UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

FABIANO PINTO TAVARES

Sobre Reticulados Rotacionados para Codificação em Sistemas de Transmissão

Campinas

2022

Fabiano Pinto Tavares

Sobre Reticulados Rotacionados para Codificação em Sistemas de Transmissão

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática Aplicada.

Orientador: João Eloir Strapasson

Coorientadora: Sueli Irene Rodrigues Costa

Este trabalho corresponde à versão final da Tese defendida pelo aluno Fabiano Pinto Tavares e orientada pelo Prof. Dr. João Eloir Strapasson.

Campinas

2022

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

T197s

Tavares, Fabiano Pinto, 1980-
Sobre reticulados rotacionados para codificação em sistemas de transmissão / Fabiano Pinto Tavares. – Campinas, SP : [s.n.], 2022.

Orientador: João Eloir Strapasson.
Coorientador: Sueli Irene Rodrigues Costa.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. I. Strapasson, João Eloir, 1979-. II. Costa, Sueli Irene Rodrigues. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: About lattices rotated to coding in transmission systems
Palavras-chave em inglês:
Lattice theory
Área de concentração: Matemática Aplicada
Titulação: Doutor em Matemática Aplicada
Banca examinadora:
João Eloir Strapasson [Orientador]
Antonio Aparecido de Andrade
Agnaldo José Ferrari
Giuliano Gadioli La Guardia
Grasiele Cristiane Jorge
Data de defesa: 23-02-2022
Programa de Pós-Graduação: Matemática Aplicada

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-4023-312X
- Currículo Lattes do autor: http://lattes.cnpq.br/7904117473302138

Tese de Doutorado defendida em 23 de fevereiro de 2022 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

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

Prof(a). Dr(a). AGNALDO JOSÉ FERRARI

Prof(a). Dr(a). GIULIANO GADIOLI LA GUARDIA

Prof(a). Dr(a). GRASIELE CRISTIANE JORGE

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Este trabalho é dedicado ao Pai, ao Filho e ao Espírito Santo. Deus único que subsiste em três pessoas. O arquétipo do uno e do múltiplo que os filósofos tanto investigaram.
Soli Deo Gloria.

Agradecimentos

Ao meu SENHOR e Salvador Jesus Cristo, autor e consumador da minha fé. Sem a sua misericórdia, graça e soberana ação, este trabalho não teria sido possível!

À minha amada esposa Marcela, pelo seu apoio incondicional e às minhas filhas Ester e Lídia, herança do SENHOR;

Aos meus pais Domingos e Maria, irmãos Kátia e Francisco, sogros Flora e Maurício e cunhados Martin, Leyla e Mônyka: bênçãos de Deus em minha vida e família;

Ao Instituto Federal de Educação, Ciência e Tecnologia do Maranhão e ao Departamento Acadêmico de Matemática por permitirem a realização deste trabalho através do afastamento a mim concedido e por "segurarem as pontas" ao desenvolverem os trabalhos acrescentados com o meu período de ausência;

Aos Orientadores João Strapasson e Sueli Costa. Eu apenas desenvolvi vossas ideias. Os créditos são mais vossos do que meu;

À Universidade Estadual de Campinas, ao Instituto de Matemática e à Pós-Graduação em Matemática Aplicada. Servidores e professores de excelência nessa instituição marcaram a minha vida. Viva a educação superior pública de qualidade!

À Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), pelo suporte ao grupo de pesquisa através do Projeto Temático 2013/25977-7 "Segurança e Confiabilidade da Informação: Teoria e Prática";

Aos componentes da banca, pelas sugestões para tese e para trabalhos futuros;

Às Igrejas Presbiterianas do Renascença, Barão Geraldo e em especial ao "pequeno grupo" dessa última. Obrigado por vossas orações;

Ao Fábio Alex e sua esposa Érica, grandes amigos de longa data;

Ao Reverendo Adenauer, mais que um pastor, um grande amigo;

Aos confrades Ademir, Cauê, Gigante, Hugo, Jhonilson e Lucas, grandes amigos são vocês;

Aos "mosqueteiros" Gesivaldo e Luiz Alves, à Juliana ao Samuel e ao Tacildo. Grandes amigos que o IMECC me presenteou, obrigado por tudo;

Ao André e sua esposa Débora. Grandes amigos que Campinas presenteou a mim e minha família;

Aos "Velhos Amigos do Sol e Mar": Anselmo, Erenaldo, Fábio, Gilmacy, Júnior e Ribamar Reis pela amizade em meio a distância. Quantas discussões políticas hein?

"Quando Deus criou o mundo,
também ordenou todas as características do mundo.
É ele quem especifica todas as verdades sobre o mundo,
incluindo as verdades da matemática."
(Vern S. Poythress)

Resumo

Neste trabalho, estudamos versões rotacionadas de reticulados com diversidade máxima, que possuem máximas distâncias produtos mínimas, pois, tais versões "ótimas" são úteis para codificação visando a transmissão em canais com desvanecimento do tipo Rayleigh. Efetuamos rotações de reticulados bidimensionais e tridimensionais a partir da álgebra dos complexos e da álgebra dos quatérnios. Encontramos versões "ótimas" rotacionadas do $\mathbb{Z}^2$, $\mathbb{Z}^3$, FCC e conectamos essas com as já conhecidas, obtidas via teoria algébrica dos números e assim foi possível descrever geometricamente tais reticulados algébricos. Em relação aos reticulados bidimensionais, estudamos também versões "ótimas" rotacionadas de uma família de reticulados bem arredondados, de uma família de reticulados construída via corpos quadráticos e de uma família de reticulados ortogonais. A partir da exponenciação de matrizes, construímos versões "próximas" de reticulados algébricos com dimensões superiores a 3, que possuem diversidade máxima e boas distâncias produtos. Definimos torção generalizada de um reticulado qualquer e verificamos que tal versão torcida preserva distância produto de reticulados com diversidade máxima. Encontramos versões torcidas de reticulados que possuem "boas" densidades, já que estas podem ser úteis simultaneamente a canais do tipo Rayleigh e a canais gaussianos.

Palavras-chave: Reticulados, diversidade máxima, distância produto, rotações por complexos e por quatérnios, torção generalizada.

Abstract

In this work we have studied rotated versions of lattices with maximum diversity which have maximum product distance. Such "optimal" versions are usefull for encoding in transmissions over Rayleigh fading channels. Two-dimensional and three-dimensional lattice rotations from the complex and quaternion algebras are considered and we have found "optimal" rotated versions of $\mathbb{Z}^2$, $\mathbb{Z}^3$, FCC connecting those with previously known obtained via algebraic theory of numbers in order to describe geometrically such algebraic lattices. Regarding two-dimensional lattices, we also have studied "optimal" rotated versions of a family of well-rounded lattices, a family of lattices constructed via quadratic fields and a family of orthogonal lattices. From matrix exponentiation "close" versions of algebraic lattices with dimensions greater then 3, which have maximum diversity and good product distances, have been built. We have defined generalized torsion of a lattice and verified that such twisted version preserves the product distance of lattices with maximum diversity. Twisted versions of lattices that have "good" densities have been derived since "good" densities have been derived since those can be useful simultaneously for Rayleigh and Gaussian channels.

Keywords: Lattices, maximum diversity, product distance, rotations by complex and quaternion numbers, generalized torsion

Lista de ilustrações

Lista de tabelas

Lista de símbolos

$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{H}$	Quatérnios de Hamilton
$\mathbb{R}^{m\times n}$	Conjunto das matrizes $m \times n$ reais
$B^n(\mathbf{a};\epsilon)$	Bola aberta de centro em $\mathbf{a}$ e raio ϵ
$\det(\Lambda)$	Determinante do reticulado Λ
$V(\Lambda)$	Volume do reticulado Λ
$\Delta(\Lambda)$	Densidade de empacotamento do reticulado Λ
$d_{p,\min}(\Lambda)$	Distância produto mínima do reticulado Λ
$d_{p,\mathrm{rel}}(\Lambda)$	Distância produto relativa do reticulado Λ
$d_{p,\mathrm{norm}}(\Lambda)$	Distância produto normalizada do reticulado Λ
$\mathcal{O}_{\mathbb{K}}$	Anel de inteiros do corpo $\mathbb{K}$
$d_{\mathbb{K}}$	discriminante do corpo $\mathbb{K}$
ζ_m	$m-$ésima raiz da unidade
$\mathrm{tor}_m(\Lambda)$	$m-$torção generalizada do reticulado bidimensional $\Lambda \subset \mathbb{R}^2$
$\mathrm{tor}_{(m_1,m_2,...,m_{n-1})}(\Lambda)$ $(n>2)$	$(m_1, m_2, ..., m_{n-1})-$torção generalizada do reticulado $\Lambda \subset \mathbb{R}^n$

Sumário

Introdução

Reticulados são conjuntos discretos de pontos no espaço euclidiano n-dimensional que são descritos por todas as combinações lineares inteiras de vetores linearmente independentes fixados. Conforme podemos ver em [13] os reticulados são estudados por matemáticos por suas simetrias dentre outras propriedades, estudados por engenheiros elétricos e da computação, por suas aplicações em comunicações, codificação e teoria da informação, bem como em criptografia.

Em canais com desvanecimento do tipo Rayleigh (mediante Seção 2.2) são consideradas constelações de sinais n-dimensionais esculpidas no conjunto de pontos de um reticulado $\Lambda \subset \mathbb{R}^n$. Visando minimizar a probabilidade de erro na decodificação de uma palavra-código devemos encontrar reticulados com diversidade máxima (mediante Definição 51) e máxima distância produto mínima. Conforme podemos ver em [32] e em [23], essas constelações de sinais podem ser obtidas a partir de rotações de reticulados conhecidos. Nessas referências são consideradas rotações do $\mathbb{Z}^n$ para alguns valores de n e de reticulados mais densos em diversas dimensões.

Construções de reticulados rotacionados com diversidade máxima e boas distâncias produtos geralmente são feitas via teoria algébrica dos números. A partir do homomorfismo canônico e do homomorfismo torcido (mediante Definições 50 e 53) tais reticulados são construídos e suas distâncias produtos são calculadas via estruturas algébricas. Em [3], [22], [23], [32] e [37] encontram-se construções de reticulados rotacionados nesse formato.

Neste trabalho, construímos de maneira alternativa versões rotacionadas de reticulados com diversidade máxima e sobre certas condições calculamos suas distâncias produtos[1] ou limitantes destas, escrevemos as proposições obtidas a partir das distâncias produtos normalizadas (calculadas a partir dos volumes dos reticulados) e das distâncias produtos relativas (calculadas a partir das normas mínimas dos reticulados). Rotações de reticulados bidimensionais e tridimensionais foram feitas a partir da álgebra dos complexos e da álgebra dos quatérnios, respectivamente. A vantagem dessa abordagem é que podemos descrever geometricamente[2] tais reticulados, o que em geral pode ser difícil no caso dos reticulados algébricos. Sendo assim, alguns reticulados algébricos apresentados neste trabalho são descritos geometricamente, uma vez que foram conectados com nossas construções.

[1] A "distância produto" será ínfima, mínima, relativa ou normalizada (mediante Definições 54, 57 e 58). Em cada contexto específico, tal distância está devidamente explicitada.

[2] Por "descrever geometricamente" queremos dizer que podemos descrever geometricamente a rotação e/ou a reflexão que geram os reticulados com diversidade máxima.

Encontramos também limitantes para distâncias produtos de reticulados que estão "próximos" às nossas versões rotacionadas e a alguns reticulados algébricos. Isso foi possível (nas dimensões 2 e 3) a partir de "perturbações" dos ângulos ótimos das rotações. Para dimensões 5 e 8 utilizamos exponenciação de matrizes anti-simétricas "próximas" da matriz nula para encontrarmos "perturbações" de reticulados algébricos. Verificamos numericamente e apresentamos justificativas analíticas para o fato de que se tomarmos uma coleção de reticulados com diversidade máxima que estão "próximos" a um dado reticulado, então as distâncias produtos convergem para distância produto deste reticulado. A partir da exponenciação de matrizes também construímos as mesmas versões rotacionadas obtidas via álgebra dos quatérnios.

Em canais de ruído branco gaussiano (mediante Seção 2.1) também são consideradas constelações de sinais n-dimensionais esculpidas no conjunto de pontos de um reticulado $\Lambda \subset \mathbb{R}^n$. Conforme podemos ver em [11] e em [13], para minimizarmos a probabilidade de erro de decodificação devemos maximizar as densidades[3] dos reticulados considerados. Assim, se um reticulado possuir boa distância produto e boa densidade, o mesmo pode ser útil a canais com desvanecimento do tipo Rayleigh e a canais gaussianos simultaneamente.

Neste trabalho, fixado um reticulado, obtivemos um outro reticulado com a mesma distância produto mínima e com uma densidade de empacotamento maior do que o original. A técnica utilizada foi a partir de um novo conceito, a saber, o conceito de *torção generalizada*. Esse conceito teve por motivação os homomorfismos canônico e torcido que estão relacionados aos reticulados algébricos. Portanto, a torção generalizada pôde ser aplicada a um reticulado qualquer, ou seja, não necessariamente algébrico.

Na sequência descrevemos o conteúdo desenvolvido neste trabalho.

No Capítulo 1, cujo título é Preliminares, apresentamos conceitos e resultados essenciais para o desenvolvimento do trabalho.

No Capítulo 2, apresentamos modelos de sistemas de transmissão em canais de ruído branco gaussiano e em canais com desvanecimento do tipo Rayleigh e suas relações com reticulados densos e com reticulados que possuam boas distâncias produtos, respectivamente. Em seguida, apresentamos um resumo da teoria de reticulados.

No Capítulo 3, apresentamos conceitos básicos da teoria algébrica dos números e a construção de reticulados algébricos a partir do homomorfismo canônico e do homomorfismo torcido. São construídas as versões rotacionadas da família de reticulados via corpos quadráticos e as já conhecidas versões rotacionadas do $\mathbb{Z}^n$ $(n = 2, 3, 5, 8)$ e do D_n $(n = 3, 5, 8)$, em que são explicitadas as distâncias produtos desses reticulados. Conforme podemos ver em [40], para tais valores de n, as versões rotacionadas do $\mathbb{Z}^n$ têm as maiores

[3] Sempre que escrevemos apenas "densidade", nos referimos à densidade de empacotamento.

distâncias produtos conhecidas.

No Capítulo 4, começam as nossas contribuições com o foco inicial em reticulados bidimensionais. Construímos uma versão rotacionada do $\mathbb{Z}^2$ na Proposição 1 e demonstramos que esta possui a maior distância produto possível. Na Proposição 2 descrevemos os reticulados bem arredondados e nas Proposição 3 e 4 mostramos que o $\mathbb{Z}^2$ é um reticulado bem arredondado com maior distância produto normalizada e relativa respectivamente. Nas Proposições 5 a 12 descrevemos as classes de reticulados que compõem a família dos reticulados quadráticos, onde exibimos, sob certas condições, suas distâncias produtos normalizadas e relativas. Na Proposição 13 demonstramos que não há reticulado ortogonal com distância normalizada superior à da versão rotacionada "ótima" do $\mathbb{Z}^2$ e na Proposição 14 demonstramos que não há reticulado ortogonal com distância relativa superior à de uma versão rotacionada "ótima" de uma classe de reticulados $\Lambda(\sqrt{l})$, em que l é um número inteiro maior que um que não é um quadrado perfeito e, finalmente, na Proposição 15, exibimos a distância normalizada de tal classe de reticulados.

No Capítulo 5, são apresentadas as contribuições referentes a reticulados tridimensionais, especificamente o $\mathbb{Z}^3$ e o FCC. Construímos versões rotacionadas desses reticulados nas Proposições 16, 17 e 18 e demonstramos que estas possuem as maiores distâncias produtos possíveis quando consideramos as rotações em torno da reta com vetor diretor $(1, 1, 1)$.

No Capítulo 6, é apresentada uma análise das distâncias produtos de versões "próximas" dos reticulados algébricos com dimensões superiores a 3, especificamente o $\mathbb{Z}^n$ e o D_n para $n = 5$ e $n = 8$. Essas versões ou "perturbações" dos reticulados algébricos são obtidas a partir de exponenciais de matrizes anti-simétricas próximas da matriz nula. Esta análise é justificada e generalizada a partir dos Corolários da Proposição 19, de onde decorre que se $\tilde{X}$ é uma matriz anti-simétrica "próxima" da matriz nula, então o reticulado $\Lambda_{(e^{\tilde{X}}B)}$ tem distâncias produtos (normalizada e relativa) "próximas" das distâncias produtos de Λ_B, desde que estes tenham diversidade máxima (mediante Observação 33). As Proposições 20, 21 e 22 são versões alternativas das Proposições do Capítulo 5.

No Capítulo 7, apresentamos o conceito de torção generalizada para um reticulado qualquer (conforme Definições 62 e 63). Nas Proposições 23 e 24 encontramos, sob certas condições, as distâncias produtos (normalizada e relativa) de uma classe de reticulados $\Lambda(a)$, classe esta que é uma generalização doutra classe de reticulados quadráticos construída no Capítulo 4. Na Proposição 25, conectamos por meio de uma torção generalizada um reticulado desta classe $\Lambda(a)$ com a versão rotacionada "ótima" do $\mathbb{Z}^2$. Apesar de não ter sido possível construir uma torção mais densa da versão "ótima" rotacionada do $\mathbb{Z}^2$, mostramos na Proposição 26 que existem versões torcidas desta versão "ótima" com distâncias produtos relativas superiores à da versão construída na Proposição 1. Construímos versões torcidas mais densas de outros reticulados bidimensionais, sendo

que um deles é um "quase hexagonal", a saber, o reticulado $\mathrm{tor}_{1387/10^7}(\mathrm{rot}_{\pi/4}(\Lambda(\sqrt{3})))$ da Tabela 9. Na Seção 7.2 construímos versões torcidas mais densas das versões rotacionadas "ótimas" do $\mathbb{Z}^n$, para $n = 3, 5, 8$ finalizando assim este capítulo.

No Capítulo 8, apresentamos nossas considerações finais e perspectivas futuras em relação a este trabalho.

1 Preliminares

Neste capítulo apresentamos conceitos e resultados considerados essenciais para o desenvolvimento dos demais capítulos. Na primeira seção introduzimos conceitos básicos da álgebra como grupos, anéis e corpos. Na segunda e terceira seções apresentamos os conceitos de espaços vetoriais e módulos.

Na quarta seção mostramos como efetuar rotações em $\mathbb{R}^2$ e em $\mathbb{R}^3$ via complexos $\mathbb{C}$ e via quatérnios $\mathbb{H}$ respectivamente. Alguns resultados referentes às equações diofantinas do segundo grau são apresentados na quinta seção; finalizamos este capítulo com um pequeno resumo referente às funções de várias variáveis reais.

As referências utilizadas foram: [6], [7], [12], [15], [18], [20], [24], [25], [27], [28], [30], [33], [34], [35] e [42]

1.1 Grupos, Anéis e Corpos

Nesta seção, apresentamos os conceitos de grupos, anéis, corpos e ideais, bem como alguns exemplos e resultados importantes envolvendo tais conceitos.

Definição 1 (Grupo)**.** *Seja $\mathcal{G}$ um conjunto não vazio munido com uma operação interna (que denotamos aditivamente)*

$$\mathcal{G} \times \mathcal{G} \to \mathcal{G}$$
$$(a, b) \to a + b$$

O par $(\mathcal{G}, +)$ é denominado grupo se as seguintes condições se verificam:

(1) A operação é associativa, isto é, $a+(b+c) = (a+b)+c$ para todo $a, b, c \in \mathcal{G}$.

(2) Existe um elemento neutro $0 \in \mathcal{G}$, tal que $0 + a = a + 0$ para todo $a \in \mathcal{G}$.

(3) Para todo $a \in \mathcal{G}$, existe um inverso $b \in \mathcal{G}$ tal que $a + b = b + a = 0$.

Por simplicidade dizemos que $\mathcal{G}$ é um grupo, mas isso pressupõe pela definição anterior que nos referimos ao par $(\mathcal{G}, +)$. O grupo $\mathcal{G}$ é dito *abeliano* (ou *comutativo*) se $a + b = b + a$ para todo $a, b \in \mathcal{G}$, isto é, a operação interna é comutativa. Observamos que o par $(\mathbb{R}^n, +)$ é um grupo abeliano, em que $+$ denota a operação de soma usual no $\mathbb{R}^n$.

Sejam $a, b \in \mathbb{Z}$. Dizemos que $a \equiv b \pmod{m}$ se m dividir $a - b$. A *classe residual* de um elemento a de $\mathbb{Z}$, módulo m, é o conjunto $\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$.

Dados $a, b \in \mathbb{Z}$, definimos $\overline{a} + \overline{b} = \overline{a + b}$. Conforme podemos ver em [15], o conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ é um grupo que é designado como *grupo aditivo das classes residuais módulo m.*

Definição 2 (Subgrupo)**.** *Seja $(\mathcal{G}, +)$ um grupo e $\mathcal{H}$ um subconjunto não vazio de $\mathcal{G}$. Dizemos que $\mathcal{H}$ é um subgrupo de $\mathcal{G}$ se $(\mathcal{H}, +)$ é um grupo, em que $+$ é a operação interna herdada de $\mathcal{G}$.*

Definição 3 (Anel)**.** *Seja A um conjunto não vazio munido com duas operações internas denotadas por $+$ e $\cdot$*

$$\begin{array}{lll} A \times A \to A & e & A \times A \to A \\ (a,b) \to a+b & & (a,b) \to a \cdot b \end{array}$$

A terna $(A, +, \cdot)$ é um anel se as seguintes condições se verificam:

(1) $(A, +)$ é um grupo abeliano.

(2) A operação $\cdot$ é associativa, isto é, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in A$.

(3) A operação $\cdot$ é distributiva sobre $+$, isto é, $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ para todo $a, b, c \in A$.

Caso exista $1 \in A$ tal que $1 \cdot a = a \cdot 1$ para todo a, dizemos que A é um *anel com unidade.*

Por simplicidade dizemos que A é um anel, mas isso pressupõe pela definição anterior que nos referimos à terna $(A, +, \cdot)$. Um *subanel* de A é um subconjunto $B \subseteq A$ que também é um anel com as mesmas operações internas herdadas de A. O anel A é dito *comutativo* se $a \cdot b = b \cdot a$ para todo $a, b \in A$, isto é, a operação interna $\cdot$ é comutativa.

Definição 4. *Um elemento $a \in A$ é invertível para a operação $\cdot$ se existir $b \in A$ tal que $a \cdot b = b \cdot a = 1$. O conjunto dos elementos de A que são invertíveis é denominado conjunto das unidades de A, e é denotado por A^*.*

Das Definições 3 e 4 seguem que o terno $(\mathbb{Z}, +, \cdot)$ é um anel e que $\mathbb{Z}^* = \{-1, 1\}$.

Definição 5 (Corpo)**.** *Seja $\mathbb{K}$ um conjunto não vazio. Dizemos que $\mathbb{K}$ é um corpo se ele for um anel comutativo, com unidade, tal que $\mathbb{K}^* = \mathbb{K} \backslash \{0\}$.*

O conjunto $\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$ é um corpo. Esse é o corpo das frações de $\mathbb{Z}$. Observamos ainda que o conjunto dos números reais $\mathbb{R}$ e o conjunto dos números complexos $\mathbb{C} = \left\{ a + bi : a, b \in \mathbb{R}, i = \sqrt{-1} \right\}$ também são exemplos conhecidos de corpos.

Sejam A um anel e x uma variável. Um polinômio $p(x)$ com coeficientes em A na variável x é uma expressão da forma $p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + ... + a_n x^n$, em que n é um inteiro não negativo e os $a_i's$ são elementos em A.

O conjunto de todos os polinômios na variável x com coeficientes em A será denotado por $A[x]$. Observamos que $A \subset A[x]$.

Se $p(x) = \sum_{i=0}^{n} a_i x^i, q(x) = \sum_{j=0}^{m} b_j x^j \in A[x]$, definem-se as operações de adição e multiplicação em $A[x]$ como segue:

$$p(x) + q(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i,$$

$$p(x) \cdot q(x) = \sum_{i=0}^{n+m} c_i x^i, \text{ onde } c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}.$$

Observamos que essas operações, quando restritas a A, coincidem com a adição e multiplicação em A.

Teorema 1 ([20]). *As operações de adição e multiplicação em $A[x]$ o tornam um anel.*

Definição 6 (Homomorfismo de Anéis). *Se A e B são anéis, um homomorfismo de anéis é uma aplicação $\varphi : A \to B$ que para todo $a, b \in A$ satisfaz:*

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$;

(2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Definição 7 (Ideal). *Um ideal $\mathcal{I}$ de um anel comutativo A é um subgrupo aditivo de A que é estável sobre a multiplicação por A, ie, $a\mathcal{I} \subseteq \mathcal{I}$ para todo $a \in A$.*

Definição 8 (Ideal Principal). *Um ideal $\mathcal{I}$ de A é principal se é da forma $\mathcal{I} = (x) = xA = \{xy : y \in A\}$, $x \in \mathcal{I}$.*

Observamos que se $A = \mathbb{Z}$, então $n\mathbb{Z}$ é um ideal principal de $\mathbb{Z}$, para todo $n \in \mathbb{Z}$.

1.2 Espaços Vetoriais

Nesta seção, apresentamos o conceito de espaços vetoriais, norma e isomorfismo de espaços vetoriais.

Definição 9 (Espaço Vetorial). *Sejam dados um corpo $\mathbb{K}$, cujos elementos são chamados escalares, e um conjunto V, cujos elementos são chamados vetores. Dizemos que V é um espaço vetorial sobre $\mathbb{K}$, ou um $\mathbb{K}$-espaço vetorial, se existirem uma operação de adição em V*

$$+ : V \times V \to V$$
$$(\mathbf{v}, \mathbf{w}) \to \mathbf{v} + \mathbf{w}$$

e uma multiplicação dos elementos de V por escalares,

$$\cdot : \mathbb{K} \times V \to V$$
$$(\lambda, \mathbf{v}) \to \lambda \cdot \mathbf{v}$$

possuindo as seguintes propriedades:

(1) A adição é associativa, isto é, $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ *para todo* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$.

(2) A adição é comutativa, isto é, $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ *para todo* $\mathbf{u}, \mathbf{v} \in V$.

(3) Existência de elemento neutro: existe um elemento $\mathbf{0}$ *em* V *tal que* $\mathbf{u} + \mathbf{0} = \mathbf{u}$ *para todo* $\mathbf{u} \in V$.

(4) Existência de elemento inverso: dado um elemento $\mathbf{u} \in V$*, existe um elemento* $-\mathbf{u}$*, chamado simétrico de* $\mathbf{u}$*, tal que* $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.

(5) Dados $\lambda, \mu \in \mathbb{K}$ *e* $\mathbf{u} \in V$*, vale* $(\lambda + \mu) \cdot \mathbf{u} = \lambda \cdot \mathbf{u} + \mu \cdot \mathbf{u}$.

(6) Dados $\lambda \in \mathbb{K}$ *e* $\mathbf{u}, \mathbf{v} \in V$*, vale* $\lambda \cdot (\mathbf{u} + \mathbf{v}) = \lambda \cdot \mathbf{u} + \lambda \cdot \mathbf{v}$.

(7) Dados $\lambda, \mu \in \mathbb{K}$ *e* $\mathbf{u} \in V$*, vale* $(\lambda \cdot \mu) \cdot \mathbf{u} = \lambda \cdot (\mu \cdot \mathbf{u})$.

(8) Para todo $\mathbf{u} \in V$*,* $1 \cdot \mathbf{u} = \mathbf{u}$*, em que* 1 *é a unidade de* $\mathbb{K}$.

Exemplos de espaços vetoriais canônicos são o $\mathbb{R}$-espaço vetorial $\mathbb{R}^n$ e o $\mathbb{C}$-espaço vetorial $\mathbb{C}^n$. Esses são casos particulares do $\mathbb{K}$-espaço vetorial $\mathbb{K}^n$, em que $\mathbb{K}$ é um corpo arbitrário.

Um *subespaço* de um espaço vetorial V sobre um corpo $\mathbb{K}$ é um conjunto $W \subset V$ que também é um $\mathbb{K}$-espaço vetorial sob as mesmas operações que tornam V um $\mathbb{K}$-espaço vetorial. Observamos que $\{(x, 0) : x \in \mathbb{R}\}$ é um subespaço do espaço vetorial $\mathbb{R}^2$ sobre o corpo $\mathbb{R}$.

Os exemplos dados acima são exemplos de espaços vetoriais com *dimensão finita*[1]. Um exemplo de um espaço vetorial com dimensão infinita é o $\mathbb{K}$-espaço vetorial $\mathbb{K}[x]$.

Definição 10 (Norma)**.** *Uma norma em um espaço vetorial* V *sobre um corpo* $\mathbb{K}$ *é uma aplicação* $||\cdot|| : V \to \mathbb{K}$ *satisfazendo:*

(1) Dado $\mathbf{u} \in V$*, vale* $||\mathbf{u}|| \geqslant 0$ *e* $||\mathbf{u}|| = 0 \Leftrightarrow \mathbf{u} = \mathbf{0}$.

(2) Dados $\lambda \in \mathbb{K}$ *e* $\mathbf{u} \in V$*, vale* $||\lambda \cdot \mathbf{u}|| = |\lambda| \cdot ||\mathbf{u}||$.

(3) Dados $\mathbf{u}, \mathbf{v} \in V$*, vale* $||\mathbf{u} + \mathbf{v}|| \leqslant ||\mathbf{u}|| + ||\mathbf{v}||$ *(desigualdade triangular).*

Definição 11 (Isomorfismo de Espaços Vetoriais)**.** *Dados os espaços vetoriais* V *e* W *sobre um corpo* $\mathbb{K}$*. Dizemos que uma aplicação* $f : V \to W$ *é um isomorfismo, se as condições a seguir forem satisfeitas:*

(1) f *é uma bijeção.*

[1] Um espaço vetorial tem dimensão finita quando possui uma base dada por um conjunto com cardinalinade finita. A cardinalidade desse conjunto, que é invariante com a mudança de base, é definida como a dimensão do espaço.

(2) Dados $\mathbf{u}, \mathbf{v} \in V$, *vale* $f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$.

(3) Dados $\lambda \in \mathbb{K}$ *e* $\mathbf{u} \in V$, *vale* $f(\lambda \cdot \mathbf{u}) = \lambda \cdot f(\mathbf{u})$.

Nas condições da Definição 11, quando tal aplicação f existe, dizemos que V e W são *isomorfos*.

Um exemplo de espaço vetorial bastante usado nesse trabalho é o conjunto das matrizes $m \times n$ reais que designamos por $M_{m\times n}(\mathbb{R})$. Uma vez que os conjuntos $M_{m\times n}(\mathbb{R})$ e $\mathbb{R}^{m\times n}$ são isomorfos, representamos, por uma questão de simplicidade, o conjunto das matrizes $m \times n$ reais por $\mathbb{R}^{m\times n}$.

Exemplos importantes de matrizes: Seja $A \in \mathbb{R}^{n\times n}$,

(1) dizemos que A é *simétrica* quando $A^t = A$, em que A^t é a transposta da matriz A;

(2) dizemos que A é *anti-simétrica* quando $A^t = -A$;

(3) dizemos que A é *ortogonal* quando $A^tA = AA^t = I_n$, em que $I_n \in \mathbb{R}^{n\times n}$ é a matriz identidade de ordem n;

(4) dizemos que A é *definida positiva* quando dado $0 \neq \mathbf{x} \in \mathbb{R}^n$, temos $\mathbf{x}^tA\mathbf{x} > 0$.

O conceito de *autovalor* e *autovetor* de uma matriz é apresentado na Definição 12. Os autovalores e autovetores de uma matriz podem ser úteis na análise geométrica das propriedades de determinados objetos.

Definição 12. *Seja* $A \in \mathbb{R}^{n\times n}$, *dizemos que* $\lambda \in \mathbb{C}$ *é um autovalor de* A *associado ao aotovetor* $v \in \mathbb{C}^n$ *de* A *se* $Av = \lambda v$.

Um importante exemplo de *norma matricial* (mediante Definição 10) é a *norma de Frobenius* que definimos a seguir.

Definição 13 (Norma de Frobenius)**.** *A norma de Frobenius de uma matriz* $A \in \mathbb{R}^{m\times n}$ *é dada por*

$$||A|| = ||A||_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |a_{ij}|^2}.$$

1.3 Módulos

Nesta seção, apresentamos os conceitos de módulo, submódulo, $\mathbb{Z}$-módulo finitamente gerado, independência linear sobre $\mathbb{Z}$ e $\mathbb{Z}$-base.

Definição 14 (Módulo)**.** *Seja* A *um anel comutativo e* $\mathcal{G}$ *um grupo abeliano munido de uma aplicação* $\phi : A \times \mathcal{G} \to \mathcal{G}$, *definida como* $\phi(a, g) = ag$. *Dizemos que* $\mathcal{G}$ *é um* A*-módulo se*

(1) $\phi(a, g+h) = \phi(a, g) + \phi(a, h)$, *para todo* $a \in A$ *e para todo* $g, h \in \mathcal{G}$.

(2) $\phi(a+b, g) = \phi(a, g) + \phi(b, g)$, *para todo* $a, b \in A$ *e para todo* $g \in \mathcal{G}$.

(3) $\phi(ab, g) = a(\phi(b, g))$, *para todo* $a, b \in A$ *e para todo* $g \in \mathcal{G}$.

(4) $\phi(1, g) = g$, *para todo* $g \in \mathcal{G}$.

Definição 15 (Submódulo)**.** *Um subgrupo* $\mathcal{H}$ *do* A*-módulo* $\mathcal{G}$ *é chamado* A*-submódulo de* $\mathcal{G}$ *se para todo* $a \in A$ *e* $h \in \mathcal{H}$ *temos* $ah \in \mathcal{H}$.

A noção de A-módulo é uma generalização de $\mathbb{K}$-espaço vetorial, em que $\mathbb{K}$ é um corpo.

Um $\mathbb{Z}$-módulo nada mais é que um grupo abeliano $\mathcal{G}$ (escrito aditivamente), e consequentemente, dado um grupo abeliano $\mathcal{G}$ (escrito aditivamente) podemos transformá-lo em um $\mathbb{Z}$-módulo, definindo $0g = 0, 1g = g$ $(g \in \mathcal{G})$ em que indutivamente $(z+1)g = zg + g$ $(z \in \mathbb{Z}, z > 0)$ e $(-z)g = -zg$ $(z \in \mathbb{Z}, z > 0)$.

Definição 16 ($\mathbb{Z}$-módulo Finitamente Gerado)**.** *Um grupo abeliano* $\mathcal{G}$ *é finitamente gerado como* $\mathbb{Z}$*-módulo, se existem* $g_i \in \mathcal{G}$ $(i = 1, 2, ..., n)$ *tal que todo* $g \in \mathcal{G}$ *é escrito como* $g = \sum_{i=1}^{n} z_i g_i$ $(z_i \in \mathbb{Z})$. *Os elementos* g_i $(i = 1, 2, ..., n)$ *são denominados geradores de* $\mathcal{G}$ *e o conjunto* $\{g_i\}_{i=1}^{n}$ *gera* $\mathcal{G}$.

Definição 17 (Independência Linear sobre $\mathbb{Z}$)**.** *Dizemos que os elementos* g_i $(i = 1, 2, ..., n)$ *em um grupo abeliano* $\mathcal{G}$ *são linearmente independentes (LI) se qualquer equação* $\sum_{i=1}^{n} z_i g_i = 0$ $(z_i \in \mathbb{Z})$ *implica* $z_i = 0$, *para todo* $i = 1, 2, ..., n$.

Definição 18 ($\mathbb{Z}$-base)**.** *Um conjunto* $\{g_i\}_{i=1}^{n}$ *de geradores de um grupo abeliano* $\mathcal{G}$ *cujos elementos* g_i $(i = 1, 2, ..., n)$ *são linearmente independentes (sobre* $\mathbb{Z}$*) é chamado uma base (ou* $\mathbb{Z}$*-base para ênfase) de* $\mathcal{G}$.

Se $g_i \in \mathcal{G}$ $(i = 1, 2, ..., n)$ formam uma $\mathbb{Z}$-base para $\mathcal{G}$, então todo $g \in \mathcal{G}$ tem uma única representação $g = \sum_{i=1}^{n} z_i g_i$ $(z_i \in \mathbb{Z})$. Um $\mathbb{Z}$-módulo com uma base de n elementos é denominado $\mathbb{Z}$-*módulo livre* de posto n.

1.4 Rotações por Complexos e por Quatérnios

Sabemos da álgebra linear que rotações no $\mathbb{R}^n$ são efetuadas a partir de produtos de uma matriz ortogonal por vetores (matrizes-coluna do $\mathbb{R}^n$). No caso em que $n = 2$ e $n = 3$ podemos, alternativamente, efetuar essas rotações via álgebra dos complexos $\mathbb{C}$ e via álgebra dos quatérnios $\mathbb{H}$, respectivamente. Esse procedimento será descrito nessa seção.

Definição 19 (𝕂-álgebra)**.** *Uma álgebra sobre um corpo* $\mathbb{K}$ *(ou uma* $\mathbb{K}$*-álgebra) é um espaço vetorial* A *sobre* $\mathbb{K}$ *munido de um produto bilinear, isto é,*

$$\begin{aligned} A \times A &\to A \\ (\mathbf{a}, \mathbf{b}) &\to \mathbf{a} \cdot \mathbf{b} \end{aligned}$$

em que,

(1) a operação $\cdot$ *é distributiva à esquerda sobre* $+$*, isto é,* $\mathbf{a} \cdot (\mathbf{b} + \mathbf{c}) = \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \cdot \mathbf{c}$;

(2) a operação $\cdot$ *é distributiva à direita sobre* $+$*, isto é,* $(\mathbf{a} + \mathbf{b}) \cdot \mathbf{c} = \mathbf{a} \cdot \mathbf{c} + \mathbf{b} \cdot \mathbf{c}$;

(3) dados $\lambda \in \mathbb{K}$ *e* $\mathbf{a}, \mathbf{b} \in A$*, segue-se que* $(\lambda \cdot \mathbf{a}) \cdot \mathbf{b} = \mathbf{a} \cdot (\lambda \cdot \mathbf{b}) = \lambda \cdot (\mathbf{a} \cdot \mathbf{b})$ *(compatibilidade da multiplicação por escalar com relação à multiplicação de vetores).*

Por simplicidade, denotamos o produto sem o uso do símbolo $\cdot$, ou seja, apenas justapondo os termos. Uma $\mathbb{K}$-álgebra é chamada *associativa* (respectivamente *comutativa*, respectivamente *com unidade*) se a lei do produto é associativa (respectivamente, comutativa, respectivamente, tem um elemento unidade 1_A, tal que $1_A a = a 1_A$ para todo $a \in A$.)

O anel de polinômios $\mathbb{K}[x]$ é uma $\mathbb{K}$-álgebra comutativa, associativa e com unidade.

Definição 20 (Álgebra de Divisão)**.** *Uma* $\mathbb{K}$*-álgebra* A *é dita de divisão se* A *é um anel de divisão (isto é, todo elemento não nulo de* A *é invertível).*

Definição 21 (Álgebra Normada)**.** *Uma* $\mathbb{K}$*-álgebra* A *é dita normada se o* $\mathbb{K}$*-espaço vetorial* A *é munido de uma norma* $||\cdot||$ *que satisfaz* $||\mathbf{ab}|| = ||\mathbf{a}||\ ||\mathbf{b}||$*, para todo* $\mathbf{a}, \mathbf{b} \in A$.

O conjunto dos números complexos $\mathbb{C}$ é uma $\mathbb{R}$-álgebra de divisão que é associativa, comutativa, com unidade e normada.

Relembramos a seguir alguns **conceitos relativos ao números complexos**.

Sejam $z = a + bi$ e $w = c + di$ dois números complexos arbitrários. A *adição* e *multiplicação* em $\mathbb{C}$ são dadas, respectivamente, por $z + w = (a + c) + (b + d)i$ e $zw = (ac - bd) + (ad + bc)i$. O *conjugado* do complexo $z = a + bi$ é dado por $\overline{z} = a - bi$.

Geometricamente representamos um número complexo $z = a + bi$ pelo vetor $(a, b) \in \mathbb{R}^2$; visto que a aplicação $f : \mathbb{C} \to \mathbb{R}^2$ dada por $f(a+bi) = (a, b)$ é um homomorfismo bijetor de anéis (mediante Definição 6), em que a adição em $\mathbb{R}^2$ é usual e a multiplicação é dada por $(a, b)(c, d) = (ac - bd, ad + bc)$.

Para cada $z = a + bi \neq 0$, define-se θ como *argumento* de z, que é o ângulo orientado no sentido anti-horário determinado pelo semi-eixo positivo das abcissas e o vetor $\overrightarrow{Oz}$, $0 \leqslant \theta < 2\pi$. A *norma* de z que é o comprimento do segmento $\overline{Oz}$ é definida por

$N(z) = |z| = \sqrt{a^2 + b^2}$. Se $N(z) = 1$, dizemos que z é um *complexo unitário*. Observamos que o ângulo θ é tal que $\cos(\theta) = a/N(z)$, $\text{sen}(\theta) = b/N(z)$, $\theta = \arctan(b/a)$ se $a \neq 0$ e desta forma z pode ser reescrito como $z = N(z)[\cos(\theta) + i\text{sen}(\theta)] = N(z)e^{i\theta}$ que é a chamada *forma polar* de z. Observamos que um número complexo $z \neq 0$ fica completamente determinado pela sua norma e argumento.

Sejam $z, w \in \mathbb{C}$. As *propriedades*, a seguir, são válidas:

(1) $N(zw) = N(z)N(w)$;

(2) $\overline{z + w} = \overline{z} + \overline{w}$;

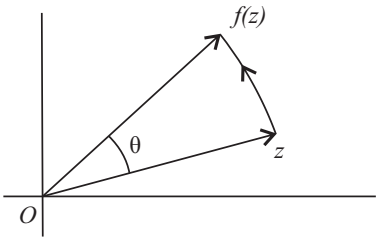
(3) $\overline{zw} = \overline{z}\ \overline{w}$;

(4) $[N(z)]^2 = z\overline{z}$.

O resultado, a seguir, estabelece como efetuar rotações em $\mathbb{R}^2$ via complexos.

Teorema 2 ([12]). *Seja u um número complexo unitário de argumento θ, ou seja, $u = \cos(\theta) + i\text{sen}(\theta)$; $0 \leqslant \theta < 2\pi$. Então a aplicação $f : \mathbb{C} \to \mathbb{C}$ dada por $f(z) = uz$ estabelece uma rotação anti-horária de ângulo θ do vetor $\overrightarrow{Oz}$.*

Figura 1 – Rotação via Complexos



Apresentamos, agora, alguns **conceitos relativos aos quatérnios** cujo conjunto designamos por $\mathbb{H}$. Os quatérnios, conforme vemos em [12] e [24], foram descobertos por William Rowan Hamilton em outubro de 1843. Eles compõem uma $\mathbb{R}$-álgebra de divisão que é associativa, com unidade e normada.

O conjunto de quatérnions (quatérnios de Hamilton), com as duas operações de adição e multiplicação, formam um anel de divisão não comutativo. Essa denominação enfatiza que o produto de quatérnios, em geral, não é comutativo, e também que o inverso multiplicativo existe, como de costume, para cada elemento diferente de zero no conjunto.

Em resumo: O conjunto de quatérnios sob as operações de adição e multiplicação satisfaz todos os axiomas de um corpo, exceto para a lei comutativa da multiplicação.

Um quatérnio é um número da forma $q = q_0 + q_1 i + q_2 j + q_3 k$ em que q_0, q_1, q_2, q_3 são números reais e i, j, k são unidades simbólicas satisfazendo os produtos registrados na Tabela 1.

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Tabela 1 – Produto das unidades simbólicas em $\mathbb{H}$

O conjunto dos quatérnios de Hamilton é definido por:

$$\mathbb{H} = \{q = q_0 + q_1 i + q_2 j + q_3 k : q_0, q_1, q_2, q_3 \in \mathbb{R}; i^2 = j^2 = k^2 = ijk = -1\}$$

Existe uma correspondência biunívica entre $\mathbb{H}$ e $\mathbb{R}^4$ que associa cada quatérnio $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H}$ ao vetor $(q_0, q_1, q_2, q_3) \in \mathbb{R}^4$. Isso decorre do fato de $\mathbb{H}$ ser um espaço vetorial sobre $\mathbb{R}$ de dimensão 4 com base $\{1, i, j, k\}$.

Dado $q = q_0 + q_1 i + q_2 j + q_3 k$, denotamos q_0 a *parte escalar* de q e a *parte vetorial* de q será definida como $\mathbf{q} = q_1 i + q_2 j + q_3 k$, assim temos $q = q_0 + \mathbf{q}$.

Um quatérnio q *imaginário puro* é aquele em que $q_0 = 0$. O conjunto dos quatérnios imaginários puros será designado por $\Im(\mathbb{H})$. A aplicação $f : \Im(\mathbb{H}) \to \mathbb{R}^3$ dada por $f(q_1 i + q_2 j + q_3 k) = (q_1, q_2, q_3)$ é um *isomorfismo de espaços vetoriais* (mediante Definição 11), logo, do ponto de vista da Álgebra Linear, $\Im(\mathbb{H})$ e $\mathbb{R}^3$ são isomorfos, isto é, $\Im(\mathbb{H}) \simeq \mathbb{R}^3$. Assim, dado um quatérnio $q = q_0 + \mathbf{q}$, segue que sua parte vetorial $\mathbf{q} = q_1 i + q_2 j + q_3 k \in \Im(\mathbb{H})$ é identificada com o vetor $(q_1, q_2, q_3) \in \mathbb{R}^3$, onde escrevemos $i = \mathbf{i} = (1, 0, 0)$, $j = \mathbf{j} = (0, 1, 0)$ e $k = \mathbf{k} = (0, 0, 1)$.

A *soma* de dois quatérnios $p = p_0 + p_1 i + p_2 j + p_3 k = p_0 + \mathbf{p}$ e $q = q_0 + q_1 i + q_2 j + q_3 k = q_0 + \mathbf{q}$ é dada por

$$p + q = (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k$$

e seu *produto* é dado por

$$pq = (p_0 q_0 - p_1 q_1 - p_2 q_2 - p_3 q_3) + (p_0 q_1 + p_1 q_0 + p_2 q_3 - p_3 q_2)i + (p_0 q_2 - p_1 q_3 + p_2 q_0 + p_3 q_1)j + (p_0 q_3 + p_1 q_2 - p_2 q_1 + p_3 q_0)k,$$

ou na forma compacta

$$pq = p_0 q_0 - \mathbf{p} \cdot \mathbf{q} + p_0 \mathbf{q} + q_0 \mathbf{p} + \mathbf{p} \times \mathbf{q}, \tag{1.1}$$

em que $\mathbf{p} \cdot \mathbf{q}$ e $\mathbf{p} \times \mathbf{q}$ representam o produto escalar e o produto vetorial de $\mathbf{p}$ e $\mathbf{q}$ em $\mathbb{R}^3$, respectivamente.

O conjugado e a norma de um quatérnio $q = q_0 + q_1 i + q_2 j + q_3 k = q_0 + \mathbf{q}$ são dados, respectivamente, por $\overline{q} = q_0 - q_1 i - q_2 j - q_3 k = q_0 - \mathbf{q}$ e $N(q) = |q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2} = \sqrt{q_0^2 + |\mathbf{q}|^2}$.

Sejam $p, q \in \mathbb{H}$. As *propriedades* a seguir são válidas:

(1) $N(pq) = N(p)N(q)$;

(2) $\overline{p+q} = \overline{p} + \overline{q}$;

(3) $\overline{pq} = \overline{q}\ \overline{p}$;

(4) $[N(q)]^2 = q\overline{q}$.

Se $N(q) = 1$, dizemos que q é um *quatérnio unitário*. Observamos ainda que se $q \neq 0$, então $q^{-1} = \overline{q}/N(q)^2$.

Dado o quatérnio $q = q_0 + \mathbf{q} \neq 0$ com norma $N(q)$, vamos associar a este o ângulo θ tal que $\cos(\theta) = q_0/N(q)$ e $\text{sen}(\theta) = |\mathbf{q}|/N(q)$. Observamos que θ está bem definido pois $-1 \leqslant \cos(\theta) \leqslant 1$, $0 \leqslant \text{sen}(\theta) \leqslant 1$, $\cos^2(\theta) + \text{sen}^2(\theta) = 1$ e existe um único θ, $0 \leqslant \theta \leqslant \pi$ que satisfaz estas condições. Admitindo $\mathbf{q} \neq \mathbf{0}$ $(0 < \theta < \pi)$, podemos reescrever q como $q = q_0 + (\mathbf{q}/|\mathbf{q}|)|\mathbf{q}|$ e escrevendo $\hat{q} = \mathbf{q}/|\mathbf{q}|$ que é um imaginário puro unitário temos: $q = N(q)\cos(\theta) + N(q)\text{sen}(\theta)\hat{q}$, ou ainda:

$$q = N(q)[\cos(\theta) + \hat{q}\ \text{sen}(\theta)]$$

que é a *forma polar* de q.

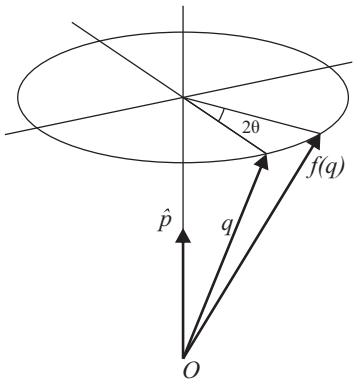
Finalizamos esta seção exibindo o resultado a seguir, que estabelece como efetuar rotações em $\mathbb{R}^3$ via quatérnios.

Teorema 3 ([18])**.** *Seja $p = \cos(\theta) + \hat{p}\ \text{sen}(\theta)$; $0 < \theta < \pi$, um quatérnio unitário, em que $\hat{p}$ é um imaginário puro unitário. A função $f : \mathbb{H} \to \mathbb{H}$ dada por $f(q) = pqp^{-1}$ é tal que*

(1) a restrição $f|\Im(\mathbb{H}) : \Im(\mathbb{H}) \to \Im(\mathbb{H})$ está bem definida;

(2) quando consideramos $\Im(\mathbb{H}) \simeq \mathbb{R}^3$, f representa uma rotação de ângulo 2θ em torno de $\hat{p}$.

Figura 2 – Rotação via Quatérnios (mediante [24])



Observamos que nos termos da proposição anterior e a partir da Eq. (1.1) temos:

$$\begin{aligned} f(q) &= pqp^{-1} = pq\overline{p} = (p_0+\mathbf{p})(0+\mathbf{q})(p_0-\mathbf{p}) = [(p_0+\mathbf{p})(0+\mathbf{q})](p_0-\mathbf{p}) \\ &= [-\mathbf{p}\cdot\mathbf{q} + (p_0\mathbf{q} + \mathbf{p}\times\mathbf{q})](p_0-\mathbf{p}) \\ &= (\mathbf{p}\cdot\mathbf{q})\mathbf{p} + p_0^2\mathbf{q} + 2p_0(\mathbf{p}\times\mathbf{q}) - (\mathbf{p}\times\mathbf{q})\times\mathbf{p} \qquad (1.2) \\ &= (p_0^2 - |\mathbf{p}|^2)\mathbf{q} + 2(\mathbf{p}\cdot\mathbf{q})\mathbf{p} + 2p_0(\mathbf{p}\times\mathbf{q}) \qquad (1.3) \\ &= (2p_0^2 - 1)\mathbf{q} + 2(\mathbf{p}\cdot\mathbf{q})\mathbf{p} + 2p_0(\mathbf{p}\times\mathbf{q}), \qquad (1.4) \end{aligned}$$

em que usamos $(\mathbf{p}\times\mathbf{q})\cdot\mathbf{p} = 0$ em (1.2) e para encontrarmos (1.3) usamos a *identidade vetorial de Lagrange*[2]. O cálculo de $f(p)$ pode ser feito a partir de (1.3) ou (1.4).

