UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

William Lima da Silva Pinto

Construção de reticulados circulantes densos

São José do Rio Preto
2022

William Lima da Silva Pinto

Construção de reticulados circulantes densos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Orientadora: Profa. Dra. Carina Alves

Financiadora: CAPES

São José do Rio Preto
2022

P659c

Pinto, William Lima da Silva
Construção de Reticulados Circulantes Densos / William Lima da Silva Pinto. -- São José do Rio Preto, 2022
108 p. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientadora: Carina Alves

1. Matemática. 2. Teoria dos reticulados. 3. Matrizes (matemática). 4. Sistemas não lineares. 5. Formas quadráticas. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

William Lima da Silva Pinto

Construção de reticulados circulantes densos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Profa. Dra. Carina Alves
Orientadora

Prof. Dr. João Eloir Strapasson
Departamento de Matemática - Unicamp

Prof. Dr. Agnaldo José Ferrari
Departamento de Matemática - UNESP (Bauru)

São José do Rio Preto
17 de março de 2022

A Nina, Dora e Chuvisco

AGRADECIMENTOS

Ao concluir este trabalho, agradeço:

À minha orientadora e amiga Profª Drª Carina Alves por ter me acompanhado e me mostrado o caminho em toda minha vida acadêmica.

Aos professores da banca examinadora pela atenção e disponibilidade.

Aos professores do Departamento de Matemática da UNESP, em especial Profª Drª Suzete Afonso, Profª Drª Thais Monis, Profª Drª Eliris Rizziolli, Prof Dr Thiago de Melo, Profª Drª Renata Zotin, Profª Rúbia Barcelos e Profª Drª Alice Libardi pela excelente e inspiradora postura como docentes, jamais subestimando a capacidade de nós alunos de graduação e pós-graduação, e jamais se esquecendo dos direitos dos alunos e do recíproco tratamento digno que podemos receber.

À minha amiga Daniela, pela companhia, inspiração e ajuda.

Aos meus amigos que conheci durante graduação, em especial Leonardo, João Gabriel, Marina, Isaac e Matheus, que sempre estiveram presentes, e pelas noites de descontração. É o melhor grupo que eu poderia desejar fazer parte.

À minha mãe, que me ajudou tanto durante esse tempo, me visitando e me ajudando a cuidar dos meus gatos, quando precisei.

À minha tia Márcia e minhas primas Ligia e Cynthia, por terem me acolhido sem nem pensar duas vezes quando precisei, mesmo em um período difícil de isolamento social.

À minha psicóloga Mariana Tavares, pelos essenciais anos de terapia durante quase toda minha vida acadêmica.

À CAPES, pelo auxílio financeiro, processo 88887.474145/2020-00.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

O lar é o lugar onde,
quando você precisa ir lá, eles têm que te receber.
Infelizmente, também é o lugar em que, quando você entra,
não querem deixar você sair.
(Stephen King, [1])

RESUMO

Reticulados circulantes são aqueles que admitem uma matriz circulante como matriz geradora, isto é, que admitem como base um vetor real e suas $n-1$ rotações uma coordenada à direita. Neste trabalho, apresentamos determinadas condições sob as quais a expressão da norma de um vetor arbitrário de um reticulado circulante é substancialmente simplificada, e então investigamos alguns reticulados obtidos dentro dessas condições. A principal contribuição deste trabalho é exibir sistemas de equações não-lineares cujas soluções dão origem a reticulados tão densos quanto D_n em dimensões ímpares.

Palavras-chave: Reticulados, Formas quadráticas, Matrizes circulantes, Sistemas não-lineares, Problema do vetor mínimo.

ABSTRACT

Circulant lattices are those having a circulant matrix as generator matrix, that is, having as basis a real vector along with its $n-1$ circular shifts. In this paper, we present certain conditions under which the norm expression of an arbitrary vector of a circulant lattice is substantially simplified, and then investigate some of the lattices obtained under these conditions. The main contribution of this work is to exhibit nonlinear systems whose solutions yield lattices as dense as D_n in odd dimensions.

Keywords: Lattices, Quadratic forms, Circulant matrices, Nonlinear Systems, Shortest vector problems.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

Reticulados são subgrupos aditivos discretos de $\mathbb{R}^n$, cujos elementos são combinações lineares de vetores linearmente independentes e coeficientes inteiros. Na prática, trata-se de um conjunto de pontos no espaço distribuídos de acordo com um padrão determinado pela base. As propriedades de um reticulado estão associadas a diversas áreas, como o processamento de sinais [2, 3, 4] e a criptografia [5, 6, 7].

Para o processamento de sinais geralmente são cobiçados os reticulados com alta densidade de empacotamento, isto é, aqueles em que, descrevendo esferas ao redor de seus pontos de modo que seus raios sejam os maiores possíveis dentro da condição de que duas esferas quaisquer devem se intersectar em no máximo um ponto, tem-se o interior dessas esferas ocupando grande parte do espaço todo, proporcionalmente. O reticulado ideal para esse propósito é conhecido apenas em algumas dimensões, e então, para resolver esse problema, procuramos diversificar os métodos de geração de reticulados. Dependendo do tipo de canal para a transmissão de sinais, outras propriedades são procuradas, como alta diversidade [4], poucos vetores mínimos [8] ou muitos vetores mínimos [4].

A relação com criptografia é intuitivamente esperada, devido à estrutura algébrica dos reticulados e sua relação com programação inteira [9, 10]. O problema do vetor mínimo, por exemplo, pode ser entendido como um problema de otimização com restrições [11], NP-difícil em geral [12, 13]. Criptossistemas baseados em reticulados têm se mostrado mais resistentes a ataques quânticos do que criptossistemas mais usuais como RSA ou Diffie-Helman, o que faz dos reticulados um importante objeto de estudo para a criptografia pós-quântica.

Geralmente procuramos algoritmos [14, 15, 16, 17] ou construções convenientes de reticulados de modo a simplificar o cálculo dos parâmetros associados ao reticulado [18, 4]. A finalidade deste trabalho é apresentar uma nova classe de reticulados: os reticulados circulantes, obtidos através de matrizes circulantes. A vantagem desse tipo de reticulado é que matrizes circulantes são determinadas por um único vetor. Estudamos diferentes hipóteses sobre esse vetor de modo a simplificar a norma de um vetor arbitrário do reticulado circulante correspondente. Em seguida, dentro dessas hipóteses, buscamos maximizar a densidade de centro e o kissing number (número de vetores mínimos) do reticulado. Essa tarefa pode

ser traduzida em um sistema de equações não-lineares com restrições, isto é, um problema de otimização não-linear, o que pode ser explorado computacionalmente nesse sentido em trabalhos futuros. Interessantemente, algumas classes conhecidas de reticulados podem ser representadas por reticulados circulantes.

No Capítulo 2, definimos conceitos básicos da teoria de reticulados e exemplos clássicos de construções de reticulados.

No Capítulo 3, discutimos resultados a respeito de matrizes circulantes e seu determinante.

No Capítulo 4, apresentamos os reticulados circulantes de maneira geral, e em seguida investigamos alguns casos em particular.

2 Reticulados

2.1 Definições básicas

Considere um conjunto de vetores linearmente independente em $\mathbb{R}^n$. Suas combinações lineares com coeficientes reais dão origem a subespaços lineares de $\mathbb{R}^n$. Se são n vetores, em particular, então o resultado é que geramos o próprio espaço $\mathbb{R}^n$. De qualquer forma, como os coeficientes são reais, o conjunto obtido é evidentemente conexo. Agora, o que aconteceria se tomássemos coeficientes inteiros? O resultado é um conjunto discreto de vetores chamado de *reticulado*. Intuitivamente, pode ser entendido como um conjunto de pontos no espaço espalhados de acordo com algum padrão (determinado pela base).

Definição 2.1. Um conjunto $\Lambda \subset \mathbb{R}^n$ é denominado *reticulado de posto* m se existe um conjunto $\mathcal{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_m\} \subset \mathbb{R}^n$ de vetores linearmente independentes, chamado de *base* de Λ, tal que

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

Geralmente, são estudados os reticulados de posto completo, isto é, o caso $m = n$, já que são esses reticulados que têm maior aplicação prática. Desse modo, se não for especificado o

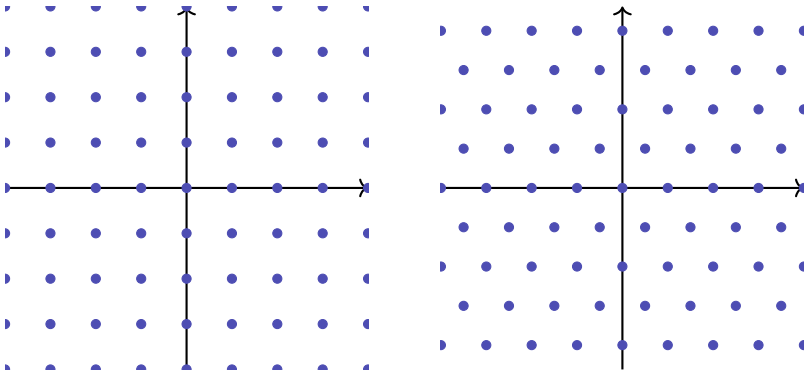

Figura 2.1: Reticulados gerados pelas bases $\{(1,0),(0,1)\}$ e $\{(1,0),(\frac{1}{2},\frac{\sqrt{3}}{2})\}$. Fonte: Elaborado pelo autor.

posto de um reticulado daqui em diante, assume-se que se trata de um reticulado de posto completo. É interessante também observar que um reticulado de posto m pode ser visto como um reticulado de posto completo em $\mathbb{R}^m$. Por exemplo, um reticulado em $\mathbb{R}^3$ de posto 2 está contido no plano determinado pelos vetores da base. Logo, se comporta como um reticulado de posto completo em $\mathbb{R}^2$. Isso pode ser observado mais formalmente através da Definição 2.8.

Evidentemente, se $\Lambda \subset \mathbb{R}^n$ é um reticulado, então $(\Lambda, +)$ é um grupo.

A matriz G real $m \times n$, cuja i-ésima linha é o vetor $\mathbf{b}_i$, é denominada *matriz geradora* do reticulado $\Lambda \subset \mathbb{R}^n$ de base $\{\mathbf{b}_i\}_{1 \leq i \leq m}$. Desse modo, escrevemos

$$\Lambda = \{G^T \mathbf{x}^T : \mathbf{x} \in \mathbb{Z}^n\} = G^T \mathbb{Z}^n$$

ou então

$$\Lambda = \{\mathbf{x}G : \mathbf{x} \in \mathbb{Z}^n\} = \mathbb{Z}^n G.$$

É claro que, implicitamente, estamos dizendo que por $\mathbf{x} \in \mathbb{Z}^n$ denotamos um vetor $1 \times n$.

A matriz geradora de um reticulado não é única; ou alternativamente, a base de um reticulado não é única. De fato, é sabido que duas bases diferentes geram o mesmo reticulado se, e somente se, uma é obtida da outra através de uma multiplicação por uma matriz $n \times n$ unimodular, isto é, uma matriz com entradas inteiras e determinante ± 1.

Vejamos algumas classes de reticulados bastante conhecidas.

Exemplo 2.2. O conjunto $\mathbb{Z}^n$ é um reticulado, denominado *reticulado ortogonal*. Ele pode ser gerado, por exemplo, através da matriz identidade. Consequentemente, como se trata de uma matriz unimodular, então qualquer outra matriz $n \times n$ unimodular é capaz de gerar $\mathbb{Z}^n$, já que é produto dela mesma com a matriz identidade.

Exemplo 2.3. O conjunto $A_n = \{(x_1, \cdots, x_{n+1}) \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0\}$ é um reticulado de posto n em $\mathbb{R}^{n+1}$. Uma base $\{\mathbf{b}_i\}_{1 \leq i \leq n}$ pode ser descrita por $\mathbf{b}_i = \mathbf{e}_i - \mathbf{e}_{i+1}$ para cada $i \in \{1, 2, \cdots, n\}$.

Exemplo 2.4. O conjunto $D_n = \{(x_1, \cdots, x_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \equiv 0 \pmod 2\}$ é um reticulado, denominado reticulado *Checkerboard*.

2.2 Empacotamentos reticulados

Chamamos de *empacotamento esférico* uma configuração de esferas de mesmo raio em $\mathbb{R}^n$, onde cada par de esferas se intersecta em no máximo um ponto. A proporção do espaço ocupado pelo interior dessas esferas em relação ao espaço todo, chamada de *densidade de empacotamento* e geralmente denotada por Δ, é um parâmetro associado a problemas da Teoria da Informação. Pode ser obtida, por exemplo, através do limite da proporção do

espaço ocupado pelas esferas em uma região limitada, como uma bola centrada no origem, quando o raio tende ao infinito.

Shannon demonstra em [19] que códigos corretores de erros eficientes diminuem tanto quanto se queira a probabilidade de erro para transmissões de dados abaixo da capacidade do canal. Em particular, a prova do teorema implica que canais com ruído gaussiano branco (AWGN) estão associados a empacotamentos esféricos densos. Para ilustrar essa associação, suponha que sinais são representados como pontos em um conjunto limitado $L \subset \mathbb{R}^n$, como uma esfera centrada na origem. Suponha também que queremos transmitir para um receptor um conjunto finito S de sinais sobre um canal ruidoso. Cada sinal $\mathbf{x} \in S$ é recebido como um ponto $\mathbf{y} \in \mathbb{R}^n$, onde em geral tem-se $\mathbf{x} \neq \mathbf{y}$, uma vez que se trata de um canal ruidoso. Em um modelo de ruído simples, podemos assumir que $\|\mathbf{x} - \mathbf{y}\| < \eta$ sempre é verdadeiro para algum $\eta > 0$ suficientemente pequeno. O receptor decodifica $\mathbf{y}$ pelo mais próximo vetor $\mathbf{x} \in S$. Isto é, ao receber $\mathbf{y}$, sabe-se que a mensagem emitida foi $\mathbf{x}$ através desse critério. Deve-se ter certeza de que $B(\mathbf{x}_1, \eta) \cap B(\mathbf{x}_2, \eta) = \emptyset$ para qualquer par de sinais $\mathbf{x}_1, \mathbf{x}_2 \in S$, já que caso contrário, uma mensagem recebida como $\mathbf{y} \in B(\mathbf{x}_1, \eta) \cap B(\mathbf{x}_2, \eta)$ poderia eventualmente ser decodificada como $\mathbf{x}_1$ ou como $\mathbf{x}_2$, resultando assim em uma ambiguidade. Evidentemente, deseja-se uma taxa de informação alta, isto é, maximizar o número de pontos de S. Equivalentemente, queremos o maior número de esferas de raio η possível em L. Quando o raio de L tende ao infinito, obtemos o problema de encontrar um empacotamento esférico denso.

Se os centros das esferas de um empacotamento esférico são precisamente os pontos de um reticulado em $\mathbb{R}^n$, então trata-se de um *empacotamento reticulado*. É conveniente pois o conjunto dos centros das esferas passa a ter estrutura de grupo em relação à adição. O Teorema de Minkowski–Hlawka [20] garante a existência de reticulados de dimensão n com densidade de empacotamento Δ satisfazendo

$$\Delta \geq \frac{\zeta(n)}{2^{n-1}},$$

onde ζ denota a função zeta de Riemann. Uma cota inferior ligeiramente melhorada foi obtida por Ball em 1992 [21]:

$$\Delta \geq (n-1)\frac{\zeta(n)}{2^{n-1}}.$$

Queremos então reticulados com densidade de empacotamento maior possível. Em algumas dimensões, sabe-se qual o empacotamento reticulado mais denso. Em dimensão 1, trata-se de um problema trivial: basta considerar o reticulado $\mathbb{Z}$, com esferas de raio $\frac{1}{2}$ centradas em seus pontos. Em dimensão 2, o reticulado com maior densidade de empacotamento é o *reticulado hexagonal*, de base $\{(1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\}$ [20], ilustrado na Figura 2.1. Para a dimensão 3, apesar de Kepler conjecturar um resultado, não se tinha prova até 1998, quando Thomas Hales apresentou um trabalho envolvendo variados cálculos computacionais. Provou-se de

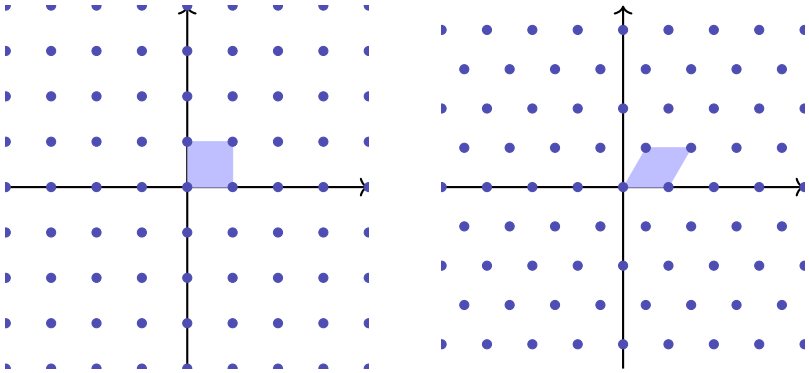

Figura 2.2: Regiões fundamentais dos reticulados gerados pelas bases $\{(1,0),(0,1)\}$ e $\{(1,0),(\frac{1}{2},\frac{\sqrt{3}}{2})\}$. Fonte: elaborado pelo autor.

fato que a maior densidade possível para a dimensão é de $\frac{\pi}{\sqrt{18}} \approx 0.74$, como conjecturava Kepler. Uma prova mais detalhada foi publicada em 2005 [22].

Nem sempre a melhor configurações de esferas pode ser descrita por um empacotamento reticulado. Todavia, empacotamentos reticulados, devido à sua estrutura algébrica, possuem parâmetros como a densidade de empacotamento muito bem definidos por expressões matemáticas. Veremos isso com mais detalhes, a seguir.

Definição 2.5. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de base $\{\mathbf{b}_i\}_{1\leq i\leq n}$. O paralelepípedo

$$\left\{ \sum_{i=1}^{n} \theta_i \mathbf{b}_i \colon \theta_i \in [0,1)\ \forall i \in \{1,2,\cdot,n\} \right\}$$

é denominado *região fundamental* (ou paralelepípedo fundamental) de Λ.

É claro que a região fundamental de um reticulado Λ não é única, já que mais de uma base para ele é possível, como já observamos. No entanto, o volume da região fundamental de Λ, denotado por $\mathrm{vol}(\Lambda)$, é sempre o mesmo, independentemente da base. Isto é, ele está bem definido. De fato, se G e G' são matrizes geradoras de Λ, então existe uma matriz integral invertível U de determinante ± 1 tal que $G = G'U$. Daí,

$$|\det(G)| = |\det(G'U)| = |\det(G')|.$$

Agora, precisamos do raio de uma esfera de um empacotamento reticulado para determinar o volume das esferas que o determinam.

Definição 2.6. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Chamamos de *norma mínima* de Λ o parâmetro

$$|\Lambda| := \min\{\|\mathbf{v}\|^2 \colon \mathbf{v} \in \Lambda \backslash \{\mathbf{0}\}\}.$$

Os vetores de norma mínima de Λ são chamados de *vetores mínimos* de Λ:

$$S(\Lambda) := \{\mathbf{v} \in \Lambda \colon \|\mathbf{v}\|^2 = |\Lambda|\}.$$

Assim, em um reticulado Λ, o raio das esferas do empacotamento reticulado determinado por Λ deve ser

$$\rho = \frac{\sqrt{|\Lambda|}}{2},$$

já que queremos o maior raio tal que as esferas de intersectam em no máximo um ponto.

Podemos agora dar uma definição precisa da densidade de empacotamento $\Delta(\Lambda)$ de um empacotamento determinado por um reticulado Λ de matriz geradora G. Se V_n é o volume de uma esfera unitária em $\mathbb{R}^n$, então

$$\begin{aligned}\Delta(\Lambda) &= \frac{\text{volume de uma esfera do empacotamento}}{\text{volume da região fundamental}} \\ &= \frac{\text{volume de uma esfera do empacotamento}}{\text{volume da região fundamental}} \\ &= \frac{V_n \rho^n}{\text{vol}(\Lambda)} \\ &= \frac{V_n \left(\frac{\sqrt{|\Lambda|}}{2}\right)^n}{|\det(G)|}.\end{aligned}$$

Como V_n é fixo para cada n, então o parâmetro relevante que queremos maximizar é $\frac{\Delta(\Lambda)}{V_n}$.

Definição 2.7. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Definimos a *densidade de centro* de Λ por

$$\delta(\Lambda) := \frac{\Delta(\Lambda)}{V_n} = \frac{\left(\frac{\sqrt{|\Lambda|}}{2}\right)^n}{|\det(G)|}.$$

Definição 2.8. Dois reticulados Λ e Ω de matrizes geradoras G e G', respectivamente, são ditos *semelhantes* se existem uma matriz ortogonal real B, uma matriz integral invertível U, e um número real $\alpha > 0$, tais que

$$G' = \alpha UGB.$$

Denotamos nesse caso $\Lambda \sim \Omega$.

Em termos práticos, dois reticulados são semelhantes se um pode ser obtido do outro por meio de uma rotação, reflexão ou mudança de escala. A importância disso é que reticulados semelhantes preservam propriedades como a densidade de centro, já que o padrão sob o qual os vetores se espalham é essencialmente o mesmo.

Proposição 2.9. *Sejam $\Lambda, \Omega \subset \mathbb{R}^n$ reticulados tais que $\Lambda \sim \Omega$. Então $\delta(\Lambda) = \delta(\Omega)$.*

Demonstração. Sejam G e G' matrizes geradoras de Λ e Ω, respectivamente. Como $\Lambda \sim \Omega$, sejam $\alpha > 0$, U uma matriz integral com determinante ± 1 e B uma matriz ortogonal, tais que $G' = \alpha UGB$. Então

$$\begin{aligned}
\mathrm{vol}(\Omega) &= |\det(G')| \\
&= |\det(\alpha UGB)| \\
&= |\det(\alpha \mathrm{Id}_n)\det(U)\det(G)\det(B)| \\
&= \alpha^n |\det(G)| \\
&= \alpha^n \mathrm{vol}(\Lambda).
\end{aligned}$$

Além disso, é claro da definição de norma mínima que $|\Omega| = \alpha^2|\Lambda|$. Com efeito,

$$\begin{aligned}
|\Omega| &= \min_{\mathbf{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}} \|\mathbf{x}G'\|^2 \\
&= \min_{\mathbf{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}} \|\mathbf{x}(\alpha UGB)\|^2 \\
&= \min_{\mathbf{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}} \alpha^2\|\mathbf{x}UGB\|^2 \\
&= \alpha^2 \min_{\mathbf{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}} \|\mathbf{x}G\|^2 \\
&= \alpha^2|\Lambda|.
\end{aligned}$$

Assim,

$$\begin{aligned}
\delta(\Omega) &= \frac{\left(\frac{\sqrt{|\Omega|}}{2}\right)^n}{\mathrm{vol}(\Omega)} \\
&= \frac{|\Omega|^{\frac{n}{2}}}{2^n\alpha^n\mathrm{vol}(\Lambda)} \\
&= \frac{(\alpha^2|\Lambda|)^{\frac{n}{2}}}{2^n\alpha^n\mathrm{vol}(\Lambda)} \\
&= \frac{(|\Lambda|)^{\frac{n}{2}}}{2^n\mathrm{vol}(\Lambda)} \\
&= \delta(\Lambda).
\end{aligned}$$

□

Vejamos um exemplo.

Proposição 2.10. *O reticulado A_2 é semelhante ao reticulado $\Lambda \subset \mathbb{R}^2$ de base $\{(1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\}$, chamado de reticulado hexagonal.*

Demonstração. O reticulado $A_2 \subset \mathbb{R}^3$ de posto 2 está contido no plano $x + y + z = 0$. Tal plano intersecta o plano $z = 0$ na reta $\{\mu(1, -1, 0) \colon \mu \in \mathbb{R}\}$, e possui vetor normal $(1, 1, 1)$, que faz um ângulo θ com o vetor $(1, -1, 0)$ tal que

$$\cos(\theta) = \frac{1}{\sqrt{3}}.$$

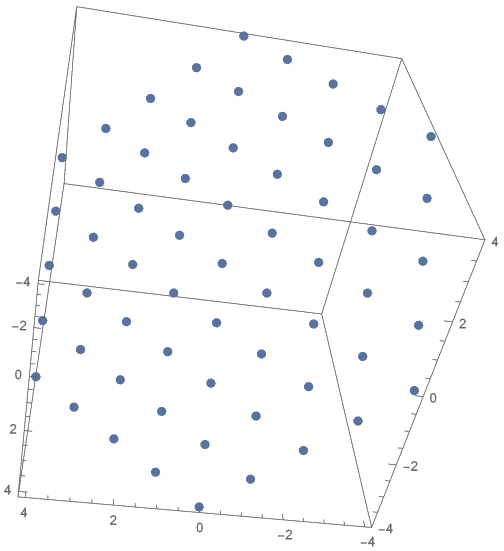

Figura 2.3: Reticulado A_2. Fonte: elaborado pelo autor

Então, para rotacionar A_2 de modo a posicioná-lo no plano $z = 0$, precisamos rotacionar o conjunto ao redor de $(1, -1, 0)$ pelo ângulo θ. Isso é equivalente a fazer o mesmo ao redor de seu versor $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0)$, o que não altera θ e facilita os cálculos. A saber [23], a matriz de rotação ao redor de um vetor da forma (u_1, u_2, u_3) por um ângulo θ é dada por

$$R = \begin{pmatrix} \cos(\theta) + u_1^2(1 - \cos(\theta)) & u_1u_2(1 - \cos(\theta)) - u_3\text{sen}(\theta) & u_1u_3(1 - \cos(\theta)) + u_2\text{sen}(\theta) \\ u_1u_2(1 - \cos(\theta)) + u_3\text{sen}(\theta) & \cos(\theta) + u_2^2(1 - \cos(\theta)) & u_2u_3(1 - \cos(\theta)) - u_1\text{sen}(\theta) \\ u_1u_3(1 - \cos(\theta)) - u_2\text{sen}(\theta) & u_2u_3(1 - \cos(\theta)) + u_1\text{sen}(\theta) & \cos(\theta) + u_3^2(1 - \cos(\theta)) \end{pmatrix}. \tag{2.1}$$

Observe que essa matriz é ortogonal, já que sua transposta é a matriz de rotação ao redor de (u_1, u_2, u_3) pelo ângulo $-\theta$, isto é, trata-se do processo reverso de rotação. De fato, basta notar que as funções cosseno e seno são par e ímpar, respectivamente. Então, pondo $\gamma = -\theta$,

$$\begin{aligned} R^T &= \begin{pmatrix} \cos(\theta) + u_1^2(1 - \cos(\theta)) & u_1u_2(1 - \cos(\theta)) + u_3\text{sen}(\theta) & u_1u_3(1 - \cos(\theta)) - u_2\text{sen}(\theta) \\ u_1u_2(1 - \cos(\theta)) - u_3\text{sen}(\theta) & \cos(\theta) + u_2^2(1 - \cos(\theta)) & u_2u_3(1 - \cos(\theta)) + u_1\text{sen}(\theta) \\ u_1u_3(1 - \cos(\theta)) + u_2\text{sen}(\theta) & u_2u_3(1 - \cos(\theta)) - u_1\text{sen}(\theta) & \cos(\theta) + u_3^2(1 - \cos(\theta)) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\gamma) + u_1^2(1 - \cos(\gamma)) & u_1u_2(1 - \cos(\gamma)) - u_3\text{sen}(\gamma) & u_1u_3(1 - \cos(\gamma)) + u_2\text{sen}(\gamma) \\ u_1u_2(1 - \cos(\gamma)) + u_3\text{sen}(\gamma) & \cos(\gamma) + u_2^2(1 - \cos(\gamma)) & u_2u_3(1 - \cos(\gamma)) - u_1\text{sen}(\gamma) \\ u_1u_3(1 - \cos(\gamma)) - u_2\text{sen}(\gamma) & u_2u_3(1 - \cos(\gamma)) + u_1\text{sen}(\gamma) & \cos(\gamma) + u_3^2(1 - \cos(\gamma)) \end{pmatrix}. \end{aligned}$$

No nosso caso, obtemos

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

e

$$R^T = \frac{1}{6}\begin{pmatrix} \sqrt{3}+3 & \sqrt{3}-3 & -2\sqrt{3} \\ \sqrt{3}-3 & \sqrt{3}+3 & -2\sqrt{3} \\ -2\sqrt{3} & -2\sqrt{3} & 2\sqrt{3} \end{pmatrix}.$$

Verifica-se com efeito que $RR^T = R^T R = \mathrm{Id}_n$.

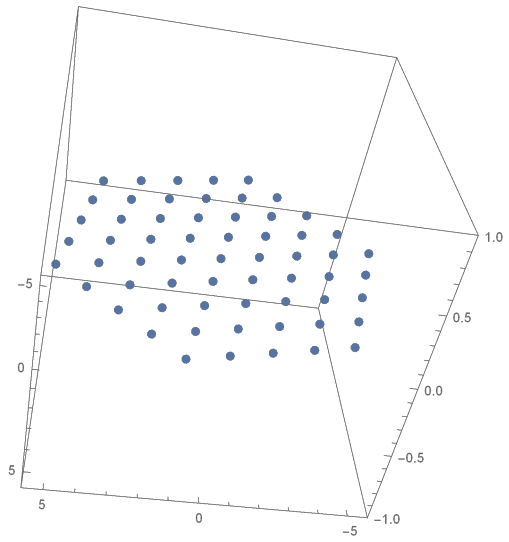

Figura 2.4: Reticulado $\mathbb{Z}^3 GR^T$. Fonte: elaborado pelo autor.

