ_1 e Λ_2 reticulados equivalentes com matrizes de Gram G_1 e G_2, respectivamente,temos:*

$$\Delta_2 = \frac{V_n \rho_2^n}{|det(G_2)|^{1/2}} = \frac{V_n \lambda^n \rho_1^n}{\lambda^n |det(G_1)|^{1/2}} = \frac{V_n \rho_1^n}{|det(G_1)|^{1/2}} = \Delta_1$$

■

Na comparação entre densidades de reticulados na mesma dimensão, o volume V_n da esfera unitária aparece como fator comum. Ao dividir a densidade de empacotamento Δ por V_n, tem-se uma medida δ denominada *densidade de centro* do reticulado. Vamos defini-la.

Definição 1.17 *A **densidade de centro** δ é dada por:*

$$\delta = \frac{\Delta(\Lambda)}{V_n}$$

Para empacotamentos reticulados, podemos escrever:

$$\delta = \rho^n \left(det(\Lambda)\right)^{\frac{-1}{2}}.$$

Exemplo 1.13 *Se $\Lambda = \mathbb{Z}^2$ com base $\beta = \{(1,0),(0,2)\}$, temos que $\rho_\Lambda = \frac{1}{2}$, $V_n = \pi \cdot 1 = \pi$, o volume do reticulado é $vol(\Lambda) = (det\Lambda)^{1/2} = 4^{1/2} = 2$, a densidade de empacotamento é*

$$\Delta_\Lambda = \frac{V_n \rho^n}{(det\Lambda)^{\frac{1}{2}}} = \frac{\pi \cdot \left(\frac{1}{2}\right)^2}{2} = \frac{\pi}{8}$$

e a densidade de centro é

$$\delta = \frac{\Delta(\Lambda)}{V_n} = \frac{\frac{\pi}{8}}{\pi} = \frac{1}{8}$$

Notemos que, para determinar a densidade de empacotamento, precisamos encontrar dois valores: o volume da região fundamental, o que em geral não é muito complexo, e a menor norma dentre os elementos não nulos do reticulado. Este último por sua vez é um problema computacionalmente muito complexo. No próximo capítulo comentaremos a respeito deste problema.

1.3 Problema da Cobertura

De alguma forma, este é um problema dual do problema de empacotamento. Pergunta - se pelo caminho mais econômico para cobrir o espaço Euclidiano n-dimensional com esferas (que se sobrepõem) de mesmo raio. Esse problema é ainda mais interessante do que seus antecessores, e ainda mais difícil de resolver. Tem aplicações importantes, como por exemplo, a utilização em radares, em comunicações digitais, etc.

Vejamos na figura 1.20 os dois reticulados planos mais destacados, juntamente com suas coberturas. É óbvio que a cobertura que pertence ao reticulado quadrado é menos econômica do que aquele que pertence ao reticulado hexagonal

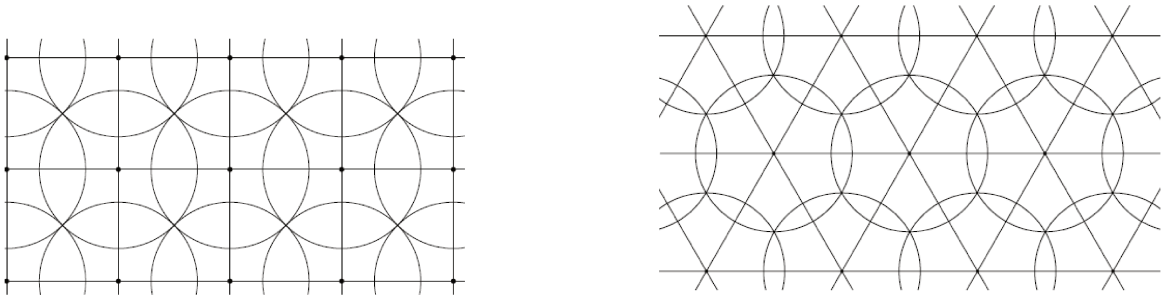


Figura 1.20: Cobertura plana com circulos: No primeiro os centros dos círculos pertencem ao reticulado quadrado $\mathbb{Z}^2$, e no segundo pertencem ao reticulado hexagonal que mostra menos sobreposições entre os círculos tornando a cobertura mais eficiente.

Para fazer isto precisamos definir a densidade Θ de uma cobertura da mesma forma como a densidade Δ de um empacotamento.

Definição 1.18 *Suponha que um arranjo de esferas de raio R abrange $\mathbb{R}^n$. Se os centros formam um reticulado Λ a* ***densidade de cobertura*** *é definida por*

$$\Theta = \frac{\textit{Volume de uma esfera}}{(det\Lambda)^{1/2}} = \frac{V_n R^n}{(det\Lambda)^{1/2}}.$$

onde V_n é o volume de uma esfera unitária n-dimensional e R é denominado raio de cobertura. R é o menor raio que resulta em uma cobertura do espaço gerado por Λ.

Capítulo 2

Reticulados Raízes

Neste capítulo iremos introduzir as definições dos reticulados raízes $\mathbb{Z}^n (n \geq 1)$, $\mathbb{A}_n (n \geq 1)$ e $\mathbb{D}_n (n \geq 3)$ e seus duais. Faremos um resumo das propriedades básicas de cada um desses reticulados. Estes reticulados se destacam pois possuem densidade de centro recorde, além disso, é provado que essas densidades são as melhores até a dimensão 8. Em dimensões maiores que 8, existem reticulados com densidades de centro ótimas são eles, K_{12} e Λ_{24}, e existem reticulados com densidades de centro recordes, mas não se sabe se essas densidades são ótimas.

Os reticulados raízes, são somas ortogonais de reticulados irredutíveis. Eles desempenham um papel crucial no desenvolvimento desta dissertação pois, como possuem propriedades bastante definidas podem ser usados em algoritmos para uma decodificação que busque o vetor mais próximo de um ponto qualquer de um reticulado.

As principais referências para este capítulo são [4, 12, 14, 16, 20].

2.1 O reticulado n-dimensional $\mathbb{Z}^n$

Definição 2.1 *O conjunto dos inteiros,* $..., -2, -1, 0, 1, 2, ...$, *é denotado por* $\mathbb{Z}$, *e*

$$\mathbb{Z}^n = \{x \in \mathbb{R}^n : x_i \in \mathbb{Z}\}$$

é o reticulado n-dimensional ou reticulado inteiro.

Observação 2.1 *$\mathbb{Z}^2$ é melhor chamado "reticulado quadrado", como visto no papel de gráfico comum.*

Observação 2.2 *Como matriz geradora M podemos considerar a matriz identidade.*

O reticulado $\mathbb{Z}^n$ possui as seguintes propriedades:

1. $det(\mathbb{Z}^n) = 1$.
2. A norma mínima é igual a 1 e os vetores minimais são da forma $(0, ..., \pm 1, ..., 0)$.
3. O raio de empacotamento é $\rho = \frac{1}{2}$ e o raio de cobertura é $R = \frac{\sqrt{n}}{2} = \rho\sqrt{n}$.
4. A densidade de empacotamento é $\Delta = V_n \cdot 2^{-n}$ e a densidade de centro $\delta = 2^{-n}$.
5. O *kissing number* $\tau = 2n$.
6. O reticulado $\mathbb{Z}^n$ é autodual.

Assim, $\mathbb{Z}$ tem densidade $\Delta = 1$, mas as densidades de $\mathbb{Z}^2$, $\mathbb{Z}^3$ e $\mathbb{Z}^4$ são apenas $\frac{\pi}{4} = 0.785...$, $\frac{\pi}{6} = 0.524...$ e $\frac{\pi^2}{32} = 0.308....$

2.2 Os reticulados n-dimensionais $\mathbb{A}_n$ e $\mathbb{A}_n^*$

Definição 2.2 *Para $n \geq 1$, temos que:*

$$\mathbb{A}_n = \left\{ x \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

Observação 2.3 *Este reticulado utiliza $n + 1$ coordenadas para definir um reticulado n - dimensional.*

O reticulado $\mathbb{A}_n$ mora no hiperplano H definido pela equação $\sum_{i=0}^{n} x_i = 0 \in \mathbb{R}^{n+1}$ e como se pode perceber na definição ele é a intersecção entre $\sum_{i=0}^{n} x_i = 0$ e $\mathbb{Z}^{n+1}$. Sua matriz geradora M (que não é quadrada) é dada por:

$$M_{\mathbb{A}_n} = \begin{pmatrix} -1 & 0 & 0 & ... & 0 \\ 1 & -1 & 0 & ... & 0 \\ 0 & 1 & -1 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ . & . & . & ... & . \\ 0 & 0 & 0 & ... & -1 \\ 0 & 0 & 0 & ... & 1 \end{pmatrix}$$

cuja matriz de Gram é dada por,

$$G_{\mathbb{A}_n} = \begin{pmatrix} 2 & -1 & 0 & ... & 0 & 0 \\ -1 & 2 & -1 & ... & 0 & 0 \\ 0 & -1 & 2 & ... & 0 & 0 \\ . & . & . & ... & . & . \\ 0 & 0 & 0 & ... & 2 & -1 \\ 0 & 0 & 0 & ... & -1 & 2 \end{pmatrix}$$

O reticulado $\mathbb{A}_n$ possui as seguintes propriedades:

1. $det(\mathbb{A}_n) = n + 1$.
2. A norma mínima é igual a 2 e os vetores minimais são todas as permutações de $(1, -1, ..., 0, 0)$.
3. O raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$ e o raio de cobertura é $R = \rho \cdot \sqrt{\frac{2a(n+1-a)}{n+1}}$, onde a é a parte inteira de $\frac{(n+1)}{2}$.
4. A densidade de centro é $\delta = 2^{\frac{-n}{2}} \cdot (n+1)^{\frac{-1}{2}}$.
5. O *kissing number* $\tau = n \cdot (n + 1)$.

6. O reticulado $\mathbb{A}_n$ é autodual.

Vamos demonstrar algumas das propriedades acima iniciando pelo cálculo do determinante. Tendo em conta que é o determinante do reticulado $\mathbb{A}_n$, se desenvolvermos o determinante pela primera linha da matriz obtemos a seguinte recursão:

$$det(\mathbb{A}_n) = 2 \cdot det(\mathbb{A}_{n-1}) - det(\mathbb{A}_{n-2})$$

De onde sai que

$$det(\mathbb{A}_n) = n + 1.$$

■

Seja $\mathcal{B}$ uma base de $\mathbb{Z}^{n+1}$, um vetor diferente de zero em $\mathbb{A}_n$ tem pelo menos dois componentes diferentes de zero em $\mathcal{B}$. Isto imediatamente mostra que $\mathbb{A}_n$ tem norma 2. Por outra parte, é claro que os vetores de norma mínima em $\mathbb{A}_n$ são os da forma $(1, -1, ..., 0, 0)$ o que implica que o raio de empacotamento de $\mathbb{A}_n$ é $\rho = \frac{\sqrt{2}}{2}$.

Vamos calcular a densidade de centro para todo n:

$$\delta(\mathbb{A}_n) = \frac{\Delta(\mathbb{A}_n)}{V_n} = \frac{\rho^n}{\sqrt{det(\mathbb{A}_n)}} = \frac{1}{(\sqrt{2})^n} \frac{1}{\sqrt{n+1}} = 2^{\frac{-n}{2}} \cdot (n+1)^{\frac{-1}{2}}$$

■

Um grande exemplo para o reticulado $\mathbb{A}_n$ é o reticulado $\mathbb{A}_2$ conhecido como *reticulado hexagonal*. Vamos detalhá-lo agora.

O reticulado hexagonal

O reticulado hexagonal é assim chamado porque as regiões de Voronoi são hexágonos, conforme mostra a figura 2.1.

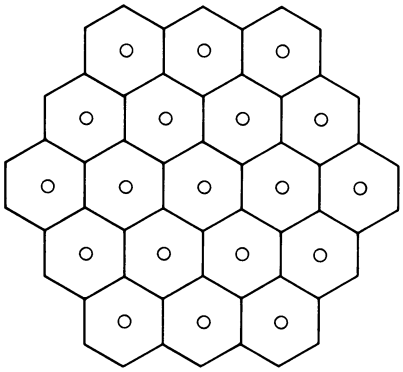


Figura 2.1: As regiões de Voronoi são hexagonos.

O reticulado hexagonal $\Lambda = \mathbb{A}_2$ é um reticulado gerado pelos vetores $u_1 = (1, 0)$ e $u_2 = \left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$. Uma possível matriz geradora é

$$M_{\mathbb{A}_2} = \begin{pmatrix} 1 & \frac{-1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}$$

A figura 2.2 mostra o reticulado hexagonal no plano.

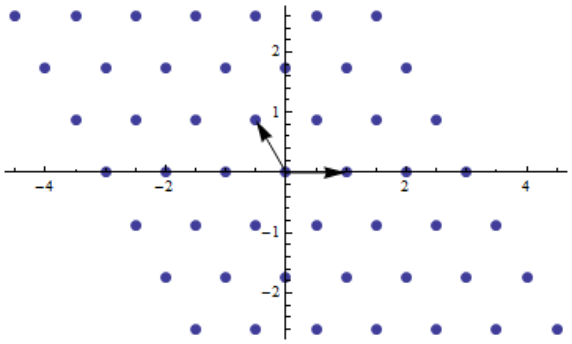


Figura 2.2: Reticulado hexagonal $\Lambda = \mathbb{A}_2$. Destaque para os vetores da base.