1.5 Equações Diofantinas do Segundo Grau

Nesta seção, apresentamos uma pequena discussão referente às equações diofantinas

$$x^2 - ly^2 = k, \qquad (1.5)$$

em que l é um número natural que não é um quadrado perfeito e k um inteiro não nulo qualquer.

Se $x = u$ e $y = v$ são inteiros que satisfazem à Eq. (1.5) dizemos, por simplicidade, que $u + v\sqrt{l}$ é uma solução desta. Duas soluções $u + v\sqrt{l}$ e $u' + v'\sqrt{l}$ são iguais se $u = u'$ e $v = v'$. A primeira solução é maior que a segunda se $u + v\sqrt{l} > u' + v'\sqrt{l}$.

A equação

$$x^2 - ly^2 = 1, \qquad (1.6)$$

é chamada *equação de Pell*, embora segundo [30] seja injustificada tal nomenclatura uma vez que Pell não fez nenhuma contribuição independente à teoria desta equação.

Teorema 4 ([30])**.** *Se l é um número natural que não é um quadrado perfeito, então existe pelo menos um par de números naturais x_0 e y_0 que satisfazem à Eq. (1.6).*

Dentre todas as soluções $x + y\sqrt{l}$ da Eq. (1.6) existe uma solução mínima $x_1 + y_1\sqrt{l}$, em que x_1 e y_1 têm os seus valores mínimos (positivos). Essa solução é chamada *solução fundamental*.

Teorema 5 ([30])**.** *Se l é um número natural que não é um quadrado perfeito, então a Eq. (1.6) tem infinitas soluções $x + y\sqrt{l}$. Todas as soluções com x e y positivos são obtidas pela fórmula*

$$x_n + y_n\sqrt{l} = (x_1 + y_1\sqrt{l})^n,$$

[2] A identidade vetorial de Lagrange nos diz que dados $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^3$ vale que $\mathbf{a}\times(\mathbf{b}\times\mathbf{c}) = (\mathbf{a}\cdot\mathbf{c})\mathbf{b} - (\mathbf{a}\cdot\mathbf{b})\mathbf{c}$.

em que $x_1 + y_1\sqrt{l}$ *é a solução fundamental,* n *é um número natural qualquer e*

$$\begin{aligned} x_n &= x_1^n + \sum_{k=1} \binom{n}{2k} x_1^{n-2k} y_1^{2k} l^k, \\ y_n &= \sum_{k=1} \binom{n}{2k-1} x_1^{n-2k+1} y_1^{2k-1} l^{k-1}. \end{aligned}$$

Quando l é dado, a solução fundamental da Eq. (1.6) pode ser encontrada por inspeção. Na expressão

$$1 + ly^2 \tag{1.7}$$

atribuímos $y = 1, 2, 3, 4...$, até que esta se torne um quadrado perfeito.

Consideremos agora a Eq. (1.5). Suponhamos que ela seja solúvel e que $u + v\sqrt{l}$ seja uma de suas soluções. Se $x + y\sqrt{l}$ é uma solução qualquer da Eq. (1.6), então $(u + v\sqrt{l})(x + y\sqrt{l}) = ux + vyl + (uy + vx)\sqrt{l}$ é também solução da Eq. (1.5) que é dita *solução associada* à $u + v\sqrt{l}$.

O conjunto de todas as soluções associadas entre si forma uma *classe de soluções* da Eq. (1.5). Segue do Teorema 5 que toda classe tem uma infinidade de soluções.

Podemos ver em [30] que a condição necessária e suficiente para que duas soluções $u + v\sqrt{l}$ e $u' + v'\sqrt{l}$ da Eq. (1.5) pertençam à mesma classe é que os números $\dfrac{uu' - vv'l}{k}$ e $\dfrac{u'v - uv'}{k}$ sejam inteiros.

Observamos que se K é uma classe de soluções $u_i + v_i\sqrt{l}$, $i = 1, 2, 3, ...$, da Eq. (1.5) então $u_i - v_i\sqrt{l}$, $i = 1, 2, 3, ...$, também constitui uma classe de soluções desta equação que será chamada *classe conjugada* de K e denotada por $\overline{K}$. Dizemos ainda que K é *ambígua* quando $K = \overline{K}$.

Dentre todas as soluções $u + v\sqrt{l}$ de uma classe K vamos escolher a solução $u_1 + v_1\sqrt{l}$ em que v_1 seja o menor valor não negativo de v que ocorre em K. Se K não é ambígua, então segundo [30], o número u_1 é univocamente determinado pois a solução $-u_1 + v_1\sqrt{l}$ pertence à classe conjugada $\overline{K}$. Se K é ambígua obtemos um u_1 univocamente determinado ao tomarmos $u_1 \geqslant 0$. A solução $u_1 + v_1\sqrt{l}$ encontrada deste modo é dita *solução fundamental* da classe K.

Teorema 6 ([30])**.** *Se* $u_1 + v_1\sqrt{l}$ *é a solução fundamental da classe* K *da Eq. (1.5) e* $x_1 + y_1\sqrt{l}$ *é a solução fundamental da Eq. (1.6), temos as desigualdades:*

$$0 \leqslant v_1 \leqslant \frac{y_1}{\sqrt{2(x_1 + 1)}}\sqrt{n}, \tag{1.8}$$

$$0 < |u_1| \leqslant \sqrt{\frac{1}{2}(x_1 + 1)n}, \tag{1.9}$$

desde que $k = n$ *onde* $n > 0$ *ou as desigualdades:*

$$0 < v_1 \leqslant \frac{y_1}{\sqrt{2(x_1 - 1)}}\sqrt{n}, \tag{1.10}$$

$$0 \leqslant |u_1| \leqslant \sqrt{\frac{1}{2}(x_1 - 1)n}, \tag{1.11}$$

desde que $k = -n$ *onde* $n > 0$.

Observação 1. *Segundo [30] a Eq. (1.5) tem um número finito de classes de soluções e as soluções fundamentais de todas as classes podem ser encontradas após um número finito de tentativas por meio das desigualdades (1.8) e (1.9) ou das desigualdades (1.10) e (1.11). A equação não terá solução alguma quando não tem solução que satisfaça essas desigualdades.*

Exemplo 1. *Considere as equações*

$$x^2 - 3y^2 = \pm 2.$$

Fazendo $l = 3$ *em (1.7) vemos que a solução fundamental da equação*

$$x^2 - 3y^2 = 1$$

é $2 + \sqrt{3}$. *Substituindo* $x_1 = 2$ *e* $y_1 = 1$ *na desigualdade (1.8) temos* $0 \leqslant v_1 \leqslant \frac{1}{\sqrt{3}}$. *Como não existe solução de* $x^2 - 3y^2 = 2$ *em que* $y = v_1 = 0$, *segue que esta equação é insolúvel. Por outro lado, as desigualdades (1.10) e (1.11) resultam em* $0 < v_1 \leqslant 1$ *e* $0 < |u_1| \leqslant 1$, *portanto* $1 + \sqrt{3}$ *é a solução fundamental da única classe de soluções da equação* $x^2 - 3y^2 = -2$.

Exemplo 2. *Considere as equações*

$$x^2 - 15y^2 = \pm 2.$$

Fazendo $l = 15$ *em (1.7) vemos que a solução fundamental da equação*

$$x^2 - 15y^2 = 1$$

é $4 + \sqrt{15}$. *Substituindo* $x_1 = 4$ *e* $y_1 = 1$ *na desigualdade (1.8) temos* $0 \leqslant v_1 \leqslant \frac{1}{\sqrt{5}}$. *Como não existe solução de* $x^2 - 15y^2 = 2$ *em que* $y = v_1 = 0$, *segue que esta equação é insolúvel. Por outro lado a desigualdade (1.10) resulta em* $0 < v_1 \leqslant \frac{1}{\sqrt{3}}$ *e como não existe* v_1 *inteiro que satisfaça a última desigualdade, segue que a equação* $x^2 - 15y^2 = -2$ *também é insolúvel.*

1.6 Funções de Várias Variáveis Reais

Nesta seção, apresentamos conceitos básicos da topologia no espaço euclidiano, bem como o conceito de continuidade. Finalizamos com alguns resultados importantes referentes às funções contínuas.

Definição 22 (Bola Aberta)**.** *Uma bola aberta de centro num ponto* $\mathbf{a} \in \mathbb{R}^n$ *e raio* $\epsilon > 0$ *é o conjunto* $B^n(\mathbf{a}; \epsilon) = \{\mathbf{x} \in \mathbb{R}^n : ||\mathbf{x} - \mathbf{a}|| < \epsilon\}$.

Definição 23 (Ponto de Acumulação)**.** *Seja* $X \subset \mathbb{R}^n$*. Um ponto* $\mathbf{a} \in \mathbb{R}^n$ *é dito ponto de acumulação do conjunto* X *se para todo* $\epsilon > 0$*, existir* $\mathbf{x} \in X$ *tal que* $0 < ||\mathbf{x} - \mathbf{a}|| < \epsilon$.

Definição 24 (Ponto Isolado e Conjunto Discreto)**.** *Se* $\mathbf{a} \in X \subset \mathbb{R}^n$ *não é ponto de acumulação de* X*, então será um ponto isolado de* X*. Isso ocorrerá se existir um* $\epsilon > 0$ *tal que* $B^n(\mathbf{a}; \epsilon) \cap X = \{\mathbf{a}\}$*. Quando todo ponto* $\mathbf{a} \in X$ *é isolado, dizemos que* X *é um conjunto discreto.*

Teorema 7 ([27])**.** *Dados* $X \subset \mathbb{R}^n$ *e* $\mathbf{a} \in \mathbb{R}^n$*, as seguintes afirmações são equivalentes:*

(1) $\mathbf{a}$ *é ponto de acumulação de* X;

(2) Existe uma sequência de pontos $\mathbf{x}_k \in X$*, com* $\lim \mathbf{x}_k = \mathbf{a}$ *e* $\mathbf{x}_k \neq \mathbf{a}$ *para todo* $k \in \mathbb{N}$;

(3) Toda bola aberta de centro $\mathbf{a}$ *contém uma infinidade de pontos de* X*.*

Definição 25 (Função Contínua)**.** *Seja* $X \subset \mathbb{R}^m$ *e* $f : X \to \mathbb{R}^n$*. Dizemos que* f *é contínua no ponto* $\mathbf{a} \in X$ *quando para toda bola aberta* B' *de centro* $f(\mathbf{a})$ *em* $\mathbb{R}^n$ *existe uma bola aberta* B *de centro* $\mathbf{a}$ *em* $\mathbb{R}^m$ *tal que* $f(B \cap X) \subset B'$*. Se* f *é contínua em todos os pontos do conjunto* X*, dizemos que* f *é contínua.*

Teorema 8 ([27])**.** *A composta de aplicações contínuas é contínua.*

Seja $\mathbf{a}$ um ponto isolado de $X \subset \mathbb{R}^m$, conforme podemos ver em [27], toda aplicação $f : X \to \mathbb{R}^n$ é contínua em $\mathbf{a}$. Por outro lado, se $\mathbf{a}$ é um ponto de acumulação de $X \subset \mathbb{R}^n$, segue que f é contínua no ponto $\mathbf{a}$ se, e somente se, $\lim\limits_{\mathbf{x} \to \mathbf{a}} f(\mathbf{x}) = f(\mathbf{a})$.

Teorema 9 ([27])**.** *Sejam* f *e* g *aplicações tais que a composta* $f \circ g$ *está bem definida. Se* $\lim\limits_{\mathbf{x} \to \mathbf{a}} f(\mathbf{x}) = \mathbf{b}$ *e* g *é contínua em* $\mathbf{b}$*, então* $\lim\limits_{\mathbf{x} \to \mathbf{a}} g(f(\mathbf{x})) = g(\mathbf{b})$.

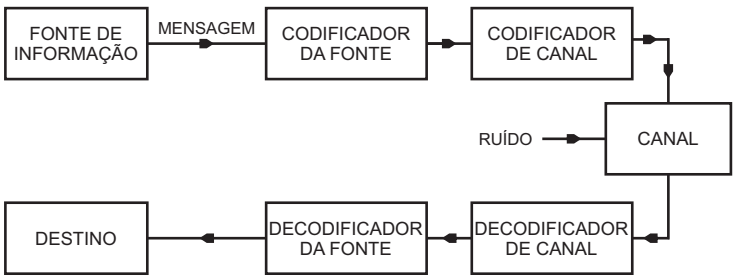
2 Reticulados e Aplicações em Problemas na Área de Comunicação

Apresentamos aqui modelos de sistemas de transmissão em canais de ruído branco gaussiano e em canais com desvanecimento do tipo Rayleigh e suas relações com o uso de reticulados densos e reticulados rotacionados que possuem maior distância produto mínima possível. Em seguida, apresentamos um resumo da teoria de reticulados: definimos reticulados e seus principais parâmetros, bem como reticulados importantes em diversas aplicações. As referências utilizadas foram: [9], [11], [13], [26] e [32].

2.1 Canais com Ruído Branco Gaussiano

Conforme pode ser visto em [11] um sistema típico para transmissão de dados é mostrado na Figura 3. As mensagens são produzidas por uma fonte de informação (um computador, por exemplo) e o codificador da fonte converte as mensagens em formato digital. Essas mensagens, por sua vez, devem ser transmitidas ao destino por meio de um canal de transmissão de dados. Por conta do ruído presente no canal, o que é recebido (ou recuperado) pode ser diferente do que foi transmitido.

Figura 3 – Diagrama de blocos de transmissão de dados ou sistema de armazenamento conforme Subseção 1.1 do Capítulo 3 de [11]



Para que as mensagens sejam transmitidas de forma confiável, eficiente e com baixo custo, procura-se para o sistema de comunicação descrito na Figura 3 um conjunto de sinais especiais denominado código que permite a identificação dos sinais mesmo com a presença de ruído. O codificador de canal substitui a saída do codificador da fonte por um dos sinais do código que é então transmitido pelo canal (ou armazenado no dispositivo de gravação). O decodificador de canal reverte este processo tomando o sinal recebido (ou recuperado) e fazendo uma estimativa (esperançosamente correta) do sinal de código; o decodificador da fonte então converte essa informação de volta para a mensagem original.

Um modelo idealizado para o canal da Figura 3 é o de ruído branco gaussiano. O ruído branco é um sinal discreto cujas amostras são dadas por uma sequência de variáveis aleatórias independentes com média zero e variância finita. Em particular, se cada amostra tem uma distribuição normal com média zero, o sinal, conforme podemos ver em [10], é chamado ruído branco gaussiano.

Na transmissão de um vetor $\mathbf{x}$ pertencente a um conjunto discreto de pontos $S \subset \mathbb{R}^n$ sobre um canal de ruído gaussiano aditivo, o sinal recebido $\mathbf{y}$ tem a forma

$$\mathbf{y} = \mathbf{x} + \mathbf{n}$$

onde $\mathbf{n}$ é um vetor aleatório cujas componentes são variáveis aleatórias gaussianas independentes com média 0 e variância σ^2. Conforme podemos ver em [13], o problema de codificação do canal gaussiano consiste em descobrir (decodificar) $\mathbf{x}$ a partir de $\mathbf{y}$, apesar da presença do ruído $\mathbf{n}$. A fim de que não seja desperdiçada muita potência na transmissão de $\mathbf{x}$, todos os pontos de S deverão estar dentro de uma esfera de raio $\sqrt{nP}$, onde P define uma restrição de potência média. Suponhamos que S seja um subconjunto de um reticulado Λ e que todos os pontos $\mathbf{x}$ são igualmente prováveis de serem enviados. Denotando por $P_e(S)$ a probabilidade de erro de se decodificar um ponto $\hat{\mathbf{x}} \neq \mathbf{x}$ quando $\mathbf{x}$ é enviado temos, segundo [13], que

$$P_e(S) \leqslant \frac{\kappa e^{-\Delta^{2/n}|S|^{-2/n}}}{2}$$

onde κ é o *kissing number*[1] de Λ e $\Delta = \Delta(\Lambda)$ é a densidade de empacotamento de Λ. Portanto, para um número fixo de pontos, o objetivo de minimizar a probabilidade de erro pode ser alcançado maximizando a densidade de empacotamento do reticulado subjacente.

2.2 Canais com Desvanecimento do tipo Rayleigh

Em comunicações sem fio (wireless communications) o desvanecimento (fading) conforme pode ser visto em [39] é o desvio da atenuação que um sinal de telecomunicação de frequência modulada pelo portador experimenta sob certos meios de propagação. O desvanecimento pode variar de acordo com o tempo, posição geográfica ou frequência de rádio, e é frequentemente definido como um processo estocástico. O desenvolvimento acelerado no uso de comunicação "wireless" levaram os teóricos da comunicação a trabalharem em canais com desvanecimento.

Novos métodos de projetos de códigos foram desenvolvidos para melhorar o baixo desempenho dos sistemas de transmissão sem fio. Tais códigos são construídos como conjunto de sinais de reticulados n-dimensionais (ou constelações) com determinadas

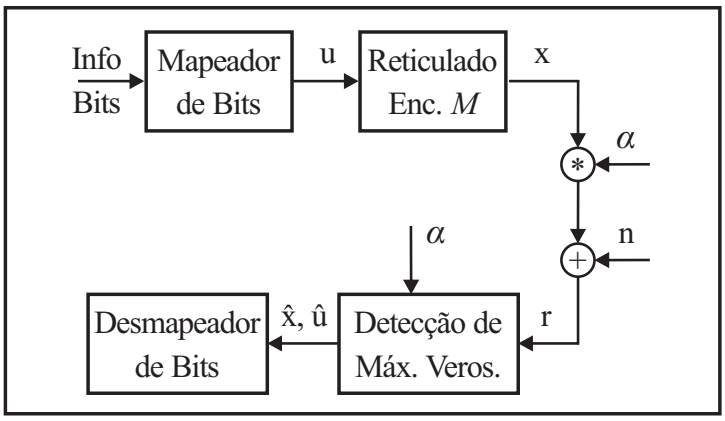
[1] O *kissing number* de um reticulado é o número de bolas do empacotamento que tocam uma bola fixa, que coincide com o número de vetores do reticulado que têm norma mínima não nula.

propriedades geométricas. A maior parte do ganho de codificação é obtido pela introdução da diversidade de modulação (ou diversidade de espaço de sinais) no conjunto de sinais, que resulta em eficiência na largura de banda. Foi percebido que uma diversidade de alta modulação pode ser obtida a partir de uma rotação particular a uma constelação de sinal de forma que dois pontos distintos dessa constelação obtivessem *distância de Hamming*[2] máxima.

Em geral, canais com desvanecimento do tipo Rayleigh são canais cujos modelos assumem que a magnitude de um sinal que passou através de um meio poderá variar aleatoriamente ou mesmo desaparecer. Consideramos os canais de desvanecimento plano de Rayleigh independente e admitimos que a informação do estado do canal é perfeita e está disponível no receptor, além do fato de que nenhuma interferência entre símbolos está presente.

A partir de constelações de sinais n-dimensionais S esculpidas no conjunto de pontos do reticulado $\Lambda = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} = M\mathbf{u}\}$, em que $\mathbf{u}$ é um vetor de coordenadas inteiras e M é a matriz geradora do reticulado, obtemos, conforme o modelo do sistema descrito na Figura 4, o ponto decodificado $\hat{\mathbf{x}}$ e o vetor de componentes inteiras correspondente $\hat{\mathbf{u}}$, no qual os bits decodificados podem ser extraídos. Neste caso, $\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n}$, onde $\boldsymbol{\alpha}$ em $\mathbb{R}^n$ é tal que α_i são variáveis aleatórias Rayleigh reais independentes com segundo momento unitário (i.e. $E[\alpha_i^2] = 1$), $\mathbf{n}$ é tal que n_i são variáveis aleatórias Gaussianas com média zero e variância $N_0/2$ e $\mathbf{r}$ são as amostras de sinal recebidas. A operação $*$ representa o produto componente a componente, ou seja, $(\alpha * x)_i = \alpha_i x_i$.

Figura 4 – Modelo do sistema conforme Subseção 2.2 de [32]



Conforme podemos ver em [8] e em [9] a estimativa da probabilidade de erro da palavra-código $P_e(S)$ do sistema de transmissão descrito é dada por

[2] Sejam $\mathbf{x} = (x_1, x_2, ..., x_n)$ e $\mathbf{y} = (y_1, y_2, ..., y_n)$, definimos a distância de Hamming entre $\mathbf{x}$ e $\mathbf{y}$ como $d_h(\mathbf{x}, \mathbf{y}) = |\{i; x_i \neq y_i\}|$ onde $|C|$ representa a cardinalidade do conjunto C.

$$P_e(S) \leqslant P_e(\Lambda) \leqslant \sum_{\mathbf{y}\neq\mathbf{x}} P(\mathbf{x}\to\mathbf{y})$$

em que

$$P(\mathbf{x}\to\mathbf{y}) \leqslant \frac{1}{2}\prod_{x_i\neq y_i}\frac{4N_0}{(x_i-y_i)^2} = \frac{1}{2}\frac{(4N_0)^l}{d_p^{(l)}(\mathbf{x},\mathbf{y})^2}$$

em que $P(\mathbf{x}\to\mathbf{y})$ é a probabilidade de erro aos pares e $d_p^{(l)}(\mathbf{x},\mathbf{y})$ é a l-distância produto de $\mathbf{x}$ a $\mathbf{y}$, quando esses dois pontos diferem em l componentes, isto é,

$$d_p^{(l)}(\mathbf{x},\mathbf{y}) = \prod_{x_i\neq y_i}|x_i-y_i|.$$

Observamos que para uma dada constelação, o "pior caso" irá ocorrer quando a l-distância produto for mínima, pois temos um aumento na probabilidade de erro.

Com o objetivo de reduzir a estimativa da probabilidade de erro da palavra-código $P_e(S)$ do sistema de transmissão, em nosso trabalho investigamos reticulados rotacionados em que a distância produto mínima seja a maior possível. Naturalmente, decorre da seção anterior que dentre tais reticulados, os que são mais densos podem ser utilizados também nos canais de transmissão do tipo gaussiano.

2.3 Reticulados

Um reticulado em $\mathbb{R}^n$ é um conjunto de vetores que é composto por todas as combinações lineares inteiras de vetores linearmente independentes (LI) fixados. Neste trabalho, adotamos a forma coluna para um vetor em $\mathbb{R}^n$.

Definição 26 (Reticulado)**.** *Sejam $\mathbf{b}_1,\mathbf{b}_2,...,\mathbf{b}_m$ vetores LI em $\mathbb{R}^n$. Um reticulado $\Lambda\subset\mathbb{R}^n$ com base $\{\mathbf{b}_1,\mathbf{b}_2,...,\mathbf{b}_m\}$ é definido por*

$$\Lambda = \left\{\sum_{i=1}^{m} u_i\mathbf{b}_i : u_i \in \mathbb{Z}\right\}.$$

O inteiro m é dito posto de Λ; se m=n dizemos que Λ tem posto completo.

Definição 27 (Matriz Geradora)**.** *Uma matriz geradora para um reticulado Λ é uma matriz $n\times m$ formada pelas colunas dos vetores que formam uma base deste, isto é, $B=[\mathbf{b}_1\ \mathbf{b}_2\ ...\ \mathbf{b}_m]$.*

Um vetor $\mathbf{x} \in \mathbb{R}^n$ está em Λ se, e somente se, suas coordenadas x_i, $i = 1, 2, ..., n$, são escritas como segue:

$$\begin{bmatrix} x_1 \\ ... \\ x_n \end{bmatrix} = [\mathbf{b}_1\ \mathbf{b}_2\ ...\ \mathbf{b}_m] \begin{bmatrix} u_1 \\ ... \\ u_m \end{bmatrix}, u_1, ..., u_m \in \mathbb{Z},$$

assim podemos escrever $\Lambda = \{\mathbf{x} = B\mathbf{u} \in \mathbb{R}^n : \mathbf{u} \in \mathbb{Z}^n\}$.

Definição 28 (Reticulado Ortogonal)**.** *Um reticulado $\Lambda \subset \mathbb{R}^n$ é dito ortogonal se Λ possui uma base de vetores ortogonais.*

Exemplo 3. *O reticulado hipercúbico $\mathbb{Z}^n$ é definido como $\mathbb{Z}^n = \{(x_1, x_2, ..., x_n) : x_i \in \mathbb{Z},\ i = 1, 2, ..., n\}$. Uma base para $\mathbb{Z}^n$ é a base canônica do $\mathbb{R}^n$, $\{\mathbf{e}_1, ..., \mathbf{e}_n\}$, onde $\mathbf{e}_i = (0, ..., 1, ..., 0)$ é o vetor com 1 na i-ésima coordenada e 0 nas demais. Dessa forma segue da Definição 28 que $\mathbb{Z}^n$ é ortogonal. Particularmente, para $n = 2$, temos o reticulado $\mathbb{Z}^2$ que geometricamente representa o conjunto de pares ordenados do plano cujas coordenadas são inteiras.*

Exemplo 4. *O reticulado D_n é definido como*

$$D_n = \{(x_1, x_2, ..., x_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \text{ é par}\}.$$

Uma base para D_n é dada por $\{\mathbf{v}_1, ..., \mathbf{v}_n\}$, em que $\mathbf{v}_1 = (2, 0, 0, ..., 0)$, $\mathbf{v}_2 = (1, 1, 0, ..., 0)$, $\mathbf{v}_3 = (1, 0, 1, 0, ..., 0), ..., \mathbf{v}_n = (1, 0, ..., 0, 0, 1)$. Particularmente, para $n = 3$, temos o reticulado D_3 que é conhecido como FCC, cuja sigla do inglês é Face-Centered Cubic, devido a geometria dos vetores da base deste reticulado.

Uma matriz $U = [u_{ij}]$ de ordem n é dita *unimodular* se $u_{ij} \in \mathbb{Z}$ e $\det(U) = \pm 1$. Observamos, que neste caso, $U^{-1} = [u'_{ij}]$ é tal que $u'_{ij} \in \mathbb{Z}$.

Teorema 10 ([13])**.** *Duas matrizes B e $\overline{B}$ geram o mesmo reticulado se, e somente se, existe uma matriz unimodular U tal que $\overline{B} = BU$.*

Definição 29 (Matriz de Gram)**.** *Dada uma matriz geradora B para um reticulado Λ, definimos sua matriz de Gram por $G = B^t B$.*

A matriz de Gram G é simétrica definida positiva, além disso, ela não é única, uma vez que um reticulado tem infinitas matrizes geradoras (conseqência imediata do Teorema 10). Por outro lado, se G_1 e G_2 são matrizes de Gram arbitrárias do reticulado Λ, segue também do Teorema 10 que $\det G_1 = \det G_2$. Isso motiva a definição a seguir.

Definição 30 (Determinante e Volume de um Reticulado)**.** *Seja G uma matriz de Gram de um reticulado Λ. O determinante de Λ é dado por $\det(\Lambda) = \det(G)$ e seu volume por $V(\Lambda) = \sqrt{\det(\Lambda)}$.*

Exemplo 5. *Segue da definição anterior que* $\det(\mathbb{Z}^n) = V(\mathbb{Z}^n) = 1$, $\det(D_n) = 4$ *e que* $V(D_n) = 2$.

Definição 31 (Norma Mínima de um Reticulado)**.** *A norma mínima corresponde ao mínimo entre todas as normas euclidianas dos vetores não-nulos do reticulado* Λ*, isto é,* $\mu = \min_{0 \neq \mathbf{x} \in \Lambda} ||\mathbf{x}||$*, em que* $||\mathbf{x}|| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$.

Dizemos que o conjunto de vetores $\{\mathbf{b}_1, ..., \mathbf{b}_i\} \subset \Lambda$ é *primitivo* se ele pode ser estendido a uma base de Λ, isto é, se existe $\{\mathbf{b}_{i+1}, ..., \mathbf{b}_m\}$ tal que $\{\mathbf{b}_1, ..., \mathbf{b}_i, \mathbf{b}_{i+1}, ..., \mathbf{b}_m\}$ é uma base de Λ.

Definição 32 (Base Minkowski-Reduzida)**.** *Uma base* $\{\mathbf{b}_1, ..., \mathbf{b}_m\}$ *para um reticulado n-dimensional* Λ *é dita Minkowski-reduzida se:*

(1) $\mathbf{b}_1$ *é um vetor de norma mínima em* Λ.

(2) Para todo $i = 1, ..., m-1$, $\mathbf{b}_{i+1}$ *é um vetor de menor norma em* Λ *tal que* $\{\mathbf{b}_1, ..., \mathbf{b}_i, \mathbf{b}_{i+1}\}$ *é primitivo.*

Observação 2. *No caso específico em que* $\Lambda \subset \mathbb{R}^2$*, vemos em [36] que se* $\{\mathbf{b}_1, \mathbf{b}_2\}$ *é uma base de* Λ *tal que* $\langle \mathbf{b}_1, \mathbf{b}_1 \rangle \leqslant \langle \mathbf{b}_2, \mathbf{b}_2 \rangle$ *e* $\dfrac{|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle|}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle} \leqslant \dfrac{1}{2}$*, então* $\{\mathbf{b}_1, \mathbf{b}_2\}$ *é Minkowski-reduzida e* $\mu = ||\mathbf{b}_1||$ *é a norma mínima de* Λ.

O Algoritmo 1, a seguir, fornece o procedimento para o cálculo da base Minkowski-reduzida e da norma mínima de um reticulado bidimensional. Ele foi obtido a partir do que foi desenvolvido na Seção 1.2.1 de [36]. Usamos a notação $[x]$ para denotar o inteiro mais próximo de x.

Algoritmo 1: Cálculo da base Minkowski-reduzida de um reticulado bidimensional

1. Entrada: base $\{\mathbf{b}_1, \mathbf{b}_2\}$;
2. Ordenar base: Se $\langle \mathbf{b}_1, \mathbf{b}_1 \rangle > \langle \mathbf{b}_2, \mathbf{b}_2 \rangle$, então $\mathbf{b}_1 \leftarrow \mathbf{b}_2$ e $\mathbf{b}_2 \leftarrow \mathbf{b}_1$, caso contrário, $\mathbf{b}_1 \leftarrow \mathbf{b}_1$ e $\mathbf{b}_2 \leftarrow \mathbf{b}_2$;
3. Calcular $t = \dfrac{|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle|}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle}$;
4. Enquanto $t > \dfrac{1}{2}$ faça
   - 4.1 $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - \left[\dfrac{\langle \mathbf{b}_1, \mathbf{b}_2 \rangle}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle}\right] \mathbf{b}_1$;
   - 4.2. Ordenar nova base: repetir etapa 2;
   - 4.3. Calcular novo t : repetir etapa 3;
5. Saída: Base Minkowski-reduzida $\{\mathbf{b}_1, \mathbf{b}_2\}$. Norma mínima $\mu = \sqrt{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle}$.

Nas condições da Definição 31, tomemos $\epsilon = \mu/2$ que é o maior valor pelo qual a translação das bolas $B^n(\mathbf{0}; \mu/2) = \{\mathbf{x} \in \mathbb{R}^n : ||\mathbf{x}|| < \mu/2\}$ centradas nos pontos do reticulado Λ são disjuntas. Desta forma $\mu/2$ será designado o *raio de empacotamento* de Λ.

Definição 33 (Densidade de Empacotamento)**.** *A densidade de empacotamento de Λ é definida como*

$$\Delta(\Lambda) = \frac{V(B^n((\mathbf{0}; \mu/2))}{V(\Lambda)}.$$

Conforme podemos ver em [13] temos que $V(B^n((\mathbf{0}; \rho)) = \rho^n V(B^n((\mathbf{0}; 1))$ e que

$$V(B^n(1)) = \begin{cases} \dfrac{\pi^{n/2}}{(n/2)!}, & \text{se} \quad n \text{ par} \\ \dfrac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!}, & \text{se} \quad n \text{ ímpar} \end{cases}$$

Exemplo 6 (Reticulado Hexagonal)**.** *O reticulado $\Lambda \subset \mathbb{R}^2$ com base $\{(1,0), (1/2, \sqrt{3}/2)\}$ é chamado de reticulado hexagonal. Esse reticulado possui seis vetores de norma mínima $\mu = 1$, cujas extremidades são vértices de um hexágono com centro na origem. Observamos que a densidade de empacotamento do reticulado hexagonal é dada por $\Delta(\Lambda) = \pi/\sqrt{12} \simeq 0.9069$. Conforme podemos ver em [13], este reticulado tem a maior densidade de empacotamento dentre todos os reticulados de dimensão 2.*

Definição 34 (Densidade de Centro)**.** *A densidade de centro de Λ é definida como*

$$\delta(\Lambda) = \frac{\Delta(\Lambda)}{V(B^n(\mathbf{0}; 1))} = \frac{(\mu/2)^n}{V(\Lambda)}.$$

A densidade de centro fornece um modo de comparar reticulados da mesma dimensão.

Exemplo 7. *Segue das definições anteriores que se $\Lambda_1 = \mathbb{Z}^n$ e $\Lambda_2 = D_n$, então as normas mínimas destes reticulados são dadas respectivamente por $\mu_1 = 1$ e $\mu_2 = \sqrt{2}$. Suas densidades de centro são dadas, respectivamente, por $\delta(\Lambda_1) = V(B^n(\mathbf{0}; 1))/2^n$ e $\delta(\Lambda_2) = 2^{-\frac{n}{2}-1}$.*

A seguir, definimos reticulados equivalentes que são reticulados obtidos por rotação, reflexão ou escalonamento do reticulado original.

Definição 35 (Reticulados Equivalentes)**.** *Dois reticulados $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ são equivalentes se existirem uma matriz ortogonal Q, um número real $c \neq 0$, matrizes geradoras B_1 e B_2 para Λ_1 e Λ_2, respectivamente, de modo que $B_1 = cQB_2$.*

Escrevemos $\Lambda_1 \sim \Lambda_2$ para dois reticulados equivalentes. Em particular, nas condições da Definição 35, dizemos que Λ_1 e Λ_2 são *congruentes* desde que $|c| = 1$. Observamos que reticulados congruentes possuem as mesmas matrizes de Gram.

Exemplo 8. *A família de reticulados* $\Lambda(t) = \{(k_1\cos(t) - k_2\text{sen}(t), k_1\text{sen}(t) + k_2\cos(t)) : k_1, k_2 \in \mathbb{Z}; 0 < t < \pi/2\}$ *é formada por reticulados que são congruentes ao reticulado* $\mathbb{Z}^2$.

O Teorema 11 expressa uma forma alternativa de caracterizar um reticulado em $\mathbb{R}^n$ a partir das Definições 2 e 24.

Teorema 11 ([29])**.** *Um subconjunto* $\Lambda \subset \mathbb{R}^n$ *é um reticulado se, e somente se, é um subgrupo aditivo discreto de* $\mathbb{R}^n$.

Definição 36 (Sub-Reticulado)**.** *Sejam* Λ *e* Λ' *reticulados tais que* $\Lambda' \subseteq \Lambda$. *Dizemos que* Λ' *é um sub-reticulado de* Λ.

Um subconjunto de um reticulado é um sub-reticulado, se e somente se, for um subgrupo aditivo.

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto completo com matriz geradora B e seja M uma matriz de ordem n com elementos inteiros. Conforme podemos ver em [13] se $\det M \neq 0$, então BM é uma matriz geradora de um sub-reticulado de posto completo Λ' de Λ. Reciprocamente, qualquer matriz geradora de um sub-reticulado de posto completo Λ' de Λ pode ser escrita como BM para alguma matriz M com coeficientes inteiros.

Dos Exemplos 3 e 4 e do que foi exposto no parágrafo anterior, segue que D_n é um sub-reticulado de $\mathbb{Z}^n$.

3 Reticulados Algébricos

Apresentamos conceitos básicos da teoria algébrica dos números, destacando os principais teoremas para construção de reticulados algébricos, a saber, o homomorfismo canônico e o homomorfismo torcido. Exibimos a família de reticulados via corpos quadráticos e determinamos suas distâncias produtos no caso em que o corpo quadrático é totalmente real. Posteriormente, exibimos versões rotacionadas de reticulados importantes via extensões finitas de corpos algébricos. Estamos particularmente interessados nas já conhecidas versões rotacionadas do $\mathbb{Z}^2, \mathbb{Z}^3, \mathbb{Z}^5, \mathbb{Z}^8$, FCC, D_5 e D_8 sendo que as quatro primeiras versões apresentam as maiores distâncias produtos conhecida na literatura, conforme exibido em [40]. As referências utilizadas foram: [3], [22], [32], [33], [35], [37] e [40].

3.1 Teoria Algébrica dos Números

A construção de um reticulado algébrico está relacionada ao conceito de *número algébrico* e a uma *extensão finita do corpo dos racionais*, conceitos que serão vistos nesta seção.

Definição 37 (Extensão de um Corpo)**.** *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *dois corpos. Se* $\mathbb{K} \subseteq \mathbb{L}$*, dizemos que* $\mathbb{L}$ *é uma extensão do corpo* $\mathbb{K}$ *e denotamos por* $\mathbb{L}/\mathbb{K}$.

Se $\mathbb{L}/\mathbb{K}$ é extensão de um corpo, então $\mathbb{L}$ também é uma $\mathbb{K}$-álgebra comutativa, associativa e com unidade (mediante Definição 19).

Observamos que $\mathbb{R}/\mathbb{Q}$ e que $\mathbb{C}/\mathbb{Q}$ são exemplos de extensões de corpos.

Definição 38 (Extensão Finita de um Corpo)**.** *Seja* $\mathbb{L}/\mathbb{K}$ *uma extensão de um corpo. A dimensão de* $\mathbb{L}$ *como espaço vetorial sobre* $\mathbb{K}$ *é chamada o grau de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *e denotada por* $[\mathbb{L} : \mathbb{K}]$*. Se* $[\mathbb{L} : \mathbb{K}]$ *é finito, dizemos que* $\mathbb{L}$ *é uma extensão finita de* $\mathbb{K}$.

Observamos que $\mathbb{R}/\mathbb{Q}$ e que $\mathbb{C}/\mathbb{Q}$ não são extensões finitas.

Dizemos que um $d \in \mathbb{Z}$ é *livre de quadrados* se d não é divisível por um quadrado de um primo. Observamos que 5 é livre de quadrados, assim como 6 e 7, por outro lado, 8 e 9 não o são.

Seja $1 \neq d \in \mathbb{Z}$ livre de quadrados e $\mathbb{Q}(\sqrt{d})$ a menor extensão de $\mathbb{Q}$ contendo o elemento $\sqrt{d}$. Conforme podemos ver em [35] o conjunto $\mathbb{Q}(\sqrt{d})$ é dado por $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, além disso, tal conjunto é uma extensão finita de $\mathbb{Q}$, onde $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$.

Daqui em diante, quando nos referirmos a $\mathbb{Q}(\sqrt{d})$, estamos admitindo que $1 \neq d \in \mathbb{Z}$ e que d é livre de quadrados.

Definição 39 (Corpo de Números)**.** *Uma extensão finita de* $\mathbb{Q}$ *é denominada corpo de números.*

Definição 40 (Algébrico e Transcendente)**.** *Seja* $\mathbb{L}/\mathbb{K}$ *e seja* $\alpha \in \mathbb{L}$*. Se existir* $q \in \mathbb{K}[x]$ *tal que* $q(\alpha) = 0$*, com* $q \not\equiv 0$*, dizemos que* α *é algébrico sobre* $\mathbb{K}$*, caso contrário* α *será transcendente sobre* $\mathbb{K}$*.*

Conforme podemos ver em [35], se α é algébrico sobre $\mathbb{K}$, então existe um único polinômio mônico (com coeficiente do termo de maior grau 1) $p_\alpha \in \mathbb{K}[x]$ de grau mínimo tal que $p_\alpha(\alpha) = 0$. Neste caso, p_α é chamado *polinômio mínimo* de α sobre $\mathbb{K}$.

Observamos que $\mathbb{Q}(\sqrt{d})$ é um corpo de números, $\alpha = \sqrt{d}$ é algébrico sobre $\mathbb{Q}$ e $x^2 - d$ é o polinômio mínimo de $\alpha = \sqrt{d}$ sobre $\mathbb{Q}$.

Um *corpo quadrático* é um corpo de números $\mathbb{K}$ de grau 2 sobre $\mathbb{Q}$. Do que foi exposto, segue que $\mathbb{Q}(\sqrt{d})$ é um corpo quadrático. Ademais, pode-se provar que (mediante [35]) todo corpo quadrático é precisamente da forma $\mathbb{Q}(\sqrt{d})$.

Definição 41 (Extensão Algébrica e Número algébrico)**.** *Se todos os elementos de* $\mathbb{K}$ *são algébricos sobre* $\mathbb{Q}$*, dizemos que* $\mathbb{K}$ *é uma extensão algébrica de* $\mathbb{Q}$*. Os elementos algébricos sobre* $\mathbb{Q}$ *serão denominados números algébricos.*

Observamos que qualquer $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Q}$ é uma raiz do polinômio $p_\alpha(x) = x^2 - 2ax + a^2 - b^2 d$ com coeficientes racionais. Dessa forma, segue que $\mathbb{Q}(\sqrt{d})$ é uma extensão algébrica sobre $\mathbb{Q}$.

Teorema 12 ([35])**.** *Se* $\mathbb{K}$ *é um corpo de números, então* $\mathbb{K} = \mathbb{Q}(\theta)$ *para algum número algébrico* $\theta \in \mathbb{K}$*.*

O número θ nas condições do Teorema 12 será chamado de *elemento primitivo.*

Definição 42 (Inteiro Algébrico)**.** *Seja* $\mathbb{K}$ *um corpo de números. Dizemos que* $\alpha \in \mathbb{K}$ *é um inteiro algébrico, se é uma raiz de um polinômio mônico com coeficientes em* $\mathbb{Z}$*.*

Observamos que $\sqrt{d}$ é um elemento primitivo e um inteiro algébrico de $\mathbb{Q}(\sqrt{d})$.

Teorema 13 ([35])**.** *Os inteiros algébricos formam um subanel de* $\mathbb{K}$*.*

O Teorema 13 motiva a definição a seguir.

Definição 43 (Anel de Inteiros)**.** *O conjunto de inteiros algébricos de um corpo de números* $\mathbb{K}$ *é denominado anel de inteiros de* $\mathbb{K}$ *e denotado por* $\mathcal{O}_\mathbb{K}$*.*

Teorema 14 ([35]). *O anel de inteiros de* $\mathbb{Q}(\sqrt{d})$ *é dado por:*

(i) $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$, *se* $d \not\equiv 1 \pmod 4$

(ii) $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, *se* $d \equiv 1 \pmod 4$

Teorema 15 ([35]). *Se* $\mathbb{K}$ *é um corpo de números, então* $\mathbb{K} = \mathbb{Q}(\theta)$ *para algum inteiro algébrico* $\theta \in \mathcal{O}_{\mathbb{K}}$.

Do que foi exposto concluímos que sempre podemos encontrar um elemento primitivo que é um inteiro algébrico. Consequentemente, o polinômio mínimo $p_\theta(x)$ tem coeficientes em $\mathbb{Z}$.

O anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é de fundamental importância para construção de reticulados algébricos. Dessa forma, vamos caracterizá-lo de maneira mais precisa, isto é, como um $\mathbb{Z}$-módulo (mediante Seção 1.3).

Teorema 16 ([35]). *Seja* $\mathbb{K}$ *um corpo de números de grau* n. *O anel de inteiros* $\mathcal{O}_{\mathbb{K}}$ *forma um* $\mathbb{Z}$*-módulo livre de posto* n.

Definição 44 (Base Integral). *Seja* $\{\omega_i\}_{i=1}^n$ *uma base do* $\mathbb{Z}$*-módulo* $\mathcal{O}_{\mathbb{K}}$. *Dizemos que* $\{\omega_i\}_{i=1}^n$ *é uma base integral de* $\mathbb{K}$.

Exemplo 9. *Observamos do Teorema 14 e da Definição 44 que os conjuntos* $\{1, \sqrt{d}\}$ *e* $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ *são bases integrais do corpo de números* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *quando* $d \not\equiv 1 \pmod 4$ *e* $d \equiv 1 \pmod 4$, *respectivamente.*

Definição 45 ($\mathbb{Q}-$homomorfismo). *Sejam* $\mathbb{K}/\mathbb{Q}$ *e* $\mathbb{L}/\mathbb{Q}$ *duas extensões de corpos. Chamamos* $\varphi : \mathbb{K} \to \mathbb{L}$ *um* $\mathbb{Q}-$*homomorfismo se* φ *é um homomorfismo de anéis que satisfaz* $\varphi(a) = a$ *para todo* $a \in \mathbb{Q}$, *isto é,* φ *fixa* $\mathbb{Q}$.

Vemos na Definição 46 como um corpo de números $\mathbb{K}$ pode ser representado a partir de uma imersão em $\mathbb{C}$.

Definição 46 (Mergulho). *Um* $\mathbb{Q}-$*homomorfismo injetor é chamado um mergulho de* $\mathbb{K}$ *em* $\mathbb{C}$.

Os próximos resultados são de fundamental importância para a construção de reticulados algébricos.

Teorema 17 ([35]). *Seja* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números de grau* n *sobre* $\mathbb{Q}$. *Existem exatamente* n *mergulhos de* $\mathbb{K}$ *em* $\mathbb{C} : \sigma_i : \mathbb{K} \to \mathbb{C}, i = 1, ..., n$ *definidos por* $\sigma_i(\theta) = \theta_i$, *em que* θ_i *são os zeros distintos em* $\mathbb{C}$ *do polinômio mínimo de* θ *sobre* $\mathbb{Q}$.

Definição 47 (Conjugado, Norma e Traço)**.** *Seja $x \in \mathbb{K}$. Os elementos $\sigma_i(x)$ $(i = 1, ..., n)$ são chamados os conjugados de x e*

$$N(x) = \prod_{i=1}^{n} \sigma_i(x), \; Tr(x) = \sum_{i=1}^{n} \sigma_i(x)$$

são chamados, respectivamente, a norma e o traço de x.

Teorema 18 ([35])**.** *Para qualquer $x \in \mathbb{K}$, temos $N(x), Tr(x) \in \mathbb{Q}$. Se $x \in \mathcal{O}_{\mathbb{K}}$, temos $N(x), Tr(x) \in \mathbb{Z}$.*

Exemplo 10. *Seja $x \in \mathbb{Q}(\sqrt{d})$, ou seja, $x = a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$. Como já exposto anteriormente, o polinômio mínimo de $\theta = \sqrt{d}$ é $x^2 - d$, logo pelo Teorema 17 os mergulhos são $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$. Da Definição 47, temos: $N(x) = \sigma_1(x)\sigma_2(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$ e $Tr(x) = \sigma_1(x) + \sigma_2(x) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$.*

Definição 48 (Discriminante)**.** *Seja $\{\omega_i\}_{i=1}^n$ uma base integral de $\mathbb{K}$. O discriminante de $\mathbb{K}$ é definido como $d_{\mathbb{K}} = \det[\sigma_i(\omega_j)_{i,j=1}^n]^2$.*

Pode ser mostrado (mediante [33]) que o discriminante independe da escolha da base.

Teorema 19 ([35])**.** *O discriminante $d_{\mathbb{K}}$ de um corpo de números pertence a $\mathbb{Z}$.*

Para fixar as ideias, exibimos a prova do próximo teorema.

Teorema 20 ([35])**.** *(a) Se $d \not\equiv 1 \pmod 4$, então $\mathbb{Q}(\sqrt{d})$ tem discriminante $4d$. (b) Se $d \equiv 1 \pmod 4$, então $\mathbb{Q}(\sqrt{d})$ tem discriminante d.*

Demonstração. Da Definição 48 e pelo Exemplo 9, temos:

(a)

$$d_{\mathbb{K}} = \left[\det \begin{bmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{bmatrix}\right]^2 = \left[\det \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}\right]^2 = 4d.$$

(b)

$$d_{\mathbb{K}} = \left[\det \begin{bmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{bmatrix}\right]^2 = \left[\det \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix}\right]^2 = d.$$

□

3.2 Construção de Reticulados Algébricos

Nesta seção, fazemos a construção de reticulados algébricos. O que será apresentado aqui difere da bibliografia citada apenas na forma de como escrevemos a matriz de um reticulado, isto é, adotamos a forma coluna para um vetor, em harmonia com o que foi apresentado no Capítulo 2 deste trabalho.

Definição 49 (Assinatura)**.** *Sejam $\mathbb{K}$ um corpo de números de grau n, σ_i $(i = 1, ..., n)$ os n mergulhos de $\mathbb{K}$ em $\mathbb{C}$. Seja r_1 o número de mergulhos com imagem em $\mathbb{R}$, e $2r_2$ o número de mergulhos com imagem em $\mathbb{C}$ de modo que $r_1 + 2r_2 = n$. O par (r_1, r_2) é denominado assinatura de $\mathbb{K}$. Se $r_2 = 0$ temos um corpo de números algébricos totalmente real. Se $r_1 = 0$ temos um corpo de números algébricos totalmente complexo.*

Definição 50 (Homomorfismo Canônico)**.** *Vamos ordenar os $\sigma_i's$ de modo que para todo $x \in \mathbb{K}$, $\sigma_i(x) \in \mathbb{R}$, $1 \leqslant i \leqslant r_1$ e $\sigma_{j+r_2}(x)$ é o complexo conjugado de $\sigma_j(x)$ para $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. A aplicação $\sigma : \mathbb{K} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definida por*

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), \sigma_{r_1+1}(x), ..., \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

é chamada de homomorfismo canônico. Se identificarmos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$, o homomorfismo canônico pode ser reescrito como

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), ..., \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)) \in \mathbb{R}^n$$

onde $\Re$ e $\Im$ denotam as partes real e imaginária respectivamente[1]*.*

A construção de um reticulado algébrico é feita a partir do próximo teorema.

Teorema 21 ([35])**.** *Seja $\mathbb{K}$ um corpo de números com uma base integral $\{\omega_i\}_{i=1}^n$. Os n vetores $v_i = \sigma(\omega_i) \in \mathbb{R}^n$ são linearmente independentes, de modo que definem um reticulado de posto completo $\Lambda = \Lambda(\mathcal{O}_\mathbb{K}) = \sigma(\mathcal{O}_\mathbb{K})$.*

Da Definição 27, temos que o reticulado $\Lambda = \sigma(\mathcal{O}_\mathbb{K})$ pode ser expresso por meio de sua matriz geradora B que é dada explicitamente por:

[1] A *parte real* e a *parte imaginária* de um complexo $z = a + bi$ são dadas respectivamente por $\Re z = a$ e $\Im z = b$.

$$\begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\omega_1) & \sigma_{r_1}(\omega_2) & \cdots & \sigma_{r_1}(\omega_n) \\ \Re\sigma_{r_1+1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_2) & \cdots & \Re\sigma_{r_1+1}(\omega_n) \\ \Im\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_2) & \cdots & \Im\sigma_{r_1+1}(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \Re\sigma_{r_1+r_2}(\omega_1) & \Re\sigma_{r_1+r_2}(\omega_2) & \cdots & \Re\sigma_{r_1+r_2}(\omega_n) \\ \Im\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_2) & \cdots & \Im\sigma_{r_1+r_2}(\omega_n) \end{bmatrix} \tag{3.1}$$

onde os vetores $v_i = \sigma(\omega_i)$ são as colunas de B.