Verifiquemos agora que, de fato, o reticulado determinado por GR^T está contido no plano $z = 0$. Se G denota a matriz geradora de A_2, então

$$\begin{aligned} \mathbf{x}GR^T &= (x_1 \quad x_2 \quad x_3)\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & 0 & 1 \end{pmatrix}\frac{1}{6}\begin{pmatrix} \sqrt{3}+3 & \sqrt{3}-3 & -2\sqrt{3} \\ \sqrt{3}-3 & \sqrt{3}+3 & -2\sqrt{3} \\ 2\sqrt{3} & 2\sqrt{3} & 2\sqrt{3} \end{pmatrix} \\ &= (x_1 \quad x_2 \quad x_3)\frac{1}{2}\begin{pmatrix} 2 & -2 & 0 \\ \sqrt{3}-1 & \sqrt{3}+1 & 0 \\ -\sqrt{3}-1 & -\sqrt{3}+1 & 0 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 2x_1 + (\sqrt{3}-1)x_2 - (\sqrt{3}+1)x_3 \\ -2x_1 + (\sqrt{3}+1)x_2 + -(\sqrt{3}-1)x_3 \\ 0 \end{pmatrix}, \end{aligned}$$

para todo $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$.

Precisamos de mais algumas manipulações sobre o reticulado. Queremos rotacionar $\mathbb{Z}^3GR^T$ ao redor de $(0,0,1)$ pelo ângulo $\psi = \pi/4$. Dividimos também o reticulado pelo escalar $\sqrt{2}$, para simplificar os cálculos.

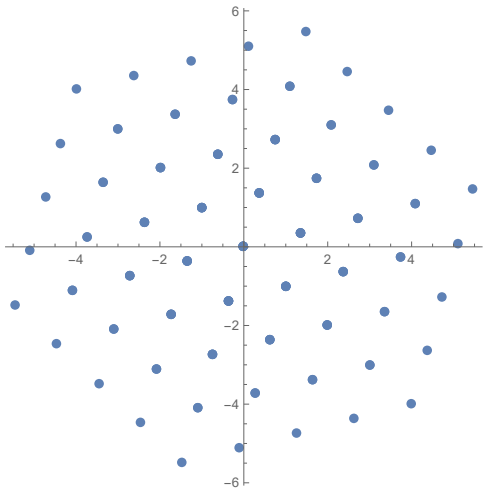

Figura 2.5: Representação gráfica de $\mathbb{Z}^3GR^T$ no plano $z = 0$. Fonte: Elaborado pelo autor.

Utilizando a equação (2.1), a rotação é obtida ao multiplicar o conjunto pela esquerda pela matriz ortogonal

$$R_0 = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

ou pela direita por R_0^T. Temos agora

$$\begin{aligned} \frac{1}{\sqrt{2}} GR^T R_0^T &= \frac{1}{2\sqrt{2}} \begin{pmatrix} 2 & -2 & 0 \\ \sqrt{3}-1 & \sqrt{3}+1 & 0 \\ -\sqrt{3}-1 & -\sqrt{3}+1 & 0 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ \frac{-\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ -1 & \sqrt{3} & 0 \\ -1 & -\sqrt{3} & 0 \end{pmatrix}. \end{aligned}$$

Agora basta modificar a matriz geradora com uma matriz integral invertível conveniente. Considere então

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

Então

$$\frac{1}{\sqrt{2}} UGR^T R_0^T = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ -1 & \sqrt{3} & 0 \\ -1 & -\sqrt{3} & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Assim, como o produto de matrizes ortogonais é ortogonal, então temos $B = R^T R_0^T$ ortogonal. Pondo também $\alpha = \frac{1}{\sqrt{2}}$, tem-se portanto que

$$\begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} = \alpha UGB,$$

o que conclui a demonstração. □

Dessa forma, se A_2 é visto como um reticulado de posto completo em $\mathbb{R}^2$, ele é essencialmente o reticulado hexagonal.

São conhecidos os reticulados mais densos nas dimensões $1-8$ e 24, enquanto nas demais dimensões, ainda se trata de um problema em aberto. As classes conhecidas A_n e D_n são relativamente densas em dimensões baixas, atingindo a melhor densidade até dimensão 5, mas se distanciam do ideal quanto maior for n, como se pode observar na Figura 2.6. Para a dimensão 8, por exemplo, o reticulado $E_8 = D_8^+ = D_8 \cup ((\frac{1}{2}, \cdots, \frac{1}{2}) + D_8)$, construído a partir de duas translações de D_8, é mais apropriado [20]. Os reticulados mais densos para as dimensões 6 e 7 são construídos a partir de E_8:

$$E_7 = \{(x_1, \cdots, x_8) \in E_8 \colon x_7 = x_8\}$$

e

$$E_6 = \{(x_1, \cdots, x_8) \in E_8 \colon x_6 = x_7 = x_8\}.$$

Em [24, 20] é possível consultar mais informações a respeito dos empacotamentos reticulados (e não reticulados) mais densos para cada dimensão. Exibimos uma versão resumida nas Tabelas 2.1, e 2.2, para dimensão $n \leq 30$.

n	**Densidade de centro para reticulados**	**Reticulado correspondente**
1	$\frac{1}{2} = 0.5$	$\Lambda_1 \sim A_1 \sim \mathbb{Z}$
2	$\frac{1}{2\sqrt{3}} \approx 0.28868$	$\Lambda_2 \sim A_2$
3	$\frac{1}{4\sqrt{2}} \approx 0.17678$	$\Lambda_3 \sim A_3 \sim D_3$

Tabela 2.1: Maior densidade de centro conhecida para reticulados para $n \leq 3$

n	**Densidade de centro para reticulados**	**Reticulado correspondente**
4	$\frac{1}{8} = 0.125$	$\Lambda_4 \sim D_4$
5	$\frac{1}{8\sqrt{2}} \approx 0.08839$	$\Lambda_5 \sim D_5$
6	$\frac{1}{8\sqrt{3}} \approx 0.07217$	$\Lambda_6 \sim E_6$
7	$\frac{1}{16} = 0.0625$	$\Lambda_7 \sim E_7$
8	$\frac{1}{16} = 0.0625$	$\Lambda_8 \sim E_8$
9	$\frac{1}{16\sqrt{2}} \approx 0.04419$	Λ_9
10	$\frac{1}{16\sqrt{3}} \approx 0.03608$	Λ_{10}
11	$\frac{1}{18\sqrt{3}} \approx 0.03208$	K_{11}
12	$\frac{1}{27} \approx 0.03704$	K_{12}
13	$\frac{1}{18\sqrt{3}} \approx 0.03208$	K_{13}
14	$\frac{1}{16\sqrt{3}} \approx 0.03608$	Λ_{14}
15	$\frac{1}{16\sqrt{2}} \approx 0.04419$	Λ_{15}
16	$\frac{1}{16} = 0.0625$	Λ_{16}
17	$\frac{1}{16} = 0.0625$	Λ_{17}
18	$\frac{1}{8\sqrt{3}} \approx 0.07217$	Λ_{18}
19	$\frac{1}{8\sqrt{2}} \approx 0.08839$	Λ_{19}
20	$\frac{1}{8} = 0.125$	Λ_{20}
21	$\frac{1}{4\sqrt{2}} \approx 0.17678$	Λ_{21}
22	$\frac{1}{2\sqrt{3}} \approx 0.28868$	Λ_{22}
23	$\frac{1}{2} = 0.5$	Λ_{23}
24	1	Λ_{24}
25	$\frac{1}{\sqrt{2}} \approx 0.70711$	Λ_{25}
26	$\frac{1}{\sqrt{3}} \approx 0.57735$	Λ_{26}, T_{26}
20	$\frac{1}{\sqrt{3}} \approx 0.57735$	B_{27}
28	$\frac{2}{3} \approx 0.66667$	B_{28}
29	$\frac{1}{\sqrt{3}} \approx 0.57735$	B_{29}
30	$\frac{3^{\sqrt{26}}}{2^{22}} \approx 0.65838$	Q_{30}

Tabela 2.2: Maior densidade de centro conhecida para reticulados para $4 \leq n \leq 30$

O problema de se encontrar reticulados densos é que $|\Lambda|$ nem sempre é fácil de se calcular. Na verdade, trata-se de um problema NP-difícil, em geral [12, 13]. No entanto, existem algoritmos para se computar o vetor mínimo (e norma mínima) de reticulados de determinadas classes, como A_n, D_n, seus duais e o reticulado de Leech Λ_{24} [20, 14, 15, 16, 17].

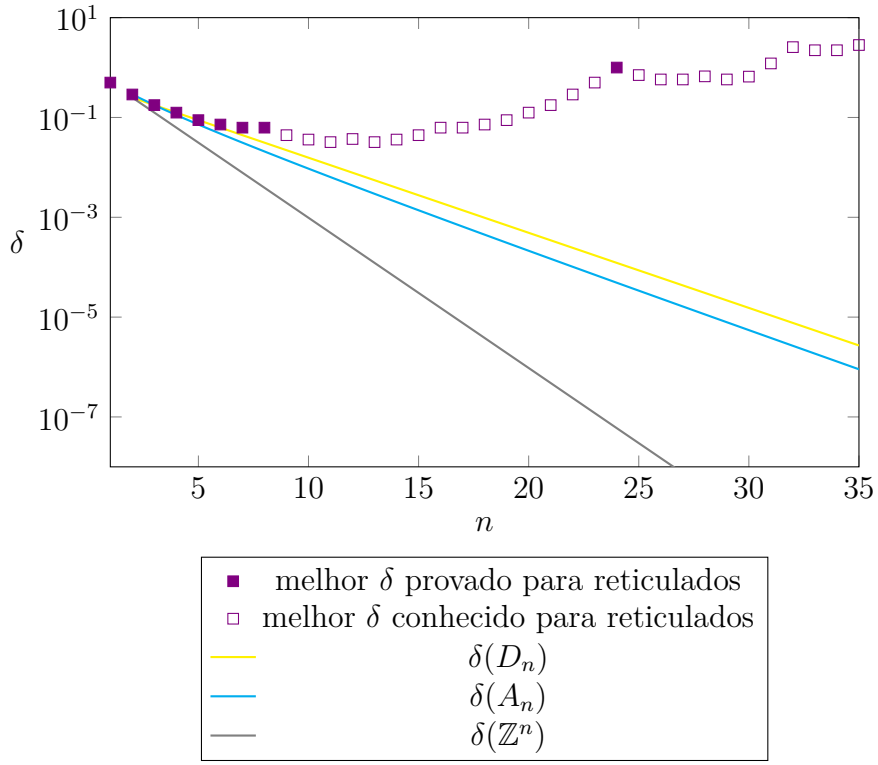

Figura 2.6: Densidade de centro de classes conhecidas em comparação com as melhores encontradas. Fonte: elaborado pelo autor.

2.3 Kissing number

O problema do *kissing number* consiste em determinar, dada uma esfera de dimensão n, o número máximo de outras esferas de mesmo raio da primeira que podem "tocá-la" simultaneamente, cada uma intersectando qualquer outra em no máximo um ponto. Em um empacotamento reticulado, o número de intersecções que uma esfera tem com outras é único.

Definição 2.11. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Chamamos de *kissing number* (ou *número de contato*) de Λ, o número

$$\kappa(\Lambda) := |S(\Lambda)|.$$

Dessa forma, para cada n, queremos encontrar $\kappa_n := \max\{\kappa(\Lambda) \colon \Lambda \subset \mathbb{R}^n \text{ é um reticulado}\}$. Não necessariamente κ_n se trata da configuração com mais esferas em geral, e sim apenas dentre as configurações que podem ser descritas por reticulados. Por exemplo, é sabido [25] que $\kappa_9 \leq 272$, mas há empacotamentos esféricos não-reticulados de dimensão 9 contendo esferas que tocam um número maior de esferas, como o empacotamento P_{9a} [20], que em particular possui esferas que tocam 306 outras.

Denotaremos o melhor kissing number para reticulados conhecido até o presente momento por κ_n^*, enquanto κ'_n denotará o maior kissing number para empacotamentos não-reticulados. Uma estratégia para o problema do kissing number é estreitar as cotas inferior e superior para κ'_n, por exemplo. Sabe-se até o momento [26, 27] que $2^{0.2041n(1+o(1))} \leq \kappa'_n \leq 2^{0.2075n(1+o(1))}$. O valor numérico para essa cota pode ser computado através de algoritmos como em [28]. Apresentamos na Figura 2.7 as melhores cotas encontradas, recentemente [29], em comparação com classes de reticulados conhecidas.

Nas dimensões $1-4$, 8 e 24, é conhecido o maior kissing number entre empacotamentos reticulados e não-reticulados. É importante notar que o problema do kissing number não é equivalente ao problema da densidade de empacotamento, haja vista que D_5 é o reticulado mais denso para a dimensão 5, mas o kissing number ideal para essa dimensão ainda é desconhecido, estando entre 40 e 44. Na verdade, é intuitivo que se possa tomar um reticulado denso qualquer, e modificar ligeiramente os vetores da base de modo a obter um novo reticulado: denso e com baixo kissing number. Isso pode ser visto com mais detalhes em [30].

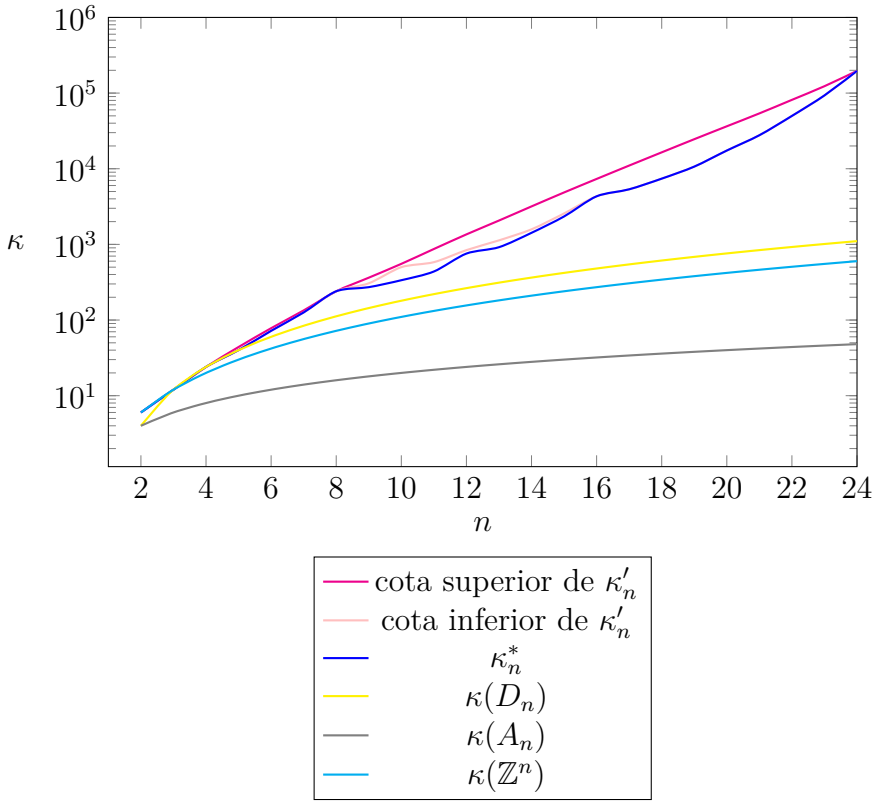

Figura 2.7: Cota inferior para o kissing number de reticulados circulantes obtidos do Teorema 4.19 se $r_0 = 2^\alpha$. Fonte: Elaborado pelo autor.

2.4 Reticulados bem-arredondados

Dentre os reticulados comprovadamente mais densos em suas respectivas dimensões, há uma propriedade em comum. Todos eles satisfazem o fato de que seus vetores mínimos geram o espaço em que estão contidos. Dizemos que reticulados que cumprem essa propriedade são *bem-arredondados*. Essa classe de reticulados tem chamado atenção, também por sua relação com a Conjectura de Minkowski [31] e pelo problema do kissing number [32].

A partir daqui utilizaremos a notação x para um vetor arbitrário de um reticulado, ao invés de $\mathbf{x}$, para que não haja confusão entre vetores de um reticulado e vetores de coeficientes $\mathbf{x}$ que multiplicam a matriz geradora.

Definição 2.12. Um reticulado $\Lambda \subset \mathbb{R}^n$ é dito *bem-arredondado* se $S(\Lambda)$ gera $\mathbb{R}^n$.

Observação 2.13. O bem-arredondamento é uma propriedade preservada com relação à semelhança.

Exemplo 2.14. Sejam Λ o reticulado de base $\{(1,0),(0,1)\}$ e $x = x_1(1,0) + x_2(0,1) \in \Lambda$ arbitrário. Então

$$\|x\|^2 = x_1^2 + x_2^2,$$

que assume valor não-nulo mínimo quando $x_1 = \pm 1$ e $x_2 = 0$, ou quando $x_1 = 0$ e $x_2 = \pm 1$. Então

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

Dessa forma, como $\{(1,0),(0,1)\} \subset S(\Lambda)$ é uma base de $\mathbb{R}^2$, conclui-se que Λ é bem-arredondado.

É claro que, como o problema do kissing number exemplifica, o número de vetores mínimos de um reticulado de dimensão n é limitado. Para $n = 2$, em particular, o número de vetores mínimos não deve passar de seis. Agora, é razoável se perguntar se é possível um reticulado com seis vetores mínimos, mas que não seja semelhante ao reticulado hexagonal, por exemplo.

Teorema 2.15 ([33])**.** *Seja $\Lambda \subset \mathbb{R}^2$ um reticulado de posto completo. Então*

1. $|S(\Lambda)| \in \{2,4,6\}$;

2. Λ *é bem-arredondado se, e somente se,* $|S(\Lambda)| \in \{4,6\}$;

3. Λ *é semelhante ao reticulado hexagonal se, e somente se,* $|S(\Lambda)| = 6$.

Demonstração. Seja $x \in S(\Lambda)$. Então é claro que $-x \in S(\Lambda)$. Sabemos que se dois vetores mínimos distintos são linearmente dependentes, então são opostos, já que possuem mesma norma. Assim, $S(\Lambda)$ tem um número par de elementos, e contem dois vetores linearmente independentes se, e somente se, $|S(\Lambda)| \geq 4$. Vejamos agora que $S(\Lambda)$ não pode ter mais de seis elementos.

Suponha que o ângulo θ entre dois vetores mínimos distintos x e y de Λ seja tal que $\theta < \frac{\pi}{3}$. Pela lei dos cossenos,

$$\|x - y\|^2 = \|x\|^2 - 2\|x\|\|y\|\cos(\theta) + \|y\|^2 < \|x\|^2 - \|x\|\|y\| + \|y\|^2.$$

Como x e y são vetores mínimos (e portanto de mesma norma), segue que

$$\|x - y\|^2 < \|x\|^2,$$

o que é absurdo, pois $x - y \neq \mathbf{0}$ e $x \in S(\Lambda)$. Portanto, o ângulo entre dois vetores mínimos distintos deve ser maior ou igual a $\frac{\pi}{3}$. Como os vetores mínimos estão compreendidos em uma mesma circunferência, então

$$\frac{2\pi}{|S(\Lambda)|} \geq \frac{\pi}{3},$$

donde segue que $|S(\Lambda)| \leq 6$.

Portanto, $|S(\Lambda)| \in \{2, 4, 6\}$, e Λ é bem-arredondado se, e somente se, $|S(\Lambda)| \in \{4, 6\}$.

Agora mostremos que se $|S(\Lambda)| = 6$, então $S(\Lambda)$ é semelhante ao reticulado hexagonal. Ora, se $|S(\Lambda)| = 6$, ordene os vetores mínimos $x_1, \cdots, x_6$ de Λ de forma que, se $\theta_1, \cdots, \theta_6$ são seus respectivos ângulos com o vetor $(1, 0)$, então $\theta_1 < \theta_2 < \cdots < \theta_6$. Dessa forma, o ângulo entre x_j e x_{j+1} é precisamente $\frac{\pi}{3}$, $\forall j \in \{1, 2, \cdots, 5\}$. De fato, se $\theta(x_j, x_{j+1})$ denota o ângulo entre x_j e x_{j+1}, e se $\theta(x_k, x_{k+1}) > \frac{\pi}{3}$ para algum $k \in \{1, 2, 3, 4, 5\}$, então

$$2\pi = \sum_{j=1}^{5} \theta(x_j, x_{j+1}) = \theta(x_k, x_{k+1}) + \sum_{\substack{j=1 \\ j \neq k}}^{5} \theta(x_j, x_{j+1}) < \tfrac{\pi}{3} + 5\tfrac{\pi}{3} = 2\pi,$$

o que é absurdo.

Basta então rotacionar Λ e multiplicar a base por um escalar conveniente, de modo que $(1, 0)$ seja um vetor mínimo. Obtém-se dessa forma o reticulado hexagonal. □

Observação 2.16. Existem infinitas classes de reticulados de posto completo em $\mathbb{R}^2$ com quatro vetores mínimos. Ou seja, $|S(\Lambda)| = 4$ não implica necessariamente em $\Lambda \sim \mathbb{Z}^2$. De fato, seja Λ um reticulado de quatro vetores mínimos. Dado $x \in S(\Lambda)$, tem-se $-x \in S(\Lambda)$, e esse vetores formam um ângulo de π entre si. Agora, um outro vetor $y \in S(\Lambda) \backslash \{x, -x\}$ deve fazer ângulos com x e $-x$ maiores que $\frac{\pi}{3}$. Mas existe uma infinidade de pontos na circunferência centrada em $\mathbf{0}$ de raio $|\Lambda|$ satisfazendo essa condição. Cada solução corresponde a

uma classe de reticulados com quatro vetores mínimos. Essa configuração está representada na Figura 2.8. Em outras palavras, os vetores mínimos de um reticulado em $\mathbb{R}^2$ com quatro vetores mínimos podem descrever infinitas classes de retângulos.

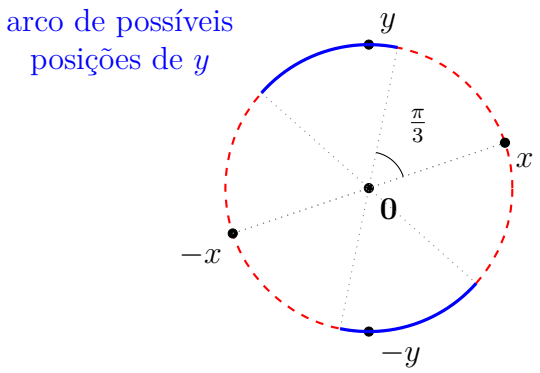

Figura 2.8: Configurações de reticulados com quatro vetores mínimos, onde $S(\Lambda) = \{x, -x, y, -y\}$. Fonte: Elaborado pelo autor.

2.5 O homomorfismo canônico

Vimos que, para gerar um reticulado, basta que se exiba uma base. Poderíamos gerar bases arbitrárias até que se obtenha um reticulado com boas propriedades, mas evidentemente não é uma estratégia razoável. Calcular parâmetros como a densidade de centro não é uma tarefa simples dada uma base arbitrária, ainda mais quando existe uma infinidade de classes de reticulados. Queremos então uma maneira consistente de gerar reticulados. É possível alcançar isso através de algoritmos que geram ponto a ponto de um reticulado, como a Construção A, que o faz através de códigos binários [20]. Outra maneira é obter bases – ou equivalentemente, matrizes reais invertíveis – através de estruturas algébricas. A ação do *homomorfismo canônico* sobre uma base integral de um corpo de números algébrico é capaz de gerar bases interessantes [4]. Vejamos isso com detalhes.

Definição 2.17. Sejam $\mathbb{K}$ e $\mathbb{K}'$ corpos contendo $\mathbb{Q}$. Dizemos que um homomorfismo $\varphi : \mathbb{K} \to \mathbb{K}'$ é um $\mathbb{Q}$-*homomorfismo* se $\varphi(a) = a$, $\forall a \in \mathbb{Q}$. Se $\mathbb{K}' = \mathbb{C}$, então chamamos φ de *imersão* ou *mergulho* de $\mathbb{K}$ em $\mathbb{C}$.

Dada uma extensão algébrica de $\mathbb{Q}$ da forma $\mathbb{K} = \mathbb{Q}(\alpha)$, onde $\alpha \in \mathbb{C}$ é evidentemente algébrico sobre $\mathbb{Q}$, vejamos quais são exatamente as imersões de $\mathbb{K}$ sobre $\mathbb{C}$.

Sejam $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}$ as raízes do polinômio minimal de α sobre $\mathbb{Q}$, denotado por $\min_{\mathbb{Q}}(\alpha)$, onde $\alpha = \alpha_1$. Então cada elemento $\beta \in \mathbb{K}$ arbitrário é da forma

$$\beta = \sum_{j=1}^{n} b_j \alpha^j,$$

onde $b_j \in \mathbb{Q}$, $\forall j \in \{1, 2, \cdots, n\}$.

Então, dado uma imersão σ de $\mathbb{K}$ sobre $\mathbb{C}$ arbitrária, tem-se por definição que

$$\sigma(\beta) = \sum_{j=1}^{n} b_j \sigma(\alpha)^j.$$

Assim, qualquer imersão de $\mathbb{K}$ pode ser diretamente determinada por $\sigma(\alpha)$. Então os n $\mathbb{Q}$-homomomorfismos determinados por

$$\sigma_j(\alpha) = \alpha_j$$

para cada $j \in \{1, 2, \ldots, n\}$, são imersões de $\mathbb{K}$. Na verdade, são as únicas imersões, já que toda imersão deve levar α em uma raiz de α. De fato, se $g = \min_{\mathbb{Q}}(\alpha)$, então

$$g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0.$$

Denotamos o número de imersões σ_j tais que $\sigma_j(\alpha) \in \mathbb{R}$ por r_1, e o número de imersões com $\sigma_j \notin \mathbb{R}$ por $2r_2$, já que cada imersão dessa forma sempre acompanha outra (seu conjugado). É usual ordenar as imersões σ_j de $\mathbb{K}$ de modo que $\sigma_j(\alpha) \in \mathbb{R}$ para $1 \leq j \leq r_1$ e $\sigma_{j+r_2} = \overline{\sigma_j}$ para $r_1 + 1 \leq j \leq r_1 + r_2$.

Definição 2.18. Seja $\mathbb{K} = \mathbb{Q}(\alpha)$ uma extensão algébrica de grau n. Chamamos o isomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(\beta) = (\sigma_1(\beta), \cdots, \sigma_{r_1}(\beta), \Re\sigma_{r_1+1}(\beta), \Im\sigma_{r_1+1}(\beta), \cdots, \Re\sigma_{r_1+r_2}(\beta), \Im\sigma_{r_1+r_2}(\beta)),$$

para todo $\beta \in \mathbb{K}$, de *homomorfismo canônico*.

Agora, precisamos aplicar o homomorfismo canônico sobre um subconjunto conveniente de $\mathbb{K}$ de modo a obter n vetores linearmente independentes. Esse subconjunto pode ser, por exemplo, uma $\mathbb{Z}$-base de um ideal não-nulo $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$, onde $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros algébricos de $\mathbb{K}$.

Proposição 2.19 ([18])**.** *Sejam $\mathbb{K} = \mathbb{Q}(\alpha)$ uma extensão algébrica de grau n e $\mathcal{I}$ um ideal não-nulo de $\mathcal{O}_{\mathbb{K}}$. Então $\sigma_{\mathbb{K}}(\mathcal{I})$ é um reticulado, com*

$$\mathrm{vol}(\sigma_{\mathbb{K}}(\mathcal{I})) = 2^{-r_2} \left| \det_{1 \leq j,k \leq n} (\sigma_j(\omega_k)) \right| \mathcal{N}(\mathcal{I}),$$

onde $\{\omega_k\}_{1 \leq k \leq n}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$.

Exemplo 2.20. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Sabe-se que $\{1, \frac{1+\sqrt{-3}}{2}\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$ [18]. Os $\mathbb{Q}$-homomorfismos sao determinados por $\sigma_1(\sqrt{-3}) = \sqrt{-3}$ e $\sigma_2(\sqrt{-3}) = -\sqrt{-3}$. Nesse caso, $r_1 = 0$ e $r_2 = 1$. Temos $\sigma_\mathbb{K} = (\Re\sigma_1, \Im\sigma_1)$. Calculando $\sigma_\mathbb{K}$ sobre a $\mathbb{Z}$-base, obtemos a base $\{(1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\}$, isto é, o reticulado hexagonal.

A dificuldade desse método de geração de reticulados é a escolha do elemento primitivo α e encontrar uma $\mathbb{Z}$-base de $\mathcal{I}$. Há variações para o método, como o *homomorfismo canônico torcido* [34], que consiste em aplicar o homomorfismo canônico sobre um ideal, mas dilatando cada coordenada por um escalar específico. Em [33], é apresentada a construção de infinitas extensões algébricas $\mathbb{K}$ de grau 2 tais que o anel dos inteiros algébricos contém um ideal $\mathcal{I}$ tal que $|S(\sigma_\mathbb{K}(\mathcal{I}))| = 4$, o que corrobora para a Observação 2.16.

3 Matrizes Circulantes

Este capítulo trata dos resultados fundamentais a respeito de matrizes circulantes, que podem ser encontrados principalmente em [35]. Destacamos o cálculo do determinante de uma matriz circulante, e sua diagonalização pela matriz de Fourier. Tratar de matrizes circulantes requer alguns resultados a respeito de permutações, os quais também exibidos, e que podem ser encontrados em [36].

3.1 Permutações

Seja $I_n = \{1, 2, \cdots, n\}$. Uma função $\sigma : I_n \to I_n$ bijetiva é denominada *permutação*. O conjunto de permutações sobre I_n é denotado por S_n, e tem estrutura de grupo com respeito à composição de funções.