Ja definimos propriedades como o empacotamento reticulado e a densidade de empacotamento. Para o reticulado hexagonal essas propriedades são bem definidas.

Proposição 2.1 *O melhor empacotamento reticulado em dimensão 2 é o hexagonal.*
Demonstração: *Suponha que Λ seja ideal. Se em Λ não existir duas esferas que se tocam, então não é ideal, já que haverá uma escalar t, $0 < t < 1$ tal que $t \cdot \Lambda$ teria uma densidade maior que Λ. Então existem duas esferas que se tocam, assim nós temos uma*

fila de esferas, uma após a outra. Além disso, Λ é a união dessas filas de esferas, todas paralelas. Agora, se essas filas paralelas não se tocam, então, novamente Λ não seria ideal. Portanto, devem se tocar. Ao tocar-se, vemos que há infinitas posições possíveis, mas é evidente que o melhor é a correspondente ao reticulado hexagonal.

■

Teorema 2.1 *(Thue, 1890). A maior densidade possível de um empacotamento de esferas em dimensão 2 é dada pelo empacotamento hexagonal, com* $\Delta = \frac{\pi}{\sqrt{12}} \cong 0,907$.

Embora pareça muito fácil, esse teorema não é. Veja, por exemplo, uma prova em [9], que é levar um empacotamento arbitrário do plano com as esferas de raio 1 e logo particionar o plano em três tipos de regiões, cada uma com uma densidade inferior ou igual a $\frac{\pi}{\sqrt{12}}$.

2.2.1 O Reticulado $\mathbb{A}_n^*$

O dual do reticulado $\mathbb{A}_n$ é o reticulado $\mathbb{A}_n^*$ definido por:

$$\mathbb{A}_n^* = \bigcup_{i=0}^{n} ([i] + \mathbb{A}_n)$$

Sua matriz geradora $(n) \times (n+1)$ é dada por:

$$M_{\mathbb{A}_n^*} = \begin{pmatrix} 1 & 1 & ... & 1 & \frac{-n}{n+1} \\ -1 & 0 & ... & 0 & \frac{1}{n+1} \\ 0 & -1 & ... & 0 & \frac{1}{n+1} \\ 0 & 0 & ... & 0 & \frac{1}{n+1} \\ . & . & . & ... & . \\ 0 & 0 & ... & -1 & \frac{1}{n+1} \\ 0 & 0 & ... & 0 & \frac{1}{n+1} \end{pmatrix}$$

cuja matriz de Gram é,

$$G_{\mathbb{A}_n^*} = \begin{pmatrix} 2 & 1 & 1 & ... & 1 & -1 \\ 1 & 2 & 1 & ... & 1 & -1 \\ 1 & 1 & 2 & ... & 1 & -1 \\ . & . & . & ... & . & . \\ 1 & 1 & 1 & ... & 2 & -1 \\ -1 & -1 & -1 & ... & -1 & \frac{n}{n+1} \end{pmatrix}.$$

Como vimos na subseção 1.1.4, as matrizes de Gram de reticulados duais estão relacionados de forma que

$$det(G^*) = det(G)^{-1},$$

logo

$$det(A^*) = det(A)^{-1} = \frac{1}{n+1}$$

O reticulado $\mathbb{A}_n^*$ possui as seguintes propriedades:

1. A norma mínima quadrada é igual a $\frac{n}{n+1}$.
2. A densidade de centro é $\delta = \frac{n^{\frac{n}{2}}}{2^n(n+1)^{\frac{n-1}{2}}}$.
3. O *kissing number* $\tau = 2$ para $n = 1$ e $\tau = 2n + 2$ para $n \leq 2$.
4. O raio de empacotamento é $\rho = \frac{1}{2}\sqrt{\frac{n}{n+1}}$ e o raio de cobertura é $R = \rho\sqrt{\frac{n+2}{3}}$.
5. A densidade de empacotamento é $\Delta = V_n\left(\rho\right)^n\left(n+1\right)^2$ e a densidade de cobertura é $\Theta = V_n\sqrt{n+1}\left[\frac{n(n+2)}{12(n+1)}\right]^{\frac{n}{2}}$.

2.3 Os reticulados n-dimensionais $\mathbb{D}_n$ e $\mathbb{D}_n^*$

Para todo $n \geq 3$, temos que

$$\mathbb{D}_n = \left\{ x \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \in 2 \cdot \mathbb{Z} \right\}.$$

é um reticulado.

Em outras palavras, este reticulado pode ser obtido colorindo os pontos de $\mathbb{Z}^n$ alternadamente com vermelho e branco e tomando os pontos vermelhos como num tabuleiro de xadrez *(checkerboard)*, devido a isso, o reticulado $\mathbb{D}_n$ as vezes é chamado de *reticulado checkerboard*.

Possui matriz geradora, dada por:

$$M_{\mathbb{D}_n} = \begin{pmatrix} -1 & 1 & 0 & ... & 0 & 0 \\ -1 & -1 & 1 & ... & 0 & 0 \\ 0 & 0 & -1 & ... & 0 & 0 \\ . & . & . & ... & . & . \\ 0 & 0 & 0 & ... & 0 & -1 \\ 0 & 0 & 0 & ... & 0 & -1 \end{pmatrix}.$$

Consequentemente sua matriz de Gram é:

$$G_{\mathbb{D}_n} = \begin{pmatrix} 2 & 0 & -1 & ... & 0 & 0 \\ 0 & 2 & -1 & ... & 0 & 0 \\ -1 & -1 & 2 & ... & 0 & 0 \\ . & . & . & ... & . & . \\ 0 & 0 & 0 & ... & 2 & -1 \\ 0 & 0 & 0 & ... & -1 & 2 \end{pmatrix}.$$

O reticulado $\mathbb{D}_n$ possui as seguintes propriedades:

1. O determinante de $\mathbb{D}_n$ é 4.
2. A norma mínima é $\sqrt{2}$ e os vetores minimais são todas as permutações de $(\pm 1, \pm 1, 0, ...0)$;
3. O "kissing number"$\tau = 2n(n-1)$;
4. O raio de empacotamento é $\frac{\sqrt{2}}{2}$ e o raio de cobertura $R = \rho\sqrt{2}$ para n = 3 e $\rho\sqrt{\frac{n}{2}}$ para $n \geq 4$;
5. A densidade de centro $\delta = 2^{-\left(\frac{n+2}{2}\right)}$

Quando $n = 2$ ou 3, $\mathbb{D}_2$ é semelhante a $\mathbb{Z}^2$, e $\mathbb{D}_3$ é isométrica a $\mathbb{A}_3$.

Vejamos alguns exemplos do reticulado $\mathbb{D}_n$.

Exemplo 2.1 *Reticulado 3-dimensional* $\mathbb{D}_3$.

É definido por

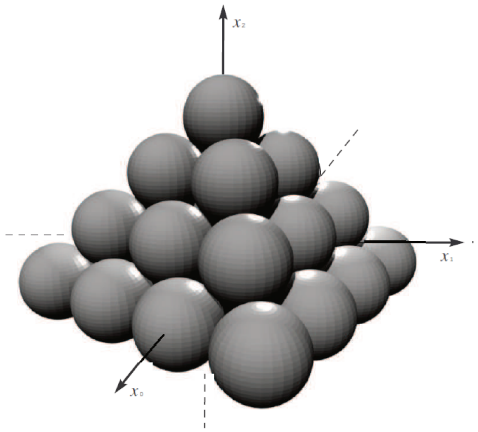
$$\mathbb{D}_3 = \left\{(x_1; x_2; x_3) \in \mathbb{Z}^3 : x_1 + x_2 + x_3 \in 2 \cdot \mathbb{Z}\right\}.$$

Uma matriz geradora para $\mathbb{D}_3$ *é dada por*

$$M_{\mathbb{D}_3} = \begin{pmatrix} -1 & 1 & 0 \\ -1 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

A figura 2.1 abaixo mostra o arranjo das esferas do empacotamento associado a $\mathbb{D}_3$.

Já contamos a história deste empacotamento que possui algumas propriedades como raio de empacotamento $\rho = \frac{\sqrt{2}}{2}$ *e densidade de centro* $\delta = \frac{1}{4\sqrt{3}} = 0,17678$ *que é a densidade de centro máxima para dimensão 3.*



Exemplo 2.2 *Reticulado 4-dimensional* $\mathbb{D}_4$ *ou reticulado checkerboard.*

É definido por

$$\mathbb{D}_4 = \left\{(x_1; x_2; x_3; x_4) \in \mathbb{Z}^4 : x_1 + x_2 + x_3 + x_4 \in 2 \cdot \mathbb{Z}\right\}.$$

Assim, $(1, 1, 0, 0) \in \mathbb{D}_4$, *porém* $(1, 0, 0, 0) \notin \mathbb{D}_4$. *De fato, note que cada vetor em* $\mathbb{D}_4$ *deve ter norma maior ou igual que 2, pois se apenas uma de suas coordenadas é não*

nula, esta deve ser par, logo sua norma será ao menos 4; e se tiver duas coordenadas não nulas, então sua norma é ao menos 2. Isto nos diz que o raio de empacotamento de $\mathbb{D}_4$ *é* $\frac{\sqrt{2}}{2}$.

Nos falta calcular o determinante de $\mathbb{D}_4$. *Para isso, notemos que os vetores da forma* $(2,0,0,0)$ *estão em* $\mathbb{D}_4$ *e que uma matriz geradora de* $\mathbb{D}_4$ *é dada por*

$$M_{\mathbb{D}_4} = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

Portanto, $det(\mathbb{D}_4) = det(M_{\mathbb{D}_4})^2 = 4$.

Logo, $vol(\mathbb{D}_4) = 2$.

2.3.1 O Reticulado $\mathbb{D}_n^*$

O dual do reticulado $\mathbb{D}_n$ é o reticulado $\mathbb{D}_n^*$ definido por:

$$\mathbb{D}_n^* = \mathbb{D}_n \cup ([1] + \mathbb{D}_n) \cup ([2] + \mathbb{D}_n) \cup ([3] + \mathbb{D}_n)$$

Sua matriz geradora é dada por:

$$G_{\mathbb{D}_n^*} = \begin{pmatrix} 1 & 0 & ... & 0 & \frac{1}{2} \\ 0 & 1 & ... & 0 & \frac{1}{2} \\ . & . & . & ... & . \\ 0 & 0 & ... & 1 & \frac{1}{2} \\ 0 & 0 & ... & 0 & \frac{1}{2} \end{pmatrix}.$$

O reticulado $\mathbb{D}^*{}_n$ possui as seguintes propriedades:

1. O determinante de $\mathbb{D}^*{}_n$ é $\frac{1}{4}$.
2. A norma mínima é $\sqrt{\frac{3}{4}}$ para n = 3 ou 1 para $n \geq 4$;
3. O "kissing number"$\tau = 8$ para n = 3, $\tau = 24$ para n = 4 ou $\tau = 2n$ para $n \geq 5$;

4. O raio de empacotamento é $\frac{\sqrt{3}}{4}$ para $n = 3$ e $\frac{1}{2}$ para $n \geq 4$, o raio de cobertura $R = \rho\frac{n^{\frac{1}{2}}}{\sqrt{2}}$ para n par e $R = \rho\sqrt{\frac{5}{3}}$ para $n = 4$ e $R = \rho\frac{(2n-1)^{1/2}}{2}$ para n ímpar $n \geq 5$;

5. A densidade de centro $\delta = 3^{1.5}2^{-5}$ para $n = 3$ ou $\delta = 2^{-(n-1)}$ para $n \geq 4$;

2.4 Análise geométrica das densidades dos reticulados raízes $\mathbb{Z}^n$, $\mathbb{A}_n$, $\mathbb{D}_n$ e seus duais

Já sabemos que a densidade de um empacotamento reticulado é a proporção do espaço ocupado pelas esferas. Sabemos também, que a densidade de centro de um reticulado é o número dos pontos do reticulado por unidade de volume e que pode ser obtido dividindo-se sua densidade pelo volume da esfera unitária. Portanto, a maior densidade (centro) implica que o seu dual é um reticulado de amostragem mais eficiente.

A figura 2.3 mostra a densidade de centro dos reticulados raízes que foram considerados neste trabalho. O gráfico indica a eficiência de amostragem mais pobres do reticulado cartesiano $\mathbb{Z}^n$ em comparação com outros reticulados raízes.