Teorema 22 ([33])**.** *Seja* $\mathbb{K}$ *um corpo de números e* $d_{\mathbb{K}}$ *o discriminante de* $\mathbb{K}$*. O volume do reticulado* $\Lambda = \Lambda(\mathcal{O}_{\mathbb{K}}) = \sigma(\mathcal{O}_{\mathbb{K}})$ *é dado por*

$$V(\Lambda) = |\det(B)| = 2^{-r_2}\sqrt{|d_{\mathbb{K}}|} \tag{3.2}$$

onde B *é matriz dada em (3.1). Consequentemente,*

$$\det(\Lambda) = 2^{-2r_2}|d_{\mathbb{K}}|.$$

Do que foi exposto na Seção 2.2 deste trabalho, formalizamos a Definição 51.

Definição 51 (Diversidade)**.** *Um reticulado* Λ *tem diversidade* $L \leqslant n$ *se* L *é o número máximo tal que qualquer vetor* $\mathbf{0} \neq \mathbf{y} \in \Lambda$ *tenha pelo menos* L *coordenadas diferentes de zero.*

Teorema 23 ([9])**.** *Reticulados algébricos possuem diversidade* $L = r_1 + r_2$*.*

Teorema 24 ([32])**.** *Reticulados algébricos construídos sobre corpos de números totalmente reais tem diversidade máxima* $L = n$*.*

Demonstração. A prova é uma consequência imediata do Teorema 23. Uma vez que $(r_1, r_2) = (n, 0)$, temos que $L = r_1 + r_2 = n + 0 = n$. □

Reticulados algébricos construídos sobre corpos de números totalmente reais terão matriz geradora (mediante (3.1)) dada por:

$$\begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{bmatrix} \tag{3.3}$$

Exemplo 11 (Reticulados via Corpos Quadráticos)**.** *Considere a família de reticulados algébricos* $\Lambda = \Lambda(\mathcal{O}_{\mathbb{K}}) = \sigma(\mathcal{O}_{\mathbb{K}})$*, onde* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$*. Essa família pode ser dividida em quatro classes de reticulados. Observamos que se* $d > 0$ *segue do Exemplo 10 que* $\sigma_1(\sqrt{d}) = \sqrt{d}$ *e* $\sigma_2(\sqrt{d}) = -\sqrt{d}$*, logo pelo Teorema 24, segue que* Λ *tem diversidade máxima, portanto, temos as classes* Λ_1 *e* Λ_2 *a seguir:*

(a) Se $d \not\equiv 1 \pmod 4$*, segue de (3.3) que* $\Lambda_1 = \Lambda_1(d)$ *tem matriz geradora dada por*

$$B = \begin{bmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{bmatrix} = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}. \tag{3.4}$$

Neste caso, calculando o volume do reticulado pela fórmula (3.2), ou pelo cálculo direto do determinante da última matriz temos $V(\Lambda_1) = |\det B| = 2\sqrt{d}$*.*

(b) Se $d \equiv 1 \pmod 4$*, segue de (3.3), que* $\Lambda_2 = \Lambda_2(d)$ *tem matriz geradora dada por*

$$B = \begin{bmatrix} \sigma_1(1) & \sigma_1\left(\dfrac{1+\sqrt{d}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\dfrac{1+\sqrt{d}}{2}\right) \end{bmatrix} = \begin{bmatrix} 1 & \dfrac{1+\sqrt{d}}{2} \\ 1 & \dfrac{1-\sqrt{d}}{2} \end{bmatrix}. \tag{3.5}$$

Neste caso, o volume do reticulado é dado por $V(\Lambda_2) = |\det B| = \sqrt{d}$*.*

Observamos que se $d < 0$*, segue do Exemplo 10, que* $\sigma_1(\sqrt{d}) = i\sqrt{l}$ *e* $\sigma_2(\sqrt{d}) = -i\sqrt{l}$*, onde* $d = -l$*, portanto a assinatura de* $\mathbb{K}$ *é dada por* $(r_1, r_2) = (0, 1)$*. Logo, pelo Teorema 23, segue que* Λ *tem diversidade* $L = 1$*, portanto, temos as classes* Λ_3 *e* Λ_4 *a seguir:*

(c) Se $-l \not\equiv 1 \pmod 4$*, segue de (3.1), que* $\Lambda_3 = \Lambda_3(l)$ *tem matriz geradora dada por*

$$B = \begin{bmatrix} \Re\sigma_1(1) & \Re\sigma_1(i\sqrt{l}) \\ \Im\sigma_1(1) & \Im\sigma_1(i\sqrt{l}) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{l} \end{bmatrix}. \tag{3.6}$$

Neste caso, o volume do reticulado é dado por $V(\Lambda_3) = |\det B| = \sqrt{l}$*.*

(d) Se $-l \equiv 1 \pmod 4$*, segue de (3.1), que* $\Lambda_4 = \Lambda_4(l)$ *tem matriz geradora dada por*

$$B = \begin{bmatrix} \Re\sigma_1(1) & \Re\sigma_1\left(\frac{1+i\sqrt{l}}{2}\right) \\ \Im\sigma_1(1) & \Im\sigma_1\left(\frac{1+i\sqrt{l}}{2}\right) \end{bmatrix} = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{l}}{2} \end{bmatrix}. \tag{3.7}$$

Neste caso, o volume do reticulado é dado por $V(\Lambda_4) = |\det B| = \sqrt{l}/2$.

Até o momento temos construído reticulados algébricos a partir do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números $\mathbb{K}$. Segundo o Teorema 16, $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Por outro lado, existem outros subconjuntos de $\mathcal{O}_{\mathbb{K}}$ que também têm esta estrutura de $\mathbb{Z}$-módulo livre de posto n (mediante [35]). Esses são os ideais de $\mathcal{O}_{\mathbb{K}}$ e sobre eles também construímos reticulados algébricos.

Teorema 25 ([35])**.** *Todo ideal* $\mathcal{I} \neq \{0\}$ *de* $\mathcal{O}_{\mathbb{K}}$ *tem* $\mathbb{Z}$*-base* $\{v_i\}_{i=1}^n$*, em que* n *é o grau de* $\mathbb{K}$.

Segundo [32], os Teoremas 21 e 23 podem ser estendidos quando substituímos uma base de $\mathcal{O}_{\mathbb{K}}$ por uma base de um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$, e ainda, um reticulado algébrico Λ' construído a partir de $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ fornece um subreticulado (mediante Definição 36) Λ construído de $\mathcal{O}_{\mathbb{K}}$.

Reticulado ideal será definido a seguir. No que segue, $\mathbb{K}$ é um corpo de números totalmente real de grau n, $\{\sigma_i\}_{i=1}^n$ denotam os n mergulhos de $\mathbb{K}$ em $\mathbb{R}$.

Definição 52 (Reticulado Ideal)**.** *Um reticulado ideal é um reticulado* $\Lambda = (\mathcal{I}, q_\alpha)$ *em que* $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ *é um ideal de* $\mathcal{O}_{\mathbb{K}}$ *e* $q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Q}$, $q_\alpha(x, y) = Tr(\alpha xy)$*, para todo* $x, y \in \mathcal{I}$*, em que* $\alpha \in \mathbb{K}$ *é totalmente positivo (ie,* $\sigma_i(\alpha) > 0$ *para todo* $i = 1, ..., n$*).*

Definição 53 (Homomorfismo Torcido)**.** *Seja* $\mathcal{I}$ *um ideal de* $\mathcal{O}_{\mathbb{K}}$*. O homomorfismo torcido é dado por* $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ *tal que* $\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_n}\sigma_n(x))$*, em que* $\alpha \in \mathbb{K}$ *é totalmente positivo e* $\alpha_i = \sigma_i(\alpha)$, $i = 1, ..., n$.

Seja $\{\omega_i\}_{i=1}^n$ uma $\mathbb{Z}$-base do reticulado ideal $\Lambda = \sigma_\alpha(\mathcal{I})$ conforme as Definições 52 e 53. A matriz geradora de Λ é dada por:

$$B = \begin{bmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_1}\sigma_1(\omega_2) & \cdots & \sqrt{\alpha_1}\sigma_1(\omega_n) \\ \sqrt{\alpha_2}\sigma_2(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_2) & \cdots & \sqrt{\alpha_2}\sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_n}\sigma_n(\omega_1) & \sqrt{\alpha_n}\sigma_n(\omega_2) & \cdots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{bmatrix}. \tag{3.8}$$

Observamos que $B = [b_{ij}]$, em que $b_{ij} = \sqrt{\alpha_i}\sigma_i(\omega_j)$, logo sua correspondente matriz de Gram será $G = B^tB = [g_{ij}]$, em que

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{n} b_{ki}b_{kj} \\ &= \sum_{k=1}^{n} \sqrt{\alpha_k}\sigma_k(\omega_i)\sqrt{\alpha_k}\sigma_k(\omega_j) \\ &= \sum_{k=1}^{n} \sigma_k(\alpha\omega_i\omega_j) \\ &= q_\alpha(\omega_i, \omega_j). \end{aligned} \tag{3.9}$$

Do que foi exposto na Seção 2.2 deste trabalho, formalizamos a Definição 54.

Definição 54 (Distância Produto Ínfima)**.** *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto completo com diversidade máxima, ie, $L = n$. A distância produto ínfima*[2] *de Λ é definida como*

$$d_{p,\inf}(\Lambda) = \inf_{\mathbf{0}\neq\mathbf{x}\in\Lambda} d_p^{(n)}(\mathbf{0}, \mathbf{x}) = \inf_{\mathbf{0}\neq\mathbf{x}\in\Lambda} \prod_{i=1}^{n} |x_i|.$$

Teorema 26 ([32])**.** *Seja $\mathcal{I}$ um ideal principal de $\mathcal{O}_\mathbb{K}$ e $\Lambda = (\mathcal{I}, q_\alpha)$ um reticulado. A distância produto mínima de Λ é*

$$d_{p,\min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_\mathbb{K}}}.$$

Apresentamos, a seguir, a *construção ciclotômica* que permitiu encontrar versões rotacionadas do reticulado $\mathbb{Z}^n$ com maior distância produto mínima conhecida na literatura, conforme podemos ver em [40].

A construção ciclotômica nos permitirá obter um reticulado equivalente (mediante Definição 35) ao reticulado $\mathbb{Z}^n$ para $n = (p-1)/2$, onde $p \geqslant 5$ é um primo.

Definição 55 (Corpo Ciclotômico)**.** *Um corpo ciclotômico é um corpo de números $\mathbb{K} = \mathbb{Q}(\zeta_m)$ gerado pela m-ésima raiz da unidade $\zeta_m = e^{2i\pi/m}$.*

Definição 56 (Subcorpo Real Maximal)**.** *Seja $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ um subcorpo de $\mathbb{Q}(\zeta_p)$ gerado por $\zeta_p + \zeta_p^{-1} = 2\cos(2\pi/p)$, em que $p \geqslant 5$ é um número primo. Uma vez que $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = 2$ e $\mathbb{K}$ é totalmente real, ele será chamado o subcorpo real maximal de um corpo ciclotômico.*

Em relação ao subcorpo real maximal temos: $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = (p-1)/2$ e ainda

$$d_\mathbb{K} = p^{\frac{p-3}{2}}, \tag{3.10}$$

[2] Especificamente, poderíamos definir distância produto mínima, isto é, substituindo o inf onde houver por min . Utilizamos a distância produto mínima quando há certeza que o mínimo é alcançado.

conforme pode ser visto em [38].

Conforme vemos em [41], o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ tem uma base integral

$$\{e_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^n \tag{3.11}$$

e os n mergulhos de $\mathbb{K}$ em $\mathbb{C}$ dados por

$$\sigma_k(e_j) = \zeta_p^{kj} + \zeta_p^{-kj} = 2\cos\left(\frac{2\pi kj}{p}\right) \tag{3.12}$$

Teorema 27 ([32])**.** *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_p+\zeta_p^{-1})$. *Então* $\Lambda = (\mathcal{O}_{\mathbb{K}}, \frac{1}{p}q_\alpha)$, *onde* $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$ *e* $q_\alpha(x,y) = Tr(\alpha xy)$, *é equivalente ao reticulado* $\mathbb{Z}^n$.

Na demonstração do Teorema 27 que é feita em detalhes em [32] verifica-se que em relação à base $\{e'_j\}_{j=1}^n$, onde $e'_n = e_n$, $e'_j = e_j + e'_{j+1}$ e e_j é dado em (3.11), tem-se que $\frac{1}{p}q_\alpha(e'_i, e'_j)$ é a matriz identidade de ordem n. Dessa forma, escrevendo $R = [r_{ij}]$, onde $r_{ij} = \frac{1}{\sqrt{p}}\sqrt{\alpha_i}\sigma_i(e'_j)$, tem-se por (3.9) que R é ortogonal, portanto, é uma *matriz geradora do reticulado* $\mathbb{Z}^n$ *em uma versão rotacionada.*

Observamos que R pode ser escrita da forma

$$R = \frac{1}{\sqrt{p}}D\Sigma T \tag{3.13}$$

onde D, Σ e T são matrizes quadradas de ordem n tais que $D = \text{diag}(\sqrt{\alpha_1}, ..., \sqrt{\alpha_n})$, $\Sigma = [\sigma_{ij}]$, $\sigma_{ij} = \sigma_i(e_j)$ e $T = [t_{ij}]$,

$$t_{ij} = \begin{cases} 1, & \text{se} \quad i \geqslant j \\ 0, & \text{se} \quad i < j. \end{cases}$$

Teorema 28 ([32])**.** *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. *A distância produto mínima do reticulado* $\Lambda = (\mathcal{O}_{\mathbb{K}}, \frac{1}{p}q_\alpha)$, *em que* $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$ *e* $q_\alpha(x,y) = Tr(\alpha xy)$, *é*

$$d_{p,\min}(\Lambda) = p^{-\frac{n-1}{2}}.$$

Demonstração. A prova é imediata, basta ver que $\det(\Lambda) = 1$, usar o Teorema 26 e a igualdade (3.10). □

A seguir, apresentamos construções explícitas resultantes do Teorema 28 e que serão usadas no decorrer do trabalho.

Exemplo 12. *Para encontrarmos uma matriz geradora* R *da versão rotacionada do* $\mathbb{Z}^2$, *temos que considerar o corpo de números* $\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. *Observamos que as matrizes* D, Σ *e* T, *conforme a igualdade (3.13), são dadas por:*

$$D = \begin{bmatrix} \sqrt{\alpha_1} & 0 \\ 0 & \sqrt{\alpha_2} \end{bmatrix} = \begin{bmatrix} \sqrt{2-2\cos(2\pi/5)} & 0 \\ 0 & \sqrt{2-2\cos(4\pi/5)} \end{bmatrix},$$

$$\Sigma = \begin{bmatrix} \sigma_1(e_1) & \sigma_1(e_2) \\ \sigma_2(e_1) & \sigma_2(e_2) \end{bmatrix} = \begin{bmatrix} 2\cos(2\pi/5) & 2\cos(4\pi/5) \\ 2\cos(4\pi/5) & 2\cos(8\pi/5) \end{bmatrix},$$

$$T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Logo, temos que

$$R = \frac{1}{\sqrt{5}} D\Sigma T = \begin{bmatrix} -0.525731 & -0.850651 \\ -0.850651 & 0.525731 \end{bmatrix}. \tag{3.14}$$

Do Teorema 28, temos que $d_{p,\min}(\mathbb{Z}^2) = \frac{1}{\sqrt{5}}$.

Exemplo 13. *Para encontrarmos a matriz geradora R da versão rotacionada do $\mathbb{Z}^3$, temos que considerar o corpo de números $\mathbb{K} = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Observamos que as matrizes D, Σ e T conforme (3.13) são dadas por:*

$$D = \begin{bmatrix} \sqrt{\alpha_1} & 0 & 0 \\ 0 & \sqrt{\alpha_2} & 0 \\ 0 & 0 & \sqrt{\alpha_3} \end{bmatrix} = \begin{bmatrix} \sqrt{2-2\cos(2\pi/7)} & 0 & 0 \\ 0 & \sqrt{2-2\cos(4\pi/7)} & 0 \\ 0 & 0 & \sqrt{2-2\cos(6\pi/7)} \end{bmatrix},$$

$$\Sigma = \begin{bmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \sigma_1(e_3) \\ \sigma_2(e_1) & \sigma_2(e_2) & \sigma_2(e_3) \\ \sigma_3(e_1) & \sigma_3(e_2) & \sigma_3(e_3) \end{bmatrix} = \begin{bmatrix} 2\cos(2\pi/7) & 2\cos(4\pi/7) & 2\cos(6\pi/7) \\ 2\cos(4\pi/7) & 2\cos(8\pi/7) & 2\cos(12\pi/7) \\ 2\cos(6\pi/7) & 2\cos(12\pi/7) & 2\cos(18\pi/7) \end{bmatrix},$$

$$T = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Logo, temos que

$$R = \frac{1}{\sqrt{7}} D\Sigma T = \begin{bmatrix} -0.327985 & -0.736976 & -0.591009 \\ -0.591009 & -0.327985 & 0.736976 \\ -0.736976 & 0.591009 & -0.327985 \end{bmatrix}. \tag{3.15}$$

Do Teorema 28, temos que $d_{p,\min}(\mathbb{Z}^3) = \frac{1}{7}$.

Exemplo 14. *Para encontrarmos uma matriz geradora R da versão rotacionada do $\mathbb{Z}^5$, temos que considerar o corpo de números $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$. As matrizes D, Σ e T são*

encontradas de modo análogo ao que foi feito nos Exemplos 12 e 13, logo de (3.13) temos que

$$R = \begin{bmatrix} -0.169891 & -0.455734 & -0.596885 & -0.548529 & -0.326019 \\ -0.326019 & -0.596885 & -0.169891 & 0.455734 & 0.548529 \\ -0.455734 & -0.326019 & 0.548529 & 0.169891 & -0.596885 \\ -0.548529 & 0.169891 & 0.326019 & -0.596885 & 0.455734 \\ -0.596885 & 0.548529 & -0.455734 & 0.326019 & -0.169891 \end{bmatrix}. \tag{3.16}$$

Do Teorema 28, temos que $d_{p,\min}(\mathbb{Z}^5) = \dfrac{1}{11^2}$.

Exemplo 15. *Para encontrarmos uma matriz geradora R da versão rotacionada do $\mathbb{Z}^8$, temos que considerar o corpo de números $\mathbb{K} = \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$. As matrizes D, Σ e T são encontradas de modo análogo ao que foi feito nos Exemplos 12 e 13, logo de (3.13), temos que R é dada por*

$$\begin{bmatrix} -0.0891316 & -0.255357 & -0.387095 & -0.466554 & -0.483002 & -0.434218 & -0.32679 & -0.175228 \\ -0.175228 & -0.434218 & -0.466554 & -0.255357 & 0.0891316 & 0.387095 & 0.483002 & 0.32679 \\ -0.255357 & -0.483002 & -0.175228 & 0.32679 & 0.466554 & 0.0891316 & -0.387095 & -0.434218 \\ -0.32679 & -0.387095 & 0.255357 & 0.434218 & -0.175228 & -0.466554 & 0.0891316 & 0.483002 \\ -0.387095 & -0.175228 & 0.483002 & -0.0891316 & -0.434218 & 0.32679 & 0.255357 & -0.466554 \\ -0.434218 & 0.0891316 & 0.32679 & -0.483002 & 0.255357 & 0.175228 & -0.466554 & 0.387095 \\ -0.466554 & 0.32679 & -0.0891316 & -0.175228 & 0.387095 & -0.483002 & 0.434218 & -0.255357 \\ -0.483002 & 0.466554 & -0.434218 & 0.387095 & -0.32679 & 0.255357 & -0.175228 & 0.0891316 \end{bmatrix}.$$

Do Teorema 28, temos que $d_{p,\min}(\mathbb{Z}^8) = \dfrac{1}{17^{7/2}}$.

Segundo podemos ver em [22] a construção de reticulados algébricos via homomorfismo torcido pode ser feita em um $\mathbb{Z}$-módulo livre de posto n qualquer, ou seja, não necessariamente é preciso tomarmos um ideal de $\mathcal{O}_{\mathbb{K}}$. Dessa forma, a Definição 53 continua válida para um $\mathbb{Z}$-módulo livre $I \subseteq \mathcal{O}_{\mathbb{K}}$ ao invés de um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Sendo assim, tomando α totalmente positivo (mediante Definição 52) e $\{\omega_i\}_{i=1}^n$ uma $\mathbb{Z}$-base de I, temos que $\sigma_\alpha(I)$ é um reticulado com matriz geradora dada por (3.8), que ainda, segundo [22] possui diversidade máxima.

Teorema 29 ([22])**.** *Seja I um $\mathbb{Z}-$módulo de posto n e $\Lambda = (I, q_\alpha)$ um reticulado. A distância produto mínima de Λ é*

$$d_{p,\min}(\Lambda) = \sqrt{N(\alpha)} \min_{0 \neq y \in I} |N(y)|.$$

Para o próximo resultado consideramos o reticulado que denotamos por $\Lambda = \dfrac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ cuja matriz geradora R é dada por (3.13). Desta forma, ainda temos $n = (p-1)/2$, onde $p \geqslant 5$ é um primo. Uma versão análoga ao Teorema 30 é encontrado em [22] e aqui enunciamos com uma $\mathbb{Z}$-base diferente para I, uma vez que consideramos a base do D_n dada no Exemplo 4.

Teorema 30 ([22]). *Considere o $\mathbb{Z}$-módulo $I \subseteq \mathcal{O}_{\mathbb{K}}$ com $\mathbb{Z}$-base*

$$\left\{ f_1 = 2\sum_{i=1}^{n} e_i, f_2 = e_1 + 2\sum_{i=2}^{n} e_i, f_3 = e_1 + e_2 + 2\sum_{i=3}^{n} e_i, ..., f_n = e_1 + e_2 + ... + e_{n-1} + 2e_n \right\} \tag{3.17}$$

em que e_i é dado conforme em (3.11). Temos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$, em que $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$ é um D_n rotacionado.

Demonstração. Aplicando a matriz de rotação R à matriz E geradora do reticulado D_n (mediante Exemplo 4), temos que

$$\begin{aligned} RE &= \frac{1}{\sqrt{p}} D\Sigma T E = \frac{1}{\sqrt{p}} D \begin{bmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_n) \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 0 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix} E \\ &= \frac{1}{\sqrt{p}} D \begin{bmatrix} \sigma_1(e_1 + e_2 + ... + e_n) & \cdots & \sigma_1(e_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(e_1 + e_2 + ... + e_n) & \cdots & \sigma_n(e_n) \end{bmatrix} E \\ &= \frac{1}{\sqrt{p}} D \begin{bmatrix} \sigma_1(f_1) & \sigma_1(f_2) & \cdots & \sigma_1(f_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(f_1) & \sigma_n(f_2) & \cdots & \sigma_n(f_n) \end{bmatrix}. \end{aligned}$$

Assim, observamos que a matriz geradora para o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$ é dada por

$$RE = R \begin{bmatrix} 2 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}. \tag{3.18}$$

Como $(RE)^t(RE) = E^tE$ que é uma matriz de Gram do reticulado D_n, temos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$ é um D_n rotacionado. □

Teorema 31 ([22]). *Seja $I \subseteq \mathcal{O}_{\mathbb{K}}$ o $\mathbb{Z}$-módulo com $\mathbb{Z}$-base dada por (3.17), em que e_i é descrito como em (3.11). Temos que o reticulado $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(I)$, onde $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$, tem distância produto mínima dada por*

$$d_{p,\min}(\Lambda) = p^{-\frac{n-1}{2}}.$$

Demonstração. Vemos em [22] que $N(\alpha) = p$ e que $|N(e_1)| = 1$; portanto, pelo Teorema 29, temos que $d_{p,\min}\sigma_\alpha(I) = \sqrt{N(\alpha)} \min\limits_{0\neq y\in I} |N(y)| = \sqrt{p}$, pois $\min\limits_{0\neq y\in I} |N(y)| \geqslant 1$ e $f_1 - f_2 = e_1 \in I$. Assim,

$$d_{p,\min}(\Lambda) = d_{p,\min}\left(\frac{1}{\sqrt{p}}\sigma_\alpha(I)\right) = \frac{1}{(\sqrt{p})^n} d_{p,\min}\left(\sigma_\alpha(I)\right) = \frac{1}{(\sqrt{p})^n}\sqrt{p} = p^{-\frac{n-1}{2}}.$$

□

A fim de compararmos reticulados em uma mesma dimensão no que se refere à distância produto, é necessário que se faça mais duas definições.

Definição 57 (Distância Produto Ínfima Relativa)**.** *Seja μ a norma mínima de um reticulado Λ. A distância produto ínfima relativa de Λ, denotada por $d_{p,\mathrm{rel}}(\Lambda)$ é a distância produto ínfima*[3] *do reticulado escalado $\frac{1}{\mu}\Lambda$.*

Definição 58 (Distância Produto Ínfima Normalizada)**.** *A distância produto ínfima normalizada de um reticulado Λ, denotada por $d_{p,\mathrm{norm}}(\Lambda)$, é a distância produto ínfima*[4] *da versão escalada $\frac{1}{\sqrt[2n]{\det(\Lambda)}}\Lambda$, ou seja, $d_{p,\mathrm{norm}}(\Lambda) = \frac{1}{\sqrt{\det(\Lambda)}} d_{p,\mathrm{inf}}(\Lambda)$.*

Nos trabalhos mais recentes têm-se usado a distância produto mínima normalizada ao invés da relativa, como podemos observar em [23] e em [37].

Observação 3. *Uma vez que a norma mínima do $\mathbb{Z}^n$ é $\mu = 1$ e que $\det(\mathbb{Z}^n) = 1$, segue que $d_{p,\min}(\mathbb{Z}^n) = d_{p,\mathrm{rel}}(\mathbb{Z}^n) = d_{p,\mathrm{norm}}(\mathbb{Z}^n)$.*

Exemplo 16 (Distância Produto de Reticulados via Corpos Quadráticos Totalmente Reais)**.** *Considere a família de reticulados algébricos $\Lambda = \Lambda(\mathcal{O}_\mathbb{K}) = \sigma(\mathcal{O}_\mathbb{K})$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ com $d > 0$, discutida no Exemplo 11. Neste caso, $\mathbb{K}$ é totalmente real e tomando $\alpha = 1$ vemos que o homormofismo torcido é canônico (mediante Definições 50 e 53) de modo que o Teorema 26 pode ser aplicado neste caso para o cálculo da distância produto mínima. Dessa forma temos:*

(a) Se $d \not\equiv 1 \pmod 4$, então $\{\mathbf{v}_1 = (1,1), \mathbf{v}_2 = (\sqrt{d}, -\sqrt{d})\}$ é uma base de Λ_1 de modo que sua norma mínima é $\mu = ||\mathbf{v}_1|| = \sqrt{2}$ (mediante Observação 2). Das Definições 57 e 58, temos que

$$d_{p,\mathrm{rel}}(\Lambda_1) = \frac{1}{\mu^2} d_{p,\min}(\Lambda_1) = \frac{1}{(\sqrt{2})^2}\cdot 1 = \frac{1}{2}$$

e

$$d_{p,\mathrm{norm}}(\Lambda_1) = \frac{1}{V(\Lambda_1)} d_{p,\min}(\Lambda_1) = \frac{1}{2\sqrt{d}}\cdot 1 = \frac{1}{2\sqrt{d}}.$$

[3] Se considerarmos aqui a "distância produto mínima", naturalmente teremos a definição de *distância produto mínima relativa.*

[4] Se considerarmos aqui a "distância produto mínima", naturalmente teremos a definição de *distância produto mínima normalizada.*

(b) Se $d \equiv 1 \pmod 4$ então $\{\mathbf{v}_1 = (1,1), \mathbf{v}_2 = ((1+\sqrt{d})/2, (1-\sqrt{d})/2)\}$ é uma base de Λ_2 de modo que sua norma mínima é $\mu = ||\mathbf{v}_1|| = \sqrt{2}$ (mediante Observação 2). Das Definições 57 e 58 temos que

$$d_{p,\text{rel}}(\Lambda_2) = \frac{1}{\mu^2} d_{p,\min}(\Lambda_2) = \frac{1}{(\sqrt{2})^2} \cdot 1 = \frac{1}{2}$$

e

$$d_{p,\text{norm}}(\Lambda_2) = \frac{1}{V(\Lambda_2)} d_{p,\min}(\Lambda_2) = \frac{1}{\sqrt{d}} \cdot 1 = \frac{1}{\sqrt{d}}.$$

Finalizamos essa seção com as construções, decorrentes do Teorema 30, das versões rotacionadas dos reticulados D_3 (FCC), D_5 e D_8 exibindo suas distâncias produtos.

Exemplo 17. *Para encontrarmos uma matriz geradora F da versão rotacionada do FCC, podemos efetuar o produto RE (mediante (3.18)), onde $n = 3$ e R é a matriz do Exemplo 13. Temos:*

$$\begin{aligned} F = RE &= \begin{bmatrix} -0.327985 & -0.736976 & -0.591009 \\ -0.591009 & -0.327985 & 0.736976 \\ -0.736976 & 0.591009 & -0.327985 \end{bmatrix} \begin{bmatrix} 2 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} -0.655971 & -1.06496 & -0.918994 \\ -1.18202 & -0.918994 & 0.145967 \\ -1.47395 & -0.145967 & -1.06496 \end{bmatrix} \end{aligned} \tag{3.19}$$

Do Teorema 31, temos que $d_{p,\min}(FCC) = \frac{1}{7}$. Das Definições (57) e (58), temos:

$$d_{p,\text{rel}}(FCC) = \frac{1}{\mu^3} d_{p,\min}(FCC) = \frac{1}{(\sqrt{2})^3} \cdot \frac{1}{7} = \frac{1}{7\sqrt{2^3}}$$

e

$$d_{p,\text{norm}}(FCC) = \frac{1}{V(FCC)} d_{p,\min}(FCC) = \frac{1}{2} \cdot \frac{1}{7} = \frac{1}{14}.$$

Exemplo 18. *Para encontrarmos uma matriz geradora F da versão rotacionada do D_5, podemos efetuar o produto RE (mediante (3.18)), onde $n = 5$ e R é a matriz do Exemplo 14. Temos:*

$$F = \begin{bmatrix} -0.339782 & -0.625625 & -0.766776 & -0.71842 & -0.49591 \\ -0.652037 & -0.922903 & -0.49591 & 0.129715 & 0.22251 \\ -0.911468 & -0.781753 & 0.0927946 & -0.285843 & -1.05262 \\ -1.09706 & -0.378638 & -0.22251 & -1.14541 & -0.0927946 \\ -1.19377 & -0.0483561 & -1.05262 & -0.270866 & -0.766776 \end{bmatrix} \tag{3.20}$$

Do Teorema 31, temos que $d_{p,\min}(D_5) = \frac{1}{11^2}$. Das Definições (57) e (58), temos:

$$d_{p,\text{rel}}(D_5) = \frac{1}{\mu^5} d_{p,\min}(D_5) = \frac{1}{(\sqrt{2})^5} \cdot \frac{1}{11^2} = \frac{1}{121\sqrt{2^5}}$$

e

$$d_{p,\mathrm{norm}}(D_5) = \frac{1}{V(D_5)} d_{p,\min}(D_5) = \frac{1}{2} \cdot \frac{1}{11^2} = \frac{1}{242}.$$

Exemplo 19. *Para encontrarmos uma matriz geradora F da versão rotacionada do D_8, podemos efetuar o produto RE (mediante (3.18)), onde $n = 8$ e R é a matriz do Exemplo 15. Temos que F é dada por:*

$$\begin{bmatrix}
-0.178263 & -0.344489 & -0.476227 & -0.555686 & -0.572134 & -0.52335 & -0.415922 & -0.26436 \\
-0.350456 & -0.609446 & -0.641782 & -0.430585 & -0.0860963 & 0.211867 & 0.307774 & 0.151562 \\
-0.510714 & -0.738359 & -0.430585 & 0.0714333 & 0.211197 & -0.166225 & -0.642452 & -0.689575 \\
-0.653581 & -0.713886 & -0.0714333 & 0.107428 & -0.502018 & -0.793344 & -0.237659 & 0.156212 \\
-0.77419 & -0.562323 & 0.0959068 & -0.476227 & -0.821313 & -0.0603048 & -0.131738 & -0.853649 \\
-0.868436 & -0.345086 & -0.107428 & -0.91722 & -0.178861 & -0.25899 & -0.900772 & -0.0471228 \\
-0.933108 & -0.139764 & -0.555686 & -0.641782 & -0.0794588 & -0.949556 & -0.032336 & -0.721911 \\
-0.966004 & -0.0164481 & -0.91722 & -0.0959068 & -0.809792 & -0.227645 & -0.65823 & -0.39387
\end{bmatrix}$$

Do Teorema 31, temos que $d_{p,\min}(D_8) = \frac{1}{17^{7/2}}$. Das Definições (57) e (58), temos:

$$d_{p,\mathrm{rel}}(D_8) = \frac{1}{\mu^8} d_{p,\min}(D_8) = \frac{1}{(\sqrt{2})^8} \cdot \frac{1}{17^{7/2}} = \frac{1}{17^{7/2} \cdot 2^4}$$

e

$$d_{p,\mathrm{norm}}(D_8) = \frac{1}{V(D_8)} d_{p,\min}(D_8) = \frac{1}{2} \cdot \frac{1}{17^{7/2}} = \frac{1}{2 \cdot 17^{7/2}}.$$

4 Reticulados Rotacionados via Complexos

Neste capítulo, apresentamos as primeiras contribuições deste trabalho que são referentes a reticulados bidimensionais.

Construímos, via números complexos, as versões rotacionadas do reticulado $\mathbb{Z}^2$ e determinamos qual tem a maior distância produto mínima. Mostramos que o reticulado algébrico descrito no Capítulo 3 que tem a mesma densidade é uma reflexão específica da rotação "ótima", o que possibilita uma descrição geométrica do reticulado algébrico, o que não é feito nas referências citadas nas construções algébricas.

Estudamos, a partir dos complexos, uma família de reticulados bem arredondados, uma família de reticulados quadráticos apresentada no Capítulo 3 e uma família de reticulados ortogonais. Sob certas condições exibimos as distâncias produtos de algumas classes de reticulados dessas famílias.

O programa usado para os cálculos simbólicos e plotagem dos gráficos foi o *Wolfram Mathematica* em sua versão 12.3 [43].

4.1 Reticulados Congruentes em $\mathbb{R}^2$

Nesta seção, iremos estudar os reticulados congruentes a um reticulado $\Lambda \subset \mathbb{R}^2$.

Da Definição 35 decorre que se Λ_1 e Λ_2 são reticulados congruentes com matrizes geradoras dadas por B_1 e B_2, respectivamente, então existe uma matriz ortogonal Q tal que $B_1 = QB_2$. Em [18] vemos que toda matriz ortogonal em $\mathbb{R}^2$ é de uma das formas

$$R = \begin{bmatrix} \cos(\theta) & -\text{sen}(\theta) \\ \text{sen}(\theta) & \cos(\theta) \end{bmatrix} \text{ ou } R' = \begin{bmatrix} \cos(\theta) & \text{sen}(\theta) \\ \text{sen}(\theta) & -\cos(\theta) \end{bmatrix},$$

em que a primeira representa uma rotação do plano em torno da origem de ângulo θ e a segunda uma reflexão através de uma reta que passa pela origem e faz um ângulo de $\theta/2$ com o eixo das abscissas.

Escrevendo

$$S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tag{4.1}$$

observamos que um reticulado $\Lambda \subset \mathbb{R}^2$ com matriz geradora dada por B e o reticulado $\tilde{\Lambda}$ com matriz geradora dada por SB têm a mesma norma mínima e a mesma distância produto mínima que são dadas por

$$\mu = \tilde{\mu} = \min_{(k_1,k_2)\neq(0,0)} \sqrt{(ak_1 + bk_2)^2 + (ck_1 + dk_2)^2}$$

e

$$d_{p,\min}(\Lambda) = d_{p,\min}(\tilde{\Lambda}) = \min_{(k_1,k_2)\neq(0,0)} |(ak_1 + bk_2)(ck_1 + dk_2)|,$$

em que $(k_1, k_2) \in \mathbb{Z}^2$. Assim, os reticulados Λ e $\tilde{\Lambda}$ têm também as mesmas distâncias produtos mínimas relativas e a mesmas distâncias produtos mínimas normalizadas.

Por outro lado,

$$SR' = \begin{bmatrix} \cos\left(\frac{\pi}{2} - \theta\right) & -\text{sen}\left(\frac{\pi}{2} - \theta\right) \\ \text{sen}\left(\frac{\pi}{2} - \theta\right) & \cos\left(\frac{\pi}{2} - \theta\right) \end{bmatrix} = L,$$

em que L representa uma rotação do plano em torno da origem de ângulo $\pi/2 - \theta$.

Dessa forma, se uma matriz M gera um reticulado bidimensional com diversidade máxima, então os reticulados gerados por $R'M$ e $S(R'M)$ têm as mesmas distância produtos (mínimas, relativas ou normalizadas). Como $SR'M = LM$, segue que os reticulados gerados por $R'M$ e LM têm as mesmas distâncias produtos mínimas (relativas ou normalizadas). Registramos este resultado na Observação 4 a seguir.

Observação 4. *Seja Λ_M um reticulado bidimensional com diversidade máxima gerado pela matriz M. Uma reflexão de Λ_M através de uma reta que passa pela origem e faz um ângulo de $\theta/2$ com o eixo das abscissas e uma rotação de Λ_M de ângulo $\pi/2 - \theta$ em torno da origem geram reticulados com as mesmas distâncias produtos mínimas (relativas ou normalizadas). Assim, o estudo em termos de distância produto de todos os reticulados congruentes a Λ_M se reduz ao estudo de todas as rotações de Λ_M.*

Nos termos da Observação 4, se $\Lambda_M = \mathbb{Z}^2$, encontramos um resultado ainda mais específico. Com efeito, ao observarmos que

$$R'S = \begin{bmatrix} \cos\left(\theta - \frac{\pi}{2}\right) & -\text{sen}\left(\theta - \frac{\pi}{2}\right) \\ \text{sen}\left(\theta - \frac{\pi}{2}\right) & \cos\left(\theta - \frac{\pi}{2}\right) \end{bmatrix}$$

concluímos que uma reflexão do $\mathbb{Z}^2$ pode também ser descrita por meio de uma rotação, uma vez que S é unimodular (mediante Teorema 10). Registramos este resultado na Observação 5 a seguir.

Observação 5. *Uma reflexão do $\mathbb{Z}^2$ através de uma reta que passa pela origem e faz um ângulo de $\theta/2$ com o eixo das abscissas e uma rotação de $\mathbb{Z}^2$ de ângulo $\theta - \pi/2$ em torno da origem geram reticulados idênticos. Assim, um estudo de todos os reticulados congruentes a $\mathbb{Z}^2$ se reduz ao estudo de todas as suas rotações.*

4.2 Versões Rotacionadas por Complexos do Reticulado $\mathbb{Z}^2$

Nesta seção, mostramos que a maior distância produto mínima conhecida de uma versão rotacionada do reticulado $\mathbb{Z}^2$ é, de fato, a maior possível. Seguem os resultados referentes às versões rotacionadas deste reticulado.

Proposição 1. *A máxima distância produto mínima normalizada para um reticulado* $\mathbb{Z}^2$ *rotacionado é* $\frac{1}{\sqrt{5}}$.

Demonstração. Como $\mathbb{Z}^2 = \{(k_1, k_2) : k_1, k_2 \in \mathbb{Z}\}$, tomando uma rotação de ângulo t, pelo Teorema 2 temos que

$$(\cos(t) + i\text{sen}(t))(k_1 + ik_2) = (k_1 \cos(t) - k_2\text{sen}(t)) + i(k_1\text{sen}(t) + k_2 \cos(t)).$$

Dessa forma, designando por $\text{Rot}(\mathbb{Z}^2, t)$ a família de reticulados obtida por esta rotação temos: $\text{Rot}(\mathbb{Z}^2, t) = \{(k_1 \cos(t) - k_2\text{sen}(t), k_1\text{sen}(t) + k_2 \cos(t)) : k_1, k_2 \in \mathbb{Z}; 0 < t < \pi/2\}$ (trata-se da família de reticulados do Exemplo 8). Levando em conta a simetria de $\mathbb{Z}^2$ podemos tomar $0 < t < \pi/4$. Observamos que neste intervalo devem ser considerados apenas os valores de t tais que $\text{tg}(t) \notin \mathbb{Q}$, de modo que tenhamos uma família de reticulados com diversidade máxima. O valor absoluto do produto de coordenadas de um ponto em $\text{Rot}(\mathbb{Z}^2, t)$ é

$$F(k_1, k_2, t) = \left| \frac{\text{sen}(2t)}{2}(k_1^2 - k_2^2) + k_1 k_2 \cos(2t) \right|. \tag{4.2}$$

Observemos que para um t qualquer em $0 < t < \pi/4$ podemos estabelecer os limitantes superiores $F(1, 0, t) = \text{sen}(2t)/2$ e $F(1, 1, t) = cos(2t)$ para o valor mínimo desse produto F. Quando consideramos a função $\alpha(t) = \min(F(1, 0, t), F(1, 1, t))$ que também é um limitante superior, concluímos que o maior valor para esse limitante ocorre quando $\frac{\text{sen}(2t)}{2} = cos(2t) \Leftrightarrow \text{tg}(2t) = 2$. De fato, a função $\alpha(t)$ é crescente em $(0, c)$, em que c é tal que $\text{tg}(2c) = 2$, pois neste intervalo $\alpha(t) = \frac{\text{sen}(2t)}{2}$ é uma função crescente. Por outro lado, $\alpha(t)$ é decrescente em $\left(c, \frac{\pi}{4}\right)$, pois neste intervalo $\alpha(t) = \cos(2t)$ é uma função decrescente. Dessa forma, concluímos que $t = c$, onde c é tal que $\text{tg}(2c) = 2$ é um máximo global para $\alpha(t)$. Ver Figuras 5 e 6.

Vamos definir a aplicação $f(k_1, k_2) = F(k_1, k_2, c)$, em que c é tal que $\text{tg}(2c) = 2$, assim, $f(k_1, k_2) = cos(2c)|k_1^2 - k_2^2 + k_1 k_2| = \cos(2c)|g(k_1, k_2)|$, em que $g(k_1, k_2) = k_1^2 - k_2^2 + k_1 k_2$. Observamos que o mínimo de f ocorre no mínimo de $|g|$.

Afirmação: $g(k_1, k_2) = 0 \Leftrightarrow k_1 = k_2 = 0$, portanto, $\min |g(k_1, k_2)| = 1$, se $(k_1, k_2) \neq (0, 0)$.

Com efeito, considerando $k_1^2 + k_2 k_1 - k_2^2 = 0$ como uma equação quadrática na variável k_1, temos $k_1 = \frac{-k_2 \pm \sqrt{5}|k_2|}{2}$, ou ainda, $2k_1 + k_2 = \pm\sqrt{5}|k_2|$. Como devemos ter

Figura 5 – Limitantes $F(1,0,t)$ e $F(1,1,t)$ ($\mathbb{Z}^2$ rotacionado)

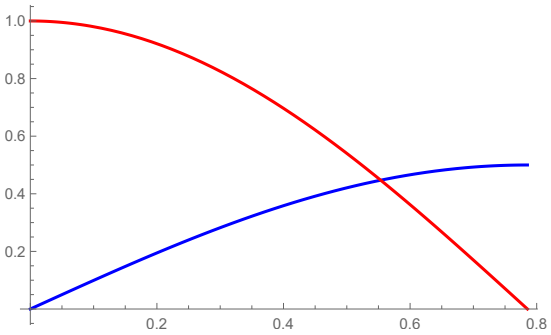
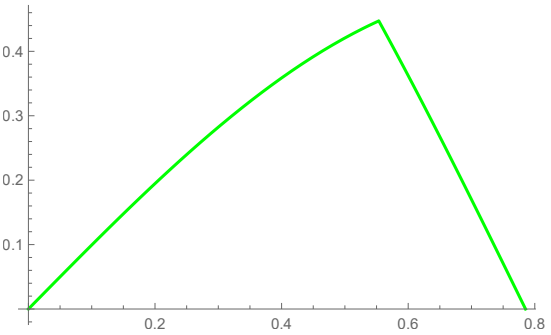


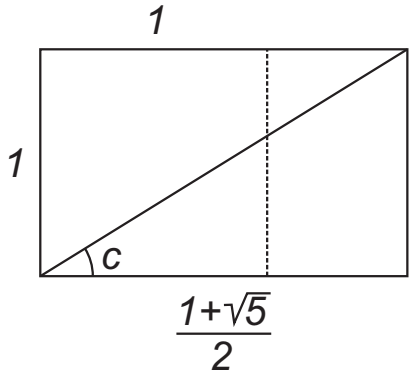
Figura 6 – Limitante $\alpha(t)$ ($\mathbb{Z}^2$ rotacionado)



$k_1, k_2 \in \mathbb{Z}$, então $k_1 = k_2 = 0$. Portanto, temos $g(1,0) = 1$, por exemplo, e o valor mínimo de f será atingido em $cos(2c)$, em que c é tal que $\text{tg}(2c) = 2$.

Finalmente, concluímos que a máxima distância produto mínima normalizada para um reticulado em $\text{Rot}(\mathbb{Z}^2, t)$ é $d_{p,\text{norm}}(\mathbb{Z}^2) = cos(2c)$, em que c é tal que $\text{tg}(2c) = 2$. Por outro lado, $\text{tg}(2c) = 2 \Leftrightarrow \text{sen}(2c) = 2\cos(2c)$. Como $\text{sen}^2(2c) + cos^2(2c) = 1$, temos $4\cos^2(2c) + \cos^2(2c) = 1$ e uma vez que $0 < c < \pi/4$, temos $\cos(2c) = \dfrac{1}{\sqrt{5}}$. Assim, $d_{p,\text{norm}}(\mathbb{Z}^2) = \dfrac{1}{\sqrt{5}}$. □

Figura 7 – O ângulo ótimo de rotação do reticulado $\mathbb{Z}^2$ é o associado à diagonal de um retângulo áureo



Observação 6. *Em relação ao ângulo ótimo c na demonstração da Proposição 1, ou seja, c tal que* $\text{tg}(2c) = 2$, *uma curiosidade é que* $1/\text{tg}(c)$ *resulta no conhecido número de ouro. Assim,* $\phi = 1/\text{tg}(c) = (1 + \sqrt{5})/2$. *Conforme podemos ver em [5], Euclides determinou o valor de* ϕ *como a "divisão de um segmento em média e extrema razão", ou seja, como a divisão de um segmento em duas partes distintas com tal propriedade: o quociente entre o segmento inteiro e a parte maior é igual ao quociente do segmento maior pelo segmento menor. Geometricamente, temos então, que o ângulo c é o dado pela diagonal de um retângulo áureo (mediante Figura 7), que é tal que ao retirarmos um quadrado obtemos um retângulo semelhante ao original (Ex. bandeira do Brasil).*

Corolário 1. *Seja $\Lambda(t)$ a família de reticulados*

$$\begin{aligned}\Lambda(t) &= Rot(\mathbb{Z}^2, t)\\ &= \{(k_1\cos(t) - k_2\text{sen}(t), k_1\text{sen}(t) + k_2\cos(t)) : k_1, k_2 \in \mathbb{Z}; 0 < t < \pi/4\}. \quad (4.3)\end{aligned}$$

O reticulado $\Lambda = \Lambda\left(\frac{1}{2}\arctan(2)\right)$ é a versão rotacionada de $\mathbb{Z}^2$ com diversidade máxima que apresenta máxima distância produto mínima normalizada. Tomando $(k_1, k_2) = \left(\frac{-k_2 \pm \sqrt{5k_2^2 \pm 4}}{2}, k_2\right)$, onde $5k_2^2 \pm 4 = k^2$ para $k, k_1, k_2 \in \mathbb{Z}$, encontramos as condições para que os pontos do reticulado Λ alcancem essa máxima distância produto mínima normalizada.

Demonstração. Da demonstração da Proposição 1, segue que o reticulado "ótimo" é $\Lambda = \Lambda(t)$ para t satisfazendo $\text{tg}(2t) = 2$, logo $\Lambda = \Lambda\left(\frac{1}{2}\arctan(2)\right)$. Observamos que os pontos de Λ em que a máxima distância produto mínima normalizada é alcançada são os pontos para os quais $(k_1, k_2) \in \mathbb{Z}^2$ minimizam $|g(k_1, k_2)|$, onde $(k_1, k_2) \neq (0, 0)$, ou seja, pela demonstração da Proposição 1 devemos ter $(k_1, k_2) = \left(\frac{-k_2 \pm \sqrt{5k_2^2 \pm 4}}{2}, k_2\right)$. Dessa forma, quando temos $5k_2^2 \pm 4 = k^2$, para $k, k_1, k_2 \in \mathbb{Z}$, o mínimo em $|g(k_1, k_2)|$ é alcançado. De fato, se k^2 é par, então k_2^2 é par, pois caso contrário existiria $s \in \mathbb{Z}$ tal que $5k_2^2 \pm 4 = 5(2s+1) \pm 4 = 2(5s \pm 2 + 2) + 1$ o que é uma contradição. Analogamente, se k^2 é ímpar, temos que k_2^2 é ímpar. Usando os conhecidos resultados: n^2 par $\Rightarrow n$ par e n^2 ímpar $\Rightarrow n$ ímpar para $n \in \mathbb{Z}$, temos que se $5k_2^2 \pm 4 = k^2$, para algum $k \in \mathbb{Z}$, então para $(k_1, k_2) = \left(\frac{-k_2 \pm \sqrt{5k_2^2 \pm 4}}{2}, k_2\right) \in \mathbb{Z}^2$ encontramos os pontos de Λ em que a máxima distância produto mínima normalizada é alcançada. □

A matriz geradora do reticulado Λ do Corolário 1 é dada por

$$Q = \begin{bmatrix} \cos\left(\frac{1}{2}\arctan(2)\right) & -\text{sen}\left(\frac{1}{2}\arctan(2)\right) \\ \text{sen}\left(\frac{1}{2}\arctan(2)\right) & \cos\left(\frac{1}{2}\arctan(2)\right) \end{bmatrix} = \begin{bmatrix} 0.850651 & -0.525731 \\ 0.525731 & 0.850651 \end{bmatrix} \quad (4.4)$$

Corolário 2. *Sejam Λ e $\tilde{\Lambda}$ as versões rotacionadas do reticulado $\mathbb{Z}^2$ via números complexos e via corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ ([32]), cujas matrizes são dadas, respectivamente, por (4.4) e (3.14). Os reticulados Λ e $\tilde{\Lambda}$ são distintos, além disso, Λ é obtido por uma reflexão em torno da reta $x = y$ do reticulado $\tilde{\Lambda}$. Ou ainda, o reticulado $\tilde{\Lambda}$ é uma rotação de $\mathbb{Z}^2$ de ângulo $-c$ em torno da origem, onde c é o ângulo "ótimo" da matriz de rotação (4.4), ou seja, $c = \frac{1}{2}\arctan(2)$.*

Demonstração. Como $Q^{-1}R$ não é unimodular, segue do Teorema 10, que os reticulados Λ e $\tilde{\Lambda}$ são distintos. Escrevendo $a = 0.525731$ e $b = 0.850651$, segue que as matrizes de Λ e

$\tilde{\Lambda}$ são dadas, respectivamente, por

$$Q = \begin{bmatrix} b & -a \\ a & b \end{bmatrix}, R = \begin{bmatrix} -a & -b \\ -b & a \end{bmatrix}.$$

Observamos que Q e R são as mesmas matrizes a menos de permutação de elementos e troca de sinais e ainda, $-I_2SR = Q$, onde I_2 é a matriz identidade de ordem 2 e

$$S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Como a matriz $-I_2$ não altera o reticulado e S representa uma reflexão em torno da reta $y = x$, segue que Λ é obtido por uma reflexão em torno dessa reta do reticulado $\tilde{\Lambda}$. Observamos que

$$R(-S) = \begin{bmatrix} b & a \\ -a & b \end{bmatrix},$$

como a matriz do segundo membro da última igualdade representa uma rotação de ângulo $-c$ em torno da origem e $-S$ é unimodular, concluímos a prova. □

A distância produto mínima encontrada no reticulado do Corolário 3, está presente em [40], quando consideramos $n = 2$ e construções de reticulados algébricos a partir dos Teoremas 27 e 28.

