



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



Geometria Discreta e Códigos[★]

João Eloir Strapasson

jes@ime.unicamp.br/joaoeloir@gmail.com

Tese de Doutorado

Orientadora: **Prof^a. Dr^a. Sueli I. R. Costa**

Co-orientador: **Prof. Dr. Marcelo Muniz Silva Alves**

11 de abril de 2007

Campinas - SP

★ Este trabalho contou com apoio financeiro da FAPESP - processo 02/14134-4.

Geometria Discreta e Códigos

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **João Eloir Strapasson** e aprovada pela comissão julgadora.

Campinas, 11 de abril de 2007.



Prof.^a. Dr.^a. **Sueli I. R. Costa**

Orientadora



Prof. Dr. **Marcelo Muniz Silva Alves**

Co-orientador

Banca Examinadora:

Prof.^a. Dr.^a. Sueli I. R. Costa IMECC - UNICAMP

Prof. Dr. Jayme Luiz Szwarcfiter NCE - UFRJ

Prof. Dr. Ricardo Dahab IC - UNICAMP

Prof. Dr. Vilmar Trevisan DMPA - UFRGS

Prof. Dr. Yoshiharu Kohayakawa IME - USP

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

**FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DO IMECC DA UNICAMP**

Bibliotecária: Miriam Cristina Alves - CRB8a / 5094

Strapasson, João Eloir

St81g Geometria Discreta e Códigos/João Eloir Strapasson – Campinas,
[S.P.:s.n.], 2005.

Orientadores: Sueli Irene Rodrigues Costa; Marcelo Muniz Silva
Alves

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de
Matemática, Estatística e Computação Científica.

1. Geometria discreta. 2. Teoria da codificação. 3. Teoria dos
reticulados. 4. Teoria dos Grafos I. Costa, Sueli Irene Rodrigues. II. Alves,
Marcelo Muniz Silva. III. Universidade Estadual de Campinas. Instituto de
Matemática, Estatística e Computação Científica. IV. Título.

Título em inglês: Discrete Geometry and Codes

Palavras-chave em inglês (keywords): 1. Discret geometry. 2. Codes theory. 3. Lattices. 4.
Graphs theory.

Área de concentração: Geometria/Topologia

Titulação: Doutor em matemática

Banca examinadora: Prof.^a. Dr.^a. Sueli Irene Rodrigues Costar (IMECC-Unicamp)
Prof. Dr. Jayme Luiz Szwarcfiter (NCE-UFRJ)
Prof. Dr. Ricardo Dahab (IC-UNICAMP)
Prof. Dr. Vilmar Trevisan (DMPA-UFRGS)
Prof. Dr. Yoshiharu Kohayakawa (IME-USP)

Data da defesa: 11/04/2007

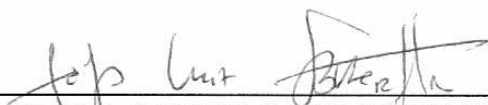
Programa de Pós-Graduação: Doutorado em Matemática

Tese de Doutorado defendida em 11 de abril de 2007 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.



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



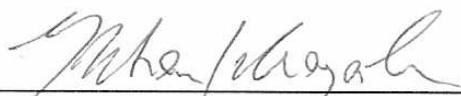
Prof. (a). Dr (a). JAYME LUIZ SZWARCFITER



Prof. (a). Dr (a). RICARDO DAHAB



Prof. (a). Dr (a). VILMAR TREVISAN



Prof. (a) Dr. (a) YOSHIHARU KOHAYAKAWA

À minha mãe **Maria** (*in memoriam*),
À minha esposa **Adriana**,

Dedico

Agradecimentos

Ao meu Deus, pela presença constante em minha vida e por ter me dado saúde, força e esperança.

À Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), pelo apoio financeiro (Processo 02/14134-4) concedido durante o período de abril de 2003 a fevereiro de 2007, sem o qual não seria possível a realização do Programa de Doutorado em Matemática.

Ao parecerista Fapesp, pelo acompanhamento deste trabalho desde seu projeto inicial.

À minha esposa, Adriana, pela compreensão, pelo companherismo e apoio.

À minha família, por todo apoio e compreensão durante este doutorado, em especial ao meu irmão Altair e sua esposa Daniele.

À minha mãe, a maior responsável por tudo que envolve este trabalho. Acreditando, motivando e preparando o caminho de forma muito especial e sábia.

Aos meus professores de graduação, que contribuíram muito para a minha formação em matemática. Em especial aos professores: Alexandre Kirilov, Aurélio Sartoreli, João B. de Mendonça Xavier, Liangzhong Hu, Pedro D. Damázio.

Aos meus professores de pós-graduação, que contribuíram muito para a minha consolidação como matemático. Em especial aos professores: Jorge T. Mujica Ascui, Luiz S. Martin, Marcelo Firer, Paulo R. Brumatti, Paulo R. C. Ruffino

Aos meus orientadores de iniciação científica, Adonai A. Sant'Anna e José Carlos Cifuentes, pela contribuição à formação como pesquisador e pelo companherismo.

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

Ao meu orientador, Marcelo Muniz, pela excelente contribuição através de discussões, sugestões e críticas construtivas.

À minha orientadora, Sueli Costa, por sua excelente contribuição que transcendeu a orientação.

Aos meus colegas de grupo de pesquisa do grupo de “Códigos geometricamente uniformes”, Andréia, Carina, Cristiano, Mércio, Rogério e Tatiana e prof Carlile.

Aos colegas de IMECC e aos colegas das disciplinas da FEF.

Aos funcionários do IMECC, secretaria do instituto, secretaria de pós-graduação, secretaria de graduação e demais funcionários.

Os meus sinceros agradecimentos.

Resumo

Este trabalho está dividido em duas partes. A primeira é dedicada ao problema de encontrar o menor vetor não nulo de um reticulado. Este é um problema de alta complexidade computacional e que tem grande interesse tanto para a Teoria dos Códigos, como para diversas outras áreas. Esse mínimo está associado à performance do reticulado em termos da codificação: quanto maior for a razão entre este mínimo e o determinante do reticulado, melhor é a distribuição dos pontos no espaço (alta densidade de empacotamento). Nesta tese demos ênfase ao caso especial dos reticulados obtidos por uma projeção ortogonal do reticulado n -dimensional dos inteiros na direção de um de seus elementos. Tais reticulados estão associados ao problema de codificação contínua fonte/canal. Mostramos nos casos tri e quadridimensionais em que condições podemos garantir reticulados bons, ou seja, com alta densidade de empacotamento. Neste processo foram também construídos dois novos algoritmos, um para cálculo da base de Minkowski de um reticulado e outro específico para a busca da norma mínima do reticulado-projeção. Na segunda parte trabalhamos com grafos em toros planares que são quocientes de reticulados, os quais são isomorfos a grafos circulantes. Estabelecemos a conexão entre estes últimos e códigos esféricos rotulados por grupos cíclicos e códigos perfeitos na métrica de Lee. A partir de tal associação foram também obtidos resultados sobre o gênero de grafos circulantes, como a classificação completa dos grafos de gênero 1 e a determinação do gênero de uma classe especial de grafos circulantes que tem número arbitrariamente grande de conexões (grau).

Palavras-chave: Geometria discreta, Teoria da codificação, Teoria dos reticulados, Teoria dos Grafos

Abstract

The research developed here is related and inspired by problems in coding theory. It is presented in two parts. In the first we focus on the search for the minimum non-vanishing vector of a lattice, specially in the case of a projection of the n -dimensional integer lattice in the direction of one of its vectors. This is a problem of high computational complexity which is related to the search for efficient joint source-channel continuous coding. In the second part we deal with flat torus graphs generated by a quotient of lattices and which are labeled by a cyclic group of isometries. We show that any circulant graph is isomorphic to one of these graphs and hence associated to a spherical code. Through these isomorphism a complete classification of circulant graphs of genus one and the genus of an arbitrarily high order class of circulant graphs is obtained.

Key-words: Discret geometry, Codes theory, Lattices, Graphs theory.

Sumário

Agradecimentos	ix
Resumo	xi
Abstract	xiii
Lista de Símbolos	xix
Lista de Figuras	xxii
Lista de Tabelas	xxiii
Introdução	xxv
I Reticulados-Projeção	1
1 O Problema da Norma Mínima em Reticulados	3
1.1 Reticulados e Empacotamentos	3
1.1.1 Reticulados	3
1.1.2 Empacotamento	6
1.1.3 Sub-reticulados e Quocientes de Reticulados	8
1.2 Redução de Minkowski	9
1.2.1 Vetores Mínimos em \mathcal{L}^n	10
1.2.2 Proposta de Algoritmo para Redução de Minkowski	11
1.2.3 Relação entre as Regiões de Voronoi e Fundamental	12
1.3 Outras Formas de Redução	13
1.3.1 Relação entre as Reduções	15
1.4 Experimentos com os Algoritmos: Minkowski e LLL	16

2	O Problema da Projeção	19
2.1	Codificação Contínua Fonte/Canal	19
2.2	Formulação do Problema da Projeção	21
2.3	Como Obter $\mathcal{N}(\mathcal{L}_v)$	22
2.4	Projeção de \mathbb{Z}^3	24
2.4.1	Vetores do Tipo $v = (1, a, b)$	25
2.4.2	Vetores do Tipo $v = (a, b, c)$	29
2.5	Projeção de \mathbb{Z}^4	35
2.6	Algoritmo para Encontrar Mínimo em Reticulados-projeção	48
2.6.1	Distância de um Conjunto Discreto a uma Reta	48
2.6.2	Utilizando as Regiões de Voronoi (Algoritmo RV).	49
II	Grafos Circulantes	53
3	Grafos e Grafos Circulantes	55
3.1	Grafos: Definições e Terminologia	55
3.2	Exemplos de Grafos	56
3.3	Grafos sobre o Toro Plano	58
3.3.1	Ladrilhamento e Grafos em Toros	58
3.4	Grafos Circulantes	60
3.4.1	Grafos circulantes realizados como grafos sobre o toro planar	62
3.5	Grafos Circulantes e Códigos Esféricos	65
3.6	Conexidade dos Grafos Circulantes	69
4	Gênero de Grafos Circulantes	71
4.1	Gênero de um Grafo	71
4.1.1	Exemplo de gênero de grafos	72
4.1.2	Limitantes para o Gênero	73
4.2	Grafos Circulantes	73
4.2.1	Grafos Circulantes Planares	74
4.2.2	Grafos Circulantes Toroidais	74
4.3	Gênero de Grafos Circulantes Quadriláteros	77