$\mathbb{Z}^n$	$\mathcal{A}_n$	$\mathcal{A}_n^*$	$\mathcal{D}_n$	$\mathcal{D}_n^*$
2^{-n}	$2^{-n/2}(n+1)^{-1/2}$	$\frac{n^{n/2}}{2^n(n+1)^{(n-1)/2}}$	$2^{-(n+2)/2}$	$\begin{cases} 3^{1.5}2^{-5} & (n=3) \\ 2^{-(n-1)} & (n>3) \end{cases}$

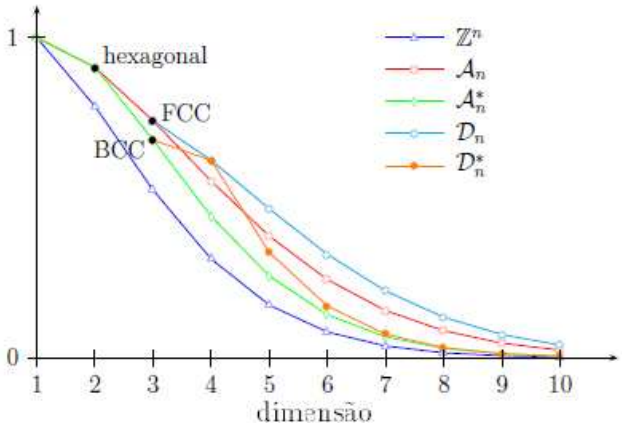


Figura 2.3: Densidade dos vários reticulados raizes até dimensão 10.Figura extraída de [18]

Capítulo 3

Problemas em Reticulados

3.1 O Problema da Redução de Base em Reticulados

A redução de base de um reticulado ou, simplesmente, redução de base, é um processo pelo qual uma base reduzida, que consiste em vetores curtos e ortogonalmente próximos, é construída a partir de uma base dada. Para apresentar este assunto nos limitaremos a três formas de redução de base, são elas:

- A redução das bases de dimensão 2 que foi dada por Lagrange e Gauss, de onde observaremos que o algoritmo está muito relacionado ao algoritmo de Euclides.
- A redução LLL devida a Lenstra, Lenstra e Lovász que é importante do ponto de vista prático e a redução de Minkowski.

As referências para este capítulo, são [2, 8, 11, 22]

3.1.1 Redução de bases em reticulados de duas dimensões

Sejam $b_1, b_2 \in \mathbb{R}^2$ dois vetores linearmente independentes e denotamos por Λ o reticulado gerado por b_1 e b_2. O objetivo é tomar uma base para o reticulado tal que os comprimentos dos vetores da base sejam os mais curtos possíveis (neste caso tendem a ser minimos). Gauss mostrou os seguintes critérios para a redução de uma base e então desenvolveu uma algoritmo para calcular esta base.

Definição 3.1 *Uma base ordenada $b_1, b_2 \in \mathbb{R}^2$ é* ***Gauss reduzida*** *se $||b_1|| \leq ||b_2|| \leq ||b_2 + qb_1||$ para todo $q \in \mathbb{Z}$.*

O seguinte teorema mostra que os vetores da base Gauss reduzida são os mais curtos possíveis. Este resultado serve para qualquer norma, apesar do algoritmo apresentado abaixo seja apenas para a norma Euclidiana.

Teorema 3.1 *Sejam λ_1, λ_2 os mínimos sucessivos de Λ. Se Λ possuir uma base ordenada $\{b_1, b_2\}$ que seja Gauss reduzida então $||b_i|| = \lambda_i$ para $i = 1, 2$.*
Demonstração: *Por definição temos que*

$$||b_2 + qb_1|| \geq ||b_2|| \geq ||b_1||$$

para todo $q \in \mathbb{Z}$

Seja $v = l_1 \cdot b_1 + l_2 \cdot b_2$ qualquer ponto não-nulo em Λ.

- *Se $l_2 = 0$, então $||v|| \geq ||b_1||$;*
- *Se $l_2 \neq 0$ então escrevemos $l_1 = q \cdot l_2 + r$ com $q, r \in \mathbb{Z}$ tal que $0 \leq r \leq |l_2|$. Logo $v = r \cdot b_1 + l_2 \cdot (b_2 + qb_1)$ e, pela desigualdade triangular*

$$||v|| \geq |l_2| \cdot ||b_2 + qb_1|| - r \cdot ||b_1||$$

$$= (|l_2| - r)||b_2 + qb_1|| + r(||b_2 + qb_1|| - ||b_1||)$$

$$\geq ||b_2 + qb_1|| \geq ||b_2|| \geq ||b_1||.$$

Isto completa a demostração.

■

Definição 3.2 *Seja $b_1, ..., b_n$ uma lista de vetores $\in \mathbb{R}^n$. Escrevemos $B_i = ||b_i||^2 = \langle b_i, b_i \rangle$.*

Um componente crucial para o algoritmo de Gauss é que

$$||b_2 - \mu b_1||^2 = B_2 - 2\mu \langle b_1, b_2 \rangle + \mu^2 B_1$$

é minimizado em $\mu = \langle b_1, b_2 \rangle / B_1$. Já que estamos trabalhando com reticulados devemos substituir b_2 por $b_2 - \lfloor \mu \rceil b_1$ onde $\lfloor \mu \rceil$ é um inteiro mais próximo a μ. Assim as linhas 3 e 9 do algoritmo de Gauss reduzem o tamanho de b_2 usando tanto quanto possível b_1. No caso de unidimensional a fórmula $b_2 - \lfloor \mu \rceil b_1$ é a operação familiar $r_{i+1} = r_{i-1} - \lfloor r_{i-1}/r_i \rceil r_i$ do algoritmo de Euclides.

Lema 3.1 *[8] Uma base ordenada* $\{b_1, b_2\}$ *é* ***Gauss reduzida*** *se, e somente se*

$$||b_1|| \leq ||b_2|| \leq ||b_2 \pm b_1||.$$

Lema 3.2 *[8] O algoritmo abaixo produz uma base de Gauss reduzida para o reticulado* Λ

Algoritmo de Redução de Gauss

INPUT: Bases $b_1, b_2 \in \mathbb{Z}^2$ para um reticulado Λ
OUTPUT: Bases (b_1, b_2) para Λ tal que $\|b_i\| = \lambda_i$

1: $B_1 = \|b_1\|^2$
2: $\mu = \langle b_1, b_2 \rangle / B_1$
3: $b_2 = b_2 - \lfloor \mu \rceil b_1$
4: $B_2 = \|b_2\|^2$
5: enquanto $B_2 < B_1$ faça
6: troque b_1 e b_2
7: $B_1 = B_2$
8: $\mu = \langle b_1, b_2 \rangle / B_1$
9: $b_2 = b_2 - \lfloor \mu \rceil b_1$
10: $B_2 = \|b_2\|^2$
11: fim enquanto
12: retorna (b_1, b_2)

Figura 3.1: Algoritmo de Redução de Gauss

As figuras 3.2, 3.3 e 3.4 mostram geometricamente cada etapa desta redução.

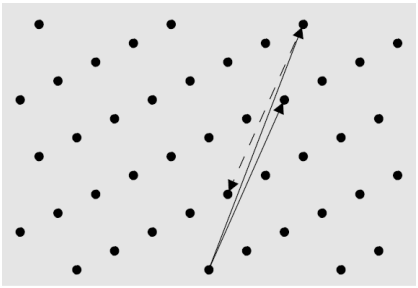


Figura 3.2: Primeira etapa de redução

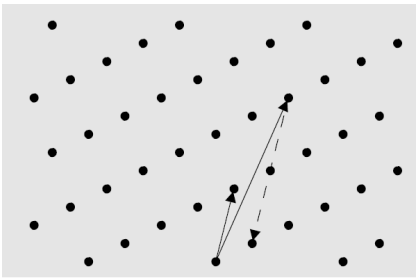


Figura 3.3: Segunda etapa de redução

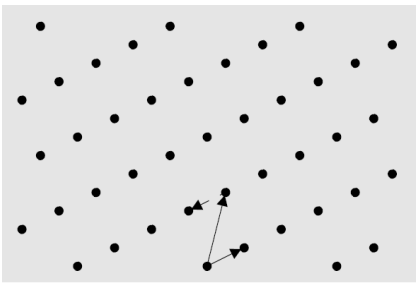


Figura 3.4: Terceira etapa de redução

Exemplo 3.1 *Apliquemos o algoritmo de Redução de Gauss às colunas da matriz*

$$A = \begin{pmatrix} 1 & 6 \\ 5 & 21 \end{pmatrix},$$

com $b_1 = (1, 5)$ *e* $b_2 = (6, 21)$. *Na primeira iteração fazemos* $\lfloor \mu \rceil = \frac{111}{26} \approx 4.27$ *e assim nós atualizamos* $b_2 = b_2 - 4b_1 = (2, 1)$. *Em seguida trocamos* b_1 *e* b_2 *para que*

os valores no loop sejam agora $b_1 = (2,1)$ *e* $b_2 = (1,5)$. *Dessa vez,* $\lfloor \mu \rceil = \frac{7}{5} = 1.4$ *e assim* $b_2 = b_2 - b_1 = (-1,4)$. *Desde* $||b_2|| > ||b_1||$ *o algoritmo pára e as saidas são* $\{(2,1),(-1,4)\}$.

Em 1982, Lenstra, Lenstra e Lovász descobriram uma classe de redução de bases, o chamado algoritmo LLL, que oferece um método eficiente para encontrar vetores curtos em um reticulado. Este método é importante para os nossos propósitos, na próxima seção iremos defini-lo com mais detalhes.

3.1.2 Métodos de Redução.

Redução LLL (Lenstra, Lenstra e Lovász) ou Método de Redução de Base.

Seja $(b_1, ..., b_m)$ uma base para um reticulado Λ e seja $(b_1^*, ..., b_m^*)$ a sua ortogonalização de Gram-Schmidt. A base $(b_1, ..., b_m)$ é dita *LLL - reduzida* se os coeficientes de Gram-Schmidt satisfazerem $|\mu_{i,j}| \leq \frac{1}{2}$ para $1 \leq j < i \leq n$, e

$$||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \geq \frac{3}{4} ||b_{i-1}^*||^2$$

para $1 < i \leq n$, ou equivalentemente

$$||b_i^*||^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) ||b_{i-1}^*||^2$$

para $1 < i \leq n$.

Note que os vetores $b_i^* + \mu_{i,i-1} b_{i-1}^*$ e b_{i-1}^* são as projeções de b_i e b_{i-1}, respectivamente, sobre o complemento ortogonal do posto de $(b_1, ..., b_{i-2})$.

Uma propriedade muito útil de uma base LLL-reduzida, conforme o teorema a seguir demonstra, é que existem limites para cada um dos vetores da base e estes limites dependem apenas da dimensão do reticulado e do volume. O resultado é para reticulados inteiros $\Lambda \subseteq \mathbb{Z}^n$, o que significa, simplesmente, que cada vetor do reticulado tem apenas componentes inteiros.

Teorema 3.2 *[8] Seja* $(b_1, ..., b_m)$ *uma base LLL-reduzida de um reticulado* $\Lambda \subseteq \mathbb{Z}^n$. *Então*

$$||b_1|| \leq 2^{(m-1)/4} vol(\Lambda)^{1/m},$$

e quando $||b_1|| \geq 2^{(l-2)/2}$, *os vetores da base restante satisfazem*

$$||b_l|| \leq 2^{(m+l-2)/4} vol(\Lambda)^{1/(m-l+1)}.$$

O limite do vetor de base menor foi mostrado por Lenstra, Lenstra e Lovász, enquanto os limites para os outros vetores da base foram mostrados por J.A Proos.

Na situação improvável de que $||2|| < 2^{(l-2)/2}$, o limite

$$||b_l|| \leq 2^{\frac{m(m-1)}{4(m-l-1)}} vol(\Lambda)^{1/(m-l+1)}.$$

pode ser usado sem restrições.

Teorema 3.3 *[8] Seja* $(b_1, ..., b_m)$ *uma base LLL-reduzida de um reticulado* $\Lambda \subseteq \mathbb{Z}^n$. *Para todo* $x \in \Lambda, x \neq 0$,

$$||b_1|| \leq 2^{(m-1)/2} ||x||.$$

Além dessas propriedades, as bases LLL-reduzidas são uma importante classe de bases reduzidas, de um ponto de vista prático, porque elas podem ser calculadas de forma eficiente.

Para um reticulado m-dimensional com vetores n-dimensionais ($\Lambda \in \mathbb{Z}^n$, por exemplo), o algoritmo LLL tem tempo de execução de ordem $O(nm^5B^3)$, onde B é um limite no tamanho dos vetores da base de entrada [8]. Embora o tempo de execução seja polinomial no tamanho da entrada (a base inicial para o reticulado), o algoritmo é ineficiente quando a dimensão do reticulado é muito grande e quando os vetores dos reticulado são muito grandes. O algoritmo mais rápido que calcula uma base LLL-reduzida é o *Nguyen e Stehlé's do algoritmo* L^2, que é uma variante de ponto flutuante do algoritmo LLL [8]. O tempo de execução desse algoritmo é de ordem $O(nm^4(m+B)B)$, que oferece uma melhora significativa quando os vetores da base são muito grandes.

Redução de Minkowski

Seja f uma forma quadrática positiva definida n-dimensional sobre $\mathbb{R}$. Dizemos que f é uma forma reduzida de Minkowski se ela pode ser expressa em termos de uma base $(b_1, ..., b_m)$ tal que para cada t, $1 \leq t \leq n$,

$$f(b_t) \leq f(v)$$

para todos os vetores inteiros v para o qual $b_1, ..., b_{t-1}, v$ podem ser extendidos a uma base de Λ.

Em outras palavras, cada b_t sucessivo é escolhido tal que $f(b_t)$ seja tão pequeno quanto possível. Deixando v percorrer todos os vetores do reticulados, a condição dada acima implica em desigualdades sobre a matriz com entradas a_{ij}.

Definição 3.3 *Dado um reticulado Λ em $\mathbb{R}^n$ e $f(x) = \langle x, x \rangle$, diremos que $B = \{b_1, ..., b_n\}$ é uma base de Minkowski se para cada t, $1 \leq t \leq n$,*

$$||b_t||^2 \leq ||r||^2$$

para todos os vetores inteiros r para o qual $b_1, ..., b_{t-1}, r$ podem ser estendidos a uma base de Λ.