Seja $\sigma \in S_n$. Podemos denotar

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

A notação admite qualquer ordem entre as colunas.

A *matriz de permutação* de σ é definida como

$$P_\sigma = \begin{pmatrix} \mathbf{e}_{\sigma(1)} \\ \mathbf{e}_{\sigma(2)} \\ \vdots \\ \mathbf{e}_{\sigma(n)} \end{pmatrix}.$$

Dessa forma,

$$P_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ x_{\sigma(2)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix}.$$

Logo, se $A = (a_{j,k})$ é uma matriz $n \times r$, então $P_\sigma A = (a_{\sigma(j),k})$, isto é, $P_\sigma A$ é A com suas linhas permutadas por σ.

É natural também observar que

$$(x_1 \quad x_2 \quad \cdots \quad x_n)P_\sigma = (x_{\sigma^{-1}(1)} \quad x_{\sigma^{-1}(2)} \quad \cdots \quad x_{\sigma^{-1}(n)}).$$

Logo, se $A = (a_{j,k})$ é uma matriz $r \times n$, então $AP_\sigma = (a_{j,\sigma^{-1}(k)})$, isto é, AP_σ é A com suas colunas permutadas por σ^{-1}.

Podemos nos perguntar no que resulta um produto entre duas matrizes de permutação.

Proposição 3.1. *Sejam $\sigma, \tau \in S_n$. Então $P_\sigma P_\tau = P_{\tau\sigma}$.*

Demonstração. Computar $P_\sigma P_\tau$ é computar o produto interno entre as linhas de P_σ e as colunas de P_τ. Sabemos que a j-ésima linha de P_σ é, por definição, $\mathbf{e}_{\sigma(j)}$. Agora, pondo $\mathrm{Id}_n = (a_{j,k})$, note que $P_\tau = \mathrm{Id}_n P_\tau = (a_{j,\tau^{-1}(k)})$. Mas

$$a_{j,\tau^{-1}(k)} = \begin{cases} 1 & \text{se } j = \tau^{-1}(k) \\ 0 & \text{caso contrário} \end{cases}.$$

Então a k-ésima coluna de P_τ é da forma $\mathbf{e}^T_{\tau^{-1}(k)}$.

Assim, estamos interessados em calcular $(\langle \mathbf{e}_{\sigma(j)}, \mathbf{e}_{\tau^{-1}(k)} \rangle)$. Tem-se

$$\begin{aligned} \langle \mathbf{e}_{\sigma(j)}, \mathbf{e}_{\tau^{-1}(k)} \rangle &= \begin{cases} 1 & \text{se } \sigma(j) = \tau^{-1}(k) \\ 0 & \text{caso contrário} \end{cases} \\ &= \begin{cases} 1 & \text{se } (\tau\sigma)(j) = k \\ 0 & \text{caso contrário} \end{cases}. \end{aligned}$$

Portanto, $P_\sigma P_\tau = P_{\tau\sigma}$. □

Da demonstração da Proposição 3.1 também tiramos que $P^T_\sigma = P_{\sigma^{-1}}$. Consequentemente, $P^T_\sigma P_\sigma = P_{\sigma^{-1}} P_\sigma = P_{\sigma\sigma^{-1}} = P_{\mathrm{id}} = \mathrm{Id}_n$, isto é, $P^T_\sigma = P^{-1}_\sigma = P_{\sigma^{-1}}$.

Vejamos agora uma classe importante de permutações.

Definição 3.2. Seja $\sigma \in S_n$. Se existem $x_1, \cdots, x_r \in I_n$ distintos tais que $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, $\cdots$, $\sigma(x_{r-1}) = x_r$, $\sigma(x_r) = x_1$ e $\sigma(j) = j \ \forall j \in I_n \backslash \{x_1, \cdots, x_r\}$, então σ é denominado *r-ciclo* e é denotado por $(x_1 \ \cdots \ x_r)$. Dizemos que r é o *comprimento* de σ.

Exemplo 3.3. $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right) \in S_4$ não é um r-ciclo, qualquer que seja r, pois $\sigma(1) = 3$ e $\sigma(3) = 1$, mas $\sigma(2) \neq 2$. No entanto, podemos escrever σ como uma composição de 2-ciclos:

$$\sigma = (1\ 3)(2\ 4). \tag{3.1}$$

Assim,

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = P_\sigma = P_{(1\ 3)(2\ 4)} = P_{(2\ 4)} P_{(1\ 3)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

A fatoração de σ em ciclos como em 3.1 evidentemente não é única, já que

$$\sigma = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4).$$

No entanto, veremos que a fatoração por ciclos disjuntos é, sim, única.

Definição 3.4. Sejam $\sigma \in S_n$ um r-ciclo e $\tau \in S_n$ um s-ciclo. Dizemos que σ e τ são permutações *disjuntas* se $\forall a \in I_n$, tem-se $\sigma(a) = a$ ou $\tau(a) = a$.

Exemplo 3.5. As permutações (1 3) e (2 4) como em 3.1 são disjuntas. Observe que comutam, isto é,

$$(1\ 3)(2\ 4) = (2\ 4)(1\ 3).$$

Proposição 3.6 ([36])**.** *Sejam $\sigma, \tau \in S_n$ dois ciclos disjuntos. Então $\sigma\tau = \tau\sigma$.*

Demonstração. Ponha $\sigma = (x_1\ x_2\ \cdots\ x_r)$ e $\tau = (y_1\ y_2\ \cdots\ y_s)$, e seja $x_j \in \{x_1, \cdots, x_r\}$. Então $\tau(x_j) = x_j$, uma vez que σ, τ são disjuntos e $\sigma(x_j) \in \{x_1, \cdots, x_r\}$. Assim, $(\sigma\tau)(x_j) = \sigma(x_j)$. Agora, $(\tau\sigma)(x_j) = \sigma(x_j)$ pois $\sigma(x_j) \in \{x_1, \cdots, x_r\}$. Portanto, $\sigma\tau = \tau\sigma$ em $\{x_1, \cdots, x_r\}$. A demonstração é análoga para $\{y_1, \cdots, y_s\}$. □

Proposição 3.7 ([36])**.** *Seja $\sigma \in S_n \backslash \{id\}$. Então σ é um produto de ciclos disjuntos de comprimentos ≥ 2. A fatoração é única a menos da ordem dos fatores.*

Demonstração. Como $\sigma \neq \mathrm{id}$, então $\exists x_1 \in I_n$ tal que $\sigma(x_1) \neq x_1$. Como σ é uma função sobre I_n, um conjunto finto, então $\exists r_1 \in \{2, 3, \cdots, n\}$ tal que $x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1)$ são distintos e $\sigma^{r_1}(x_1) \in \{x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1)\}$. Daí, $\sigma^{r_1}(x_1) = x_1$ pois caso contrário, digamos, $\sigma^{r_1}(x_1) = \sigma^j(x_1)$ para algum $j \in \{1, 2, \cdots, r_1 - 1\}$, teríamos então $\sigma^{r_1-j}(x_1) = x_1$, o que é absurdo pela construção de r_1. Portanto, temos

$$\sigma|_{\{x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1)\}} = (x_1\ \sigma(x_1)\ \cdots\ \sigma^{r_1-1}(x_1)).$$

Ponha $\sigma_1 = \sigma|_{\{x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1)\}}$.

Se σ fixa todos os elementos de

$$I_n \backslash \{x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1)\},$$

isto é, se σ restrita a esse conjunto é a identidade, então $\sigma = \sigma_1$ e conclui-se a demonstração. Se esse não é o caso, então seja $x_2 \in I_n \backslash \{x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1)\}$ tal que $\sigma(x_2) \neq x_2$. Repetindo o processo feito anteriormente, $\exists r_2 \in \{2, 3, \cdots, n\}$ tal que

$$\sigma|_{\{x_2, \sigma(x_2), \sigma^2(x_2) \cdots, \sigma^{r_2-1}(x_2)\}} = (x_2\ \sigma(x_2)\ \cdots\ \sigma^{r_2-1}(x_2)),$$

um r_2-ciclo o qual denotaremos por σ_2. Se σ restrita a

$$I_n \backslash \{x_1, \sigma(x_1), \sigma^2(x_1) \cdots, \sigma^{r_1-1}(x_1), x_2, \sigma(x_2), \sigma^2(x_2) \cdots, \sigma^{r_2-1}(x_2)\}$$

é a função identidade, então conclui-se a demonstração: $\sigma = \sigma_1\sigma_2 = \sigma_2\sigma_1$. Se esse não é o caso, continuamos o processo.

É claro que eventualmente esse processo termina, uma vez que I_n é finito. Obtemos dessa forma $\sigma = \sigma_1\sigma_2\cdots\sigma_t$, onde $\sigma_1, \sigma_2, \cdots, \sigma_t$ são ciclos disjuntos de comprimentos ≥ 2. O que significa que resta demonstrar a unicidade da fatoração.

Suponha que $\sigma = \tau_1\tau_2\cdots\tau_s$, onde $\tau_1, \tau_2, \cdots, \tau_s$ são ciclos disjuntos de comprimento ≥ 2. Como $(\tau_1\cdots\tau_s)(x_1) = \sigma(x_1) \neq x_1$, então $\exists j \in \{1, 2, \cdots, s\}$ tal que $\tau_j(x_1) \neq x_1$. Porém, como $\tau_1, \tau_2, \cdots, \tau_s$ são ciclos disjuntos, então $\tau_k(x_1) = x_1$ para todo $k \neq j$. Então

$$\sigma(x_1) = (\tau_1\cdots\tau_s)(x_1) = (\tau_j\tau_1\cdots\tau_{j-1}\tau_{j+1}\cdots\tau_s)(x_1) = \tau_j(x_1).$$

Podemos supor sem perda de generalidade que $\tau_j = \tau_1$ justamente porque $\tau_1, \tau_2, \cdots, \tau_s$ comutam. Mostraremos que $\tau_1 = \sigma_1$.

Como τ_1 é uma bijeção e $\tau_1(x_1) = \sigma(x_1)$, então $\tau_1(\sigma(x_1)) \neq \sigma(x_1)$, já que $\sigma(x_1) \neq x_1$. Daí, como $\tau_1, \tau_2, \cdots, \tau_s$ são disjuntos, então $\tau_k(\sigma(x_1)) = \sigma(x_1)$ para todo $k \geq 2$. Assim,

$$\sigma^2(x_1) = \sigma(\sigma(x_1)) = (\tau_1\cdots\tau_s)(\sigma(x_1)) = \tau_1(\sigma(x_1)).$$

De maneira análoga se obtém $\sigma^k(x_1) = \tau_1(\sigma^{k-1}(x_1))$, para todo $k \geq 1$. Em particular, $\tau_1(\sigma^{r_1-1}(x_1)) = \sigma^{r_1}(x_1) = x_1$ Portanto, $\tau_1 = (x_1\ \sigma(x_1)\ \cdots\ \sigma^{r_1-1}(x_1)) = \sigma_1$. Prossegue-se de maneira análogo com x_2 ao invés de x_2 para concluir que $\tau_2 = \sigma_2$, e assim por diante. □

3.2 Matrizes circulantes

Seja $\mathbf{v} = (c_1, \cdots, c_n) \in \mathbb{C}^n$. Uma matriz da forma

$$C_{\mathbf{v}} = \begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{pmatrix}$$

é denominada *circulante* de ordem n. Também podemos denotar $C_{\mathbf{v}} = \operatorname{circ}(c_1, \cdots, c_n)$. Os elementos de cada linha de $C_{\mathbf{v}}$ são os mesmos da linha anterior, mas movidos uma posição para a direita. Dessa forma, uma matriz circulante é determinada por um único vetor $\mathbf{v}$.

É fácil verificar que $\operatorname{circ}(a_1, \cdots, a_n) + \operatorname{circ}(b_1, \cdots, b_n) = \operatorname{circ}(a_1 + b_1, \cdots, a_n + b_n)$ e $\alpha \operatorname{circ}(c_1, \cdots, c_n) = \operatorname{circ}(\alpha c_1, \cdots, \alpha c_n)$ para todo escalar α. Portanto, as matrizes circulantes de ordem n formam um subespaço linear do espaço das matrizes de ordem n.

Nosso principal objetivo agora é encontrar os autovalores de $C_{\mathbf{v}} = \operatorname{circ}(c_1, \cdots, c_n)$. Para

isso, considere a matriz de permutação

$$\Pi = \operatorname{circ}(0,1,0,\cdots,0) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

associada ao ciclo $\sigma = (1\ 2\ \cdots\ n)$. Assim, se M é uma matriz de ordem n, então a primeira linha de ΠM é a segunda de M; a segunda linha de ΠM é a terceira de M, e assim por diante. Dessa forma,

$$\begin{aligned} \operatorname{circ}(c_1,c_2,\cdots,c_n) &= \operatorname{circ}(c_1,0,\cdots,0) + \operatorname{circ}(0,c_2,\cdots,0) + \cdots + \operatorname{circ}(0,0,\cdots,c_n) \\ &= c_1 \operatorname{circ}(1,0,\cdots,0) + c_2 \operatorname{circ}(0,1,\cdots,0) + \cdots + c_n \operatorname{circ}(0,0,\cdots,1) \\ &= c_1 I + c_2 \Pi + \cdots + c_n \Pi^{n-1} \\ &= p_{\mathbf{v}}(\Pi), \end{aligned}$$

onde $p_{\mathbf{v}}(z) = \sum_{k=1}^{n} c_k z^{k-1}$, denominado polinômio *representante* de $\operatorname{circ}(c_1,\cdots,c_n)$.

Acabamos de demonstrar a

Proposição 3.8 ([35])**.** *C é circulante se, e somente se, $\exists \mathbf{v} = (c_1,\cdots,c_n)$ tal que $C = p_{\mathbf{v}}(\Pi)$.*

Uma consequência disso é que duas matrizes circulantes de mesma ordem comutam.

Corolário 1 ([35])**.** Sejam A, B matrizes circulantes de ordem n. Então $AB = BA$.

Demonstração. Ponha $A = \operatorname{circ}(a_1,a_2,\cdots,a_n)$ e $B = \operatorname{circ}(b_1,b_2,\cdots,b_n)$. Se $\mathbf{v_a} = (a_1,\cdots,a_n)$ e $\mathbf{v_b} = (b_1,\cdots,b_n)$, então $A = p_{\mathbf{v_a}}(\Pi)$ e $B = p_{\mathbf{v_b}}(\Pi)$. Então $AB = p_{\mathbf{v_a}}(\Pi)p_{\mathbf{v_b}}(\Pi) = p_{\mathbf{v_b}}(\Pi)p_{\mathbf{v_a}}(\Pi) = BA$. □

A seguir apresentamos mais uma caracterização para matrizes circulantes, fornecida novamente por Π.

Proposição 3.9 ([35])**.** *Uma matriz C é circulante se, e somente se, $C\Pi = \Pi C$.*

Demonstração. Ponha $C = (c_{j,k})$. Então $\Pi C \Pi^{-1} = P_\sigma C P_\sigma^{-1} = P_\sigma C P_{\sigma^{-1}} = (c_{\sigma(j),\sigma(k)})$. Evidentemente podemos dizer que $C = (c_{j,k})$ é circulante se, e somente se, $c_{\sigma(j),\sigma(k)} = c_{j,k}$. Assim, C é circulante se, e somente se, $\Pi C \Pi^{-1} = C$, o que conclui a demonstração multiplicando a equação por Π. □

A Proposição 3.9 quer dizer que matrizes circulantes são aquelas em que tanto "empurrar" as linhas uma posição para baixo quanto as colunas uma posição para a esquerda surte o mesmo efeito.

Além disso, temos como consequência imediata o seguinte resultado.

Corolário 2 ([35]). *C é circulante se, e somente se, C^* é circulante.*

Demonstração. Da Proposição 3.9, C é circulante se, e somente se, $C\Pi = \Pi C$, isto é, $\Pi^{-1}C^* = \Pi^*C^* = (C\Pi)^* = (\Pi C)^* = C^*\Pi^* = C^*\Pi^{-1}$, ou seja, $C^*\Pi = \Pi C^*$. □

Denotaremos a raiz n-ésima da unidade $e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + \operatorname{sen}(\frac{2\pi}{n})$ por ζ_n, como usual.

Tome agora $\Omega = \operatorname{diag}(1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1})$, e considere a matriz de Fourier de grau n definida como $F = (\zeta_n^{jk}/\sqrt{n})_{j,k=0,1,\cdots,n-1}$, isto é,

$$F = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \zeta_n^3 & \cdots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \zeta_n^6 & \cdots & \zeta_n^{2(n-1)} \\ 1 & \zeta_n^3 & \zeta_n^6 & \zeta_n^9 & \cdots & \zeta_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \zeta_n^{3(n-1)} & \cdots & \zeta_n^{(n-1)(n-1)} \end{pmatrix}.$$

Trata-se de uma matriz de Vandermonde para o vetor $(1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1})$. É sabido que $F^{-1} = F^*$. Como F é simétrica, então $F^{-1} = \overline{F}$.

Observe que a j-ésima linha de F é da forma $n^{-\frac{1}{2}}(\zeta_n^{(j-1)0}, \zeta_n^{(j-1)1}, \cdots, \zeta_n^{(j-1)(n-1)})$. Logo, a j-ésima linha de $F\Omega$ é da forma $(n^{-\frac{1}{2}}(\zeta_n^{(j-1)r}\zeta_n^r))_{0\le r\le n-1} = (n^{-\frac{1}{2}}(\zeta_n^{jr}))_{0\le r\le n-1}$. Além disso, como $F^{-1} = \overline{F}$ e $\overline{\zeta_n^m} = \cos(\frac{2m\pi}{n}) - \operatorname{sen}(\frac{2m\pi}{n}) = \cos(\frac{-2m\pi}{n}) + \operatorname{sen}(\frac{-2m\pi}{n}) = \zeta_n^{-m}$ seja qual for $m \in \mathbb{Z}$, então a k-ésima coluna de F^{-1} é da forma $(n^{-\frac{1}{2}}\zeta_n^{-(k-1)r})_{0\le r\le n-1}$. Portanto, o (j,k)-ésimo elemento da matriz $F\Omega F^{-1}$ é

$$\begin{aligned} \frac{1}{n}\sum_{r=0}^{n-1} \zeta_n^{jr}\zeta_n^{(k-1)r} &= \frac{1}{n}\sum_{r=0}^{n-1} \zeta_n^{(j-k+1)r} \\ &= \begin{cases} 1 & \text{se } j \equiv k-1 \,(\operatorname{mod} n) \\ 0 & \text{se } j \not\equiv k-1 \,(\operatorname{mod} n) \end{cases}. \end{aligned}$$

Assim, $F\Omega F^{-1} = \Pi$. Daí, $\operatorname{circ}(c_1, c_2, \cdots, c_n) = p_{\mathbf{v}}(\Pi) = p_{\mathbf{v}}(F\Omega F^{-1}) = Fp_{\mathbf{v}}(\Omega)F^{-1}$. Portanto, toda matriz circulante é diagonalizada pela matriz de Fourier F.

Teorema 3.10 ([35]). *Seja $C = \operatorname{circ}(c_1, \cdots, c_n)$ uma matriz circulante. Então $C = FDF^{-1}$, onde*

$$F = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \zeta_n^3 & \cdots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \zeta_n^6 & \cdots & \zeta_n^{2(n-1)} \\ 1 & \zeta_n^3 & \zeta_n^6 & \zeta_n^9 & \cdots & \zeta_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \zeta_n^{3(n-1)} & \cdots & \zeta_n^{(n-1)(n-1)} \end{pmatrix}$$

e $D = \sum_{k=1}^{n} c_k(\operatorname{diag}(1, \zeta_n, \cdots, \zeta_n^{n-1}))^{k-1}$.

Como os autovalores de uma matriz diagonalizável são os elementos que compõem a diagonal, então temos a seguinte consequência.

Corolário 3 ([35])**.** Seja $C = \text{circ}\,(c_1, \cdots, c_n)$ uma matriz circulante. Então seus autovalores são da forma

$$\lambda_j = \sum_{k=1}^{n} c_k \zeta_n^{j(k-1)},$$

para $j \in \{0, 1, \cdots, n-1\}$.

Trata-se de um resultado importante, já que o determinante de uma matriz é o produto de seus autovalores.

O próximo teorema fornece uma espécie de recíproca do Teorema 3.10.

Teorema 3.11 ([35])**.** *Seja* $\Delta = \text{diag}(d_1, \cdots, d_n)$*. Então* $C = F\Delta F^{-1}$ *é circulante.*

Demonstração. Pelo conhecido Teorema Fundamental de Interpolação Polinomial, existe um único polinômio de grau $\leq n-1$ que interpola $\{(\zeta_n^{j-1}, d_j)\}_{1 \leq j \leq n}$. Escreva tal polinômio como

$$q(z) = b_1 + b_2 z + \cdots + b_n z^{n-1}.$$

Então basta observar pelo Teorema 3.10 que $\text{circ}\,(b_1, \cdots, b_n) = F\Delta F^{-1}$, já que os elementos da diagonal de $D = \sum_{k=1}^{n} b_k (\text{diag}(1, \zeta_n, \cdots, \zeta_n^{n-1}))^{k-1}$ são da forma $q(\zeta_n^{j-1}) = d_j$ para $1 \leq j \leq n$, isto é, $D = \Delta$. □

Isso significa que conseguimos uma terceira caracterização para matrizes circulantes.

Corolário 4 ([35])**.** Uma matriz C é circulante se, e somente se, existe uma matriz diagonal D tal que $C = FDF^{-1}$, onde F é a matriz de Fourier.

Uma consequência das caracterizações descritas pela Proposição 3.8 e pelo Corolário 4 é que matrizes circulantes cumprem algumas propriedades. A seguir demonstramos essas propriedades usando a última caracterização.

Teorema 3.12 ([35])**.** *Sejam* $r \in \mathbb{N}$*,* A *e* B *matrizes circulantes de ordem* n*, e* $\alpha_0, \cdots, \alpha_r$ *escalares. Então* A^T*,* A^**,* $\alpha_1 A + \alpha_2 B$*,* AB *e* $\sum_{k=0}^{r} \alpha_k A^k$ *são circulantes. Se* A *admite inversa, então* A^{-1} *é circulante. Além disso,* $AB = BA$*.*

Demonstração. Sejam D_1 e D_2 matrizes diagonais tais que $A = FD_1F^{-1}$ e $B = FD_2F^{-1}$. Então $AB = (FD_1F^{-1})(FD_2F^{-1}) = F(D_1D_2)F^{-1}$. Produtos entre matrizes diagonais são matrizes diagonais, e portanto AB é circulante. O caso particular $B = A$ demonstra que

potências de matrizes circulantes são circulantes. A saber, para todo inteiro $k \geq 0$, tem-se $A^k = (FD_1F^{-1})^k = FD^kF^{-1}$. Então $\sum_{k=0}^{r} \alpha_k A^k$ é circulante como combinação linear de matrizes circulantes.

Já sabemos que A e B comutam pelo Corolário 1. A saber, utilizando o Corolário 4, $AB = (FD_1F^{-1})(FD_2F^{-1}) = FD_1D_2F^{-1} = FD_2D_1F^{-1} = (FD_2F^{-1})(FD_1F^{-1}) = BA$.

Sabemos também que A^* é circulante pelo Corolário 2. A saber, como $F^* = F^{-1}$, então $A^* = (FDF^{-1})^* = (F^{-1})^*(FD)^* = FD^*F^{-1}$.

Consequentemente, $A^T = \overline{A^*}$ é circulante.

Já vimos que combinações lineares de matrizes circulantes são circulantes. Mas vamos exibir $\alpha_1 A + \alpha_2 B$ como no Corolário 4. Temos $\alpha_1 A + \alpha_2 B = \alpha_1(FD_1F^{-1}) + \alpha_2(FD_2F^{-1}) = F(\alpha_1 D_1)F^{-1} + F(\alpha_2 D_2)F^{-1} = F(\alpha_1 D_1F^{-1} + \alpha_2 D_2F^{-1}) = F(\alpha_1 D_1 + \alpha_2 D_2)F^{-1}$, isto é, trata-se de fato de uma matriz circulante.

Se A é não-singular, então $A^{-1} = (FDF^{-1})^{-1} = (F^{-1})^{-1}(FD)^{-1} = FD^{-1}F^{-1}$. A matriz D^{-1} é diagonal. A saber, se $D = \text{diag}\,(d_1, \cdots, d_n)$, então $D^{-1} = \text{diag}\,(d_1^{-1}, \cdots, d_n^{-1})$. Portanto, A^{-1} é circulante. □

4 Reticulados Circulantes

Neste capítulo, propomos uma maneira consistente de se obter bases de reticulados. Esse método envolve definir uma classe de reticulados, os reticulados circulantes, isto é, aqueles que aditem uma base geradora circulante. Essa caracterização tem algumas consequências relevantes, como o cálculo facilitado do determinante, e consequentemente da densidade de centro. Mostramos que, dentro de determinadas hipóteses sobre o vetor que determina a matriz geradora circulante, é possível simplificar substancialmente o cálculo da norma mínima. Dentro ainda dessas hipóteses, conseguimos construir reticulados densos.

Trata-se de um método original de geração de reticulados, desde que se tenha o devido cuidado, evidentemente, de ilustrar os trabalhos anteriores que propuseram abordagens semelhantes, e aqueles que precederam a ideia original. O reticulado A_n, por exemplo, notoriamente admite uma matriz geradora circulante, ainda que não conheçamos trabalhos que abordem essa particularidade até então. Uma classe mais abrangente de reticulados, aqueles que são preservados pelo operador de rotação, mas para entradas inteiras, foram abordados por exemplo em [37]. Reticulados gerados via polinômios possuem matrizes circulantes e foram propostos até a dimensão 3 em [38], encontrando inclusive condições sobre os coeficientes do polinômio para que a melhor densidade de centro fosse atingida. O método enfrenta um problema a partir da dimensão 4, a qual foi explorada em [39] pelos mesmos autores da presente dissertação, que é o fato de que não se consegue de maneira geral a norma de um vetor arbitrário do reticulado em função dos coeficientes do polinômio, já que o coeficiente b é separado em duas "parcelas". A solução para isso pode ser, por exemplo, inserir a hipótese de que uma dessas parcelas é nula, o que significa restringir os coeficientes do polinômio, e consequentemente suas raízes, a uma condição. Isso torna a definição de "reticulados via polinômios" pouco suscetível a generalizações, e portanto passamos a tratar o polinômio não mais como elemento determinante do reticulado, mas como uma ferramenta: o polinômio cujas raízes são os números reais que geram uma matriz circulante, e com coeficientes que aparecem nos cálculos de determinante e norma.

Agora, podemos generalizar a definição e estudar essas "parcelas" mencionadas, que nada mais são que uma forma quadrática específica aplicada ao vetor $\mathbf{u}$ que determina a matriz

circulante. O resultado desse estudo é justamente o presente capítulo. Essa forma quadrática aparece, curiosamente, em vários momentos de nosso estudo. Buscamos então condições sobre ela, quando aplicada a $\mathbf{u}$, de modo a simplificar a expressão da norma. Isso significa resolver sistemas não-lineares, o que pode ser abordado de maneira computacional. Além disso, observando computacionalmente alguns casos particulares, observamos que uma hipótese conveniente aumentaria o número de vetores mínimos, e exploramos essa hipótese. Vimos que ela possui interpretações geométricas e acarreta em resultados relevantes a respeito da densidade de centro.

Reiteramos que as definições e resultados a seguir, a menos da definição do operador de rotação de vetores, são originais.

4.1 Generalização

Seja $n \geq 2$ e defina o operador $\mathrm{rot} : \mathbb{R}^n \to \mathbb{R}^n$ por

$$\mathrm{rot}(x_1, x_2, \cdots, x_{n-1}, x_n) = (x_n, x_1, x_2, \cdots, x_{n-1}).$$

Isto é, o operador rot é aquele que "arrasta" as coordenadas de um vetor uma posição para a direita. Evidentemente, $\mathrm{rot}^n = \mathrm{id}$ em $\mathbb{R}^n$, ou seja, o grupo $\langle \mathrm{rot} \rangle$ munido da composição de funções é cíclico de ordem n.

Dizemos que um reticulado $\Lambda \subset \mathbb{R}^n$ é *circulante* se ele admite uma base da forma

$$\{\mathbf{u}, \mathrm{rot}(\mathbf{u}), \cdots, \mathrm{rot}^{n-1}(\mathbf{u})\}$$

para algum $\mathbf{u} = (\rho_1, \rho_2, \cdots, \rho_n) \in \mathbb{R}^n$. O vetor $\mathbf{u}$ determina uma matriz circulante $G_{\mathbf{u}}$ da forma

$$G_{\mathbf{u}} := \begin{pmatrix} \rho_1 & \rho_2 & \cdots & \rho_n \\ \rho_n & \rho_1 & \cdots & \rho_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_2 & \rho_3 & \cdots & \rho_1 \end{pmatrix}.$$

Assim, reticulados circulantes são aqueles que admitem uma matriz geradora circulante.

Definição 4.1. Dado $n \geq 2$, sejam $\rho_1, \rho_2, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \rho_2, \cdots, \rho_n)$. Se $\det G_{\mathbf{u}} \neq 0$, então definimos o reticulado circulante determinado por $\mathbf{u}$ por

$$\Lambda_{\mathbf{u}} := \left\{ \sum_{i=1}^{n} x_i \, \mathrm{rot}^{i-1}(\mathbf{u}) \ : \ x_i \in \mathbb{Z} \right\}.$$

Reforçamos que um único vetor $\mathbf{u}$ é suficiente para definir um reticulado circulante. Naturalmente, queremos condições sobre esse vetor de modo a maximizar $\delta(\Lambda_{\mathbf{u}})$ e $\kappa(\Lambda_{\mathbf{u}})$. Para isso, precisamos simplificar a expressão da norma de um vetor arbitrário $x = \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$.