Perspectivas Futuras	83
-----------------------------	-----------

Referências Bibliográficas	85
-----------------------------------	-----------

Lista de símbolos

\mathcal{B}	base de vetores no \mathbb{R}^n
$\mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b}$	vetores no \mathbb{R}^n
\mathcal{L}	reticulado no \mathbb{R}^n
$\text{vol}(\cdot)$	volume n -dimensional
$\text{vor}(\mathcal{L})$	região de Voronoi
\mathcal{A}_n	reticulado raiz
$\mathcal{N}(\mathcal{L})$	norma mínima de \mathcal{L}
S^n	esfera unitária n -dimensional contida no \mathbb{R}^n
$\Delta(\mathcal{L})$	densidade de empacotamento de \mathcal{L}
$\delta(\mathcal{L})$	densidade de centro de \mathcal{L}
f_{cc}	reticulado face center cubic
$\text{Aut}(\cdot)$	grupo de automorfismo
B_r	bola de raio r
adj	operador adjunto
\mathcal{G}	grafo
$\Gamma = \frac{\mathcal{L}}{\mathcal{L}'}$	quociente de reticulados vistos como grupo
$\mathcal{G}_B = \frac{\mathcal{L}_B}{\mathcal{L}'}$	grafo no toro obtido do quociente de reticulados
f	número de faces de um grafo
\mathbf{a}	número de arestas de grafo
\mathcal{K}_n	grafo completo de n vértices
$\mathcal{K}_{m,n}$	grafo bipartido completo de $m + n$ vértices
\mathfrak{g}	gênero um grafo
$\mathcal{C}_n(\mathbf{a})$	grafo circulante de n vértices

Lista de Figuras

1.1	À esquerda um reticulado no plano, ao centro uma região fundamental deste e à direita a região de Voronoi de ponto $\mathbf{0}$	5
1.2	O reticulado hexagonal.	6
1.3	Ilustração dos empacotamentos: à esquerda o reticulado Hexagonal, ao centro o reticulado gerado por $\{(3/2, 0), (1/2, \sqrt{14}/2)\}$ e à direita o reticulado \mathbb{Z}^2	7
1.4	Idéia geométrica da redução de Minkowski para dimensão 2.	11
2.1	Caso $n = 2$: Ilustramos, à esquerda, a curva dada pelo o vetor $\mathbf{v} = (2, 3)$ no toro e, à direita, o toro e curva no \mathbb{R}^3 através de uma projeção estereográfica da esfera S^3 do \mathbb{R}^4	20
2.2	Caso $n = 3$: Ilustramos, à esquerda, a curva dada pelo o vetor $\mathbf{v} = (1, 2, 3)$ no toro tridimensional, ao centro, o empacotamento de tubos com eixo suportado em pontos de \mathbb{Z}^3 com inclinação na direção de \mathbf{v} e, à direita, o mesmo empacotamento restrito ao toro tridimensional.	20
2.3	Caso $n = 3$: Ilustramos a secção ortogonal, empacotamento de tubos da Figura 2.2.	20
2.4	Intersecção da reta $a = 1$ com \mathbb{Z}^2	35
2.5	Intersecção da reta $a + b = 1$ com \mathbb{Z}^2	35
2.6	Gráfico $\delta(t), t \in [-0.5, 0.5]$	40
2.7	Vetor $\mathbf{v} = (3, 8)$	48
2.8	Vetor $\mathbf{v} = (1, 3, 8)$	48
2.9	Regiões de Voronoi dos pontos \mathbf{u} que são atingidas pelo vetor $\mathbf{v} = (3, 8)$	49
2.10	Regiões de Voronoi dos pontos \mathbf{u} que são atingidas pelo vetor $\mathbf{v} = (1, 3, 8)$	49
3.1	n -cadeia	56
3.2	n -cíclico	57
3.3	\mathcal{K}_5	57
3.4	Utility graph (UG)	57
3.5	Toro planar $\mathcal{T}_{\mathbf{u}, \mathbf{v}}$ ladrilhado por 13 quadrados.	58

3.6	Grafo Circulante $\mathcal{C}_{13}(1, 5)$	60
3.7	Grafo Circulante $\mathcal{C}_{13}(2, 3)$	63
3.8	O grafo circulante $\mathcal{C}_{13}(3, 5)$ sobre o toro planar, rotulado por $w = (2, -1)$	65
3.9	O grafo circulante $C_6(2, 3)$ mergulhado no toro planar: vértices, rotulamento e região fundamental da base $\{(10, 12), (12, 15)\}$ que definem a relação de adjacência.	67
4.1	Anti-prisma.	74
4.2	Prisma.	74
4.3	Mergulho do grafo circulante $C_{4k+2}(1, 2, 2k + 1)$ em um toro planar.	76
4.4	Mergulho do grafo circulante $C_8(1, 2, 4)$ em um toro planar.	76
4.5	Mergulho não ideal de grafo circulante de grau 6 (\bar{x} denota o vértice $x + a_3$).	78
4.6	Mergulho ideal de grafo circulante de grau 6 (\bar{x} denota o vértice $x + a_3$).	79
4.7	A figura mostra as duas componentes conexas do grafo $\mathcal{C}_{32}(8, 2)$. Utilizando o mergulho dado por 3.4.3, invertemos a orientação da segunda componente.	80

Lista de Tabelas

2.1	A tabela ilustra que alterações mínimas na maior coordenada podem alterar significativamente a densidade do reticulado-projeção.	24
2.2	Comparando as densidades de empacotamento tomando os $b(a)$ sugeridos pelos Teoremas: 2.4.1, 2.4.3, 2.4.2 e 2.4.4 (respectivamente).	28
2.3	Tabela densidades para vetores $\mathbf{v} = (1, 75, b)$	29
2.4	Ilustração dos valores de $t = [\sqrt{y^2 + (y^2 - 1)^2}] - \sqrt{x^2 + y^2}$	45
2.5	Considerando $x = 1$ e $y = 0$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.144338	46
2.6	Considerando $x = 1$ e $y = -1$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.164356	46
2.7	Considerando $x = 8$ e $y = -3$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.169779	47
2.8	Considerando $x = 99$ e $y = -10$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.176117	47
4.1	O símbolo \hat{x} significa que não há representante, $\hat{\pm y}$ significa que não podemos considerar o caso $\pm y$, pois saímos das hipóteses do Teorema 4.3.2	82

Introdução

Os temas aqui tratados estão relacionados à teoria de códigos e sua fundamentação matemática. A utilização de abordagens e técnicas geométricas foi impulsionada pelo surgimento nos anos 90 da classe dos códigos geometricamente uniformes (GU) [23]. Este conceito de uma forma mais ampla inclui outras distâncias (como a hiperbólica e de grafos), mas preservando as características importantes decorrentes da homogeneidade e rotulamento por simetrias: simplificação dos processos de codificação e decodificação, uniformidade da probabilidade de erro, etc. De um modo geral, elas refletem as interações entre teoria da codificação, grupos de simetria, grafos, reticulados, empacotamento de esferas, representações de grupos finitos e geometria diferencial.

A conexão dos problemas abordados neste trabalho com a teoria de códigos concentra-se e é motivada por dois temas: i) codificação contínua na esfera e ii) códigos de grupos cíclicos.

O uso de curvas (aplicações de \mathbb{R} em \mathbb{R}^N) em comunicações e processamento de sinais é associado a mapeamentos que expandem a largura de faixa. A análise de curvas que são subjacentes a sistemas não lineares de modulação, como é o caso de modulação em frequência, leva ao problema de se determinar curvas na esfera S^{N-1} em \mathbb{R}^N do maior comprimento possível condicionado a uma distância mínima a ser respeitada entre suas “voltas”. Uma construção homogênea de tais curvas pode ser feita colocando-as em toros planares ([47]). A procura de um bom desempenho para decodificação pode ser traduzida como a busca de reticulados-projeção com as melhores taxas de empacotamento de esferas, que é um problema muito complexo, inclusive do ponto de vista de algoritmo computacional. A estratégia tem sido contorná-lo, estabelecer limitantes e buscar em casos especiais soluções que tendem para a melhor possível, quando o comprimento da curva cresce. A busca de bons algoritmos para a determinação de melhores direções de projeção também é essencial nesta abordagem.

Os códigos de grupo foram introduzidos por D. Slepian ([42]) e são dados por constelações de pontos em esferas do \mathbb{R}^N geradas por grupos de matrizes ortogonais. Questões fundamentais associadas a estes códigos e que vem sendo abordadas desde então são a determinação do vetor inicial ótimo e o estabelecimento do número máximo de pontos da constelação fixada uma distância mínima (códigos ótimos).

Temos abordado estes problemas de forma muito geométrica no caso de códigos grupos co-

mutativos e mais particularmente para os grupos cíclicos. Esta análise é baseada no fato que as constelações geradas por tais grupos de simetria precisam estar sobre toros planares.

Na seqüência descrevemos de modo sucinto o conteúdo deste trabalho que é subdividido em: Parte I - *Reticulados-Projeção* e Parte II - *Grafos Circulantes*.

I - Reticulados-projeção: Uma boa codificação contínua fonte/canal na esfera foi introduzida no artigo [48]. Para que uma codificação tenha boa performance devemos resolver um problema equivalente à procura de direções $\mathbf{v} \in \mathbb{Z}^n$, tais que o reticulado obtido da projeção de \mathbb{Z}^n nesta direção, tenha alta densidade de empacotamento. Esta densidade mede o quão boa é a distribuição dos pontos no espaço. Existe uma grande dificuldade para cálculo do menor vetor não nulo de um reticulado, requisito necessário para o cálculo da densidade de empacotamento. O desenvolvimento deste tema dar-se-á através dos dois primeiros capítulos.

Capítulo 1: Apresentamos aqui as noções básicas de reticulados, empacotamentos e quocientes de reticulados. Ainda neste capítulo exploramos a noção de redução de bases, que é a busca de uma base onde os vetores têm normas relativamente próximas às mínimas possíveis. Destacamos três reduções conhecidas na literatura, a saber, LLL, KZ e Minkowski. As reduções KZ e Minkowski garantem que o menor vetor não nulo é o primeiro elemento da base reduzida, entretanto não existem algoritmos que determinam essas bases em tempo polinomial. Como o problema de encontrar o menor vetor não nulo é um problema NP-completo, estas reduções também o serão, ou seja, tais algoritmos polinomiais não existem salvo se $P=NP$. Para a redução LLL existe um algoritmo que determina uma base LLL em tempo polinomial. O principal resultado demonstrado neste capítulo é o seguinte: *Seja $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ uma base Minkowski-reduzida e seja \mathcal{F} o paralelepípedo fundamental determinado por esta base. Então as regiões de Voronoi dos vértices formam uma cobertura para \mathcal{F}* (Proposição 1.2.1). Em outras palavras, dado um ponto P dentro do paralelepípedo definido pelos vetores $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, o ponto do reticulado mais próximo de P é um dos vértices do paraleloto. Este resultado possibilitou a criação de um novo algoritmo para a redução de Minkowski.