Corolário 3. *O reticulado obtido através de uma rotação do* $\mathbb{Z}^2$ *com ângulo* $t = \frac{\pi}{8}$, *possui distância produto normalizada* $\frac{1}{2\sqrt{2}}$.

Demonstração. Para provarmos este resultado, suponha que nos termos da demonstração da Proposição 1, para um t qualquer em $0 < t < \pi/4$ estabeleçamos os limitantes superiores $F(1,0,t) = \frac{1}{2}\text{sen}(2t)$ e $F(2,-1,t) = \left|\frac{3}{2}\text{sen}(2t) - 2\cos(2t)\right|$ para o valor mínimo do produto F. Quando consideramos a função $\beta(t) = \min(F(1,0,t), F(2,-1,t))$, que também é um limitante superior, concluímos que um máximo local para este limitante ocorrerá na menor solução da equação $\frac{1}{2}\text{sen}(2t) = \left|\frac{3}{2}\text{sen}(2t) - 2\cos(2t)\right|$, ou seja, na primeira das interseções entre os gráficos de $F(1,0,t)$ e $F(2,-1,t)$. Ver Figuras 8 e 9.

Da última igualdade, temos que $t = \frac{\pi}{8}$ é a solução procurada. Definimos a aplicação $f_1(k_1,k_2) = F(k_1,k_2,\frac{\pi}{8})$, ou seja, $f_1(k_1,k_2) = \frac{1}{2\sqrt{2}}|g_1(k_1,k_2)|$, onde $g_1(k_1,k_2) = k_1^2 + 2k_1k_2 - k_2^2$. Observamos que o mínimo de f_1 ocorre no mínimo de $|g_1|$.

Afirmação: $g_1(k_1,k_2) = 0 \Leftrightarrow k_1 = k_2 = 0$, portanto, $\min|g_1(k_1,k_2)| = 1$, se $(k_1,k_2) \neq (0,0)$.

Figura 8 – Limitantes $F(1,0,t)$ e $F(2,-1,t)$ ($\mathbb{Z}^2$ rotacionado)

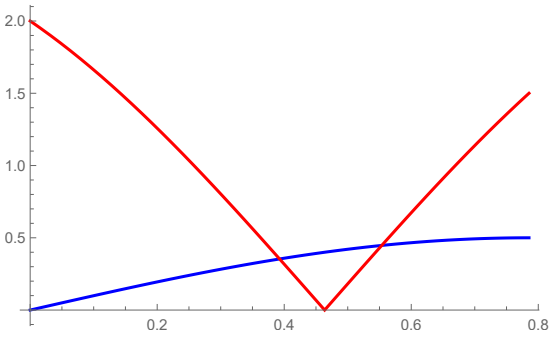
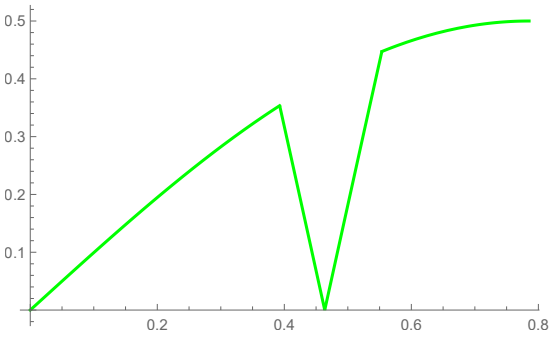


Figura 9 – Limitante $\beta(t)$ ($\mathbb{Z}^2$ rotacionado)



Com efeito, considerando $k_1^2 + 2k_1k_2 - k_2^2 = 0$ como uma equação quadrática na variável k_1, temos $k_1 = -k_2 \pm \sqrt{2}|k_2|$, ou ainda, $k_1 + k_2 = \pm\sqrt{2}|k_2|$. Como devemos ter $k_1, k_2 \in \mathbb{Z}$, então $k_1 = k_2 = 0$. Portanto, temos $g(1,0) = 1$, por exemplo, e o valor mínimo de f será atingido em $\dfrac{1}{2\sqrt{2}}$. Finalmente, concluímos que a distância produto mínima para o reticulado que é obtido através de uma rotação do reticulado $\mathbb{Z}^2$ com ângulo $t = \dfrac{\pi}{8}$ será $F(1,0,\dfrac{\pi}{8}) = F(2,-1,\dfrac{\pi}{8}) = \dfrac{1}{2\sqrt{2}}$, ou ainda, a distância produto normalizada desse reticulado será $d_{p,\text{norm}}(\mathbb{Z}^2) = \dfrac{1}{2\sqrt{2}}$. □

Observação 7. *Reunindo os limitantes superiores apresentados na demonstração do Corolário 3 e na demonstração da Proposição 1, podemos definir a aplicação*

$$\gamma(t) = \min\left(F(1,0,t), F(1,1,t), F(2,-1,t)\right)$$

que também é um limitante superior. O valor máximo global de $\gamma(t)$ também ocorre em $t = \dfrac{1}{2}\arctan(2)$ corroborando com os resultados encontrados na Proposição 1 e no Corolário 1, pois para este valor de t encontramos a máxima distância produto mínima normalizada para um reticulado em $Rot(\mathbb{Z}^2, t)$, a saber, $\dfrac{1}{\sqrt{5}}$. Ver Figuras 10 e 11.

Figura 10 – Limitantes $F(1,0,t)$, $F(1,1,t)$ e $F(2,-1,t)$ ($\mathbb{Z}^2$ rotacionado)

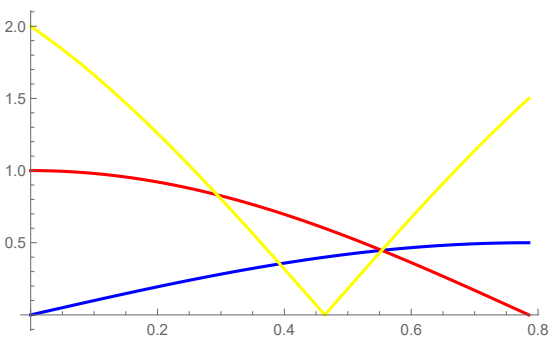
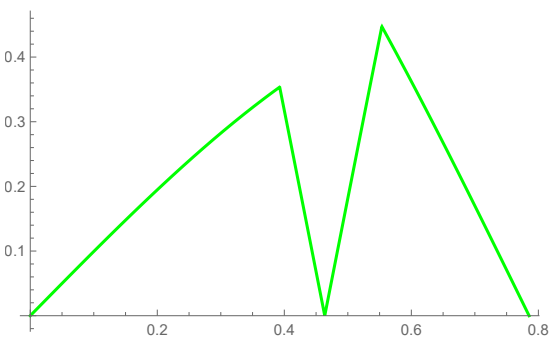


Figura 11 – Limitante $\gamma(t)$ ($\mathbb{Z}^2$ rotacionado)



Agora, vamos analisar o que ocorre com as distâncias produto dos reticulados $\Lambda(t)$ dado por (4.3), quando t é tomado em uma perturbação do ângulo ótimo $t_{\max} = \frac{1}{2}\arctan(2)$, ou seja, quando tomamos $t = t_{\max} + \epsilon$ para ϵ arbitrariamente pequeno. Para estes valores de t escrevemos

$$d_{p,\text{norm}}(\Lambda(t)) = \inf_{(k_1,k_2)\neq(0,0)} F(k_1, k_2, t),$$

onde F é a função dada por (4.2).

Abordamos, inicialmente, o problema em uma perspectiva numérica. Resolvendo as dezoito equações $F(k_1, k_2, t_{\max} + \epsilon) = 0$, onde $\epsilon = \pm\frac{1}{10^i}$ para $i = 1, 2, ..., 9$, nas variáveis inteiras k_1 e k_2 com a restrição $|k_1, k_2| \leqslant 10000$, encontramos sempre a solução $k_1 = k_2 = 0$. Isso nos permite admitir, com certo grau de segurança, que nestes casos os reticulados $\Lambda(t_{\max} + \epsilon)$ têm diversidade máxima. Em segundo lugar, minimizamos as funções $F(k_1, k_2, t_{\max} + \epsilon)$ nas variáveis inteiras k_1, k_2 quando consideramos a restrição $1 \leqslant k_1^2 + k_2^2 \leqslant 10^j$ [1]. Dessa forma, encontramos limitantes para as distâncias produtos destes reticulados. Estes resultados estão sistematizados na Tabela 2.

i	$d_{p,\text{norm}}(\Lambda(t_{\max} + 1/10^i))$	$d_{p,\text{norm}}(\Lambda(t_{\max} - 1/10^i))$
1	$\leqslant 0.260604$	$\leqslant 0.0503628$
2	$\leqslant 0.317441$	$\leqslant 0.107264$
3	$\leqslant 0.434244$	$\leqslant 0.413224$
4	$\leqslant 0.445917$	$\leqslant 0.443815$
5	$\leqslant 0.447084$	$\leqslant 0.446874$
6	$\leqslant 0.447201$	$\leqslant 0.44718$
7	$\leqslant 0.447212$	$\leqslant 0.44721$
8	$\leqslant 0.447213$	$\leqslant 0.447213$
9	$\leqslant 0.447214$	$\leqslant 0.447214$

Tabela 2 – Distância produto normalizada de $\Lambda(t_{\max} + \epsilon)$, onde $\Lambda(t)$ é dada por $\text{Rot}(\mathbb{Z}^2, t)$

Observação 8. *Em relação aos resultados que constam na Tabela 2, a menos que o mínimo seja encontrado fora da coroa circular* $1 \leqslant k_1^2 + k_2^2 \leqslant 10^6$, *podemos afirmar que o valor encontrado é de fato a distância produto do reticulado associado com a precisão apresentada. Percebemos numericamente que quando i é "grande", o limitante da distância produto do reticulado* $\Lambda(t_{\max} \pm 1/10^i)$ *associado é "próximo" de* $\frac{1}{\sqrt{2}}$. *Essa análise foi a motivação para o Corolário 4 a seguir.*

Corolário 4. *Seja* $\Lambda(t)$ *a família de reticulados dada por (4.3) .O reticulado*

$$\Lambda\left(\frac{1}{2}\arctan(2) + \epsilon\right)$$

[1] Verificamos numericamente que os valores mínimos encontrados não se alteraram para $j = 2, 3, 4, 5, 6$.

tem diversidade máxima, desde que

$$\epsilon \neq \frac{z\pi - \arctan(2)}{2} (z \in \mathbb{Z}) \ e \ \frac{-\cos(2\epsilon + \arctan(2)) \pm 1}{\text{sen}(2\epsilon + \arctan(2))} \notin \mathbb{Q}. \tag{4.5}$$

Temos, ainda, que se F é a aplicação dada por(4.2), então

$$\inf_{(k_1,k_2)\neq(0,0)} \lim_{\epsilon\to 0} F\left(k_1, k_2, t_{max} + \epsilon\right) = d_{p,\text{norm}}(\mathbb{Z}^2) = \frac{1}{\sqrt{5}}.$$

Demonstração. Observamos que para $\Lambda\left(\frac{1}{2}\arctan(2) + \epsilon\right)$ ter diversidade máxima, devemos ter

$$F\left(k_1, k_2, \frac{1}{2}\arctan(2) + \epsilon\right) = 0 \Leftrightarrow k_1 = k_2 = 0. \tag{4.6}$$

Dessa forma, vamos analisar a equação $F\left(k_1, k_2, \frac{1}{2}\arctan(2) + \epsilon\right) = 0$, ou seja, $\text{sen}(\alpha)k_1^2 + 2k_2\cos(\alpha)k_1 - k_2^2\text{sen}(\alpha) = 0$, onde $\alpha = 2\epsilon + \arctan(2)$. Resolvendo a penúltima igualdade como uma equação quadrática na variável k_1, temos $k_1 = k_2\left(\frac{-\cos(\alpha) \pm 1}{\text{sen}(\alpha)}\right)$, desde que $\alpha \neq z\pi$ $(z \in \mathbb{Z})$. Por outro lado, se $\alpha = z\pi$, ou seja, se $\epsilon = \frac{z\pi - \arctan(2)}{2}$, temos $F\left(k_1, k_2, \frac{1}{2}\arctan(2) + \epsilon\right) = k_1k_2\cos(z\pi) + \frac{1}{2}(k_1^2 - k_2^2)\text{sen}(z\pi) = \pm k_1k_2$ e neste caso, $\Lambda\left(\frac{1}{2}\arctan(2) + \epsilon\right)$ não tem diversidade máxima. Uma vez que k_1 e k_2 são inteiros, segue que (4.6) será verdade, se e somente se, (4.5) for verdade. Por outro lado, escrevendo $t_{max} = \frac{1}{2}\arctan(2)$, segue da continuidade de $F\left(k_1, k_2, t_{max} + \epsilon\right)$ que

$$\begin{aligned} & \lim_{\epsilon\to 0} F\left(k_1, k_2, t_{max} + \epsilon\right) \\ = \ & F(k_1, k_2, t_{\max}) \\ = \ & \left|k_1k_2\cos(\arctan(2)) + \frac{1}{2}(k_1^2 - k_2^2)\text{sen}(\arctan(2))\right| \\ = \ & \frac{1}{\sqrt{5}}\left|k_1k_2 + k_1^2 - k_2^2\right|. \end{aligned} \tag{4.7}$$

Tomando o inf, temos:

$$\inf_{(k_1,k_2)\neq(0,0)} \lim_{\epsilon\to 0} F\left(k_1, k_2, t_{max} + \epsilon\right) = \inf_{(k_1,k_2)\neq(0,0)} \frac{1}{\sqrt{5}}\left|k_1k_2 + k_1^2 - k_2^2\right| = \frac{1}{\sqrt{5}}.$$

□

Observação 9. *Todos os reticulados $\Lambda(t_{\max} + \epsilon)$ da Tabela 2 possuem diversidade máxima, pois $\epsilon = \pm 1/10^i$, $(i = 1, 2, ..., 15)$ satisfazem as condições dadas em (4.5).*

Observação 10. *Considere os valores de ϵ "próximos de zero", para os quais*

$$\Lambda\left(\frac{1}{2}\arctan(2)+\epsilon\right)$$

tenha diversidade máxima. Da Proposição 1, temos que

$$d_{p,\text{norm}}\left(\Lambda\left(\frac{1}{2}\arctan(2)+\epsilon\right)\right) \leqslant \frac{1}{\sqrt{5}},$$

por outro lado, o Corolário 4 nos permite concluir que o lado esquerdo da desigualdade pode tornar-se arbitrariamente próximo de $\frac{1}{\sqrt{5}}$, desde que tomemos ϵ suficientemente próximo de zero.

Observação 11. *Observamos que qualquer reticulado $\Lambda(t)$ dado por (4.3) tem norma mínima e determinante iguais a 1. Dessa forma, todos os resultados desta seção permaneçerão inalterados se considerarmos a distância produto relativa ao invés da normalizada.*

4.3 Estudo da Família de Reticulados Bem Arredondados do $\mathbb{R}^2$ a partir de Rotações por Complexos

Nesta seção, definimos reticulados *bem arredondados* e um estudo sobre a distância produto de uma família específica de tais reticulados é feito. As referências utilizadas foram: [2], [14], [17], [31] e [36].

Para definirmos reticulados bem arredondados, lançamos mão do conceito de norma mínima (mediante Definição 31). Os reticulados bem arredondados são designados por WR por conta da abreviação inglesa *well-rounded*.

Definição 59 (Reticulados Bem Arredondados)**.** *Sejam $n \geqslant 2$ um inteiro e $\Lambda \subset \mathbb{R}^n$ um reticulado de posto completo. Sejam μ a norma mínima de Λ e S o conjunto de vetores mínimos de Λ, o seja, $S = \{\mathbf{x} \in \Lambda : ||\mathbf{x}|| = \mu\}$. Dizemos que Λ é um reticulado bem arredondado (WR) se S gera o $\mathbb{R}^n$.*

Observação 12. *Da Definição 59, segue que reticulados bem arredondados são reticulados de posto completo que possuem uma base formada por vetores de norma mínima.*

Exemplo 20. *Os reticulados $\mathbb{Z}^2$ e hexagonal vistos nos Exemplos 3 e 6 são reticulados bem arredondados. Observamos que os seus conjuntos de vetores mínimos são dados, respectivamente, por $S_1 = \{(1,0),(0,1),(-1,0),(0,-1)\}$ e $S_2 = \{(1,0),(1/2,\sqrt{3}/2),(-1/2,\sqrt{3}/2),(-1,0),(-1/2,-\sqrt{3}/2),(1/2,-\sqrt{3}/2)\}$.*

Definição 60 (Quase Ortogonalidade)**.** *Uma coleção ordenada de vetores linearmente independentes $\{\mathbf{x}_1,...,\mathbf{x}_k\} \subset \mathbb{R}^n$, $2 \leqslant k \leqslant n$, é chamada quase ortogonal se para cada*

$1 < i \leqslant k$, *o ângulo entre* $\mathbf{x}_i$ *e o subespaço do* $\mathbb{R}^n$ *gerado por* $\mathbf{x}_1, ..., \mathbf{x}_{i-1}$ *está no intervalo* $[\pi/3, 2\pi/3]$. *Em outras palavras, essa condição significa que para cada* $1 < i \leqslant k$,

$$\frac{|\mathbf{x}_i^t \mathbf{y}|}{||\mathbf{x}_i||\ ||\mathbf{y}||} \leqslant \frac{1}{2},$$

para todo $\mathbf{y}$ *pertencente ao subespaço gerado por* $\mathbf{x}_1, ..., \mathbf{x}_{i-1}$.

Segundo [17], o Teorema 32, a seguir, foi demonstrado por Gauss para o caso particular $n = 2$.

Teorema 32 ([31])**.** *Suponha que uma base ordenada* $\{\mathbf{x}_1, ..., \mathbf{x}_k\}$ *de um reticulado* $\Lambda \subset \mathbb{R}^n$ *de posto* $1 < k \leqslant n$ *seja quase ortogonal. Então essa base contém um vetor mínimo de* Λ.

Observação 13. *Em relação ao Teorema 32, temos: se* $k = n$ *e todos os vetores* $\mathbf{x}_1, ..., \mathbf{x}_n$ *têm a mesma norma, segue da Observação 12, que* Λ *é WR. Neste caso,* $\{\mathbf{x}_1, ..., \mathbf{x}_n\}$ *será chamada de base minimal de* Λ.

Observação 14. *Seja* $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$, *onde* $||\mathbf{v}_1|| = ||\mathbf{v}_2||$, *uma base do reticulado* $\Lambda \subset \mathbb{R}^2$. *Decorre da Seção 1.2 de [36] que se* $\mathcal{B}$ *é minimal, então* $\mathcal{B}$ *é quase ortogonal.*

A proposição, a seguir, descreve o conjunto de todos os reticulados bem arredondados em $\mathbb{R}^2$.

Proposição 2. *Os reticulados bem arredondados em* $\mathbb{R}^2$ *com vetores de norma* μ *são dados pelo conjunto*

$$\begin{aligned}&\Lambda(a, \mu, t) = \\ &\{\mu(k_2 \cos(a + t) + k_1 \cos(t)), \mu(k_2 \text{sen}(a + t) + k_1 \text{sen}(t))) : (a, k_1, k_2, t) \in \mathbb{D}\}, \quad (4.8)\\ &\textit{onde } \mathbb{D} = [\pi/3, \pi/2] \times \mathbb{Z} \times \mathbb{Z} \times [0, 2\pi]\end{aligned}$$

Demonstração. Seja $\Lambda \subset \mathbb{R}^2$ com base $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$, onde $||\mathbf{v}_1|| = ||\mathbf{v}_2||$. Segue do Teorema 32, das Observações 13 e 14 que Λ é WR se, e somente se, $\mathcal{B}$ é quase ortogonal. Dessa forma, os reticulados em $\mathbb{R}^2$ com base $\mathcal{B}_1 = \{(\mu, 0), \mu(\cos(a), \text{sen}(a))\}$, são bem arredondados se, e somente se, $\pi/3 \leqslant a \leqslant 2\pi/3$. Observamos que para tais reticulados é sempre possível escolher uma base cujo ângulo entre os vetores desta está no intervalo $[\pi/3, \pi/2]$. Com efeito, caso tenhamos $\pi/2 < a \leqslant 2\pi/3$, podemos então tomar a base $\mathcal{B}_2 = \{(\mu, 0), \mu(\cos(\pi + a), \text{sen}(\pi + a))\}$, uma vez que $\mathcal{B}_1$ e $\mathcal{B}_2$ geram o mesmo reticulado. Dessa forma, consideramos os reticulados bem arredondados em $\mathbb{R}^2$ com base $\mathcal{B}_1$, onde $\pi/3 \leqslant a \leqslant \pi/2$. Observamos que se considerarmos todas as rotações de ângulo t destes últimos reticulados, ou seja, todas as rotações de ângulo t de $\{k_1(\mu, 0) + k_2(\mu \cos(a), \mu \text{sen}(a)) : k_1, k_2 \in \mathbb{Z}, \pi/3 \leqslant a \leqslant \pi/2\}$, descrevemos todos os reticulados bem arredondados em $\mathbb{R}^2$ com vetores de norma mínima μ. Sendo assim, do Teorema 2, temos

$$(\cos(t) + i\text{sen}(t))((k_1\mu + k_2\mu \cos(a)) + ik_2\mu \text{sen}(a)) = (\mu(k_1 \cos(t) + k_2 \cos(t + a)) +$$

$$+i\mu(k_1\text{sen}(t) + k_2\text{sen}(t+a)),$$

onde consideramos $0 \leqslant t \leqslant 2\pi$, de onde segue o resultado. □

Pra analisarmos a distância produto normalizada da classe de reticulados bem arredondados $\Lambda(a,\mu)$ com base $\{(\mu,0), \mu(\cos(a), \text{sen}(a))\}$, onde $\mu > 0$ e $\pi/3 \leqslant a \leqslant \pi/2$, devemos considerar o conjunto $\Lambda(a,\mu,t)$ dado por (4.8). Tomando o valor absoluto do produto de coordenadas de um ponto em $\Lambda(a,\mu,t)$ e dividindo-o pelo volume de um reticulado qualquer desse conjunto cujo valor é $\mu^2\text{sen}(a)$, definimos a função[2]

$$F(a,k_1,k_2,t) = \text{cossec}(a)\left|\frac{1}{2}\text{sen}(2t)k_1^2 + k_2\text{sen}(a+2t)k_1 + \frac{1}{2}k_2^2\text{sen}(2(a+t))\right|. \tag{4.9}$$

Uma vez que $F(a,k_1,k_2,t) = F(a,k_1,k_2,t+\pi/2)$ é suficiente que tomemos a variação de t no intervalo $0 \leqslant t \leqslant \pi/2$, logo o domínio de F será dado por

$$\mathbb{D} = [\pi/3, \pi/2] \times \mathbb{Z} \times \mathbb{Z} \times [0, \pi/2]. \tag{4.10}$$

Sendo assim, o supremo da distância produto ínfima normalizada para um reticulado $\Lambda(\tilde{a},\mu)$, será dada por $d_{p,\text{norm}}(\Lambda(\tilde{a},\mu)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(\tilde{a},k_1,k_2,t)$, onde $0 \leqslant t \leqslant \pi/2$, $k_1, k_2 \in \mathbb{Z}$.

Do que foi exposto no parágrafo anterior, se fizermos $\tilde{a} = \pi/3$ e $\mu = 1$, segue que o reticulado $\Lambda(\pi/3, 1)$ encontrado será o hexagonal (mediante Exemplo 6). Em [23] foi demonstrado que a máxima distância produto mínima relativa (mediante Definição 57) do hexagonal é 1/4. Uma vez que a norma mínima do hexagonal é $\mu = 1$, segue que esse resultado coincide com a máxima distância produto mínima deste reticulado. Assim, para encontrarmos a máxima distância produto mínima normalizada, basta dividirmos o último resultado pelo volume do hexagonal. Portanto,

$$d_{p,\text{norm}}(\text{hexagonal}) = d_{p,\text{norm}}(\Lambda(\pi/3,1)) = \frac{1}{2\sqrt{3}}. \tag{4.11}$$

Fazendo, agora, $\tilde{a} = \pi/2$ e $\mu = 1$, segue que $\Lambda(\pi/2,1) = \mathbb{Z}^2$ e conforme demonstrado na Proposição 1, temos $d_{p,\text{norm}}(\Lambda(\pi/2,1)) = \frac{1}{\sqrt{5}}$.

Dessa forma, para a classe de reticulados bem arredondados $\Lambda(a,1)$ conhecemos a máxima distância produto mínima normalizada dos reticulados $\Lambda(\pi/3,1)$ e $\Lambda(\pi/2,1)$, ou seja, quando a assume os valores extremos do intervalo $[\pi/3,\pi/2]$. Para alguns valores de a tomados no interior deste intervalo, a saber $a \in A = \{13\pi/36 < 7\pi/18 < 5\pi/12 < 4\pi/9 < 17\pi/36\}$, encontramos cotas superiores para as distâncias produtos dos reticulados correspondentes. Para cada $a \in A$, essas cotas superiores foram encontradas a partir do

[2] Observamos que essa função independe do valor da norma μ.

valor de $t = t_{\max}$ que maximiza o limitante[3]

$$\alpha(t) = \min(F(a,1,0,t), F(a,0,1,t), F(a,1,-1,t), F(a,1,2,t), F(a,2,1,t),$$
$$F(a,3,-5,t), F(a,5,-3,t)).$$

Em cada um desses casos verificamos que $\min_{k_1,k_2} F(a,k_1,k_2,t_{\max}) < \alpha(t_{\max})$, quando tomamos $k_1, k_2 \in \mathbb{Z}$ tais que $1 \leqslant k_1^2 + k_2^2 \leqslant 10^i$ [4] (i inteiro positivo suficientemente grande), de onde concluímos que $d_{p,\text{norm}}(\Lambda(a),1) \leqslant \alpha(t_{\max})$. Estes resultados estão sistematizados na Tabela 3.

a	$d_{p,\text{norm}}(\Lambda(a),1)$
$\pi/3$	$= 0.288675$
$13\pi/36$	$\leqslant 0.31738$
$7\pi/18$	$\leqslant 0.328734$
$5\pi/12$	$\leqslant 0.327415$
$4\pi/9$	$\leqslant 0.346285$
$17\pi/36$	$\leqslant 0.394708$
$\pi/2$	$= 0.447214$

Tabela 3 – Distância produto normalizada da classe de reticulados bem arredondados $\Lambda(a,1)$

A seguir, temos a Proposição 3, que nos dá a classe de reticulados bem arredondados do $\mathbb{R}^2$ com maior distância produto normalizada.

Proposição 3. *Se $\Lambda(a,\mu)$ é a classe de reticulados bem arredondados com base $\{(\mu,0), \mu(\cos(a),\text{sen}(a))\}$, onde $\mu > 0$, $\pi/3 \leqslant a \leqslant \pi/2$, e $d_{p,\text{norm}}(\Lambda(a,\mu)) = \sup_t d_{p,\text{norm}}(\Lambda(a,\mu,t))$, onde $\Lambda(a,\mu,t)$ dado por (4.8) é o conjunto das rotações de $\Lambda(a,\mu)$, então*

$$\max_a [d_{p,\text{norm}}(\Lambda(a,\mu))] = d_{p,\text{norm}}(\Lambda(\pi/2,\mu)) = \frac{1}{\sqrt{5}}.$$

Demonstração. Observamos que o supremo da distância produto ínfima normalizada de uma versão rotacionada de $\Lambda(\tilde{a},\mu)$, onde $\tilde{a}$ é um valor fixo no intervalo $[\pi/3,\pi/2]$ é dado por $d_{p,\text{norm}}(\Lambda(\tilde{a},\mu)) = \sup_t d_{p,\text{norm}}(\Lambda(\tilde{a},\mu,t)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(\tilde{a},k_1,k_2,t)$, onde F é a função dada em (4.9) que estabelece o valor absoluto do produto das coordenadas de um ponto em $\Lambda(a,\mu,t)$ dividido pelo volume de um reticulado qualquer desse conjunto. Uma vez que $F(a,k_1,k_2,t) = F(a,k_1,k_2,t+\pi/2)$, é suficiente que tomemos a variação

[3] Este limitante foi considerado após diversos testes na tentativa de encontrarmos limitantes "melhores" que $\beta(t) = \min(F(a,1,0,t), F(a,0,1,t), F(a,1,-1,t))$ para refinarmos as cotas superiores da distância produto.

[4] Verificamos numericamente que os valores mínimos encontrados não se alteraram para $i = 2,3,4,5,6$.

de t, no intervalo $0 \leqslant t \leqslant \pi/2$, logo o domínio de F será dado por (4.10). Sendo assim, consideremos a aplicação $\omega : [\pi/3, \pi/2] \to \mathbb{R}$ dada por $\omega(a) = d_{p,\text{norm}}(\Lambda(a,\mu)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(a,k_1,k_2,t)$. Temos:

$$\begin{aligned}\omega(a) &= \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(a,k_1,k_2,t)\\ &\leqslant \sup_t(\min(F(a,1,0,t),F(a,0,1,t),F(a,-1,1,t)))\\ &\leqslant \max_{a,t}(\min(F(a,1,0,t),F(a,0,1,t),F(a,-1,1,t))).\end{aligned}$$

Observamos que podemos definir a aplicação $\alpha : [\pi/3, \pi/2] \times [0, \pi/2] \to \mathbb{R}$ dada por

$$\alpha(a,t) = \min(F(a,1,0,t),F(a,0,1,t),F(a,-1,1,t)) \tag{4.12}$$

e como α é contínua, segue que ela tem máximo global. Assim justificamos o uso do max e min ao invés de sup e inf nas desigualdades anteriores.

Afirmação: O máximo global de α é $1/\sqrt{5}$, ou seja, $\max_{a,t}(\min(F(a,1,0,t),F(a,0,1,t),F(a,1,-1,t))) = 1/\sqrt{5}$.

Com efeito, observamos que das Figuras 12 e 13, para encontrarmos o máximo global de α devemos analisar as interseções $F(a,1,0,t) = F(a,0,1,t)$, $F(a,1,0,t) = F(a,-1,1,t)$ e $F(a,0,1,t) = F(a,0,1,t)$. Fazemos isso considerando três casos a seguir.

Figura 12 – Limitante $\alpha(a,t)$ (WR)

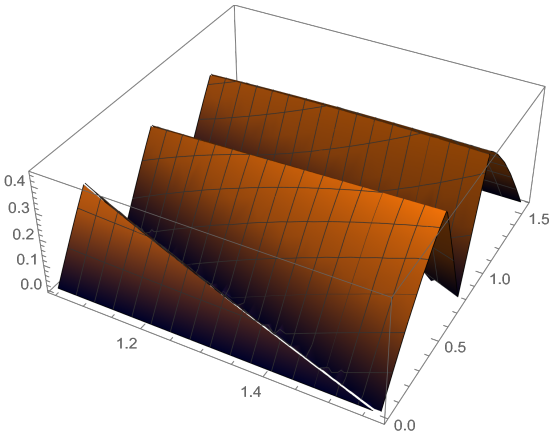
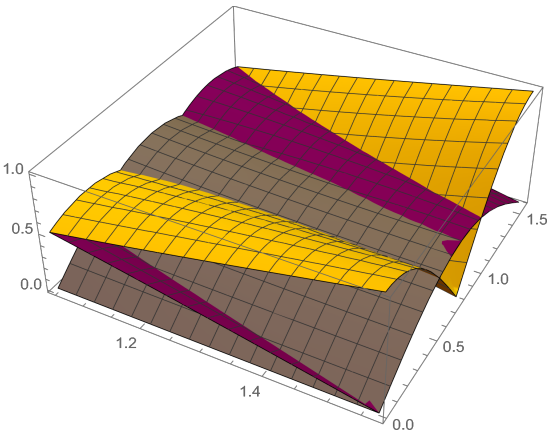


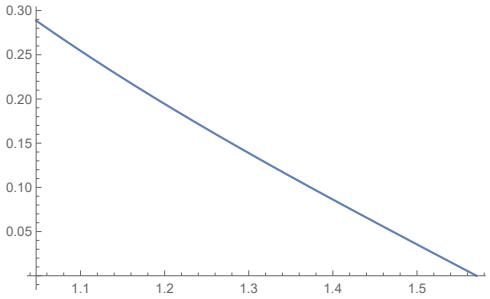
Figura 13 – Limitantes $F(a,1,0,t)$, $F(a,0,1,t)$ e $F(a,-1,1,t)$ (WR)



Caso 1: Análise da igualdade $F(a,1,0,t) = F(a,0,1,t)$. Observamos que esta igualdade equivale a $|\text{sen}(2t)| = |\text{sen}(2a+2t)|$, de onde temos $\text{sen}(2t) = \text{sen}(2a+2t)$ ou $\text{sen}(2t) = -\text{sen}(2a+2t)$. Da primeira equação $\text{sen}(2t) = \text{sen}(2a+2t)$, segue que $2a+2t = 2t+2k\pi$ ou $2a+2t = (\pi-2t)+2k\pi$, onde $k \in \mathbb{Z}$. Logo, $a = k\pi$ ou $t = (1+2k)\frac{\pi}{4} - \frac{a}{2}$.

Como devemos ter $\pi/3 \leqslant a \leqslant \pi/2$, segue que a solução $a = k\pi$ deve ser desconsiderada e como $0 \leqslant t \leqslant \pi/2$, segue da solução $t = (1+2k)\frac{\pi}{4} - \frac{a}{2}$ que $\left(\frac{2k-1}{2}\right)\pi \leqslant a \leqslant (1+2k)\frac{\pi}{2}$, logo devemos considerar $k = 0$, de onde temos $t = \frac{\pi}{4} - \frac{a}{2}$. Da Figura 14, concluímos que a função $\alpha_1 : [\pi/3, \pi/2] \to \mathbb{R}$ dada por $\alpha_1(a) = \min\left(F\left(a, 1, 0, \frac{\pi}{4} - \frac{a}{2}\right), F\left(a, 0, 1, \frac{\pi}{4} - \frac{a}{2}\right), F\left(a, -1, 1, \frac{\pi}{4} - \frac{a}{2}\right)\right)$ é estritamente decrescente.

Figura 14 – $\alpha_1(a)$ (WR)



Portanto, o máximo global de α_1 ocorre em $a = \frac{\pi}{3}$, de onde concluímos que $\left(\frac{\pi}{3}, \frac{\pi}{12}\right)$ é um ponto crítico de α e por sua vez temos $\alpha\left(\frac{\pi}{3}, \frac{\pi}{12}\right) = \frac{1}{2\sqrt{3}}$. Por outro lado, da segunda equação do Caso 1, a saber $\text{sen}(2t) = -\text{sen}(2a+2t)$, segue que $2a+2t = -2t+2k\pi$ ou $2a+2t = (\pi+2t)+2k\pi$, onde $k \in \mathbb{Z}$. Logo, $t = k\frac{\pi}{2} - \frac{a}{2}$ ou $a = (1+2k)\frac{\pi}{2}$.

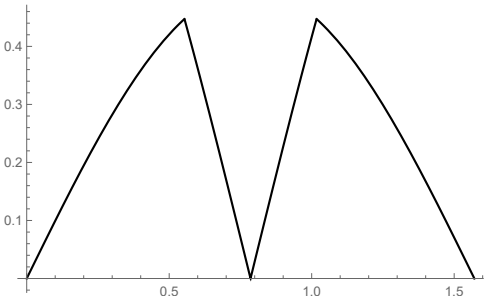
Como devemos ter $0 \leqslant t \leqslant \pi/2$, segue da solução $t = k\frac{\pi}{2} - \frac{a}{2}$ que $(k-1)\pi \leqslant a \leqslant k\pi$, logo devemos considerar $k = 1$, de onde temos $t = \frac{\pi}{2} - \frac{a}{2}$. Como $\alpha\left(a, \frac{\pi}{2} - \frac{a}{2}\right) = 0$ é óbvio que o máximo global de α não será atingido neste caso.

Como devemos ter $\pi/3 \leqslant a \leqslant \pi/2$, segue da solução $a = (1+2k)\frac{\pi}{2}$ que devemos considerar $k = 0$ e assim, $a = \frac{\pi}{2}$.

Da Figura 15, concluímos que a função $\alpha_2 : [0, \pi/2] \to \mathbb{R}$ dada por $\alpha_2(t) = \min\left(F\left(\frac{\pi}{2}, 1, 0, t\right), F\left(\frac{\pi}{2}, 0, 1, t\right), F\left(\frac{\pi}{2}, 1, -1, t\right)\right) = \min(|\text{sen}(t)\cos(t)|, |\cos(2t)|)$ possui dois extremantes que são soluções da equação $|\text{sen}(t)\cos(t)| = |\cos(2t)|$, quando consideramos $0 \leqslant t \leqslant \pi/2$. Logo, temos que $t = \frac{1}{2}\arctan(2)$ e $t = \frac{\pi}{2} - \frac{1}{2}\arctan(2)$ são pontos de máximo global de α_2.

Concluímos que $\left(\frac{\pi}{2}, \frac{1}{2}\arctan(2)\right)$ e $\left(\frac{\pi}{2}, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right)$ são pontos críticos de α e por sua vez temos $\alpha\left(\frac{\pi}{2}, \frac{1}{2}\arctan(2)\right) = \alpha\left(\frac{\pi}{2}, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right) = \frac{1}{\sqrt{5}}$.

Figura 15 – $\alpha_2(t)$ (WR)



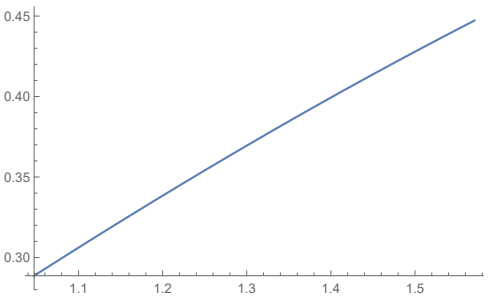
Caso 2: Análise da iguldade $F(a,1,0,t) = F(a,-1,1,t)$. Observamos que esta igualdade equivale a $\frac{1}{2}|\text{sen}(2t)| = \left|\frac{1}{2}\text{sen}(2t) + \frac{1}{2}\text{sen}(2a+2t) - \text{sen}(a+2t)\right|$, de onde temos $\text{sen}(a+2t) = \frac{1}{2}\text{sen}(2a+2t)$ ou $\text{sen}(2t) = \text{sen}(a+2t) - \frac{1}{2}\text{sen}(2a+2t)$.

Da primeira equação $\text{sen}(a+2t) = \frac{1}{2}\text{sen}(2a+2t)$, temos $\text{sen}(2t)\left(\frac{1}{2}\cos(2a) - \cos(a)\right) = \cos(2t)\left(\text{sen}(a) - \frac{1}{2}\text{sen}(2a)\right)$. Suponha que $\cos(2t)\left(\frac{1}{2}\cos(2a) - \cos(a)\right) \neq 0$, logo temos:

$$t = t_3(a) = \frac{1}{2}\arctan\left(\frac{2\text{sen}(a) - \text{sen}(2a)}{\cos(2a) - 2\cos(a)}\right) + \frac{\pi}{2}.$$

Da Figura 16, concluímos que a função $\alpha_3 : [\pi/3, \pi/2] \to \mathbb{R}$ dada por $\alpha_3(a) = \min(F(a,1,0,t_3(a)), F(a,0,1,t_3(a)), F(a,-1,1,t_3(a)))$ é estritamente crescente. Portanto, o máximo global de α_3 ocorre em $a = \frac{\pi}{2}$ e como $t_3\left(\frac{\pi}{2}\right) = \frac{\pi}{2} - \frac{1}{2}\arctan(2)$, segue que $\left(\frac{\pi}{2}, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right)$ é ponto crítico de α. Observamos que este ponto ja fora encontrado anteriormente.

Figura 16 – $\alpha_3(a)$ (WR)

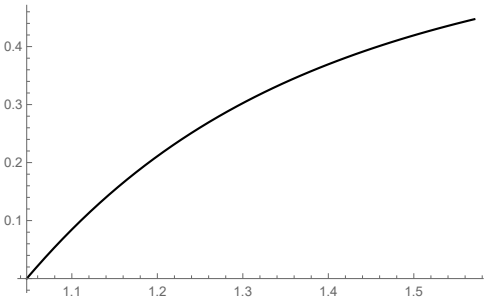


Suponha, agora, que $\cos(2t)\left(\frac{1}{2}\cos(2a)-\cos(a)\right) = 0$, ou seja, $t = \frac{\pi}{4}$ ou $a = \arccos\left(\frac{1-\sqrt{3}}{2}\right) > \frac{\pi}{2}$. Substituindo $t = \frac{\pi}{4}$ em $\text{sen}(2t)\left(\frac{1}{2}\cos(2a)-\cos(a)\right) = \cos(2t)\left(\text{sen}(a)-\frac{1}{2}\text{sen}(2a)\right)$, temos $\frac{1}{2}\cos(2a)-\cos(a)=0$, ou seja, $t=\frac{\pi}{4}$ implica em $a = \arccos\left(\frac{1-\sqrt{3}}{2}\right)$, e portanto, tal valor não deve ser considerado. Por outro lado, da segunda equação do Caso 2, a saber $\text{sen}(2t) = \text{sen}(a+2t) - \frac{1}{2}\text{sen}(2a+2t)$, temos $\text{sen}(2t)\left(1-\cos(a)+\frac{1}{2}\cos(2a)\right) = \cos(2t)\left(\text{sen}(a)-\frac{1}{2}\text{sen}(2a)\right)$. Suponha que $\cos(2t)\left(1-\cos(a)+\frac{1}{2}\cos(2a)\right) \neq 0$, logo temos:

$$t = t_4(a) = \frac{1}{2}\arctan\left(\frac{2\text{sen}(a)-\text{sen}(2a)}{2+\cos(2a)-2\cos(a)}\right).$$

Da Figura 17, concluímos que a função $\alpha_4 : [\pi/3, \pi/2] \to \mathbb{R}$ dada por $\alpha_4(a) = \min(F(a,1,0,t_4(a)), F(a,0,1,t_4(a)), F(a,-1,1,t_4(a)))$ é estritamente crescente.

Figura 17 – $\alpha_4(a)$ (WR)



Portanto, o máximo global de α_4 ocorre em $a = \frac{\pi}{2}$ e como $t_4\left(\frac{\pi}{2}\right) = \frac{1}{2}\arctan(2)$, segue que $\left(\frac{\pi}{2}, \frac{1}{2}\arctan(2)\right)$ é ponto crítico de α.

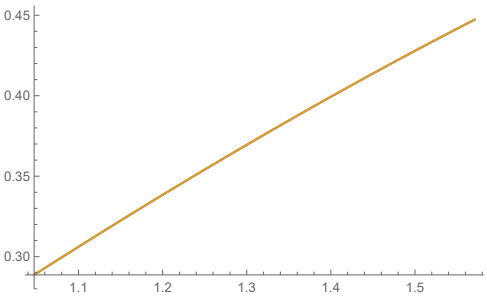
Observamos que este ponto ja fora encontrado anteriormente. Suponha agora que $\cos(2t)\left(1-\cos(a)+\frac{1}{2}\cos(2a)\right) = 0$. Como a equação $1-\cos(a)+\frac{1}{2}\cos(2a) = 0$ não tem solução, segue que $t = \frac{\pi}{4}$. Observamos que $t = \frac{\pi}{4}$ não deve ser considerado, pois se o substituirmos em $\text{sen}(2t)\left(1-\cos(a)+\frac{1}{2}\cos(2a)\right) = \cos(2t)\left(\text{sen}(a)-\frac{1}{2}\text{sen}(2a)\right)$, temos $1-\cos(a)+\frac{1}{2}\cos(2a)=0$.

Caso 3: Análise da iguldade $F(a,0,1,t) = F(a,-1,1,t)$. Observamos que esta igualdade equivale a $\frac{1}{2}|\text{sen}(2a+2t)| = \left|\frac{1}{2}\text{sen}(2t) + \frac{1}{2}\text{sen}(2a+2t) - \text{sen}(a+2t)\right|$, de onde temos $\frac{1}{2}\text{sen}(2t) = \text{sen}(a+2t)$ ou $\frac{1}{2}\text{sen}(2t) = \text{sen}(a+2t) - \text{sen}(2a+2t)$. Da primeira equação $\frac{1}{2}\text{sen}(2t) = \text{sen}(a+2t)$, temos $\text{sen}(2t)\left(\frac{1}{2} - \cos(a)\right) = \cos(2t)\text{sen}(a)$. Suponha que $\cos(2t)\left(\frac{1}{2} - \cos(a)\right) \neq 0$, logo temos:

$$t = t_5(a) = \frac{1}{2}\arctan\left(\frac{2\text{sen}(a)}{1-2\cos(a)}\right).$$

Da Figura 18, concluímos que a função $\alpha_5 : (\pi/3, \pi/2] \to \mathbb{R}$ dada por $\alpha_5(a) = \min(F(a,1,0,t_5(a)), F(a,0,1,t_5(a)), F(a,-1,1,t_5(a)))$ é estritamente crescente. Portanto, o máximo global de α_5 ocorre em $a = \frac{\pi}{2}$ e como $t_5\left(\frac{\pi}{2}\right) = \frac{1}{2}\arctan(2)$, segue que $\left(\frac{\pi}{2}, \frac{1}{2}\arctan(2)\right)$ é ponto crítico de α. Observamos que este ponto já fora encontrado anteriormente.

Figura 18 – $\alpha_5(a)$ (WR)



Suponha, agora, que $\cos(2t)\left(\frac{1}{2} - \cos(a)\right) = 0$, ou seja, $t = \frac{\pi}{4}$ ou $a = \frac{\pi}{3}$. Substituindo $t = \frac{\pi}{4}$ em $\text{sen}(2t)\left(\frac{1}{2} - \cos(a)\right) = \cos(2t)\text{sen}(a)$ temos $\frac{1}{2} - \cos(a) = 0$. Substituindo agora $a = \frac{\pi}{3}$ em $\text{sen}(2t)\left(\frac{1}{2} - \cos(a)\right) = \cos(2t)\text{sen}(a)$ temos $\cos(2t) = 0$.

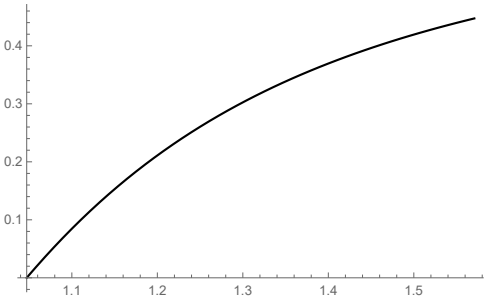
Portanto, $\left(\frac{\pi}{3}, \frac{\pi}{4}\right)$ é um ponto crítico de α e por sua vez temos $\alpha\left(\frac{\pi}{3}, \frac{\pi}{4}\right) = \frac{1}{2\sqrt{3}}$.

Por outro lado, da segunda equação do Caso 3, a saber $\frac{1}{2}\text{sen}(2t) = \text{sen}(a+2t) - \text{sen}(2a+2t)$, temos $\text{sen}(2t)\left(\frac{1}{2} - \cos(a) + \cos(2a)\right) = \cos(2t)(\text{sen}(a) - \text{sen}(2a))$. Suponha que $\cos(2t)\left(\frac{1}{2} - \cos(a) + \cos(2a)\right) \neq 0$, logo temos:

$$t = t_6(a) = \frac{1}{2}\arctan\left(\frac{2\text{sen}(a) - 2\text{sen}(2a)}{1 - 2\cos(a) + 2\cos(2a)}\right) + \frac{\pi}{2}.$$

Da Figura 19, concluímos que a função $\alpha_6 : [\pi/3, \pi/2] \to \mathbb{R}$ dada por $\alpha_6(a) = \min(F(a, 1, 0, t_6(a)), F(a, 0, 1, t_6(a)), F(a, -1, 1, t_6(a)))$ é estritamente crescente. Portanto o máximo global de α_6 ocorre em $a = \frac{\pi}{2}$ e como $t_6\left(\frac{\pi}{2}\right) = \frac{\pi}{2} - \frac{1}{2}\arctan(2)$, segue que $\left(\frac{\pi}{2}, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right)$ é um ponto crítico de α. Observamos que este ponto ja fora encontrado anteriormente.

Figura 19 – $\alpha_6(a)$ (WR)



Suponha, agora, que $\cos(2t)\left(\frac{1}{2} - \cos(a) + \cos(2a)\right) = 0$, ou seja, $t = \frac{\pi}{4}$ ou $a = \arccos\left(\frac{1 \pm \sqrt{5}}{4}\right) \notin \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$. Observamos que $t = \frac{\pi}{4}$ não deve ser considerado, pois se o substituirmos em $\text{sen}(2t)\left(\frac{1}{2} - \cos(a) + \cos(2a)\right) = \cos(2t)(\text{sen}(a) - \text{sen}(2a))$, temos $\frac{1}{2} - \cos(a) + \cos(2a) = 0$ cuja solução é $a = \arccos\left(\frac{1 \pm \sqrt{5}}{4}\right)$.

Finalmente, após analisarmos os Casos 1, 2 e 3, concluímos que $\left(\frac{\pi}{2}, \frac{1}{2}\arctan(2)\right)$ e $\left(\frac{\pi}{2}, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right)$ são os únicos extremantes globais de α, o que prova a afirmação anterior. Portanto, $\omega(a) \leqslant \frac{1}{\sqrt{5}}$ e como $\omega\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{5}}$, segue que $a = \frac{\pi}{2}$ é extremante global de ω, o que completa a demonstração. □

Observação 15. *Como na demonstração da Proposição 3, levamos em consideração o conjunto de reticulados dado pela Proposição 2, segue que não há reticulado bem arredondado em* $\mathbb{R}^2$ *com distância produto normalizada superior a de um reticulado da classe* $\Lambda(\pi/2, \mu)$*, e ainda, cada reticulado pertencente a esta classe (em particular o* $\mathbb{Z}^2$*) tem distância produto normalizada dada por* $\frac{1}{\sqrt{5}}$.