Dada uma base qualquer de um reticulado, uma base de Minkowski pode ser obtida de forma recursiva. O algoritmo aplicado na matriz geradora é de alta complexidade computacional, o que dificulta a obtenção de redução para dimensões altas.

Existem outras formas de redução, como a redução HKZ que não citamos neste trabalho. Porém uma referência sobre o assunto ver [15].

3.2 O Problema do Vetor mais Curto e mais Próximo.

Nesta seção, iremos estudar os problemas do Vetor mais Curto (PVMC) e do Vetor mais Próximo (PVMP). Inicialmente citaremos o estudo do Problema do Vetor mais Curto de um reticulado e o relacionaremos com o Problema do Vetor mais Próximo .

Mostraremos também, que existe um algoritmo polinomial, que permite determinar um limite superior para o vetor mais curto de um reticulado, considerando para tal o vetor de norma mínima da base construída. As referências para esta seção são [15, 17].

3.2.1 O Problema do Vetor mais Curto

Seja Λ um reticulado de dimensão $dim(\Lambda) = m \geq 2$. Dado uma base para Λ, o ***Problema do Vetor mais Curto - (PVMC)*** como o nome sugere, consiste em encontrar um vetor (diferente de zero) $t \in \Lambda$ tal que $||t|| = \lambda_1(\Lambda)$. Existem também duas versões de **aproximação do problema do vetor mais curto**, a primeira **(Problema do vetor mais curto aproximado - PVMCA)** tem por objetivo encontrar um vetor não-nulo $x \in \Lambda$ tal que $||x|| = f(m)\lambda_1(\Lambda)$ por algum fator de aproximação $f(m)$, onde m é a dimensão do reticulado e a segunda **(Problema do vetor mais curto de Hermite - PVMCH)** tem por objetivo encontrar um vetor não-nulo $x \in \Lambda$ tal que $||x|| = f(m)vol(\Lambda)^{\frac{1}{n}}$.

Um resultado clássico de Minkowski estabelece um limite superior para a norma euclidiana minima de um vetor não nulo de um reticulado:

Teorema 3.4 *[2] Seja $\Lambda \in \mathbb{R}^n$ um reticulado de dimensão completa. Então existe $t \in \Lambda \backslash \{0\}$, tal que:*

$$||t|| \leq 2\left(\frac{det\Lambda}{V(n)}\right)^{\frac{1}{n}}$$

onde $V(n)$ representa o volume da bola unitária de dimensão n

Demonstração: *Seja $r = \frac{1}{2}min\{||t|| : t \in \Lambda \backslash \{0\}\}$. Então, para todo $x, y \in \Lambda$ com $x \neq y$ tem-se $||x - y|| > r$. Por isso*

$$B_r(x) \cap B_r(y) = \oslash,$$

onde $B_r(x)$ representa a bola aberta de raio r centrada em x. A medida de $\bigcup_{x\in\Lambda} B_r(x)$ em $\mathbb{R}^n$ é inferior ou igual a medida de $\bigcup_{x\in\Lambda}(x+\pi)$. Como estes conjuntos são disjuntos e têm volume constante, então

$$\frac{r^n V(n)}{det\Lambda} \leq 1$$

que é a razão entre o volume de $B_r(x)$ *e* $(x + \pi)$*, para qualquer* $x \in \Lambda$*, de onde decorre*

$$||t|| \leq 2\left(\frac{det\Lambda}{V(n)}\right)^{\frac{1}{n}}.$$

■

No entanto, ainda não foi encontrado nenhum algoritmo polinomial que determine um t que satisfaça o resultado acima. O Método LLL permite-nos encontrar, em tempo polinomial, um limite superior para a norma desse vetor e uma aproximação para o vetor mais curto.

Teorema 3.5 *[2] Seja* A *uma matriz não singular de racionais de ordem* n*. Então, existe um algoritmo polinomial que permite encontrar um vetor não nulo* t *que pertence ao reticulado gerado pelas colunas de* A*, tal que*

$$||t|| \leq 2^{\frac{(n-1)}{4}}(det\Lambda)^{\frac{1}{n}}.$$

Demonstração: *Seja* $\{t_1, ..., t_n\}$ *uma base reduzida determinada pelo algoritmo LLL para uma matriz de Gram* $G = A^T A$*. Então,*

$$||At_i|| = ||t_1|| = ||t_1^*||.$$

Se a base é reduzida então, usando o fato de que $||t_i^*||^2 \leq 2||t_{i+1}^*||^2$ *para* $1 \leq i \leq n$*, temos* $||t_1^*|| \leq 2^{(k-1)}||t_k^*||, \quad k = 1, ..., n$

assim,

$$||At_1|| = \left(\prod_{k=1}^{n} ||t_1^*||\right)^{\frac{1}{n}}$$

$$\leq \left(\prod_{k=1}^{n} 2^{(k-1)/2}||t_k^*||\right)^{\frac{1}{n}}$$

$$= \left(2^{n(n-1)/4}\prod_{k=1}^{n} ||t_k^*||\right)^{\frac{1}{n}}$$

$$= \left(2^{n(n-1)/4} det\Lambda\right)^{\frac{1}{n}}$$

$$= 2^{(n-1)/4} \left(det\Lambda\right)^{\frac{1}{n}}$$

■

Assim sempre que um vetor t de um reticulado Λ satisfizer a este teorema, devemos considerar que t é um vetor curto de Λ.

3.2.2 O Problema do Vetor mais Próximo

O ***Problema do Vetor mais Próximo - PVMP*** de um ponto reticulado está muito relacionado ao PVMC. É um dos problemas computacionais centrais na geometria dos números sendo considerado $\mathcal{NP} - completo$ [17]. Este problema é definido da seguinte maneira: "Dado um reticulado Λ base $B \in \mathbb{R}^{m \times n}$ e um vetor $t \in \mathbb{R}^m$, deve-se encontrar um vetor reticulado $B \cdot x$ mais próximo de t, i.e, encontrar um vetor inteiro $x \in \mathbb{Z}^n$ tal que $||B \cdot x - t|| \leq ||B \cdot y - t||$ para todo $y \in \mathbb{Z}^n$".

O PVMP pode ser definido a respeito de qualquer norma, mas a norma Euclidiana é a mais comum. Uma versão mais simplificada do problema (usado muito em teoria da complexidade) somente pede para calcular a distância do alvo a partir do reticulado, sem encontrar o vetor reticulado mais próximo da verdade.

O PVMP tem sido estudado em Matemática (linguagem equivalente de formas quadráticas) desde o século XIX. Uma das primeiras referências ao nome PVMP na literatura da ciência da computação surgiram no momento em que o problema foi indicado para ser "$\mathcal{NP} - difícil$"de se resolver [17].

Muitas aplicações do PVMP exigem apenas a descoberta de um vetor do reticulado que não esteja tão distante do alvo, mesmo se não for necessariamente o mais próximo. Uma g - *aproximação* de um algoritmo para o PVMP encontra um vetor reticulado dentro da distância "g" vezes a distância da solução ótima. Os algoritmos polinomiais mais conhecidos para resolver o PVMP são devidos a Babai e Kannak [17], que são baseados em reticulados reduzidos alcançando os fatores de aproximação que são essencialmente exponenciais na dimensão do reticulado. Na prática, as aproximações heuristicas pare-

cem encontrar relativamente boas aproximações ao PVMP em uma quantia de tempo razoável quando a dimensão do reticulado é suficientemente pequena.

O PVMP é a base de vários criptosistemas modernos [6] onde a decriptação corresponde incitosamente para o cálculo do PVMP. Esses criptosistemas são baseados no fato de que qualquer reticulado admite muitas representações diferentes e algumas delas podem ter propriedades geométricas uma melhor do que a outra, isso ajuda para que elas possam ser usadas como resposta secreta de uma decriptação. Contudo, há reticulados que não admitem boas representações, isto é, resolver o PVMP (mesmo aproximadamente) é "$\mathcal{NP} - difícil$" não importando a base dada. Portanto, os exemplos de PVMP usados em criptosistemas baseados em reticulados (para o qual o PVMP possa ser eficientemente resolvido usando a resposta da decriptação) são possivelmente mais fáceis do que os exemplos gerais do PVMP.

Decisão versus Pesquisa

De maneira precisa, pode-se considerar três variantes do $PVMP$, dependendo se temos realmente que encontrar vetor o mais próximo , encontrar a sua distância, ou apenas decidir se ele está mais perto do que algum número dado:

- **PVMP de Decisão:** Dado um reticulado de base $B \in \mathbb{R}^{m\times n}$, o vetor alvo $t \in \mathbb{R}^m$ um racional $r \in \mathbb{Q}$, determinar se $dist\,(t, \Lambda(B)) \leq r$ ou $dist\,(t, \Lambda(B)) > r$.

- **PVMP de Otimização:** Dado um reticulado de base $B \in \mathbb{R}^{m\times n}$ e o vetor alvo $t \in \mathbb{R}^m$, calcular $dist\,(t, \Lambda(B))$.

- **PVMP de pesquisa:** Dado um reticulado de base $B \in \mathbb{R}^{m\times n}$ e o vetor alvo $t \in \mathbb{R}^m$ encontrar um vetor $x \in \mathbb{R}^n$ que minimize $||B \cdot x - t||$.

Não é difícil ver que uma solução para a variante de pesquisa implica imediatamente uma solução para a variante de otimização, além disso, uma solução para a variante de otimização implica em uma solução para a variante de decisão.

Capítulo 4

Encontrando um ponto mais próximo de um reticulado.

Este capítulo descreve alguns dos algoritmos que, dado um ponto arbitrário de $\mathbb{R}^n$, encontram um ponto mais próximo dos reticulados $\mathbb{Z}^n$, $\mathbb{A}_n$ e $\mathbb{D}_n$. Para estudar a aplicabilidade destes algoritmos, faremos algumas implementações computacionais com o software livre *scilab*. A referência para este capítulo é [4].

4.1 Uma breve introdução

Para diversas aplicações é essencial que existam algoritmos "decodificadores"rápidos tal que, dado um ponto arbitrário do espaço, possa encontrar o ponto mais próximo do reticulado.

Neste capítulo, nós vamos descrever algoritmos para decodificação nos reticulados $\mathbb{Z}^n$, $\mathbb{A}_n (n \geq 1)$, $\mathbb{D}_n (n \geq 3)$.

Nas próximas seções estudaremos o problema do vetor mais próximo nos reticulados raízes, que ja foram apresentados no capítulo 2 desta dissertação. A principal referência utilizada foi o capítulo 20 de [4].

Iniciaremos este capítulo fixando algumas notações para uso geral.

Para $x \in \mathbb{R}$ definimos uma função $\lceil x \rfloor$ e a função $w(x)$ que aproxima de modo inverso como a seguir. (Consideremos m sempre inteiro).

- Se $x = 0$ então $\lceil x \rfloor = 0, \quad w(x) = 1.$
- Se $0 < m \leq x \leq m + \frac{1}{2}$ então $\lceil x \rfloor = m, \quad w(x) = m + 1.$
- Se $0 < m + \frac{1}{2} < x < m + 1$ então $\lceil x \rfloor = m + 1, \quad w(x) = m.$
- Se $-m - \frac{1}{2} \leq x \leq -m < 0$ então $\lceil x \rfloor = -m, \quad w(x) = -m - 1.$
- Se $-m - 1 < x < -m - \frac{1}{2}$ então $\lceil x \rfloor = -m - 1, \quad w(x) = -m.$

Observação 4.1 *Os empates são controlados afim de dar preferência aos pontos de norma menor.*

Também podemos escrever

$$x = \lceil x \rfloor + \delta(x),$$

para que $|\delta(x)| \leq \frac{1}{2}$ seja a distância de x até o inteiro mais próximo.

Dado $x = (x_1, ..., x_n) \in \mathbb{R}^n$, seja $k (1 \leq k \leq n)$ tal que

$$|\delta(x_k)| \leq |\delta(x_i)|$$

para todo $1 \leq i \leq n$ e

$$|\delta(x_k)| = |\delta(x_i)| \Longrightarrow k \leq i.$$

Então $g(x)$ é definida por

$$g(x) = \left(\lceil x_1 \rfloor, \lceil x_2 \rfloor, ..., w(x_k), ..., \lceil x_n \rfloor\right).$$

4.2 O problema do vetor mais próximo nos reticulados $\mathbb{Z}^n$.

Dado $x \in \mathbb{R}^n$, o ponto mais próximo de $\mathbb{Z}^n$ é $\lceil x \rfloor$. (Se x está equidistante de dois ou mais pontos de $\mathbb{Z}^n$, este procedimento encontra um ponto de norma menor).

Para verificar se este procedimento funciona, seja $u = (u_1, ..., u_n)$ qualquer ponto de $\mathbb{Z}^n$.

Então

$$||(u - x)|| = \sum_{i=1}^{n} (u_i - x_i)^2$$

que é minimizado escolhendo-se $u_i = \lceil x_i \rfloor$ para $i = 1, ..., n$. Por causa de $0 < m + \frac{1}{2} < x < m + 1$ então $\lceil x \rfloor = m + 1$, logo $w(x) = m$ os empates são partidos corretamente, favorecendo o ponto de menor norma.

Como exemplo, vamos encontrar um ponto mais próximo para $\mathbb{Z}^2$.