Capítulo 2: Introduzimos o problema da codificação contínua fonte/canal e apresentamos inicialmente dois resultados contidos no artigo [47]: O primeiro descreve uma maneira de encontrar um bom valor para b , restrito a certas condições, tal que o reticulado-projeção determinado por $\mathbf{v} = (1, a, b) \in \mathbb{Z}^3$ tenha densidade que se aproxima da densidade máxima possível quando a norma de \mathbf{v} cresce. Outro resultado garante para cada a qual é o melhor b que gera o reticulado-projeção mais denso. Estabelecemos um resultado dual do primeiro (Teorema 2.4.3) e também descobrimos (Teorema 2.4.4) que o melhor b deve ser procurado entre o primeiro resultado do

artigo [47] e o resultado dual que encontramos.

A procura de vetores que dependem de mais parâmetros resultou em um teorema que engloba os resultados supra mencionados (Teorema 2.4.5 e Corolário 2.4.1). Através deste, estabelecemos uma família a três parâmetros de boas direções de projeção para vetores na dimensão 4 (Teorema 2.5.1). Nesta dimensão nem todos os parâmetros permitem a convergência ao reticulado tri-dimensional mais denso, o fcc. Entretanto existem escolhas cuja convergência vai para o ótimo (Corolário 2.5.1) sendo que as demais convergem a reticulados bem densos com densidade sendo no mínimo a densidade do reticulado $\mathcal{A}_2 \times \mathbb{Z}$.

Finalizamos o capítulo construindo um algoritmo que busca o vetor mínimo no caso específico de reticulados-projeção. Tal algoritmo leva em conta as regiões de Voronoi de \mathbb{Z}^n , o que faz com que seja exato e dependa linearmente das entradas do vetor \mathbf{v} .

II - Grafos Circulantes: No artigo [16] mostramos que grafos circulantes podem ser vistos como grafos em toros k -dimensionais. Graças a esta visão foi possível estabelecer uma conexão entre estes grafos e códigos, em especial códigos esféricos. O desenvolvimento do tema é feito através de dois capítulos.

Capítulo 3: Introduzimos inicialmente conceitos da teoria de grafos. Apresentamos grafos em toros k -dimensionais obtidos como quocientes de reticulados, utilizando para isto os resultados do artigo [14]. Descrevemos os grafos circulantes e sua realização como grafos obtidos do quociente de reticulados. O principal resultado deste capítulo estabelece uma conexão entre grafos circulantes e códigos esféricos (Proposição 3.5.1), isto é, cada grafo circulante pode ser visto como um código esférico. Um resultado recíproco (Proposição 3.5.2) também é demonstrado: cada código esférico dado por um grupo cíclico está associado a único grafo circulante, a menos de um isomorfismo.

Fechamos o capítulo falando sobre conexidade de grafos o que será útil na determinação do gênero que é estudado no próximo capítulo.

Capítulo 4: Este capítulo é dedicado ao problema da determinação do gênero de um grafo circulante, o qual é uma importante medida de sua complexidade. Iniciamos introduzindo a definição de gênero e exibindo alguns resultados conhecidos na literatura a respeito do gênero de grafos, como por exemplo limitantes gerais e a segunda fórmula de Euler. No artigo [33] é mostrado um resultado que classifica todos os grafos circulantes planares. Exceto os casos em que o grafo circulante é um grafo planar, ou um grafo completo ou ainda um grafo bibartido-completo, o gênero de um grafo circulante não era conhecido. Conseguimos estabelecer a classificação dos grafos circulantes toroidais (gênero 1), Proposições 4.2.2 e 4.2.3.

Em geral nos grafos circulantes, $\mathcal{C}_n(a_1, \dots, a_k)$, a maioria das faces devem ser compostas por 4 lados, com vértices: $P, P + a_i, P + a_i + a_j, P + a_j$, salvo as exceções onde: $a_i = \pm 2 a_j$, $a_i = \pm(a_j \pm a_m)$. Ambas as situações podem ser resumidas na seguinte fórmula: existem combinações da forma $a_i + a_j + a_m = 0$ onde a_i, a_j e $a_m \in \{\pm a_1, \dots, \pm a_k\}$. Nesses grafos circulantes pode acontecer que as seqüências $0, a_i, a_i + a_j, a_i + a_j + a_m = 0$ sejam triângulos quando mergulhamos o grafo numa superfície de menor gênero, como acontece nas condições dos teoremas que classificam os grafos planares e toroidais.

Desconsiderando esses casos, o gênero g de um grafo circulante deve satisfazer a seguinte desigualdade $g \geq \frac{nk-2n+4}{4}$. Exibimos no Teorema 4.3.2 uma classe relativamente grande de grafos circulantes que satisfazem à igualdade para k arbitrário. Como conseqüência deste resultado, temos o Corolário 4.3.1 que determina o gênero de supergrafos, obtidos pelo acréscimo de algumas diagonais a estes grafos.

Dentre as perspectivas futuras de pesquisa destacamos duas questões, que continuam em aberto nos dois temas pesquisados: Procedimentos análogos aos seguidos aqui, para determinar famílias de reticulados-projeção que convergem para um empacotamento ótimo, podem ser estendidos para dimensões ≥ 5 (pelo menos até dimensão 9 onde conhecemos os empacotamentos ótimos)? Quanto ao gênero de grafos circulantes, a busca será por uma classificação completa de todos os grafos satisfazendo $g = \frac{nk-2n+4}{4}$.

Parte I

Reticulados-Projeção

Capítulo 1

O Problema da Norma Mínima em Reticulados

Este capítulo aborda o problema de se encontrar o menor vetor não nulo de um reticulado. Iniciamos definindo os conceitos fundamentais da teoria de reticulados: base, matriz geradora, matriz de Gram, norma mínima e empacotamento. Falamos também a respeito de reduções de bases, ou seja, da procura de uma base para um reticulado cujos vetores tenham normas pequenas. Destacamos três reduções, com ênfase à redução de Minkowski. Esta redução, além de determinar o menor vetor não nulo do reticulado, possui diversas propriedades importantes. Conseguimos estabelecer uma nova propriedade geométrica, a qual permitiu a criação de um novo algoritmo para determinar a redução de Minkowski.

1.1 Reticulados e Empacotamentos

Nesta seção introduzimos o conceito de reticulados e suas propriedades dando ênfase aos tópicos distância mínima, densidade e quociente de reticulados que serão muito utilizados no decorrer do trabalho. As principais referências utilizadas foram [12], [10] e [37].

1.1.1 Reticulados

Definição 1.1.1. Seja $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ um conjunto linearmente independente em \mathbb{R}^m . Um *reticulado n -dimensional* $\mathcal{L}_{\mathcal{B}}$ é um conjunto de todas as combinações lineares inteiras de \mathcal{B} , i.e., $\mathcal{L}_{\mathcal{B}} = \{\mathbf{v} \in \mathbb{R}^m; \mathbf{v} = \sum_{i=1}^n k_i \mathbf{v}_i, k_i \in \mathbb{Z}\}$. O conjunto \mathcal{B} é dito *base* do reticulado $\mathcal{L}_{\mathcal{B}}$.

Para que não haja confusão com espaços vetoriais adotaremos a seguinte notação: $\langle S \rangle$ denota o espaço vetorial gerado por S , ou seja, o conjunto das combinações lineares dos elementos de S com coeficientes reais e $\langle S \rangle_{\mathbb{Z}}$ denota o reticulado gerado por S , ou seja, conjunto das combinações lineares dos elementos de S com coeficientes inteiros.

Naturalmente diferentes bases de \mathbb{R}^m podem definir o mesmo reticulado, na verdade isso ocorre se, e somente se, existe uma matriz $\mathcal{U}_{n \times n}$, integral invertível, isto é, com entradas inteiras e com determinante 1 (Unimodular), que leva uma base na outra. Como em espaços vetoriais a notação matricial aqui é bem-vinda.

Definição 1.1.2. Seja $\{\mathbf{v}_i = (v_{1i}, \dots, v_{mi})\}, i = 1, \dots, n$ uma base do reticulado $\mathcal{L}_{\mathcal{B}}$. Definimos *matriz geradora* \mathcal{M} como sendo a matriz cujas colunas são os vetores \mathbf{v}_i , i.e.,

$$\mathcal{M} = \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mn} \end{bmatrix}. \quad (1.1)$$

Nesta notação, os vetores do reticulado $\mathcal{L}_{\mathcal{B}}$ são vetores da forma $\mathcal{M}\mathbf{k}$, onde $\mathbf{k} \in \mathbb{Z}^n$. Qualquer reticulado está bem determinado se conhecemos uma matriz geradora. Em outras palavras, um reticulado n -dimensional é a imagem de \mathbb{Z}^n por uma transformação linear $\varphi: \mathbb{R}^n \rightarrow \mathbb{R}^m, m \geq n$, de posto máximo.

Observação 1.1.1. Quando o posto não é máximo a imagem de \mathbb{Z}^n pela φ pode não ser reticulado, como veremos no Capítulo 2, pois pode não ser um conjunto discreto.

Definição 1.1.3. O paralelepípedo (\mathcal{F}) constituído pelos pontos $\sum_{i=1}^n \theta_i \mathbf{v}_i$ com $\theta_i \in [0, 1)$ é dito *paralelepípedo fundamental* (ou *região fundamental*) do reticulado $\mathcal{L}_{\mathcal{B}}$.

Embora existam diferentes bases e, portanto diferentes regiões fundamentais para um reticulado $\mathcal{L}_{\mathcal{B}}$, o volume desta região é univocamente determinado por $\mathcal{L}_{\mathcal{B}}$. Isto não é surpreendente uma vez que duas bases diferem por uma matriz de determinante ± 1 , que está associado a uma transformação linear que preserva volumes n -dimensionais. Tal volume é dito *discriminante* do reticulado e denotaremos por $\text{vol}(\mathcal{L}_{\mathcal{B}})$. No caso em que $n = m$ tem-se $\text{vol}(\mathcal{L}_{\mathcal{B}}) = |\det(\mathcal{M})|$.