Vejamos alguns exemplos. Sejam $a, b \in \mathbb{R}$ os coeficientes que multiplicam os termos t^{n-1} e t^{n-2} de $f(t) = \prod_{i=1}^{n}(t - \rho_i) \in \mathbb{R}[x]$. Pelas fórmulas de Viète [40],

$$\begin{cases} -a = \sum_{i=1}^{n} \rho_i \\ b = \sum_{i<j} \rho_i \rho_j \end{cases}.$$

Uma consequência disso é que

$$\|\mathbf{u}\|^2 = \sum_{i=1}^{n} \rho_i^2 = a^2 - 2b. \tag{4.1}$$

Dessa forma, se $n = 4$, então por verificação direta tem-se que

$$\begin{aligned} \left\| \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \right\|^2 =& (a^2 - 2b) \sum_{i=1}^{5} x_i^2 \\ &+ 2(\rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_4 + \rho_1\rho_4)(x_1x_2 + x_2x_3 + x_3x_4 + x_1x_4) \\ &+ 4(\rho_1\rho_3 + \rho_2\rho_4)(x_1x_3 + x_2x_4). \end{aligned}$$

Por outro lado, se $n = 5$, verifica-se que

$$\begin{aligned} \left\| \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \right\|^2 =& (a^2 - 2b) \sum_{i=1}^{5} x_i^2 \\ &+ 2(\rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_4 + \rho_4\rho_5 + \rho_1\rho_5)(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_1x_5) \\ &+ 2(\rho_1\rho_3 + \rho_2\rho_4 + \rho_3\rho_5 + \rho_1\rho_4 + \rho_2\rho_5)(x_1x_3 + x_2x_4 + x_3x_5 + x_1x_4 + x_2x_5). \end{aligned}$$

Observa-se um padrão sobre os índices ρ_i e x_j nas verificações acima. Isso é porque os termos obtidos nada mais são do que produtos internos entre o vetor $\mathbf{u}$ (ou $\mathbf{x} = (x_1, \cdots, x_n)$) e rotações dele mesmo. Por exemplo, para $n = 4$,

$$\langle \mathbf{u}, \mathrm{rot}(\mathbf{u}) \rangle = \rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_4 + \rho_1\rho_4.$$

Alternativamente, se $1 \leq i < j \leq 4$ então $\rho_i\rho_j$ é um termo da soma $\rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_4 + \rho_1\rho_4$ se $j \equiv i+1 \pmod 4$, isto é, $j - i = 1$ ou $j - i = 3$. Em outras palavras, ρ_i arbitrário multiplica ρ_j se j é obtido a partir de i saltando-se uma posição módulo 4, ou equivalentemente, se o i-ésimo vértice é conectado ao j-ésimo vértice por uma aresta no grafo circulante $\mathcal{C}_4(1)$.

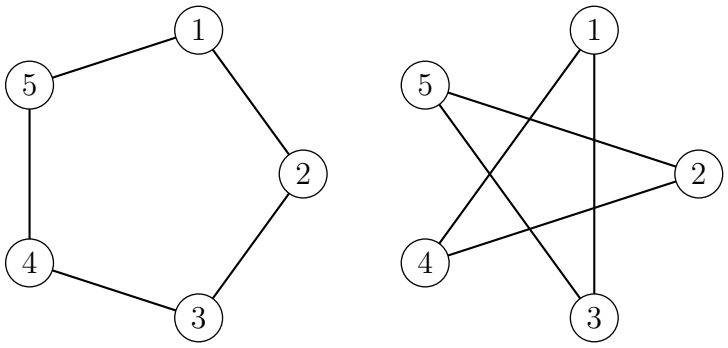

Figura 4.1: $\mathcal{C}_5(1)$ e $\mathcal{C}_5(2)$. Fonte: Elaborado pelo autor.

Defina então, dado $r \geq 0$, a forma quadrática

$$P_n(r)\,\mathbf{x} := \sum_{\substack{i,j \in I_n \\ i<j \\ j-i=r}} x_i x_j$$

para todo $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{R}^n$. Mostremos que essa definição de fato está relacionada com o produto interno de um vetor e sua r-ésima rotação.

Lema 4.2. *Sejam $n \geq 2$ e $\mathbf{x} = (x_1, \cdots, x_n)$. Se $0 \leq i < j \leq n-1$, então*

$$\langle \mathrm{rot}^i(\mathbf{x}), \mathrm{rot}^j(\mathbf{x}) \rangle = P_n(j-i)\,\mathbf{x} + P_n(n-(j-i))\,\mathbf{x}.$$

Demonstração. Temos

$$\begin{aligned}
\langle \mathrm{rot}^i(\mathbf{x}), \mathrm{rot}^j(\mathbf{x}) \rangle &= \langle \mathbf{x}, \mathrm{rot}^{j-i}(\mathbf{x}) \rangle \\
&= \langle (x_1, x_2, \cdots, x_n), (x_{n-(j-i-1)}, x_{n-(j-i-2)}, \cdots, x_n, x_1, \cdots, x_{n-(j-i)}) \rangle \\
&= \underbrace{x_1 x_{n-(j-i)+1} + x_2 x_{n-(j-i)+2} + \cdots + x_{j-i} x_n}_{P_n(n-(j-i))\,\mathbf{x}} + \underbrace{x_{j-i+1} x_1 + \cdots + x_n x_{n-(j-i)}}_{P_n(j-i)\,\mathbf{x}}.
\end{aligned}$$

□

Podemos melhorar a expressão definindo, para cada $r \in \{1, 2, \cdots, n-1\}$,

$$\mathcal{P}_n(r)\,\mathbf{x} := \sum_{\substack{i<j \\ j-i \in \{r, n-r\}}} x_i x_j.$$

Assim,

$$P_n(j-i)\,\mathbf{x} + P_n(n-(j-i))\,\mathbf{x} = \begin{cases} 2\mathcal{P}_n(j-i)\,\mathbf{x}, & \text{se } j-i = \frac{n}{2} \\ \mathcal{P}_n(j-i)\,\mathbf{x}, & \text{se } j-i \neq \frac{n}{2} \end{cases}.$$

Observe que, como feito anteriormente, podemos associar $b = \sum_{i<j} \rho_i\rho_j$ ao grafo completo $\mathcal{C}_n(1, 2, \cdots, \lfloor \frac{n}{2} \rfloor) = \mathcal{K}_n$.

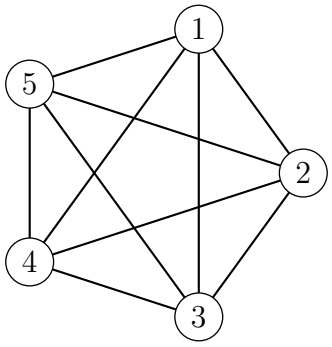

Figura 4.2: $\mathcal{C}_5(1, 2)$. Fonte: Elaborado pelo autor.

Dessa forma, podemos inferir a seguinte relação entre b e a forma quadrática $\mathcal{P}_n$.

Proposição 4.3. *Sejam* $\rho_1, \cdots, \rho_n \in \mathbb{R}$, $\mathbf{u} = (\rho_1, \cdots, \rho_n)$ *e* $f(t) = \prod_{i=1}^{n}(t - \rho_i)$. *Se* b *é o coeficiente que multiplica* t^{n-2} *em* $f(t)$, *então*

$$b = \sum_{r=1}^{\lfloor \frac{n}{2} \rfloor} \mathcal{P}_n(r)\,\mathbf{u}. \tag{4.2}$$

Demonstração. Ora, pelas Fórmulas de Viète,

$$\begin{aligned} b &= \sum_{\substack{i,j \in I_n \\ i<j}} \rho_i\rho_j \\ &= \sum_{r=1}^{n-1} \sum_{\substack{i,j \in I_n \\ i<j \\ j-i=r}} \rho_i\rho_j \\ &= \sum_{r=1}^{n-1} P_n(r)\,\mathbf{u} \\ &= \tau_n P_n(\tfrac{n}{2})\,\mathbf{u} + \sum_{\substack{r=1 \\ r\neq\frac{n}{2}}}^{n-1} P_n(r)\,\mathbf{u} \end{aligned}$$

Assim, se n é par,

$$b = P_n\left(\frac{n}{2}\right)\mathbf{u} + \underbrace{\left(P_n(1)\,\mathbf{u} + P_n(2)\,\mathbf{u} + \cdots + P_n\left(\frac{n}{2}-1\right)\mathbf{u} + P_n\left(\frac{n}{2}+1\right)\mathbf{u} + \cdots + P_n(n-1)\,\mathbf{u}\right)}_{n-2 \text{ parcelas}}$$

$$= \mathcal{P}_n\left(\frac{n}{2}\right)\mathbf{u} + \left[\mathcal{P}_n(1)\,\mathbf{u} + \mathcal{P}_n(2)\,\mathbf{u} + \cdots + \mathcal{P}_n\left(\frac{n}{2}-1\right)\mathbf{u}\right]$$
$$= \sum_{r=1}^{\frac{n}{2}} \mathcal{P}_n(r)\,\mathbf{u}$$
$$= \sum_{r=1}^{\lfloor\frac{n}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u}.$$

Por outro lado, se n é ímpar,

$$b = \underbrace{P_n(1)\,\mathbf{u} + P_n(2)\,\mathbf{u} + \cdots + P_n(n-1)\,\mathbf{u}}_{n-1 \text{ parcelas}}$$
$$= \mathcal{P}_n(1)\,\mathbf{u} + \mathcal{P}_n(2)\,\mathbf{u} + \cdots + \mathcal{P}_n\left(\frac{n-1}{2}\right)\mathbf{u}$$
$$= \sum_{r=1}^{\frac{n-1}{2}} \mathcal{P}_n(r)\,\mathbf{u}$$
$$= \sum_{r=1}^{\lfloor\frac{n}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u}.$$

□

Teorema 4.4. *Dado $n \geq 2$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$ tais que $\det G_u \neq 0$. Então, para todo $x = \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$,*

$$\|x\|^2 = (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2\sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x} + \tau_n\Big(4\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x}\Big),$$

onde $a, b \in \mathbb{R}$ são os coeficientes que multiplicam os termos t^{n-1} e t^{n-2} de $f(t) = \sum_{i=1}^{n}(t-\rho_i)$, e $\tau_n := \frac{1+(-1)^n}{2}$.

Demonstração. Seja $x = \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$ arbitrário.

$$\|x\|^2 = \langle x, x\rangle$$
$$= \left\langle \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}), \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \right\rangle$$
$$= \sum_{i=1}^{n} \left\langle x_i \mathrm{rot}^{i-1}(\mathbf{u}), \sum_{j=1}^{n} x_j \mathrm{rot}^{j-1}(\mathbf{u}) \right\rangle$$

$$
\begin{aligned}
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\langle x_i \mathrm{rot}^{i-1}(\mathbf{u}), x_j \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \sum_{i=1}^{n} x_i^2 \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{i-1}(\mathbf{u})\rangle + \sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \sum_{i=1}^{n} x_i^2 \|\mathrm{rot}^{i-1}(\mathbf{u})\|^2 + \sum_{r=1}^{n-1}\sum_{\substack{i,j\in I_n\\ |i-j|=r}} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \|\mathbf{u}\|^2 \sum_{i=1}^{n} x_i^2 + \tau_n 2 \sum_{\substack{i,j\in I_n\\ i<j\\ j-i=\frac{n}{2}}} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=r}} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= (\rho_1^2 + \cdots + \rho_n^2)\sum_{i=1}^{n} x_i^2 + \tau_n 2 \sum_{\substack{i,j\in I_n\\ i<j\\ j-i=\frac{n}{2}}} x_i x_j \Big(2\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\Big) + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=r}} x_i x_j \mathcal{P}_n(r)\,\mathbf{u} \\
&= (a^2-2b)\sum_{i=1}^{n} x_i^2 + \tau_n 4\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=\frac{n}{2}}} x_i x_j + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\left(\mathcal{P}_n(r)\,\mathbf{u}\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=r}} x_i x_j\right) \\
&= (a^2-2b)\sum_{i=1}^{n} x_i^2 + \tau_n 4\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x}.
\end{aligned}
$$

Agora, observe que, se $r \neq \frac{n}{2}$, então

$$\mathcal{P}_n(r)\,\mathbf{u} = P_n(r)\,\mathbf{x} + P_n(n-r)\,\mathbf{x} = P_n(n-(n-r))\,\mathbf{x} + P_n(n-r)\,\mathbf{x} = \mathcal{P}_n(n-r)\,\mathbf{x}.$$

Daí, se n é par,

$$
\begin{aligned}
2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x} &= 2\Big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x} + \mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x} + \cdots + \mathcal{P}_n(\tfrac{n}{2}-1)\,\mathbf{u}\,P_n(\tfrac{n}{2}-1)\,\mathbf{x} + \\
&\quad + \mathcal{P}_n(\tfrac{n}{2}+1)\,\mathbf{u}\,P_n(\tfrac{n}{2}+1)\,\mathbf{x} + \cdots + \mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x}\Big) \\
&= 2\Big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x} + \mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x} + \\
&\quad + \mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x} + \mathcal{P}_n(n-2)\,\mathbf{u}\,P_n(n-2)\,\mathbf{x} + \\
&\quad + \cdots + \mathcal{P}_n(\tfrac{n}{2}-1)\,\mathbf{u}\,P_n(\tfrac{n}{2}-1)\,\mathbf{x} + \mathcal{P}_n(\tfrac{n}{2}+1)\,\mathbf{u}\,P_n(\tfrac{n}{2}+1)\,\mathbf{x}\Big) \\
&= 2\sum_{r=1}^{\frac{n}{2}-1}\mathcal{P}_n(r)\,\mathbf{u}\,(P_n(r)\,\mathbf{x} + P_n(n-r)\,\mathbf{x})
\end{aligned}
$$

$$= 2 \sum_{r=1}^{\frac{n}{2}-1} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}$$
$$= 2 \sum_{r=1}^{\frac{n-2}{2}} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}.$$

Por outro lado, se n é ímpar,

$$2 \sum_{\substack{r=1 \\ r\neq\frac{n}{2}}}^{n-1} \mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x} = 2\big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x} + \mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x} + \cdots + \mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x}\big)$$
$$= 2\Big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x} + \mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x} +$$
$$+ \mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x} + \mathcal{P}_n(n-2)\,\mathbf{u}\,P_n(n-2)\,\mathbf{x} +$$
$$+ \cdots + \mathcal{P}_n(\tfrac{n-1}{2})\,\mathbf{u}\,P_n(\tfrac{n-1}{2})\,\mathbf{x} + \mathcal{P}_n(\tfrac{n-1}{2}+1)\,\mathbf{u}\,P_n(\tfrac{n-1}{2}+1)\,\mathbf{x}\Big)$$
$$= 2 \sum_{r=1}^{\frac{n-1}{2}} \mathcal{P}_n(r)\,\mathbf{u}\,(P_n(r)\,\mathbf{x} + P_n(n-r)\,\mathbf{x})$$
$$= 2 \sum_{r=1}^{\frac{n-1}{2}} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}.$$

Como

$$\left\lfloor \frac{n-1}{2} \right\rfloor = \begin{cases} \frac{n-1}{2} & \text{se } n \text{ é ímpar} \\ \frac{n-2}{2} & \text{se } n \text{ é par} \end{cases},$$

então

$$2 \sum_{\substack{r=1 \\ r\neq\frac{n}{2}}}^{n-1} \mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x} = 2 \sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}.$$

Assim,

$$\|x\|^2 = (a^2 - 2b) \sum_{i=1}^{n} x_i^2 + \tau_n 4 \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} + 2 \sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}.$$

□

4.2 Reticulados circulantes tipo $(1, r_0)$

Nossa primeira estratégia será zerar todos os termos $\mathcal{P}_n(r)\,\mathbf{u}$, exceto no máximo por um $r_0 \in \{1, 2, \cdots, \lfloor\frac{n}{2}\rfloor\}$. Dessa forma, teremos a norma de um vetor arbitrário $\mathbf{x}G_{\mathbf{u}} \in \Lambda_{\mathbf{u}}$ em função dos coeficientes de f e de $\mathbf{x}$. Isso significa resolver o sistema $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0-1)\,\mathbf{u} = \mathcal{P}_n(r_0+1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor\frac{n}{2}\rfloor)\,\mathbf{u} = 0$. Nem sempre é simples obter uma solução

algébrica. Em dimensões altas, é de se esperar que, do ponto de vista computacional, seja mais simples encontrar soluções numéricas para o sistema.

O sistema é equivalente a $\langle \mathbf{u}, \mathrm{rot}^r(\mathbf{u})\rangle = 0$ para cada $r \in \{1, 2, \cdots, r_0-1, r_0+1, \cdots, \lfloor \frac{n}{2} \rfloor\}$. Geometricamente, portanto, queremos um vetor $\mathbf{u}$ ortogonal em relação às suas rotações, exceto no máximo pela r_0-ésima rotação.

Corolário 5. Dado $n \geq 2$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$ tais que $\det G_{\mathbf{u}} \neq 0$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$ então, para todo $x = \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$,

$$\|x\|^2 = \begin{cases} (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 4b\mathcal{P}_n(r_0)\,\mathbf{x}, & \text{se } n \text{ é par e } r_0 = \frac{n}{2} \\ (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2b\mathcal{P}_n(r_0)\,\mathbf{x}, & \text{caso contrário} \end{cases},$$

onde $a, b \in \mathbb{R}$ são os coeficientes que multiplicam os termos x^{n-1} e x^{n-2} de $f(x) = \prod_{i=1}^{n}(x - \rho_i)$.

Demonstração. Teorema 4.4 e Proposição 4.3. □

Definição 4.5. Chamaremos um reticulado $\Lambda_{\mathbf{u}}$ que satisfaz as hipóteses do teorema interior de *reticulado circulante tipo* $(1, r_0)$.

Exemplo 4.6. Ponha $n = 4$. Se $\rho_1 = -\rho_3$, então $\mathcal{P}_4(1)\,\mathbf{u} = 0$. Logo,

$$\|x\|^2 = (a^2 - 2b)\sum_{i=1}^{4} x_i^2 + 4b\mathcal{P}_n(2)\,\mathbf{x} = (a^2 - 2b)\sum_{i=1}^{4} x_i^2 + 4b(x_1x_3 + x_2x_4).$$

Recordamos que ζ_n denota a raiz n-ésima da unidade $e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + \mathrm{sen}\,(\frac{2\pi}{n})$.

Teorema 4.7. *Dado $n \geq 2$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$, então*

$$\det G_{\mathbf{u}} = \begin{cases} -a\prod_{j=1}^{\frac{n-1}{2}} \left(a^2 - 2b + b\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right), & \text{se } n \text{ é ímpar} \\ \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + b\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right), & \text{se } n \text{ é par e } r_0 \text{ é par} \\ \pm a\sqrt{a^2 - 4b} \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + b\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right), & \text{se } n \text{ é par e } r_0 \text{ é ímpar} \end{cases}.$$

Demonstração. Como $G_{\mathbf{u}}$ é circulante, segue do Corolário 3 que seus autovalores são da forma $\lambda_j = \rho_1 + \rho_2\zeta_n^j + \cdots + \rho_n\zeta_n^{(n-1)j}$, $j = 0, 1, \cdots, n-1$.

Suponha primeiramente que n é ímpar.

Sabe-se que o determinante de uma matriz é o produto de seus autovalores, isto é,

$$\begin{aligned}\det G_{\mathbf{u}} &= \prod_{j=0}^{n-1}(\rho_1 + \rho_2\zeta_n^j + \cdots + \rho_n\zeta_n^{(n-1)j}) \\ &= (\rho_1 + \rho_2 + \cdots + \rho_n)\prod_{j=1}^{n-1}(\rho_1 + \rho_2\zeta_n^j + \cdots + \rho_n\zeta_n^{(n-1)j}) \\ &= -a\prod_{j=1}^{n-1}(\rho_1 + \rho_2\zeta_n^j + \cdots + \rho_n\zeta_n^{(n-1)j}).\end{aligned}$$

Agora,

$$\prod_{j=1}^{n-1}(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n\zeta_n^{(n-1)j})$$

$$=\prod_{j=1}^{\frac{n-1}{2}}(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n\zeta_n^{(n-1)j})(\rho_1+\rho_2\zeta_n^{n-j}+\cdots+\rho_n\zeta_n^{(n-(n-1))j})$$

$$=\prod_{j=1}^{\frac{n-1}{2}}(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n\zeta_n^{(n-1)j})(\rho_1+\rho_2\zeta_n^{-j}+\cdots+\rho_n\zeta_n^{-(n-1)j}).$$

Observe que cada termo do produto acima é da forma

$$(\rho_1^2+\cdots+\rho_n^2)+\mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j+\zeta_n^{-j})+\mathcal{P}_n(2)\,\mathbf{u}\,(\zeta_n^{2j}+\zeta_n^{-2j})+\cdots+\mathcal{P}_n(\tfrac{n-1}{2})\,\mathbf{u}\left(\zeta_n^{\frac{n-1}{2}j}+\zeta_n^{-\frac{n-1}{2}j}\right).$$

Logo, como $\mathcal{P}_n(1)\,\mathbf{u}=\cdots=\mathcal{P}_n(r_0-1)\,\mathbf{u}=\mathcal{P}_n(r_0+1)\,\mathbf{u}=\cdots=\mathcal{P}_n(\frac{n-1}{2})\,\mathbf{u}=0$, tem-se

$$\det G_{\mathbf{u}}=-a\prod_{j=1}^{\frac{n-1}{2}}\left(a^2-2b+\mathcal{P}_n(r_0)\,\mathbf{u}\left(\zeta_n^{r_0j}+\zeta_n^{-r_0j}\right)\right)$$

$$=-a\prod_{j=1}^{\frac{n-1}{2}}\left(a^2-2b+b\left(\zeta_n^{r_0j}+\zeta_n^{-r_0j}\right)\right).$$

Por outro lado, suponha n par.

$$\det G_{\mathbf{u}}=\prod_{j=0}^{n-1}(\rho_1+\rho_2\zeta_n^j+\rho_3\zeta_n^{2j}+\cdots+\rho_n\zeta_n^{(n-1)j})$$

$$=(\rho_1+\cdots+\rho_n)(\rho_1+\rho_2\zeta_n^{\frac{n}{2}}+\rho_3+\cdots+\rho_{n-1}+\rho_n\zeta_n^{\frac{n}{2}})\prod_{\substack{j=1\\ j\neq\frac{n}{2}}}^{n-1}(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n\zeta_n^{(n-1)j})$$

$$=-a(\rho_1-\rho_2+\rho_3-\cdots+\rho_{n-1}-\rho_n)\prod_{\substack{j=1\\ j\neq\frac{n}{2}}}^{n-1}(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n\zeta_n^{(n-1)j}).$$

Se r_0 é par, mostremos que $\rho_1-\rho_2+\cdots+\rho_{n-1}-\rho_n=\pm a$. Por um lado, se $\rho_2+\rho_4+\cdots+\rho_n=0$, então $\rho_1-\rho_2+\cdots+\rho_{n-1}+\rho_n=\rho_1+\rho_3+\cdots+\rho_{n-1}=-a$. Por outro lado, se $\rho_2+\rho_4+\cdots+\rho_n\neq 0$, como

$$(\rho_2+\rho_4+\cdots+\rho_n)(-a)=(\rho_2+\rho_4+\cdots+\rho_n)[(\rho_2+\rho_4+\cdots+\rho_n)+(\rho_1+\rho_3+\cdots+\rho_{n-1})]$$

$$=(\rho_2+\rho_4+\cdots+\rho_n)^2+\sum_{\substack{i,j\in I_n\\ i\text{ par}\\ j\text{ ímpar}}}\rho_i\rho_j$$

$$=(\rho_2+\rho_4+\cdots+\rho_n)^2+\sum_{\substack{1\leq r\leq\frac{n}{2}\\ r\text{ ímpar}}}\mathcal{P}_n(r)\,\mathbf{u}$$

$$= (\rho_2 + \rho_4 + \cdots + \rho_n)^2,$$

então $-a = \rho_2 + \rho_4 + \cdots + \rho_n$. Observe que nos cálculos acima utilizamos o fato de que se n é par, então $n - r$ tem a mesma paridade de r, para todo $r \in \{1, 2, \cdots, \frac{n}{2}\}$. Assim, cada termo da soma $\mathcal{P}_n(r)\,\mathbf{u}$ tem índices de mesma paridade quando r é par, e de paridade diferente se r é ímpar.

Agora, $-a = \rho_1 + \cdots + \rho_n$, e então $\rho_1 + \rho_3 + \cdots + \rho_{n-1} = 0$. Daí, $\rho_1 - \rho_2 + \cdots + \rho_{n-1} - \rho_n = -(\rho_2 + \rho_4 + \cdots + \rho_n) = a$.

Assim, se r_0 é par,

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a^2 \prod_{\substack{j=1 \\ j \neq \frac{n}{2}}}^{n-1} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n \zeta_n^{(n-1)j}) \\
&= \pm a^2 \prod_{j=1}^{\frac{n}{2}-1} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n \zeta_n^{(n-1)j})(\rho_1 + \rho_2 \zeta_n^{-j} + \cdots + \rho_n \zeta_n^{-(n-1)j}) \\
&= \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n \zeta_n^{(n-1)j})(\rho_1 + \rho_2 \zeta_n^{-j} + \cdots + \rho_n \zeta_n^{-(n-1)j}).
\end{aligned}$$

Novamente, cada termo do produto acima é da forma

$$(\rho_1^2 + \cdots + \rho_n^2) + \mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j + \zeta_n^{-j}) + \mathcal{P}_n(2)\,\mathbf{u}\,(\zeta_n^{2j} + \zeta_n^{-2j}) + \cdots + \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\left(\zeta_n^{\frac{n}{2}j} + \zeta_n^{-\frac{n}{2}j}\right).$$

Logo, como $P_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = 0$, tem-se

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + \mathcal{P}_n(r_0)\,\mathbf{u}\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right) \\
&= \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + b\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right).
\end{aligned}$$

Agora, se r_0 é ímpar, mostremos que $\rho_1 - \rho_2 + \cdots + \rho_{n-1} - \rho_n = \pm\sqrt{a^2 - 4b}$.

$$\begin{aligned}
(\rho_1 - \rho_2 + \rho_3 - \cdots + \rho_{n-1} - \rho_n)^2 &= [(\rho_1 + \rho_3 + \cdots + \rho_{n-1}) - (\rho_2 + \rho_4 + \cdots + \rho_n)]^2 \\
&= (\rho_1 + \rho_3 + \cdots + \rho_{n-1})^2 + (\rho_2 + \rho_4 + \cdots + \rho_n)^2 \\
&\quad - 2(\rho_1 + \rho_3 + \cdots + \rho_{n-1})(\rho_2 + \rho_4 + \cdots + \rho_n) \\
&= (\rho_1^2 + \rho_2^2 + \cdots + \rho_n^2) + 2\sum_{\substack{i,j \in I_n \\ i,j \text{ ímpares} \\ i \neq j}} \rho_i \rho_j + 2\sum_{\substack{i,j \in I_n \\ i,j \text{ pares} \\ i \neq j}} \rho_i \rho_j - 2\sum_{\substack{i,j \in I_n \\ i \text{ par} \\ j \text{ ímpar}}} \rho_i \rho_j
\end{aligned}$$

$$
\begin{aligned}
&= (a^2 - 2b) + 2\left(b - \sum_{\substack{i,j\in I_n \\ i \text{ par} \\ j \text{ ímpar}}} \rho_i\rho_j\right) - 2\sum_{\substack{i,j\in I_n \\ i \text{ par} \\ j \text{ ímpar}}} \rho_i\rho_j \\
&= a^2 - 4\sum_{\substack{i,j\in I_n \\ i \text{ par} \\ j \text{ ímpar}}} \rho_i\rho_j \\
&= a^2 - 4\sum_{\substack{1\le r\le \frac{n}{2} \\ r \text{ ímpar}}} \mathcal{P}_n(r)\,\mathbf{u} \\
&= a^2 - 4\mathcal{P}_n(r_0)\,\mathbf{u} \\
&= a^2 - 4b.
\end{aligned}
$$

Assim, se r_0 é ímpar,

$$
\begin{aligned}
\det G_{\mathbf{u}} &= \pm a\sqrt{a^2-4b}\prod_{j=1}^{\frac{n-2}{2}}\left(a^2 - 2b + \mathcal{P}_n(r_0)\,\mathbf{u}\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right) \\
&= \pm a\sqrt{a^2-4b}\prod_{j=1}^{\frac{n-2}{2}}\left(a^2 - 2b + b\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right).
\end{aligned}
$$

□

4.2.1 O caso $r_0 \neq \frac{n}{2}$

Investiguemos primeiramente o caso em que $\|x\|^2$ é da forma $(a^2-2b)\sum_{i=1}^{n} x_i^2 + 2b\mathcal{P}_n(r_0)\,\mathbf{x}$, isto é, quando $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0-1)\,\mathbf{u} = \mathcal{P}_n(r_0+1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor\frac{n}{2}\rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor\frac{n-1}{2}\rfloor\}$. Em outras palavras, $\Lambda_{\mathbf{u}}$ é um reticulado circulante tipo $(1, r_0)$, com $r_0 \neq \frac{n}{2}$. No entanto, um cuidado deve ser tomado. Algumas soluções para o sistema podem implicar em $\det G_{\mathbf{u}} = 0$. Por exemplo, se em particular n é par com r_0 ímpar e $a^2 = 4b$, então pelo Teorema 4.7, o determinante é nulo. O próximo teorema apresenta uma condição suficiente para que se tenha $\det G_{\mathbf{u}} \neq 0$.