Exemplo 4.1 *Encontre o ponto mais próximo de* $\mathbb{Z}^2$ *até* $x = (1.7, 4.7)$.

Iniciemos analizando a figura 4.1:

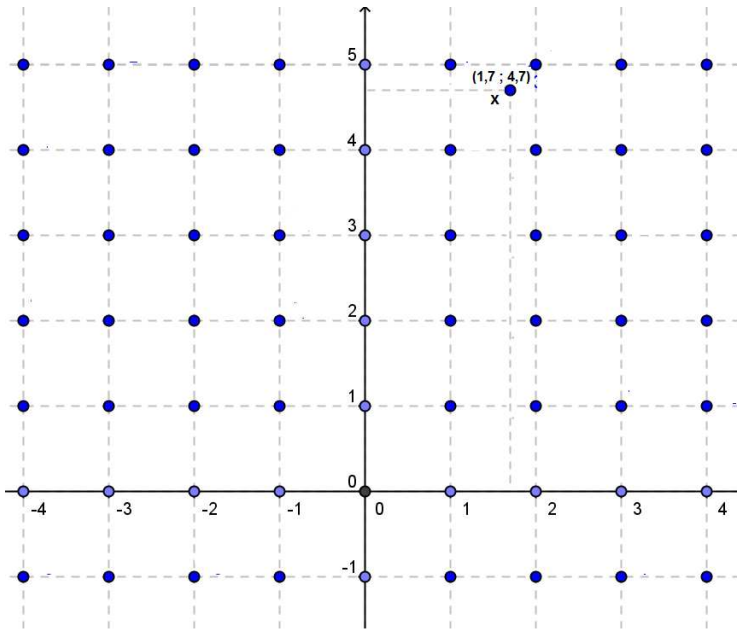


Figura 4.1: *1° Passo*: Ponto aleatório $x = (1.7; 4.7) \in \mathbb{Z}^2$

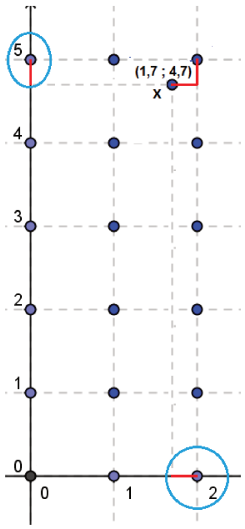


Figura 4.2: *2° Passo:* $\lceil (1.7; 4.7) \rfloor = (2, 5)$

Arrendondando a abscissa e a ordenada para os valores inteiros mais próximos de x*, temos que,* $\lceil (1.7; 4.7) \rfloor = (2, 5)$*. Ver figura 4.2.*

Logo $u = (2, 5) \in \Lambda = \mathbb{Z}^2$ *é o vetor de menor norma mais próximo de* x*.*

Recorrendo ao software *scilab*, podemos implementar um algoritmo simples que forneça a aproximação para o vetor mais próximo do reticulado gerado por qualquer vetor x.

O algoritmo denominado *decZ2* está assim definido na figura 4.3:

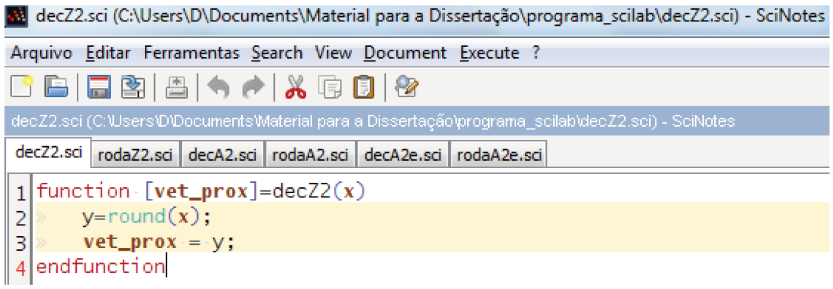


Figura 4.3: Algoritmo para decodificação em $\mathbb{Z}^2$

Neste simples algoritmo, a variável x é arredondada para os valores inteiros mais próximos através da função $y = round(x)$ sendo dado em seguida o vetor mais próximo *vet_prox*.

Na figura 4.4 mostramos o funcionamento do algoritmo para três vetores distintos, dentre eles o vetor do exemplo 4.1.

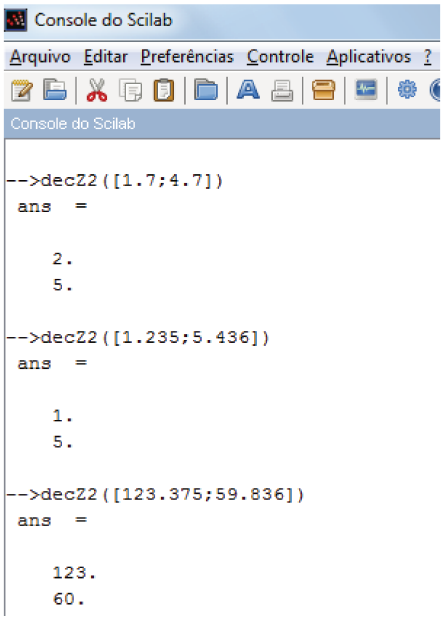


Figura 4.4: Decodificação em $\mathbb{Z}^2$ de três vetores distintos.

Utilizando esta implementação, investigamos o *"tempo de decodificação"* no $\mathbb{Z}^n$, para isso, também foi criado um algoritmo denominado *rodaZ2* que simplesmente chama o algoritmo *decZ2*, um número fixado de vezes para que se possa computar o tempo médio.

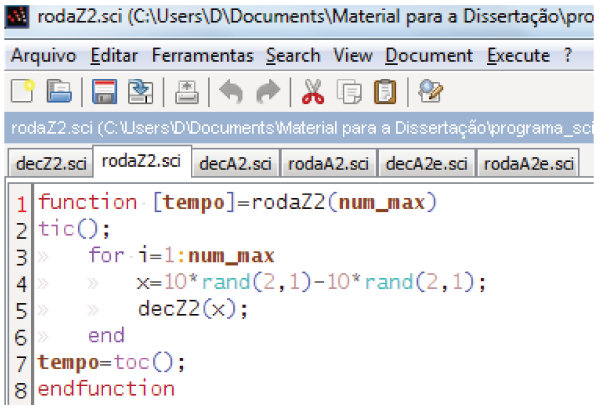


Figura 4.5: Algoritmo *rodaZ2* que analisa o tempo de decodificação.

O programa da figura 4.5 tem a variável de entrada num_max onde é computado o tempo para fazer num_max decodificações do $\mathbb{Z}^n$ para tirar uma média. Na tabela abaixo temos o tempo para a decodificação de 100, 1.000, 10.000 , 50.000 e 100.000.

Tempo de decodificação	
Numero de decodificações	Tempo
100	0
1000	0.016
10000	0.093
50000	0.406
100000	0.796

Tabela 4.1: Tabela para o tempo de decodificação

4.3 O problema do vetor mais próximo nos reticulados $\mathbb{A}_n$.

Antes de trabalharmos com algoritmos para $\mathbb{A}_n$, vamos tentar encontrar o vetor mais próximo no reticulado hexagonal $\mathbb{A}_2$ pelo método utilizado em $\mathbb{Z}^2$ e mostrar que este método falha.Na figura 4.6 observamos o reticulado hexagonal $\mathbb{A}_2$ gerado pela base $\left\{(1,0)\,;\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)\right\}$. Assim sendo, vamos pegar o ponto recebido x, localizar em 4.6 e procurar arrendondar as coordenadas para os inteiros mais próximos.

Como exemplo, vamos tomar o vetor $x = (2.1, 2.2)$.

Resolvendo o sistema $A \cdot z = x$, onde $A = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}$, temos $z = (0.83, 2.54)$. Arredondando as coordenadas de z, temos $\lfloor z \rceil = (1, 3)$, o que indicaria que o ponto de $\mathbb{A}_2$ mais próximo de x é o ponto $y = A\lceil z \rfloor = (2.5, 2.598)$, de onde temos que $||x - y|| = 0.5643$.

No entanto, se tomarmos $k = (2, 1.73) \in \mathbb{A}_2$ temos $||x - k|| = 0.478$ e portanto, o ponto mais próximo de x é $k = \left(2, \sqrt{3}\right)$ e não $y = \left(2.5, \frac{3\sqrt{3}}{2}\right)$.

Assim, concluímos que o algoritmo do $\mathbb{Z}^2$ não serve para o $\mathbb{A}_2$, e que na verdade cada reticulado possui um algoritmo próprio de decodificação.

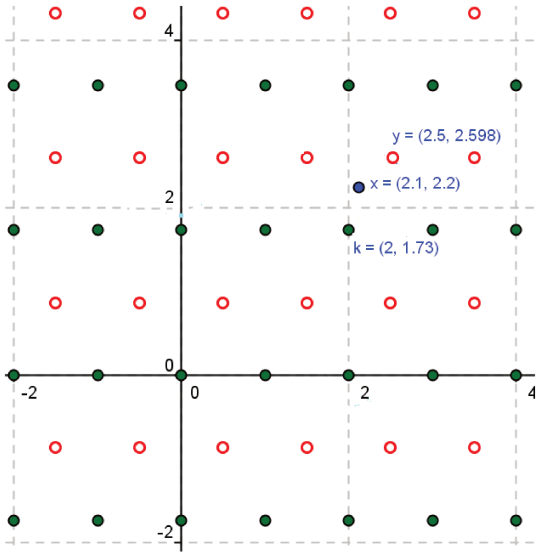


Figura 4.6: O ponto $y = (2.5, 2.598)$ não é o ponto mais próximo de x.

Em se tratando da decodificação em $\mathbb{A}_n$ iremos trabalhar na próxima seção com duas formas de algoritmo para decoficação, no primeiro algoritmo, mostraremos uma decodificação em $\mathbb{A}_n$ por classes laterais e no segundo tomaremos um ponto $x \in \mathbb{R}^{n+1}$ e iremos decodificá-lo no plano de coordenadas inteiras de soma igual a zero, ou seja, no $\mathbb{A}_n$

Decodificando por Classes Laterais

Suponha que $\mathcal{L}$ seja um reticulado (ou de fato qualquer conjunto de pontos) que é a união das classes laterais de Λ:

$$\mathcal{L} = \bigcup_{i=0}^{t-1} (r_i + \Lambda) .$$

Se tivermos um algoritmo eficiente para decodificar em cada uma das classes laterais de Λ, podemos resolver o problema do vetor mais próximo neste reticulado resolvendo sub-problemas em cada classe lateral e considerando o vetor mais próximo dentre os candidatos obtidos.

Exemplo 4.2 *Vamos encontrar o ponto de* $\mathbb{A}_2$ *mais próximo de* $x = (1.7, 2.3)$.

Analisando o gráfico 4.7, percebemos que o reticulado hexagonal é a união de um subreticulado retangular Γ e um transladado denominado classe lateral $\mathcal{C}$.

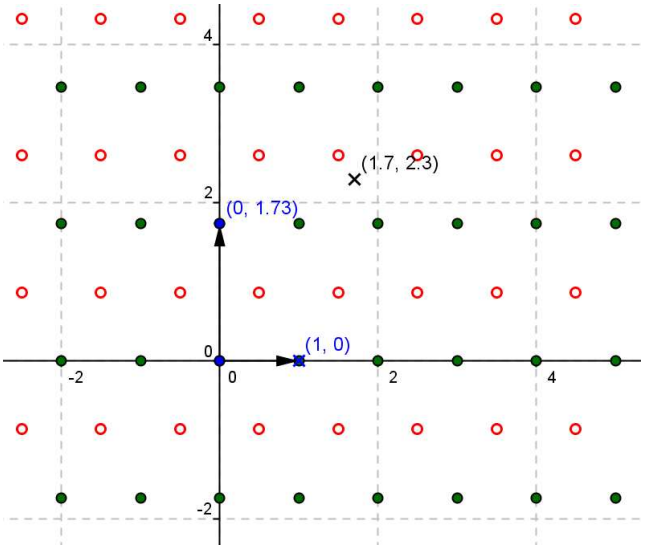


Figura 4.7: Reticulado hexagonal $\mathbb{A}_2$.

Na figura:

- *O subreticulado $\Gamma \subset \mathbb{A}_2$ é gerado pelos vetores $\langle (1,0), (0,\sqrt{3}) \rangle$.*
- *$\mathcal{C}$ é a classe lateral $\Gamma + r$, com $\mathcal{C} \subset \mathbb{A}_2$ e $r = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.*

Observe que a decodificação em Γ pode ser feita por arredondamento na base, já que o mesmo é ortogonal.

Assim sendo, devemos resolver o sistema

$$(1,0) \cdot a + (0,\sqrt{3}) \cdot b = (1.7, 2.3)$$

de onde obtemos

$$a = 1.7 \quad e \quad b = 1.32$$

cujo arredondamento é igual a $\lceil a \rfloor = 2 \quad e \quad \lceil b \rfloor = 1$.