Definição 1.1.4. Sejam $\mathcal{L}_{\mathcal{B}}$ um reticulado, \mathcal{B} uma base para $\mathcal{L}_{\mathcal{B}}$ e \mathcal{V} o espaço vetorial gerado por esta base e $\mathbf{v} \in \mathcal{L}_{\mathcal{B}}$. Definimos a *região de Voronoi* de \mathbf{v} ($\text{vor}(\mathbf{v})$) como sendo a região que contém todos os pontos de \mathcal{V} que estão mais próximos de \mathbf{v} do que qualquer outro ponto \mathbf{u} do reticulado, i.e., $\text{vor}(\mathbf{v}) = \{\mathbf{x} \in \mathcal{V}; \|\mathbf{x} - \mathbf{v}\| \leq \|\mathbf{x} - \mathbf{u}\|, \forall \mathbf{u} \in \mathcal{L}_{\mathcal{B}}\}$

O volume da região de Voronoi é igual ao volume da região fundamental. Isto se deve ao fato que tanto a região fundamental quanto a região de Voronoi serem ladrilhos de \mathcal{V} sob o mesmo grupo

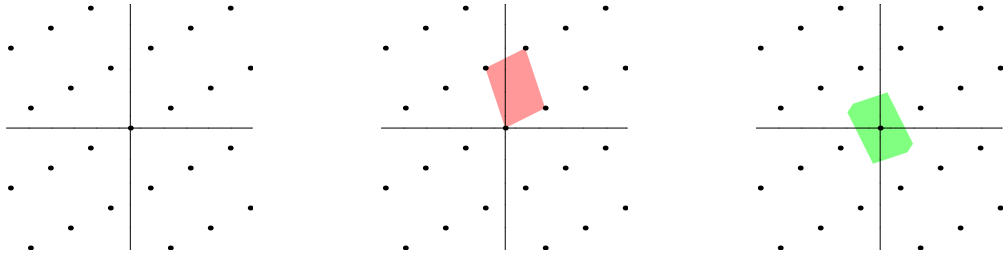


Figura 1.1: À esquerda um reticulado no plano, ao centro uma região fundamental deste e à direita a região de Voronoi de ponto $\mathbf{0}$.

de isometrias, grupo este composto pelas translações nas direções dos vetores \mathbf{v}_i ([34]). A Figura 1.1 ilustra estes conceitos.

Definição 1.1.5. Seja \mathcal{M} a matriz geradora do reticulado \mathcal{L}_B . A matriz $\mathcal{A} = \mathcal{M}^t \mathcal{M}$ é dita *matriz de Gram* do reticulado \mathcal{L}_B .

Observação 1.1.2. Note que a matriz de Gram do reticulado \mathcal{L}_B , nos fornece todos os produtos internos dos vetores da base, assim, podemos obter o reticulado a partir da sua matriz de Gram, a menos, é claro, de um movimento rígido (isometria), que é dado por uma matriz ortogonal.

Definição 1.1.6. O determinante da matriz \mathcal{A} , é chamado de *determinante* de \mathcal{L}_B .

No caso em que a matriz geradora \mathcal{M} é quadrada temos que: $\mathcal{A} = \det(\mathcal{M}^t \mathcal{M}) = \det(\mathcal{M}^t) \det(\mathcal{M}) = (\det(\mathcal{M}))^2$, ou seja, o quadrado do discriminante de \mathcal{L}_B é igual ao determinante de \mathcal{L}_B . Por isso, é comum definir o determinante de \mathcal{L}_B como sendo o quadrado do discriminante de \mathcal{L}_B ([12]).

Se aplicarmos uma transformação ortogonal do \mathbb{R}^m a um reticulado \mathcal{L}_B é razoável esperar que o reticulado obtido é essencialmente o mesmo, pois tal transformação não altera a estrutura geométrica do reticulado. Por isso cabe aqui a seguinte definição de equivalências de reticulados:

Definição 1.1.7. Sejam \mathcal{M} e \mathcal{M}' matrizes geradoras dos reticulados \mathcal{L}_B e \mathcal{L}'_B respectivamente. Dizemos que os reticulados são *equivalentes* se, e somente se, a seguinte relação é satisfeita $\mathcal{M}' = c\mathcal{O}\mathcal{M}\mathcal{U}$, onde $c \in \mathbb{R}, c > 0$, \mathcal{O} é uma matriz $m \times m$ ortogonal e \mathcal{U} é uma matriz unimodular (determinante igual a ± 1 e com entradas inteiras). Nestas condições denotamos por $\mathcal{L}_B \sim \mathcal{L}'_B$ esta equivalência, e quando $c = 1$ dizemos que os reticulados são congruentes e denotamos por $\mathcal{L}_B \simeq \mathcal{L}'_B$.

Exemplo 1.1.1. O reticulado no plano conhecido como reticulado hexagonal, ou \mathcal{A}_2 , pode ser caracterizado pela matriz geradora $\mathcal{M} = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$ ou pela matriz de Gram $\mathcal{A} = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}$. Mas

também pode ser caracterizado, a menos de equivalência, por $\mathcal{M}' = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 0 & -1 \end{bmatrix}$ ou pela matriz de Gram $\mathcal{A}' = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, como reticulado bidimensional no \mathbb{R}^3 . A Figura 1.2 ilustra o reticulado hexagonal e a região de Voronoi de $\mathbf{0}$.

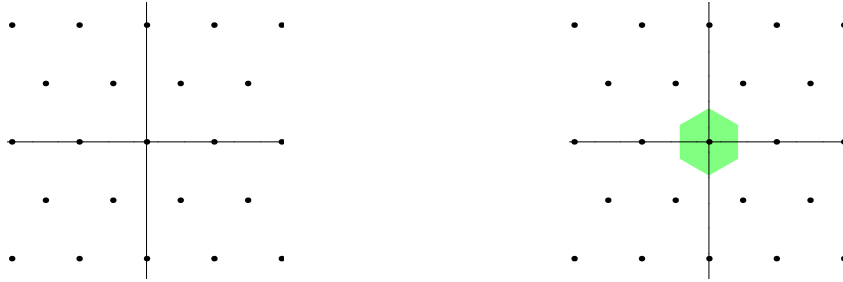


Figura 1.2: O reticulado hexagonal.

1.1.2 Empacotamento

Um empacotamento de esferas é uma distribuição de esferas disjuntas, que se tocam apenas no bordo, sobre um espaço vetorial real. Nestas condições, um bom empacotamento é aquele em que a taxa do volume ocupado pelas esferas numa porção do espaço está próxima do maior valor possível.

Definição 1.1.8. Um *empacotamento reticulado* é um empacotamento onde os centros das esferas determinam um reticulado.

Até a dimensão 3 já se sabe que, dentre os empacotamentos, os reticulados são melhores. A conjectura de que o melhor empacotamento para dimensão 3 é o reticulado *fcc*, face-centered cubic, foi feita por Johannes Kepler (1571 - 1630), Carl F. Gauss (1777 - 1855) provou parcialmente mostrando que ela era a melhor dentre os empacotamentos reticulados.

Em 1998 Thomas Hales, atualmente professor na universidade de Pittsburgh, anunciou que teve uma prova da conjectura de Kepler. A prova de Hales é uma prova pelo método de exaustão que envolve verificação de muitos casos individuais usando cálculos computacionais complexos. Os Referees disseram que a prova de Hales está “99% certa”. Assim a conjectura de Kepler está agora muito perto de transformar-se um teorema. Em 2003, T. Hales publicou um artigo descrevendo a parte não computacional desta prova, em detalhes. Ele trabalha em uma prova formal para remover qualquer resto de incerteza, ele também estima que uma prova formal tomará cerca de 20 anos

de trabalho. Mais detalhes sobre a conjectura de Kepler pode ser obtida na página do wikipedia em inglês: http://en.wikipedia.org/wiki/Kepler_conjecture, trabalhos de Hales sobre o assunto são [27, 28, 32, 29, 30, 31].

A partir da dimensão 4, dentre os empacotamentos conhecidos, em geral os melhores são os reticulados, mas existem dimensões em que um não reticulado é melhor. A figura abaixo ilustra três exemplos de empacotamento reticulados.

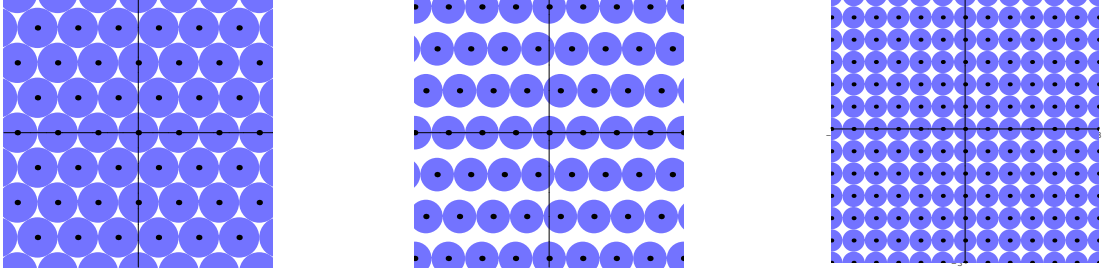


Figura 1.3: Ilustração dos empacotamentos: à esquerda o reticulado Hexagonal, ao centro o reticulado gerado por $\{(3/2, 0), (1/2, \sqrt{14}/2)\}$ e à direita o reticulado \mathbb{Z}^2

Definição 1.1.9. A *norma mínima* de um reticulado \mathcal{L}_B é a menor norma dentre os elementos não nulos de \mathcal{L}_B :

$$\mathcal{N}(\mathcal{L}_B) = \min\{\|\mathbf{x}\|; \mathbf{x} \in \mathcal{L}_B, \mathbf{x} \neq 0\} \quad (1.2)$$

Definição 1.1.10. A *densidade* (Δ) de empacotamento de um reticulado é a proporção do espaço ocupado pelas esferas

$$\begin{aligned} \Delta(\mathcal{L}_B) &= \frac{\text{vol}(\text{uma esfera})}{\text{vol}(\text{região fundamental})} \\ &= \frac{\text{vol}(S^n(\frac{\mathcal{N}(\mathcal{L}_B)}{2}))}{\det(\mathcal{L}_B)^{1/2}}, \text{ onde } S^n(\frac{\mathcal{N}(\mathcal{L}_B)}{2}) \text{ é a esfera } n\text{-dimensional de raio } \frac{\mathcal{N}(\mathcal{L}_B)}{2} \end{aligned}$$

A densidade de empacotamento nos diz o quão bom é o empacotamento. Observe que ela é invariante sob qualquer transformação linear ortogonal e dilatações. Portanto reticulados equivalentes tem a mesma densidade de empacotamento. Destacamos aqui dois reticulados que serão constantemente citados ao longo deste trabalho, e que possuem o melhor desempenho nas dimensões 2 e 3.