Teorema 4.8. *Dado $n \geq 2$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$ tais que $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0-1)\,\mathbf{u} = \mathcal{P}_n(r_0+1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor\frac{n}{2}\rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor\frac{n-1}{2}\rfloor\}$. Se D é a forma quadrática em $\mathbb{Z}$ definida por*

$$D\mathbf{x} = (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2b\mathcal{P}_n(r_0)\,\mathbf{x},$$

então são equivalentes:

(i) $\det G_{\mathbf{u}} \neq 0$*;*

(ii) D *é positiva definida;*

Além disso, se $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$*,* $a \neq 0$ *e* $a^2 \geq 4b$*, então* D *é positiva definida.*

Demonstração.

- ((i) $\iff$ (ii))

  Se $\det G_{\mathbf{u}} \neq 0$, então $\{\mathbf{u}, \mathrm{rot}(\mathbf{u}), \cdots, \mathrm{rot}^{n-1}(\mathbf{u})\}$ é um conjunto de vetores linearmente independentes, e $\Lambda_{\mathbf{u}}$ é o reticulado gerado por essa base. Suponha que D não seja positiva definida, isto é, que $\exists \mathbf{x} \in \mathbb{Z}^n \backslash \{0\}$ tal que $D\mathbf{x} \leq 0$. Dessa forma, se $x = \mathbf{x}G_{\mathbf{u}} \in \Lambda_{\mathbf{u}}$, tem-se

  $$\|x\|^2 = \|G_{\mathbf{u}}\mathbf{x}^T\|^2 = D\mathbf{x} \leq 0,$$

  o que é absurdo. Portanto, D é positiva definida.

  Por outro lado, suponha D positiva definida, e mostremos que $\det G_{\mathbf{u}} \neq 0$, isto é, que $\{\mathbf{u}, \mathrm{rot}(\mathbf{u}), \cdots, \mathrm{rot}^{n-1}(\mathbf{u})\}$ é um conjunto de vetores linearmente independentes. De fato, seja $x = \mathbf{x}G_{\mathbf{u}}$ um vetor gerado pelo conjunto, tal que $x = 0$.

  $$D\mathbf{x} = \|\mathbf{x}G_{\mathbf{u}}\|^2 = \|x\|^2 = 0.$$

  Como D é positiva definida, só pode ser que $\mathbf{x} = 0$. Portanto, $\{\mathbf{u}, \mathrm{rot}(\mathbf{u}), \cdots, \mathrm{rot}^{n-1}(\mathbf{u})\}$ é um conjunto de vetores linearmente independentes.

- ($\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$, $a^2 \geq 4b$, $a \neq 0 \implies$ D é positiva definida)

  Observe que, para todo $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$,

  $$\begin{aligned} D\mathbf{x} &= (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2b\mathcal{P}_n(r_0)\,\mathbf{x} \\ &= (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2b\sum_{\substack{i,j\in I_n \\ i<j \\ j-i\in\{r_0,n-r_0\}}} x_i x_j \\ &= \frac{a^2}{4}\sum_{\substack{i,j\in I_n \\ i<j \\ j-i\in\{r_0,n-r_0\}}}(x_i + x_j)^2 + \frac{a^2-4b}{4}\sum_{\substack{i,j\in I_n \\ i<j \\ j-i\in\{r_0,n-r_0\}}}(x_i - x_j)^2. \end{aligned}$$

  Observe que, se $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$, então $\mathbf{x} \neq 0 \implies (x_i + x_j)^2 \geq 1$ para algum par $(i,j) \in \{(i,j) \in I_n \times I_n \colon i < j,\ j - i \in \{r_0, n - r_0\}\}$.

  Com efeito, observe que $\forall i \in \mathbb{N}$, $\exists! j \in I_n$ tal que $\overline{i} = \overline{j}$. Defina

  $$\varphi \colon \mathbb{N} \to I_n\,,$$

$$i \mapsto j$$

e seja $\mathbf{x} = (x_1, \cdots, x_n) \neq 0$. Sem perda de generalidade, suponha que $x_1 \neq 0$, uma vez que, caso contrário, basta rotacionar $\mathbf{x}$ um número suficiente de vezes.

Suponha que $(x_i + x_j)^2 = 0$ para todo par $(i, j) \in \{(i, j) \in I_n^2 \colon i < j,\ j - i \in \{r_0, n - r_0\}\}$. Em particular,

$$x_1 = -x_{\varphi(1+r_0)} = x_{\varphi(1+2r_0)} = \cdots = -x_{\varphi(1+(k_0-1)r_0)},$$

onde $k_0 = \min\{k \in \mathbb{Z}_+^* \colon \overline{1 + kr_0} = \overline{1}\}$.

Daí, k_0 é par, pois caso contrário, $x_1 = -x_1$.

Por outro lado, $\frac{n}{(r_0,n)} \in \{k \in \mathbb{Z}_+^* \colon \overline{1 + kr_0} = \overline{1}\}$, e

$$\overline{1 + k_0 r_0} = \overline{1} \implies \overline{k_0 r_0} = \overline{0} \implies n \mid k_0 r_0 \implies \frac{n}{(r_0, n)} \mid k_0 \frac{r_0}{(r_0, n)} \implies \frac{n}{(r_0, n)} \mid k_0.$$

Consequentemente, $k_0 = \frac{n}{(r_0,n)}$. Portanto, $\frac{n}{(r_0,n)} \in 2\mathbb{Z}$.

Assim, se $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$ com $a^2 \geq 4b$ e $a \neq 0$, então

$$D\mathbf{x} \geq \frac{a^2}{4} > 0$$

Daí, D é positiva e definida.

□

Dessa forma, contanto que escolhamos r_0 conveniente, temos $\Lambda_{\mathbf{u}}$ definido se $0 \neq a^2 \geq 4b$. Veremos que a situação $0 \neq a^2 = 4b$, em particular, é bastante conveniente.

Dentro da hipótese do Teorema 4.8, como $r_0 \neq \frac{n}{2}$, então $a^2 = 4b \iff a^2 - 2b = 2b \iff \|\mathbf{u}\|^2 = 2\mathcal{P}_n(r_0)\,\mathbf{u} \iff \langle \mathbf{u}, \mathbf{u} \rangle = 2\langle \mathbf{u}, \mathrm{rot}^{r_0}(\mathbf{u}) \rangle \iff \mathrm{rot}^{r_0}(\mathbf{u}) \in \{\mathbf{v} \in \mathbb{R}^n \colon \langle \mathbf{v}, \mathbf{u} \rangle = \frac{1}{2}\|\mathbf{u}\|^2\} \cap \Lambda_{\mathbf{u}}$, tendo em vista as equações (4.1) e (4.2). Em outras palavras, $\mathbf{u} - \mathrm{rot}^{r_0}(\mathbf{u})$ é um vetor do reticulado $\Lambda_{\mathbf{u}}$ pertencente ao semi-espaço de dimensão $n - 1$ dos vetores tão próximos da origem quanto de $\mathbf{u}$. De fato, temos $\|\mathbf{u} - \mathrm{rot}^{r_0}(\mathbf{u})\|^2 = \langle \mathbf{u} - \mathrm{rot}^{r_0}(\mathbf{u}), \mathbf{u} - \mathrm{rot}^{r_0}(\mathbf{u}) \rangle = \langle \mathrm{rot}^{r_0}(\mathbf{u}), \mathrm{rot}^{r_0}(\mathbf{u}) \rangle = \|\mathrm{rot}^{r_0}(\mathbf{u})\|^2 = \|\mathbf{u}\|^2$. Geometricamente, portanto, o triângulo determinado por $\mathbf{0}, \mathbf{u}$ e $\mathrm{rot}^{r_0}(\mathbf{u})$ é isósceles. Daí, se $\mathbf{u}$ é em particular um vetor mínimo, então $\mathbf{u} - \mathrm{rot}^{r_0}(\mathbf{u})$ também o é, além das próprias rotações de $\mathbf{u}$. É de se esperar que $|S(\Lambda_{\mathbf{u}})|$ aumente, nesse caso.

Definição 4.9. Sejam $n \geq 2$ e $r \in \{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$. Defina a forma quadrática $Q_r^{(n)} : \mathbb{Z}^n \to \mathbb{Z}$ por

$$Q_r^{(n)}\mathbf{x} := \sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r)\,\mathbf{x}.$$

Teorema 4.10. *Dado $n \geq 2$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ tais que $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ tal que $\frac{n}{(r_0, n)} \notin 2\mathbb{Z}$.*

Então, se $0 \neq a^2 = 4b$, tem-se

$$|\Lambda_{\mathbf{u}}| = \frac{a^2}{2}$$

e

$$|S(\Lambda_{\mathbf{u}})| = \#\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon Q_{r_0}^{(n)}\mathbf{x} = 1\}.$$

Demonstração. Como $a^2 = 4b$, então $a^2 - 2b = 2b = \frac{a^2}{2}$. Pelo Teorema 4.8, $\forall \mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$,

$$D\mathbf{x} = \frac{a^2}{2}\left(\sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r_0)\,\mathbf{x}\right) \geq 0,$$

onde vale a igualdade se, e somente se, $\mathbf{x} = 0$. Daí, se $\mathbf{x} \neq 0$, como $\frac{a^2}{2} > 0$, tem-se

$$Q_{r_0}^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r_0)\,\mathbf{x} > 0,$$

isto é,

$$Q_{r_0}^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r_0)\,\mathbf{x} \geq 1,$$

pois $x_1, \cdots, x_n \in \mathbb{Z}$.

Agora, observe que

$$\mathbf{x} = (x_1, \cdots, x_n) = (1, 0, \cdots, 0) \implies Q_{r_0}^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r_0)\,\mathbf{x} = 1.$$

Portanto, $\{D\mathbf{x} \colon \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\}\}$ é limitado inferiormente por $\frac{a^2}{2}$, ao mesmo tempo que $D(1, 0, \cdots, 0) = \frac{a^2}{2}$. Portanto,

$$|\Lambda_{\mathbf{u}}| := \min\{D\mathbf{x} \colon \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\}\} = \frac{a^2}{2},$$

e

$$\begin{aligned}
|S(\Lambda_{\mathbf{u}})| &:= \#D^{-1}(\{|\Lambda_{\mathbf{u}}|\}) \\
&= \#D^{-1}\left(\left\{\frac{a^2}{2}\right\}\right) \\
&= \#\left\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon D\mathbf{x} = \frac{a^2}{2}\right\} \\
&= \#\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon Q_{r_0}^{(n)}\mathbf{x} = 1\}.
\end{aligned}$$

□

Graças ao Teorema 4.10, fixado $n \geq 2$, podemos mais facilmente calcular $|S(\Lambda_{\mathbf{u}})|$ através de um software. Em dimensões baixas, não temos dificuldade em encontrar soluções algébricas para o sistema não-linear $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$. Vejamos alguns exemplos.

Exemplo 4.11. Sejam $\rho_1, \cdots, \rho_5 \in \mathbb{R}$ e $u = (\rho_1, \cdots, \rho_5)$. Se $\rho_1 = \rho_3 = \rho_4 = 0$ e $\rho_2 \neq -\rho_5$, então

$$a^2 = 4b \implies \begin{cases} \delta(\Lambda_{\mathbf{u}}) = \delta(D_5) \\ \kappa(\Lambda_{\mathbf{u}}) = \kappa(D_5) \end{cases}.$$

Demonstração. Como $\rho_1 = \rho_3 = \rho_4 = 0$, então $\mathcal{P}_5(1)\,\mathbf{u} = \rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_4 + \rho_4\rho_5 + \rho_1\rho_5 = 0$.

Além disso, pelas Fórmulas de Viète, $a = -(\rho_2 + \rho_5) \neq 0$. Além disso, pelo Teorema 4.7,

$$\det G_{\mathbf{u}} = -a\Big(a^2 - 2b + b\Big(\zeta_5^2 + \zeta_5^{-2}\Big)\Big)\Big(a^2 - 2b + b\Big(\zeta_5 + \zeta_5^{-1}\Big)\Big).$$

Logo, se $a^2 = 4b$, tem-se

$$\begin{aligned} \det G_{\mathbf{u}} &= -ab^2\Big(\zeta_5^2 + \zeta_5^{-2} + 2\Big)\Big(\zeta_5 + \zeta_5^{-1} + 2\Big) \\ &= -\frac{a^5}{16}\Big(\zeta_5^2 + \zeta_5^{-2} + 2\Big)\Big(\zeta_5 + \zeta_5^{-1} + 2\Big) \\ &= -\frac{a^5}{16}. \end{aligned}$$

Assim, de $0 \neq a^2 = 4b$, tem-se que $\Lambda_{\mathbf{u}}$ é um reticulado tal que, dado $x \in \Lambda_{\mathbf{u}}$ arbitrário, tem-se

$$\|x\|^2 = (a^2 - 2b)\sum_{i=1}^{5} x_i^2 + 2b\mathcal{P}_n(2)\,\mathbf{x}.$$

Com o auxílio de um software, observa-se facilmente que:

$$|S(\Lambda_{\mathbf{u}})| = \#\{\mathbf{x} \in \mathbb{Z}^5 \backslash \{\mathbf{0}\} \colon Q_2^{(5)}\mathbf{x} = 1\} = 40 = \kappa(D_5).$$

Em outras palavras, $\Lambda_{\mathbf{u}}$ possui o mesmo número de vetores mínimos que D_5. Agora,

$$\begin{aligned} \delta(\Lambda_{\mathbf{u}}) :&= \frac{\left(\frac{\sqrt{|\Lambda_{\mathbf{u}}|}}{2}\right)^5}{|\det G|} \\ &= \frac{16\left(\frac{\sqrt{a^2}}{2\sqrt{2}}\right)^5}{|a^5|} \\ &= \frac{16}{2^7\sqrt{2}} \\ &= \frac{1}{8\sqrt{2}} \\ &= \delta(D_5). \end{aligned}$$

□

No exemplo anterior, obtemos $\Lambda_{\mathbf{u}}$ com a melhor densidade de centro possível para a dimensão 5. Vale notar que se $\rho_1 = \rho_3 = \rho_4 = 0$, então $a^2 = 4b \iff \rho_2 = \rho_5$. Logo, $\Lambda_{\mathbf{u}}$ como no exemplo anterior é uma dilatação de $\Lambda_{\mathbf{v}}$, onde $\mathbf{v} = (0, 1, 0, 0, 1)$.

De maneira geral, é possível mostrar o

Exemplo 4.12. Sejam $\rho_1, \cdots, \rho_5 \in \mathbb{R}$ e $u = (\rho_1, \cdots, \rho_5)$ tais que $\mathcal{P}_5(r)\,\mathbf{u} = 0$ exceto para um $r = r_0 \in \{1, 2\}$. Então

$$0 \neq a^2 = 4b \implies \begin{cases} \delta(\Lambda_{\mathbf{u}}) = \delta(D_5) \\ \kappa(\Lambda_{\mathbf{u}}) = \kappa(D_5) \end{cases}.$$

Demonstração. Vimos no exemplo anterior que $a^2 = 4b$ implica em

$$\det G = -\frac{a^5}{16}.$$

Logo, se $a \neq 0$, tem-se $\det G_{\mathbf{u}} \neq 0$.

Além disso, novamente, calcula-se facilmente com um software que

$$\begin{aligned} |S(\Lambda_{\mathbf{u}})| &= \#\{\mathbf{x} \in \mathbb{Z}^5 \backslash \{\mathbf{0}\} \colon Q_1^{(5)}\mathbf{x} = 1\} \\ &= \#\{\mathbf{x} \in \mathbb{Z}^5 \backslash \{\mathbf{0}\} \colon Q_2^{(5)}\mathbf{x} = 1\} \\ &= 40 \\ &= \kappa(D_5). \end{aligned}$$

Isso significa que não importa qual o $r_0 \in \{1, 2\}$ escolhido, $S(\Lambda_{\mathbf{u}})$ sempre terá precisamente 40 elementos distintos.

Além disso, de $0 \neq a^2 = 4b$ tem-se $|\Lambda_{\mathbf{u}}| = \frac{a^2}{2}$. Daí,

$$\begin{aligned} \delta(\Lambda_{\mathbf{u}}) :&= \frac{\left(\frac{\sqrt{|\Lambda_{\mathbf{u}}|}}{2}\right)^5}{|\det G|} \\ &= \frac{16\left(\frac{\sqrt{a^2}}{2\sqrt{2}}\right)^5}{|a^5|} \\ &= \frac{16}{2^7\sqrt{2}} \\ &= \frac{1}{8\sqrt{2}} \\ &= \delta(D_5). \end{aligned}$$

□

Notavelmente, algo semelhante pode-se dizer a respeito de $n = 7$.

Exemplo 4.13. Sejam $\rho_1, \cdots, \rho_7 \in \mathbb{R}$ e $u = (\rho_1, \cdots, \rho_5)$ tais que $\mathcal{P}_7(r)\,\mathbf{u} = 0$ exceto para um $r = r_0 \in \{1, 2, 3\}$. Então

$$0 \neq a^2 = 4b \implies \Lambda_{\mathbf{u}} \begin{cases} \delta(\Lambda_{\mathbf{u}}) = \delta(D_7) \\ \kappa(\Lambda_{\mathbf{u}}) = \kappa(D_7) \end{cases} .$$

Demonstração. Um simples cálculo em um software verifica que, se $a^2 = 4b$, tem-se

$$\det G = -\frac{a^7}{64}.$$

Logo, se $a \neq 0$, tem-se $\det G_{\mathbf{u}} \neq 0$.

Além disso, calcula-se facilmente com um software que

$$\begin{aligned} |S(\Lambda_{\mathbf{u}})| &= \#\{\mathbf{x} \in \mathbb{Z}^7 \backslash \{\mathbf{0}\} \colon Q_1^{(7)}\mathbf{x} = 1\} \\ &= \#\{\mathbf{x} \in \mathbb{Z}^7 \backslash \{\mathbf{0}\} \colon Q_2^{(7)}\mathbf{x} = 1\} \\ &= \#\{\mathbf{x} \in \mathbb{Z}^7 \backslash \{\mathbf{0}\} \colon Q_3^{(7)}\mathbf{x} = 1\} \\ &= 84 \\ &= \kappa(D_7). \end{aligned}$$

Novamente, não importa qual o $r_0 \in \{1, 2, 3\}$ escolhido, $S(\Lambda_{\mathbf{u}})$ sempre terá precisamente 84 elementos distintos.

Além disso, se $0 \neq a^2 = 4b$, tem-se $|\Lambda_{\mathbf{u}}| = \frac{a^2}{2}$. Daí,

$$\begin{aligned} \delta(\Lambda_{\mathbf{u}}) :&= \frac{\left(\frac{\sqrt{|\Lambda_{\mathbf{u}}|}}{2}\right)^7}{|\det G|} \\ &= \frac{64\left(\frac{\sqrt{a^2}}{2\sqrt{2}}\right)^7}{|a^7|} \\ &= \frac{64}{2^{10}\sqrt{2}} \\ &= \frac{1}{16\sqrt{2}} \\ &= \delta(D_7). \end{aligned}$$

□

A condição $0 \neq a^2 = 4b$ parece conveniente nos casos em que $\|x\|^2 = (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2b\mathcal{P}_n(r_0)\,\mathbf{x}$. No entanto, reforçamos que a escolha de r_0 é delicada. Dentro da condição $0 \neq a^2 = 4b$, a suposição $\frac{n}{(r_0, n)} \notin 2\mathbb{Z}$ é *necessária* para que $\det G_{\mathbf{u}} \neq 0$.

Proposição 4.14. *Dado $n \geq 2$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$, e $0 \neq a^2 = 4b$, então*

$$\det G_{\mathbf{u}} \neq 0 \iff \frac{n}{(r_0, n)} \notin 2\mathbb{Z}$$

Demonstração. Suponha que $\frac{n}{(r_0,n)} \in 2\mathbb{Z}$, isto é, que $\exists c \in 2\mathbb{Z}$ tal que $n = c(r_0, n)$. Então n é par. Além disso, $\frac{r_0}{(r_0,n)}$ é impar, pois caso contrário, teríamos $(r_0, n) = (r_0, n)\left(\frac{r_0}{(r_0,n)}, \frac{n}{(r_0,n)}\right)$, e então $\underbrace{\left(\frac{r_0}{(r_0,n)}, \frac{n}{(r_0,n)}\right)}_{\text{par}} = 1$ (absurdo).

Como c é par, podemos considerar a entrada

$$\mathbf{x} = (x_1, \cdots, x_n) = (\underbrace{\underbrace{1, 0, 0, \cdots, 0}_{(r_0,n)\text{ coordenadas}}, \underbrace{-1, 0, 0, \cdots, 0}_{(r_0,n)\text{ coordenadas}}, \cdots, \underbrace{1, 0, 0, \cdots, 0}_{(r_0,n)\text{ coordenadas}}, \underbrace{-1, 0, 0, \cdots, 0}_{(r_0,n)\text{ coordenadas}}}_{c\text{ blocos de }(r_0,n)\text{ coordenadas}}).$$

Dar um salto de r_0 coordenadas significa dar um salto de $\frac{r_0}{(r_0,n)}$ blocos de (r_0, n) coordenadas. Dessa forma, como $\frac{r_0}{(r_0,n)}$ é ímpar, então $\mathcal{P}_n(r_0)\,\mathbf{x} = -c$. Nesse caso,

$$D\mathbf{x} = c(a^2 - 2b) + 2b(-c) = c(a^2 - 4b) = 0,$$

e portanto D não é positiva definida.

A volta é imediata do Teorema 4.8.

□

Em particular, se n é par, então não podemos escolher r_0 ímpar. De fato, o máximo divisor comum entre um número par e um número impar é ímpar. Então, pondo $n = 2^\alpha \prod_{i \in I} p_i^{\alpha_i}$, tem-se $(r_0, n) = \prod_{i \in J} p_i^{\beta_i}$, onde $J \subset I$. Então $\frac{n}{(r,n)} = 2^\alpha \prod_{i \in I} p_i^{\gamma_i} \in 2\mathbb{Z}$.

Em alguns casos, nunca é possível uma escolha de r_0, a saber, para qualquer potência de 2.

Proposição 4.15. *Seja $n \geq 2$. Então n é uma potência de 2 se, e somente se, $\nexists r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ tal que $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$.*

Demonstração. Se n não é uma potência de 2, então ponha $n = 2^\alpha \prod p_i^{\alpha_i}$, onde p_i são primos ímpares e $\alpha_i \in \mathbb{Z}_+^*$. Dessa forma, $n > 2^{\alpha+1}$, donde $2^\alpha < \frac{n}{2}$. Assim, se $r_0 = 2^\alpha$, então $\frac{n}{(r_0,n)} = \prod p_i^{\alpha_i} \notin 2\mathbb{Z}$.

Por outro lado se n é uma potência de 2, então, não importa qual r_0 escolhido, tem-se $\frac{n}{(r_0,n)} \in 2\mathbb{Z}$. □

Agora, assumindo que escolhemos r_0 apropriado, o que podemos dizer sobre $|S(\Lambda_{\mathbf{u}})|$? Se estamos interessados no problema do kissing number, então precisamos de condições para maximizar $|S(\Lambda_{\mathbf{u}})|$. Por exemplo, se $n = 6$ e assumirmos $\rho_2 = 0$, $\rho_1 = \rho_3$ e $\rho_4 = -\rho_6$, obtemos $\mathcal{P}_6(1)\,\mathbf{u} = \mathcal{P}_6(3)\,\mathbf{u} = 0$. No entanto, observa-se que

$$\#\{\mathbf{x} \in \mathbb{Z}^6 \backslash \{\mathbf{0}\} \colon Q_2^{(6)}\mathbf{x} = 1\} = 24.$$

Nesse caso, portanto, se $0 \neq a^2 = 4b$, temos $|S(\Lambda_{\mathbf{u}})| = 24 < \kappa(A_6) < \kappa(D_6)$.

Isso significa que talvez possamos refinar ainda mais a escolha de r_0, dentro desse propósito.

Lema 4.16. *Sejam $r, n \in \mathbb{N}$, com $r < n$. Então, $\forall m \in I_n$, existem $q \in \{0, 1, \cdots, \frac{n}{(r,n)} - 1\}$ e $s \in \{1, 2, \cdots, (r, n)\}$ tais que $\overline{m} = \overline{qr + s}$.*

Demonstração. Divida m por (r, n).

$$m = q_0(r, n) + s_0$$

com $0 \leq s_0 < (r, n)$.

- (CASO 1: $s_0 > 0$)

  Observe que

  $$\overline{m} = \overline{q_0(r,n) + s_0} = \underbrace{q_0\overline{(r,n)}}_{\in\left\langle\overline{(r,n)}\right\rangle} + \overline{s_0}. \tag{4.3}$$

  Mas

  $$\begin{aligned}\left\langle\overline{(r,n)}\right\rangle &= \left\{k\overline{(r,n)} \colon k = 1, 2, \cdots, \tfrac{n}{(r,n)}\right\} \\ &= \left\{k\overline{(r,n)} \colon k = 0, 1, 2, \cdots, \tfrac{n}{(r,n)} - 1\right\}.\end{aligned}$$

  Mostremos que $\left\langle\overline{(r,n)}\right\rangle = \left\{k\,\overline{r} \colon k = 0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$. De fato, defina

  $$\begin{aligned}\psi \colon \left\langle\overline{(r,n)}\right\rangle &\to \mathbb{Z}_n \\ k\,\overline{(r,n)} &\mapsto k\,\overline{r}\end{aligned}$$

  onde $k \in \left\{0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$.

  ψ dessa forma está bem definida. De fato, sejam $k_1, k_2 \in \left\{0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$ tais que $k_1\overline{(r,n)} = k_2\overline{(r,n)}$. Suponha sem perda de generalidade que $k_1 \geq k_2$. Assim,

$n \mid (k_1 - k_2)(r,n)$. Mas $0 \leq k_1 - k_2 \leq \frac{n}{(r,n)} - 1$, isto é, $0 \leq (k_1 - k_2)(r,n) \leq n - (r,n) < n$. Daí, $k_1 = k_2$, e portanto $k_1\overline{r} = k_2\overline{r}$.

Trata-se também de uma função injetiva. Para mostrar isso, suponha que $\exists k \in \left\{1, 2, \cdots, \frac{n}{(r,n)} - 1\right\}$ tal que $k\overline{(r,n)} \in \ker(\psi)$. Então $k\,\overline{r} = \overline{0}$, donde $n \mid kr$. Daí, $\frac{n}{(r,n)} \mid k\frac{r}{(r,n)}$. Como $\frac{n}{(r,n)}$ e $\frac{r}{(r,n)}$ são relativamente primos, então $\frac{n}{(r,n)} \mid k$, e portanto $\frac{n}{(r,n)} \leq k < \frac{n}{(r,n)}$ (absurdo). Portanto, $\ker(\psi) = \{0\}$.

Observe além disso que $\left\{k\,\overline{r} \colon k = 0, 1, \cdots, \frac{n}{(r,n)} - 1\right\} \subset \left\langle \overline{(r,n)} \right\rangle$. De fato, como $(r,n) \mid r$, então $\exists c \in \mathbb{Z}$ tal que $r = c(r,n)$. Como $(r,n) \leq r < n$, então $1 \leq c \leq \frac{n}{(r,n)} - 1$. Assim, dado $k\overline{r} \in \left\{k\,\overline{r} \colon k = 0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$, arbitrário, tem-se $k\overline{r} = k\,\underbrace{c\overline{(r,n)}}_{\in \left\langle \overline{(r,n)} \right\rangle} \in \left\langle \overline{(r,n)} \right\rangle$.

Como ψ é injetiva, os dois conjuntos possuem a mesma cardinalidade, e portanto da inclusão obtemos $\left\langle \overline{(r,n)} \right\rangle = \left\{k\,\overline{r} \colon k = 0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$.

Voltando em (4.3), seja $q_1 \in \left\{0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$ tal que $q_0\overline{(r,n)} = q_1\,\overline{r}$. Temos

$$\overline{m} = q_1\,\overline{r} + \overline{s_0} = \overline{q_1 r + s_0}.$$

Basta então tomar $q = q_1$ e $s = s_0$.

- (CASO 2: $s_0 = 0$)

  Nesse caso, $m = q_0(r,n) = (q_0 - 1)(r,n) + (r,n)$, e então

  $$\overline{m} = \underbrace{(q_0 - 1)\overline{(r,n)}}_{\in \left\langle \overline{(r,n)} \right\rangle} + \overline{(r,n)}.$$

  Seja $q_1 \in \left\{0, 1, \cdots, \frac{n}{(r,n)} - 1\right\}$ tal que $(q_0 - 1)\overline{(r,n)} = q_1\,\overline{r}$. Então

  $$\overline{m} = q_1\,\overline{r} + \overline{(r,n)} = \overline{q_1 r + (r,n)}.$$

  Basta tomar então $q = q_1$ e $s = (r,n)$.

□

Exemplo 4.17. Para $n = 14$ e $r = 4$, tem-se $\overline{12} = \overline{6 \cdot 4 + 2}$.

Teorema 4.18. *Seja $n \geq 3$. Se $r \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$, então $Q_r^{(n)} \sim Q_{(r,n)}^{(n)}$.*

Demonstração. Observe que $\forall i \in \mathbb{N}$, $\exists! j \in I_n$ tal que $\overline{i} = \overline{j}$. Recordamos a definição

$$\begin{aligned} \varphi \colon \mathbb{N} &\to I_n \,. \\ i &\mapsto j \end{aligned}$$

Dessa forma, $\overline{\varphi(i)} = \overline{i}$. Usaremos esse fato ao longo da demonstração.