Multiplicando o resultado obtido pela base teremos

$$(1,0) \cdot 2 + (0,\sqrt{3}) \cdot 1 = (2,\sqrt{3})$$

Com isso, concluímos que $(2, \sqrt{3})$ *é o primeiro candidato a vetor mais próximo de* $(1.7, 2.3)$*, vamos chamá-lo de* y_1*.*

Para a classe lateral $\mathcal{C} = \Gamma + r, com\ r = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ *usamos a expressão,*

$$y_2 = \phi + r$$

onde y_2 *é um segundo canditado.*

Inicialmente vamos calcular ϕ*, de onde temos* $x = (1.7, 2.3)$ *e* $r = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = (0.5, 0.867)$*.*

- *façamos* $x - r = (1.7, 2.3) - (0.5, 0.867) = (1.2, 1.43)$
- *resolvemos o sistema*

$$(1, 0) \cdot a + (0, \sqrt{3}) \cdot b = (1.2, 1.43)$$

de onde obtemos

$$a = 1.2 \quad e \quad b = 0.85$$

cujo arredondamento é igual a

$$\lceil a \rfloor = 1 \quad e \quad \lceil b \rfloor = 1$$

Multiplicando o resultado obtido pela base teremos

$$(1, 0) \cdot 1 + (0, \sqrt{3}) \cdot 1 = (1, \sqrt{3})$$

- *Assim, temos que* $\phi = (1, \sqrt{3})$

Agora devemos fazer

$$y_2 = \phi + r$$

$$y_2 = (1, \sqrt{3}) + \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$$

Logo nosso segundo candidado é

$$y_2 = \left(\frac{3}{2}, \frac{3\sqrt{3}}{2}\right)$$

Agora vamos fazer os cálculos das normas e verificar aquele que possui a menor distância.

$$||x - y_1|| = ||(1.7, 2.3) - (2, \sqrt{3})|| = 0.64$$

$$||x - y_2|| = ||(1.7, 2.3) - \left(\frac{3}{2}, \frac{3\sqrt{3}}{2}\right)|| = 0.35$$

Como o segundo cálculo possui menor norma, concluímos que $(\frac{3}{2}, \frac{3\sqrt{3}}{2}) = (1.5, 2.59)$ *é o vetor mais próximo de* $x = (1.7, 2.3)$.

Na figura 4.8, apresentamos uma implementação do algoritmo no software livre *scilab* para a decodificação de $\mathbb{A}_2$.

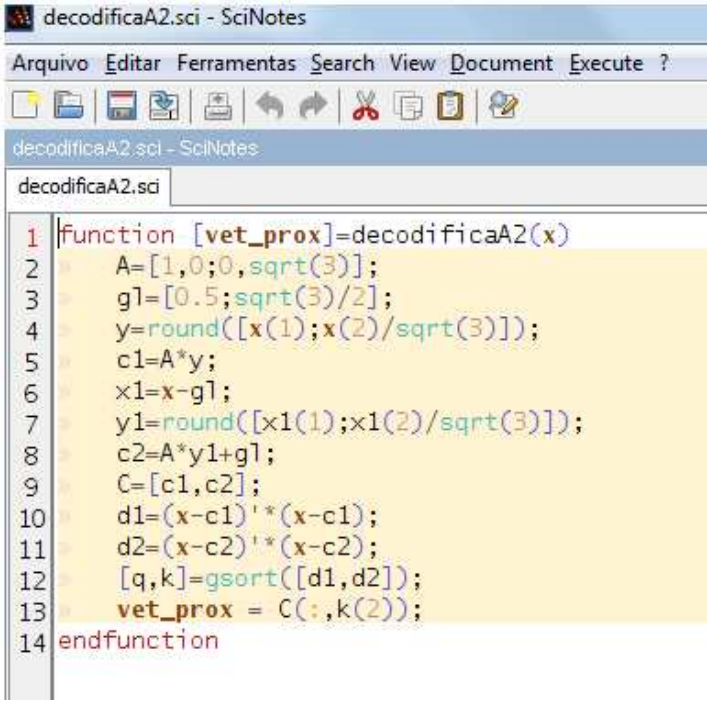


Figura 4.8: Algoritmo para decodificação em classes laterais de $\mathbb{A}_2$

Na figura 4.9 mostramos o funcionamento do algoritmo para dois vetores distintos, dentre eles o vetor do exemplo 4.2.

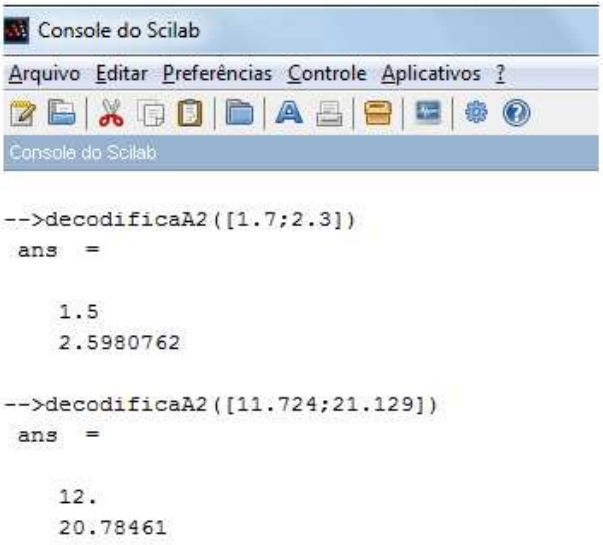


Figura 4.9: Decodificação em $\mathbb{A}_2$ de dois vetores distintos.

Assim como em $\mathbb{Z}^2$ o fator "tempo de decodificação"no $\mathbb{A}_2$ foi estudado, para isso, também foi criado um algoritmo denominado *rodadecodificaA2*. Este algoritmo pode ser visto na figura 4.10.

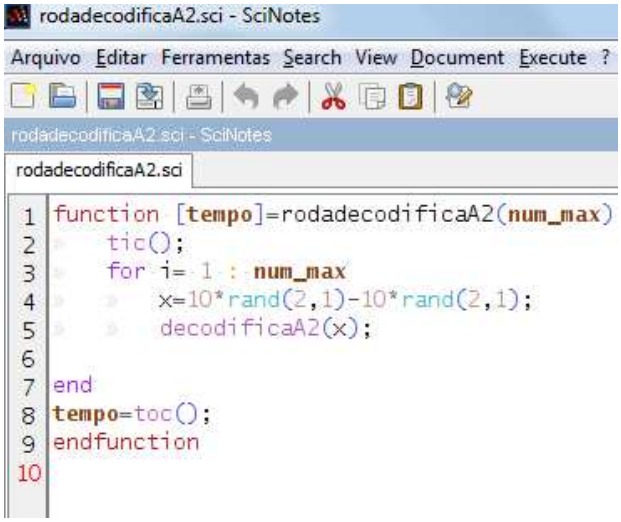


Figura 4.10: Algoritmo *rodadecodificaA2* que analisa o tempo de decodificação.

Este algoritmo tem a variável de entrada *num_max* onde é computado o tempo para fazer *num_max* decodificações do $\mathbb{A}_2$ para tirar uma média. Na tabela 4.2, fazemos uma

análise da eficiência do algoritmo no que diz respeito ao ***número de decodificações*** em um certo ***tempo***.

Número de decodificações	Tempo
100	0.16
1.000	0.062
2.000	0.109
3.000	0.171
4.000	0.172
5.000	0.234
6.000	0.25
7.000	0.328
8.000	0.359
9.000	0.374
10.000	0.406
50.000	1.981
100.000	4.009
500.000	19.75
1000.000	39.499

Tabela 4.2: Tempo para decodificação de 100 a 1000.000

Decodificação pelo algoritmo que joga um ponto do $\mathbb{R}^{n+1}$ no plano de soma zero.

O algoritmo foi obtido de *Conway, J. H. e Sloane*[4] (cap.20). Durante a sua construção é importante o seguimento de alguns passos. Veja:

Passo 1: Dado $x \in \mathbb{R}^{n+1}$, calcule $s = \sum x_i$ e substitua x por

$$x' = x - \frac{s}{n+1}(1, 1, ..., 1).$$

Observação 4.2 *O **passo 1** projeta x em um ponto x' dentro do hiperplano $\sum x_i = 0$ contendo $\mathbb{A}_n$. Então $\lceil x' \rfloor$ é o ponto mais próximo de $\mathbb{Z}^{n+1}$ até x'.*

Passo 2: Calcule $\lceil x' \rfloor = (\lceil x'_0 \rfloor, ..., \lceil x'_n \rfloor)$ e o discriminante $\Delta \sum \lceil x'_i \rfloor$.

Passo 3: Selecione x'_1 numa ordem de valores ascendente de $\delta(x'_i)$ (definido no passo 2). Obtemos uma reorganização dos números $0, 1, 2, 3, ..., n$, onde $i_0, i_1, ..., i_n$, tal que

$$-\frac{1}{2} \leq \delta(x'_{i_0}) \leq ... \leq \delta(x'_{i_n}) \leq \frac{1}{2}.$$

Passo 4:

- Se $\Delta = 0, \lceil x' \rfloor$ é o ponto mais próximo de $\mathbb{A}_n$ até x.
- Se $\Delta > 0$, o ponto mais próximo é obtido subtraindo 1 das coordenadas

$$\left\lceil x'_{i_0} \right\rfloor, ..., \left\lceil x'_{i_{\Delta-1}} \right\rfloor.$$

- Se $\Delta < 0$, o ponto mais próximo é obtido adicionando 1 das coordenadas

$$\left\lceil x'_{i_n} \right\rfloor, \left\lceil x'_{i_{n-1}} \right\rfloor, ..., \left\lceil x'_{i_{n-\Delta+1}} \right\rfloor.$$

Observação 4.3 *Os **passos 3 e 4** fazem as mudanças menores necessárias à norma de $\lceil x' \rfloor$ afim de que $\sum \lceil x'_i \rfloor$ diminua.*

Vamos ver a implementação no software livre *scilab* para a decodificação de $\mathbb{A}_2$ na figura 4.11.

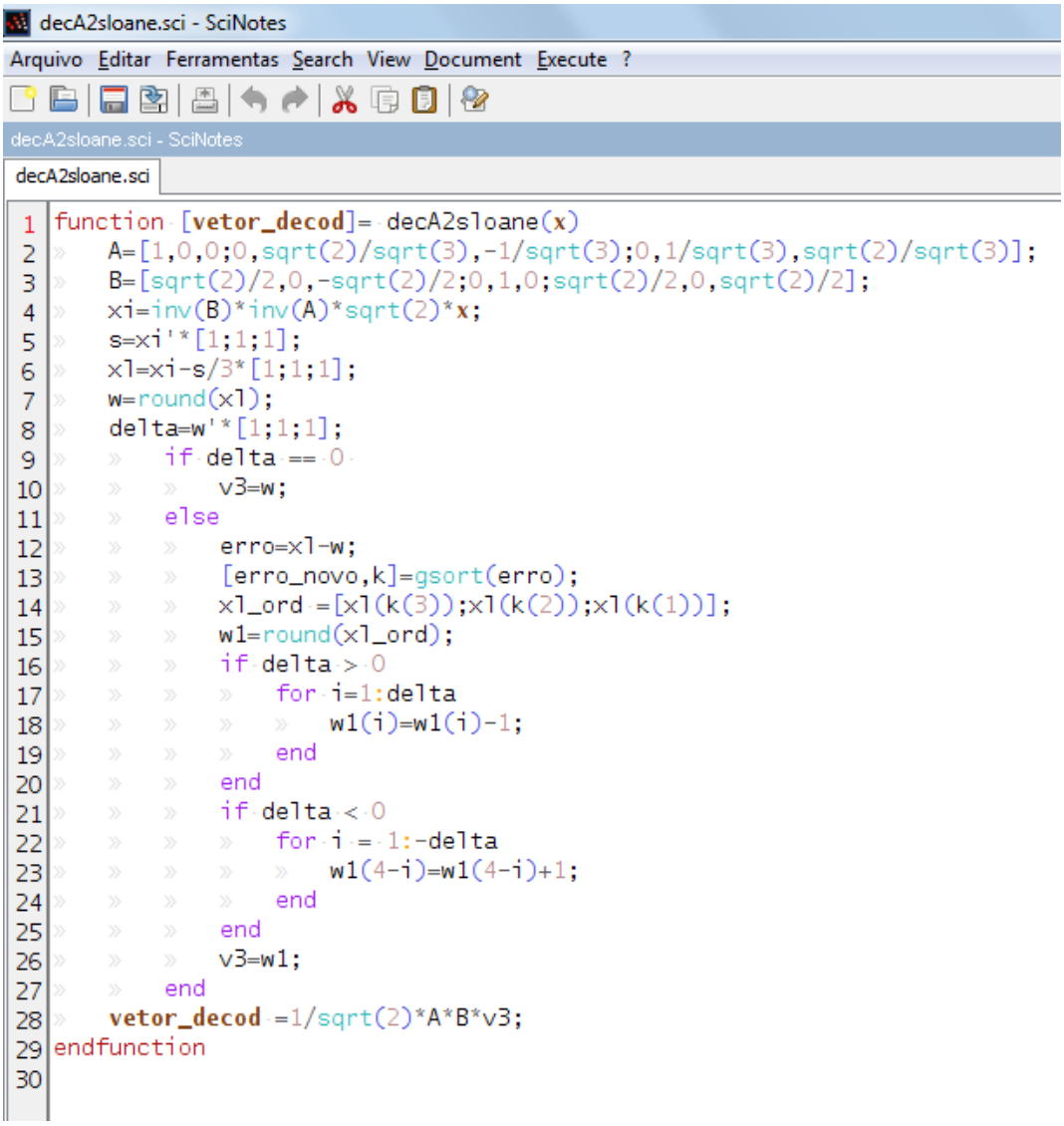


Figura 4.11: Algoritmo para encontrar o vetor mais próximo de $\mathbb{A}_2$

Vamos observar o funcionamento deste algoritmo para dois vetores distintos.