Observação 16. *Do que foi exposto no desfecho da demonstração da Proposição 3, segue que os reticulados* $\Lambda\left(\frac{\pi}{2}, 1, \frac{1}{2}\arctan(2)\right)$ *e* $\Lambda\left(\frac{\pi}{2}, 1, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right)$ *são versões rotacio-*

nadas do $\mathbb{Z}^2$ *com máxima distância produto mínima normalizada* $\frac{1}{\sqrt{5}}$. *Estes reticulados têm suas matrizes dadas por (4.4) e (4.13), respectivamente.*

$$\begin{aligned} L &= \begin{bmatrix} \cos\left(\frac{\pi}{2} - \frac{1}{2}\arctan(2)\right) & -\text{sen}\left(\frac{\pi}{2} - \frac{1}{2}\arctan(2)\right) \\ \text{sen}\left(\frac{\pi}{2} - \frac{1}{2}\arctan(2)\right) & \cos\left(\frac{\pi}{2} - \frac{1}{2}\arctan(2)\right) \end{bmatrix} \\ &= \begin{bmatrix} 0.525731 & -0.850651 \\ 0.850651 & 0.525731 \end{bmatrix} \end{aligned} \tag{4.13}$$

Corolário 5. *Seja* $\Lambda_1 = \Lambda\left(\frac{\pi}{2}, 1, \frac{\pi}{2} - \frac{1}{2}\arctan(2)\right)$ *a versão rotacionada do* $\mathbb{Z}^2$ *via números complexos cuja matriz é dada, respectivamente, por (4.13) e seja* Λ_2 *a versão rotacionada do* $\mathbb{Z}^2$ *via corpo ciclotômico* $\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ *([32]) cuja matriz é dada por (3.14). Os reticulados* Λ_1 *e* Λ_2 *são idênticos.*

Demonstração. Como $L^{-1}R$ é unimodular, segue do Teorema 10 que Λ_1 e Λ_2 são idênticos. Na verdade, escrevendo $a = 0.525731$ e $b = 0.850651$, temos

$$R = \begin{bmatrix} -a & -b \\ -b & a \end{bmatrix} = LS_1 = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} S_1,$$

onde

$$S_1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

é unimodular. □

A Proposição 3 pode ser reescrita em termos da distância produto relativa. Observamos que para garantirmos tal resultado devemos tomar o valor absoluto do produto de coordenadas de um ponto em $\Lambda(a, \mu, t)$ e dividirmos o resultado por μ^2, assim temos a função

$$G(a, k_1, k_2, t) = \text{sen}(a)F(a, k_1, k_2, t),$$

em que G tem o mesmo domínio de F cuja lei é dada por (4.9). Na demonstração da Proposição 3, a aplicação ω seria dada por $\omega(a) = d_{p,\text{rel}}(\Lambda(a, \mu)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} G(a, k_1, k_2, t)$ de onde teríamos

$$\begin{aligned} \omega(a) &= \sup_t \inf_{(k_1,k_2)\neq(0,0)} G(a, k_1, k_2, t) \\ &\leqslant \max_{a,t}(\min(G(a, 1, 0, t), G(a, 0, 1, t), G(a, -1, 1, t))). \end{aligned}$$

Definindo a aplicação $\beta : [\pi/3, \pi/2] \times [0, \pi/2] \to \mathbb{R}$ dada por

$$\beta(a,t) = \min(G(a,1,0,t), G(a,0,1,t), G(a,-1,1,t)), \tag{4.14}$$

ou seja, $\beta(a,t) = \text{sen}(a)\alpha(a,t)$, temos $\max\limits_{a,t} \beta(a,t) \leqslant \max\limits_{a} \text{sen}(a) \max\limits_{a,t} \alpha(a,t) = 1\dfrac{1}{\sqrt{5}} = \dfrac{1}{\sqrt{5}}$.

Portanto, $\omega(a) \leqslant \dfrac{1}{\sqrt{5}}$ e como $\omega\left(\dfrac{\pi}{2}\right) = \dfrac{1}{\sqrt{5}}$, segue que $a = \dfrac{\pi}{2}$ é extremante global de ω. Com isso, temos a Proposição 4 que é dada a seguir.

Proposição 4. *Se $\Lambda(a,\mu)$ é a classe de reticulados bem arredondados com base $\{(\mu,0), \mu(\cos(a), \text{sen}(a))\}$, onde $\mu > 0$, $\pi/3 \leqslant a \leqslant \pi/2$, e $d_{p,\text{rel}}(\Lambda(a,\mu)) = \sup\limits_{t} d_{p,\text{rel}}(\Lambda(a,\mu,t))$, onde $\Lambda(a,\mu,t)$ dado por (4.8) é o conjunto das rotações de $\Lambda(a,\mu)$, então*

$$\max_{a}[d_{p,\text{rel}}(\Lambda(a,\mu))] = d_{p,\text{rel}}(\Lambda(\pi/2,\mu)) = \frac{1}{\sqrt{5}}.$$

A partir das aplicações $\alpha(a,t)$ dada por (4.12) e $\beta(a,t)$ dada por (4.14) encontramos cotas superiores para as distâncias produtos dos reticulados $\Lambda(a,1)$, onde a é um ponto qualquer da partição $P = \left\{a = a(i) = \dfrac{\pi}{3} + \dfrac{\pi}{600}i\right\}_{i=0}^{100}$ do intervalo $\left[\dfrac{\pi}{3}, \dfrac{\pi}{2}\right]$. Essas cotas superiores foram encontradas maximizando as 101 aplicações $\alpha(a(i),t)$ e 101 aplicações $\beta(a(i),t)$, quando t é tomado no intervalo $\left[0, \dfrac{\pi}{2}\right]$. Numericamente, percebemos que em ambos os casos (quando consideramos $\alpha(a,t)$ e quando consideramos $\beta(a,t)$) a menor cota superior foi alcançada no reticulado hexagonal, ou seja, quando $a = \dfrac{\pi}{3}$ e essa cota é exatamente sua distância produto (normalizada ou relativa). Diante do exposto, finalizamos essa seção com as Conjecturas 1 e 2.

Conjectura 1. *Se $\Lambda(a,\mu)$ é a classe de reticulados bem arredondados com base $\{(\mu,0), \mu(\cos(a), \text{sen}(a))\}$, em que $\mu > 0$, $\pi/3 \leqslant a \leqslant \pi/2$, e $d_{p,\text{norm}}(\Lambda(a,\mu)) = \sup\limits_{t} d_{p,\text{norm}}(\Lambda(a,\mu,t))$, em que $\Lambda(a,\mu,t)$ dado por (4.8) é o conjunto das rotações de $\Lambda(a,\mu)$, então*

$$\min_{a}[d_{p,\text{norm}}(\Lambda(a,\mu))] = d_{p,\text{norm}}(\Lambda(\pi/3,\mu)) = \frac{1}{2\sqrt{3}}.$$

Conjectura 2. *Se $\Lambda(a,\mu)$ é a classe de reticulados bem arredondados com base $\{(\mu,0), \mu(\cos(a), \text{sen}(a))\}$, onde $\mu > 0$, $\pi/3 \leqslant a \leqslant \pi/2$, e $d_{p,\text{rel}}(\Lambda(a,\mu)) = \sup\limits_{t} d_{p,\text{rel}}(\Lambda(a,\mu,t))$, onde $\Lambda(a,\mu,t)$ dado por (4.8) é o conjunto das rotações de $\Lambda(a,\mu)$, então*

$$\min_{a}[d_{p,\text{rel}}(\Lambda(a,\mu))] = d_{p,\text{rel}}(\Lambda(\pi/3,\mu)) = \frac{1}{4}.$$

4.4 Estudo da Família de Reticulados via Corpos Quadráticos a partir de Rotações por Complexos

Nesta seção, estudamos a família de reticulados via corpos quadráticos a partir de rotações por complexos. Como foi observado no Exemplo 11, trata-se da família de

reticulados $\Lambda = \Lambda(\mathcal{O}_{\mathbb{K}}) = \sigma(\mathcal{O}_{\mathbb{K}})$, em que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ ($1 \neq d \in \mathbb{Z}$ livre de quadrados), dividida nas classes $\Lambda_1 = \Lambda_1(d)$, em que $0 < d \not\equiv 1 \pmod 4$, $\Lambda_2 = \Lambda_2(d)$, em que $0 < d \equiv 1 \pmod 4$, $\Lambda_3 = \Lambda_3(l)$, em que $l > 0$ é tal que $-l \not\equiv 1 \pmod 4$ e $\Lambda_4 = \Lambda_4(l)$, em que $l > 0$ é tal que $-l \equiv 1 \pmod 4$. Do Exemplo 11, vemos que os reticulados $\mathbb{Z}^2$ e hexagonal pertencem às classes Λ_3 e Λ_4, respectivamente.

Foi observado no Exemplo 16, que os reticulados das classes Λ_1 e Λ_2 têm diversidade máxima e suas distâncias produtos normalizadas são dadas por $d_{p,\text{norm}}(\Lambda_1) = \dfrac{1}{2\sqrt{d}}$ e $d_{p,\text{norm}}(\Lambda_2) = \dfrac{1}{\sqrt{d}}$. Mostramos nas Proposições 5 e 6 que essas distâncias não serão alteradas quando consideramos os conjuntos de todas as rotações de Λ_1 e Λ_2.

Proposição 5. *Se $0 < d \not\equiv 1 \pmod 4$ é livre de quadrados e $\Lambda_1(d)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.4), então a máxima distância produto mínima normalizada para um reticulado $\Lambda_1(d)$ rotacionado é $d_{p,\text{norm}}(\Lambda_1(d)) = \dfrac{1}{2\sqrt{d}}$.*

Demonstração. Como $\Lambda_1(d) = \{(k_1 + k_2\sqrt{d}, k_1 - k_2\sqrt{d}) : k_1, k_2 \in \mathbb{Z}\}$, tomando uma rotação de ângulo t, temos pelo Teorema 2 que:

$$(\cos(t) + i\text{sen}(t))(k_1 + k_2\sqrt{d} + i(k_1 - k_2\sqrt{d})) = k_2(\sqrt{d}\text{sen}(t) + \sqrt{d}\cos(t)) + k_1(\cos(t) - \text{sen}(t)) + i(k_2(\sqrt{d}\text{sen}(t) - \sqrt{d}\cos(t)) + k_1(\text{sen}(t) + \cos(t))).$$

Dessa forma, o conjunto de reticulados obtido por essa rotação é $\Lambda_1(d,t) = \{(k_2(\sqrt{d}\text{sen}(t) + \sqrt{d}\cos(t)) + k_1(\cos(t) - \text{sen}(t)), k_2(\sqrt{d}\text{sen}(t) - \sqrt{d}\cos(t)) + k_1(\text{sen}(t) + \cos(t))) : k_1, k_2 \in \mathbb{Z}; 0 \leqslant t < 2\pi\}$. O valor absoluto do produto de coordenadas de um ponto em $\Lambda_1(d,t)$ dividido pelo volume de um reticulado qualquer desse conjunto é

$$F(d, k_1, k_2, t) = \frac{1}{2\sqrt{d}} \left| \left(k_1^2 - dk_2^2\right) \cos(2t) + 2\sqrt{d}k_1k_2\text{sen}(2t) \right|.$$

Como $F\left(d, k_1, k_2, t + \dfrac{\pi}{2}\right) = F\left(d, k_1, k_2, t\right)$, podemos tomar a variação de t no intervalo $\left[0, \dfrac{\pi}{2}\right]$, logo tomando o sup neste intervalo temos:

$$d_{p,\text{norm}}(\Lambda_1(d)) = \sup_t d_{p,\text{norm}}(\Lambda_1(d,t)) =$$

$$\sup_t \inf_{(k_1,k_2)\neq(0,0)} F(d, k_1, k_2, t) \leqslant \sup_t F(d, 1, 0, t) = \sup_t \frac{|\cos(2t)|}{2\sqrt{d}} = \frac{1}{2\sqrt{d}}.$$

Por outro lado, $F\left(d, k_1, k_2, 0\right) = F\left(d, k_1, k_2, \dfrac{\pi}{2}\right) = \dfrac{1}{2\sqrt{d}}|k_1^2 - dk_2^2| = 0 \Leftrightarrow k_1 = k_2 = 0$, e ainda, $d_{p,\text{norm}}(\Lambda_1(d,0)) = \inf\limits_{(k_1,k_2)\neq(0,0)} F\left(d, k_1, k_2, 0\right) = \dfrac{1}{2\sqrt{d}}$ e $d_{p,\text{norm}}\left(\Lambda_1\left(d, \dfrac{\pi}{2}\right)\right) = \inf\limits_{(k_1,k_2)\neq(0,0)} F\left(d, k_1, k_2, \dfrac{\pi}{2}\right) = \dfrac{1}{2\sqrt{d}}$.

Portanto, $d_{p,\text{norm}}(\Lambda_1(d)) = d_{p,\text{norm}}(\Lambda_1(d,0)) = d_{p,\text{norm}}\left(\Lambda_1\left(d, \dfrac{\pi}{2}\right)\right) = \dfrac{1}{2\sqrt{d}}$. □

Proposição 6. *Se $0 < d \neq 1$ é livre de quadrados, $d \equiv 1 \pmod 4$ e $\Lambda_2(d)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.5), então a máxima distância produto mínima normalizada para um reticulado $\Lambda_2(d)$ rotacionado é* $d_{p,\text{norm}}(\Lambda_2(d)) = \dfrac{1}{\sqrt{d}}$.

Demonstração. Como $\Lambda_2(d) = \{(k_1 + k_2(1+\sqrt{d})/2, k_1 + k_2(1-\sqrt{d})/2) : k_1, k_2 \in \mathbb{Z}\}$, tomando uma rotação de ângulo t, temos pelo Teorema 2 que:

$$(\cos(t) + i\text{sen}(t))(k_1 + k_2(1+\sqrt{d})/2 + i(k_1 + k_2(1-\sqrt{d})/2)) = (k_2/2)((\sqrt{d}+1)\cos(t)$$
$$-(1-\sqrt{d})\text{sen}(t)) + k_1(\cos(t) - \text{sen}(t) + i((k_2/2)((\sqrt{d}+1)\text{sen}(t) + (1-\sqrt{d})\cos(t))$$
$$+k_1(\text{sen}(t) + \cos(t))$$

Dessa forma, o conjunto de reticulados obtido por essa rotação é $\Lambda_2(d,t) = \{((k_2/2)((\sqrt{d}+1)\cos(t) - (1-\sqrt{d})\text{sen}(t)) + k_1(\cos(t) - \text{sen}(t), (k_2/2)((\sqrt{d}+1)\text{sen}(t) + (1-\sqrt{d})\cos(t)) + k_1(\text{sen}(t) + \cos(t)) : k_1, k_2 \in \mathbb{Z}; 0 \leqslant t < 2\pi\}$. O valor absoluto do produto de coordenadas de um ponto em $\Lambda_2(d,t)$ dividido pelo volume de um reticulado qualquer desse conjunto é

$$F(d,k_1,k_2,t) = \frac{1}{4\sqrt{d}}\left|\cos(2t)\left(-(d-1)k_2^2 + 4k_1^2 + 4k_1k_2\right) + 2\sqrt{d}k_2(2k_1+k_2)\text{sen}(2t)\right|.$$

Como $F\left(d,k_1,k_2,t+\dfrac{\pi}{2}\right) = F\left(d,k_1,k_2,t\right)$, podemos tomar a variação de t no intervalo $\left[0,\dfrac{\pi}{2}\right]$, logo tomando o sup neste intervalo, temos:

$$d_{p,\text{norm}}(\Lambda_2(d)) = \sup_t d_{p,\text{norm}}(\Lambda_2(d,t)) =$$
$$\sup_t \inf_{(k_1,k_2)\neq(0,0)} F(d,k_1,k_2,t) \leqslant \sup_t F(d,1,0,t) = \sup_t \frac{|\cos(2t)|}{\sqrt{d}} = \frac{1}{\sqrt{d}}.$$

Por outro lado, $F\left(d,k_1,k_2,0\right) = F\left(d,k_1,k_2,\dfrac{\pi}{2}\right) = \dfrac{1}{4\sqrt{d}}|4k_1k_2 - (d-1)k_2^2 + 4k_1^2| = \dfrac{1}{\sqrt{d}}|k_1k_2 - sk_2^2 + k_1^2| = 0 \Leftrightarrow k_1 = k_2\left(\dfrac{-1\pm\sqrt{1+4s}}{2}\right) = k_2\left(\dfrac{-1\pm\sqrt{d}}{2}\right)$, onde $s = \dfrac{d-1}{4} \in \mathbb{Z}$. Como $0 < d \neq 1$ é livre de quadrados, segue que $F\left(d,k_1,k_2,0\right) = F\left(d,k_1,k_2,\dfrac{\pi}{2}\right) = 0 \Leftrightarrow k_1 = k_2 = 0$.

Dessa forma, temos que $d_{p,\text{norm}}(\Lambda_2(d,0)) = \inf\limits_{(k_1,k_2)\neq(0,0)} F\left(d,k_1,k_2,0\right) = \dfrac{1}{\sqrt{d}}$ e $d_{p,\text{norm}}\left(\Lambda_2\left(d,\dfrac{\pi}{2}\right)\right) = \inf\limits_{(k_1,k_2)\neq(0,0)} F\left(d,k_1,k_2,\dfrac{\pi}{2}\right) = \dfrac{1}{\sqrt{d}}$.

Portanto, $d_{p,\text{norm}}(\Lambda_2(d)) = d_{p,\text{norm}}(\Lambda_2(d,0)) = d_{p,\text{norm}}\left(\Lambda_2\left(d,\dfrac{\pi}{2}\right)\right) = \dfrac{1}{\sqrt{d}}$. □

Foi observado, no Exemplo 11, que os reticulados das classes Λ_3 e Λ_4 não têm diversidade máxima. Dessa forma, a Proposição 7 estabelece a máxima distância produto mínima quando consideramos o conjuntos de todas as rotações de Λ_3 e se as equações

diofantinas $x^2 - ly^2 = \pm 2$ (mediante Seção 1.5) não tiverem solução, a Proposição 8 estabelece a máxima distância produto mínima quando consideramos o conjunto de todas as rotações de Λ_4.

Proposição 7. *Seja $l > 0$ livre de quadrados tal que $-l \not\equiv 1 \pmod 4$. Se $\Lambda_3(l)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.6), então a máxima distância produto mínima normalizada para um reticulado $\Lambda_3(l)$ rotacionado é* $d_{p,\text{norm}}(\Lambda_3(l)) = \begin{cases} 1/\sqrt{5}, & se \quad l = 1 \\ 1/(2\sqrt{l}), & se \quad l > 1 \end{cases}$

Demonstração. Como $\Lambda_3(l) = \{(k_1, k_2\sqrt{l}) : k_1, k_2 \in \mathbb{Z}\}$, tomando uma rotação de ângulo t, temos pelo Teorema 2 que:

$$(\cos(t) + i\text{sen}(t))(k_1 + ik_2\sqrt{l}) = k_1\cos(t) - k_2\sqrt{l}\text{sen}(t) + i(k_1\text{sen}(t) + k_2\sqrt{l}\cos(t)).$$

Dessa forma, o conjunto de reticulados obtido por essa rotação é $\Lambda_3(l,t) = \{(k_1\cos(t) - k_2\sqrt{l}\text{sen}(t), k_1\text{sen}(t) + k_2\sqrt{l}\cos(t)) : k_1, k_2 \in \mathbb{Z}; 0 \leqslant t < 2\pi\}$. O valor absoluto do produto de coordenadas de um ponto em $\Lambda_3(l,t)$ dividido pelo volume de um reticulado qualquer desse conjunto é

$$F(l, k_1, k_2, t) = \frac{1}{\sqrt{l}}\left|\frac{1}{2}\text{sen}(2t)\left(k_1^2 - k_2^2 l\right) + k_1k_2\sqrt{l}\cos(2t)\right|.$$

Observamos, que se $l = 1$, então $\Lambda_3(l) = \Lambda_3(1) = \mathbb{Z}^2$ e $F(1, k_1, k_2, t)$ trata-se da função (4.2), dessa forma segue, da Proposição 1, que $d_{p,\text{norm}}(\Lambda_3(1)) = \dfrac{1}{\sqrt{5}}$.

Como $F\left(l, k_1, k_2, t + \dfrac{\pi}{2}\right) = F\left(l, k_1, k_2, t\right)$, podemos tomar a variação de t no intervalo $\left[0, \dfrac{\pi}{2}\right]$, logo tomando o sup neste intervalo temos:

$$d_{p,\text{norm}}(\Lambda_3(l)) = \sup_t d_{p,\text{norm}}(\Lambda_3(l,t)) =$$

$$\sup_t \inf_{(k_1,k_2)\neq(0,0)} F(l, k_1, k_2, t) \leqslant \sup_t F(l, 1, 0, t) = \sup_t \frac{|\text{sen}(2t)|}{2\sqrt{l}} = \frac{1}{2\sqrt{l}}.$$

Por outro lado, se $l > 1$, temos $F\left(l, k_1, k_2, \dfrac{\pi}{4}\right) = \dfrac{1}{2\sqrt{l}}|k_1^2 - lk_2^2| = 0 \Leftrightarrow k_1 = k_2 = 0$, e ainda, $d_{p,\text{norm}}\left(\Lambda_3\left(l, \dfrac{\pi}{4}\right)\right) = \inf_{(k_1,k_2)\neq(0,0)} F\left(l, k_1, k_2, \dfrac{\pi}{4}\right) = \dfrac{1}{2\sqrt{l}}$.

Portanto, $d_{p,\text{norm}}(\Lambda_3(l)) = d_{p,\text{norm}}\left(\Lambda_3\left(l, \dfrac{\pi}{4}\right)\right) = \dfrac{1}{2\sqrt{l}}$ desde que $l > 1$. □

Proposição 8. *Seja $l > 0$ livre de quadrados tal que $-l \equiv 1 \pmod 4$ e que as equações diofantinas $x^2 - ly^2 = \pm 2$ não tenham solução. Se $\Lambda_4(l)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.7), então a máxima distância produto mínima normalizada para um reticulado $\Lambda_4(l)$ rotacionado é $d_{p,\text{norm}}(\Lambda_4(l)) = \dfrac{1}{\sqrt{l}}$.*

Demonstração. Como $\Lambda_4(l) = \{(k_1 + k_2/2, k_2\sqrt{l}/2) : k_1, k_2 \in \mathbb{Z}\}$, tomando uma rotação de ângulo t, temos pelo Teorema 2 que:

$$(\cos(t) + i\text{sen}(t))(k_1 + k_2/2 + ik_2\sqrt{l}/2) = k_1\cos(t) + k_2(\cos(t)/2 - \sqrt{l}\text{sen}(t)/2) + \\ +i(k_1\text{sen}(t) + k_2(\sqrt{l}\cos(t)/2 + \text{sen}(t)/2)).$$

Dessa forma, o conjunto de reticulados obtido por essa rotação é $\Lambda_4(l,t) = \{(k_1\cos(t) + k_2(\cos(t)/2 - \sqrt{l}\text{sen}(t)/2), k_1\text{sen}(t) + k_2(\sqrt{l}\cos(t)/2 + \text{sen}(t)/2)) : k_1, k_2 \in \mathbb{Z}; 0 \leqslant t < 2\pi\}$. O valor absoluto do produto de coordenadas de um ponto em $\Lambda_4(l,t)$ dividido pelo volume de um reticulado qualquer desse conjunto é

$$F(l,k_1,k_2,t) = \frac{1}{4\sqrt{l}}\left|\text{sen}(2t)\left((2k_1+k_2)^2 - k_2^2 l\right) + 2k_2\sqrt{l}(2k_1+k_2)\cos(2t)\right|. \quad (4.15)$$

Como $F\left(l,k_1,k_2,t+\frac{\pi}{2}\right) = F\left(l,k_1,k_2,t\right)$, podemos tomar a variação de t no intervalo $\left[0,\frac{\pi}{2}\right]$, logo tomando o sup neste intervalo temos:

$$d_{p,\text{norm}}(\Lambda_4(l)) = \sup_t d_{p,\text{norm}}(\Lambda_4(l,t)) = \\ \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(l,k_1,k_2,t) \leqslant \sup_t F(l,1,0,t) = \sup_t \frac{|\text{sen}(2t)|}{\sqrt{l}} = \frac{1}{\sqrt{l}}. \quad (4.16)$$

Por outro lado, $F\left(l,k_1,k_2,\frac{\pi}{4}\right) = \frac{1}{4\sqrt{l}}\left|(2k_1+k_2)^2 - k_2^2 l\right| = 0 \Leftrightarrow k_1 = k_2\left(\frac{-1\pm\sqrt{l}}{2}\right)$. Como l é diferente de 1 e livre de quadrados, segue que $F\left(l,k_1,k_2,\frac{\pi}{4}\right) = 0 \Leftrightarrow k_1 = k_2 = 0$.

Pondo $l = 4s-1$, onde $0 < s \in \mathbb{Z}$, temos $(2k_1+k_2)^2 - k_2^2 l = 2(2k_1^2 + 2k_1k_2 - 2sk_2^2 + k_2^2)$ que é par, logo $\left|(2k_1+k_2)^2 - k_2^2 l\right| \neq 1$ e $\left|(2k_1+k_2)^2 - k_2^2 l\right| \neq 3$ quaisquer que sejam os inteiros k_1 e k_2. A equação $\left|(2k_1+k_2)^2 - k_2^2 l\right| = 2$ é equivalente a $k_1 = \left(\frac{-k_2 \pm \sqrt{k_2^2 l \pm 2}}{2}\right)$, logo ela terá solução desde que $k_2^2 l \pm 2$ seja um quadrado perfeito, uma vez que k_2 e $k_2^2 l \pm 2$ têm a mesma paridade.

Dessa forma, se $k_2^2 l \pm 2$ não for um quadrado perfeito, ou de igual modo, se as equações diofantinas $x^2 - ly^2 = \pm 2$ não tiverem solução temos $d_{p,\text{norm}}\left(\Lambda_4\left(l,\frac{\pi}{4}\right)\right) = \inf_{(k_1,k_2)\neq(0,0)} F\left(l,k_1,k_2,\frac{\pi}{4}\right) = \frac{1}{4\sqrt{l}}\inf_{(k_1,k_2)\neq(0,0)}\left|(2k_1+k_2)^2 - k_2^2 l\right| = \frac{1}{4\sqrt{l}}4 = \frac{1}{\sqrt{l}}$.

Portanto, $d_{p,\text{norm}}(\Lambda_4(l)) = d_{p,\text{norm}}\left(\Lambda_4\left(l,\frac{\pi}{4}\right)\right) = \frac{1}{\sqrt{l}}$ desde que $x^2 - ly^2 = \pm 2$ não tenham solução. □

Exemplo 21. *Embora* $-3 \equiv 1 \pmod 4$*, a equação diofantina* $x^2 - 3y^2 = -2$ *é solúvel (mediante Exemplo 1), logo* $l = 3$ *não satisfaz as hipóteses da Proposição 8. Por outro lado,* $\Lambda_4(3)$ *é o reticulado hexagonal cuja distância produto normalizada foi determinada na Seção 4.3 (mediante 4.11). Temos* $d_{p,\text{norm}}(\Lambda_4(3)) = \frac{1}{2\sqrt{3}}$.

Exemplo 22. *Uma vez que* $-15 \equiv 1 \pmod 4$ *e as equações diofantinas* $x^2 - 15y^2 = \pm 2$ *são insolúveis (mediante Exemplo 2), segue da Proposição 8 que* $d_{p,\text{norm}}(\Lambda_4(15)) = \dfrac{1}{\sqrt{15}}$.

Conjectura 3. *Seja* $l > 0$ *livre de quadrados tal que* $-l \equiv 1 \pmod 4$. *Existem infinitos valores de* l *para os quais* $x^2 - ly^2 = \pm 2$ *não têm solução.*

Observação 17. *Caso a Conjectura 3 seja verdadeira, segue da Proposição 8 que existem infinitos reticulados* $\Lambda_4(l)$ *para os quais temos* $d_{p,\text{norm}}(\Lambda_4(l)) = \dfrac{1}{\sqrt{l}}$.

Consideramos, agora, os reticulados $\Lambda_4(l)$, em que $l = 7, 11, 19, 23, 31, 43, 47, 51,$ 59 e 67. Estes são os menores valores para os quais $l > 0$ é livre de quadrados, $-l \equiv 1 \pmod 4$ e pelo menos uma das equações diofantinas $x^2 - ly^2 = \pm 2$ admite solução (essa última afirmação pode ser verificada a partir do Teorema 6). A partir da aplicação $F(l, k_1, k_2, t)$ dada por (4.15) encontramos t na partição $P = \left\{ t = t(i) = \dfrac{\pi i}{198} \right\}_{i=0}^{99}$ do intervalo $\left[0, \dfrac{\pi}{2}\right]$ para o qual tenhamos o maior limitante da distância produto do reticulado $\Lambda_4(l, t)$. Para isso, procedemos do seguinte modo: Para cada valor de l, minimizamos as 100 funções $F(l, k_1, k_2, t(i))$ nas variáveis inteiras k_1, k_2 quando consideramos a restrição $1 \leqslant k_1^2 + k_2^2 \leqslant 10^6$ e tomamos o maior valor dentre estes resultados. Observamos que essa é uma estimativa da máxima distância produto mínima normalizada do reticulado $\Lambda_4(l)$ rotacionado. Estes resultados estão sistematizados na Tabela 4.

l	$t_{\max}$	$d_{p,\text{norm}}(\Lambda_4(l, t_{\max}))$	$1/\sqrt{l}$
7	$38\pi/198$	$\leqslant 0.351169$	0.377964
11	$40\pi/198$	$\leqslant 0.287914$	0.301511
19	$49\pi/198$	$\leqslant 0.229387$	0.229416
23	$48\pi/198$	$\leqslant 0.208278$	0.208514
31	$49\pi/198$	$\leqslant 0.179583$	0.179605
43	$49\pi/198$	$\leqslant 0.152479$	0.152499
47	$48\pi/198$	$\leqslant 0.1457$	0.145865
51	$47\pi/198$	$\leqslant 0.139588$	0.140028
59	$49\pi/198$	$\leqslant 0.130173$	0.130189
67	$49\pi/198$	$\leqslant 0.122154$	0.122169

Tabela 4 – Distância produto normalizada da classe de reticulados quadráticos $\Lambda_4(l, t_{\max})$ como estimativa da $d_{p,\text{norm}}(\Lambda_4(l))$

Observação 18. *A quarta coluna da Tabela 4 nos traz o valor de* $\dfrac{1}{\sqrt{l}}$, *que conforme podemos ver em (4.16) é um limitante para máxima distância produto mínima normalizada do reticulado* $\Lambda_4(l)$ *rotacionado. Observamos que estes valores são razoavelmente "próximos" às estimativas encontradas na terceira coluna desta Tabela.*

A Proposição 8, o Exemplo 21 e a Observação 18 nos motivam à Conjectura 4 a seguir.

Conjectura 4. *Seja $l > 0$ livre de quadrados tal que $-l \equiv 1 \pmod 4$. Se $\Lambda_4(l)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.7), então a máxima distância produto mínima normalizada para um reticulado $\Lambda_4(l)$ rotacionado é* $d_{p,\text{norm}}(\Lambda_4(l)) = \begin{cases} 1/(2\sqrt{3}), & se \quad l = 3 \\ 1/\sqrt{l}, & se \quad l > 3 \end{cases}$

Toda discussão feita nessa seção sobre a ótica da distância normalizada, poderia ser feita para distância relativa.

Para mostrarmos, por exemplo, que com as hipóteses da Proposição 5, temos $d_{p,\text{rel}}(\Lambda_1(d)) = \frac{1}{2}$, observamos primeiramente no Exemplo 16 que a norma mínima de $\Lambda_1(d)$ é $\mu = \sqrt{2}$, logo segue que a norma mínima de qualquer reticulado de $\Lambda_1(d,t)$ (definido na demonstração da Proposição 5) também vale $\mu = \sqrt{2}$. Daí segue que o valor absoluto do produto de coordenadas de um ponto em $\Lambda_1(d,t)$ dividido por μ^2 é

$$F_1(d,k_1,k_2,t) = \frac{1}{2}\left|\left(k_1^2 - dk_2^2\right)\cos(2t) + 2\sqrt{d}k_1k_2\text{sen}(2t)\right|.$$

Usando na demonstração da Proposição 5 a aplicação $F_1(d,k_1,k_2,t)$ ao invés da aplicação $F(d,k_1,k_2,t)$ concluímos a prova.

A norma mínima do reticulado $\Lambda_2(d)$ que também é encontrada no Exemplo 16, vale $\mu = \sqrt{2}$ e as normas mínimas dos reticulados $\Lambda_3(l)$ e $\Lambda_4(l)$ valem $\mu = 1$ (mediante Observação 2).

De posse destes resultados concluímos de maneira análoga ao que foi feito para o reticulado $\Lambda_1(d)$ que admitindo as hipóteses das Proposições 6, 7 e 8, temos $d_{p,\text{rel}}(\Lambda_2(d)) = d_{p,\text{rel}}(\Lambda_3(l)) = d_{p,\text{rel}}(\Lambda_4(l)) = \frac{1}{2}$, sendo que para o reticulado $\Lambda_3(l)$ devemos ter $l > 1$.

Tais resultados são registrados nas Proposições 9, 10, 11 e 12.

Proposição 9. *Se $0 < d \not\equiv 1 \pmod 4$ é livre de quadrados e $\Lambda_1(d)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.4), então a máxima distância produto mínima relativa para um reticulado $\Lambda_1(d)$ rotacionado é $d_{p,\text{rel}}(\Lambda_1(d)) = \frac{1}{2}$.*

Proposição 10. *Se $0 < d \neq 1$ é livre de quadrados, $d \equiv 1 \pmod 4$ e $\Lambda_2(d)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.5), então a máxima distância produto mínima relativa para um reticulado $\Lambda_2(d)$ rotacionado é $d_{p,\text{rel}}(\Lambda_2(d)) = \frac{1}{2}$.*

Proposição 11. *Seja $l > 0$ livre de quadrados tal que $-l \not\equiv 1 \pmod 4$. Se $\Lambda_3(l)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.6),*

então a máxima distância produto mínima relativa para um reticulado $\Lambda_3(l)$ rotacionado é $d_{p,\mathrm{rel}}(\Lambda_3(l)) = \begin{cases} 1/\sqrt{5}, & se \quad l = 1 \\ 1/2, & se \quad l > 1 \end{cases}$

Proposição 12. *Seja $l > 0$ livre de quadrados tal que $-l \equiv 1 \pmod 4$ e que as equações diofantinas $x^2 - ly^2 = \pm 2$ não tenham solução. Se $\Lambda_4(l)$ é a classe de reticulados via corpos quadráticos cuja matriz geradora é dada por (3.7), então a máxima distância produto mínima relativa para um reticulado $\Lambda_4(l)$ rotacionado é $d_{p,\mathrm{rel}}(\Lambda_4(l)) = \frac{1}{2}$.*

4.5 Estudo da Família de Reticulados Ortogonais do $\mathbb{R}^2$ a partir de Rotações por Complexos

Nesta seção, estudamos a família de reticulados ortogonais (mediante Definição 28) do $\mathbb{R}^2$ a partir de rotações por complexos.

Em primeiro lugar, observemos que se Λ_1 é um reticulado de diversidade máxima cuja matriz geradora é

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{4.17}$$

e Λ_2 é um reticulado cuja matriz geradora é

$$B = \begin{bmatrix} a/m & b/m \\ c/m & d/m \end{bmatrix}, \tag{4.18}$$

em que $m \neq 0$, então dado $(k_1, k_2) \in \mathbb{Z}^2$, temos:

$$\begin{aligned} d_{p,\mathrm{norm}}(\Lambda_2) &= \min_{(k_1,k_2)\neq(0,0)} \frac{\left|\left(\frac{ak_1}{m} + \frac{bk_2}{m}\right)\left(\frac{ck_1}{m} + \frac{dk_2}{m}\right)\right|}{|\det(B)|} \\ &= \min_{(k_1,k_2)\neq(0,0)} \frac{|(ak_1 + bk_2)(ck_1 + dk_2)|}{|\det(A)|} = d_{p,\mathrm{norm}}(\Lambda_1). \end{aligned} \tag{4.19}$$

Consideramos os reticulados ortogonais $\Lambda(a)$ cuja base é $\{(1,0),(0,a)\}$, com $a \neq 0$. A fim de encontrarmos todas as rotações de ângulo t de $\Lambda(a)$, vemos do Teorema 2 que

$$(\cos(t) + i\mathrm{sen}(t))(k_1 + iak_2) = k_1\cos(t) - ak_2\mathrm{sen}(t) + i(ak_2\cos(t) + k_1\mathrm{sen}(t)).$$

Assim, a família de tais rotações é

$$\Lambda(a,t) = \{(k_1\cos(t) - ak_2\mathrm{sen}(t), ak_2\cos(t) + k_1\mathrm{sen}(t)) : (a,k_1,k_2,t) \in \mathbb{D}\}, \tag{4.20}$$

onde $\mathbb{D} = \mathbb{R} - \{0\} \times \mathbb{Z} \times \mathbb{Z} \times [0, 2\pi]$.

Observamos que uma matriz geradora de $\Lambda(a,t)$ é dada por

$$\begin{bmatrix} \cos(t) & -a\mathrm{sen}(t) \\ \mathrm{sen}(t) & a\cos(t) \end{bmatrix}.$$

Por outro lado, podemos tomar por Λ_1 (mediante a igualdade (4.17)) um reticulado ortogonal de diversidade máxima com base $\{\mathbf{u}_1, \mathbf{u}_2\}$, onde $||\mathbf{u}_1|| \geqslant ||\mathbf{u}_2||$, e por Λ_2 (mediante a igualdade (4.18)) o reticulado com base $\{\mathbf{v}_1, \mathbf{v}_2\}$, onde $\mathbf{v}_i = \mathbf{u}_i/||\mathbf{u}_1|$, de modo que a igualdade (4.19) seja válida. Observamos, ainda, que uma matriz geradora de Λ_2 é

$$\begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix}.$$

Pondo

$$\mathbf{v}_i = \begin{bmatrix} v_{1i} \\ v_{2i} \end{bmatrix},$$

mostremos que existem a e t tais que

$$\begin{bmatrix} \cos(t) & -a\text{sen}(t) \\ \text{sen}(t) & a\cos(t) \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}.$$

Com efeito, uma vez que $\mathbf{v}_1$ tenha norma unitária e seja ortogonal a $\mathbf{v}_2$ certamente existem a e t tais que $\cos(t) = v_{11}$, $\text{sen}(t) = v_{21}$ e $a = -\dfrac{v_{12}}{v_{21}} = \dfrac{v_{22}}{v_{11}}$.[5]

Supondo $|a| > 1$, temos $|v_{12}| > |v_{21}|$ e $|v_{22}| > |v_{11}|$, de onde temos $v_{12}^2 + v_{22}^2 > v_{11}^2 + v_{21}^2$ o que é uma contradição já que $||\mathbf{v}_1|| \geqslant ||\mathbf{v}_2||$, logo $|a| \leqslant 1$. Assim, concluímos que o reticulado Λ_2 pertence ao conjunto $\Lambda(a,t)$, onde $0 < |a| \leqslant 1$. Uma vez que $(0,-a) \in \Lambda(a)$, restringimos a ao intervalo $0 < a \leqslant 1$. Do que foi exposto temos a Observação 19 a seguir.

Observação 19. *Sejam Λ_1 um reticulado ortogonal com base $\{\mathbf{u}_1, \mathbf{u}_2\}$, em que $||\mathbf{u}_1|| \geqslant ||\mathbf{u}_2||$ e $\Lambda(a,t)$ o conjunto dado por (4.20). Existe $\Lambda_2 \in \Lambda(a,t)$, em que $0 < a \leqslant 1$ tal que $d_{p,\text{norm}}(\Lambda_1) = d_{p,\text{norm}}(\Lambda_2)$.*

A seguir, temos a Proposição 13, que nos dá o reticulado ortogonal com máxima distância produto mínima normalizada.

Proposição 13. *Se $\Lambda(a)$ é a classe de reticulados ortogonais com base $\{(1,0),(0,a)\}$, em que $0 < a \leqslant 1$, e $d_{p,\text{norm}}(\Lambda(a)) = \sup_t d_{p,\text{norm}}(\Lambda(a,t))$, onde $\Lambda(a,t)$ dado por (4.20) é o conjunto das rotações de $\Lambda(a)$, então $\max_a[d_{p,\text{norm}}(\Lambda(a))] = d_{p,\text{norm}}(\Lambda(1)) = \dfrac{1}{\sqrt{5}}$.*

Demonstração. Observamos que o volume de $\Lambda(a)$ é a, dessa forma tomando o valor absoluto do produto de coordenadas de um ponto em $\Lambda(a,t)$ e dividindo-o pelo volume de um reticulado qualquer desse conjunto, temos a aplicação

$$F(a,k_1,k_2,t) = \frac{|ak_1k_2\cos(2t) + (k_1 - ak_2)(k_1 + ak_2)\cos(t)\text{sen}(t)|}{a}. \tag{4.21}$$

Uma vez que $F(a,k_1,k_2,t) = F(a,k_1,k_2,t+\pi/2)$ é suficiente que tomemos a variação de t no intervalo $0 \leqslant t \leqslant \pi/2$, logo o domínio de F será dado por $\mathbb{D}' = (0,1] \times \mathbb{Z} \times \mathbb{Z} \times [0,\pi/2]$.

[5] Como Λ_2 tem diversidade máxima os v_{ij}'s são todos não nulos.

Observamos que o supremo da distância produto ínfima normalizada de uma versão rotacionada de $\Lambda(\tilde{a})$, onde $\tilde{a}$ é um valor fixo no intervalo $(0,1]$ é dado por $d_{p,\text{norm}}(\Lambda(\tilde{a})) = \sup_t d_{p,\text{norm}}(\Lambda(\tilde{a},t)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(\tilde{a},k_1,k_2,t)$. Sendo assim, consideramos a aplicação $\omega : (0,1] \to \mathbb{R}$ dada por $\omega(a) = d_{p,\text{norm}}(\Lambda(a)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(a,k_1,k_2,t)$. Temos:

$$\begin{aligned}\omega(a) &= \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(a,k_1,k_2,t)\\ &\leqslant \sup_t(\min(F(a,0,1,t),F(a,-1,1,t)))\\ &\leqslant \sup_{a,t}(\min(F(a,0,1,t),F(a,-1,1,t))).\end{aligned}$$

Observamos que podemos definir as aplicações $\alpha_1 : (0,1] \times [0,\pi/2] \to \mathbb{R}$ dada por

$$\alpha_1(a,t) = \min(F(a,0,1,t),F(a,-1,1,t))$$

e $\alpha_2 : [0,1] \times [0,\pi/2] \to \mathbb{R}$ dada por

$$\alpha_2(a,t) = \begin{cases} \alpha_1(a,t), & \text{se} \quad a \neq 0 \\ 0, & \text{se} \quad a = 0 \end{cases}$$

e uma vez que

$$\alpha_1(a,t) = \min\left(|a\cos(t)\text{sen}(t)|, \left|\frac{(1-a^2)\cos(t)\text{sen}(t) - a\cos(2t)}{a}\right|\right),$$

segue que α_2 é contínua, e portanto, tem máximo global.

Afirmação: $\sup_{a,t}(\min(F(a,0,1,t),F(a,-1,1,t))) = 1/\sqrt{5}$.

Figura 20 – $\alpha_2(a,t)$ (Reticulados Ortogonais)

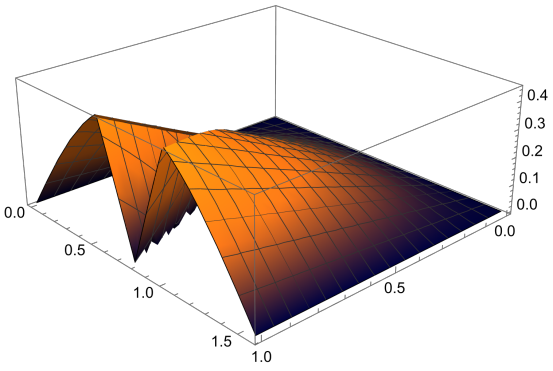
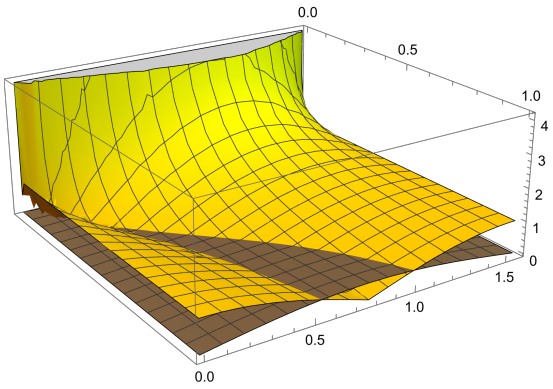


Figura 21 – Limitantes $F(a,0,1,t), F(a,-1,1,t)$ (Reticulados Ortogonais)



Uma vez que $\max_{a,t} \alpha_2 = \max_{a,t} \alpha_1$, para provarmos a afirmação anterior é suficiente mostrarmos que o máximo global de α_2 é $1/\sqrt{5}$. Das Figuras 20 e 21, concluímos que para encontrarmos o máximo global de α_2 devemos analisar a interseção $F(a,0,1,t) = F(a,-1,1,t)$.

Observamos que a igualdade $F(a,0,1,t) = F(a,-1,1,t)$ equivale a $|a\cos(t)\,\text{sen}(t)| = \left|\dfrac{(1-a^2)\cos(t)\text{sen}(t) - a\cos(2t)}{a}\right|$, de onde temos

$$\pm a\text{sen}(t)\cos(t) = \frac{(1-a^2)\cos(t)\text{sen}(t) - a\cos(2t)}{a}.$$

Da última igualdade, temos $\text{sen}(2t) = 2a\cos(2t)$ ou $(1-2a^2)\text{sen}(2t) = 2a\cos(2t)$. Supondo $\cos(2t) \neq 0$ na equação $\text{sen}(2t) = 2a\cos(2t)$, temos $\text{tg}(2t) = 2a$, de onde temos $t = t_1(a) = \dfrac{1}{2}\arctan(2a)$. A aplicação $\alpha_{21} : [0,1] \to \mathbb{R}$ dada por $\alpha_{21}(a) = \alpha_2(a, t_1(a))$ é tal que $\alpha_{21}(a) = \dfrac{a^2}{\sqrt{4a^2+1}}$ e seu máximo global ocorre em $a = 1$. Portanto $\left(1, \dfrac{1}{2}\arctan(2)\right)$ é ponto crítico de α_2 e por sua vez temos $\alpha_2\left(1, \dfrac{1}{2}\arctan(2)\right) = \dfrac{1}{\sqrt{5}}$. Supondo $\cos(2t) = 0$ na equação $\text{sen}(2t) = 2a\cos(2t)$, temos $\text{sen}(2t) = \cos(2t) = 0$, que é claramente uma contradição.

Supondo $\cos(2t)(1-2a^2) \neq 0$ na equação $(1-2a^2)\text{sen}(2t) = 2a\cos(2t)$, temos $\text{tg}(2t) = \dfrac{2a}{1-2a^2}$, de onde temos $t = t_2(a) = \dfrac{1}{2}\arctan\left(\dfrac{2a}{1-2a^2}\right) + \dfrac{\pi}{2}$. A aplicação $\alpha_{22} : [0,1] - \{1/\sqrt{2}\} \to \mathbb{R}$ dada por $\alpha_{22}(a) = \alpha_2(a, t_2(a))$ é tal que $\alpha_{22}(a) = \dfrac{a^2}{\sqrt{4a^2+1}}$ e seu máximo global ocorre em $a = 1$. Portanto, $\left(1, \dfrac{\pi}{2} - \dfrac{1}{2}\arctan(2)\right)$ é um ponto crítico de α_2 e por sua vez temos $\alpha_2\left(1, \dfrac{\pi}{2} - \dfrac{1}{2}\arctan(2)\right) = \dfrac{1}{\sqrt{5}}$.

Supondo $\cos(2t)(1-2a^2) = 0$ na equação $(1-2a^2)\text{sen}(2t) = 2a\cos(2t)$, temos $a = \dfrac{1}{\sqrt{2}} \Leftrightarrow t = \dfrac{\pi}{4}$. Portanto, $\left(\dfrac{1}{\sqrt{2}}, \dfrac{\pi}{4}\right)$ é ponto crítico de α_2 e por sua vez $\alpha_2\left(\dfrac{1}{\sqrt{2}}, \dfrac{\pi}{4}\right) = \dfrac{1}{2\sqrt{2}}$.

Concluímos que $\left(1, \dfrac{1}{2}\arctan(2)\right)$ e $\left(1, \dfrac{\pi}{2} - \dfrac{1}{2}\arctan(2)\right)$ são os únicos extremantes globais de α_2, o que prova a afirmação anterior. Portanto $\omega(a) \leqslant \dfrac{1}{\sqrt{5}}$ e como $\omega(1) = \dfrac{1}{\sqrt{5}}$, segue que $a = 1$ é extremante global de ω, o que completa a demonstração. □

Observação 20. *Do que foi exposto na Observação 19 e na Proposição 13, podemos concluir que não há reticulado ortogonal $\Lambda \subset \mathbb{R}^2$ com distância produto normalizada superior a da versão rotacionada do $\mathbb{Z}^2$ dada pela Proposição 1, ou seja, não existe Λ com distância produto normalizada superior a $\dfrac{1}{\sqrt{5}}$.*

Antes de exibirmos a "versão da Proposição 13" referente a distância produto relativa, observemos que se a norma mínima do reticulado Λ_1 (cuja matriz geradora é (4.17)) for $\mu_1 = \mu$, então a norma mínima do reticulado Λ_2 (cuja matriz geradora é (4.18))

será $\mu_2 = \dfrac{\mu}{|m|}$. Com efeito, dado $(k_1, k_2) \in \mathbb{Z}^2$, temos:

$$\begin{aligned}\mu_2 &= \min_{(k_1,k_2)\neq(0,0)} \sqrt{\left(\frac{a}{m}k_1 + \frac{b}{m}k_2\right)^2 + \left(\frac{c}{m}k_1 + \frac{d}{m}k_2\right)^2} \\ &= \frac{1}{|m|} \min_{(k_1,k_2)\neq(0,0)} \sqrt{(ak_1 + bk_2)^2 + (ck_1 + dk_2)^2} = \frac{1}{|m|}\mu. \end{aligned} \tag{4.22}$$

Da igualdade (4.22), decorre que

$$\begin{aligned} d_{p,\mathrm{rel}}(\Lambda_2) &= \min_{(k_1,k_2)\neq(0,0)} \frac{\left|\left(\frac{ak_1}{m} + \frac{bk_2}{m}\right)\left(\frac{ck_1}{m} + \frac{dk_2}{m}\right)\right|}{\left(\frac{\mu}{|\mu|}\right)^2} \\ &= \min_{(k_1,k_2)\neq(0,0)} \frac{|(ak_1 + bk_2)(ck_1 + dk_2)|}{\mu^2} = d_{p,\mathrm{rel}}(\Lambda_1). \end{aligned} \tag{4.23}$$

Observamos que podemos tomar por Λ_1 (mediante a igualdade (4.17)) um reticulado ortogonal de diversidade máxima com base $\{\mathbf{u}_1, \mathbf{u}_2\}$, onde $||\mathbf{u}_1|| \leqslant ||\mathbf{u}_2||$ e por Λ_2 (mediante a igualdade (4.18)) o reticulado com base $\{\mathbf{v}_1, \mathbf{v}_2\}$, onde $\mathbf{v}_i = \mathbf{u}_i/||\mathbf{u}_1|$, de modo que a igualdade (4.23) seja válida. E ainda, de maneira análoga ao argumento apresentado no início dessa seção que levou à Observação 19, podemos concluir que o reticulado Λ_2 pertence ao conjunto $\Lambda(a, t)$, onde $|a| \geqslant 1$. Uma vez que $(0, -a) \in \Lambda(a)$, restringimos a ao intervalo $a \geqslant 1$. Do que foi exposto temos a Observação 21 a seguir.