Seja $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$ arbitrário e ponha $k = (r, n)$ e

$$\mathbf{y} = \Big(\underbrace{x_1, x_2, \cdots, x_k}_{k \text{ coordenadas}}, \underbrace{x_{\varphi(1+r)}, x_{\varphi(2+r)}, \cdots, x_{\varphi(k+r)}}_{k \text{ coordenadas}}, \cdots, \underbrace{x_{\varphi(1+(\frac{n}{k}-1)r)}, \cdots, x_{\varphi(k+(\frac{n}{k}-1)r)}}_{k \text{ coordenadas}} \Big).$$

Os índices em $\mathbf{y}$ percorrem todo o conjunto $\{1, 2, \cdots, n\}$, isto é,

$$\left\{ \overline{1}, \overline{2}, \cdots, \overline{k}, \overline{1+r}, \overline{2+r}, \cdots, \overline{k+r}, \cdots, \overline{1+\Big(\tfrac{n}{k}-1\Big)r}, \cdots, \overline{k+(\tfrac{n}{k}-1)r} \right\} = \mathbb{Z}_n.$$

De fato, temos

$$\bigcup_{q=0}^{\frac{n}{k}-1} \Big(\{\overline{qr}\} + \left\{ \overline{1}, \cdots, \overline{k} \right\} \Big) = \mathbb{Z}_n, \tag{4.4}$$

pois a primeira inclusão é trivial, enquanto a segunda segue do Lema 4.3.

Afirmação: $Q_k^{(n)}\mathbf{y} = Q_r^{(n)}\mathbf{x}$.

Com efeito, temos

$$\begin{aligned} Q_k^{(n)}\mathbf{y} = \sum_{i=1}^{n} x_i^2 &+ x_1 x_{\varphi(1+r)} + \cdots + x_k x_{\varphi(k+r)} \\ &+ x_{\varphi(1+r)} x_{\varphi(1+2r)} + \cdots + x_{\varphi(k+r)} x_{\varphi(k+2r)} \\ &+ \cdots + \\ &+ x_{\varphi(1+(\frac{n}{k}-2)r)} x_{\varphi(1+(\frac{n}{k}-1)r)} + \cdots + x_{\varphi(k+(\frac{n}{k}-2)r)} x_{\varphi(k+(\frac{n}{k}-1)r)} \\ &+ x_1 x_{\varphi(1+(\frac{n}{k}-1)r)} + \cdots + x_k x_{\varphi(k+(\frac{n}{k}-1)r)}, \end{aligned}$$

isto é,

$$Q_k^{(n)}\mathbf{y} = \sum_{i=1}^{n} x_i^2 + \sum_{j=1}^{k} \left(\sum_{\substack{\alpha,\beta \in \{0,1,\cdots,\frac{n}{k}-1\} \\ \alpha<\beta \\ \beta-\alpha \in \{1,\frac{n}{k}-1\}}} x_{\varphi(j+\alpha r)} x_{\varphi(j+\beta r)} \right).$$

Então $Q_k^{(n)}\mathbf{y} = Q_r^{(n)}\mathbf{x}$ se, e somente se,

$$\sum_{j=1}^{k} \left(\sum_{\substack{\alpha,\beta \in \{0,1,\cdots,\frac{n}{k}-1\} \\ \alpha<\beta \\ \beta-\alpha \in \{1,\frac{n}{k}-1\}}} x_{\varphi(j+\alpha r)} x_{\varphi(j+\beta r)} \right) = \mathcal{P}_n(r)\,\mathbf{x}.$$

Nenhum par de índices na equação acima se repete. De fato, mostremos que o índice da $k-$ésima coordenada seguinte e o índice da k-ésima coordenada anterior de uma coordenada fixa arbitrária de $\mathbf{y}$ não coincidem. Ora, se a coordenada fixa em questão está no primeiro bloco de k coordenadas, isto é, se ela é da forma x_j com $1 \leq j \leq k$, então queremos mostrar que $\varphi(j+r) \neq \varphi(j+(\frac{n}{k}-1)r)$. Se tivéssemos a igualdade, então $\overline{r(\frac{n}{k}-2)} = \overline{0}$, isto é, $n \mid r(\frac{n}{k}-2)$. Daí, $\frac{n}{k} \mid \frac{r}{k}(\frac{n}{k}-2)$, e portanto, $\frac{n}{k} \mid \frac{n}{k}-2$, o que é absurdo, já que $k \leq r < \frac{n}{2}$ e portanto $\frac{n}{k}-2 > 0$. Agora, se a coordenada fixada de $\mathbf{y}$ for do último bloco, isto é, da forma $x_{\varphi(j+(\frac{n}{k}-1)r)}$ com $1 \leq j \leq k$, então queremos $j \neq \varphi(j+(\frac{n}{k}-2)r)$. Se tivéssemos igualdade, então concluiríamos novamente que $\frac{n}{k} \mid \frac{n}{k}-2$ (absurdo). Por último, se a coordenada fixada não pertence ao primeiro nem último bloco, então a escreva como $x_{\varphi(j+\alpha r)}$, para algum $\alpha \in \{0,1,\cdots,\frac{n}{k}-1\}$ e algum $j \in \{1,2,\cdots,k\}$. Nesse caso, queremos $\varphi(j+(\alpha-1)r) \neq \varphi(j+(\alpha+1)r)$. Se tivéssemos igualdade, então $\overline{j+(\alpha-1)r} = \overline{j+(\alpha+1)r}$, donde $n \mid 2r$. Mas $0 < 2r < n$, e portanto chegamos a um absurdo. Portanto, ao se multiplicar uma coordenada com a próxima $k-$ésima e a k-ésima anterior, obtém-se dois pares de índices distintos. Então nenhum par obtido dessa forma se repete. Ponha então

$$\mathcal{A}_j = \left\{(\varphi(j+\alpha r), \varphi(j+\beta r)) \in I_n \times I_n \colon \alpha, \beta \in \left\{0,1,\cdots,\tfrac{n}{k}-1\right\},\ \alpha < \beta,\ \beta-\alpha \in \{1,\tfrac{n}{k}-1\}\right\},$$

$$\mathcal{A} = \bigcup_{j=1}^{k} \mathcal{A}_j$$

e

$$\mathcal{B} = \{(i,j) \in I_n \times I_n \colon i < j,\ j-i \in \{r, n-r\}\},$$

temos que $Q_k^{(n)}\mathbf{y} = Q_r^{(n)}\mathbf{x}$ se, e somente se,

$$\sum_{(s,t)\in\mathcal{A}} x_s x_t = \sum_{(i,j)\in\mathcal{B}} x_i x_j.$$

Mostremos que $\mathcal{A} = \mathcal{B}$.

Seja $(\varphi(j+\alpha r), \varphi(j+\beta r)) \in \mathcal{A}$.

Suponha primeiramente que $\varphi(j+\beta r) > \varphi(j+\alpha r)$, e sejam $s,t \in I_n$ tais que $\overline{j+\alpha r} = \overline{s}$ e $\overline{j+\beta r} = \overline{t}$. Dessa forma, $\varphi(j+\alpha r) = s$ e $\varphi(j+\beta r) = t$, isto é, $(s,t) \in \mathcal{A}$. Se $\beta-\alpha = 1$, então $\overline{t-s} = \overline{t}-\overline{s} = \overline{r}\,\overline{\beta-\alpha} = \overline{r}$, donde $t-s = r$, uma vez que $r, t-s \in \{1,\cdots,n-1\}$. Logo, $(s,t) \in \mathcal{B}$. Agora, se $\beta-\alpha = \frac{n}{k}-1$, então $\overline{t-s} = \overline{t}-\overline{s} = \overline{r}\,\overline{\beta-\alpha} = \overline{r}\,\overline{\frac{n}{k}-1} = \overline{\frac{rn}{k}-r} = \overline{-r} = \overline{n-r}$, donde $t-s = n-r$, uma vez que $t-s, n-r \in \{1,\cdots,n-1\}$.

Se por outro lado $\varphi(j+\beta r) < \varphi(j+\alpha r)$, pelo mesmo processo se conclui que $s-t \in \{r, n-r\}$.

Portanto, $\mathcal{A} \subset \mathcal{B}$. Como os dois conjuntos possuem ambos n elementos, então $\mathcal{A} = \mathcal{B}$.

Assim, $\sum_{(s,t)\in\mathcal{A}} x_s x_t = \sum_{(i,j)\in\mathcal{B}} x_i x_j$, e portanto,

$$Q_k^{(n)}\mathbf{y} = Q_r^{(n)}\mathbf{x}.$$

Observe que

$$\mathbf{y}^T = \sigma \mathbf{x}^T,$$

onde

$$\sigma = \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_k \\ \mathbf{e}_{\varphi(1+r)} \\ \mathbf{e}_{\varphi(2+r)} \\ \vdots \\ \mathbf{e}_{\varphi(k+r)} \\ \vdots \\ \mathbf{e}_{\varphi(1+(\frac{n}{k}-1)r)} \\ \vdots \\ \mathbf{e}_{\varphi(k+(\frac{n}{k}-1)r)} \end{pmatrix}.$$

Pelo observado em (4.4), temos que da matriz σ se obtém a matriz identidade Id_n trocando as linhas (ou as colunas) um número suficiente de vezes, o que significa que σ é uma matriz de permutação e $|\det \sigma| = \det \mathrm{Id}_n = 1 \neq 0$.

Portanto, $Q_k^{(n)} \sim Q_r^{(n)}$, o que conclui a demonstração. □

A matriz σ tem posto n, e portanto a transformação linear associada a σ é injetiva. Uma consequência imediata disso é que

$$\#\{\mathbf{x} \in \mathbb{Z} \colon Q_{r_0}^{(n)}\mathbf{x} = 1\} = \#\{\mathbf{x} \in \mathbb{Z} \colon Q_{(r_0,n)}^{(n)}\mathbf{x} = 1\}.$$

Ora, de fato, cada solução $\mathbf{x}$ de $Q_{r_0}^{(n)}\mathbf{x} = 1$ determina unicamente uma solução de $Q_{(r_0,n)}^{(n)}\mathbf{x} = 1$, uma vez que $\sigma \in GL_n(\mathbb{Z})$. Então $\#\{\mathbf{x} \in \mathbb{Z} \colon Q_{r_0}^{(n)}\mathbf{x} = 1\} \leq \#\{\mathbf{x} \in \mathbb{Z} \colon Q_{(r_0,n)}^{(n)}\mathbf{x} = 1\}$. Vale a outra desigualdade, pelo mesmo argumento, bastando considerar σ^{-1}.

Consequentemente, sabemos mais sobre a escolha de r_0, como queríamos. Se n é primo ímpar, então não importa qual $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ escolhamos, o número de soluções para a forma $Q_{r_0}^{(n)}\mathbf{x} = 1$ é o mesmo, e $\frac{n}{(r_0,n)} = n \notin 2\mathbb{Z}$.

Se n não for primo, não temos essa garantia, e a escolha de r_0 volta a ser delicada. Por exemplo, analisando apenas as entradas $\mathbf{x} = (x_1, \cdots, x_n)$ onde $|x_i| \leq 1$, mostra-se facilmente utilizando um software que

$$\#\{\mathbf{x} \in \mathbb{Z}^9 \colon Q_1^{(9)}\mathbf{x} = 1\} \geq 144 = \kappa(D_9),$$

mas

$$\#\{\mathbf{x} \in \mathbb{Z}^9 \colon Q_3^{(9)}\mathbf{x} = 1\} \geq 36.$$

Parece ser mais vantajoso sempre escolher r_0 tal que $(n, r_0) = 1$, por esse motivo.

Observe que, se n é par, então $(r_0, n) = 1$ não possui solução par $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$, ao passo que n par com r_0 ímpar sempre implica em $a^2 > 4b$, pois caso contrário, $\det G_{\mathbf{u}} = 0$.

Teorema 4.19. *Dado $n \geq 3$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ tais que $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ tal que $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$. Então*

$$0 \neq a^2 = 4b \implies |S(\Lambda_{\mathbf{u}})| \geq 2n\left(\frac{n}{(r_0, n)} - 1\right).$$

Demonstração. Ponha $k = (r_0, n)$. Pelos teoremas 4.10 e 4.18,

$$|S(\Lambda_{\mathbf{u}})| = \#\{\mathbf{x} \in \mathbb{Z}^n \colon Q_{r_0}^{(n)}\mathbf{x} = 1\} = \#\{\mathbf{x} \in \mathbb{Z}^n \colon Q_k^{(n)}\mathbf{x} = 1\}.$$

Defina o conjunto

$$\mathcal{S}_0 = \{(1, 0, 0, \cdots, 0), (\underbrace{1, 0, \cdots, 0}_{k \text{ coordenadas}}, -1, 0, 0, \cdots, 0), (\underbrace{1, 0, \cdots, 0}_{k \text{ coordenadas}}, \underbrace{-1, 0, \cdots, 0}_{k \text{ coordenadas}}, 1, 0, \cdots, 0), \cdots\}.$$

Observe que, em um vetor de n coordenadas, cabem $\frac{n}{k}$ blocos de k coordenadas. Logo, é um número ímpar de blocos, uma vez que $\frac{n}{k} \notin 2\mathbb{Z}$. Defina então

$$\mathcal{S} = \mathcal{S}_0 \backslash \{\underbrace{(\underbrace{1, 0, \cdots, 0}_{k \text{ coordenadas}}, \underbrace{-1, 0, \cdots, 0}_{k \text{ coordenadas}} \cdots, \underbrace{1, 0, \cdots, 0}_{k \text{ coordenadas}})}_{\frac{n}{k} \text{ blocos de } k \text{ coordenadas}}\}.$$

Dessa forma, $\mathcal{S}$ possui $\frac{n}{k} - 1$ vetores diferentes, e

$$\mathcal{S} \subset \{\mathbf{x} \in \mathbb{Z}^n \colon Q_k^{(n)}\mathbf{x} = 1\}.$$

Além disso, como o operador rot preserva a norma euclidiana, então para cada vetor $\mathbf{v} \in \mathcal{S}$ tem-se

$$\{\pm \mathrm{rot}^i(\mathbf{v}) \colon i \in \{0, 1, \cdots, n-1\}\} \subset \{\mathbf{x} \in \mathbb{Z}^n \colon Q_k^{(n)}\mathbf{x} = 1\}.$$

Então

$$\bigcup_{\mathbf{v} \in \mathcal{S}} \{\pm \mathrm{rot}^i(\mathbf{v}) \colon i \in \{0, 1, \cdots, n-1\}\} \subset \{\mathbf{x} \in \mathbb{Z}^n \colon Q_k^{(n)}\mathbf{x} = 1\}.$$

Como cada rotação gera um vetor diferente, a para cada rotação há dois vetores (opostos) associados, tem-se $\#\{\pm \mathrm{rot}^i(\mathbf{v}) \colon i \in \{0, 1, \cdots, n-1\}\} = 2n$. Como

$$\mathbf{v_1} \neq \mathbf{v_2} \implies \{\pm \mathrm{rot}^i(\mathbf{v_1}) \colon i \in \{0, 1, \cdots, n-1\}\} \cap \{\pm \mathrm{rot}^i(\mathbf{v_2}) \colon i \in \{0, 1, \cdots, n-1\}\} = \varnothing,$$

para quaisquer $\mathbf{v_1}, \mathbf{v_2} \in \mathcal{S}$, e como $\mathcal{S}$ possui $\frac{n}{k} - 1$ elementos, então

$$2n(\tfrac{n}{k} - 1) \leq |S(\Lambda_{\mathbf{u}})|.$$

□

A cota inferior no Teorema 4.19 é maximizada ao minimizar (r_0, n). Dessa forma, para n ímpar toma-se $r_0 = 1$, enquanto que para n par, como r_0 não pode ser ímpar, toma-se $r_0 = 2^\alpha$, onde α é a potência de 2 na decomposição prima de n. Apresentamos na Figura 4.3 melhores cotas inferiores para cada n.

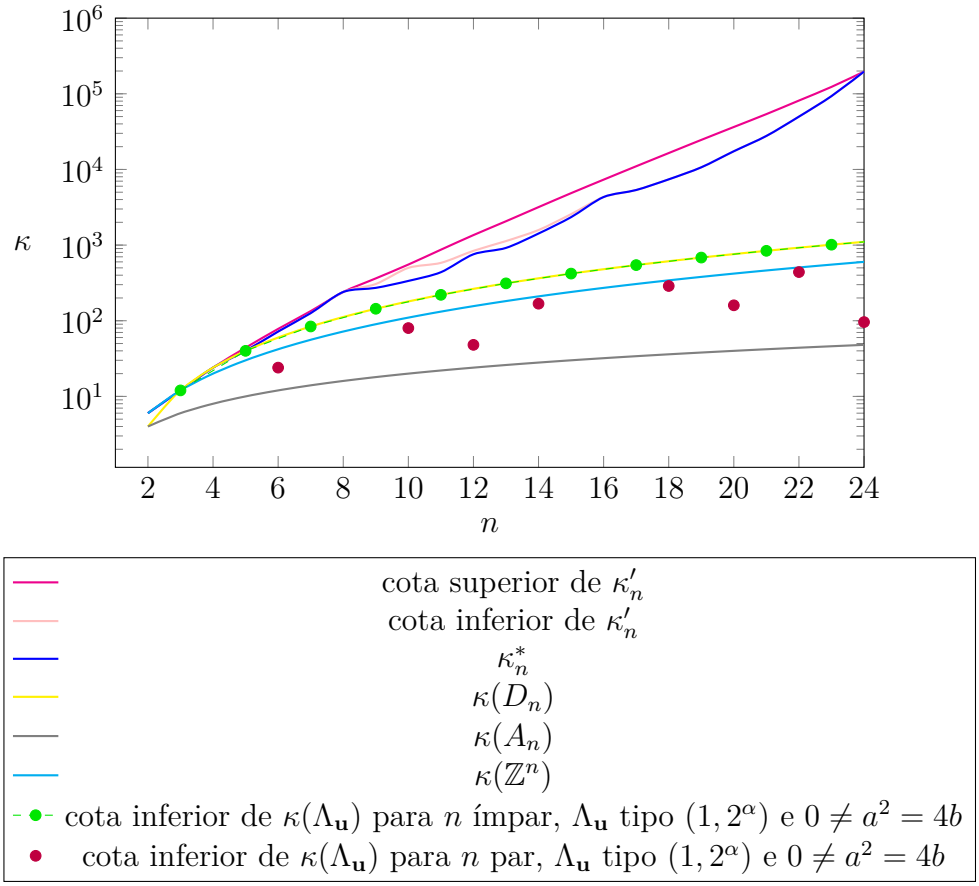

Figura 4.3: Cota inferior para o kissing number de reticulados circulantes obtidos do Teorema 4.19 se $r_0 = 2^\alpha$. Fonte: Elaborado pelo autor.

Observe que para n ímpar, obtemos kissing numbers tão bons quanto os de D_n. Além disso, ao contrário do que o gráfico sugere, a cota inferior do kissing number de $\Lambda_\mathbf{u}$, quando $n \in 2\mathbb{Z}\backslash 4\mathbb{Z}$, não se aproxima do kissing number de A_n, uma vez que $\kappa(A_n) - 2n(\frac{n}{2} - 1) = 3n$. A ilusão ocorre pois o gráfico tem seu eixo vertical na escala logarítmica.

Exemplo 4.20. Dado $n \geq 3$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Podemos desenvolver códigos em softwares que encontram soluções numéricas para o sistema

$$\begin{cases} \mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = 0 \\ 0 \neq a^2 = 4b \end{cases},$$

onde $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ com $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$.

Por exemplo, para $n = 9$ e $r_0 = 1$, é solução para o sistema:

$$\begin{aligned}
\rho_1 &= 4.472360011072218 \\
\rho_2 &= -29.666398854489902 \\
\rho_3 &= 9.939990273411874 \\
\rho_4 &= 133.7818721947125 \\
\rho_5 &= 132.97835421952914 \\
\rho_6 &= -1.5431563254234053 \\
\rho_7 &= 20.775902895645668 \\
\rho_8 &= 5.027880683129741 \\
\rho_9 &= -3.54770969331386
\end{aligned}$$

Sabemos de antemão pelo Teorema 4.8 que $\det G_{\mathbf{u}} \neq 0$, pois $0 \neq a^2 = 4b$ e $\frac{n}{(r_0,n)} = 9 \notin 2\mathbb{Z}$. E de fato,

$$\det G_{\mathbf{u}} = 3.20647 \cdot 10^{19}.$$

Além disso, pelo Teorema 4.10, $|\Lambda_{\mathbf{u}}| = \frac{a^2}{2} = \frac{(\rho_1+\rho_2+\cdots+\rho_9)^2}{2} = 37051.6$, e portanto

$$\begin{aligned}
\delta(\Lambda_{\mathbf{u}}) &= \frac{\left(\frac{\sqrt{|\Lambda_{\mathbf{u}}|}}{2}\right)^9}{|\det G_{\mathbf{u}}|} \\
&= 0.0220971 \\
&= \delta(D_9).
\end{aligned}$$

Agora, pelo Teorema 4.19, $\kappa(\Lambda_{\mathbf{u}}) \geq 144$. Utilizando um software, podemos verificar que de fato $\kappa(\Lambda_{\mathbf{u}}) = \#\{\mathbf{x} \in \mathbb{Z}^n \colon Q_1^{(9)}\mathbf{x} = 1\} = 144$.

Observação 1. Nas condições do exemplo anterior, não encontramos soluções reais para o sistema quando $r_0 = 3$. Porém, isso não significa que toda solução de $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \mathcal{P}_n(4)\,\mathbf{u} = 0$ implica em $b < 0$. Por exemplo, para

$$\begin{aligned}
\rho_1 &= -2.26102 \\
\rho_2 &= -6.84173 \\
\rho_3 &= -1.50927 \\
\rho_4 &= 7.67675 \\
\rho_5 &= -6.23603 \\
\rho_6 &= -0.760659 \\
\rho_7 &= -3.02887
\end{aligned}$$

$$\rho_8 = -7.40918$$
$$\rho_9 = -0.431692$$

obtém-se $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \mathcal{P}_n(4)\,\mathbf{u} = 0$ e $b = 107.928 > 0$. Além disso, $\det G_{\mathbf{u}} = -1.16334 \cdot 10^{10} \neq 0$ e $a^2 < 4b$. Isso mostra também que a condição $\frac{n}{(r_0,n)} \in 2\mathbb{Z}$, $0 \neq a^2 \geq 4b$, $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0-1)\,\mathbf{u} = \mathcal{P}_n(r_0+1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$, não é necessária para que $\det G_{\mathbf{u}} \neq 0$, apesar de suficiente.

A dificuldade do método que apresentamos até aqui é encontrar soluções não-nulas para o sistema

$$\begin{cases} \mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0-1)\,\mathbf{u} = \mathcal{P}_n(r_0+1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0 \\ a^2 = 4b \end{cases},$$

onde $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ com $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$.

Trata-se de um problema de programação. Quanto maior n, maior o número de equações a serem anuladas, o que dificulta o processamento. Além disso, a otimização de sistemas não-lineares que envolvem igualdades não é um problema fácil de se resolver. Nesse sentido, em dimensões altas é certamente mais conveniente resolver

$$(a^2 - 4b)^2 + \sum_{\substack{r=1 \\ r \neq r_0}}^{\lfloor \frac{n}{2} \rfloor} (\mathcal{P}_n(r)\,\mathbf{u})^2 < \epsilon,$$

para $\epsilon > 0$ suficientemente pequeno. A questão é se as soluções para esse sistema adaptado respeitam as propriedades discutidas até aqui.

Já temos informações a respeito do mínimo dos reticulados circulantes tipo $(1, r_0)$ tais que $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$ e $0 \neq a^2 = 4b$. Para o cálculo da densidade de centro, só resta uma expressão razoável para o determinante.

Teorema 4.21. *Dado $n \geq 3$, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(r_0-1)\,\mathbf{u} = \mathcal{P}_n(r_0+1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor \frac{n}{2} \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, \cdots, \lfloor \frac{n-1}{2} \rfloor\}$ tal que $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$, e se $a^2 = 4b$, então*

$$\det G_{\mathbf{u}} = \pm \frac{a^n}{2^{n-(r_0,n)}}$$

Demonstração. Pelo Teorema 4.7, como $a^2 = 4b$, tem-se

$$\begin{aligned} \det G_{\mathbf{u}} &= -a \prod_{j=1}^{\frac{n-1}{2}} \left(a^2 - 2b + b\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right) \\ &= -a b^{\frac{n-1}{2}} \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j} + 2) \end{aligned}$$

$$= -\frac{a^n}{2^{n-1}} \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j} + 2).$$

Como $(2, n) = 1$, então ζ_n^2 é uma n-ésima raiz primitiva da unidade, bem como ζ_n. Então

$$\begin{aligned}
\prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j} + 2) &= \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{2r_0 j} + \zeta_n^{-2r_0 j} + 2) \\
&= \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j})^2 \\
&= \left[\prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \right]^2 \\
&= \prod_{j=1}^{n-1} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \\
&= (\underbrace{\zeta_n \zeta_n^2 \cdots \zeta_n^{n-1}}_{=1})^{r_0} \prod_{j=1}^{n-1} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \\
&= \prod_{j=1}^{n-1} \zeta_n^{r_0 j} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \\
&= \prod_{j=1}^{n-1} (1 + \zeta_n^{2r_0 j}) \\
&= \prod_{j=1}^{n-1} (1 + \zeta_n^{r_0 j}).
\end{aligned}$$

Agora, note que $\zeta_n^{r_0 j} = 1 \iff n \mid r_0 j \iff \frac{n}{(r_0,n)} \mid \frac{r_0}{(r_0,n)} j \iff \frac{n}{(r_0,n)} \mid j \iff j \in \left\{ \frac{n}{(r_0,n)}, \frac{2n}{(r_0,n)}, \cdots, \frac{((r_0,n)-1)n}{(r_0,n)} \right\}$. Logo,

$$\prod_{j=1}^{n-1} (1 + \zeta_n^{r_0 j}) = 2^{(r_0,n)-1} \left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j}) \right).$$

Além disso, tem-se

$$\left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{r_0 j}) \right) \left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j}) \right) = \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{2r_0 j}) = \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{r_0 j}).$$

Na última igualdade utilizamos o fato de que $\{\zeta_n^{2r_0j} : \zeta_n^{r_0j} \neq 1,\ 1 \leq j \leq n-1\} = \{\zeta_n^{r_0j} : \zeta_n^{r_0j} \neq 1,\ 1 \leq j \leq n-1\}$. E de fato, seja $\zeta_n^{2r_0j}$ um elemento do primeiro conjunto. Então $n \nmid 2j$ pois, caso contrário, teríamos $n \mid j$ e portanto $\zeta_n^{r_0j} = 1$, o que não ocorre. Seja então $l \in \{1, \cdots, n-1\}$ tal que $\overline{2j} = \overline{l}$. Então $\zeta_n^{2r_0j} = \zeta_n^{r_0(2j)} = \zeta_n^{r_0l}$, e portanto vale a primeira inclusão. Para a segunda inclusão, basta observar que $\zeta_n^{r_0j} = \zeta_n^{2r_0l}$, onde $l = \frac{j}{2}$ se j é par, e $l = \frac{n+j}{2}$ se j é ímpar. É lícito tomar l dessa forma. De fato, em primeiro lugar, $\frac{n+j}{2} \leq n-1$. Ora, se tivéssemos $\frac{n+j}{2} \geq n$, então $j \geq n$ (absurdo). Em segundo lugar, $\zeta_n^{\frac{n+j}{2}r_0} \neq 1$, já que, caso contrário, teríamos $n \mid \frac{n+j}{2}r_0$, e então $\frac{n}{(n,r_0)} \mid \frac{n+j}{2}$. Daí, $\exists q \in \mathbb{Z}$ tal que $j = \frac{n(2q-(r_0,n))}{(r_0,n)}$. Logo, $\frac{n}{(r_0,n)} \mid j$, o que é absurdo pois $\zeta_n^{r_0j} \neq 1$. Verifica-se que $l = \frac{n}{2}$ também é apropriado (quando j é par), sem dificuldade.