- * O reticulado hexagonal, \mathcal{A}_2 , gerado por $\mathbf{v}_1 = (1, -1, 0)$ e $\mathbf{v}_2 = (0, 1, -1)$
- * O reticulado fcc, gerado por $\mathbf{v}_1 = (1, -1, 0, 0)$, $\mathbf{v}_2 = (0, 1, -1, 0)$ e $\mathbf{v}_3 = (0, 0, 1, -1)$

As densidades desses dois reticulados são $\Delta_{\text{hexagonal}} = \frac{\pi}{\sqrt{12}} \simeq 0.90690$ e $\Delta_{\text{fcc}} = \frac{\pi}{3\sqrt{2}} \simeq 0.74048$. Como elas são as melhores possíveis sempre procuraremos reticulados que tenham densidade de empacotamento próximas desses valores.

Definição 1.1.11. A *densidade de centro* (δ) é a proporção do número de esferas pelo espaço ocupado por elas: $\delta(\mathcal{L}_{\mathcal{B}}) = \frac{\Delta(\mathcal{L}_{\mathcal{B}})}{\text{vol}(S^n(1))}$.

Ao compararmos reticulados na mesma dimensão o volume da esfera n -dimensional pode ser deixado de lado já que todas as densidades de empacotamento a têm como fator; sendo assim, trabalharemos com a densidade de centro. As densidades de centro dos reticulados hexagonal e fcc são $\delta_{\text{hexagonal}} = \frac{1}{\sqrt{12}} \simeq 0.28868$ e $\delta_{\text{fcc}} = \frac{\pi}{4\sqrt{2}} \simeq 0.17677$, respectivamente.

Notemos que, para determinar a densidade de empacotamento, precisamos encontrar dois valores: volume da região fundamental, o que em geral não é muito complexo, e a menor norma dentre os elementos não nulos do reticulado. Este último por sua vez é um problema computacionalmente muito complexo. Na próxima seção 1.2 falaremos a respeito deste problema.

1.1.3 Sub-reticulados e Quocientes de Reticulados

Em teoria de Códigos, o conceito de quociente de um reticulado por um sub-reticulado pode ser usado para rotulamento de sinais e na caracterização de códigos esféricos.

Definição 1.1.12. Sejam \mathcal{L} um reticulado e $\mathcal{L}' \subseteq \mathcal{L}$. Dizemos que \mathcal{L}' é *sub-reticulado* de \mathcal{L} se \mathcal{L}' é um reticulado.

Como em espaços vetoriais e grupos, aqui também pode-se definir quocientes. No caso dos reticulados, quando quocientamos reticulados de mesma dimensão, a estrutura obtida pode ser considerada tanto um grafo especial ou ainda um grupo finito de pontos, ou um misto dos dois, um grafo rotulado por um grupo. Para não haver confusões posteriores fixaremos a seguinte notação: Seja \mathcal{L}' um sub-reticulado do reticulado \mathcal{L} (de mesma dimensão), denotaremos $\Gamma = \frac{\mathcal{L}}{\mathcal{L}'}$ como o grupo finito de pontos, a saber $\frac{\text{vol}(\mathcal{L}')}{\text{vol}(\mathcal{L})}$ pontos, gerados por alguma base de \mathcal{L} ; Nas mesmas condições mas fixando uma base \mathcal{B} de \mathcal{L} , denotaremos o reticulado $\mathcal{G}_{\mathcal{B}} = \frac{\mathcal{L}_{\mathcal{B}}}{\mathcal{L}'}$ como sendo o grafo de vértices $\frac{\mathcal{L}}{\mathcal{L}'}$ e cuja arestas são dadas pelos vetores da base \mathcal{B} , ou seja, dois vértices estão conectados se eles diferem por algum elemento de \mathcal{B} .

Na verdade, o quociente de reticulados é um módulo sobre o anel dos inteiros \mathbb{Z} : onde temos a parte *livre* que constitui um reticulado, no sentido em que trabalhamos, e a parte da *torção* que pode ser visto como um toro plano n -dimensional.

Quando o quociente é entre reticulados de mesma dimensão, esse quociente possui propriedades geométricas muito interessantes as quais utilizamos em teoria de códigos, como veremos nos próximos capítulos. No Capítulo 2 abordamos um problema de maximizar a densidade de empacotamento associada a um quociente de reticulados. Isto permite relacionar uma distribuição de pontos no \mathbb{R}^n com uma distribuição de pontos no toro planar n -dimensional mergulhado isometricamente na esfera do \mathbb{R}^{2n} . Na Parte II veremos que tais quocientes estão associados a grafos circulantes os quais têm sido objeto de grande interesse na área de computação paralela.

1.2 Redução de Minkowski

Estamos interessados em encontrar o vetor de menor norma num reticulado n -dimensional.

Sob certas condições, que a matriz de Gram deve satisfazer, podemos assegurar que o primeiro vetor da base é o vetor de menor norma procurado. Tal método é conhecido como *Redução de Minkowski*. Desejamos encontrar uma base (Minkowski-reduzida) $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ do reticulado n -dimensional \mathcal{L} , de tal forma que para cada $t, 1 \leq t \leq n$ nós tenhamos que:

$$\langle \mathbf{v}_t, \mathbf{v}_t \rangle \leq \langle \mathbf{v}, \mathbf{v} \rangle, \quad (1.3)$$

para todo vetor $\mathbf{v} \in \mathcal{L}$ de tal forma que $\mathbf{v}_1, \dots, \mathbf{v}_{t-1}, \mathbf{v}$ pode ser estendido a uma base de \mathcal{L} . Isso implica, como é mostrado em [12], que a matriz de Gram satisfazer as condições:

$$0 < a_{11} \leq a_{22} \leq \dots \leq a_{nn}. \quad (1.4)$$

$$2 \left(\sum_{s \in S} \epsilon_s a_{st} - \sum_{\substack{r, s \in S \\ r < s}} \epsilon_r \epsilon_s a_{rs} \right) \leq \sum_{s \in S} a_{ss}, \quad (1.5)$$

onde $S \subset \{1, 2, \dots, t-1\}$ e $\epsilon_i \pm 1$.

Observação 1.2.1. Para $n \leq 4$, vale a recíproca, ou seja, restringindo a condição $\epsilon_i = \pm 1$, teremos uma base Minkowski-reduzida. A prova disto encontra-se em [8].

Provemos que a condição (1.3) implica às condições (1.4) e (1.5). É claro que (1.4) decorre de (1.3); agora, fixado t tome um vetor $\mathbf{v} = \mathbf{v}_t - \sum_{s \in S} \epsilon_s \mathbf{v}_s$, com S, ϵ_i como acima; então

$$\begin{aligned} \langle \mathbf{v}_t, \mathbf{v}_t \rangle \leq \langle \mathbf{v}, \mathbf{v} \rangle &\iff \langle \mathbf{v}_t, \mathbf{v}_t \rangle \leq \langle \mathbf{v}_t - \sum_{s \in S} \epsilon_s \mathbf{v}_s, \mathbf{v}_t - \sum_{s \in S} \epsilon_s \mathbf{v}_s \rangle \\ &\iff \langle \mathbf{v}_t, \mathbf{v}_t \rangle \leq -2 \left(\sum_{s \in S} \epsilon_s a_{st} - \sum_{\substack{r, s \in S \\ r < s}} \epsilon_r \epsilon_s a_{rs} \right) + \sum_{s \in S} a_{ss} \end{aligned}$$

$$\Leftrightarrow 2 \left(\sum_{s \in S} \epsilon_s a_{st} - \sum_{\substack{r, s \in S \\ r < s}} \epsilon_r \epsilon_s a_{rs} \right) \leq \sum_{s \in S} a_{ss}. \quad (1.6)$$

Evidentemente \mathbf{v} foi escolhido de maneira que $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{t-1}, \mathbf{v}$ gera o mesmo sub-reticulado de \mathcal{L} que $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_t$.

J. H. Conway e N. J. Sloane fazem a seguinte observação em [12]: “Embora esse método garanta que \mathbf{v}_1 seja o vetor mais próximo da origem, e portanto o que realiza a distância mínima, ele não deixa a matriz de Gram na forma desejada de modo computacionalmente eficiente.” Motivados a encontrar uma maneira de obter a redução de Minkowski acabamos por construir um algoritmo de ordem exponencial que calcula a base de Minkowski, tal algoritmo será descrito em detalhes na próxima seção. Naturalmente já são conhecidos outros algoritmos para este cálculo e comentaremos sobre eles na seção 1.4.

1.2.1 Vetores Mínimos em \mathcal{L}^n

Iniciamos a construção do algoritmo com o caso de reticulados bi-dimensional considere $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$ base para o reticulado \mathcal{L} , com $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$. \mathcal{B} não será uma base de Minkowski apenas se não satisfizer a condição (1.5) que, para $n = 2$, se reduz a $t = 2$ e $S = \{1\}$. Assim, para que \mathcal{B} não seja Minkowski é necessário que a razão $\frac{|\langle \mathbf{v}_1, \mathbf{v}_2 \rangle|}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} > \frac{1}{2}$. E quando isso ocorre podemos trocar \mathbf{v}_2 pelo vetor $\mathbf{v}_2 - \left[\frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \right] \mathbf{v}_1$ ($[x]$ é o inteiro mais próximo de x) neste caso. Essa troca equivale a multiplicar a matriz geradora pela matriz unimodular

$$\begin{bmatrix} 1 & -m \\ 0 & 1 \end{bmatrix}.$$

Vamos analisar os vetores $\mathbf{v} = \mathbf{v}_2 - m \mathbf{v}_1$ e provar que $m = \left[\frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \right]$ é a melhor escolha.

Decompondo \mathbf{v} na base $\{\mathbf{v}_1, \mathbf{v}_1^\perp\}$ temos

$$\mathbf{v} = \left(\frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} - m \right) \mathbf{v}_1 + \frac{\langle \mathbf{v}_1^\perp, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1^\perp, \mathbf{v}_1^\perp \rangle} \mathbf{v}_1^\perp.$$

Como a base é ortogonal, temos.

$$\|\mathbf{v}\|^2 = \left| \frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} - m \right|^2 \|\mathbf{v}_1\|^2 + \left| \frac{\langle \mathbf{v}_1^\perp, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1^\perp, \mathbf{v}_1^\perp \rangle} \right|^2 \|\mathbf{v}_1^\perp\|^2.$$

Então, para minimizar $\|\mathbf{v}\|$ basta minimizar $\left| \frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} - m \right|$, ou seja tomar $m = \left[\frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \right]$.