Observação 21. *Sejam Λ_1 um reticulado ortogonal com base $\{\mathbf{u}_1, \mathbf{u}_2\}$, em que $||\mathbf{u}_1|| \leqslant ||\mathbf{u}_2||$ e $\Lambda(a, t)$ o conjunto dado por (4.20). Existe $\Lambda_2 \in \Lambda(a, t)$, em que $a \geqslant 1$ tal que $d_{p,\mathrm{rel}}(\Lambda_1) = d_{p,\mathrm{rel}}(\Lambda_2)$.*

A seguir, temos a Proposição 14 que nos dá uma classe de reticulados ortogonais com máxima distância produto mínima relativa.

Proposição 14. *Se $\Lambda(a)$ é a classe de reticulados ortogonais com base $\{(1, 0), (0, a)\}$, onde $a \geqslant 1$, e $d_{p,\mathrm{rel}}(\Lambda(a)) = \sup_t d_{p,\mathrm{rel}}(\Lambda(a, t))$, onde $\Lambda(a, t)$ dado por (4.20) é o conjunto das rotações de $\Lambda(a)$, então $\max_a[d_{p,\mathrm{rel}}(\Lambda(a))] = d_{p,\mathrm{rel}}(\Lambda(\sqrt{l})) = \dfrac{1}{2}$, onde $a = \sqrt{l}$ e l é um inteiro maior que 1 que não é um quadrado perfeito.*

Demonstração. Observamos que a norma mínima de $\Lambda(a)$ é 1, dessa forma, tomando o valor absoluto do produto de coordenadas de um ponto em $\Lambda(a, t)$, temos a aplicação

$$G(a, k_1, k_2, t) = |ak_1k_2\cos(2t) + (k_1 - ak_2)(k_1 + ak_2)\cos(t)\mathrm{sen}(t)|.$$

Uma vez que $G(a, k_1, k_2, t) = G(a, k_1, k_2, t + \pi/2)$ é suficiente que tomemos a variação de t no intervalo $0 \leqslant t \leqslant \pi/2$, logo o domínio de G será dado por $\tilde{\mathbb{D}} = [1, \infty) \times \mathbb{Z} \times$

$\mathbb{Z} \times [0, \pi/2]$. Consideramos a aplicação $\omega : [1, \infty) \to \mathbb{R}$ dada por $\omega(a) = d_{p,\text{rel}}(\Lambda(a)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} G(a, k_1, k_2, t)$. Temos:

$$\omega(a) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} G(a, k_1, k_2, t) \leqslant \sup_t G(a, 1, 0, t) = \sup_t \frac{|\text{sen}(2t)|}{2} = \frac{1}{2}.$$

Por outro lado, $G\left(a, k_1, k_2, \frac{\pi}{4}\right) = \frac{1}{2}|k_1^2 - a^2 k_2^2| = 0 \Leftrightarrow |k_1| = a|k_2|$. Pondo $a^2 = l > 1$, onde $l \in \mathbb{Z}$ não é quadrado perfeito, temos $G\left(a, k_1, k_2, \frac{\pi}{4}\right) = 0 \Leftrightarrow k_1 = k_2 = 0$, e ainda, $d_{p,\text{rel}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = \inf_{(k_1,k_2)\neq(0,0)} G\left(\sqrt{l}, k_1, k_2, \frac{\pi}{4}\right) = \inf_{(k_1,k_2)\neq(0,0)} \frac{1}{2}|k_1^2 - l k_2^2| = \frac{1}{2}$.

Portanto,

$$\omega(\sqrt{l}) = d_{p,\text{rel}}(\Lambda(\sqrt{l})) = \sup_t d_{p,\text{rel}}(\Lambda(a,t)) = d_{p,\text{rel}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = \frac{1}{2} \tag{4.24}$$

de onde segue que $a = \sqrt{l}$, onde $1 < l \in \mathbb{Z}$ não é um quadrado perfeito, é extremante global de ω, o que completa a demonstração.

□

Observação 22. *Do que foi exposto na Observação 21 e na Proposição 14, podemos concluir que não há reticulado ortogonal em $\mathbb{R}^2$ com distância produto relativa superior a de um reticulado da classe $\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)$, ou seja, não existe reticulado ortogonal em $\mathbb{R}^2$ com distância produto relativa superior a $\frac{1}{2}$. Observamos, ainda, que o reticulado quadrático Λ_3 do Exemplo 11 pertence à classe $\Lambda(a)$ e como podemos ver nas Proposições 7 e 11, uma rotação de $\frac{\pi}{4}$ deste reticulado possui diversidade máxima com distância produto relativa igual a $\frac{1}{2}$.*

Proposição 15. *Seja l um inteiro maior que 1 que não é um quadrado perfeito. Se $\Lambda(\sqrt{l})$ é a classe de reticulados ortogonais com base $\{(1,0),(0,\sqrt{l})\}$, então a máxima distância produto mínima normalizada para um reticulado $\Lambda(\sqrt{l})$ rotacionado é $d_{p,\text{norm}}(\Lambda(\sqrt{l})) = \frac{1}{2\sqrt{l}}$.*

Demonstração. Observamos que

$$d_{p,\text{norm}}(\Lambda(\sqrt{l})) = \sup_t d_{p,\text{norm}}(\Lambda(\sqrt{l}, t)) = \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(\sqrt{l}, k_1, k_2, t) \leqslant$$
$$\leqslant \sup_t F(\sqrt{l}, 1, 0, t) \leqslant \sup_t \frac{|\text{sen}(2t)|}{2\sqrt{l}} = \frac{1}{2\sqrt{l}},$$

onde $\Lambda(a,t)$ e F são dados por (4.20) e (4.21), respectivamente. Por outro lado, como a norma mínima de $\Lambda(\sqrt{l})$ é 1, segue da igualdade (4.24), que $d_{p,\text{min}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = d_{p,\text{rel}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = \frac{1}{2}$ de onde segue que

$$d_{p,\text{norm}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = \frac{1}{V(\Lambda(\sqrt{l}))} d_{p,\text{min}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = \frac{1}{2\sqrt{l}}.$$

Portanto $d_{p,\text{norm}}(\Lambda(\sqrt{l})) = \sup_t d_{p,\text{norm}}(\Lambda(\sqrt{l}, t)) = d_{p,\text{norm}}\left(\Lambda\left(\sqrt{l}, \frac{\pi}{4}\right)\right) = \frac{1}{2\sqrt{l}}$.

□

Conjectura 5. *Não existe reticulado $\Lambda \subset \mathbb{R}^2$ com distância produto normalizada superior a $\frac{1}{\sqrt{5}}$.*

Conjectura 6. *Não existe reticulado $\Lambda \subset \mathbb{R}^2$ com distância produto relativa superior a $\frac{1}{2}$.*

Finalizamos este capítulo com a Observação 23 a seguir.

Observação 23. *Decorre da Seção 4.1, em especial das Observações 4 e 5, que todas as proposições deste capítulo podem ser escritas em termos do conjunto de reticulados congruentes ao invés do conjunto das rotações consideradas. A Proposição 1, por exemplo, poderia ser reescrita da seguinte maneira: "A máxima distância produto mínima normalizada para um reticulado congruente a $\mathbb{Z}^2$ é $\frac{1}{\sqrt{5}}$."*

5 Reticulados Rotacionados via Quatérnios

Neste capítulo, construímos via quatérnios versões rotacionadas de $\mathbb{Z}^3$ e FCC. Para estas, encontramos as mesmas distâncias produtos dos reticulados algébricos apresentados no Capítulo 3, relacionando-os geometricamente com tais versões rotacionadas ao descrevê-las a partir de reflexões e rotações específicas dos reticulados algébricos. Essa será uma forma de descrever geometricamente os reticulados algébricos, o que não é feito nas construções apresentadas no Capítulo 3 e nem nas referências citadas neste.

O programa usado para os cálculos simbólicos e plotagem dos gráficos foi o *Wolfram Mathematica* em sua versão 12.3 [43].

5.1 Versões Rotacionadas por Quatérnios do Reticulado $\mathbb{Z}^3$

Nesta seção, mostramos que a maior distância produto mínima conhecida de uma versão rotacionada do reticulado $\mathbb{Z}^3$ é de fato a maior possível quando consideramos versões rotacionadas deste reticulado em torno da reta com vetor diretor dado por $(1,1,1)$.

O motivo para considerarmos rotações do reticulado $\mathbb{Z}^3$ em torno desta reta é que $(1,0,0),(0,1,0),(0,0,1)$ são vetores da base deste reticulado equidistantes a esta e por isso temos uma simetria em relação ao reticulado.

Proposição 16. *Seja* $Rot(\mathbb{Z}^3,(1,1,1))$ *o conjunto de todas as rotações possíveis do reticulado* $\mathbb{Z}^3$ *em torno da reta cujo vetor diretor é* $(1,1,1)$. *A máxima distância produto mínima normalizada para um reticulado em* $Rot(\mathbb{Z}^3,(1,1,1))$ *é* $\frac{1}{7}$.

Demonstração. Como $\mathbb{Z}^3 = \{(k_1,k_2,k_3) : k_1,k_2,k_3 \in \mathbb{Z}\}$, se tomarmos uma rotação de ângulo $2t$ em torno da reta cujo vetor diretor é $(1,1,1)$, ou seja, considerando $\hat{p} = \frac{1}{\sqrt{3}}\mathbf{i} + \frac{1}{\sqrt{3}}\mathbf{j} + \frac{1}{\sqrt{3}}\mathbf{k}$, pelo Teorema 3, temos:

$$\left(\cos(t) + \left(\frac{1}{\sqrt{3}}\mathbf{i} + \frac{1}{\sqrt{3}}\mathbf{j} + \frac{1}{\sqrt{3}}\mathbf{k}\right)\operatorname{sen}(t)\right)\cdot(k_1\mathbf{i} + k_2\mathbf{j} + k_3\mathbf{k})\cdot$$
$$\left(\cos(t) - \left(\frac{1}{\sqrt{3}}\mathbf{i} + \frac{1}{\sqrt{3}}\mathbf{j} + \frac{1}{\sqrt{3}}\mathbf{k}\right)\operatorname{sen}(t)\right) = A\mathbf{i} + B\mathbf{j} + C\mathbf{k},$$

em que

$$A = \frac{1}{3}(k_1 + k_2 + k_3 + (2k_1 - k_2 - k_3)\cos(2t) - \sqrt{3}(k_2 - k_3)\operatorname{sen}(2t)),$$
$$B = \frac{1}{3}(k_1 + k_2 + k_3 - (k_1 - 2k_2 + k_3)\cos(2t) + \sqrt{3}(k_1 - k_3)\operatorname{sen}(2t)),$$
$$C = \frac{1}{3}(k_1 + k_2 + k_3 - (k_1 + k_2 - 2k_3)\cos(2t) - \sqrt{3}(k_1 - k_2)\operatorname{sen}(2t)).$$

Dessa forma, temos que $\mathrm{Rot}(\mathbb{Z}^3,(1,1,1))$ é o conjunto das ternas ordenadas (A,B,C) com A,B e C descritos pelas igualdades acima, onde $k_1,k_2,k_3 \in \mathbb{Z}$ e $0<t<\pi$. Levando em conta a simetria do vetor $(1,1,1)$ em relação ao $\mathbb{Z}^3$, podemos tomar $0<t<\pi/6$. O valor absoluto do produto das coordenadas de um ponto em $\mathrm{Rot}(\mathbb{Z}^3,(1,1,1))$ é:

$$F(k_1,k_2,k_3,t) = |ABC| = |1/27(-(k_1+k_2+k_3)(2k_1^2-5k_1k_2+2k_2^2-5(k_1+k_2)k_3 + \\ +2k_3^2)+(k_1+k_2-2k_3)(2k_1-k_2-k_3)(k_1-2k_2+k_3)\cos(6t)-3\sqrt{3}(k_1-k_2)(k_1-k_3) \\ (k_2-k_3)\mathrm{sen}(6t))|. \tag{5.1}$$

Observamos que, para um t qualquer em $0<t<\pi/6$, podemos estabelecer os limitantes superiores $F(1,0,0,t)=\dfrac{1}{27}|-2+2\cos(6t)|=\dfrac{1}{27}(2-2\cos(6t))$ e $F(-1,1,0,t)=\dfrac{2|\mathrm{sen}(6t)|}{3\sqrt{3}}=\dfrac{2\mathrm{sen}(6t)}{3\sqrt{3}}$ para o valor mínimo desse produto F.

Quando consideramos a função $\alpha(t)=\min\left(F(1,0,0,t),F(-1,1,0,t)\right)$ que também é um limitante superior, concluímos que o maior valor para esse limitante ocorre quando $\dfrac{1}{27}(2-2\cos(6t))=\dfrac{2\mathrm{sen}(6t)}{3\sqrt{3}}$. De fato, para encontrarmos os valores de t que satisfaçam a última igualdade façamos $\mathrm{sen}(6t)=a$ e $\cos(6t)=b$. Logo, devemos ter $a^2+b^2=1$ e $\dfrac{2}{3\sqrt{3}}a=\dfrac{1}{27}(2-2b)$. Substituindo a última equação na penúltima, temos $14b^2-b-13=0$, onde encontramos $b=1$ e $b=-\dfrac{13}{14}$. Logo, temos $(a,b)=(0,1)$ e $(a,b)=(\dfrac{3\sqrt{3}}{14},-\dfrac{13}{14})$. Dessa forma, temos $t=\dfrac{1}{6}\arccos\left(\dfrac{-13}{14}\right)$ já que consideramos a restrição $0<t<\pi/6$.

Observamos que a função $\alpha(t)$ é crescente em $\left(0,\dfrac{1}{6}\arccos\left(\dfrac{-13}{14}\right)\right)$, pois neste intervalo $\alpha(t)=\dfrac{1}{27}(2-2\cos(6t))$ que é uma função crescente. Por outro lado, $\alpha(t)$ é decrescente em $\left(\dfrac{1}{6}\arccos\left(\dfrac{-13}{14}\right),\dfrac{\pi}{6}\right)$, pois neste intervalo $\alpha(t)=\dfrac{2\mathrm{sen}(6t)}{3\sqrt{3}}$ que é uma função decrescente. Dessa forma, concluímos que $t=\dfrac{1}{6}\arccos\left(\dfrac{-13}{14}\right)$ é um máximo global de $\alpha(t)$. Ver Figuras 22 e 23.

Vamos definir a aplicação $f(k_1,k_2,k_3)=F\left(k_1,k_2,k_3,\dfrac{1}{6}\arccos\left(\dfrac{-13}{14}\right)\right)$, ou seja, $f(k_1,k_2,k_3)=\dfrac{1}{7}|g(k_1,k_2,k_3)|$, onde $g(k_1,k_2,k_3)=k_1^3-k_1^2k_2-2k_1k_2^2+k_2^3-2k_1^2k_3-k_1k_2k_3-k_2^2k_3-k_1k_3^2-2k_2k_3^2+k_3^3$. Observamos que o mínimo de f ocorre no mínimo de $|g|$.

Afirmação: $g(k_1,k_2,k_3)=0 \Leftrightarrow k_1=k_2=k_3=0$, portanto, $\min|g(k_1,k_2,k_3)|=1$ se considerarmos $(k_1,k_2,k_3)\neq(0,0,0)$.

Com efeito, como k_1,k_2 e k_3 são pares ou ímpares, temos $2^3=8$ possibilidades distintas:

Figura 22 – Limitantes $F(1,0,0,t)$ e $F(-1,1,0,t)$ ($\mathbb{Z}^3$ rotacionado)

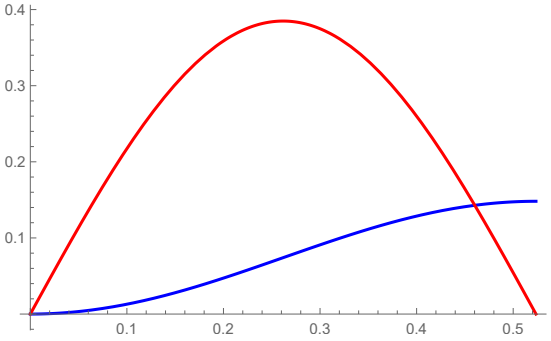
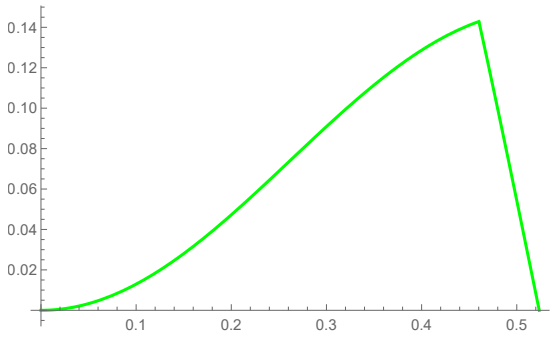


Figura 23 – Limitante $\alpha(t)$ ($\mathbb{Z}^3$ rotacionado)



Caso 1: todos ímpares (1 possibilidade); Caso 2: dois ímpares (3 possibilidades); Caso 3: um ímpar (3 possibilidades); Caso 4: nenhum ímpar, ou seja, todos pares (1 possibilidade).

Em relação aos Casos 1, 2 e 3, vamos mostrar que $g(k_1,k_2,k_3)$ será ímpar, portanto $g(k_1,k_2,k_3)=0$ não pode ser verdade.

Caso 1: Escrevendo $k_i = 2w_i+1$, onde $w_i \in \mathbb{Z}$, para $i=1,2,3$, temos: $g(2w_1+1, 2w_2+1, 2w_3+1) = 1+2(-4-7w_1+4w_1^3-7w_2-14w_1w_2-4w_1^2w_2-8w_1w_2^2+4w_2^3-7w_3-14w_1w_3-8w_1^2w_3-14w_2w_3-4w_1w_2w_3-4w_2^2w_3-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Caso 2: Escrevendo $k_1 = 2w_1+1, k_2 = 2w_2+1, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i=1,2,3$, temos: $g(2w_1+1, 2w_2+1, 2w_3) = 1+2(-1-w_1+4w_1^2+4w_1^3-2w_2-12w_1w_2-4w_1^2w_2+2w_2^2-8w_1w_2^2+4w_2^3-4w_3-10w_1w_3-8w_1^2w_3-6w_2w_3-4w_1w_2w_3-4w_2^2w_3-6w_3^2-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Escrevendo $k_1 = 2w_1+1, k_2 = 2w_2, k_3 = 2w_3+1$, onde $w_i \in \mathbb{Z}$, para $i=1,2,3$, temos: $g(2w_1+1, 2w_2, 2w_3+1) = 1+2(-1-2w_1+2w_1^2+4w_1^3-4w_2-6w_1w_2-4w_1^2w_2-6w_2^2-8w_1w_2^2+4w_2^3-w_3-12w_1w_3-8w_1^2w_3-10w_2w_3-4w_1w_2w_3-4w_2^2w_3+4w_3^2-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Escrevendo $k_1 = 2w_1, k_2 = 2w_2+1, k_3 = 2w_3+1$, onde $w_i \in \mathbb{Z}$, para $i=1,2,3$, temos: $g(2w_1, 2w_2+1, 2w_3+1) = 1+2(-1-4w_1-6w_1^2+4w_1^3-w_2-10w_1w_2-4w_1^2w_2+4w_2^2-8w_1w_2^2+4w_2^3-2w_3-6w_1w_3-8w_1^2w_3-12w_2w_3-4w_1w_2w_3-4w_2^2w_3+2w_3^2-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Caso 3: Escrevendo $k_1 = 2w_1+1, k_2 = 2w_2, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i=1,2,3$, temos: $g(2w_1+1, 2w_2, 2w_3) = 1+2(3w_1+6w_1^2+4w_1^3-w_2-4w_1w_2-4w_1^2w_2-4w_2^2-8w_1w_2^2+4w_2^3-2w_3-8w_1w_3-8w_1^2w_3-2w_2w_3-4w_1w_2w_3-4w_2^2w_3-2w_3^2-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Escrevendo $k_1 = 2w_1, k_2 = 2w_2 + 1, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i = 1, 2, 3$, temos: $g(2w_1, 2w_2+1, 2w_3) = 1+2(-2w_1-2w_1^2+4w_1^3+3w_2-8w_1w_2-4w_1^2w_2+6w_2^2-8w_1w_2^2+4w_2^3-w_3-2w_1w_3-8w_1^2w_3-4w_2w_3-4w_1w_2w_3-4w_2^2w_3-4w_3^2-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Escrevendo $k_1 = 2w_1, k_2 = 2w_2, k_3 = 2w_3 + 1$, onde $w_i \in \mathbb{Z}$, para $i = 1, 2, 3$, temos: $g(2w_1, 2w_2, 2w_3+1) = 1+2(-w_1-4w_1^2+4w_1^3-2w_2-2w_1w_2-4w_1^2w_2-2w_2^2-8w_1w_2^2+4w_2^3+3w_3-4w_1w_3-8w_1^2w_3-8w_2w_3-4w_1w_2w_3-4w_2^2w_3+6w_3^2-4w_1w_3^2-8w_2w_3^2+4w_3^3)$ que é ímpar.

Finalmente, em relação ao Caso 4, vamos mostrar que $g(k_1, k_2, k_3) = 0$ não pode ser verdade se considerarmos $(k_1, k_2, k_3) \neq (0, 0, 0)$.

Caso 4: Escrevendo $k_1 = 2w_1, k_2 = 2w_2, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i = 1, 2, 3$, temos $g(k_1, k_2, k_3) = 0 \Leftrightarrow 8g(w_1, w_2, w_3) = 0 \Leftrightarrow g(w_1, w_2, w_3) = 0$. De igual modo, como w_1, w_2 e w_3 são pares ou ímpares temos $2^3 = 8$ possibilidades, que conforme anteriormente estão descritas nos quatros casos mencionados. Os primeiros três casos resultarão em $g(w_1, w_2, w_3)$ ímpar, portanto, a igualdade $g(w_1, w_2, w_3) = 0$ não poderá ser verdadeira. Se ocorrer o quarto caso, escrevemos $w_1 = 2y_1, w_2 = 2y_2, w_3 = 2y_3$, o que resulta, como antes, em $g(y_1, y_2, y_3) = 0$.

Daí prosseguimos da mesma forma, pois como y_1, y_2 e y_3 são pares ou ímpares temos as mesmas $2^3 = 8$ possibilidades que podem ser descritas nos mesmos quatro casos. Os três primeiros irão resultar em $g(y_1, y_2, y_3)$ ímpar, portanto, a igualdade $g(y_1, y_2, y_3) = 0$ não será verdadeira. Ocorrendo o quarto caso, somos conduzidos a uma nova igualdade da forma $g(x_1, x_2, x_3) = 0$ e prosseguimos como antes.

Observamos que, após uma quantidade finita de etapas, temos uma igualdade $g(z_1, z_2, z_3) = 0$, onde ao menos um dos termos z_1, z_2, z_3 será ímpar, mas isso é uma contradição, pois dos três primeiros casos que descrevemos, $g(z_1, z_2, z_3)$ será ímpar, portanto, $g(z_1, z_2, z_3) = 0$ não poderá ser verdadeiro. Assim a igualdade $g(k_1, k_2, k_3) = 0$ só é verdadeira para $k_1 = k_2 = k_3 = 0$.

Portanto, temos $g(1, 0, 0) = 1$, por exemplo, e o valor mínimo de f será $\frac{1}{7}$. Em outras palavras, concluímos que a *máxima distância produto mínima normalizada* para um reticulado em $\mathrm{Rot}(\mathbb{Z}^3, (1, 1, 1))$ será igual ao limitante superior:

$$F\left(1, 0, 0, \frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right) = F\left(-1, 1, 0, \frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right) = \frac{1}{7},$$

ou ainda, a *máxima distância produto mínima normalizada* para um reticulado em $\mathrm{Rot}(\mathbb{Z}^3, (1, 1, 1))$ será:

$$d_{\mathrm{p,norm}}(\mathbb{Z}^3) = \frac{1}{7}.$$

□

A matriz do reticulado cuja distância produto mínima é dada pela Proposição 16 é

$$Q = \begin{bmatrix} 0.736976 & -0.327985 & 0.591009 \\ 0.591009 & 0.736976 & -0.327985 \\ -0.327985 & 0.591009 & 0.736976 \end{bmatrix} \tag{5.2}$$

As distâncias produtos mínimas encontradas nos reticulados do Corolário 6 estão presentes em [40] quando consideramos $n = 3$, sendo que a última delas consta também em [4].

Corolário 6. *Os reticulados obtidos por meio de uma rotação do reticulado* $\mathbb{Z}^3$ *com ângulos* $\frac{2\pi}{9}$ *e* $\frac{1}{3}\arccos\left(-\frac{1}{26}\right)$ *em torno da reta cujo vetor diretor é* $(1,1,1)$*, possuem distâncias produtos mínimas normalizadas* $\frac{1}{9}$ *e* $\frac{1}{13}$*, respectivamente.*

Demonstração. Para provarmos este resultado, suponha que nos termos da demonstração da Proposição 16, para $0 < t < \frac{\pi}{6}$, estabeleçamos os limitantes superiores $F(1,0,0,t) = \frac{1}{27}|-2+2\cos(6t)| = \frac{1}{27}(2-2\cos(6t))$ e $F(-1,1,1,t) = \frac{1}{27}|11+16\cos(6t)|$, para o valor mínimo do produto F.

Quando consideramos a função $\beta(t) = \min\left(F(1,0,0,t), F(-1,1,1,t)\right)$ que também é um limitante superior, concluímos que um máximo local para $\beta(t)$ e um vértice no gráfico de $\beta(t)$ ocorrerão quando $\frac{1}{27}(2-2\cos(6t)) = \frac{1}{27}|11+16\cos(6t)|$, ou seja, nas interseções entre os gráficos de $F(1,0,0,t)$ e $F(-1,1,1,t)$. Ver Figuras 24 e 25.

Figura 24 – Limitantes $F(1,0,0,t)$ e $F(-1,1,1,t)$ ($\mathbb{Z}^3$ rotacionado)

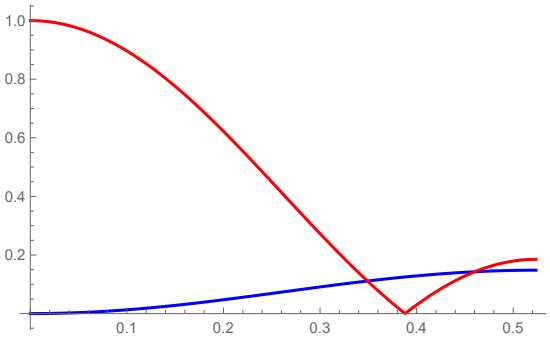
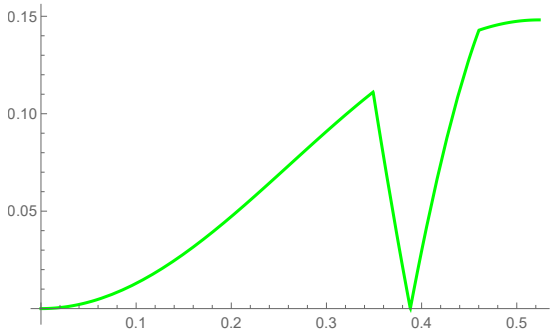


Figura 25 – Limitante $\beta(t)$ ($\mathbb{Z}^3$ rotacionado)



Para encontrarmos os valores de t $\left(0 < t < \frac{\pi}{6}\right)$ que satisfaçam a última igualdade, façamos $\cos(6t) = a$. Logo, devemos ter $2 - 2a = |11 + 16a| \Leftrightarrow a = -\frac{1}{2}; a = -\frac{13}{14}$. Dessa forma, temos $t = \frac{\pi}{9}$ e $t = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$. Observamos que o último valor de t é o mesmo encontrado na Proposição 16, que neste caso, trata-se apenas de um vértice

do gráfico de $\beta(t)$, desta forma vamos considerar o primeiro valor de t que é um máximo local desta função.

Definimos a aplicação $f_1(k_1,k_2,k_3) = F\left(k_1,k_2,k_3,\frac{\pi}{9}\right)$, ou seja, $f_1(k_1,k_2,k_3) = \frac{1}{9}|g_1(k_1,k_2,k_3)|$, onde $g_1(k_1,k_2,k_3) = k_1^3 + k_2^3 - 3k_1^2k_3 - 3k_2k_3^2 + k_3^3 - 3k_1k_2(k_2+k_3)$. Observamos que o mínimo de f_1 ocorre no mínimo de $|g_1|$.

Como na afirmação da Proposição 16, aqui temos $g_1(k_1,k_2,k_3) = 0 \Leftrightarrow k_1 = k_2 = k_3 = 0$, portanto, $\min|g_1(k_1,k_2,k_3)| = 1$ se considerarmos $(k_1,k_2,k_3) \neq (0,0,0)$. A demonstração é inteiramente análoga à anterior.

Portanto, o valor mínimo de f_1 será $\frac{1}{9}$. Concluímos que a *distância produto mínima* para o reticulado que é obtido através de uma rotação do reticulado $\mathbb{Z}^3$ com ângulo $2t = \frac{2\pi}{9}$ em torno da reta cujo vetor diretor é $(1,1,1)$ será $F\left(1,0,0,\frac{\pi}{9}\right) = F\left(-1,1,1,\frac{\pi}{9}\right) = \frac{1}{9}$, ou ainda, a *distância produto mínima normalizada* deste reticulado será $d_{\mathrm{p,norm}}(\mathbb{Z}^3) = \frac{1}{9}$.

Suponhamos que nos termos da demonstração da Proposição 16, para $0 < t < \frac{\pi}{6}$, estabeleçamos os limitantes superiores $F(-1,1,0,t) = \frac{2|\mathrm{sen}(6t)|}{3\sqrt{3}} = \frac{2\mathrm{sen}(6t)}{3\sqrt{3}}$ e $F(-1,1,1,t) = \frac{1}{27}|11 + 16\cos(6t)|$ para o valor mínimo do produto F.

Quando consideramos a função $\gamma(t) = \min\left(F(-1,1,0,t), F(-1,1,1,t)\right)$ que também é um limitante superior, concluímos que um máximo local para $\gamma(t)$ e um vértice no gráfico de $\gamma(t)$ ocorrerão quando $\frac{2\mathrm{sen}(6t)}{3\sqrt{3}} = \frac{1}{27}|11+16\cos(6t)|$, ou seja, nas interseções entre os gráficos de $F(-1,1,0,t)$ e $F(-1,1,1,t)$. O máximo global de $\gamma(t)$ ocorre em $t = \frac{\pi}{12}$ que não é um ponto de interseção entre os gráficos de $F(-1,1,0,t)$ e $F(-1,1,1,t)$. Ver Figuras 26 e 27.

Figura 26 – Limitantes $F(-1,1,0,t)$ e $F(-1,1,1,t)$ ($\mathbb{Z}^3$ rotacionado)

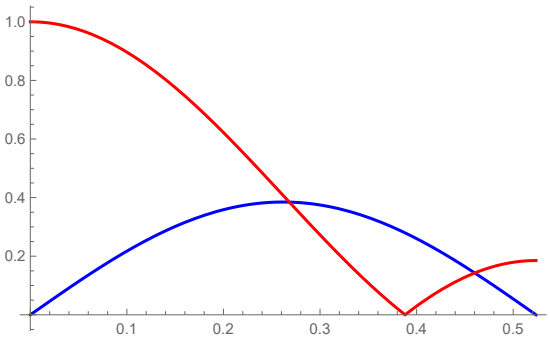
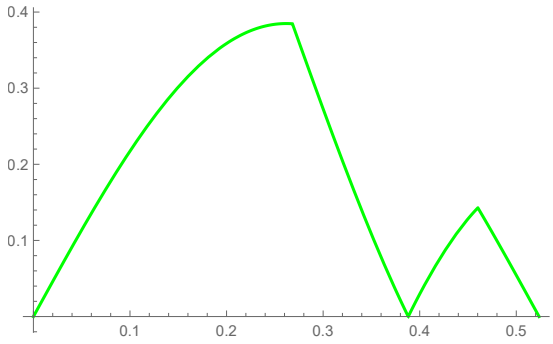


Figura 27 – Limitante $\gamma(t)$ ($\mathbb{Z}^3$ rotacionado)



Para encontrarmos os valores de t $\left(0 < t < \frac{\pi}{6}\right)$ que satisfaçam a penúltima igualdade façamos $\mathrm{sen}(6t) = a$ e $\cos(6t) = b$. Logo, devemos ter $a^2 + b^2 = 1$ e $\frac{2}{3\sqrt{3}}a =$

$\frac{1}{27}|11+16b|$. Das duas últimas igualdades anteriores encontramos $(a,b) = \left(\pm\frac{3\sqrt{3}}{14}, -\frac{13}{14}\right)$ e $(a,b) = \left(\pm\frac{15\sqrt{3}}{26}, -\frac{1}{26}\right)$. Dessa forma, temos $t = \frac{1}{6}\arccos\left(\frac{-1}{26}\right)$ e $t = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$. Observamos que o último valor de t é o mesmo encontrado na Proposição 16 e é um máximo local de $\gamma(t)$. Vamos considerar o primeiro valor de t, que é um vértice do gráfico de $\gamma(t)$.

Definimos a aplicação $f_2(k_1,k_2,k_3) = F\left(k_1,k_2,k_3,\frac{1}{6}\arccos\left(\frac{-1}{26}\right)\right)$, ou seja, $f_2(k_1,k_2,k_3) = \frac{1}{13}|g_2(k_1,k_2,k_3)|$, em que $g_2(k_1,k_2,k_3) = k_1^3 + k_1^2k_2 - 4k_1k_2^2 + k_2^3 - 4k_1^2k_3 - 7k_1k_2k_3 + k_2^2k_3 + k_1k_3^2 - 4k_2k_3^2 + k_3^3$. Observamos que o mínimo de f_2 ocorre no mínimo de $|g_2|$.

Como na afirmação da Proposição 16, aqui temos $g_2(k_1,k_2,k_3) = 0 \Leftrightarrow k_1 = k_2 = k_3 = 0$, portanto, $\min|g_2(k_1,k_2,k_3)| = 1$ se considerarmos $(k_1,k_2,k_3) \neq (0,0,0)$. A demonstração também é inteiramente análoga.

Portanto, o valor mínimo de f_2 será $\frac{1}{13}$. Finalmente, concluímos que a *distância produto mínima* para o reticulado que é obtido por meio de uma rotação do reticulado $\mathbb{Z}^3$ com ângulo $2t = \frac{1}{3}\arccos\left(-\frac{1}{26}\right)$ em torno da reta cujo vetor diretor é $(1,1,1)$ será $F\left(-1,1,0,\frac{1}{6}\arccos\left(\frac{-1}{26}\right)\right) = F\left(-1,1,1,\frac{1}{6}\arccos\left(\frac{-1}{26}\right)\right) = \frac{1}{13}$, ou ainda, a *distância produto mínima normalizada* deste reticulado será $\mathrm{d_{p,norm}}(\mathbb{Z}^3) = \frac{1}{13}$. □

Figura 28 – Limitantes $F(1,0,0,t), F(-1,1,0,t)$ e $F(-1,1,1,t)$ ($\mathbb{Z}^3$ rotacionado)

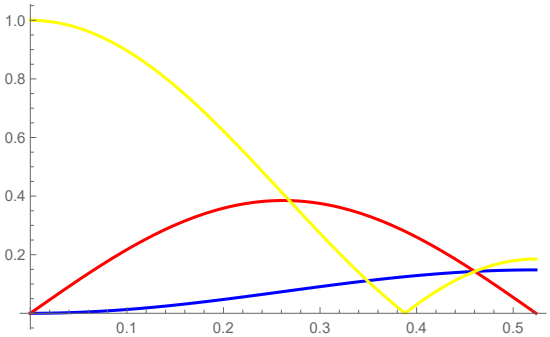
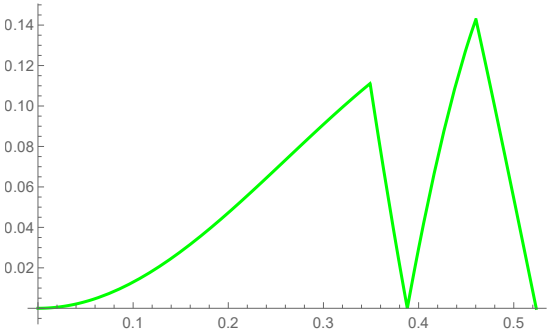


Figura 29 – Limitante $\delta(t)$ ($\mathbb{Z}^3$ rotacionado)



Observação 24. *Reunindo todos os limitantes superiores apresentados na demonstração do Corolário 6 e na demonstração da Proposição 16, podemos definir a aplicação*

$$\delta(t) = \min\left(F(1,0,0,t), F(-1,1,0,t), F(-1,1,1,t)\right)$$

que também é um limitante superior. O máximo global de $\delta(t)$ também ocorre em $t = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$ corroborando com o resultado encontrado na Proposição 16, pois para este valor de t encontramos a máxima distância produto mínima normalizada para um reticulado em $Rot(\mathbb{Z}^3,(1,1,1))$, a saber, $\frac{1}{7}$. Ver Figuras 28 e 29.

Corolário 7. *Sejam Λ e $\tilde{\Lambda}$ as versões rotacionadas do reticulado $\mathbb{Z}^3$ via quatérnios e via corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ ([32]) cujas matrizes são dadas, respectivamente, por (5.2) e (3.15). Os reticulados Λ e $\tilde{\Lambda}$ são distintos, além disso, Λ é obtido por meio de uma rotação anti-horária de $\pi/2$ em torno do eixo Oy, seguida de uma reflexão em torno do plano $y = 0$ do reticulado $\tilde{\Lambda}$.*

Demonstração. Como $Q^{-1}R$ não é unimodular, segue do Teorema 10, que os reticulados Λ e $\tilde{\Lambda}$ são distintos. Escrevendo $a = 0.327985$, $b = 0.591009$ e $c = 0.736976$, segue que as matrizes de Λ e $\tilde{\Lambda}$ são dadas, respectivamente, por

$$Q = \begin{bmatrix} c & -a & b \\ b & c & -a \\ -a & b & c \end{bmatrix}, R = \begin{bmatrix} -a & -c & -b \\ -b & -a & c \\ -c & b & -a \end{bmatrix}.$$

Observamos que Q e R são as mesmas matrizes a menos de permutação de elementos e troca de sinais e ainda,

$$S_2 S_1 R U = Q, \tag{5.3}$$

onde

$$S_1 = \begin{bmatrix} \cos(\pi/2) & 0 & -\text{sen}(\pi/2) \\ 0 & 1 & 0 \\ \text{sen}(\pi/2) & 0 & \cos(\pi/2) \end{bmatrix}, S_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}.$$

Como a matriz U não altera o reticulado por ser unimodular (mediante Teorema 10), S_1 representa uma rotação anti-horária de $\pi/2$ em torno do eixo Oy e S_2 representa uma reflexão em torno do plano $y = 0$, segue o resultado. □

Agora, vamos analisar o que ocorre com as distâncias produto dos reticulados $\Lambda(t) = \text{Rot}(\mathbb{Z}^3,(1,1,1))$ (mediante demonstração da Proposição 16), quando t é tomado em uma perturbação do ângulo ótimo $t_{\max} = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$, ou seja, quando tomamos $t = t_{\max} + \epsilon$ para ϵ arbitrariamente pequeno. Para estes valores de t, escrevemos

$$d_{p,\text{norm}}(\Lambda(t)) = \inf_{(k_1,k_2,k_3)\neq(0,0,0)} F(k_1,k_2,k_3,t),$$

onde F é a função dada por (5.1).

Abordamos, inicialmente, o problema em uma perspectiva numérica. Resolvendo as dezesseis equações $F(k_1, k_2, k_3, t_{\max} + \epsilon) = 0$, em que $\epsilon = \pm\frac{1}{10^i}$, para $i = 1, 2, ..., 8$, nas variáveis inteiras k_1, k_2 e k_3, com a restrição $|k_1, k_2, k_3| \leqslant 1000$, encontramos sempre a solução $k_1 = k_2 = k_3 = 0$. Isso nos permite admitir, com certo grau de segurança, que nesses casos os reticulados $\Lambda(t_{\max} + \epsilon)$ têm diversidade máxima. Em segundo lugar, minimizamos as funções $F(k_1, k_2, k_3, t_{\max} + \epsilon)$ nas variáveis inteiras k_1, k_2, k_3 quando consideramos a restrição $1 \leqslant k_1^2 + k_2^2 + k_3^2 \leqslant 10^j$ [1]. Dessa forma, encontramos limitantes para as distâncias produtos destes reticulados. Tais resultados estão sistematizados na Tabela 5.

i	$d_{p,\text{norm}}(\Lambda(t_{\max} + 1/10^i))$	$d_{p,\text{norm}}(\Lambda(t_{\max} - 1/10^i))$
1	$\leqslant 0.0480955$	$\leqslant 0.0774436$
2	$\leqslant 0.0477441$	$\leqslant 0.0294264$
3	$\leqslant 0.0854395$	$\leqslant 0.124189$
4	$\leqslant 0.137102$	$\leqslant 0.140993$
5	$\leqslant 0.142281$	$\leqslant 0.142671$
6	$\leqslant 0.1428$	$\leqslant 0.142839$
7	$\leqslant 0.142851$	$\leqslant 0.142855$
8	$\leqslant 0.142857$	$\leqslant 0.142857$

Tabela 5 – Distância produto normalizada de $\Lambda(t_{\max} + \epsilon)$, onde $\Lambda(t)$ é dada por $\text{Rot}(\mathbb{Z}^3, (1, 1, 1))$

Observação 25. *Em relação aos resultados que constam na Tabela 5, a menos que o mínimo seja encontrado fora da coroa esférica* $1 \leqslant k_1^2 + k_2^2 + k_3^2 \leqslant 10^6$, *podemos afirmar que o valor encontrado é de fato a distância produto do reticulado associado com a precisão apresentada. Percebemos numericamente que quando i é "grande", o limitante da distância produto do reticulado* $\Lambda(t_{\max} \pm 1/10^i)$ *associado é "próximo" de* $\frac{1}{7}$. *Essa análise foi a motivação para o Corolário 8 a seguir.*

Corolário 8. *Se F é a aplicação dada por (5.1), então*

$$\inf_{(k_1,k_2,k_3)\neq(0,0,0)} \lim_{\epsilon\to 0} F\left(k_1, k_2, k_3, t_{max} + \epsilon\right) = d_{p,\text{norm}}(\mathbb{Z}^3) = \frac{1}{7}.$$

Demonstração. Escrevendo $t_{max} = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$, temos da continuidade de $F(k_1, k_2, k_3, t_{max} + \epsilon)$ que

[1] Verificamos numericamente que os valores mínimos encontrados não se alteraram para $j = 2, 3, 4, 5, 6$.

$$
\begin{aligned}
& \lim_{\epsilon \to 0} F\left(k_1, k_2, k_3, t_{max} + \epsilon\right) \\
= \; & F(k_1, k_2, k_3, t_{\max}) \\
= \; & |1/27(-(k_1+k_2+k_3)(2k_1^2 - 5k_1k_2 + 2k_2^2 - 5(k_1+k_2)k_3 + 2k_3^2) + (k_1+k_2-2k_3) \\
& (2k_1 - k_2 - k_3)(k_1 - 2k_2 + k_3)\cos(\arccos(-13/14)) - 3\sqrt{3}(k_1-k_2)(k_1-k_3)(k_2- \\
& k_3)\text{sen}(\arccos(-13/14)))|. \\
= \; & \frac{1}{7}|k_1^3 - k_1^2k_2 - 2k_1k_2^2 + k_2^3 - 2k_1^2k_3 - k_1k_2k_3 - k_2^2k_3 - k_1k_3^2 - 2k_2k_3^2 + k_3^3|
\end{aligned}
$$

Tomando o inf temos:

$$
\begin{aligned}
& \inf_{(k_1,k_2,k_3)\neq(0,0,0)} \lim_{\epsilon \to 0} F\left(k_1, k_2, k_3, t_{max} + \epsilon\right) \\
= \; & \inf_{(k_1,k_2,k_3)\neq(0,0,0)} \frac{1}{7}|k_1^3 - k_1^2k_2 - 2k_1k_2^2 + k_2^3 - 2k_1^2k_3 - k_1k_2k_3 - k_2^2k_3 - k_1k_3^2 - 2k_2k_3^2 + k_3^3| \\
= \; & \frac{1}{7}.
\end{aligned}
$$

□

Observação 26. *Consideremos os valores de ϵ "próximos de zero", para os quais*

$$\Lambda\left(\frac{1}{6}\arccos\left(\frac{-13}{14}\right) + \epsilon\right)$$

tenha diversidade máxima. Da Proposição 16, temos que

$$d_{p,\text{norm}}\left(\Lambda\left(\frac{1}{6}\arccos\left(\frac{-13}{14}\right) + \epsilon\right)\right) \leqslant \frac{1}{7},$$

por outro lado, o Corolário 8 nos permite concluir que o lado esquerdo da desigualdade pode tornar-se arbitrariamente próximo de $\frac{1}{7}$, desde que tomemos ϵ suficientemente próximo de zero.

Observação 27. *Observamos que qualquer reticulado do conjunto Rot$(\mathbb{Z}^3, (1,1,1))$ (mediante Proposição 16) tem norma mínima e determinante iguais a 1. Dessa forma, todos os resultados desta seção permaneçerão inalterados se considerarmos a distância produto relativa ao invés da normalizada.*

5.2 Versões Rotacionadas por Quatérnios do Reticulado FCC

Apresentamos, a seguir, os resultados referentes às versões rotacionadas do reticulado FCC.

Na Proposição 17, consideramos rotações do reticulado FCC em torno da reta cujo vetor diretor é $(1,1,1)$, pois uma vez que $(1,1,0),(1,0,1),(0,1,1)$ são vetores de norma mínima de FCC, $(2,0,0),(0,2,0),(0,0,2)$ são vetores de FCC, já que $2\mathbb{Z}^3 \subset$ FCC, temos a simetria do vetor $(1,1,1)$ em relação ao FCC. Pela complexidade dos cálculos e pela limitação do programa Wolfram Mathematica, tornou-se inviável considerarmos rotações do reticulado FCC em torno de uma reta cujo vetor diretor é equidistante aos vetores da base deste reticulado.

Proposição 17. *Seja Rot(FCC,* $(1,1,1)$*) o conjunto de todas as rotações possíveis do reticulado FCC em torno da reta cujo vetor diretor é* $(1,1,1)$*. A máxima distância produto mínima normalizada para um reticulado em Rot(FCC,* $(1,1,1)$*) é* $\frac{1}{14}$.

Demonstração. Como FCC $= \{(2k_1+k_2+k_3, k_2, k_3) : k_1,k_2,k_3 \in \mathbb{Z}\}$, se tomarmos uma rotação de ângulo $2t$ em torno da reta cujo vetor diretor é $(1,1,1)$, ou seja, considerando $\hat{p} = \frac{1}{\sqrt{3}}\mathbf{i} + \frac{1}{\sqrt{3}}\mathbf{j} + \frac{1}{\sqrt{3}}\mathbf{k}$, pelo Teorema 3, temos:

$$\left(\cos(t) + \left(\frac{1}{\sqrt{3}}\mathbf{i} + \frac{1}{\sqrt{3}}\mathbf{j} + \frac{1}{\sqrt{3}}\mathbf{k}\right)\text{sen}(t)\right) \cdot ((2k_1+k_2+k_3)\mathbf{i} + k_2\mathbf{j} + k_3\mathbf{k}) \cdot$$

$$\left(\cos(t) - \left(\frac{1}{\sqrt{3}}\mathbf{i} + \frac{1}{\sqrt{3}}\mathbf{j} + \frac{1}{\sqrt{3}}\mathbf{k}\right)\text{sen}(t)\right) = A\mathbf{i} + B\mathbf{j} + C\mathbf{k},$$

em que

$$A = \frac{1}{3}(2(k_1+k_2+k_3) + (4k_1+k_2+k_3)\cos(2t) + \sqrt{3}(-k_2+k_3)\text{sen}(2t)),$$
$$B = k_2\cos^2 t + \frac{1}{3}(4k_1+k_2+4k_3)\text{sen}^2 t + \frac{(2k_1+k_2)\text{sen}(2t)}{\sqrt{3}},$$
$$C = k_3\cos^2 t + \frac{\text{sen}t}{3}(-2\sqrt{3}(2k_1+k_3)\cos t + (4(k_1+k_2)+k_3)\text{sen}t).$$

Dessa forma, temos que Rot(FCC, $(1,1,1)$) é o conjunto das ternas ordenadas (A,B,C) com A,B e C descritos pelas igualdades acima, onde $k_1,k_2,k_3 \in \mathbb{Z}$ e $0 < t < \pi$. Levando em conta a simetria do vetor $(1,1,1)$ em relação ao FCC, podemos tomar $0 < t < \pi/6$. O valor absoluto do produto das coordenadas de um ponto em Rot(FCC, $(1,1,1)$) é:

$$F(k_1,k_2,k_3,t) = |ABC| = |(1/27)\ (-2(k_1+k_2+k_3)(8k_1^2 - 2k_1(k_2+k_3) - k_2^2 - 11k_2k_3 - k_3^2) - 3\sqrt{3}(2k_1+k_2)(2k_1+k_3)(k_2-k_3)\text{sen}(6t) + \cos(6t)(2(k_1+k_2)-k_3)(4k_1+k_2+k_3)(2k_1-k_2+2k_3))|. \quad (5.4)$$

Observamos que para um t qualquer em $0 < t < \pi/6$ podemos estabelecer os limitantes superiores $F(-1,1,1,t) = \frac{1}{27}|2-2\cos(6t)| = \frac{1}{27}(2-2\cos(6t))$ e $F(-1,1,0,t) = \frac{2|\text{sen}(6t)|}{3\sqrt{3}} = \frac{2\text{sen}(6t)}{3\sqrt{3}}$ para o valor mínimo desse produto F.

Quando consideramos a função $\alpha(t) = \min\left(F(-1,1,1,t), F(-1,1,0,t)\right)$ que também é um limitante superior, concluímos que o maior valor para esse limitante ocorre em $t = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$, já que se trata da mesma função $\alpha(t)$ definida na demonstração da Proposição 16. Ver Figuras 22 (que agora representa $F(-1,1,1,t)$ e $F(-1,1,0,t)$) e 23.

Vamos definir a aplicação $f(k_1,k_2,k_3) = F\left(k_1,k_2,k_3,\frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right)$, ou seja, $f(k_1,k_2,k_3) = \frac{1}{7}|g(k_1,k_2,k_3)|$, onde $g(k_1,k_2,k_3) = 4k_1^2(2k_2+k_3) + 8k_1^3 - 2k_1(k_2^2 + k_2k_3 + 2k_3^2) - 5k_2^2k_3 - k_2^3 - 6k_2k_3^2 - k_3^3$. Observamos que o mínimo de f ocorre no mínimo de $|g|$.

Afirmação: $g(k_1,k_2,k_3) = 0 \Leftrightarrow k_1 = k_2 = k_3 = 0$, portanto, $\min|g(k_1,k_2,k_3)| = 1$ se considerarmos $(k_1,k_2,k_3) \neq (0,0,0)$.

Com efeito, como k_1, k_2 e k_3 são pares ou ímpares, temos $2^3 = 8$ possibilidades distintas:

Caso 1: todos eles ímpares (1 possibilidade); Caso 2: dois deles ímpares (3 possibilidades); Caso 3: um deles ímpar (3 possibilidades); Caso 4: nenhum deles ímpar, ou seja, todos eles pares (1 possibilidade).