Assim,

$$\prod_{\substack{1 \leq j \leq n-1 \\ \zeta_n^{r_0j} \neq 1}} (1 + \zeta_n^{r_0j}) = 1,$$

e portanto,

$$\det G_{\mathbf{u}} = -\frac{a^n}{2^{n-1}} 2^{(r_0,n)-1} = -\frac{a^n}{2^{n-(r_0,n)}}.$$

Suponha agora n par. Como por hipótese $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$, então r_0 é par. Novamente, pelo Teorema 4.7 e como $a^2 = 4b$,

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + b\left(\zeta_n^{r_0j} + \zeta_n^{-r_0j}\right)\right) \\
&= \pm a^2 b^{\frac{n-2}{2}} \prod_{j=1}^{\frac{n-2}{2}} (\zeta_n^{r_0j} + \zeta_n^{-r_0j} + 2) \\
&= \pm \frac{a^n}{2^{n-2}} \prod_{j=1}^{\frac{n-2}{2}} (\zeta_n^{r_0j} + \zeta_n^{-r_0j} + 2).
\end{aligned}$$

Ponha $k = (r_0, n)$. Dessa forma, $\zeta_n^{r_0} = \zeta_{n/k}^{r_0/k}$. Além disso, como $\frac{n}{k} \notin 2\mathbb{Z}$, então $(\frac{n}{k}, 2) = 1$. Assim,

$$\begin{aligned}
\prod_{j=1}^{\frac{n-2}{2}} (\zeta_n^{r_0j} + \zeta_n^{-r_0j} + 2) &= \prod_{j=1}^{\frac{n-2}{2}} \left(\zeta_{n/k}^{\frac{r_0j}{k}} + \zeta_{n/k}^{-\frac{r_0j}{k}} + 2\right) \\
&= \prod_{j=1}^{\frac{n-2}{2}} \left(\zeta_{n/k}^{\frac{2r_0j}{k}} + \zeta_{n/k}^{-\frac{2r_0j}{k}} + 2\right) \\
&= \prod_{j=1}^{\frac{n-2}{2}} \left(\zeta_{n/k}^{\frac{r_0j}{k}} + \zeta_{n/k}^{-\frac{r_0j}{k}}\right)^2
\end{aligned}$$

$$
\begin{aligned}
&= \prod_{j=1}^{\frac{n-2}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j})^2 \\
&= \left[\prod_{j=1}^{\frac{n-2}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \right]^2 \\
&= \frac{1}{\zeta_n^{\frac{r_0 n}{2}} + \zeta_n^{-\frac{r_0 n}{2}}} \prod_{j=1}^{n-1} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \\
&= \frac{1}{2} \prod_{j=1}^{n-1} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \\
&= (\underbrace{\zeta_n \zeta_n^2 \cdots \zeta_n^{n-1}}_{=1})^{r_0} \frac{1}{2} \prod_{j=1}^{n-1} (\zeta_n^{j} + \zeta_n^{-j}) \\
&= \frac{1}{2} \prod_{j=1}^{n-1} \zeta_n^{r_0 j} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}) \\
&= \frac{1}{2} \prod_{j=1}^{n-1} (1 + \zeta_n^{2 r_0 j}) \\
&= \frac{1}{2} \prod_{j=1}^{n-1} \left(1 + \zeta_{n/k}^{\frac{2 r_0 j}{k}} \right) \\
&= \frac{1}{2} \prod_{j=1}^{n-1} \left(1 + \zeta_{n/k}^{\frac{r_0 j}{k}} \right) \\
&= \frac{1}{2} \prod_{j=1}^{n-1} (1 + \zeta_n^{r_0 j}).
\end{aligned}
$$

Mas vimos que $\prod_{j=1}^{n-1} (1 + \zeta_n^{r_0 j}) = 2^{(r_0,n)-1} \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j})$. Novamente,

$$
\begin{aligned}
\left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{r_0 j}) \right) \left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j}) \right) &= \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{2 r_0 j}) \\
&= \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} \left(1 - \zeta_{n/k}^{\frac{2 r_0 j}{k}} \right) \\
&= \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} \left(1 - \zeta_{n/k}^{\frac{r_0 j}{k}} \right)
\end{aligned}
$$

$$= \prod_{\substack{1\leq j\leq n-1\\ \zeta_n^{r_0 j}\neq 1}} (1-\zeta_n^{r_0 j}),$$

onde usamos o fato de que $\left\{\zeta_{n/k}^{\frac{2r_0 j}{k}} : \zeta_n^{r_0 j}\neq 1,\ 1\leq j\leq n-1\right\} = \left\{\zeta_{n/k}^{\frac{r_0 j}{k}} : \zeta_n^{r_0 j}\neq 1,\ 1\leq j\leq n-1\right\}$, o que pode ser mostrado completamente analogamente ao que foi feito anteriormente, por dupla inclusão, notando que $\frac{n}{k}\nmid 2j$ para todo $j\in\{1,2,\cdots,n-1\}$ com $\zeta_n^{r_0 j}\neq 1$, e que $\zeta_{n/k}^2$ é uma $\frac{n}{k}$-ésima raiz primitiva da unidade.

Logo,

$$\prod_{j=1}^{n-1}(1+\zeta_n^{r_0 j}) = 2^{(r_0,n)-1}$$

e portanto

$$\det G_{\mathbf{u}} = \pm\frac{a^n}{2^{n-2}}2^{(r_0,n)-2} = \pm\frac{a^n}{2^{n-(r_0,n)}}.$$

□

Corolário 6. Dado $n\geq 3$, sejam $\rho_1,\cdots,\rho_n\in\mathbb{R}$ e $\mathbf{u}=(\rho_1,\cdots,\rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u}=\cdots=\mathcal{P}_n(r_0-1)\,\mathbf{u}=\mathcal{P}_n(r_0+1)\,\mathbf{u}=\cdots=\mathcal{P}_n(\lfloor\frac{n}{2}\rfloor)\,\mathbf{u}=0$ para algum $r_0\in\{1,2,\cdots,\lfloor\frac{n-1}{2}\rfloor\}$ tal que $\frac{n}{(r_0,n)}\notin 2\mathbb{Z}$, e se $0\neq a^2=4b$, então

$$\delta(\Lambda_{\mathbf{u}}) = \frac{1}{2^{(r_0,n)+\frac{n}{2}}}.$$

Demonstração. Por hipótese, vimos que $|\Lambda_{\mathbf{u}}| = \frac{a^2}{2}$ e $\det G_{\mathbf{u}} = \pm\frac{a^n}{2^{n-(r_0,n)}}$. Logo,

$$\begin{aligned}\delta(\Lambda_{\mathbf{u}}) &= \frac{\left(\frac{\sqrt{|\Lambda_{\mathbf{u}}|}}{2}\right)^n}{|\det G_{\mathbf{u}}|}\\ &= 2^{n-(r_0,n)}\frac{\left(\frac{|a|}{2\sqrt{2}}\right)^n}{|a|^n}\\ &= \frac{2^{n-(r_0,n)}}{2^{n+\frac{n}{2}}}\\ &= \frac{1}{2^{(r_0,n)+\frac{n}{2}}}\end{aligned}$$

□

Observe que, em particular, se $(r_0,n)=1$ (o que só é possível se n for ímpar), então $\delta(\Lambda_{\mathbf{u}})=\delta(D_n)$. Além disso, se n é par, então $\delta(\Lambda_{\mathbf{u}})<\delta(D_n)$. A melhor densidade de centro é obtida dessa forma quando $r=r_0$ minimiza $\min\left\{(r,n) : r\in\{1,2,\cdots,\lfloor\frac{n-1}{2}\rfloor\},\ \frac{n}{(r,n)}\notin 2\mathbb{Z}\right\}$, isto é, quando $r_0=1$ se n é ímpar e $r_0=2^\alpha$ se n é par, onde α é a potência de 2 na decomposição prima de n.

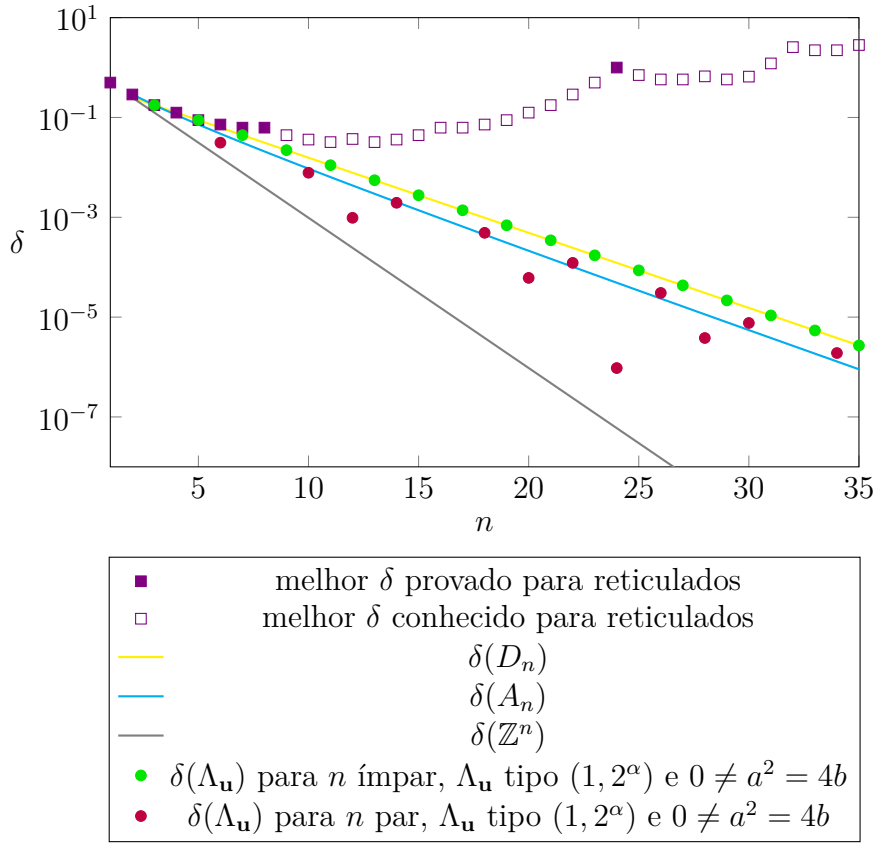

Figura 4.4: Densidade de centro de reticulados circulantes obtidos do Corolário 6 se $r_0 = 2^\alpha$. Fonte: Elaborado pelo autor.

Vale observar que, se $n \in 2\mathbb{Z}\backslash 4\mathbb{Z}$, então $r_0 = 2$ é a melhor escolha para maximizar $\delta(\Lambda_{\mathbf{u}})$ dentro de nossas hipóteses, e consequentemente

$$\delta(A_n) > \delta(\Lambda_{\mathbf{u}}) \iff \frac{1}{2^{\frac{n}{2}}(n+1)^{\frac{1}{2}}} > \frac{1}{2^{2+\frac{n}{2}}} \iff 4 > (n+1)^{\frac{1}{2}} \iff 15 > n.$$

Portanto, $\delta(\Lambda_{\mathbf{u}})$ passa a ser maior que $\delta(A_n)$ a partir de $n = 18$, nesse caso.

4.2.2 O caso $r_0 = \frac{n}{2}$

Do Corolário 5, se n é par e $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2} - 1)\,\mathbf{u} = 0$, então $\|x\|^2$ é da forma $(a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 4b\,\mathcal{P}_n(\frac{n}{2})\,\mathbf{x}$. Novamente, gostaríamos de uma condição para que $\det G_{\mathbf{u}} \neq 0$.

Teorema 4.22. *Dado $n \geq 2$ par, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2} - 1)\,\mathbf{u} = 0$, então $a^2 \geq 4b$. Além disso, se D é a forma quadrática em*

$\mathbb{Z}$ *definida por*

$$D\mathbf{x} = (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 4b\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x},$$

então são equivalentes:

(i) $\det G_{\mathbf{u}} \neq 0$*;*

(ii) D *é positiva definida;*

(iii) $0 \neq a^2 > 4b$*.*

Demonstração. Observe que $a^2-4b = a^2-2b-2b = \rho_1^2+\cdots+\rho_n^2-2\mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = \sum_{\substack{i,j\in I_n\\ i<j\\ j-i=\frac{n}{2}}}(\rho_i-\rho_j)^2 \geq 0.$

Portanto, $a^2 \geq 4b$. Agora,

- ((i) $\Longleftrightarrow$ (ii))

  Análogo à demonstração do Teorema 4.8.

- ((ii) $\Longleftrightarrow$ (iii))

  Pelo Teorema 4.7, como $\zeta_n^{\frac{n}{2}} = \zeta_n^{-\frac{n}{2}} = -1$, então

$$\det G_{\mathbf{u}} = \begin{cases} \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + b\left(\zeta_n^{\frac{n}{2}j} + \zeta_n^{-\frac{n}{2}j}\right)\right) & \text{se } \frac{n}{2} \text{ é par} \\ \pm a\sqrt{a^2-4b} \prod_{j=1}^{\frac{n-2}{2}} \left(a^2 - 2b + b\left(\zeta_n^{\frac{n}{2}j} + \zeta_n^{-\frac{n}{2}j}\right)\right) & \text{se } \frac{n}{2} \text{ é ímpar} \end{cases}$$

$$= \begin{cases} \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} (a^2 - 2b + 2b(-1)^j) & \text{se } n \in 4\mathbb{Z} \\ \pm a\sqrt{a^2-4b} \prod_{j=1}^{\frac{n-2}{2}} (a^2 - 2b + 2b(-1)^j) & \text{se } n \in 2\mathbb{Z}\backslash 4\mathbb{Z} \end{cases}.$$

  Como $a^2 \geq 4b$, então $\det G_{\mathbf{u}} \neq 0$ se, e somente se, $0 \neq a^2 > 4b$.

□

Buscamos novamente uma relação conveniente entre a^2 e b para maximizar $|S(\Lambda_{\mathbf{u}})|$ e $\delta(\Lambda_{\mathbf{u}})$. Recordando do Lema 4.2 que $\langle \mathbf{u}, \mathrm{rot}^{\frac{n}{2}}(\mathbf{u})\rangle = 2\mathcal{P}_n(\frac{n}{2})\,\mathbf{u}$, se quisermos seguir a mesma motivação geométrica da seção anterior, então queremos $a^2 - 2b = \|\mathbf{u}\|^2 = 2\langle \mathbf{u}, \mathrm{rot}^{\frac{n}{2}}(\mathbf{u})\rangle = 4\mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = 4b$, isto é, $a^2 = 6b$. Nesse caso, se $\mathbf{u}$ é mínimo, $\mathbf{u} - \mathrm{rot}^{\frac{n}{2}}(\mathbf{u})$ também o é, bem como qualquer rotação de $\mathbf{u}$. Vejamos um exemplo na prática.

Digamos que $\Lambda_{\mathbf{u}} \subset \mathbb{R}^2$, $\mathbf{u} \neq 0$ seja um vetor mínimo e $2\langle \mathbf{u}, \text{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle$. A condição $2\langle \mathbf{u}, \text{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle$ significa que $\text{rot}(\mathbf{u})$ está tão próximo da origem quando de $\mathbf{u}$. De fato, $\|\mathbf{u} - \text{rot}(\mathbf{u})\|^2 = \langle \mathbf{u} - \text{rot}(\mathbf{u}), \mathbf{u} - \text{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle + \langle \text{rot}(\mathbf{u}), \text{rot}(\mathbf{u})\rangle - 2\langle \mathbf{u}, \text{rot}(\mathbf{u})\rangle = 2\langle \mathbf{u}, \mathbf{u}\rangle - 2\langle \mathbf{u}, \text{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle = \|\mathbf{u}\|^2 = \|\text{rot}(\mathbf{u})\|^2$. Consequentemente, o vetor $\mathbf{u} - \text{rot}(\mathbf{u})$ também cumpre essa propriedade: $\|\mathbf{u} - (\mathbf{u} - \text{rot}(\mathbf{u}))\|^2 = \|\text{rot}(\mathbf{u})\|^2 = \|\mathbf{u} - \text{rot}(\mathbf{u})\|^2$. Dessa forma, os vetores $\text{rot}(\mathbf{u})$ e $\mathbf{u} - \text{rot}(\mathbf{u})$ pertencem à intersecção entre a circunferência centrada na origem com raio $\|\mathbf{u}\|$, e à reta perpendicular a $\mathbf{u}$ que passa por $\frac{1}{2}\mathbf{u}$.

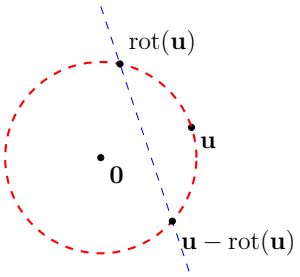

Figura 4.5: Construção de $\text{rot}(\mathbf{u})$. Fonte: Elaborado pelo autor.

Dessa forma, se $\mathbf{u}$ é mínimo, então $\text{rot}(\mathbf{u})$ e $\mathbf{u} - \text{rot}(\mathbf{u})$ também o são. Portanto, temos $\{\mathbf{u}, \text{rot}(\mathbf{u}), \mathbf{u} - \text{rot}(\mathbf{u}), -\mathbf{u}, -\text{rot}(\mathbf{u}), \text{rot}(\mathbf{u}) - \mathbf{u}\} \subset S(\Lambda_{\mathbf{u}})$. Sabemos que o kissing number de um reticulado em $\mathbb{R}^2$ é no máximo 6, e consequentemente

$$\{\mathbf{u}, \text{rot}(\mathbf{u}), \mathbf{u} - \text{rot}(\mathbf{u}), -\mathbf{u}, -\text{rot}(\mathbf{u}), \text{rot}(\mathbf{u}) - \mathbf{u}\} = S(\Lambda_{\mathbf{u}}).$$

Esses vetores são todos diferentes por construção, já que $\text{rot}(\mathbf{u})$ e $\mathbf{u} - \text{rot}(\mathbf{u})$ não podem ser opostos por pertencerem a uma mesma reta que não passa pela origem.

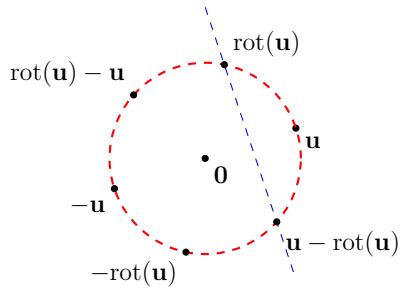

Figura 4.6: Construção de vetores mínimos se $\mathbf{u}$ é mínimo e $2\langle \mathbf{u}, \text{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle$. Fonte: Elaborado pelo autor.

Portanto, $|S(\Lambda_{\mathbf{u}})| = 6$. Pelo Teorema 2.15, construímos o reticulado hexagonal, desde que haja de fato solução não-nula para

$$2\langle \mathbf{u}, \text{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle \tag{4.5}$$

tal que $\mathbf{u}$ seja um vetor mínimo. Veremos que isso de fato é possível.

Definição 4.23. Sejam $n \geq 2$ e $r \in \{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$. Defina a forma quadrática $R_r^{(n)} : \mathbb{Z}^n \to \mathbb{Z}$ por

$$R_r^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 - \mathcal{P}_n(r)\,\mathbf{x}.$$

Teorema 4.24. *Dado $n \geq 2$ par, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ tais que $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2} - 1)\,\mathbf{u} = 0$. Então, se $0 \neq a^2 = -2b$ ou $0 \neq a^2 = 6b$, tem-se*

$$|\Lambda_{\mathbf{u}}| = \begin{cases} 2a^2 & \text{se } a^2 = -2b \\ \dfrac{2a^2}{3} & \text{se } a^2 = 6b \end{cases},$$

e

$$|S(\Lambda_{\mathbf{u}})| = \begin{cases} \#\left\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon R_{\frac{n}{2}}^{(n)}\mathbf{x} = 1\right\} & \text{se } a^2 = -2b \\ \#\left\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon Q_{\frac{n}{2}}^{(n)}\mathbf{x} = 1\right\} & \text{se } a^2 = 6b \end{cases}.$$

Demonstração. Se $0 \neq a^2 = -2b$, então $a^2 - 2b = -4b = 2a^2$ e, pelo Teorema 4.22, $\forall \mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$,

$$D\mathbf{x} = 2a^2\left(\sum_{i=1}^{n} x_i^2 - \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x}\right) \geq 0,$$

onde vale a igualdade se, e somente se, $\mathbf{x} = \mathbf{0}$, já que D é positiva definida. Daí, se $\mathbf{x} \neq 0$, como $a^2 > 0$, tem-se

$$R_{\frac{n}{2}}^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} > 0,$$

isto é,

$$R_{\frac{n}{2}}^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} \geq 1,$$

pois $x_1, \cdots, x_n \in \mathbb{Z}$.

Agora, observe que

$$\mathbf{x} = (x_1, \cdots, x_n) = (1, 0, \cdots, 0) \implies R_{\frac{n}{2}}^{(n)}\mathbf{x} = \sum_{i=1}^{n} x_i^2 - \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} = 1.$$

Portanto, $\{D\mathbf{x} \colon \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\}\}$ é limitado inferiormente por $2a^2$, ao mesmo tempo que $D(1, 0, \cdots, 0) = 2a^2$. Portanto,

$$|\Lambda_{\mathbf{u}}| := \min\{D\mathbf{x} \colon \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\}\} = 2a^2,$$

e

$$|S(\Lambda_{\mathbf{u}})| := \#D^{-1}(\{|\Lambda_{\mathbf{u}}|\})$$

$$
\begin{aligned}
&= \#D^{-1}(\{2a^2\}) \\
&= \#\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon D\mathbf{x} = 2a^2\} \\
&= \#\left\{\mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} \colon R_{\frac{n}{2}}^{(n)}\mathbf{x} = 1\right\}.
\end{aligned}
$$

Para $a^2 = 6b$, é análogo, com $Q_{\frac{n}{2}}^{(n)}$ ao invés de $R_{\frac{n}{2}}^{(n)}$. □

Aplicando o Teorema 4.24 para $n = 2$, não há sistema a ser resolvido, e portanto $0 \neq a^2 = 6b$ implica diretamente que $\|\mathbf{u}\|^2 = a^2 - 2b = \frac{2}{3}a^2 = |\Lambda_{\mathbf{u}}|$, isto é, que $\mathbf{u}$ é mínimo. Então, pelo que foi observado na Equação (4.5) construímos o reticulado hexagonal desde que haja uma solução real não-nula para $2\langle \mathbf{u}, \mathrm{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle$, ou equivalentemente, uma solução real para $0 \neq a^2 = 6b$. Note que, para a equivalência, usamos a Proposição 4.3: $6b \neq 0 \iff 6\mathcal{P}_2(1)\,\mathbf{u} \neq 0 \iff \langle \mathbf{u}, \mathrm{rot}(\mathbf{u})\rangle \neq 0 \iff \langle \mathbf{u}, \mathbf{u}\rangle \neq 0 \iff \mathbf{u} \neq \mathbf{0}$. Agora, $2\langle \mathbf{u}, \mathrm{rot}(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{u}\rangle$ pode ser reescrito como $4\rho_1\rho_2 = \rho_1^2 + \rho_2^2$. Felizmente, essa equação possui infinitas soluções reais não-nulas. De fato, para cada ρ_1 fixado, há duas soluções $\rho_2 = \rho_1(2 \pm \sqrt{3})$, representadas na Figura 4.7.

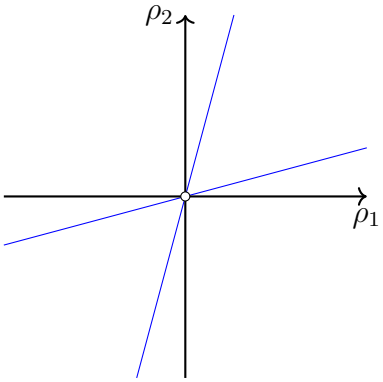

Figura 4.7: Soluções não-nulas para $4\rho_1\rho_2 = \rho_1^2 + \rho_2^2$. Fonte: Elaborado pelo autor.

Exemplo 4.25. Considere $\mathbf{u} = (1, 2 - \sqrt{3})$. Então $a^2 = (1 + 2 - \sqrt{3})^2 = 12 - 6\sqrt{3} = 6(2 - \sqrt{3}) = 6b$. Pelo Teorema 4.24, tem-se $|\Lambda_{\mathbf{u}}| = \frac{2}{3}a^2 = a^2 - 2b = 8 - 4\sqrt{3}$. Agora, observe que $\|\mathbf{u} - \mathrm{rot}(\mathbf{u})\|^2 = \|(-1 + \sqrt{3}, 1 - \sqrt{3})\|^2 = 8 - 4\sqrt{3}$. Assim, $\pm\{\mathbf{u}, \mathrm{rot}(\mathbf{u}), \mathbf{u} - \mathrm{rot}(\mathbf{u})\} = \pm\{(1, 2-\sqrt{3}), (2-\sqrt{3}, 1), (-1+\sqrt{3}, 1-\sqrt{3})\} \subset S(\Lambda_{\mathbf{u}})$. Do Teorema 2.15 tem-se $|S(\Lambda_{\mathbf{u}})| \leq 6$, e portanto

$$\pm\{(1, 2 - \sqrt{3}), (2 - \sqrt{3}, 1), (-1 + \sqrt{3}, 1 - \sqrt{3})\} = S(\Lambda_{\mathbf{u}})$$

e

$$|S(\Lambda_{\mathbf{u}})| = 6.$$

É claro que poderíamos calcular $|S(\Lambda_{\mathbf{u}})|$ através do próprio Teorema 4.24, verificando através de um software que

$$|S(\Lambda_{\mathbf{u}})| = \#\{\mathbf{x} \in \mathbb{Z}^2 \backslash \{\mathbf{0}\} \colon x_1^2 + x_2^2 + x_1x_2 = 1\} = 6.$$

Portanto, trata-se de um reticulado semelhante ao hexagonal, representado pela Figura 4.8.

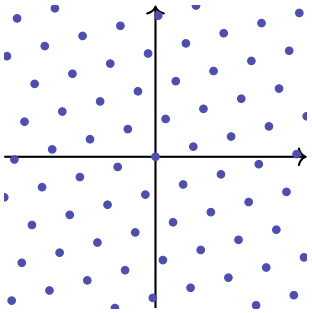

Figura 4.8: Reticulado $\Lambda_{(1,2-\sqrt{3})}$. Fonte: Elaborado pelo autor.

Na seção anterior, tínhamos a necessidade de que $b > 0$, pois trabalhamos sobre a hipótese $a^2 = 4b$. Agora, tendo em vista o Teorema 4.24, não temos mais esse obstáculo. A questão se torna, porém, se conseguimos novamente gerar reticulados com alta densidade de centro e kissing number. Isso depende, evidentemente, de $\det G_{\mathbf{u}}$ e da quantidade de soluções para $Q^{(n)}_{\frac{n}{2}}\mathbf{x} = 1$ e $R^{(n)}_{\frac{n}{2}}\mathbf{x} = 1$ em $\mathbb{Z}^n$.

Teorema 4.26. *Dado $n \geq 2$ par, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ tais que $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2} - 1)\,\mathbf{u} = 0$. Então, se $0 \neq a^2 = -2b$ ou $0 \neq a^2 = 6b$, tem-se $S(\Lambda_{\mathbf{u}}) \geq 3n$.*

Demonstração. Basta observar que $(\underbrace{1, 0, \cdots, 0}_{\frac{n}{2}\text{ coordenadas}}, -1, 0, \cdots, 0)$ é solução para $Q^{(n)}_{\frac{n}{2}}\mathbf{x} = 1$, bem como suas $\frac{n}{2}$ rotações e opostos, totalizando n soluções. Também são soluções as $2n$ rotações e opostos de $(1, 0, \cdots, 0)$. □

Teorema 4.27. *Dado $n \geq 2$ par, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \cdots = \mathcal{P}_n(\frac{n}{2} - 1)\,\mathbf{u} = 0$ então $\det G_{\mathbf{u}} = \pm a^n 3^{-\frac{n}{4}}$ se $a^2 = 6b$, e $\det G_{\mathbf{u}} = \pm a^n 3^{\frac{n}{4}}$ se $a^2 = -2b$.*

Demonstração. Suponha primeiramente que $n \in 4\mathbb{Z}$. Então $\frac{n}{2} \in 2\mathbb{Z}$, donde, pelo Teorema 4.7,

$$\begin{aligned}\det G_{\mathbf{u}} &= \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left[a^2 - 2b + b\left(\zeta_n^{\frac{n}{2}j} + \zeta_n^{-\frac{n}{2}j}\right)\right] \\ &= \pm a^2 \prod_{j=1}^{\frac{n-2}{2}} \left[a^2 - 2b + 2b(-1)^j\right]\end{aligned}$$

Como $n \in 4\mathbb{Z}$, então $\frac{n-2}{2} \notin 2\mathbb{Z}$, e portanto há $\frac{n-4}{4}$ números pares no intervalo $[1, \frac{n-2}{2}]$. Logo, se $a^2 = 6b$, então

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a^2 (2b)^{\frac{n-2}{2}} \prod_{j=1}^{\frac{n-2}{2}} \left[2 + (-1)^j\right] \\
&= \pm a^n 3^{-\frac{n-2}{2}} \prod_{j=1}^{\frac{n-2}{2}} \left[2 + (-1)^j\right] \\
&= \pm a^n 3^{-\frac{n-2}{2}} 3^{\frac{n-4}{4}} \\
&= \pm a^n 3^{-\frac{n}{4}},
\end{aligned}$$

e se $a^2 = -2b$,

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a^2 (2b)^{\frac{n-2}{2}} \prod_{j=1}^{\frac{n-2}{2}} \left[-2 + (-1)^j\right] \\
&= \pm a^n \prod_{j=1}^{\frac{n-2}{2}} \left[-2 + (-1)^j\right] \\
&= \pm a^n 3^{\frac{n}{4}}.
\end{aligned}$$

Suponha agora que $n \in 2\mathbb{Z}\backslash 4\mathbb{Z}$. Nesse caso, mais uma vez pelo Teorema 4.7,

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a\sqrt{a^2 - 4b} \prod_{j=1}^{\frac{n-2}{2}} \left[a^2 - 2b + b\left(\zeta_n^{\frac{n}{2}j} + \zeta_n^{-\frac{n}{2}j}\right)\right] \\
&= \pm a\sqrt{a^2 - 4b} \prod_{j=1}^{\frac{n-2}{2}} \left[a^2 - 2b + 2b(-1)^j\right]
\end{aligned}$$

Como $n \in 2\mathbb{Z}\backslash 4\mathbb{Z}$, então $\frac{n-2}{2} \notin 2\mathbb{Z}$, e portanto há $\frac{n-2}{4}$ números pares no intervalo $[1, \frac{n-2}{2}]$. Logo, se $a^2 = 6b$, então

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a (2b)^{\frac{1}{2} + \frac{n-2}{2}} \prod_{j=1}^{\frac{n-2}{2}} \left[2 + (-1)^j\right] \\
&= \pm a^n 3^{-\frac{n-1}{2}} \prod_{j=1}^{\frac{n-2}{2}} \left[2 + (-1)^j\right] \\
&= \pm a^n 3^{-\frac{n-1}{2}} 3^{\frac{n-2}{4}} \\
&= \pm a^n 3^{-\frac{n}{4}},
\end{aligned}$$

e se $a^2 = -2b$,

$$\begin{aligned}
\det G_{\mathbf{u}} &= \pm a(3a^2)^{\frac{1}{2}}(2b)^{\frac{n-2}{2}} \prod_{j=1}^{\frac{n-2}{2}} \Big[-2 + (-1)^j \Big] \\
&= \pm a^n 3^{\frac{1}{2}} \prod_{j=1}^{\frac{n-2}{2}} \Big[-2 + (-1)^j \Big] \\
&= \pm a^n 3^{\frac{n-2}{4}+\frac{1}{2}} \\
&= \pm a^n 3^{\frac{n}{4}}.
\end{aligned}$$

□

Corolário 7. Dado $n \geq 2$ par, sejam $\rho_1, \cdots, \rho_n \in \mathbb{R}$ e $\mathbf{u} = (\rho_1, \cdots, \rho_n)$. Se $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2} - 1)\,\mathbf{u} = 0$ e $0 \neq a^2 = 6b$ ou $0 \neq a^2 = -2b$, então $\delta(\Lambda_{\mathbf{u}}) = 2^{-\frac{n}{2}} 3^{-\frac{n}{4}}$.