Em outras palavras, *devemos escolher o vetor $\mathbf{u} \in \langle \mathbf{v}_1 \rangle_{\mathbb{Z}}$ mais próximo da projeção ortogonal de \mathbf{v}_2 no espaço gerado por \mathbf{v}_1 , i.e., encontrar o vetor \mathbf{u} do reticulado gerado por $\langle \mathbf{v}_1 \rangle_{\mathbb{Z}}$ cuja região de Voronoi contém a projeção ortogonal de \mathbf{v}_2 na direção deste reticulado.* Assim, a base estará Minkowski-reduzida quando $\mathbf{u} = \mathbf{0}$ ($m = 0$), ou ainda a projeção de \mathbf{v}_2 na direção de \mathbf{v}_1 está na região de Voronoi do vetor nulo. A Figura 1.4 ilustra esse raciocínio.

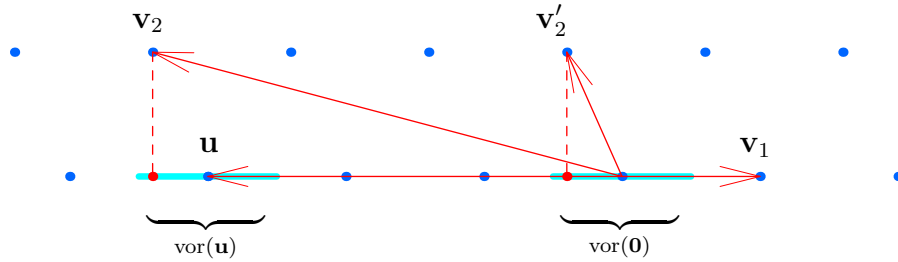


Figura 1.4: Idéia geométrica da redução de Minkowski para dimensão 2.

Com esta nova terminologia estendemos o resultado para dimensões maiores. Seja $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ base para o reticulado \mathcal{L} . Seja $\mathbf{v} = \mathbf{v}_{i+1} - \mathbf{u}$, onde $1 < i \leq n - 1$ e $\mathbf{u} \in \mathcal{L}^i = \langle \mathbf{v}_1, \dots, \mathbf{v}_i \rangle$. A base será Minkowski-reduzida se a projeção de \mathbf{v}_{i+1} na direção do reticulado \mathcal{L}^i está na região de Voronoi (reticulado \mathcal{L}^i) do vetor nulo para todo índice i , caso isso não ocorra existirá um vetor não nulo $\mathbf{u} \in \mathcal{L}^i$ tal que $\|\mathbf{v}\| = \|\mathbf{v}_i - \mathbf{u}\| < \|\mathbf{v}_i\|$.

Como encontrar o ponto de \mathcal{L}^i mais próximo da projeção do vetor \mathbf{v}_{i+1} ?

Afirmamos que se $\{\mathbf{v}_1, \dots, \mathbf{v}_i\}$ for uma base de Minkowski então o vetor $\mathbf{u} \in \mathcal{L}^i$ mais próximo da projeção de \mathbf{v}_{i+1} é um dos vértices do paralelepípedo contendo esta projeção e cujas arestas são determinadas pelos vetores $\{\mathbf{v}_1, \dots, \mathbf{v}_i\}$.

Admitamos que isso seja válido, veremos como fica o algoritmo na próxima seção.

1.2.2 Proposta de Algoritmo para Redução de Minkowski

Dada a base $\{\mathbf{v}_1, \dots, \mathbf{v}_i\}$, para obter a redução de Minkowski procedemos de maneira indutiva na dimensão, iniciando em $n = 2$. Se $\{\mathbf{v}_1, \mathbf{v}_2\}$ não for Minkowski-reduzida trocamos \mathbf{v}_2 por $\mathbf{v}'_2 = \mathbf{v}_2 - \mathbf{u}$ onde \mathbf{u} é o vetor de $\mathcal{L}^1 = \langle \mathbf{v}_1 \rangle$ mais próximo de \mathbf{v}_2 (ou equivalentemente da projeção de \mathbf{v}_2 sob \mathcal{L}^1). Caso \mathbf{v}'_2 tenha menor norma do que \mathbf{v}_1 , trocamos \mathbf{v}_1 por \mathbf{v}_2 e repetimos o procedimento. Suponhamos agora que tenhamos deixado $\{\mathbf{v}'_1, \dots, \mathbf{v}'_k\}$ Minkowski-reduzido; projetamos ortogonalmente \mathbf{v}_{k+1} sob o espaço $\mathcal{L}^k = \langle \mathbf{v}'_1, \dots, \mathbf{v}'_k \rangle$, tome $\mathbf{u} \in \mathcal{L}^k$ mais próximo desta projeção e trocamos \mathbf{v}_{k+1} por $\mathbf{v}'_{k+1} = \mathbf{v}_{k+1} - \mathbf{u}$. Caso \mathbf{v}'_{k+1} tenhamos norma estritamente menor que a norma de \mathbf{v}'_i para algum $i \leq k$, seja i_0 o menor índice com essa propriedade; reordenamos a base obtendo o conjunto $\{\mathbf{v}'_1, \dots, \mathbf{v}'_{i_0-1}, \mathbf{v}'_{k+1}, \mathbf{v}'_{i_0}, \dots, \mathbf{v}'_k\}$ e voltamos para o procedimento na

dimensão i_0 . Já que, por hipótese $\{\mathbf{v}'_1, \dots, \mathbf{v}'_{i_0-1}\}$ é Minkowski-reduzida, caso não exista nenhum índice como acima então afirmamos que $\{\mathbf{v}'_1, \dots, \mathbf{v}'_{k+1}\}$ é Minkowski-reduzida. De fato, se não fosse Minkowski-reduzida existiria um vetor $\mathbf{w} \in \mathcal{L}^{k-1}$ tal que $\mathbf{v}'_{k+1} - \mathbf{w}$ teria norma menor que \mathbf{v}'_n , o que é absurdo pois já o tomamos como sendo minimizador.

Esquematizando o algoritmo:

- 1 Entrada: $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$;
- 2 $L = 1$;
- 3 Enquanto $L < n$ faça
 - 3.1 $\mathbf{v}'_{L+1} = \mathbf{v}_{L+1} - \mathbf{u}$, onde $\mathbf{u} \in \mathcal{L}^L$ minimiza $\mathbf{v}_{L+1} - \mathbf{u}$ na norma euclidiana;
 - 3.2 Seja i_0 o menor índice tal que $\|\mathbf{v}_{i_0}\| > \|\mathbf{v}'_{L+1}\|$;
 - 3.3 Se $i_0 < L + 1$ então $L = i_0$ senão $L = L + 1$;
- 4 Saída $\{\mathbf{v}'_1, \dots, \mathbf{v}'_n\}$

O fato de estarmos trabalhando com um conjunto discreto garante que só há um número finito de vetores dentro da bola de raio $\|\mathbf{v}_i\|$ para todo índice i . Assim, o algoritmo não poderá entrar num loop infinito, pois, isto que significaria uma infinidade de vetores com norma menor que $\|\mathbf{v}_i\|$. Em outras palavras, para cada índice i , existem apenas um número finito de possibilidades de troca de vetores \mathbf{v}_i por outro \mathbf{v}'_i de menor norma.

O parâmetro L no loop do item 3 não é estritamente crescente ele pode diminuir depois de uma iteração, como é frisado no subitem 3.3.

A complexidade deste algoritmo é exponencial no caso mais complexo. Pois, no item 3.1, este algoritmo resolve um sistema linear correspondendo a solução contínua do problema: minimizar $\mathbf{v}_{L+1} - \mathbf{u}$, com $\mathbf{u} \in \langle \mathcal{L}^L \rangle$, obtendo um vetor \mathbf{u}_{cont} . Em seguida, o algoritmo considera o conjunto de todos os vértices, da região fundamental que contém esta solução \mathbf{u}_{cont} , e toma $u \in \mathcal{L}^L$ o vértice mais próximo de \mathbf{u}_{cont} , comparando um total de 2^L vértices. Portanto a complexidade do algoritmo cresce exponencialmente com a dimensão.

1.2.3 Relação entre as Regiões de Voronoi e Fundamental

Proposição 1.2.1. *Seja $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ uma base Minkowski-reduzida e seja \mathcal{F} o paralelepípedo fundamental determinado por esta base. Então as regiões de Voronoi dos vértices de \mathcal{F} formam uma cobertura para \mathcal{F} .*

Demonstração: Seja $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ uma base de Minkowski para o reticulado \mathcal{L}^n . Queremos mostrar que as regiões de Voronoi dos vértices da região fundamental $\mathcal{F} \subset \mathcal{L}^n$ cobrem esta região, ou seja, $\mathcal{F} \subset \bigcup_{\mathbf{x}_k} \text{vor}(\mathbf{x}_k)$, onde \mathbf{x}_k é um vértice qualquer de \mathcal{F} e $\text{vor}(\mathbf{x}_k)$ a sua região de Voronoi.

Suponhamos que região fundamental \mathcal{F} seja determinada pelos vetores mínimos $\mathbf{v}_1, \dots, \mathbf{v}_n$.

Passo 1) $n = 1$ não há o que fazer.

Passo 2) Suponhamos válido para dimensões estritamente menores n . Então seja $\mathbf{a} \in \mathcal{F}$ e suponhamos que $\mathbf{u} = \sum_i m_i \mathbf{v}_i, m_i \in \mathbb{Z}$ esteja mais perto de $\mathbf{a} = \sum_i \alpha_i \mathbf{v}_i, \alpha_i \in [0, 1)$, do que qualquer outro vetor em \mathcal{L}^n . Sem perda de generalidade podemos supor todos os coeficientes $m_i \geq 0$.

Se $m_k = 0$, para algum $k = 1, \dots, n$ projetamos a ortogonalmente sobre o reticulado $\mathcal{L}_k^{n-1} = \langle \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \setminus \{\mathbf{v}_k\} \rangle$. Tal projeção (P) resulta no vetor $P(\alpha_k \mathbf{v}_k) + \sum_{i=1, i \neq k}^n \alpha_i \mathbf{v}_i$. Já sabemos que $P(\mathbf{v}_k) \in \text{vor}_{\mathcal{L}^{k-1}}(0) \subseteq \mathcal{L}^{k-1}$, além disso, pode-se concluir que $P(\mathbf{v}_k) \in \text{vor}_{\mathcal{L}_k^{n-1}}(\mathbf{0}) \subseteq \mathcal{L}_k^{n-1}$, pois, se $\mathbf{v}_k \in \text{vor}(y)$ com $\sum_{j=k+1}^n \xi \mathbf{v}_j$ então $\|\mathbf{v}_k\| > \|\mathbf{v}_k - y\|$ contrariando a minimalidade de \mathbf{v}_k na definição da redução de Minkowski. E assim, o mesmo deve valer para $P(\alpha_k \mathbf{v}_k)$. Logo a soma de $\alpha_i \mathbf{v}_i$ a $P(\alpha_k \mathbf{v}_k)$ pode no máximo levar esta projeção à região de Voronoi do vértice $\mathbf{0} + \mathbf{v}_i$. Logo, os demais coeficientes também são 0 ou 1.