Em relação aos Casos 1 e 2 vamos mostrar que $g(k_1,k_2,k_3)$ será ímpar, portanto, $g(k_1,k_2,k_3) = 0$ não pode ser verdade.

Caso 1: Escrevendo $k_i = 2w_i + 1$, onde $w_i \in \mathbb{Z}$, para $i = 1,2,3$, temos: $g(2w_1 + 1, 2w_2 + 1, 2w_3 + 1) = 2(32w_1^2w_2 + 16w_1^2w_3 + 32w_1^3 + 72w_1^2 - 8w_1w_2^2 - 8w_1w_2w_3 + 20w_1w_2 - 16w_1w_3^2 - 4w_1w_3 + 40w_1 - 20w_2^2w_3 - 4w_2^3 - 20w_2^2 - 24w_2w_3^2 - 48w_2w_3 - 17w_2 - 4w_3^3 - 26w_3^2 - 26w_3 - 1) + 1$ que é ímpar.

Caso 2: Escrevendo $k_1 = 2w_1 + 1, k_2 = 2w_2 + 1, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i = 1,2,3$, temos: $g(2w_1 + 1, 2w_2 + 1, 2w_3) = 2(32w_1^2w_2 + 16w_1^2w_3 + 32w_1^3 + 64w_1^2 - 8w_1w_2^2 - 8w_1w_2w_3 + 24w_1w_2 - 16w_1w_3^2 + 12w_1w_3 + 38w_1 - 20w_2^2w_3 - 4w_2^3 - 10w_2^2 - 24w_2w_3^2 - 24w_2w_3 + w_2 - 4w_3^3 - 20w_3^2 - 3w_3 + 6) + 1$ que é ímpar.

Escrevendo $k_1 = 2w_1 + 1, k_2 = 2w_2, k_3 = 2w_3 + 1$, onde $w_i \in \mathbb{Z}$, para $i = 1,2,3$, temos: $g(2w_1 + 1, 2w_2, 2w_3 + 1) = 2(32w_1^2w_2 + 16w_1^2w_3 + 32w_1^3 + 56w_1^2 - 8w_1w_2^2 - 8w_1w_2w_3 + 28w_1w_2 - 16w_1w_3^2 + 28w_1 - 20w_2^2w_3 - 4w_2^3 - 14w_2^2 - 24w_2w_3^2 - 28w_2w_3 - 4w_3^3 - 14w_3^2 - 7w_3 + 3) + 1$ que é ímpar.

Escrevendo $k_1 = 2w_1, k_2 = 2w_2 + 1, k_3 = 2w_3 + 1$, onde $w_i \in \mathbb{Z}$, para $i = 1,2,3$, temos: $g(2w_1, 2w_2 + 1, 2w_3 + 1) = 2(32w_1^2w_2 + 16w_1^2w_3 + 32w_1^3 + 24w_1^2 - 8w_1w_2^2 - 8w_1w_2w_3 - 12w_1w_2 - 16w_1w_3^2 - 20w_1w_3 - 8w_1 - 20w_2^2w_3 - 4w_2^3 - 16w_2^2 - 24w_2w_3^2 - 44w_2w_3 - 19w_2 - 4w_3^3 - 18w_3^2 - 20w_3 - 7) + 1$ que é ímpar.

Dividimos o Caso 3 em dois subcasos. No primeiro, consideramos $g(k_1, k_2, k_3)$, quando k_1 é ímpar, k_2 e k_3 são pares. No segundo, considerando as outras duas possibilidades, temos, assim como nos Casos 1 e 2 que $g(k_1, k_2, k_3)$ é ímpar, portanto, $g(k_1, k_2, k_3) = 0$ não pode ser verdade.

Caso 3.1: Escrevendo $k_1 = 2w_1 + 1, k_2 = 2w_2, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i = 1, 2, 3$, temos: $g(2w_1 + 1, 2w_2, 2w_3) = 8(8w_1^2w_2 + 4w_1^2w_3 + 8w_1^3 + 12w_1^2 - 2w_1w_2^2 - 2w_1w_2w_3 + 8w_1w_2 - 4w_1w_3^2 + 4w_1w_3 + 6w_1 - 5w_2^2w_3 - w_2^3 - w_2^2 - 6w_2w_3^2 - w_2w_3 + 2w_2 - w_3^3 - 2w_3^2 + w_3 + 1)$ que é par.

Observamos que $g(2w_1 + 1, 2w_2, 2w_3) = 0 \Leftrightarrow h(w_1, w_2, w_3) = 0$, onde $h(w_1, w_2, w_3) = 8w_1^2w_2 + 4w_1^2w_3 + 8w_1^3 + 12w_1^2 - 2w_1w_2^2 - 2w_1w_2w_3 + 8w_1w_2 - 4w_1w_3^2 + 4w_1w_3 + 6w_1 - 5w_2^2w_3 - w_2^3 - w_2^2 - 6w_2w_3^2 - w_2w_3 + 2w_2 - w_3^3 - 2w_3^2 + w_3 + 1$.

Por outro lado, mostramos que $h(w_1, w_2, w_3)$ é ímpar, quaisquer que sejam os inteiros w_1, w_2 e w_3, o que nos leva uma contradição, logo $g(2w_1 + 1, 2w_2, 2w_3) \neq 0$.
Com efeito, considerando a paridade de w_1, w_2 e w_3 temos as 8 possibilidades a seguir para o valor de h.

Possibilidade 1: $h(2y_1 + 1, 2y_2 + 1, 2y_3 + 1) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 96y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 36y_1y_2 - 16y_1y_3^2 + 4y_1y_3 + 82y_1 - 20y_2^2y_3 - 4y_2^3 - 22y_2^2 - 24y_2y_3^2 - 50y_2y_3 - 10y_2 - 4y_3^3 - 30y_3^2 - 26y_3 + 14) + 1$ que é ímpar.

Possibilidade 2: $h(2y_1 + 1, 2y_2 + 1, 2y_3) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 88y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 40y_1y_2 - 16y_1y_3^2 + 20y_1y_3 + 76y_1 - 20y_2^2y_3 - 4y_2^3 - 12y_2^2 - 24y_2y_3^2 - 26y_2y_3 + 9y_2 - 4y_3^3 - 24y_3^2 + y_3 + 20) + 1$ que é ímpar.

Possibilidade 3: $h(2y_1 + 1, 2y_2, 2y_3 + 1) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 80y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 44y_1y_2 - 16y_1y_3^2 + 8y_1y_3 + 62y_1 - 20y_2^2y_3 - 4y_2^3 - 16y_2^2 - 24y_2y_3^2 - 30y_2y_3 + 9y_2 - 4y_3^3 - 18y_3^2 - 6y_3 + 14) + 1$ que é ímpar.

Possibilidade 4: $h(2y_1, 2y_2 + 1, 2y_3 + 1) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 48y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 4y_1y_2 - 16y_1y_3^2 - 12y_1y_3 + 10y_1 - 20y_2^2y_3 - 4y_2^3 - 18y_2^2 - 24y_2y_3^2 - 46y_2y_3 - 20y_2 - 4y_3^3 - 22y_3^2 - 24y_3 - 7) + 1$ que é ímpar.

Possibilidade 5: $h(2y_1 + 1, 2y_2, 2y_3) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 72y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 48y_1y_2 - 16y_1y_3^2 + 24y_1y_3 + 54y_1 - 20y_2^2y_3 - 4y_2^3 - 6y_2^2 - 24y_2y_3^2 - 6y_2y_3 + 18y_2 - 4y_3^3 - 12y_3^2 + 9y_3 + 13) + 1$ que é ímpar.

Possibilidade 6: $h(2y_1, 2y_2 + 1, 2y_3) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 40y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 8y_1y_2 - 16y_1y_3^2 + 4y_1y_3 + 12y_1 - 20y_2^2y_3 - 4y_2^3 - 8y_2^2 - 24y_2y_3^2 - 22y_2y_3 - 3y_2 - 4y_3^3 - 16y_3^2 - 5y_3) + 1$ que é ímpar.

Possibilidade 7: $h(2y_1, 2y_2, 2y_3 + 1) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 32y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 12y_1y_2 - 16y_1y_3^2 - 8y_1y_3 + 6y_1 - 20y_2^2y_3 - 4y_2^3 - 12y_2^2 - 24y_2y_3^2 - 26y_2y_3 - 5y_2 - 4y_3^3 - 10y_3^2 - 6y_3 - 1) + 1$ que é ímpar.

Possibilidade 8: $h(2y_1, 2y_2, 2y_3) = 2(32y_1^2y_2 + 16y_1^2y_3 + 32y_1^3 + 24y_1^2 - 8y_1y_2^2 - 8y_1y_2y_3 + 16y_1y_2 - 16y_1y_3^2 + 8y_1y_3 + 6y_1 - 20y_2^2y_3 - 4y_2^3 - 2y_2^2 - 24y_2y_3^2 - 2y_2y_3 + 2y_2 - 4y_3^3 - 4y_3^2 + y_3) + 1$ que é ímpar.

Caso 3.2: Escrevendo $k_1 = 2w_1, k_2 = 2w_2 + 1, k_3 = 2w_3$, onde $w_i \in \mathbb{Z}$, para $i = 1, 2, 3$, temos: $g(2w_1, 2w_2 + 1, 2w_3) = 2(32w_1^2w_2 + 16w_1^2w_3 + 32w_1^3 + 16w_1^2 - 8w_1w_2^2 - 8w_1w_2w_3 - 8w_1w_2 - 16w_1w_3^2 - 4w_1w_3 - 2w_1 - 20w_2^2w_3 - 4w_2^3 - 6w_2^2 - 24w_2w_3^2 - 20w_2w_3 - 3w_2 - 4w_3^3 - 12w_3^2 - 5w_3 - 1) + 1$ que é ímpar.

Escrevendo $k_1 = 2w_1, k_2 = 2w_2, k_3 = 2w_3 + 1$, onde $w_i \in \mathbb{Z}$, para $i = 1, 2, 3$, temos: $g(2w_1, 2w_2, 2w_3 + 1) = 2(32w_1^2w_2 + 16w_1^2w_3 + 32w_1^3 + 8w_1^2 - 8w_1w_2^2 - 8w_1w_2w_3 - 4w_1w_2 - 16w_1w_3^2 - 16w_1w_3 - 4w_1 - 20w_2^2w_3 - 4w_2^3 - 10w_2^2 - 24w_2w_3^2 - 24w_2w_3 - 6w_2 - 4w_3^3 - 6w_3^2 - 3w_3 - 1) + 1$ que é ímpar.

Caso 4: Finalmente, $g(k_1, k_2, k_3) = 0$ não pode ser verdade se considerarmos $(k_1, k_2, k_3) \neq (0, 0, 0)$. O argumento é exatamente o mesmo apresentado no Caso 4 da demonstração da Proposição 16. Assim, a igualdade $g(k_1, k_2, k_3) = 0$ só é verdadeira para $k_1 = k_2 = k_3 = 0$.

Portanto, temos $g(0, -1, 0) = 1$, por exemplo, e o valor mínimo de f será $\frac{1}{7}$. Dessa forma, como o volume do reticulado FCC é $V(FCC) = 2$, concluímos que a *máxima distância produto mínima normalizada* para um reticulado em $\mathrm{Rot}(\mathrm{FCC}, (1, 1, 1))$ será igual:

$$\begin{aligned} \mathrm{d_{p,norm}}(FCC) &= \frac{1}{V(FCC)} F\left(-1, 1, 1, \frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right) \\ &= \frac{1}{V(FCC)} F\left(-1, 1, 0, \frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right) \\ &= \frac{1}{2} \cdot \frac{1}{7} = \frac{1}{14}. \end{aligned}$$

□

A matriz do reticulado cuja distância produto mínima é dada pela Proposição 17 é $C = QE$, onde Q é dada por (5.2) e a matriz E é dada no Exemplo 17, logo

$$C = QE = \begin{bmatrix} 1.47395 & 0.408991 & 1.32799 \\ 1.18202 & 1.32799 & 0.263024 \\ -0.655971 & 0.263024 & 0.408991 \end{bmatrix}. \tag{5.5}$$

Poderíamos ter enunciado, na Proposição 17, a distância produto relativa ao invés da normalizada do reticulado FCC. Para encontrarmos tal distância bastaria, no final da demonstração desta Proposição, termos dividido $F\left(-1,1,1,\frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right)$ pelo cubo do vetor de norma mínima do FCC, assim teríamos:

$$\begin{aligned}\mathrm{d}_{\mathrm{p,rel}}(FCC) &= \frac{1}{\mu^3}F\left(-1,1,1,\frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right)\\ &= \frac{1}{\mu^3}F\left(-1,1,0,\frac{1}{6}\arccos\left(\frac{-13}{14}\right)\right)\\ &= \frac{1}{(\sqrt{2})^3}\cdot\frac{1}{7}=\frac{1}{7\sqrt{2^3}}.\end{aligned}$$

Essa é a maior distância produto mínima relativa conhecida do FCC conforme podemos ver em [23]. Com isso, temos a Proposição 18 que é dada a seguir.

Proposição 18. *Seja* $Rot(FCC,(1,1,1))$ *o conjunto de todas as rotações possíveis do reticulado FCC em torno da reta cujo vetor diretor é* $(1,1,1)$. *A máxima distância produto mínima relativa para um reticulado em* $Rot(FCC,(1,1,1))$ *é* $\frac{1}{7\sqrt{2^3}}$.

Corolário 9. *Sejam* Λ *e* $\tilde{\Lambda}$ *as versões rotacionadas do reticulado FCC via quatérnios e via corpo ciclotômico* $\mathbb{K}=\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ *([22]) cujas matrizes são dadas, respectivamente, por (5.5) e (3.19). Os reticulados* Λ *e* $\tilde{\Lambda}$ *são distintos; além disso,* Λ *é obtido por meio de uma rotação anti-horária de* $\pi/2$ *em torno do eixo* Oy, *seguida de uma reflexão em torno do plano* $y=0$ *do reticulado* $\tilde{\Lambda}$.

Demonstração. Como $C^{-1}F$ não é unimodular, segue do Teorema 10, que os reticulados Λ e $\tilde{\Lambda}$ são distintos. Da igualdade (5.3), temos:

$$\begin{aligned}S_2S_1RU &= Q \Leftrightarrow\\ S_2S_1REE^{-1}U &= QEE^{-1} \Leftrightarrow\\ S_2S_1(RE)(E^{-1}UE) &= QE \Leftrightarrow\\ S_2S_1F\bar{U} &= C,\end{aligned}$$

em que

$$\bar{U}=E^{-1}UE=\begin{bmatrix}1&1&1\\0&0&-1\\0&-1&0\end{bmatrix}$$

é unimodular.

Como C e F são as matrizes dos reticulados Λ e $\tilde{\Lambda}$, respectivamente, da demonstração do Corolário 7, S_1 representa uma rotação anti-horária de $\pi/2$ em torno do eixo Oy e S_2 representa uma reflexão em torno do plano $y=0$, segue o resultado. □

Agora, vamos analisar o que ocorre com as distâncias produto dos reticulados $\Lambda(t) = \text{Rot}(\text{FCC}, (1,1,1))$ (mediante demonstração da Proposição 17), quando t é tomado em uma perturbação do ângulo ótimo $t_{\max} = \frac{1}{6}\arccos\left(\frac{-13}{14}\right)$, ou seja, quando tomamos $t = t_{\max} + \epsilon$, para ϵ arbitrariamente pequeno. Para estes valores de t escrevemos

$$d_{p,\text{norm}}(\Lambda(t)) = \frac{1}{V(FCC)} \inf_{(k_1,k_2,k_3)\neq(0,0,0)} F(k_1,k_2,k_3,t),$$

onde F é a função dada por (5.4).

Abordamos, inicialmente, o problema em uma perspectiva numérica. Resolvendo as dezoito equações $F(k_1,k_2,k_3,t_{\max}+\epsilon) = 0$, onde $\epsilon = \pm\frac{1}{10^i}$, para $i = 1,2,...,9$, nas variáveis inteiras k_1, k_2 e k_3 com a restrição $|k_1,k_2,k_3| \leqslant 1000$, encontramos sempre a solução $k_1 = k_2 = k_3 = 0$. Isso nos permite admitir, com certo grau de segurança, que nestes casos os reticulados $\Lambda(t_{\max}+\epsilon)$ têm diversidade máxima. Em segundo lugar minimizamos as funções $F(k_1,k_2,k_3,t_{\max}+\epsilon)$ nas variáveis inteiras k_1,k_2,k_3 quando consideramos a restrição $1 \leqslant k_1^2+k_2^2+k_3^2 \leqslant 10^j$ [2]. Dessa forma, encontramos limitantes para as distâncias produtos destes reticulados. Estes resultados estão sistematizados na Tabela 6.

i	$d_{p,\text{norm}}(\Lambda(t_{\max}+1/10^i))$	$d_{p,\text{norm}}(\Lambda(t_{\max}-1/10^i))$
1	$\leqslant 0.0240478$	$\leqslant 0.0227706$
2	$\leqslant 0.0508436$	$\leqslant 0.00851187$
3	$\leqslant 0.0692184$	$\leqslant 0.052903$
4	$\leqslant 0.071206$	$\leqslant 0.0694692$
5	$\leqslant 0.0714063$	$\leqslant 0.0712316$
6	$\leqslant 0.0714263$	$\leqslant 0.0714089$
7	$\leqslant 0.0714283$	$\leqslant 0.0714266$
8	$\leqslant 0.0714285$	$\leqslant 0.0714284$
9	$\leqslant 0.0714286$	$\leqslant 0.0714286$

Tabela 6 – Distância produto normalizada de $\Lambda(t_{\max}+\epsilon)$, onde $\Lambda(t)$ é dada por $\text{Rot}(\text{FCC}, (1,1,1))$

Observação 28. *Em relação aos resultados que constam na Tabela 6, a menos que o mínimo seja encontrado fora da coroa esférica* $1 \leqslant k_1^2+k_2^2+k_3^2 \leqslant 10^6$, *podemos afirmar que o valor encontrado é de fato a distância produto do reticulado associado com a precisão apresentada. Percebemos numericamente que quando i é "grande", o limitante da distância produto do reticulado* $\Lambda(t_{\max} \pm 1/10^i)$ *associado é "próximo" de* $\frac{1}{14}$. *Essa análise foi a motivação para o Corolário 10 a seguir, cuja demonstração é análoga a demonstração do Corolário 8.*

[2] Verificamos numericamente que os valores mínimos encontrados não se alteraram para $j = 2,3,4,5,6$.

Corolário 10. *Se F é a aplicação dada por (5.4), então*

$$\frac{1}{V(FCC)} \inf_{(k_1,k_2,k_3)\neq(0,0,0)} \lim_{\epsilon\to 0} F\left(k_1,k_2,k_3,t_{max}+\epsilon\right) = d_{p,\text{norm}}(\text{FCC}) = \frac{1}{14}.$$

Observação 29. *Consideremos os valores de ϵ "próximos de zero", para os quais*

$$\Lambda\left(\frac{1}{6}\arccos\left(\frac{-13}{14}\right)+\epsilon\right)$$

tenha diversidade máxima. Da Proposição 17, temos que

$$d_{p,\text{norm}}\left(\Lambda\left(\frac{1}{6}\arccos\left(\frac{-13}{14}\right)+\epsilon\right)\right) \leqslant \frac{1}{14},$$

por outro lado, o Corolário 10 nos permite concluir que o lado esquerdo da desigualdade pode tornar-se arbitrariamente próximo de $\frac{1}{14}$, desde que tomemos ϵ suficientemente próximo de zero.

Finalizamos essa seção com a Observação 30 a seguir.

Observação 30. *A construção de reticulados algébricos feita no Capítulo 3, explorada na Seção 4.2 e neste capítulo foi via corpos ciclotômicos construídos em $\mathbb{R}^n$ para $n=(p-1)/2$, onde $p\geqslant 5$ é um primo. De um modo geral, se Λ é gerado pela matriz*

$$\begin{bmatrix} & & & \pm 1 \\ & & \pm 1 & \\ & \cdots & & \\ \pm 1 & & & \end{bmatrix} RU, \tag{5.6}$$

onde R é a matriz geradora de um reticulado algébrico com diversidade máxima $\tilde{\Lambda}$ e U é unimodular, então Λ tem diversidade máxima, além disso, as distâncias produtos em Λ e $\tilde{\Lambda}$ são iguais. De fato, escrevendo

$$R = \begin{bmatrix} \mathbf{r}_1^t \\ \ldots \\ \mathbf{r}_n^t \end{bmatrix}$$

onde $\mathbf{r}_i^t$ designa a i-ésima linha de R, $\mathbf{y}=R\mathbf{x}$, com $\mathbf{x}\neq\mathbf{0}$, a distância produto de $\tilde{\Lambda}$ será dada por $d_p(\tilde{\Lambda}) = d_p^{(n)}(0,\mathbf{y}) = \prod_{i=1}^{n}|y_i| = \prod_{i=1}^{n}|\mathbf{r}_i^t\mathbf{x}|$. Uma vez que U é unimodular, temos que para o cálculo da distância produto de Λ basta que consideremos apenas as duas matrizes à esquerda de (5.6). Por outro lado, o produto da matriz à esquerda de R por R em (5.6) apenas inverte a ordem (a menos de sinal) das linhas de R, logo como o reticulado gerado por R tem diversidade máxima, segue que $d_p(\Lambda) = d_p(\tilde{\Lambda}) = \prod_{i=1}^{n}|\mathbf{r}_i^t\mathbf{x}| > 0$.

Observamos, ainda, que as matrizes de Λ nos Corolários 2, 7 e 9 são da forma (5.6). No Corolário 7, por exemplo, a matriz à esquerda de R e a unimodular U em (5.6)

são dadas, respectivamente, por:

$$\begin{bmatrix} & & -1 \\ & -1 & \\ 1 & & \end{bmatrix} \text{ e } U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}.$$

6 Os reticulados $\Lambda_{(e^X B)}$

Na primeira seção, deste capítulo, definimos e apresentamos alguns resultados referentes às matrizes exponenciais. As referências utilizadas foram: [1], [19], [21], [27] e [28].

Na segunda seção, foi feita uma análise das distâncias produtos de perturbações das versões rotacionadas do $\mathbb{Z}^5$, D_5, $\mathbb{Z}^8$ e D_8 que foram construídas no Capítulo 3 e por fim exibimos resultados gerais, considerando perturbações de um reticulado com diversidade máxima Λ_B, em que B é uma matriz geradora do mesmo.

Na terceira e última seção, construímos as mesmas versões rotacionadas do $\mathbb{Z}^3$ e do FCC encontradas no Capítulo 5. Essas construções são obtidas a partir de rotações do $\mathbb{Z}^3$ e do FCC via exponenciais de matrizes anti-simétricas.

O programa usado para os cálculos simbólicos foi o *Wolfram Mathematica* em sua versão 12.3 [43].

6.1 A Matriz Exponencial

O conceito de matriz exponencial é uma generalização da série de Taylor $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$, $x \in \mathbb{R}$. Em [1], vemos que para toda matriz $X \in \mathbb{R}^{m\times n}$, a série de matrizes $\sum_{k=0}^{\infty} \frac{X^k}{k!}$ converge. Isso nos motiva à Definição 61.

Definição 61 (Matriz Exponencial)**.** *Dada a matriz $A \in \mathbb{R}^{m\times n}$, definimos a matriz exponencial e^A como sendo*

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + ... + \frac{A^k}{k!} + ...$$

Segue imediatamente da Definição 61, que $e^0 = I$. Se A e B comutam, ou seja, $AB = BA$, vemos em [21] que $e^{A+B} = e^A e^B$.

Seja $X \in \mathbb{R}^{n\times n}$, vemos em [27], que a aplicação $\exp : X \mapsto e^X$ é contínua.

Temos, ainda que, se A é anti-simétrica, então e^A é ortogonal. Com efeito, uma vez que $\frac{(A^t)^k}{k!} = \left(\frac{A^k}{k!}\right)^t$, para todo k inteiro não-negativo, segue da Definição 61, que $e^{(A^t)} = (e^A)^t$. Por outro lado, como A e $-A$ comutam, decorre da última igualdade que $(e^A)(e^A)^t = (e^A)(e^{-A}) = e^0 = I$. De modo análogo, concluímos que $(e^A)^t(e^A) = I$.

Estes resultados referentes às matrizes exponenciais são suficientes para o que será desenvolvido no restante deste capítulo.

6.2 Os Reticulados $\Lambda_{(e^X B)}$ como Perturbações do Reticulado Λ_B

Nesta seção, a partir de um reticulado Λ_B com diversidade máxima gerado pela matriz B, analisamos a distância produto do reticulado $\Lambda_{(e^X B)}$, em que X é uma matriz anti-simétrica "próxima" da matriz nula, então o motivo para usarmos tais reticulados é que se X é uma matriz anti-simétrica qualquer a norma euclidiana é preservada, ou seja, dado $\mathbf{x} \in \mathbb{R}^n$ temos $||e^X B\mathbf{x}|| = ||B\mathbf{x}||$. Assim os reticulados Λ_B e $\Lambda_{(e^X B)}$ têm a mesma norma mínima e também têm o mesmo volume, uma vez que e^X é ortogonal.

Em primeiro lugar analisamos as perturbações das versões rotacionadas do $\mathbb{Z}^5$ e do D_5 cujas matrizes geradoras R e F são dadas por (3.16) e (3.20) respectivamente. Para tal, vamos considerar as famílias de reticulados $\Lambda_{(e^X R)}$ e $\Lambda_{(e^X F)}$, ou seja, os reticulados que possuem matrizes geradoras dadas por $e^X R$ e $e^X F$, onde X é uma matriz 5×5 anti-simétrica "próxima" da matriz nula. Para estabelecermos de forma mais precisa a relação de proximidade entre matrizes consideramos a norma de Frobenius. A partir da Definição 13, dizemos que uma matriz A tende para a matriz nula, se e somente se, a norma de Frobenius desta tende para zero, ou seja, $A \to 0 \Leftrightarrow ||A|| \to 0$.

Na nossa análise das perturbações da versões rotacionadas do $\mathbb{Z}^5$ e do D_5 tomamos matrizes $X(k) = [x_{ij}^{(k)}]$ anti-simétricas tais que $x_{ij}^{(k)} = 10^{-k}$ $(i < j)$, onde k é um inteiro positivo "grande". Assim, $||X||^2 = (20)10^{-2k} \to 0$, quando $k \to \infty$; portanto, $X \to 0$. Considerando a aplicação $f : \mathbb{R}^{5\times 5} \times \mathbb{Z}^5 \to \mathbb{R}$ dada por

$$f(X, \mathbf{z}) = \prod_{i=1}^{5} |\mathbf{x}_i^t \mathbf{z}|,$$

em que $\mathbf{x}_i^t$ é a i-ésima linha da matriz X, segue que se $\Lambda_{(e^{X(k)}R)}$ e $\Lambda_{(e^{X(k)}F)}$ têm diversidade máxima, então

$$d_{p,\text{norm}}(\Lambda_{(e^{X(k)}R)}) = d_{p,\text{inf}}(\Lambda_{(e^{X(k)}R)}) = \inf_{\mathbf{z}\neq\mathbf{0}} f(e^{X(k)}R, \mathbf{z}) \tag{6.1}$$

e

$$d_{p,\text{norm}}(\Lambda_{(e^{X(k)}F)}) = \frac{1}{V(D_n)} d_{p,\text{inf}}(\Lambda_{(e^{X(k)}F)}) = \frac{1}{2} \inf_{\mathbf{z}\neq\mathbf{0}} f(e^{X(k)}F, \mathbf{z}), \tag{6.2}$$

uma vez que $|\det(e^X R)| = 1$, $|\det(e^X F)| = V(D_n)$, pois $F = RE$ e as matrizes R e e^X são ortogonais.

Dessa forma, minimizamos as funções $f(e^{X(k)}R, \mathbf{z})$ e $\frac{1}{2}f(e^{X(k)}F, \mathbf{z})$, em que $k = 1, 2, ..., 10$, na variável $\mathbf{z}$ quando consideramos a restrição $1 \leqslant ||\mathbf{z}||^2 \leqslant 10^r$ [1]. Tais resultados estão sistematizados na Tabela 7.

[1] Verificamos numericamente que os valores mínimos encontrados não se alteraram para $r = 2, 3, 4, 5, 6$.

k	$d_{p,\mathrm{norm}}(\Lambda_{(e^{X(k)}R)})$	$d_{p,\mathrm{norm}}(\Lambda_{(e^{X(k)}F)})$
1	$\leqslant 4.34085 \times 10^{-5}$	$\leqslant 5.70284 \times 10^{-6}$
2	$\leqslant 2.62652 \times 10^{-4}$	$\leqslant 2.30043 \times 10^{-4}$
3	$\leqslant 2.25437 \times 10^{-3}$	$\leqslant 1.33931 \times 10^{-4}$
4	$\leqslant 6.56336 \times 10^{-3}$	$\leqslant 3.55589 \times 10^{-3}$
5	$\leqslant 8.0943 \times 10^{-3}$	$\leqslant 4.07466 \times 10^{-3}$
6	$\leqslant 8.24745 \times 10^{-3}$	$\leqslant 4.12648 \times 10^{-3}$
7	$\leqslant 8.26276 \times 10^{-3}$	$\leqslant 4.13166 \times 10^{-3}$
8	$\leqslant 8.26434 \times 10^{-3}$	$\leqslant 4.13217 \times 10^{-3}$
9	$\leqslant 8.26445 \times 10^{-3}$	$\leqslant 4.13222 \times 10^{-3}$
10	$\leqslant 8.26446 \times 10^{-3}$	$\leqslant 4.13223 \times 10^{-3}$

Tabela 7 – Perturbações de versões rotacionadas do $\mathbb{Z}^5$ e do D_5

Observação 31. *Em relação aos resultados que constam na Tabela 7, a menos que o mínimo seja encontrado fora da coroa esférica* $1 \leqslant ||\mathbf{z}||^2 \leqslant 10^6$, *podemos afirmar que o valor encontrado é, de fato, a distância produto do reticulado associado com a precisão apresentada. Caso tal reticulado não tenha diversidade máxima, o mínimo a ser encontrado obviamente será zero. Percebemos numericamente que quando k é "grande", os limitantes das distâncias produtos dos reticulados* $\Lambda_{(e^{X(k)}R)}$ *e* $\Lambda_{(e^{X(k)}F)}$ *associados são "próximos" de* $d_{p,\mathrm{norm}}(\mathbb{Z}^5) = \dfrac{1}{121}$ *e* $d_{p,\mathrm{norm}}(D_5) = \dfrac{1}{242}$, *respectivamente.*

Ainda em relação a Tabela 7, percebemos que os limitantes das distâncias produtos dos reticulados $\Lambda_{(e^{X(k)}R)}$ e $\Lambda_{(e^{X(k)}F)}$, quando k cresce, aproximam-se de 1/121 e 1/242, sempre por valores menores a eles. Isso parece nos indicar que as versões rotacionadas do $\mathbb{Z}^5$ e do D_5 que podem ser representadas por $\Lambda_{(e^0R)}$ e $\Lambda_{(e^0F)}$ são reticulados "ótimos" de modo que suas distâncias produtos parecem ser pontos de máximos locais das funções que calculam as distâncias produtos dos reticulados perturbados. Isso nos motiva à Conjectura 7.

Conjectura 7. *Seja* X *uma matriz anti-simétrica* 5×5, $\Lambda_{(e^X R)}$ *e* $\Lambda_{(e^X F)}$ *reticulados de diversidades máximas com matrizes geradoras dadas por* $e^X R$ *e* $e^X F$, *em que* R *e* F *são as matrizes geradoras das versões rotacionadas do* $\mathbb{Z}^5$ *e do* D_5 *dadas por (3.16) e (3.20), respectivamente. Temos:*

(1) A aplicação $X \mapsto d_{p,\mathrm{norm}}(\Lambda_{(e^X R)})$ *tem máximo local dado por*

$$d_{p,\mathrm{norm}}(\Lambda_{(e^0 R)}) = d_{p,\mathrm{norm}}(\mathbb{Z}^5) = \frac{1}{121}.$$

(2) A aplicação $X \mapsto d_{p,\text{norm}}(\Lambda_{(e^X F)})$ tem máximo local dado por

$$d_{p,\text{norm}}(\Lambda_{(e^0 F)}) = d_{p,\text{norm}}(D_5) = \frac{1}{242}.$$

Agora, vamos às perturbações das versões rotacionadas do $\mathbb{Z}^8$ e do D_8 cujas matrizes geradoras R e F são dadas nos Exemplos 15 e 19 respectivamente. Para tal, vamos considerar as famílias de reticulados $\Lambda_{(e^X R)}$ e $\Lambda_{(e^X F)}$, onde X é uma matriz 8×8 anti-simétrica "próxima" da matriz nula. Tomamos as matrizes $X(k) = [x_{ij}^{(k)}]$ anti-simétricas tais que $x_{ij}^{(k)} = 10^{-k}$ $(i < j)$, onde k é um inteiro positivo "grande". Assim, $||X||^2 = (56)10^{-2k} \to 0$, quando $k \to \infty$; portanto, $X \to 0$. Considerando a aplicação $f : \mathbb{R}^{8\times 8} \times \mathbb{Z}^8 \to \mathbb{R}$ dada por

$$f(X, \mathbf{z}) = \prod_{i=1}^{8} |\mathbf{x}_i^t \mathbf{z}|, \tag{6.3}$$

segue que valem as igualdades (6.1) e (6.2) desde que $\Lambda_{(e^{X(k)} R)}$ e $\Lambda_{(e^{X(k)} F)}$ tenham diversidade máxima.

Dessa forma, minimizamos as funções $f(e^{X(k)}R, \mathbf{z})$ e $\frac{1}{2}f(e^{X(k)}F, \mathbf{z})$, onde $k = 1, 2, ..., 10$, na variável $\mathbf{z}$ quando consideramos a restrição $1 \leqslant ||\mathbf{z}||^2 \leqslant 10^r$ [2]. Estes resultados estão sistematizados na Tabela 8.

k	$d_{p,\text{norm}}(\Lambda_{(e^{X(k)} R)})$	$d_{p,\text{norm}}(\Lambda_{(e^{X(k)} F)})$
1	$\leqslant 9.06862 \times 10^{-9}$	$\leqslant 2.27287 \times 10^{-9}$
2	$\leqslant 1.87049 \times 10^{-7}$	$\leqslant 2.36278 \times 10^{-7}$
3	$\leqslant 5.50933 \times 10^{-7}$	$\leqslant 1.18847 \times 10^{-6}$
4	$\leqslant 1.59811 \times 10^{-5}$	$\leqslant 5.21592 \times 10^{-6}$
5	$\leqslant 3.34653 \times 10^{-5}$	$\leqslant 2.17172 \times 10^{-5}$
6	$\leqslant 4.7776 \times 10^{-5}$	$\leqslant 2.43867 \times 10^{-5}$
7	$\leqslant 4.92071 \times 10^{-5}$	$\leqslant 2.46534 \times 10^{-5}$
8	$\leqslant 4.93502 \times 10^{-5}$	$\leqslant 2.46801 \times 10^{-5}$
9	$\leqslant 4.93645 \times 10^{-5}$	$\leqslant 2.46828 \times 10^{-5}$
10	$\leqslant 4.93659 \times 10^{-5}$	$\leqslant 2.4683 \times 10^{-5}$

Tabela 8 – Perturbações de versões rotacionadas do $\mathbb{Z}^8$ e do D_8

Observação 32. *Em relação aos resultados que constam na Tabela 8, a menos que o mínimo seja encontrado fora da coroa esférica $1 \leqslant ||\mathbf{z}||^2 \leqslant 10^6$, podemos afirmar que o valor encontrado é de fato a distância produto do reticulado associado com a precisão apresentada. Caso tal reticulado não tenha diversidade máxima, o mínimo a ser encontrado obviamente será zero. Percebemos, numericamente, que quando k é "grande", o limitantes*

[2] Verificamos numericamente que os valores mínimos encontrados não se alteraram para $r = 2, 3, 4, 5, 6$.

das distâncias produtos dos reticulados $\Lambda_{(e^{X(k)}R)}$ e $\Lambda_{(e^{X(k)}F)}$ associados são "próximos" de $d_{p,\text{norm}}(\mathbb{Z}^8) = \dfrac{1}{17^{7/2}}$ e $d_{p,\text{norm}}(D_8) = \dfrac{1}{2\cdot 17^{7/2}}$, respectivamente.

Ainda, em relação a Tabela 8, percebemos que os limitantes das distâncias produtos dos reticulados $\Lambda_{(e^{X(k)}R)}$ e $\Lambda_{(e^{X(k)}F)}$, quando k cresce, aproximam-se de $1/17^{7/2}$ e $1/(2\cdot 17^{7/2})$ sempre por valores menores a eles. Isso parece nos indicar que as versões rotacionadas do $\mathbb{Z}^8$ e do D_8 que podem ser representadas por $\Lambda_{(e^0R)}$ e $\Lambda_{(e^0F)}$ são reticulados "ótimos" de modo que suas distâncias produtos parecem ser pontos de máximos locais das funções que calculam as distâncias produtos dos reticulados perturbados. Isso nos motiva à Conjectura 8.

Conjectura 8. *Seja X uma matriz anti-simétrica 8×8, $\Lambda_{(e^XR)}$ e $\Lambda_{(e^XF)}$ reticulados de diversidades máximas com matrizes geradoras dadas por e^XR e e^XF, onde R e F são as matrizes geradoras das versões rotacionadas do $\mathbb{Z}^8$ e do D_8 encontradas nos Exemplos 15 e 19, respectivamente. Temos:*

(1) A aplicação $X \mapsto d_{p,\text{norm}}(\Lambda_{(e^XR)})$ tem máximo local dado por

$$d_{p,\text{norm}}(\Lambda_{(e^0R)}) = d_{p,\text{norm}}(\mathbb{Z}^8) = \frac{1}{17^{7/2}}.$$

(2) A aplicação $X \mapsto d_{p,\text{norm}}(\Lambda_{(e^XF)})$ tem máximo local dado por

$$d_{p,\text{norm}}(\Lambda_{(e^0F)}) = d_{p,\text{norm}}(D_8) = \frac{1}{2\cdot 17^{7/2}}.$$

A análise das perturbações das versões rotacionadas dos reticulados $\mathbb{Z}^5$, D_5, $\mathbb{Z}^8$ e D_8 foi a motivação para a Proposição 19, os Corolários 11 e 12.

Proposição 19. *Sejam Λ_B um reticulado de diversidade máxima com matriz geradora B e $f : \{X \in \mathbb{R}^{n\times n} : X^t = -X\} \times \mathbb{Z}^n \to \mathbb{R}$ a aplicação dada por*

$$f(X, \mathbf{z}) = \prod_{i=1}^{n} |\mathbf{x}_i^t \mathbf{z}|, \tag{6.4}$$

em que $\mathbf{x}_i^t$ é a i-ésima linha da matriz X. Temos:

$$\inf_{\mathbf{z}\neq\mathbf{0}} \lim_{X\to 0} f(e^XB, \mathbf{z}) = d_{p,\text{inf}}(\Lambda_B).$$

Demonstração. Segue do Teorema 7, que a matriz nula $0 \in \mathbb{R}^{n\times n}$ é um ponto de acumulação do conjunto $\{X \in \mathbb{R}^{n\times n} : X^t = -X\}$, pois dada uma sequência de matrizes anti-simétricas distintas $X_k = [x_{ij}^{(k)}]$, onde $\max x_{ij}^{(k)} \to 0$ quando $k \to \infty$, segue que

$$||X_k||^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} |x_{ij}^{(k)}|^2 \leqslant n^2 |\max x_{ij}^{(k)}|^2 \to 0,$$

donde $X_k \to 0$. Como as aplicações f e $X \mapsto e^X B$ são contínuas, segue dos Teoremas 8 e 9, que

$$\lim_{X\to 0} f(e^X B, \mathbf{z}) = f(\lim_{X\to 0}(e^X B, \mathbf{z})) = f(e^0 B, \mathbf{z}) = f(B, \mathbf{z}),$$

daí, segue que

$$\inf_{\mathbf{z}\neq \mathbf{0}} \lim_{X\to 0} f(e^X B, \mathbf{z}) = \inf_{\mathbf{z}\neq \mathbf{0}} f(B, \mathbf{z}) = d_{p,\inf}(\Lambda_B).$$

□

Corolário 11. *Sejam Λ_B um reticulado de diversidade máxima com matriz geradora B e f dada por (6.4). Temos:*

$$\frac{1}{(\min_{0\neq \mathbf{z}\in\mathbb{Z}^n} ||e^X B\mathbf{z}||)^n} \inf_{\mathbf{z}\neq \mathbf{0}} \lim_{X\to 0} f(e^X B, \mathbf{z}) = d_{p,\mathrm{rel}}(\Lambda_B).$$

Demonstração. Dividindo $\inf_{\mathbf{z}\neq \mathbf{0}} \lim_{X\to 0} f(e^X B, \mathbf{z}) = d_{p,\inf}(\Lambda_B)$ por

$$\left(\min_{0\neq \mathbf{z}\in\mathbb{Z}^n} ||e^X B\mathbf{z}||\right)^n = \left(\min_{0\neq \mathbf{z}\in\mathbb{Z}^n} ||B\mathbf{z}||\right)^n$$

segue o resultado. □

Corolário 12. *Sejam Λ_B um reticulado de diversidade máxima com matriz geradora B e f dada por (6.4). Temos:*

$$\frac{1}{V(\Lambda_{(e^X B)})} \inf_{\mathbf{z}\neq \mathbf{0}} \lim_{X\to 0} f(e^X B, \mathbf{z}) = d_{p,\mathrm{norm}}(\Lambda_B).$$

Demonstração. Dividindo $\inf_{\mathbf{z}\neq \mathbf{0}} \lim_{X\to 0} f(e^X B, \mathbf{z}) = d_{p,\inf}(\Lambda_B)$ por $V(\Lambda_{(e^X B)}) = V(\Lambda_B)$, segue o resultado. □

Finalizamos essa seção com a Observação 33 a seguir.

Observação 33. *Se $\tilde{X} \simeq 0$ é uma matriz anti-simétrica de modo que o reticulado $\Lambda_{(e^{\tilde{X}} B)}$ tenha diversidade máxima, segue dos Corolários 11 e 12, que $d_{p,\mathrm{rel}}(\Lambda_{(e^{\tilde{X}} B)}) \simeq d_{p,\mathrm{rel}}(\Lambda_B)$ e $d_{p,\mathrm{norm}}(\Lambda_{(e^{\tilde{X}} B)}) \simeq d_{p,\mathrm{norm}}(\Lambda_B)$. Observamos que este último resultado é uma generalização dos resultados apresentados nas Observações 31 e 32.*

6.3 Os Reticulados $\Lambda_{(e^X B)}$ como Versões Rotacionadas dos Reticulados $\mathbb{Z}^3$ e FCC

Considerando a matriz anti-simétrica $X = X(t)$ dada por

$$\begin{bmatrix} 0 & -t & t \\ t & 0 & -t \\ -t & t & 0 \end{bmatrix}; t \in \mathbb{R}, \tag{6.5}$$

analisamos os reticulados $\Lambda_{e^{X(t)}}$ e $\Lambda_{(e^{X(t)}E)}$, em que E é a matriz do FCC encontrada no Exemplo 17. Estes reticulados são rotações do $\mathbb{Z}^3$ e FCC, a partir das quais construímos versões alternativas das Proposições 16, 17 e 18. Com efeito, como $e^{X(t)}$ é dada por

$$\begin{bmatrix} \frac{2}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} & -\frac{\operatorname{sen}\left(\sqrt{3}t\right)}{\sqrt{3}}-\frac{1}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} & \frac{\operatorname{sen}\left(\sqrt{3}t\right)}{\sqrt{3}}-\frac{1}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} \\ \frac{\operatorname{sen}\left(\sqrt{3}t\right)}{\sqrt{3}}-\frac{1}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} & \frac{2}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} & -\frac{\operatorname{sen}\left(\sqrt{3}t\right)}{\sqrt{3}}-\frac{1}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} \\ -\frac{\operatorname{sen}\left(\sqrt{3}t\right)}{\sqrt{3}}-\frac{1}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} & \frac{\operatorname{sen}\left(\sqrt{3}t\right)}{\sqrt{3}}-\frac{1}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} & \frac{2}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3} \end{bmatrix}$$

e uma vez que para $t \in \mathbb{R}$ temos

$$e^{X(t)}\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

segue que a matriz $e^{X(t)}$ possui autovalor 1 associado ao autovetor $(1,1,1)$ (mediante Definição 12). Por outro lado $(1,0,-1)$ não é autovetor de $e^{X(t)}$, logo, o conjunto $\Lambda_{e^{X(t)}}$ descreve versões rotacionadas do $\mathbb{Z}^3$ em torno da reta cujo vetor diretor é $(1,1,1)$. Por outro lado, como vimos que $\mathrm{Rot}(\mathbb{Z}^3,(1,1,1))$, descrito na Proposição 16 é o conjunto de todas as rotações possíveis do $\mathbb{Z}^3$ em torno da reta cujo vetor diretor é $(1,1,1)$, segue que se existir $t=t_1$ de tal forma que $\Lambda_{e^{X(t_1)}}$ represente o "reticulado ótimo" encontrado na Proposição 16, este terá a distância produto mínima normalizada dada por $\frac{1}{7}$.

Do que foi exposto no parágrafo anterior, admitamos que a matriz do reticulado $\Lambda_{e^{X(t_1)}}$ seja $Q=[q_{ij}]$ dada por (5.2). Da demonstração da Proposição 16 temos que $q_{11}=\frac{1}{3}\left(1+2\cos\left(\frac{1}{3}\arccos\left(-\frac{13}{14}\right)\right)\right)\simeq 0.736976$. Logo, temos a equação

$$\frac{2}{3}\cos\left(\sqrt{3}t\right)+\frac{1}{3}=\frac{1}{3}\left(1+2\cos\left(\frac{1}{3}\arccos\left(-\frac{13}{14}\right)\right)\right)$$

cuja solução é $t=\dfrac{\pm\frac{1}{3}\arccos\left(-\frac{13}{14}\right)+2\pi k}{\sqrt{3}}$, $k\in\mathbb{Z}$. Da última igualdade, vemos que se tomarmos

$$t=t_1=\frac{\frac{1}{3}\arccos\left(-\frac{13}{14}\right)}{\sqrt{3}},$$

temos $e^{X(t_1)}=Q$, logo $\Lambda_{e^{X(t_1)}}$ é o "reticulado ótimo" da Proposição 16, cuja matriz $e^{X(t_1)}$ é dada por (5.2).

De igual modo, o conjunto $\Lambda_{(e^{X(t)}E)}$ descreve versões rotacionadas do FCC em torno da reta cujo vetor diretor é $(1,1,1)$ e como $\mathrm{Rot}(\mathrm{FCC},(1,1,1))$, descrito nas Proposições 17 e 18, é o conjunto de todas as rotações possíveis do FCC em torno da reta cujo vetor diretor é $(1,1,1)$, segue que $\Lambda_{(e^{X(t_1)}E)}$ é o "reticulado ótimo" das Proposições 17 e 18, cuja matriz $e^{X(t_1)}E$ é dada por (5.5).

As Proposições 20, 21 e 22, a seguir, são versões alternativas das Proposições 16, 17 e 18.

Proposição 20. *Seja $\Lambda_{e^{X(t)}}$ o conjunto dos reticulados gerados por $e^{X(t)}$, onde $X(t)$ é a matriz dada por (6.5). A máxima distância produto mínima normalizada para um reticulado em $\Lambda_{e^{X(t)}}$ é $d_{p,\mathrm{norm}}(\mathbb{Z}^3) = \frac{1}{7}$.*

Proposição 21. *Sejam $\Lambda_{(e^{X(t)}E)}$ o conjunto dos reticulados gerados por $e^{X(t)}E$, onde $X(t)$ é a matriz dada por (6.5) e E é a matriz do FCC encontrada no Exemplo 17. A máxima distância produto mínima normalizada para um reticulado em $\Lambda_{(e^{X(t)}E)}$ é $d_{p,\mathrm{norm}}(FCC) = \frac{1}{14}$.*

Proposição 22. *Sejam $\Lambda_{(e^{X(t)}E)}$ o conjunto dos reticulados gerados por $e^{X(t)}E$, onde $X(t)$ é a matriz dada por (6.5) e E é a matriz do FCC encontrada no Exemplo 17. A máxima distância produto mínima relativa para um reticulado em $\Lambda_{(e^{X(t)}E)}$ é $d_{p,\mathrm{rel}}(FCC) = \frac{1}{7\sqrt{2^3}}$.*

7 Torção Generalizada

Neste capítulo definimos torção generalizada, apresentamos algumas propriedades referentes a este novo conceito e construímos versões torcidas de reticulados em dimensões 2, 3, 5 e 8.

Vemos que os reticulados *torcidos* preservam, por exemplo, distância produto mínima. Observamos que nos casos estudados (com exceção do $\mathbb{Z}^2$) foi possível aumentar a norma mínima, e consequentemente, a densidade de empacotamento de reticulados torcidos. A motivação para encontrarmos reticulados mais densos preservando uma boa distância produto mínima é que estes podem ser úteis simultaneamente para canais gaussianos e com desvanecimento do tipo Rayleigh, como vimos nas Seções 2.1 e 2.1.

7.1 Torção Generalizada em Reticulados Bidimensionais

Tendo por motivação os homomorfismos canônico e torcido (mediante Definições 50 e 53), definimos, nesta seção, *torção generalizada* em reticulados $\Lambda \subset \mathbb{R}^2$.

De (3.3) decorre que um reticulado algébrico bidimensional construído sobre um corpo de números totalmente real terá matriz geradora dada por

$$\begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) \end{bmatrix}$$

e de (3.8) decorre que um reticulado ideal bidimensional terá matriz geradora dada por

$$\begin{bmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_1}\sigma_1(\omega_2) \\ \sqrt{\alpha_2}\sigma_2(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_2) \end{bmatrix}.$$

Do Teorema 26 e da Definição 58, decorrem que esses reticulados têm distâncias produtos normalizadas dadas por $\frac{1}{\sqrt{d_{\mathbb{K}}}}$.

Pensando em termos mais gerais, temos que se Λ_1 é um reticulado de diversidade máxima cuja matriz geradora é

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

e dados $m \neq 0$ e Λ_2 um reticulado cuja matriz geradora é

$$B = \begin{bmatrix} ma & mb \\ c/m & d/m \end{bmatrix},$$

então estes reticulados têm as mesmas distâncias produtos mínimas. Com efeito, dado $(k_1, k_2) \in \mathbb{Z}^2$, temos:

$$\begin{aligned} d_{p,\min}(\Lambda_2) &= \min_{(k_1,k_2)\neq(0,0)} \left|(mak_1 + mbk_2)\left(\frac{ck_1}{m} + \frac{dk_2}{m}\right)\right| \\ &= \min_{(k_1,k_2)\neq(0,0)} |(ak_1 + bk_2)(ck_1 + dk_2)| = d_{p,\min}(\Lambda_1). \end{aligned} \tag{7.1}$$

Observamos, ainda, que como $V(\Lambda_1) = V(\Lambda_2)$, segue que

$$d_{p,\text{norm}}(\Lambda_1) = d_{p,\text{norm}}(\Lambda_2). \tag{7.2}$$

Temos, então, a motivação para a Definição 62, a seguir.