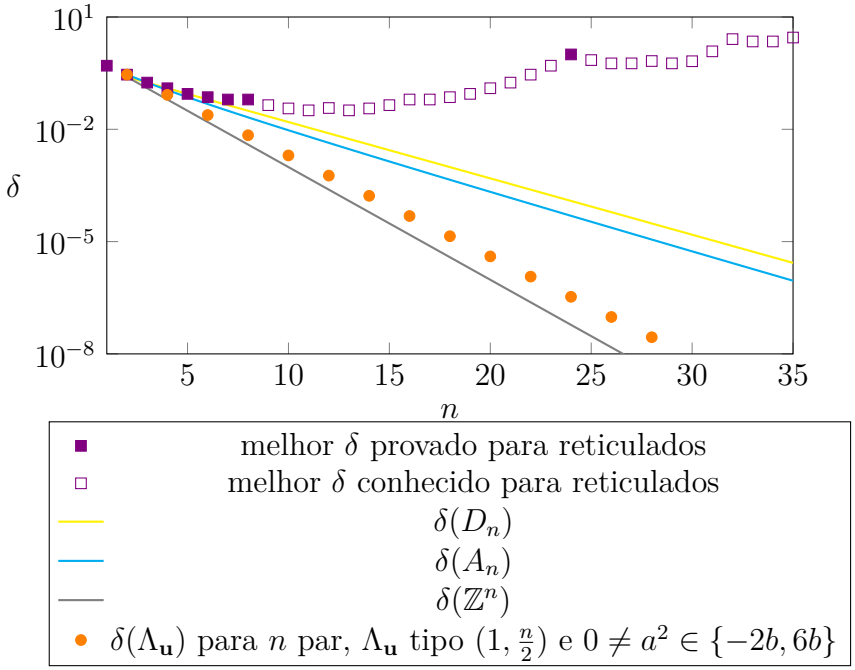

Figura 4.9: Densidade de centro de reticulados circulantes obtidos do Corolário 7. Fonte: Elaborado pelo autor.

Observe que, dessa forma, obtemos o reticulado hexagonal para $n = 2$, o melhor nessa dimensão. A partir de $n = 4$, tem-se $\delta(\Lambda_{\mathbf{u}}) < \delta(A_n)$, e consequentemente obtemos densidades piores do que os da seção anterior para $n \in 2\mathbb{Z}\backslash 4\mathbb{Z}$. Dessa forma, como a Figura 4.9 sugere, apesar do fato de que dentro de nossas hipóteses tem-se $\delta(\Lambda_{\mathbf{u}}) > \delta(\mathbb{Z}^n)$, a diferença não é substancial. A vantagem em relação ao caso $r_0 \neq \frac{n}{2}$ é que agora construímos reticulados

para quando n é uma potência de 2, o que antes não era possível por conta da condição $\frac{n}{(r_0,n)} \notin 2\mathbb{Z}$.

4.3 Reticulados circulantes tipo $(2,k)$

Até aqui, utilizamos a estratégia de anular os parâmetros $\mathcal{P}_n(r)\,\mathbf{u}$, mas podemos, naturalmente, buscar outras estratégias. Por exemplo, supondo que existem soluções reais para $\mathcal{P}_n(1)\,\mathbf{u} = \mathcal{P}_n(2)\,\mathbf{u} = \cdots = \mathcal{P}_n(\lfloor\frac{n-1}{2}\rfloor)\,\mathbf{u} = k$, e $\mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = \frac{k}{2}$ se n é par, então

$$\begin{aligned} D\mathbf{x} &= (a^2-2b)\sum_{i=1}^{n} x_i^2 + 2\sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x} + 4\tau_n \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} \\ &= (a^2-2b)\sum_{i=1}^{n} x_i^2 + 2k\sum_{r=1}^{\lfloor\frac{n}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{x} \\ &= (a^2-2b)\sum_{i=1}^{n} x_i^2 + 2k\sum_{\substack{i,j\in I_n \\ i<j}} x_i x_j, \end{aligned}$$

onde $\tau_n := \frac{1+(-1)^n}{2}$.

Denominaremos um reticulado $\Lambda_{\mathbf{u}}$ nessas condições de reticulado circulante tipo $(2,k)$.

Dentro dessas hipóteses, tem-se

$$b = \sum_{r=1}^{\lfloor\frac{n}{2}\rfloor} \mathcal{P}_n(r)\,\mathbf{u} = \tfrac{k}{2}(n-1).$$

Geometricamente, pelo Lema 4.2, a hipótese é equivalente a

$$\langle \mathbf{u}, \mathrm{rot}^r(\mathbf{u})\rangle = k \tag{4.6}$$

para todo $r \in \{1,2,\cdots,\lfloor\frac{n}{2}\rfloor\}$. Equivalentemente, dividindo cada equação por $\|\mathbf{u}\|^2$, obtemos que o ângulo entre $\mathbf{u}$ e qualquer rotação de $\mathbf{u}$ é o mesmo.

Antes de prosseguir, notemos que, $\forall j \in \{1,2,\cdots,n-1\}$, tem-se $\zeta_n^j \neq 1$, pois $n \nmid j$. Então aplicando o polinômio $1+t+\cdots+t^{n-1} = \frac{t^n-1}{t-1}$ sobre ζ_n^j, tem-se que

$$\sum_{m=1}^{n-1} \zeta_n^{jm} = -1,$$

seja qual for $j \in \{1,2,\cdots,n-1\}$.

Agora, em particular, se n é ímpar,

$$\det G_{\mathbf{u}} = \prod_{j=0}^{n-1} (\rho_1 + \rho_2\zeta_n^j + \cdots + \rho_n^{(n-1)j})$$

$$
\begin{aligned}
&= (\rho_1 + \cdots + \rho_n) \prod_{j=1}^{n-1} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n^{(n-1)j}) \\
&= -a \prod_{j=1}^{\frac{n-1}{2}} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n^{(n-1)j})(\rho_1 + \rho_2 \zeta_n^{-j} + \cdots + \rho_n^{-(n-1)j}) \\
&= -a \prod_{j=1}^{\frac{n-1}{2}} \left(\rho_1^2 + \cdots + \rho_n^2 + \mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j + \zeta_n^{-j}) + \cdots + \mathcal{P}_n(\tfrac{n-1}{2})\,\mathbf{u} \left(\zeta_n^{\frac{n-1}{2} j} + \zeta_n^{-\frac{n-1}{2} j} \right) \right) \\
&= -a \prod_{j=1}^{\frac{n-1}{2}} (a^2 - 2b + k(\zeta_n^j + \zeta_n^{2j} + \cdots + \zeta_n^{j(n-1)})) \\
&= -a \prod_{j=1}^{\frac{n-1}{2}} (a^2 - 2b - k),
\end{aligned}
$$

donde $\det G_{\mathbf{u}} \neq 0 \iff \begin{cases} a^2 - 2b \neq k \\ a \neq 0 \end{cases}$.

Por outro lado, se n é par, então, observando os cálculos feitos no Teorema 4.7,

$$
\begin{aligned}
\left(\rho_1 + \rho_2 \zeta_n^{\frac{n}{2}} + \rho_3 + \cdots + \rho_{n-1} + \rho_n \zeta_n^{\frac{n}{2}} \right)^2 &= (\rho_1 - \rho_2 + \cdots + \rho_{n-1} - \rho_n)^2 \\
&= a^2 - 4 \sum_{\substack{1 \leq r \leq \frac{n}{2} \\ r \text{ ímpar}}} \mathcal{P}_n(r)\,\mathbf{u} \\
&= a^2 - nk \\
&= a^2 - 2b - k \\
&\geq 0.
\end{aligned}
$$

Dessa forma, como $\zeta_n^{\frac{n}{2}} = \zeta_n^{-\frac{n}{2}} = -1$,

$$
\begin{aligned}
\det G_{\mathbf{u}} &= \prod_{j=0}^{n-1} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n^{(n-1)j}) \\
&= (\rho_1 + \cdots + \rho_n)(\rho_1 - \rho_2 + \cdots + \rho_{n-1} - \rho_n) \prod_{\substack{j=1 \\ j \neq \frac{n}{2}}}^{n-1} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n^{(n-1)j}) \\
&= \pm a \sqrt{a^2 - 2b - k} \prod_{j=1}^{\frac{n-2}{2}} (\rho_1 + \rho_2 \zeta_n^j + \cdots + \rho_n^{(n-1)j})(\rho_1 + \rho_2 \zeta_n^{-j} + \cdots + \rho_n^{-(n-1)j}) \\
&= \pm a \sqrt{a^2 - 2b - k} \prod_{j=1}^{\frac{n-2}{2}} \left(\rho_1^2 + \cdots + \rho_n^2 + \mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j + \zeta_n^{-j}) + \cdots + \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u} \left(\zeta_n^{\frac{n}{2} j} + \zeta_n^{-\frac{n}{2} j} \right) \right) \\
&= \pm a \sqrt{a^2 - 2b - k} \prod_{j=1}^{\frac{n-2}{2}} \left(\rho_1^2 + \cdots + \rho_n^2 + \mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j + \zeta_n^{-j}) + \cdots + \mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u} \left(\zeta_n^{\frac{n}{2} j} + \zeta_n^{\frac{n}{2} j} \right) \right)
\end{aligned}
$$

$$= \pm a\sqrt{a^2-2b-k}\prod_{j=1}^{\frac{n-2}{2}}(a^2-2b+k(\zeta_n^j+\zeta_n^{2j}+\cdots+\zeta_n^{j(n-1)}))$$
$$= \pm a\sqrt{a^2-2b-k}\prod_{j=1}^{\frac{n-2}{2}}(a^2-2b-k),$$

donde $\det G_{\mathbf{u}} \neq 0 \iff \begin{cases} a^2-2b>k \\ a\neq 0 \end{cases}$. É pertinente notar, no entanto, que dentro de nossas hipóteses, tem-se $a^2-2b-k\geq 0$, e portanto $a^2-2b>k \iff a^2-2b\neq k$.

Se $a^2-2b=2k\neq 0$, então

$$\mathbf{x}\neq\mathbf{0} \implies D\mathbf{x}=2k\left(\sum_{i=1}^{n}x_i^2+\sum_{\substack{i,j\in I_n\\ i<j}}x_ix_j\right)\geq 2k,$$

e $D(1,0,\cdots,0)=2k$. Assim, $|\Lambda_{\mathbf{u}}|=2k=a^2-2b$. Como $b=k^{\frac{n-1}{2}}$, então, $a^2-2b=2k$ se e somente se $a^2=k(n+1)$. Nesse caso, tem-se também que $|\det G_{\mathbf{u}}|=|a|k^{\frac{n-1}{2}}=(k(n+1))^{\frac{1}{2}}k^{\frac{n-1}{2}}=k^{\frac{n}{2}}(n+1)^{\frac{1}{2}}$. Assim,

$$\delta(\Lambda_{\mathbf{u}})=\frac{\left(\frac{\sqrt{|\Lambda_{\mathbf{u}}|}}{2}\right)^n}{|\det G_{\mathbf{u}}|}=\frac{(2k)^{\frac{n}{2}}}{2^nk^{\frac{n}{2}}(n+1)^{\frac{1}{2}}}=2^{-\frac{n}{2}}(n+1)^{-\frac{1}{2}}=\delta(A_n).$$

Além disso, a forma quadrática $\sum_{i=1}^{n}x_i^2+\sum_{\substack{i,j\in I_n\\ i<j}}x_ix_j=1$ possui no mínimo $n(n+1)$ soluções. De fato, são soluções os vetores $(1,\underbrace{0,\cdots,0,-1,0,\cdots,0}_{\substack{\text{uma coordenada }=-1\\ \text{e o restante nulo}}})$ e suas $n-1$ outras possíveis rotações (totalizando $n(n-1)$ soluções), bem como $(1,0,\cdots,0)$ e suas rotações e opostos (mais $2n$ soluções). Consequentemente, $|S(\Lambda_{\mathbf{u}})|\geq n(n+1)=\kappa(A_n)$.

Teorema 4.28. *Dado $n\geq 2$, sejam $\rho_1,\cdots,\rho_n\in\mathbb{R}$ e $\mathbf{u}=(\rho_1,\cdots,\rho_n)$ tais que $\mathcal{P}_n(1)\,\mathbf{u}=\cdots=\mathcal{P}_n(\frac{n-1}{2})\,\mathbf{u}=k$ e $\mathcal{P}_n(\frac{n}{2})\,\mathbf{u}=\frac{k}{2}$.*

Se n é ímpar, então $\det G_{\mathbf{u}}\neq 0 \iff \begin{cases} a^2-2b\neq k \\ a\neq 0 \end{cases}$. *Se n é par, então $a^2-2b\geq k$, e além disso,* $\det G_{\mathbf{u}}\neq 0 \iff \begin{cases} a^2-2b>k \\ a\neq 0 \end{cases}$.

Além disso, se $a^2-2b=2k$, então $|\det G_{\mathbf{u}}|=k^{\frac{n}{2}}(n+1)^{\frac{1}{2}}$, $|\Lambda_{\mathbf{u}}|=2k$, $|S(\Lambda_{\mathbf{u}})|\geq n(n+1)=\kappa(A_n)$ e $\delta(\Lambda_{\mathbf{u}})=2^{-\frac{n}{2}}(n+1)^{-\frac{1}{2}}=\delta(A_n)$.

Tendo em vista a equação (4.6) discutida anteriormente, temos que $a^2-2b=2k$ é equivalente a $\langle\mathbf{u},\mathbf{u}\rangle=2\langle\mathbf{u},\mathrm{rot}^r(\mathbf{u})\rangle$ para todo $r\in\{1,2,\cdots,\lfloor\frac{n}{2}\rfloor\}$, isto é, os vetores $\mathrm{rot}^r(\mathbf{u})$ e $\mathbf{u}-\mathrm{rot}^r(\mathbf{u})$ estão tão próximos da origem quanto de $\mathbf{u}$, como discutido na seção anterior.

Exemplo 4.29. Se $n=3$, então $\mathbf{u}=(1,0,1)$ é solução para $\begin{cases}\mathcal{P}_3(1)\,\mathbf{u}=1\\ a^2-2b=2\end{cases}$. Então $|\Lambda_{\mathbf{u}}|=2$ e $\delta(\Lambda_{\mathbf{u}})=\frac{1}{4\sqrt{2}}$. Além disso, é possível calcular por meio de um software todas as soluções de $\sum_{i=1}^{n}x_i^2+\sum_{\substack{i,j\in I_n\\ i<j}}x_ix_j=1$. A saber, são 12 soluções. Nesse caso, $\Lambda_{\mathbf{u}}\sim A_3$, pois A_3 é o reticulado de maior densidade de centro para $n=3$, e é único com essa propriedade, a menos de semelhança.

Se $n=5$, então

$$\begin{aligned}\rho_1&=0.3112182833461997\\ \rho_2&=-0.16611209524121553\\ \rho_3&=1.0259962143727757\\ \rho_4&=0.5855997148416358\\ \rho_5&=0.6927876254637826\end{aligned}$$

é solução para $\begin{cases}\mathcal{P}_n(1)\,\mathbf{u}=\mathcal{P}_n(2)\,\mathbf{u}=1\\ a^2-2b=2\end{cases}$. Nesse caso, $\delta(\Lambda_{\mathbf{u}})=\delta(A_5)$.

Observe que não podemos fazer o mesmo para n par e $\mathcal{P}_n(\frac{n}{2})\,\mathbf{u}=0$ apesar de obtermos uma expressão simplificada para $D\mathbf{x}$. Com efeito, nesse caso, $\det G_{\mathbf{u}}$ possui um fator nulo se $a^2-2b=2k$. De fato, como $b=\frac{n-2}{2}k$, então se em particular $n\in 4\mathbb{Z}$, basta observar utilizando os cálculos no Teorema 4.7 que

$$\begin{aligned}(\rho_1-\rho_2+\cdots-\rho_{n-1}+\rho_n)^2&=a^2-4\sum_{\substack{1\le r\le\frac{n}{2}\\ r\text{ ímpar}}}\mathcal{P}_n(r)\,\mathbf{u}=a^2-nk\\ &=a^2-2(b+k)\\ &=a^2-2b-2k.\end{aligned}$$

Logo, se $a^2-2b=2k$, tem-se $\det G_{\mathbf{u}}=0$. Agora, se por outro lado $n\in 2\mathbb{Z}\backslash 4\mathbb{Z}$, então o fator $(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n^{(n-1)j})(\rho_1+\rho_2\zeta_n^{-j}+\cdots+\rho_n^{-(n-1)j})$ de $\det G_{\mathbf{u}}$ pode ser reescrito como

$$\begin{aligned}&\rho_1^2+\cdots+\rho_n^2+\mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j+\zeta_n^{-j})+\cdots+\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\left(\zeta_n^{\frac{n}{2}j}+\zeta_n^{-\frac{n}{2}j}\right)\\ &=\rho_1^2+\cdots+\rho_n^2+\mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j+\zeta_n^{-j})+\cdots+\mathcal{P}_n(\tfrac{n}{2}-1)\,\mathbf{u}\left(\zeta_n^{(\frac{n}{2}-1)j}+\zeta_n^{-(\frac{n}{2}-1)j}\right)\\ &=a^2-2b+k(\zeta_n^j+\zeta_n^{2j}+\cdots+\zeta_n^{(\frac{n}{2}-1)j}+\zeta_n^{(\frac{n}{2}+1)j}+\cdots+\zeta_n^{(n-1)j}-\zeta_n^{\frac{n}{2}j})\\ &=a^2-2b+k(-1-(-1)^j),\end{aligned}$$

e portanto, se $a^2-2b=2k$, tem-se $\det G_{\mathbf{u}}=0$.

Semelhantemente, supor $\mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = k$ também implica em $\det G_{\mathbf{u}} = 0$. De fato, como $\zeta_n^{\frac{n}{2}} = \zeta_n^{-\frac{n}{2}} = -1$, então o fator $(\rho_1+\rho_2\zeta_n^j+\cdots+\rho_n^{(n-1)j})(\rho_1+\rho_2\zeta_n^{-j}+\cdots+\rho_n^{-(n-1)j})$ de $\det G_{\mathbf{u}}$ pode ser reescrito como

$$\begin{aligned}
&\rho_1^2+\cdots+\rho_n^2+\mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j+\zeta_n^{-j})+\cdots+\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\left(\zeta_n^{\frac{n}{2}j}+\zeta_n^{-\frac{n}{2}j}\right)\\
&=\rho_1^2+\cdots+\rho_n^2+\mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j+\zeta_n^{-j})+\cdots+\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\left(\zeta_n^{\frac{n}{2}j}+\zeta_n^{\frac{n}{2}j}\right)\\
&=a^2-2b+k(\zeta_n^j+\zeta_n^{2j}+\cdots+\zeta_n^{(n-1)j}+(-1)^j)\\
&=a^2-2b+k(-1+(-1)^j).
\end{aligned}$$

Logo, para j ímpar, obtém-se o fator $a^2-2b-2k$. Consequentemente, para n par e $\mathcal{P}_n(1)\,\mathbf{u} = \cdots = \mathcal{P}_n(\frac{n}{2})\,\mathbf{u} = k$, não podemos supor $a^2-2b = 2k$.

5 Conclusão

A fim de simplificar a norma de um vetor arbitrário de um reticulado circulante determinado por $\mathbf{u}$, vimos que podemos construir reticulados tão densos quanto classes conhecidas como D_n e A_n.

Podemos por exemplo simplificar a norma zerando todos os parâmetros $\mathcal{P}_n(r)\,\mathbf{u}$, exceto por no máximo $r = r_0$, onde $\frac{n}{(r_0,n)}$ é ímpar. Isso significa resolver um sistema de equações não-lineares. O significado geométrico, por sua vez, é encontrar $\mathbf{u}$ ortogonal a suas rotações, exceto pela r_0-ésima. Podemos adicionar a isso a hipótese $\langle \mathbf{u}, \mathbf{u} \rangle = 2\langle \mathbf{u}, \mathrm{rot}^{r_0}(\mathbf{u}) \rangle$, o que significa geometricamente que a r_0-ésima rotação de $\mathbf{u}$ está tão próxima da origem quanto de $\mathbf{u}$. Encontramos como consequência reticulados tão densos quanto D_n para n ímpar, o reticulado hexagonal para $n = 2$, e reticulados mais densos que A_n para $n \in 2\mathbb{Z}\backslash 4\mathbb{Z}$ a partir de $n = 18$.

Outra possibilidade que exploramos, a fim de simplificar a expressão da norma, foi exigir que o produto interno entre $\mathbf{u}$ e qualquer rotação é sempre o mesmo. Isso significa que o vetor $\mathbf{u}$ faz um mesmo ângulo com qualquer rotação. Impondo $\langle \mathbf{u}, \mathbf{u} \rangle = 2\langle \mathbf{u}, \mathrm{rot}^{r}(\mathbf{u}) \rangle$ para todo r, encontramos dessa forma reticulados com a mesma densidade de A_n, para qualquer dimensão.

A dificuldade de nosso método é encontrar soluções para sistemas não-lineares. Isto é, trata-se de um problema de otimização, que é dificultado com o aumento de n. Uma pergunta razoável que se coloca é: quais outras hipóteses podemos impor sobre $\mathbf{u}$ de modo a gerar outros reticulados eventualmente melhores? A vantagem é que o assunto pode ser explorado computacionalmente. Nosso método fornece expressões para o mínimo e o determinante em função dos parâmetros determinados por $\mathbf{u}$, como a e b. Mas nada impede que se coloque uma hipótese sobre $\mathbf{u}$ de modo que se calcule a norma mínima e outros parâmetros através de outros métodos, como algoritmos computacionais que existem na literatura.

Referências

[1] KING, S. *It: a coisa*. 1. ed. Rio de Janeiro: Objetiva, 2014.

[2] CALDERBANK, A.; SLOANE, N. New trellis codes based on lattices and cosets. *IEEE Transactions on Information Theory*, v. 33, n. 2, p. 177–195, 1987.

[3] EREZ, S. L. U.; ZAMIR, R. Lattices which are good for (almost) everything. *IEEE Transactions on Information Theory*, v. 51, n. 10, p. 3401–3416, 2005.

[4] BOUTROS E. VITERBO, C. R. J.; BELFORE, J. . Good lattice constellations for both rayleigh fading and gaussian channels. *IEEE Transactions on Information Theory*, v. 42, n. 2, p. 502–508, 1996.

[5] JOUX, A.; STERN, J. Lattice reduction: A toolbox for the cryptanalyst. *J. Cryptology*, v. 11, p. 161–185, 2005.

[6] MICCIANCIO, D.; REGEV, O. Lattice-based cryptography. In: BERNSTEIN, J. B. D. J.; DAHMEN, E. (Ed.). *Post-Quantum Cryptography*. 2nd. ed. Berlin: Springer, 2009. p. 147–191.

[7] NGUYEN, P. Q.; STERN, J. The two faces of lattices in cryptology. In: SILVERMAN, J. H. (Ed.). *Cryptography and Lattices. CaLC 2001. Lecture Notes in Computer Science*. 2nd. ed. Berlin, Germany: Springer, 2001. v. 2146, p. 146–180.

[8] DAMIR, M. T. et al. Well-rounded lattices: Towards optimal coset codes for gaussian and fading wiretap channels. *IEEE Transactions on Information Theory*, v. 67, n. 6, p. 3645–3663, 2021.

[9] KANNAN, R. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, v. 12, n. 3, p. 415–440, 1987.

[10] BABAI, L. On lova´sz' lattice reduction and the nearest lattice point problem. *Combinatorica*, v. 6, p. 1–13, 1986.

[11] SAHRAEI, S.; GASTPAR, M. Polynomially solvable instances of the shortest and closest vector problems with applications to compute-and-forward. *IEEE Transactions on Information Theory*, v. 63, n. 12, p. 7780–7792, 2017.

[12] CAI, J. The complexity of some lattice problems. In: BOSMA, W. (Ed.). *Algorithmic Number Theory. ANTS 2000. Lecture Notes in Computer Science*. [S.l.]: Springer, 2001. v. 1838, p. 1–32.

[13] MICCIANCIO, D. The hardness of the closest vector problem with preprocessing. *IEEE Transactions on Information Theory*, v. 47, n. 3, p. 1212–1215, 2001.

[14] SUN, C. G. Z.; ZHENG, Y. A review of sieve algorithms in solving the shortest lattice vector problem. *IEEE Access*, v. 8, p. 190475–190486, 2020.

[15] MCKILLIAM, R. G.; CLARKSON, I. V. L.; QUINN, B. G. An algorithm to compute the nearest point in the lattice A_n^*. *IEEE Transactions on Information Theory*, v. 54, n. 9, p. 4378–4381, 2008.

[16] CONWAY, J.; SLOANE, N. Fast quantizing and decoding and algorithms for lattice quantizers and codes. *IEEE Transactions on Information Theory*, v. 28, n. 2, p. 227–232, 1982.

[17] MCKILLIAM, R. G.; SMITH, W. D.; CLARKSON, I. V. L. Linear-time nearest point algorithms for Coxeter lattices. *IEEE Transactions on Information Theory*, v. 56, n. 3, p. 1015–1022, 2010.

[18] SAMUEL, P. *Algebraic Theory of Numbers*. [S.l.]: Hermann, 1970.

[19] SHANNON, C. E. A mathematical theory of communication. *The Bell System Technical Journal*, v. 27, p. 379–423 and 623–656, 1948.

[20] CONWAY, J. H.; SLOANE, N. J. A. *Sphere Packings, Lattices and Groups*. 3. ed. New York: Springer, 1999.

[21] BALL, K. A lower bound for the optimal density of lattice packings. *International Mathematics Research Notices*, v. 10, p. 217–221, 1992.

[22] HALES, T. C. A proof of the Kepler conjecture. *Annals of mathematics*, v. 162, p. 1065–1185, 2005.

[23] COLE, I. R. *Modelling CPV*. Tese (Doutorado) — Loughborough University, 2015. Seção 9.2.

[24] NEBE, G.; SLOANE, N. J. A. *Table of Densest Packings Presently Known*. 2012. Online; accessed 2021-12-15. Disponível em: <http://www.math.rwth-aachen.de/ Gabriele.Nebe/LATTICES/density.html>.

[25] PFENDER, F.; ZIEGLER, G. M. Kissing numbers, sphere packings, and some unexpected proofs. *Notices of the AMS*, p. 873–883, 2004.

[26] COHN, H.; ZHAO, Y. Sphere packing bounds via spherical codes. *Duke Mathematical Journal*, Duke University Press, v. 163, n. 10, Jul 2014.

[27] WYNER, A. D. Capabilities of bounded discrepancy decoding. *The Bell System Technical Journal*, v. 44, n. 6, p. 1061–1122, 1965.

[28] BACHOC, C.; VALLENTIN, F. New upper bounds for kissing numbers from semidefinite programming. *Journal of the American Mathematical Society*, American Mathematical Society (AMS), v. 21, n. 3, p. 909–924, Nov 2007.

[29] MACHADO, F. C.; FILHO, F. M. O. Improving the semidefinite programming bound for the kissing number by exploiting polynomial symmetry. *Experimental Mathematics*, Taylor and Francis, v. 27, n. 3, p. 362–369, 2016.

[30] HOLLANTI, C.; MANTILLA-SOLER, G.; MILLER, N. *Dense generic well-rounded lattices*. 2021.

[31] MCMULLEN, C. T. Minkowski's conjecture, well-rounded lattices and topological dimension. *Journal of the American Mathematical Society*, v. 18, n. 3, p. 711–734, 2005.

[32] MARTINET, J. *Perfect Lattices in Euclidean Spaces*. [S.l.]: Springer, 2003.

[33] FUKSHANSKY, L.; PETERSEN, K. On well-rounded lattices. *International Journal of Number Theory*, v. 8, n. 1, p. 189–206, 2012.

[34] ANDRADE, A. A. et al. Constructions of algebraic lattices. *Computational and Applied Mathematics. SBMAC*, v. 29, n. 3, p. 493–505, 2010.

[35] DAVIS, P. J. *Circulant Matrices*. New York, NY, USA: Wiley-Interscience, 1979.

[36] GARCIA, A.; LEQUAIN, Y. *Elementos de Álgebra*. 6. ed. Rio de Janeiro, RJ, Brasil: IMPA, 2018.

[37] FUKSHANSKY, L.; SUN, X. On the geometry of cyclic lattices. *Discrete Comput. Geom*, v. 52, p. 240–259, 2014.

[38] FLORES, A. L.; INTERLANDO, J. C.; NUNES, J. V. L. Optimal families of two and three-dimensional lattice packings from polynomials with integer coefficients. *JP Journal of Algebra, Number Theory and Applications*, v. 15, n. 1, p. 45–51, 2009.

[39] ALVES, C.; LIMA, W. Well-rounded lattices via polynomials with real roots. *International Journal of Applied Mathematics*, v. 33, n. 4, p. 663–672, 2020.

[40] VINBERG, E. B. *A Course in Algebra*. 5. ed. Province, RI, USA: AMS, 2003. v. 56.