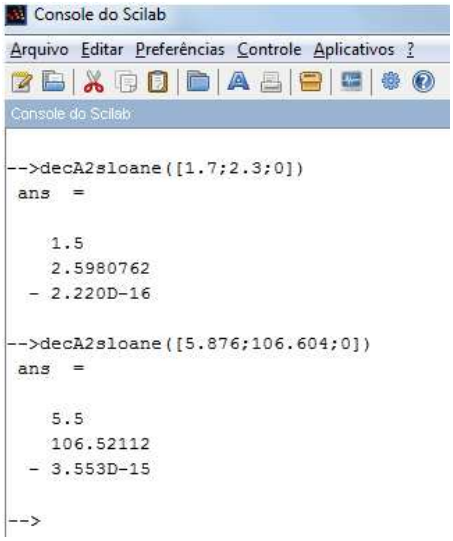


Figura 4.12: Decodificação em $\mathbb{A}_2$ de dois vetores distintos

Assim como nos anteriores, para este algoritmo também foi criado um outro algoritmo que analisa o fator "tempo de decodificação". Este algoritmo foi denominado *rodaA2sloane* e pode ser visto na figura 4.13.

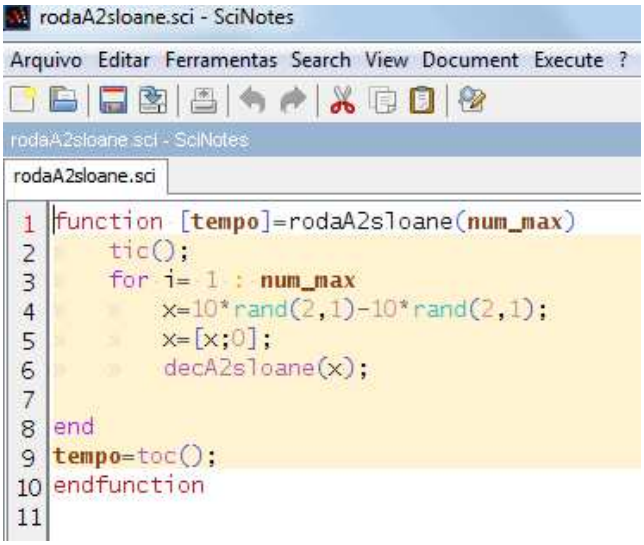


Figura 4.13: Algoritmo *rodaA2sloane* que analisa o tempo de decodificação.

Observe a tabela 4.3 que analisa o ***número de decodificações*** em um certo ***tempo***.

Número de decodificações	Tempo
100	0.031
1.000	0.109
2.000	0.171
3.000	0.265
4.000	0.343
5.000	0.39
6.000	0.483
7.000	0.561
8.000	0.64
9.000	0.702
10.000	0.811
50.000	3.885
100.000	7.753
500.000	38.985
1000.000	78.234

Tabela 4.3: Tempo para decodificação de 100 a 1000.000

Assim, concluímos que para n = 2 temos $\mathbb{A}_2$ é melhor decodificado usando a decodificação por classes laterais.

Generalização do algoritmo que joga um ponto do $\mathbb{R}^{n+1}$ no plano de soma zero.

Na figura 4.14 mostramos, utilizando o software scilab, um algoritmo generalizado que encontra o ponto mais próximo de $\mathbb{A}_n$ a um ponto dado x.

Na figura 4.15 mostramos o funcionamento do algoritmo para quatro vetores distintos de dimensões distintas.

Figura 4.14: Algoritmo para a decodificação de $\mathbb{A}_n$

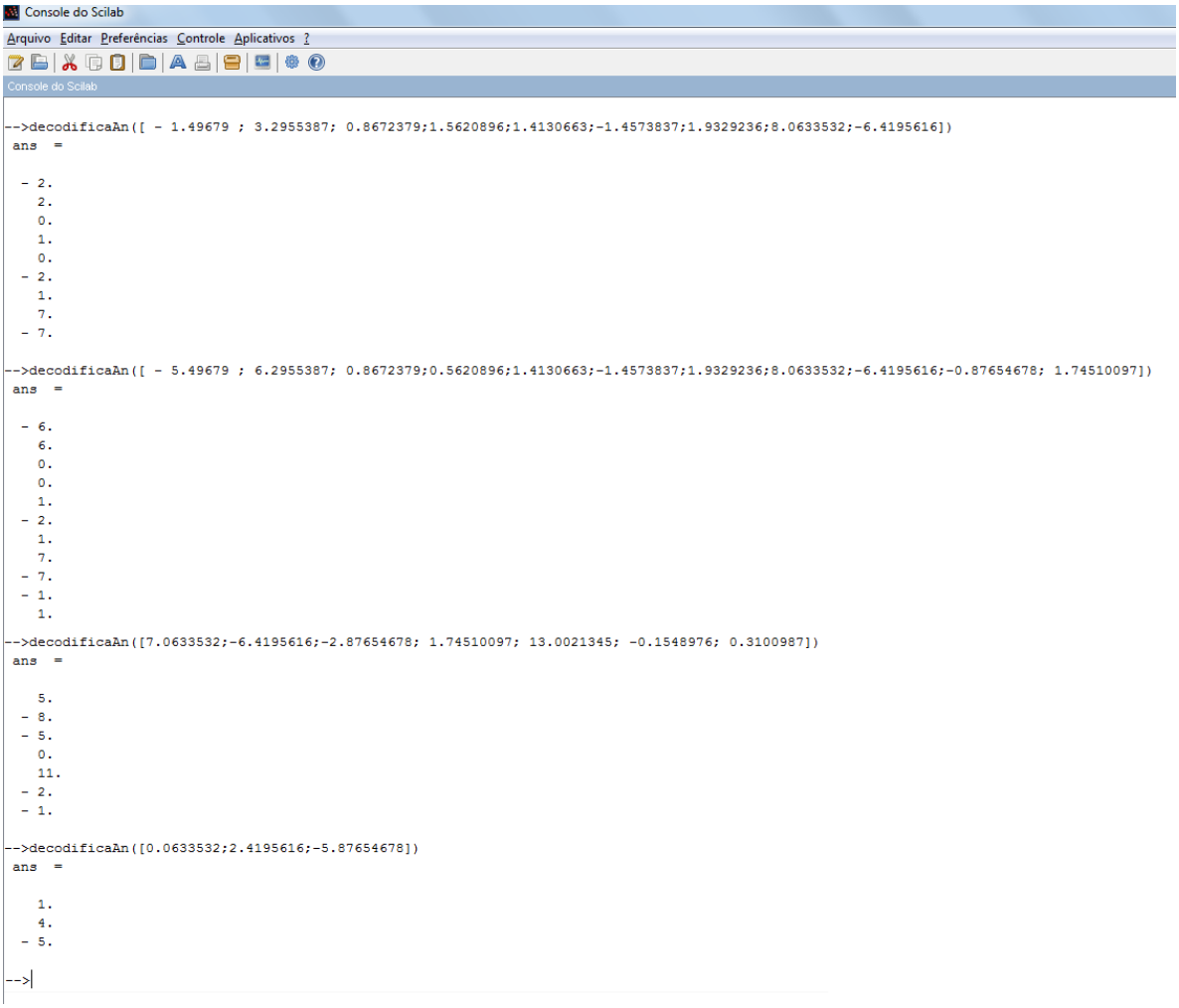


Figura 4.15: Decodificação em $\mathbb{A}_n$ para quatro vetores distintos de dimensões distintas.

Na figura 4.16 é mostrado o algoritmo responsável pelo fator "tempo de decodificação".

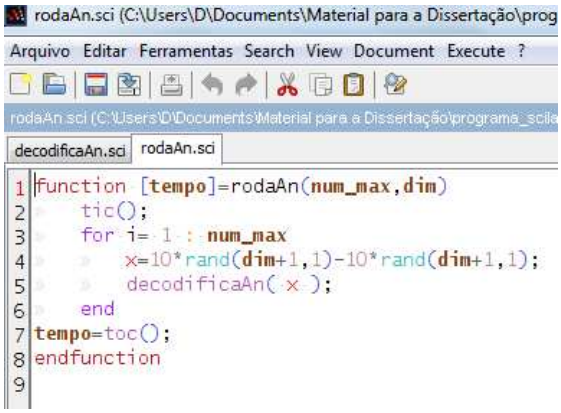


Figura 4.16: Algoritmo *rodaAn* que analisa o tempo de decodificação.

Este algoritmo tem a variável de entrada *num_max* onde é computado o tempo para fazer *num_max* decodificações do $\mathbb{A}_n$ seguida da variável *dim* que representa a dimensão em que está ocorrendo a decodificação.

Na tabela 4.4, fazemos a análise do ***número de decodificações*** em relação ao ***tempo*** tomando como exemplo a dimensão 10.

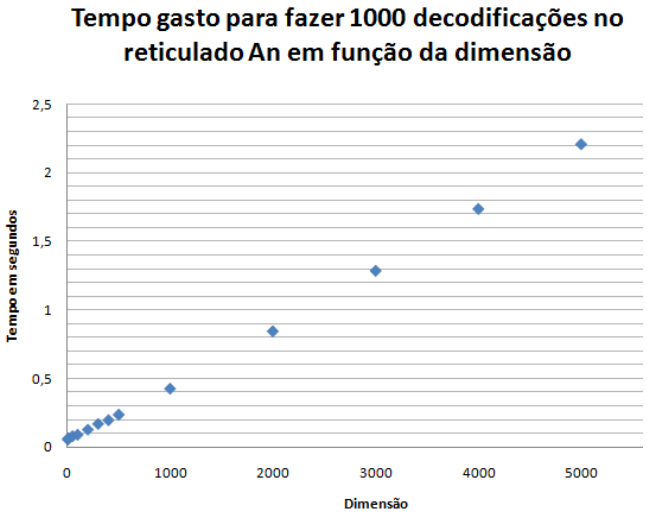
Número de decodificações	Dimensão	Tempo
100	10	0.11
1.000	10	0.056
2.000	10	0.097
3.000	10	0.147
4.000	10	0.185
5.000	10	0.236
6.000	10	0.28
7.000	10	0.324
8.000	10	0.37
9.000	10	0.41
10.000	10	0.46
50.000	10	2.238
100.000	10	4.436
500.000	10	22.298
1000.000	10	44.642

Tabela 4.4: Tempo para decodificação de 100 a 1000.000

Agora vamos investigar como o tempo de decodificacão cresce, quando a dimensão aumenta no reticulado $\mathbb{A}_n$. A tabela 4.5 mostra o comportamento do tempo de 1000 decodificações em dimensões distintas.

Número de decodificações	Dimensão	Tempo
1.000	5	0.055
1.000	10	0.064
1.000	50	0.079
1.000	100	0.09
1.000	200	0.127
1.000	300	0.169
1.000	400	0.196
1.000	500	0.236
1.000	1.000	0.425
1.000	2.000	0.843
1.000	3.000	1.283
1.000	4.000	1.733
1.000	5.000	2.204

Tabela 4.5: Tempo para fazer 1000 decodificações nas dimensões: 5, 10, 50, 100, 200, 300, 400, 500, 1000, 2000, 3000, 4000 e 5000



4.4 O problema do vetor mais próximo nos reticulados $\mathbb{D}_n$.

Dado $x \in \mathbb{R}^n$, o ponto mais próximo de $\mathbb{D}_n$ é qualquer uma das funções f(x) e g(x) que possua soma de coordendas par (uma terá soma ímpar e a outra soma par). Se x é equidistante de dois ou mais pontos de $\mathbb{D}_n$ esse procedimento produz um ponto mais próximo que possui norma menor.

Este procedimento funciona porque $f(x)$ é o ponto mais próximo de $\mathbb{Z}^n$ até x e $g(x)$ é o segundo ponto mais próximo. $f(x)$ e $g(x)$ diferem por *uma e exatamente uma coordenada*, e então, exatamente $\sum f(x_i)$ e $\sum g(x_i)$ é impar e a outra par.

Exemplo 4.3 *Encontre o ponto mais próximo de $\mathbb{D}_4$ até*

$$x = (0.6, -1.1, 1.7, 0.1)\,.$$

Calculamos $f(x) = (1, -1, 2, 0)$ e $g(x) = (0, -1, 2, 0)$, desde que a primeira coordenada de x seja a mais distante de um inteiro. A soma das coordenadas de $f(x)$ é $1 - 1 + 2 + 0 = 0$ que é par, enquanto que a de $g(x)$ é $0 - 1 + 2 + 0 = 1$, que é ímpar. Portanto, $f(x)$ é o ponto de $\mathbb{D}_4$ mais próximo de x. Para ilustrar como os empates são calculados, suponha

$$x = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right).$$

De fato x está agora equidistante de oito pontos de $\mathbb{D}_4$, isto é $(0, 0, 0, 0)$, qualquer permutação de $(1, 1, 0, 0)$, e $(1, 1, 1, 1)$. O algoritmo calcula

$$f(x) = (0, 0, 0, 0)\,, \quad soma = 0, \quad par,$$

$$g(x) = (1, 0, 0, 0)\,, \quad soma = 1, \quad ímpar,$$

e seleciona $f(x)$. Realmente, $f(x)$ possui a menor norma dos oito pontos vizinhos. O algoritmo consome em torno de $4n$ passos para decodificar $\mathbb{D}_n$ [4].