Definição 62 (Torção Generalizada)**.** *Sejam $0 \neq m \in \mathbb{R}$ e Λ um reticulado bidimensional que possui uma matriz geradora A. Uma m-torção generalizada do reticulado Λ é o reticulado $\text{tor}_m(\Lambda)$ com matriz geradora*

$$\begin{bmatrix} m & \\ & 1/m \end{bmatrix} A.$$

Observação 34. *Segue, da Definição 62, que $V(\text{tor}_m(\Lambda)) = V(\Lambda)$, e ainda, se Λ tem diversidade máxima, então temos das igualdades (7.1) e (7.2) que $\text{tor}_m(\Lambda)$ preserva a distância produto mínima e a distância produto normalizada de Λ.*

Exemplo 23. *Segue da Proposição 1, da Definição 62 e da Observação 34, que qualquer reticulado da família de reticulados $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, em que $\mathcal{L}(\mathbb{Z}^2)$ é a versão rotacionada "ótima" do $\mathbb{Z}^2$ com matriz geradora dada por (4.4), possui distância produto normalizada dada por $\dfrac{1}{\sqrt{5}}$.*

Vamos, agora, considerar a classe de reticulados $\Lambda(a) \subset \mathbb{R}^2$ cuja matriz geradora é dada por

$$\begin{bmatrix} 1 & \frac{1}{2} \\ 0 & a \end{bmatrix}, \tag{7.3}$$

em que $0 \neq a \in \mathbb{R}$. Trata-se de uma generalização da classe de reticulados Λ_4 cuja matriz geradora é dada por (3.7). Observamos que $\Lambda(a) = \Lambda_4$, desde que $a = \dfrac{\sqrt{l}}{2}$, onde $-l \equiv 1 \pmod 4$.

Proposição 23. *Seja $\Lambda(a)$ a classe de reticulados cuja matriz geradora é dada por (7.3). Se $a = \pm\sqrt{4z+1}/2$, onde z é um inteiro positivo e $4z+1$ não é um quadrado perfeito, então a máxima distância produto mínima normalizada para um reticulado $\Lambda(a)$ rotacionado é $d_{p,\text{norm}}(\Lambda(a)) = \dfrac{1}{2|a|} = \dfrac{1}{\sqrt{4z+1}}$.*

Demonstração. Como $\Lambda(a) = \{(k_1 + k_2/2, ak_2) : k_1, k_2 \in \mathbb{Z}\}$, tomando uma rotação de ângulo t, temos pelo Teorema 2 que:

$$(\cos(t) + i\text{sen}(t))(k_1 + k_2/2 + iak_2) = k_2\,(\cos(t)/2 - a\text{sen}(t)) + k_1\cos(t) + \\ +i(k_2\,(a\cos(t) + \text{sen}(t)/2) + k_1\text{sen}(t)).$$

Dessa forma, o conjunto de reticulados obtido por essa rotação é $\Lambda(a,t) = \{(k_2(\cos(t)/2 - a\text{sen}(t)) + k_1\cos(t), k_2(a\cos(t) + \text{sen}(t)/2) + k_1\text{sen}(t)) : k_1, k_2 \in \mathbb{Z}; 0 \leqslant t < 2\pi\}$. O valor absoluto do produto de coordenadas de um ponto em $\Lambda(a,t)$ dividido pelo volume de um reticulado qualquer desse conjunto é

$$F(a,k_1,k_2,t) = \left|\frac{1}{8a}(4ak_2(2k_1+k_2)\cos(2t) + (2k_1 - 2ak_2 + k_2)(2k_1 + 2ak_2 + k_2)\text{sen}(2t))\right|.$$

Como $F\left(a,k_1,k_2,t+\frac{\pi}{2}\right) = F\left(a,k_1,k_2,t\right)$, podemos tomar a variação de t no intervalo $\left[0,\frac{\pi}{2}\right]$; tomando-se o sup neste intervalo temos:

$$d_{p,\text{norm}}(\Lambda(a)) = \sup_t d_{p,\text{norm}}(\Lambda(a,t)) = \\ \sup_t \inf_{(k_1,k_2)\neq(0,0)} F(a,k_1,k_2,t) \leqslant \sup_t F(a,1,0,t) = \sup_t \left|\frac{\text{sen}(2t)}{2a}\right| = \frac{1}{2|a|}.$$

Por outro lado, $F\left(a,k_1,k_2,\frac{\pi}{4}\right) = \left|\frac{1}{8a}(4k_1^2 + 4k_1k_2 + (1-4a^2)k_2^2)\right| = 0 \Leftrightarrow k_1 = \frac{k_2}{2}(-1 \pm 2|a|)$. Tomando $a \notin \mathbb{Q}$, temos $F\left(a,k_1,k_2,\frac{\pi}{4}\right) = 0 \Leftrightarrow k_1 = k_2 = 0$.

Dessa forma, pondo $a = \pm\sqrt{4z+1}/2$, em que z é um inteiro positivo e $4z+1$ não é um quadrado perfeito, temos $d_{p,\text{norm}}\left(\Lambda\left(a,\frac{\pi}{4}\right)\right) = \inf_{(k_1,k_2)\neq(0,0)} F\left(a,k_1,k_2,\frac{\pi}{4}\right) = \inf_{(k_1,k_2)\neq(0,0)}\left|\frac{1}{8a}(4k_1^2 + 4k_1k_2 - 4zk_2^2)\right| = \frac{1}{2|a|}$.

Portanto, $d_{p,\text{norm}}(\Lambda(a)) = d_{p,\text{norm}}\left(\Lambda\left(a,\frac{\pi}{4}\right)\right) = \frac{1}{2|a|} = \frac{1}{\sqrt{4z+1}}$. □

Para mostrarmos que com as hipóteses da Proposição 23 temos $d_{p,\text{rel}}(\Lambda(a)) = \frac{1}{2}$, observemos primeiramente que a norma mínima de $\Lambda(a)$ é $\mu = 1$ (mediante Observação 2), logo segue que a norma mínima de qualquer reticulado de $\Lambda(a,t)$ (definido na demonstração da Proposição 23) também vale $\mu = 1$. Daí, segue que o valor absoluto do produto de coordenadas de um ponto em $\Lambda(a,t)$ dividido por μ^2 é

$$G(a,k_1,k_2,t) = \left|\frac{1}{8}(4ak_2(2k_1+k_2)\cos(2t) + (2k_1 - 2ak_2 + k_2)(2k_1 + 2ak_2 + k_2)\text{sen}(2t))\right|.$$

Usando na demostração da Proposição 23 a aplicação $G(a,k_1,k_2,t)$ ao invés da aplicação $F(a,k_1,k_2,t)$ concluímos a prova. Esse resultado é registrado na Proposição 24, a seguir.

Proposição 24. *Seja $\Lambda(a)$ a classe de reticulados cuja matriz geradora é dada por (7.3). Se $a = \pm\sqrt{4z+1}/2$, em que z é um inteiro positivo e $4z+1$ não é um quadrado perfeito, então a máxima distância produto mínima relativa para um reticulado $\Lambda(a)$ rotacionado é $d_{p,\mathrm{rel}}(\Lambda(a)) = \frac{1}{2}$.*

A Proposição 25, a seguir, iguala por meio de uma torção generalizada um reticulado equivalente (mediante Definição 35) a um reticulado da classe $\Lambda(a)$, cuja matriz geradora é dada por (7.3), com a versão rotacionada "ótima" do $\mathbb{Z}^2$ cuja matriz geradora é dada por (4.4).

Proposição 25. *Se $\Lambda(a)$ representa a classe de reticulados cuja matriz geradora é dada por (7.3) e $\mathcal{L}(\mathbb{Z}^2)$ é a versão rotacionada do $\mathbb{Z}^2$ com matriz geradora dada por (4.4), então a rotação anti-horária de $\frac{\pi}{4}$ de $\sqrt{\frac{2}{\sqrt{5}}}\,\Lambda\left(\frac{\sqrt{5}}{2}\right)$ é uma m-torção de $\mathcal{L}(\mathbb{Z}^2)$, em que $m = \sqrt{\frac{\sqrt{5}-1}{2}}$.*

Demonstração. Definindo $\tilde{\Lambda}$ pela rotação anti-horária de $\frac{\pi}{4}$ do reticulado $\sqrt{\frac{2}{\sqrt{5}}}\,\Lambda\left(\frac{\sqrt{5}}{2}\right)$, temos $V(\tilde{\Lambda}) = 1 = V(\mathcal{L}(\mathbb{Z}^2)$ e $d_{p,\mathrm{norm}}(\tilde{\Lambda}) = \frac{1}{\sqrt{5}} = d_{p,\mathrm{norm}}(\mathcal{L}(\mathbb{Z}^2)$ (mediante igualdades (4.17), (4.18), (4.19) e mediante Proposição 23).

Como $\Lambda\left(\frac{\sqrt{5}}{2}\right) = \left\{\left(k_1 + \frac{k_2}{2}, \frac{\sqrt{5}}{2}k_2\right) : k_1, k_2 \in \mathbb{Z}\right\}$, tomando uma rotação de ângulo $\frac{\pi}{4}$ de $\sqrt{\frac{2}{\sqrt{5}}}\,\Lambda\left(\frac{\sqrt{5}}{2}\right)$, temos pelo Teorema 2, que:

$$\left(\cos\left(\frac{\pi}{4}\right) + i\,\mathrm{sen}\left(\frac{\pi}{4}\right)\right)\sqrt{\frac{2}{\sqrt{5}}}\left(k_1 + \frac{k_2}{2} + i\frac{\sqrt{5}}{2}k_2\right) = \frac{1}{\sqrt[4]{5}}k_1 + \left(\frac{1}{2\sqrt[4]{5}} - \frac{\sqrt[4]{5}}{2}\right)k_2$$
$$+i\left(\frac{1}{\sqrt[4]{5}}k_1 + \left(\frac{1}{2\sqrt[4]{5}} + \frac{\sqrt[4]{5}}{2}\right)k_2\right).$$

Dessa forma, $\tilde{\Lambda} = \left\{\left(\frac{1}{\sqrt[4]{5}}k_1 + \left(\frac{1}{2\sqrt[4]{5}} - \frac{\sqrt[4]{5}}{2}\right)k_2, \frac{1}{\sqrt[4]{5}}k_1 + \left(\frac{1}{2\sqrt[4]{5}} + \frac{\sqrt[4]{5}}{2}\right)k_2\right) : k_1, k_2 \in \mathbb{Z}\right\}$, portanto, tem matriz geradora dada por

$$\begin{bmatrix} \frac{1}{\sqrt[4]{5}} & \frac{1}{2\sqrt[4]{5}} - \frac{\sqrt[4]{5}}{2} \\ \frac{1}{\sqrt[4]{5}} & \frac{1}{2\sqrt[4]{5}} + \frac{\sqrt[4]{5}}{2} \end{bmatrix}. \tag{7.4}$$

Uma vez que $\arctan(2) = \arccos\left(\frac{1}{\sqrt{5}}\right)$, segue das relações $\mathrm{sen}\left(\frac{x}{2}\right) = \sqrt{\frac{1-\cos(x)}{2}}$, $\cos\left(\frac{x}{2}\right) = \sqrt{\frac{1+\cos(x)}{2}}$ e da igualdade (4.4) que $\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))$ tem matriz geradora dada

por

$$\begin{bmatrix} \frac{\sqrt{(1+\sqrt{5})}m}{\sqrt{2}\sqrt[4]{5}} & -\frac{\sqrt{\sqrt{5}-1}m}{\sqrt{2}\sqrt[4]{5}} \\ \frac{\sqrt{(\sqrt{5}-1)}}{\sqrt{2}\sqrt[4]{5}m} & \frac{\sqrt{(1+\sqrt{5})}}{\sqrt{2}\sqrt[4]{5}m} \end{bmatrix}. \tag{7.5}$$

As matrizes dadas por (7.4) e (7.5) são iguais desde que $m = \sqrt{\frac{\sqrt{5}-1}{2}}$, o que conclui a prova. □

O valor de m na Proposição 25 é tal que $m^2 = \zeta_5 + \zeta_5^{-1}$ (mediante Exemplo 12). Não é difícil verificarmos este resultado. De fato, escrevendo $x = \cos\left(\frac{\pi}{5}\right)$ e $y = \text{sen}\left(\frac{\pi}{5}\right)$, temos:

$$\text{sen}\left(\frac{2\pi}{5}\right) = 2\text{sen}\left(\frac{\pi}{5}\right)\cos\left(\frac{\pi}{5}\right) = 2xy, \tag{7.6}$$

$$\cos\left(\frac{2\pi}{5}\right) = 2\cos^2\left(\frac{\pi}{5}\right) - 1 = 2x^2 - 1, \tag{7.7}$$

$$\begin{aligned} \text{sen}\left(\frac{2\pi}{5}\right) &= \text{sen}\left(\pi - \frac{2\pi}{5}\right) = \text{sen}\left(\frac{3\pi}{5}\right) = \text{sen}\left(\frac{\pi}{5} + \frac{2\pi}{5}\right) \\ &= \text{sen}\left(\frac{\pi}{5}\right)\cos\left(\frac{2\pi}{5}\right) + \text{sen}\left(\frac{2\pi}{5}\right)\cos\left(\frac{\pi}{5}\right). \end{aligned} \tag{7.8}$$

Levando em conta as igualdades (7.6) e (7.7), vemos que a igualdade (7.8) se reduz a

$$\text{sen}\left(\frac{2\pi}{5}\right) = y(2x^2 - 1) + 2xy(x) = 4x^2y - y. \tag{7.9}$$

Das igualdades (7.6) e (7.9), temos $2xy = 4x^2y - y$ e como $y \neq 0$, segue que $2x = 4x^2 - 1$, de onde encontramos $x = \frac{1+\sqrt{5}}{4}$. Por outro lado, da igualdade (3.12), temos:

$$\zeta_5 + \zeta_5^{-1} = 2\cos\left(\frac{2\pi}{5}\right). \tag{7.10}$$

Finalmente, temos das igualdades (7.7) e (7.10), que $\zeta_5 + \zeta_5^{-1} = 2\left[2\left(\frac{1+\sqrt{5}}{4}\right)^2 - 1\right] = \frac{\sqrt{5}-1}{2} = m^2$. Registramos este fato na Observação 35, a seguir.

Observação 35. *No Exemplo 12 encontramos a versão rotacionada do $\mathbb{Z}^2$ via o corpo $\mathbb{K} = \mathbb{Q}(m^2)$, onde m é dado pela Proposição 25.*

Consideramos os reticulados $\text{tor}_{m(i)}(\mathcal{L}(\mathbb{Z}^2))$, ver Exemplo 23, onde $m = m(i)$ foi tomado na partição $P = \left\{m = m(i) = \dfrac{i}{10^7}\right\}_{i=1}^{10^8}$ do intervalo $\left[\dfrac{1}{10^7}, 10\right]$. A partir do Algorítimo 1, verificamos que não existe i tal que $\mu_{m(i)} < \sqrt{\dfrac{2}{\sqrt{5}}}$ ou $\mu_{m(i)} > 1$, onde $\mu_{m(i)}$ é a norma mínima do reticulado $\text{tor}_{m(i)}(\mathcal{L}(\mathbb{Z}^2))$.

Na Proposição 26 encontramos reticulados da família $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$ com norma mínima $\mu = \sqrt{\dfrac{2}{\sqrt{5}}}$. As simulações que nos levaram ao resultado do parágrafo anterior são motivações para Conjectura 9.

Proposição 26. *Se $\mathcal{L}(\mathbb{Z}^2)$ é a versão rotacionada do $\mathbb{Z}^2$ com matriz geradora dada por (4.4), então os reticulados $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, em que $m = \pm\sqrt{\dfrac{\sqrt{5}-1}{2}}$ ou $m = \pm\sqrt{\dfrac{\sqrt{5}+1}{2}}$ têm distância produto mínima relativa $1/2$.*

Demonstração. Da igualdade (7.5), segue que uma base de $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$ é dada por

$$\left\{\mathbf{v}_1(m) = \left(\frac{\sqrt{(1+\sqrt{5})}m}{\sqrt{2}\sqrt[4]{5}}, \frac{\sqrt{(\sqrt{5}-1)}}{\sqrt{2}\sqrt[4]{5}m}\right), \mathbf{v}_2(m) = \left(-\frac{\sqrt{\sqrt{5}-1}m}{\sqrt{2}\sqrt[4]{5}}, \frac{\sqrt{(1+\sqrt{5})}}{\sqrt{2}\sqrt[4]{5}m}\right)\right\}.$$

Definindo a aplicação $f_1 : \mathbb{R} - \{0\} \to \mathbb{R}$ dada por $f_1(m) = \langle \mathbf{v}_1(m), \mathbf{v}_1(m)\rangle$, ou seja,

$$f_1(m) = \frac{\left(1+\sqrt{5}\right)m^2}{2\sqrt{5}} + \frac{\sqrt{5}-1}{2\sqrt{5}m^2},$$

temos que

$$f_1(m) = \alpha m^2 + \frac{\beta}{m^2}, \text{ onde } \alpha = \frac{\left(1+\sqrt{5}\right)}{2\sqrt{5}} \text{ e } \beta = \frac{\sqrt{5}-1}{2\sqrt{5}}. \tag{7.11}$$

Afirmação 1: f_1 tem máximo global em $m = \pm\sqrt[4]{\dfrac{\beta}{\alpha}}$, ou seja, em $m = \pm\sqrt{\dfrac{\sqrt{5}-1}{2}}$.

Com efeito, Observamos que $f_1'(m) = 2\alpha m - \dfrac{2\beta}{m^3}$. Resolvendo a equação $f_1'(m) = 0$ encontramos os pontos críticos $m = \pm\sqrt[4]{\dfrac{\beta}{\alpha}}$. Por outro lado, $f_1''(m) = 2\alpha + \dfrac{6\beta}{m^4}$, daí $f_1''\left(\pm\sqrt[4]{\dfrac{\beta}{\alpha}}\right) = 8\alpha > 0$, o que prova a afirmação 1.

Para os valores de $m = \pm\sqrt{\dfrac{\sqrt{5}-1}{2}}$, temos as bases

$$\left\{\mathbf{v}_1 = \left(\frac{1}{\sqrt[4]{5}}, \frac{1}{\sqrt[4]{5}}\right), \mathbf{v}_2 = \left(-\frac{\sqrt{5}-1}{2\sqrt[4]{5}}, \frac{1+\sqrt{5}}{2\sqrt[4]{5}}\right)\right\} \tag{7.12}$$

e

$$\left\{-\mathbf{v}_1 = \left(-\frac{1}{\sqrt[4]{5}}, -\frac{1}{\sqrt[4]{5}}\right), -\mathbf{v}_2 = \left(\frac{\sqrt{5}-1}{2\sqrt[4]{5}}, -\frac{1+\sqrt{5}}{2\sqrt[4]{5}}\right)\right\}. \tag{7.13}$$

Da Observação 2 segue que as bases (7.12) e (7.13) são Minkowski-reduzida, portanto, cada uma tem a mesma norma mínima

$$\mu = \sqrt{f_1\left(\pm\sqrt{\frac{\sqrt{5}-1}{2}}\right)} = \sqrt{\langle \mathbf{v}_1, \mathbf{v}_1\rangle} = \sqrt{\frac{2}{\sqrt{5}}}.$$

Dessa forma, os reticulados $\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, onde $m = \pm\sqrt{\dfrac{\sqrt{5}-1}{2}}$, têm distâncias produtos mínimas relativas iguais dadas por

$$d_{p,\mathrm{rel}}(\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))) = \frac{1}{\mu^2} d_{p,\min}(\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))) = \frac{1/\sqrt{5}}{2/\sqrt{5}} = \frac{1}{2}. \tag{7.14}$$

Definindo, agora, a aplicação $f_2 : \mathbb{R} - \{0\} \to \mathbb{R}$ dada por $f_2(m) = \langle \mathbf{v}_2(m), \mathbf{v}_2(m)\rangle$, ou seja,

$$f_2(m) = \frac{\left(\sqrt{5}-1\right) m^2}{2\sqrt{5}} + \frac{1+\sqrt{5}}{2\sqrt{5}m^2},$$

temos que $f_2(m) = \beta m^2 + \dfrac{\alpha}{m^2}$, onde α e β são dados pela igualdade (7.11).

Afirmação 2: f_2 tem máximo global em $m = \pm\sqrt[4]{\dfrac{\alpha}{\beta}}$, ou seja, em $m = \pm\sqrt{\dfrac{\sqrt{5}+1}{2}}$.

Com efeito, se trocarmos α por β e β por α na aplicação f_1 dada pela igualdade (7.11) esta se torna f_2. Como $\beta > 0$, concluímos da afirmação 1, que $m = \pm\sqrt[4]{\dfrac{\alpha}{\beta}}$ é máximo global de f_2, o que prova a afirmação 2.

Para os valores de $m = \pm\sqrt{\dfrac{\sqrt{5}+1}{2}}$, temos as bases

$$\left\{\mathbf{v}_1 = \left(\frac{1+\sqrt{5}}{2\sqrt[4]{5}}, \frac{\sqrt{5}-1}{2\sqrt[4]{5}}\right), \mathbf{v}_2 = \left(-\frac{1}{\sqrt[4]{5}}, \frac{1}{\sqrt[4]{5}}\right)\right\} \tag{7.15}$$

e

$$\left\{-\mathbf{v}_1 = \left(-\frac{1+\sqrt{5}}{2\sqrt[4]{5}}, -\frac{\sqrt{5}-1}{2\sqrt[4]{5}}\right), -\mathbf{v}_2 = \left(\frac{1}{\sqrt[4]{5}}, -\frac{1}{\sqrt[4]{5}}\right)\right\} \tag{7.16}$$

Aplicando o Algoritmo 1 nas bases (7.15) e (7.16) segue que as bases Minkowski-reduzidas encontradas são da forma $\{\mathbf{v}_2, \mathbf{v}_1\}$ e $\{-\mathbf{v}_2, -\mathbf{v}_1\}$, respectivamente, ou seja, há apenas

uma reordenação dos vetores em cada uma delas. Portanto, cada uma dessas novas bases Minkowski-reduzida têm a mesma norma mínima

$$\mu = \sqrt{f_2\left(\pm\sqrt{\frac{\sqrt{5}+1}{2}}\right)} = \sqrt{\langle \mathbf{v}_2, \mathbf{v}_2\rangle} = \sqrt{\frac{2}{\sqrt{5}}}.$$

Dessa forma, os reticulados $\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, em que $m = \pm\sqrt{\frac{\sqrt{5}+1}{2}}$, têm distâncias produtos mínima relativa iguais dadas por (7.14). □

Observação 36. *Observamos que um dos valores de m encontrados na Proposição 26 coincide com o da Proposição 25. Observamos, ainda, que os reticulados torcidos da Proposição 26 apresentam distância produto mínima relativa superior a da versão rotacionada "ótima" do $\mathbb{Z}^2$ com matriz geradora dada por (4.4).*

Conjectura 9. *Se $\mathcal{L}(\mathbb{Z}^2)$ é a versão rotacionada do $\mathbb{Z}^2$ com matriz geradora dada por (4.4) e μ_m é a norma mínima de um reticulado da família $\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, então $\sqrt{\frac{2}{\sqrt{5}}} \leqslant \mu_m \leqslant 1$.*

Apresentamos, agora, um estudo da torção de dois reticulados encontrados no Capítulo 4, visando aumentar a densidade das versões torcidas dos mesmos. O primeiro é o reticulado quadrático $\Lambda_2(5)$ (mediante Exemplo 11), cuja distância normalizada é $\frac{1}{\sqrt{5}}$ (mediante Proposição 6) e o segundo é a versão rotacionada "ótima" do reticulado ortogonal $\Lambda(\sqrt{3})$, cuja distância normalizada é $\frac{1}{2\sqrt{3}}$ (mediante Proposição 15).

Do que foi exposto, no parágrafo anterior, vemos que o reticulado $\Lambda_2(5)$ tem a mesma distância normalizada de $\mathcal{L}(\mathbb{Z}^2)$ que é a versão rotacionada do $\mathbb{Z}^2$ com matriz geradora dada por (4.4). Por outro lado, $\Lambda_2(5)$ tem norma mínima $\sqrt{2}$ (mediante Observação 2), portanto, sua densidade de empacotamento é $\Delta(\Lambda_2(5)) = \frac{\pi}{\sqrt{20}}$. Esta por sua vez é "bem inferior" à densidade de empacotamento de $\mathcal{L}(\mathbb{Z}^2)$ cujo valor é $\Delta(\mathcal{L}(\mathbb{Z}^2)) = \Delta(\mathbb{Z}^2) = \frac{\pi}{4}$.

Conseguimos construir uma versão torcida de $\Lambda_2(5)$ que é "melhor" que o próprio $\Lambda_2(5)$ no sentido que tal versão tem densidade de empacotamento "bem próxima" da densidade do $\mathcal{L}(\mathbb{Z}^2)$. Para isso, vemos primeiramente, que um reticulado da família $\mathrm{tor}_m(\Lambda_2(5))$ tem uma base dada por

$$\left\{\mathbf{v}_1(m) = \left(m, \frac{1}{m}\right), \mathbf{v}_2(m) = \left(\frac{1}{2}\left(1+\sqrt{5}\right)m, \frac{1-\sqrt{5}}{2m}\right)\right\}.$$

Consideramos os reticulados $\mathrm{tor}_{m(i)}(\Lambda_2(5))$, onde $m = m(i)$ foi tomado na partição $P = \left\{m = m(i) = \frac{i}{10^7}\right\}_{i=1}^{10^8}$ do intervalo $\left[\frac{1}{10^7}, 10\right]$. O cálculo da norma mínima $\mu_{m(i)}$ foi feito a partir do Algorítimo 1, onde verificamos que $\mu_{m(i)} \leqslant 1.49535$, para todo $i = 1, 2, .., 10^8$. Um valor $m(i)$ para o qual encontramos $\mu_{m(i)} = 1.49535$ foi $m(i) = 141069/10^7$.

Dessa forma, temos que o reticulado $\text{tor}_{141069/10^7}(\Lambda_2(5))$ tem a densidade "mais próxima" da densidade de $\mathcal{L}(\mathbb{Z}^2)$, a saber $\Delta(\mathcal{L}(\mathbb{Z}^2)) = \Delta(\mathbb{Z}^2) \simeq 0.785398$. Portanto, a "melhor" versão torcida encontrada do $\Lambda_2(5)$ (que é a mais densa) tem densidade dada por

$$\Delta(\text{tor}_{141069/10^7}(\Lambda_2(5))) = \frac{\mu^2_{141069/10^7}\pi}{4\sqrt{5}} \simeq \frac{1.49535^2\pi}{4\sqrt{5}} \simeq 0.785397.$$

Isso nos dá um ganho de aproximadamente 11.80 % na densidade.

Consideramos, agora, a versão rotacionada "ótima" do reticulado ortogonal $\Lambda(\sqrt{3})$ que segundo a Proposição 15, trata-se de uma rotação de $\frac{\pi}{4}$ deste. Designamos essa versão "ótima" por $\text{rot}_{\pi/4}(\Lambda(\sqrt{3}))$ que têm a mesma distância normalizada da versão rotacionada "ótima" do reticulado hexagonal (mediante igualdade (4.11)). Por outro lado, $\Lambda(\sqrt{3})$ tem norma mínima 1 (mediante Observação 2), portanto, $\Delta(\text{rot}_{\pi/4}(\Lambda(\sqrt{3}))) = \Delta(\Lambda(\sqrt{3})) = \frac{\pi}{\sqrt{48}}$. Esta densidade é por sua vez "bem inferior" a densidade de empacotamento do hexagonal que vale $\frac{\pi}{\sqrt{12}}$ (mediante Exemplo 6).

Conseguimos construir uma versão torcida de $\text{rot}_{\pi/4}(\Lambda(\sqrt{3}))$ que é "melhor" que o próprio $\text{rot}_{\pi/4}(\Lambda(\sqrt{3}))$ no sentido que tal versão tem densidade de empacotamento "bem próxima" da densidade do hexagonal. Para isso, vemos primeiramente que um reticulado da família $\text{tor}_m(\text{rot}_{\pi/4}(\Lambda(\sqrt{3})))$ tem uma base dada por

$$\left\{ \mathbf{v}_1(m) = \left(\frac{m}{\sqrt{2}}, \frac{1}{\sqrt{2}m} \right), \mathbf{v}_2(m) = \left(-\sqrt{\frac{3}{2}}m, \frac{\sqrt{\frac{3}{2}}}{m} \right) \right\}.$$

Consideramos os reticulados $\text{tor}_{m(i)}(\text{rot}_{\pi/4}(\Lambda(\sqrt{3})))$, onde $m = m(i)$ foi tomado na partição $P = \left\{ m = m(i) = \frac{i}{100} \right\}_{i=1}^{10^8}$ do intervalo $\left[\frac{1}{10^7}, 10 \right]$. O cálculo da norma mínima $\mu_{m(i)}$ foi feito a partir do Algorítimo 1, onde verificamos que $\mu_{m(i)} \leqslant 1.41421$, para todo $i = 1, 2, .., 10^8$. Um valor $m(i)$ para o qual encontramos 1.41421 foi $m(i) = 1387/10^7$.

Dessa forma temos que o reticulado $\text{tor}_{1387/10^7}(\text{rot}_{\pi/4}(\Lambda(\sqrt{3})))$ tem a densidade "mais próxima" da densidade do hexagonal a saber $\Delta(\text{hexagonal}) \simeq 0.9069$. Portanto, a "melhor" versão torcida encontrada do $\text{rot}_{\pi/4}(\Lambda(\sqrt{3}))$ (que é a mais densa) tem densidade dada por

$$\Delta(\text{tor}_{1387/10^7}(\text{rot}_{\pi/4}(\Lambda(\sqrt{3})))) = \frac{\mu^2_{1387/10^7}\pi}{4\sqrt{3}} \simeq \frac{1.41421^2\pi}{4\sqrt{3}} \simeq 0.906892.$$

Isso nos dá um ganho de aproximadamente 99.99 % na densidade.

Finalizamos, esta seção, com a Tabela 9, onde registramos as densidades dos reticulados estudados aqui bem como as de suas "melhores" versões torcidas encontradas.

Λ	$\Delta(\Lambda)$	M	$\Delta(\Lambda)$
$\mathcal{L}(\mathbb{Z}^2)$	0.785398	-	-
$\Lambda_2(5)$	0.702481	$\mathrm{tor}_{141069/10^7}(\Lambda_2(5))$	0.785397
$\mathrm{rot}_{\pi/4}(\Lambda(\sqrt{3}))$	0.453450	$\mathrm{tor}_{1387/10^7}(\mathrm{rot}_{\pi/4}(\Lambda(\sqrt{3})))$	0.906892

Tabela 9 – Densidade de $\Lambda \subset \mathbb{R}^2$ e densidade da melhor versão torcida encontrada

7.2 Torção Generalizada em Reticulados $n-$dimensionais ($n > 2$)

Nesta seção, estendemos o conceito de torção generalizada apresentada na seção anterior. Exibimos versões torcidas mais densas dos reticulados $\mathbb{Z}^3$, $\mathbb{Z}^5$ e $\mathbb{Z}^8$ que preservam as distâncias produtos mínimas encontradas na Seção 3.2.

O algoritmo usado para o cálculo da norma mínima dos reticulados estudados nessa seção foi proposto por U. Fincke e M. Pohst conforme podemos ver em [16]. Neste algoritmo, a norma mínima é calculada a partir da matriz de Gram do reticulado.

Procedendo de modo análogo a seção anterior, temos que se Λ_1 é um reticulado de diversidade máxima cuja matriz geradora é

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

dados $(m_1, m_2, ..., m_{n-1})$ com $m_i \neq 0$, $i = 1, 2, ..., n-1$ e Λ_2 um reticulado cuja matriz geradora é

$$B = \begin{bmatrix} m_1 a_{11} & m_1 a_{12} & \cdots & m_1 a_{1n} \\ m_2 a_{21} & m_2 a_{22} & \cdots & m_2 a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n-1} a_{n-11} & m_{n-1} a_{n-12} & \cdots & m_{n-1} a_{n-1n} \\ \dfrac{1}{m_1.m_2...m_{n-1}} a_{n1} & \dfrac{1}{m_1.m_2...m_{n-1}} a_{n2} & \cdots & \dfrac{1}{m_1.m_2...m_{n-1}} a_{nn} \end{bmatrix},$$

então esses reticulados têm as mesmas distâncias produtos mínimas. Com efeito, dado $(k_1, k_2, ..., k_n) \in \mathbb{Z}^n$, temos:

$$\begin{aligned} & d_{p,\min}(\Lambda_2) = \\ & \min_{(k_1,...,k_n)\neq(0,...,0)} \left| \sum_{i=1}^{n} m_1 a_{1i} k_i \sum_{i=1}^{n} m_2 a_{2i} k_i ... \sum_{i=1}^{n} m_{n-1} a_{n-1i} k_i \sum_{i=1}^{n} \frac{1}{m_1.m_2...m_{n-1}} a_{ni} k_i \right| \\ = & \min_{(k_1,...,k_n)\neq(0,...,0)} \left| \sum_{i=1}^{n} a_{1i} k_i \sum_{i=1}^{n} a_{2i} k_i ... \sum_{i=1}^{n} a_{n-1i} k_i \sum_{i=1}^{n} a_{ni} k_i \right| = d_{p,\min}(\Lambda_1). \end{aligned} \tag{7.17}$$

Observamos, ainda, que como $V(\Lambda_1) = V(\Lambda_2)$, segue que

$$d_{p,\text{norm}}(\Lambda_1) = d_{p,\text{norm}}(\Lambda_2). \tag{7.18}$$

Temos, então, a motivação para Definição 63, a seguir.

Definição 63 (Torção Generalizada)**.** *Sejam* $(m_1, m_2, ..., m_{n-1}) \in \mathbb{R}^{n-1}$, $m_i \neq 0$, $i = 1, 2, ..., n-1$ *e* $\Lambda \subset \mathbb{R}^n$ *(*$n > 2$*) um reticulado que possui uma matriz geradora* A*. Uma* $(m_1, m_2, ..., m_{n-1})$*-torção generalizada do reticulado* Λ *é o reticulado* $\text{tor}_{(m_1,m_2,...,m_{n-1})}(\Lambda)$ *com matriz geradora*

$$B = \begin{bmatrix} m_1 & & & & \\ & m_2 & & & \\ & & \ddots & & \\ & & & m_{n-1} & \\ & & & & \frac{1}{m_1.m_2...m_{n-1}} \end{bmatrix} A \tag{7.19}$$

Observação 37. *Segue, da Definição 63, que* $V(\text{tor}_m(\Lambda)) = V(\Lambda)$*, e ainda, se* Λ *tem diversidade máxima, então temos das igualdades (7.17) e (7.18), que* $\text{tor}_m(\Lambda)$ *preserva a distância produto mínima e a distância produto normalizada de* Λ*.*

Exemplo 24. *Seja* $\mathcal{L}(\mathbb{Z}^n)$ *a versão rotacionada "ótima" do* $\mathbb{Z}^n$*, em que para* $n = 3, 5$ *as matrizes geradoras são dadas por (5.2), (3.16) e para* $n = 8$ *a matriz geradora é encontrada no Exemplo 15. Segue da Proposição 16, dos Exemplos 14 e 15, da Definição 63 e da Observação 37, que as famílias* $\text{tor}_{(m_1,m_2)}(\mathcal{L}(\mathbb{Z}^3))$*,* $\text{tor}_{(m_1,m_2,m_3,m_4)}(\mathcal{L}(\mathbb{Z}^5))$ *e* $\text{tor}_{(m_1,m_2,...,m_7)}(\mathcal{L}(\mathbb{Z}^8))$ *definem reticulados que preservam as distâncias produtos normalizadas de* $\mathcal{L}(\mathbb{Z}^3)$*,* $\mathcal{L}(\mathbb{Z}^5)$ *e* $\mathcal{L}(\mathbb{Z}^8)$*, ou seja, qualquer reticulado da família* $\text{tor}_{(m_1,m_2)}(\mathcal{L}(\mathbb{Z}^3))$ *tem distância* $\frac{1}{7}$*, qualquer reticulado da família* $\text{tor}_{(m_1,m_2,m_3,m_4)}(\mathcal{L}(\mathbb{Z}^5))$ *tem distância* $\frac{1}{11^2}$ *e qualquer reticulado da família* $\text{tor}_{(m_1,m_2,...,m_7)}(\mathcal{L}(\mathbb{Z}^8))$ *tem distância* $\frac{1}{17^{7/2}}$*.*

Consideramos os reticulados $\text{tor}_{(m_1(i_1),m_2(i_2))}(\mathcal{L}(\mathbb{Z}^3))$, ver Exemplo 24, onde $(m_1(i_1), m_2(i_2))$ foi tomado no subconjunto $P = \left\{m_1(i_1) = \frac{i_1}{20}\right\}_{i_1=1}^{50} \times \left\{m_2(i_2) = \frac{i_2}{20}\right\}_{i_2=1}^{50}$ do quadrado $\left[\frac{1}{20}, \frac{5}{2}\right]^2$. Observamos que as matrizes de Gram desses reticulados são dadas por $G = G(m_1(i_1), m_2(i_2))$, em que $G = B^tB$, B é dada por (7.19) e A é a matriz Q dada por (5.2). Verificamos que $\mu_{(m_1(i_1),m_2(i_2))} \leqslant 1.01992$, para todo $i_1 = 1, 2, .., 50$ e $i_2 = 1, 2, .., 50$. Um ponto $(m_1(i_1), m_2(i_2))$ para o qual encontramos $\mu_{(m_1(i_1),m_2(i_2))} = 1.01992$ foi $(m_1(i_1), m_2(i_2)) = (7/4, 41/20)$.

Dessa forma, temos que o reticulado $\text{tor}_{(7/4,41/20)}(\mathcal{L}(\mathbb{Z}^3))$ é mais denso que o $\mathbb{Z}^3$, cuja densidade é 0.5236 e tem a maior densidade dentre todas as versões torcidas

consideradas; tal densidade é dada por

$$\Delta(\text{tor}_{(7/4,41/20)}(\mathcal{L}(\mathbb{Z}^3))) = \frac{\mu^3_{(7/4,41/20)}\pi}{6} \simeq \frac{1.01992^3\pi}{6} \simeq 0.555513.$$

Isso nos dá um ganho de aproximadamente 6.1 % na densidade.

Consideramos, agora, os reticulados $\text{tor}_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))}(\mathcal{L}(\mathbb{Z}^5))$, ver Exemplo 24, em que $(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4))$ foi tomado no subconjunto

$$P = \left\{m_1(i_1) = \frac{i_1}{3}\right\}_{i_1=1}^{7} \times \left\{m_2(i_2) = \frac{i_2}{3}\right\}_{i_2=1}^{7} \times \left\{m_3(i_3) = \frac{i_3}{3}\right\}_{i_3=1}^{7} \times \left\{m_4(i_4) = \frac{i_4}{3}\right\}_{i_4=1}^{7}$$

do hipercubo $\left[\frac{1}{3}, \frac{7}{3}\right]^4$. Observamos que as matrizes de Gram desses reticulados são dadas por $G = G(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4))$, em que $G = B^tB$, B é dada por (7.19) e A é a matriz R dada por (3.16). Verificamos que $\mu_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))} \leqslant 1.09221$, para todo $i_j = 1, 2, .., 7$, onde $j = 1, 2, 3, 4$. Um ponto $(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4))$ para o qual encontramos $\mu_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))} = 1.09221$ foi $(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4)) = (5/3, 7/3, 2, 1)$.

Temos que o reticulado $\text{tor}_{(5/3,7/3,2,1)}(\mathcal{L}(\mathbb{Z}^5))$ é mais denso que o $\mathbb{Z}^5$ cuja densidade é 0.164493 e tem a maior densidade dentre todas as versões torcidas consideradas, essa densidade por sua vez é dada por

$$\Delta(\text{tor}_{(5/3,7/3,2,1)}(\mathcal{L}(\mathbb{Z}^5))) = \frac{\mu^5_{(5/3,7/3,2,1)}\pi^2}{60} \simeq \frac{1.09221^5\pi^2}{60} \simeq 0.255673.$$

Isso nos dá um ganho de aproximadamente 55.43 % na densidade.

Finalmente, consideramos os reticulados $\text{tor}_{(m_1(i_1),m_2(i_2),...,m_7(i_7))}(\mathcal{L}(\mathbb{Z}^8))$, ver Exemplo 24, onde $(m_1(i_1), m_2(i_2), ..., m_7(i_7))$ foi tomado no subconjunto

$$P = \left\{m_1(i_1) = \frac{i_1}{2}\right\}_{i_1=1}^{3} \times \left\{m_2(i_2) = \frac{i_2}{2}\right\}_{i_2=1}^{3} \times ... \times \left\{m_7(i_7) = \frac{i_7}{2}\right\}_{i_7=1}^{3}$$

do hipercubo $\left[\frac{1}{2}, \frac{3}{2}\right]^7$. Observamos que as matrizes de Gram desses reticulados são dadas por $G = G(m_1(i_1), m_2(i_2), ..., m_7(i_7))$, em que $G = B^tB$, B é dada por (7.19) e A é a matriz R do Exemplo 15. Verificamos que $\mu_{(m_1(i_1),m_2(i_2),...,m_7(i_7))} \leqslant 1.1315$, para todo $i_j = 1, 2, 3$, onde $j = 1, 2, ..., 7$. Um ponto $(m_1(i_1), m_2(i_2), ..., m_7(i_7))$ para o qual encontramos $\mu_{(m_1(i_1),m_2(i_2),...,m_7(i_7))} = 1.1315$ foi $(m_1(i_1), m_2(i_2), ..., m_7(i_7)) = (1/2, 1, 3/2, 1, 1/2, 3/2, 1/2)$.

Dessa forma, temos que o reticulado $\text{tor}_{(1/2,1,3/2,1,1/2,3/2,1/2)}(\mathcal{L}(\mathbb{Z}^8))$ é mais denso que o $\mathbb{Z}^8$ cuja densidade é 0.0158543 e tem a maior densidade dentre todas as versões torcidas consideradas; tal densidade é dada por

$$\Delta(\text{tor}_{(1/2,1,3/2,1,1/2,3/2,1/2)}(\mathcal{L}(\mathbb{Z}^8))) = \frac{\mu^8_{(1/2,1,3/2,1,1/2,3/2,1/2)}\pi^4}{2^8 4!} \simeq \frac{1.1315^8\pi^4}{2^8 4!} \simeq 0.0425967.$$

$\mathcal{L}(\mathbb{Z}^n)$	$\Delta(\mathcal{L}(\mathbb{Z}^n))$	$\Lambda = \mathrm{tor}_{\mathbf{v}}(\mathcal{L}(\mathbb{Z}^n))$	$\Delta(\Lambda)$	M	$\Delta(M)$
$n = 3$	0.5236	$\mathbf{v} = \left(\frac{7}{4}, \frac{41}{20}\right)$	0.5555	FCC	0.7450
$n = 5$	0.1645	$\mathbf{v} = \left(\frac{5}{3}, \frac{7}{3}, 2, 1\right)$	0.2557	D_5	0.4653
$n = 8$	0.0159	$\mathbf{v} = \left(\frac{1}{2}, 1, \frac{3}{2}, 1, \frac{1}{2}, \frac{3}{2}, \frac{1}{2}\right)$	0.0426	E_8	0.2537

Tabela 10 – Densidade de $\mathcal{L}(\mathbb{Z}^n) \subset \mathbb{R}^n$ $(n > 2)$ e densidade da melhor versão torcida encontrada

Isso nos dá um ganho de aproximadamente 168.67 % na densidade.

Na Tabela 10, registramos as densidades dos reticulados estudados nessa seção bem como as de suas "melhores" versões torcidas encontradas. Nas duas últimas colunas temos os reticulados com maior densidade conhecida em cada dimensão e suas respectivas densidades.

8 Considerações Finais e Perspectivas

Neste trabalho, construímos versões rotacionadas "ótimas" de reticulados com diversidade máxima, exibindo suas distâncias produtos ou limitantes para estas (Capítulos 4, 5 e Seção 6.3). Construímos versões "perturbadas" de reticulados "ótimos", exibindo limitantes para suas distâncias produtos (Seções 4.2, 6.2 e Capítulo 5). Construímos, finalmente, versões torcidas de reticulados "ótimos" e exibimos suas normas mínimas e densidades (Capítulo 7).

Além das conjecturas enunciadas ao longo do trabalho para as quais pretendemos provar ou encontrar contra-exemplos, algumas perspectivas futuras de pesquisa que temos para a extensão dos resultados apresentados incluem:

- encontrar versões rotacionadas "ótimas" do $\mathbb{Z}^3$ e do FCC que tenham as maiores distâncias produtos possíveis quando consideramos quaisquer rotações destes reticulados;

- encontrar versões rotacionadas "ótimas" dos reticulados $\mathbb{Z}^7$ e E_7[1] com diversidade máxima e boas distâncias produtos a partir da álgebra dos octônios;

- "melhorar", se possível, os resultados referentes às perturbações de reticulados "ótimos", escrevendo-os apenas em termos das distâncias produtos;

- encontrar as condições para que tenhamos as melhores versões torcidas dos reticulados considerados neste trabalho;

- encontrar boas versões torcidas de outros reticulados com dimensões superiores aos que aqui foram estudados e as condições para que tenhamos as melhores versões torcidas destes.

[1] O E_7 é o reticulado mais denso em dimensão 7 conhecido, conforme podemos ver em [13]

Referências

[1] Apostol, T. M. *Calculus, Volume 2*, vol. 2. John Wiley & Sons Incorporated, 1967.

[2] Araujo, R. *Reticulados algébricos e aplicações a códigos e criptografia. 2018. 128 f.* PhD thesis, Tese (Doutorado em Matemática)-Instituto de Matemática, Estatística e Computação Científica, 2018.

[3] Bayer-Fluckiger, E. Lattices and number fields. *Algebraic Geometry: Hirzebruch 70 241*, BOOK_CHAP (1999).

[4] Bayer-Fluckiger, E., Oggier, F., and Viterbo, E. New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the rayleigh fading channel. *IEEE Transactions on information theory 50*, 4 (2004), 702–714.

[5] Belini, M. M. *A razão áurea e a sequência de Fibonacci.* PhD thesis, Universidade de São Paulo, 2015.

[6] Berhuy, G., and Oggier, F. *An introduction to central simple algebras and their applications to wireless communication*, vol. 191. American Mathematical Soc., 2013.

[7] Boldrini, J. L., Costa, S. I., Figueredo, V., and Wetzler, H. G. *Álgebra linear.* Harper & Row, 1980.

[8] Boutros, J., and Viterbo, E. High diversity lattices for fading channels. In *Proceedings of 1995 IEEE International Symposium on Information Theory* (1995), IEEE, p. 157.

[9] Boutros, J., Viterbo, E., Rastello, C., and Belfiore, J.-C. Good lattice constellations for both rayleigh fading and gaussian channels. *IEEE Transactions on Information Theory 42*, 2 (1996), 502–518.

[10] Carter, B., and Mancini, R. *Op Amps for everyone.* Newnes, 2017.

[11] Conway, J. H., and Sloane, N. J. A. *Sphere packings, lattices and groups*, vol. 290. Springer Science & Business Media, 2013.

[12] Conway, J. H., and Smith, D. A. *On quaternions and octonions.* CRC Press, 2003.

[13] Costa, S. I., Oggier, F., Campello, A., Belfiore, J.-C., and Viterbo, E. *Lattices Applied to Coding for Reliable and Secure Communications.* Springer, 2017.

[14] de Araujo, R. R., and Costa, S. I. Well-rounded algebraic lattices in odd prime dimension. *Archiv der Mathematik 112*, 2 (2019), 139–148.

[15] Domingues, H. H., and Iezzi, G. *Álgebra moderna*. Atual reform. São Paulo, 2003.

[16] Fincke, U., and Pohst, M. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of computation 44*, 170 (1985), 463–471.

[17] Fukshansky, L. On distribution of well-rounded sublattices of $\mathbb{Z}^2$. *Journal of Number Theory 128*, 8 (2008), 2359–2393.

[18] Gentili, E. H. Dos complexos aos números de cayley: Uma abordagem geométrica. 2002. 129f. Master's thesis, Dissertação (Mestrado em Matemática)-Instituto de Matemática, Estatística e Computação Científica, 2002.

[19] Golub, G. H., and Van Loan, C. F. *Matrix computations*, vol. 3. JHU press, 2013.

[20] Hefez, A., and Villela, M. L. T. *Códigos corretores de erros*. Instituto de Matematica Pura e Aplicada, 2008.

[21] Hogben, L. *Handbook of linear algebra*. CRC press, 2006.

[22] Jorge, G. C. *Reticulados q-ários e algébricos. 2012. 164f.* PhD thesis, Tese (Doutorado em Matemática)-Instituto de Matemática, Estatística e Computação Científica, 2012.

[23] Jorge, G. C., de Andrade, A. A., Costa, S. I., and Strapasson, J. E. Algebraic constructions of densest lattices. *Journal of Algebra 429* (2015), 218–235.

[24] Kuipers, J. B. *Quaternions and rotation sequences: a primer with applications to orbits, aerospace, and virtual reality*. Princeton university press, 1999.

[25] Lang, S. *Undergraduate algebra*. Springer Science & Business Media, 2005.

[26] Lavor, C., Alves, M., Siqueira, R., and Costa, S. Uma introdução à teoria de códigos. *Notas em Matemática Aplicada 21* (2006).

[27] Lima, E. L. Curso de análise, vol. 2.(6a ediçao). *Projeto Euclides, IMPA* (2000).

[28] Meyer, C. D. *Matrix analysis and applied linear algebra*, vol. 71. Siam, 2000.

[29] Mordell, L., et al. Jws cassels, an introduction to the geometry of numbers. *Bulletin of the American Mathematical Society 67*, 1 (1961), 89–94.

[30] Nagell, T. *Introduction to number theory*, vol. 163. American Mathematical Soc., 2021.

[31] Neelamani, R., Dash, S., and Baraniuk, R. G. On nearly orthogonal lattice bases and random lattices. *SIAM Journal on Discrete Mathematics 21*, 1 (2007), 199–219.

[32] Oggier, F., and Viterbo, E. *Algebraic number theory and code design for Rayleigh fading channels*. Now publishers inc, 2004.

[33] Samuel, P. *Algebraic Theory of Numbers: Translated from the French by Allan J. Silberger*. Courier Corporation, 2013.

[34] Spivak, M. *Cálculo en variedades*. Reverté, 2021.

[35] Stewart, I., and Tall, D. Algebraic number theory. Tech. rep., 1979.

[36] Strapasson, J. E. *Geometria discreta e codigos. 2007. 105f.* PhD thesis, Tese (Doutorado em Matemática)-Instituto de Matemática, Estatística e Computação Científica, 2007.

[37] Strapasson, J. E., Ferrari, A. J., Jorge, G. C., and Costa, S. I. R. Algebraic constructions of rotated unimodular lattices and direct sum of barnes–wall lattices. *Journal of Algebra and Its Applications* (2020), 2150029.

[38] Swinnerton-Dyer, H. P. F., and Swinnerton-Dyer, P. *A brief guide to algebraic number theory*, vol. 50. Cambridge University Press, 2001.

[39] Tse, D., and Viswanath, P. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[40] Viterbo, E., and Oggier, F. Full diversity rotations. *webpage: https://ecse.monash.edu/staff/eviterbo/rotations/rotations.html* (2005).

[41] Washington, L. C. Cyclotomic fields of class number one. In *Introduction to Cyclotomic Fields*. Springer, 1982, pp. 204–230.

[42] Watkins, D. S. *Fundamentals of matrix computations*, vol. 64. John Wiley & Sons, 2004.

[43] Wolfram, S. Wolfram mathematica 12.3. *Wolfram Research Inc., Champaign* (2020).