Se $m_k = 1$, para algum $k = 1, \dots, n$ projetamos a ortogonalmente sobre o reticulado $\mathcal{L}_k^{n-1} + \mathbf{v}_k = \langle \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \setminus \{\mathbf{v}_k\} \rangle + \mathbf{v}_k$. Tal projeção equivale a projetar $\tilde{\mathbf{a}}$ ortogonalmente sobre o reticulado \mathcal{L}_k^{n-1} , onde $\tilde{\alpha}_k = 1 - \alpha_k$ e $\tilde{\alpha}_i = \alpha_i, \forall i \neq k$. E a prova segue idêntica ao parágrafo anterior.

Se $m_k = d$, para algum $k = 1, \dots, n$ é o menor coeficiente de \mathbf{u} projetamos a ortogonalmente sobre o reticulado $\mathcal{L}_k^{n-1} + d \mathbf{v}_k = \langle \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \setminus \{\mathbf{v}_k\} \rangle + d \mathbf{v}_k$. Tal operação equivale a projetar $\tilde{\mathbf{a}}$, onde $\tilde{\alpha}_k = d - \alpha_k$ e $\tilde{\alpha}_i = \alpha_i, \forall i \neq k$, ortogonalmente sobre o reticulado \mathcal{L}_k^{n-1} . Pelo que vimos acima $P(\tilde{\alpha}_k \mathbf{v}_k) \in \text{vor}_{\mathcal{L}_k^{n-1}}(0)$ e os coeficientes de $P((d-1) \mathbf{v}_k)$ não excederão $d-1$. Assim, a soma de $P(\tilde{\alpha}_k \mathbf{v}_k)$ com $P((d-1) \mathbf{v}_k) + \sum_{i, i \neq k} \alpha_i \mathbf{v}_i$ não pertencerão a regiões de Voronoi com coeficientes superiores a d . Portanto $P(\tilde{\mathbf{a}}) \in \text{vor}_{\mathcal{L}^{k-1}}(d \sum_{i, i \neq k} \mathbf{v}_i)$. Devemos mostrar agora que $d < 2$. Isso é trivial, pois, o hiperplano mediatriz do segmento que une $\mathbf{0}$ a $d \sum_{i, i \neq k} \mathbf{v}_i$ deixa a no semi-espaço contendo o vetor nulo, sempre que $d > 1$, logo $d \leq 1$.

Portanto $m_i \in \{0, 1\}, \forall i$, o que conclui a demonstração. ■

1.3 Outras Formas de Redução

Dada a complexidade algorítmica para encontrar a forma de Minkowski foram desenvolvidos outros tipos de redução como seguem abaixo. O artigo [2] dá uma boa visão sobre as reduções existentes. Outra referência é a tese de B. A. LaMacchia [35], nela a ênfase está no “Seysen’s

algorithm” a qual não exploramos neste trabalho.

Definição 1.3.1 (Redução de Korkin-Zolotarev). Uma base $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ é dita *Korkin-Zolotarev reduzida* se satisfaz as seguintes condições:

1. \mathbf{v}_1 é o menor vetor não nulo em \mathcal{L} ;
2. Para $2 \leq i \leq n$, seja \mathcal{V}_i o subespaço $(i-1)$ -dimensional gerado pela base $\{\mathbf{v}_1, \dots, \mathbf{v}_{i-1}\}$ e seja \mathcal{V}_i^\perp o complemento ortogonal de \mathcal{V}_i em \mathbb{R}^n . Finalmente, seja $P_i(\mathcal{V})$ a projeção ortogonal de \mathcal{V} sobre \mathcal{V}_i^\perp , algoritmo de \mathbf{v}_i é tal que $P_i(\mathbf{v}_i)$ é o menor vetor não nulo em $P_i(\mathcal{L})$.
3. Condição redução do tamanho. Para $1 \leq i < j \leq n$,

$$\|\langle P_i(\mathbf{v}_i), P_i(\mathbf{v}_j) \rangle\| \leq \frac{1}{2} \|P_i(\mathbf{v}_i)\|^2,$$

onde $P_1(\mathbf{x}) = \mathbf{x}$.

Definição 1.3.2 (Redução de Lenstra-Lenstra-Lovász). Uma base \mathcal{B} é LLL-reduzida se:

1. $|\mu_{ij}| \leq \sqrt{\frac{\alpha-1}{\alpha}}$ para $1 \leq j < i \leq n$, onde $\alpha = \frac{1}{\eta - 1/4}$
2. $\|\mathbf{v}_i^* + \mu_{i,i-1} \mathbf{v}_{i-1}^*\|^2 \geq \eta \|\mathbf{v}_{i-1}^*\|^2$ para $1 < i \leq n$, onde $\mu_{i,j} = \frac{\langle \mathbf{v}_i, \mathbf{v}_j^* \rangle}{\langle \mathbf{v}_j^*, \mathbf{v}_j^* \rangle}$,
 $\mathcal{B}^* = (\mathbf{v}_1^*, \dots, \mathbf{v}_n^*)$ é obtida do processo de ortogonalização de Gram-Schmidt da base \mathcal{B} , e o parâmetro $\eta \in (1/4, 1)$

Ou equivalentemente trocando 2. por

$$2.' \|\mathbf{v}_i^*\|^2 \geq (\eta - \mu_{i,i-1}^2) \|\mathbf{v}_{i-1}^*\|^2$$

Teorema 1.3.1. [10] Seja $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ uma base LLL-reduzida com $\eta = 3/4$. Então:

$$\det(\mathcal{L}) \leq \prod_{i=1}^n \|\mathbf{v}_i\| \leq 2^{n(n-1)/4} \det(\mathcal{L}), \quad (1.7)$$

$$\|\mathbf{v}_j\| \leq 2^{(i-1)/2} \|\mathbf{v}_i^*\|, \text{ se } 1 \leq j < i \leq n, \quad (1.8)$$

$$\|\mathbf{v}_1\| \leq 2^{(n-1)/4} \det(\mathcal{L})^{1/n}, \quad (1.9)$$

$$\|\mathbf{v}_1\| \leq 2^{(n-1)/2} \|\mathbf{x}\|, \forall \mathbf{x} \in \mathcal{L} \setminus \{0\}, \quad (1.10)$$

$$\|\mathbf{v}_j\| \leq 2^{(n-1)/2} \max_{1 \leq i \leq t} \|\mathbf{x}_i\|, \{\mathbf{x}_i\}, \text{ linearmente independente e } 1 \leq j \leq t. \quad (1.11)$$

Para η qualquer, o 2 das expressões acima deve ser trocado por $\alpha = \frac{1}{\eta - 1/4}$ e utilize $\mu_{i,j}^2 \leq (\alpha - 1)/\alpha$. O $\det(\mathcal{L})$ é o determinante da matriz cujas colunas são formadas pelos vetores \mathbf{v}_i .

1.3.1 Relação entre as Reduções

Os métodos de Minkowski e Korkin-Zolotarev são reduções ótimas, no sentido que a base reduzida contém o vetor mínimo do reticulado. Minkowski também é ótima no sentido da decodificação de pontos interiores a vértices da região fundamental que os contém. Como vimos na Proposição 1.2.1. Infelizmente não existem algoritmos que a encontra em tempo polinomial, salvo algoritmos de ordem exponencial. A seguir exibimos algumas diferenças entre os métodos através de exemplos.

$$\mathcal{B} = \left\{ \mathbf{e}_1, \frac{1}{2} \mathbf{e}_1 + \mathbf{e}_2, -\frac{1}{2} \mathbf{e}_2 + 2 \mathbf{e}_3 \right\} \quad (1.12)$$

é uma base Minkowski-reduzida do reticulado $\mathcal{L} = \langle \mathcal{B} \rangle$, enquanto

$$\mathcal{B} = \left\{ \mathbf{e}_1, \frac{1}{2} \mathbf{e}_1 + \mathbf{e}_2, \frac{1}{2} \mathbf{e}_1 + \frac{1}{2} \mathbf{e}_2 + 2 \mathbf{e}_3 \right\} \quad (1.13)$$

é uma base Korkin-Zolotarev reduzida para \mathcal{L} , mas não Minkowski. Ou seja, uma base pode ser Korkin-Zolotarev mas não ser Minkowski e vice-versa.

Já o método LLL tem um algoritmo em tempo polinomial que determina uma base na forma LLL-reduzida. Mas é conhecido como um método sub-ótimo, veja os exemplos a seguir:

1. O mínimo pode não ser elemento da base LLL para dimensões $n \geq 3$. A base LLL-reduzida

$$\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\} = \left\{ (1, 0, 0), \left(\frac{1}{2}, \frac{3}{4}, 0 \right), \left(-\frac{1}{2}, \frac{3}{8}, \frac{3}{4} \right) \right\}, \quad (1.14)$$

têm normas aproximadamente

$$\{1., 0.901388, 0.976281\}, \quad (1.15)$$

mas a norma do vetor $\mathbf{v}_1 + \mathbf{v}_3 - \mathbf{v}_2$ é 0.838525.

2. Os vértices de um paralelepípedo fundamental definido pela base LLL podem não ser a melhor decodificação de seus pontos interiores: isso vale para dimensões $n \geq 4$. A base

$$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\} = \left\{ \mathbf{e}_1, \frac{1}{2} \mathbf{e}_1 + \frac{\sqrt{2}}{2} \mathbf{e}_2, \frac{1}{2} \mathbf{e}_1 + \frac{\sqrt{2}}{4} \mathbf{e}_2 + \frac{1}{2} \mathbf{e}_3, \frac{1}{2} \mathbf{e}_1 + \frac{1}{4} \mathbf{e}_3 + \frac{\sqrt{2}}{4} \mathbf{e}_4 \right\} \quad (1.16)$$

está na forma LLL-reduzida. Considere o ponto $\mathbf{x} = \frac{\mathbf{v}_1}{2} + \mathbf{v}_4$. O ponto do reticulado mais próximo de \mathbf{x} é $\mathbf{v} = 2\mathbf{v}_4$, com distância $\sqrt{3}/4$ enquanto o vértice do paralelepípedo mais próximo de \mathbf{x} está a uma distância igual a $2/4$. Logo uma base LLL-reduzida não é ótima, entretanto note que o erro não é muito grande mas tende a aumentar quando a dimensão aumenta.