Vamos ver a implementação do algoritmo utilizando o software livre scilab para a decodicação de $\mathbb{D}_n$ na figura 4.17.

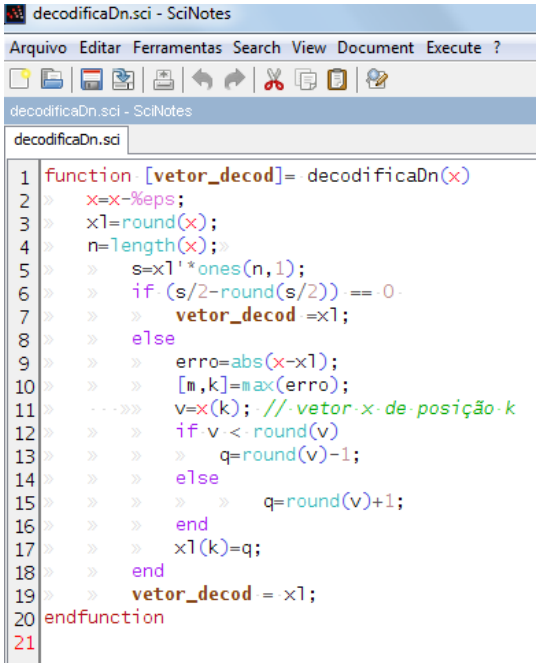


Figura 4.17: Algoritmo para decodificação em $\mathbb{D}_n$

O fator "tempo de decodificação"é calculado por meio do algoritmo denominado *rodaDn* da figura 4.18.

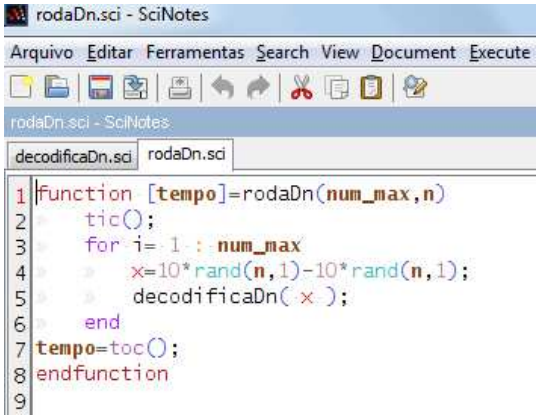


Figura 4.18: Algoritmo *rodaDn* que analisa o tempo de cada decodificação.

Na figura 4.19 mostramos o funcionamento do algoritmo para três vetores distintos de dimensões distintas.

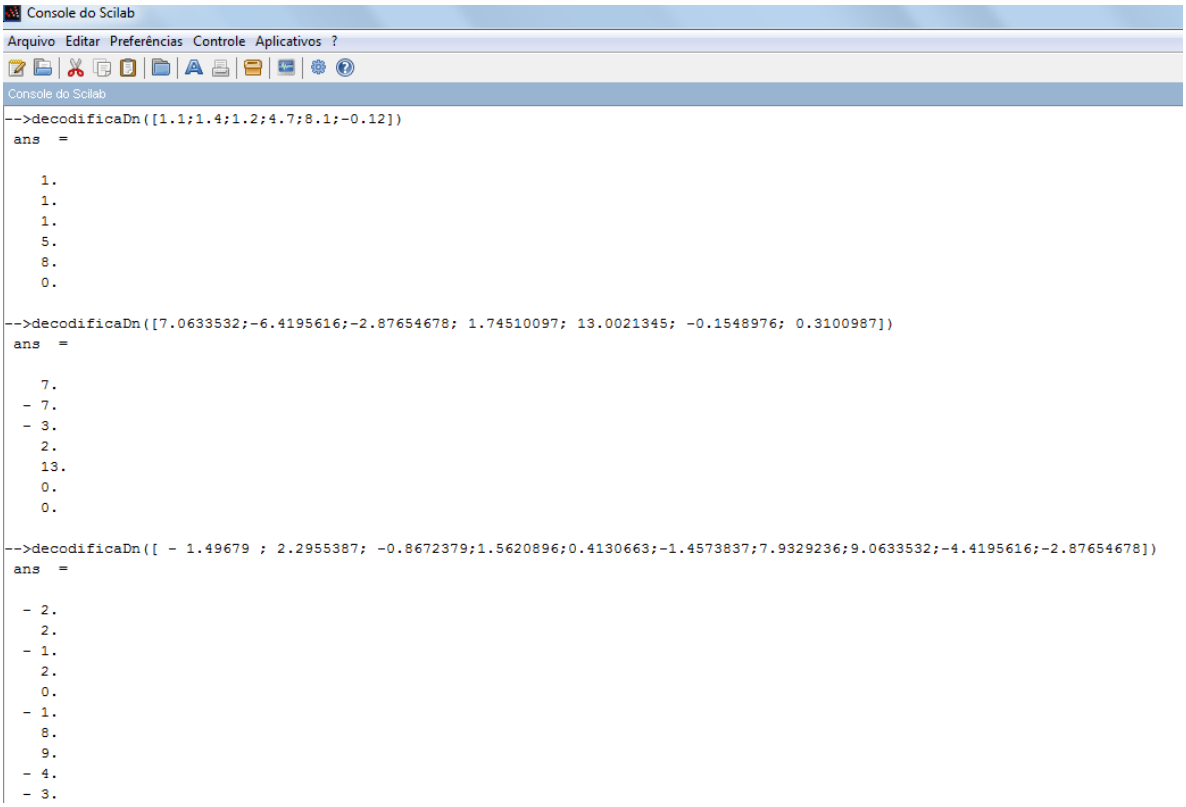


Figura 4.19: Decodificação em $\mathbb{D}_n$ para três vetores distintos de dimensões distintas.

Quando n = 2 ou 3, $\mathbb{D}_2$ é semelhante ao $\mathbb{Z}^2$, e $\mathbb{D}_3$ é isométrico a $\mathbb{A}_3$, onde neste último caso a melhor decodificação acontece pelo algoritmo $\mathbb{D}_3$. Nas tabelas seguintes, faremos uma comparação entre o tempo de decodificação entre estes reticulados.

A tabela 4.6 compara os algoritmos correspondentes a $\mathbb{Z}^2$ e $\mathbb{D}_2$.

Número de decodificações ($\mathbb{Z}^2$)	Tempo	Número de decodificações ($\mathbb{D}_2$)	Tempo
100	0	100	0.01
1000	0.016	1000	0.056
10000	0.093	10000	0.325
50000	0.406	50000	1.529
100000	0.796	100000	3.062

Tabela 4.6: Tabela para o tempo de decodificação

Observando a tabela 4.6, podemos concluir que o algoritmo de decodificação para $\mathbb{Z}^2$ é mais eficiente do que o algoritmo de decodificação para $\mathbb{D}_2$.

Agora vamos observar a tabela 4.7 que compara os algoritmos isométricos $\mathbb{A}_3$ e $\mathbb{D}_3$.

Número de decodificações ($\mathbb{A}_3$)	Tempo	Número de decodificações ($\mathbb{D}_3$)	Tempo
100	0.008	100	0.01
1000	0.055	1000	0.038
10000	0.403	10000	0.312
50000	1.903	50000	1.514
100000	3.904	100000	3.071

Tabela 4.7: Tabela para o tempo de decodificação

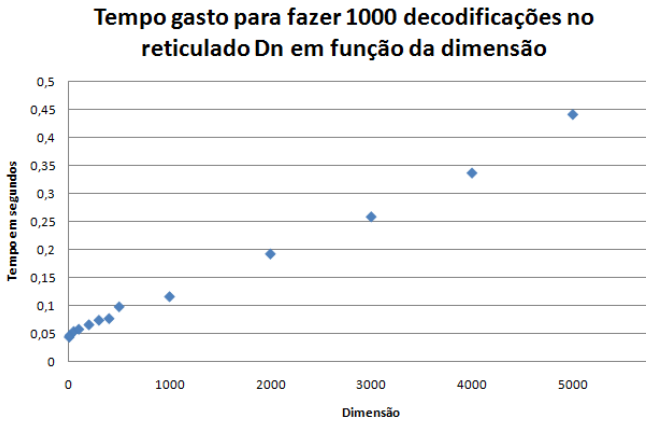
Conforme citado antes, se analisarmos a tabela 4.7 a melhor decodificação acontece pelo algoritmo $\mathbb{D}_3$.

Um objetivo importante a ser estudado é a análise do que acontece quando a dimensão do reticulado aumenta. As próximas tabelas e gráficos nos darão uma comparação entre os reticulados $\mathbb{A}_n$ e $\mathbb{D}_n$.

Iniciemos pela tabela 4.8 que mostra 1000 decodificações em $\mathbb{D}_n$ de dimensões distintas.

Número de decodificações	Dimensão	Tempo
1.000	5	0.044
1.000	10	0.047
1.000	50	0.054
1.000	100	0.058
1.000	200	0.066
1.000	300	0.074
1.000	400	0.077
1.000	500	0.098
1.000	1.000	0.116
1.000	2.000	0.192
1.000	3.000	0.258
1.000	4.000	0.336
1.000	5.000	0.44

Tabela 4.8: Tempo para fazer 1000 decodificações nas dimensões: 5, 10, 50, 100, 200, 300, 400, 500, 1000, 2000, 3000, 4000 e 5000



Com base no comportamento dos gráficos, concluímos que é linear o crescimento do tempo de decodificacão quando a dimensão aumenta em ambos os reticulados $\mathbb{A}_n$ e $\mathbb{D}_n$.

Considerações finais e perspectivas futuras

Como direções alternativas para um prosseguimento deste trabalho, podemos sugerir algumas extensões e aplicações dos resultados como se segue:

- a construção de algoritmos para o outros reticulados raízes não citados neste trabalho, como a família $\mathbb{E}_n$ e o reticulado de Leech.
- a possibilidade para apresentar uma possível (e importante) aplicação para o problema da decodificação em reticulados que diz respeito aos recentes progressos em criptografia, sobretudo alguns criptossistemas baseados em reticulados. Existe a possibilidade de explicar de modo geral o que é a criptografia pós-quântica, isto é, a criptografia segura perante Computadores Quânticos e apresentar as ideias principais de como os reticulados podem ser utilizados para geração de criptossistemas resistentes a um ataque de computador quântico.
- estudar outras aplicações de algoritmos eficientes para decodificação em reticulados, como por exemplo, na transmissão de sinais em telecomunicações.

Referências Bibliográficas

[1] Alves, C. *Reticulados e Códigos*. PhD thesis, Universidade Estadual de Campinas, 2008.

[2] Coelho, F. D. M. O algoritmo lll e aplicações. Master's thesis, Universidade de Coimbra - Portugal, 2008.

[3] Conway, J. H. *The sensual quadratic form*. The Mathematical Association of America, 1997.

[4] Conway, J. H., and Sloane, N. J. A. *Sphere packings, lattices and groups*, third ed., vol. 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[5] Costa, F. S. Áreas e contornos. Master's thesis, Universidade Estadual de Campinas, 2008.

[6] Daniel J. Bernstein ·Johannes Buchmann, E. D. E. *Post-Quantum Cryptography*. 2008.

[7] Fedorov, E. S. *Elements of the study of figures.* Zap. Mineralog, 1953.

[8] Galbraith, S. *Mathematics of Public Key Cryptography*. 0.8, 2009.

[9] Hales, T. C. Cannonballs and honeycombs. *Notices of the AMS - Number 4 47* (april 2000), 10.

[10] Hinek, J. M. *Cryptoanalysis of RSA and its variants*. 2009.

[11] Joux, A. *Algorithmc Cryptoanalysis.* Chapman & Hall/CRC Cryptography and Network Security, 2009.

[12] Kim, Y. On semistability of root lattices and perfect lattices. 19 pgs.

[13] Mark de Berg, Otfried Cheong Marc V. Kreveld, M. O. *Computational Geometry - Algorithms and Applications, 3rd Ed.* 2008.

[14] Martinet, J. *Perfect Lattices in Euclidean Spaces.* A série of Comprehensive Studies in Mathematics, 2003.

[15] Micciancio, D., and Goldwasser, S. *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.

[16] Naves, L. R. B. A densidade de empacotamentos esféricos em reticulados. Master's thesis, Universidade Estadual de Campinas, 2009.

[17] Oded Regev, I. H. Some basic complexity results,. *Lattices in Computer Science Lecture 5* (2004), 1 – 5.

[18] Peters, M. K. . J. Symmetric box-splines on root lattices. *Preprint submitted to Journal of Computational and Applied Mathematics 5* (2010), 2–6.

[19] Regev, O. Dual lattices. *Lattices in Computer Science Lecture 8* (2004), 1 – 5.

[20] Rosseti, J. P. Retículos en espacios euclídeos. In *Mathematics Subject Classification.* (1991).

[21] Samuel, P. *Algebraic theory of numbers.* Paris: Herman, 1970.

[22] Strapasson, J. E. *Geometria Discreta e Códigos.* PhD thesis, Universidade Estadual de Campinas, 2007.

[23] Sueli I.R. C, Carlile C. L, M. M. S. A. R. M. S. *Uma Introdução à Teoria de Códigos.* Notas em Matemática Aplicada, 2006.

[24] Torezzan, C. *Códigos esfericos em toros planares.* PhD thesis, Universidade Estadual de Campinas, 2009.

[25] Zong, C. *Sphere Packings.* Universitext, 1999.