Observação 1.3.1. Um detalhe interessante que vale a pena frisar é que a grande fraqueza do algoritmo *LLL* está no fato do algoritmo comparar o vetor apenas com o seu anterior, ou seja, a redução é feita basicamente entre \mathbf{v}_{i+1} e \mathbf{v}_i , isso faz com que uma base como a do Exemplo 1 acima ao ser processada pelo algoritmo *LLL* não se modifique. Entretanto se ordenarmos esta base pela ordem de norma o *LLL* apresentaria mudanças significativas a resposta seria a base

$$\left\{ \left(\frac{1}{2}, \frac{3}{4}, 0 \right), \left(0, -\frac{3}{8}, \frac{3}{4} \right), \left(-\frac{1}{2}, \frac{3}{4}, 0 \right) \right\} \quad (1.17)$$

que é uma base Minkowski a menos da permutação dos dois primeiros vetores.

1.4 Experimentos com os Algoritmos: Minkowski e LLL

Nesta seção exibiremos alguns resultados obtidos da implementação do nosso algoritmo para redução de Minkowski. Fizemos uma programação simbólica através do software Mathematica.

A Tabela 1.4 descreve o tempo (em segundos), num micro-computador 2.8MHz e 1GB de memória RAM, que o nosso algoritmo leva para testar que a base canônica do reticulado \mathcal{A}_n , base esta constituída dos vetores $\mathbf{v}_i = \{0, \dots, \underbrace{1}_{i^{\text{a}}}, -1, \dots\} \subseteq \mathbb{R}^{n+1}$ está na forma Minkowski-reduzida:

Dimensão	Tempo (Seg)	Dimensão	Tempo (Seg)	Dimensão	Tempo (Seg)
2	0.	10	0.062	18	13.844
3	0.	11	0.125	19	28.000
4	0.	12	0.219	20	56.719
5	0.	13	0.438	21	114.078
6	0.	14	0.859	22	232.14
7	0.016	15	1.687	23	485.031
8	0.031	16	3.391	24	957.031
9	0.032	17	7.437	25	1915.16

Observamos que a partir da dimensão 8 os tempos começam a dobrar com o incremento da dimensão, isso se deve ao fato de que nosso algoritmo, ao fazer uma redução numa dimensão n ,

compara para cada $2 < i \leq n$ um total 2^{i-1} normas, ou seja, um total de $\sum_{i=3}^n 2^{i-1} = 2^n - 2^3$ que na dimensão 20 resulta uma comparação de no mínimo de 1048568 normas e na dimensão 25 de 33554424 normas.

Motivados pelo problema da projeção, exibimos reduções de Minkowski para reticulados que são obtidos da projeção ortogonal de \mathbb{Z}^n na direção de um vetor $\mathbf{v} \in \mathbb{Z}^n$ o que resulta num reticulado de dimensão $n - 1$.

Uma vez que o algoritmo *LLL* processa reduções em tempo polinomial, podemos utilizá-lo para fazermos um pré-processamento da base, o que reduzirá o tempo de processamento da redução de Minkowski, como podemos ver na tabela abaixo. Entretanto pela Observação 1.3.1 aplicar o *LLL* uma vez não é muito eficiente se a base não está ordenada pela ordem da norma, sendo assim após aplicar o *LLL* vamos ordenar a base e aplicá-lo mais uma vez, e repetiremos tal procedimento até que o algoritmo *LLL* não tenha mas nenhum efeito, a este procedimento daremos o nome de $k \times LLL$.

Vejam os exemplos de desempenho dos algoritmos $k \times LLL$, Minkowski, $k \times LLL$ + Minkowski (Minkowski pré-processado pelo $k \times LLL$) e o algoritmo RV que foi desenvolvido especificamente para reticulados do tipo projeção, o que descreveremos no próximo capítulo:

Vetores	$k \times LLL$	Minkowski	$k \times LLL$ + Minkowski	RV	$\mathcal{N}(\mathcal{L})$
$\mathbf{v}_1 \in \mathbb{Z}^7$	0.016	0.093	0.016	3.141	0.01128
$\mathbf{v}_2 \in \mathbb{Z}^7$	0.016	0.125	0.031	10.281	0.00874
$\mathbf{v}_3 \in \mathbb{Z}^{16}$	0.062*	52.922	11.063	0.437	0.37950
$\mathbf{v}_4 \in \mathbb{Z}^{19}$	0.406	NA	141.625	NA	0.08767
$\mathbf{v}_5 \in \mathbb{Z}^{21}$	0.703	NA	416.344	NA	0.10222
$\mathbf{v}_6 \in \mathbb{Z}^{22}$	0.203*	NA	1262.55	1.547	0.60243

(1.18)

onde os vetores \mathbf{v}_i que determinam o reticulado-projeção são:

$$\mathbf{v}_1 = (2725, 15762, 45807, 51718, 51941, 61052, 91458),$$

$$\mathbf{v}_2 = (43006, 75987, 90538, 188028, 188576, 214076, 279085),$$

$$\mathbf{v}_3 = (1050, 1063, 1214, 1359, 1749, 2434, 2633, 2765, 2767, 2803, 3101, 3596, 3691, 4098, 4597, 4794),$$

$$\mathbf{v}_4 = (1072718048, 2860533995, 5076817510, 8496108952, 9379425414, 9691934535, 12419066769, 13894053431, 16688505542, 19154047902, 21734208193, 22084787775, 25665708164, 26806012485, 27086910559, 27157628120, 27303391762, 28421844517, 28940890068),$$

$$\begin{aligned} \mathbf{v}_5 = & (236029829, 2971745499, 3192373423, 3591434267, 4890374458, 6262651163, \\ & 6615751452, 8295093644, 9045509278, 10521543661, 12818410047, \\ & 14701988578, 14777529180, 19517181732, 20888562182, 21334900084, \\ & 23103572570, 26731731879, 27241542135, 27819847981, 28642081134), \\ \mathbf{v}_6 = & (67, 707, 1279, 1291, 1983, 2280, 3920, 5158, 5200, 5609, 6075, 6826, 6940, 7154, \\ & 7200, 7791, 7852, 8165, 8934, 9102, 9445, 9849). \end{aligned}$$

Observação 1.4.1. O símbolo (*) que aparece na coluna do algoritmo $k \times LLL$ significa que foram necessários 2 “loops” para que o mínimo fosse um elemento da base.

Observação 1.4.2. No próximo capítulo veremos que mesmo aplicando muitas vezes o algoritmo LLL como acima não há garantia que o vetor mínimo seja um elemento da base.

Observação 1.4.3. O algoritmo existente para obter reduções de Minkowski, foi proposto em [22] por U. Fincke e M. Pohst. Tal algoritmo aplicado em bases \mathcal{B} na dimensão n , deve processar as decodificações das projeções de \mathbf{v}_i sobre o reticulado gerado por $\mathcal{B}' = \mathcal{B} \setminus \{\mathbf{v}_i\}$ para todo i , ou seja, uma verificação se a base está Minkowski-reduzida deve processar n decodificações na dimensão $n - 1$. O nosso algoritmo testaria um total de $n - 1$ decodificações uma em cada dimensão entre 1 e $n - 1$, sugerindo que o nosso algoritmo seja um pouco mais rápido. Como não comparamos os algoritmos para os mesmo exemplos, nem fizemos uma análise de complexidade seria injusto concluir isso.

Capítulo 2

O Problema da Projeção

Neste capítulo introduzimos o problema de determinar densidades de reticulados que são projeção do reticulados dos inteiros por um de seus elementos. Este problema está relacionado à procura de boas codificações contínuas fonte/canal ([47]). Mostramos inicialmente alguns resultados, com dependência a 1 parâmetro, sobre projeções de \mathbb{Z}^3 , cujas densidades de empacotamento estão próximas à densidade do reticulado bidimensional mais denso. Ainda na dimensão 3 estabelecemos novos resultados determinando uma família a 3 parâmetros de projeções que convergem para a densidade ótima, estendendo os resultados já existentes. Construimos uma família de projeções de \mathbb{Z}^4 (a 3-parâmetros), cujas densidades aproximam-se de alguns reticulados tridimensionais densos. Escolhendo de forma conveniente dois destes parâmetros é possível garantir a convergência da densidade para a do reticulado tridimensional mais denso (*fcc*). Fechamos o capítulo com a construção de um algoritmo, exato e de complexidade linear na dimensão, para a busca de vetores mínimos de reticulados projeção.

2.1 Codificação Contínua Fonte/Canal

Um código bom para transmissão por fonte de alfabeto contínuo sobre um canal AWGN pode ser construído através de um sistema dinâmico simples. As trajetórias do sistema dinâmico que consideramos são curvas em esferas do \mathbb{R}^{2n} . Usamos essas curvas como conjunto de sinais para um sistema de modulação. O problema é a escolha do parâmetro do sistema de forma que o comprimento da trajetória seja maximizado sujeito a uma distância mínima construída entre as “voltas” desta curva. Este problema por sua vez é equivalente à escolha de um vetor \mathbf{v} de coordenadas inteiras em \mathbb{R}^n de comprimento suficientemente grande tal que o reticulado obtido da projeção de

\mathbb{Z}^n nesta direção tenha alta densidade de empacotamento. Esta equivalência é dada pela função $\Phi : \mathbb{R}^k \longrightarrow \mathbb{R}^{2k}$, onde

$$\Phi(x_1, \dots, x_k) = \frac{1}{\sqrt{L}} (\cos(2\pi v_1), \sin(2\pi v_1), \dots, \cos(2\pi v_k), \sin(2\pi v_k)). \quad (2.1)$$

Para $n = 2$ ilustramos esta construção na figura 2.1.

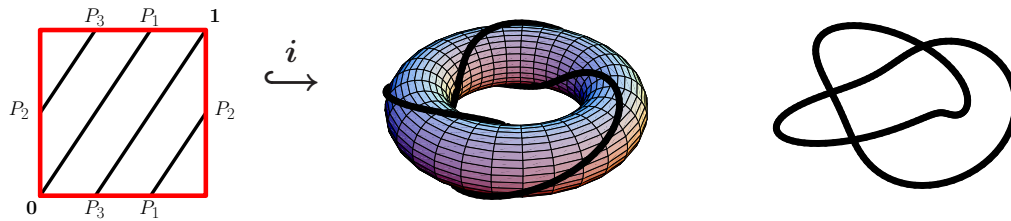


Figura 2.1: Caso $n = 2$: Ilustramos, à esquerda, a curva dada pelo o vetor $\mathbf{v} = (2, 3)$ no toro e, à direita, o toro e curva no \mathbb{R}^3 através de uma projeção estereográfica da esfera S^3 do \mathbb{R}^4 .

A figura 2.2 ilustra, para o caso $n = 3$ e $\mathbf{v} = (1, 2, 3)$, a curva e o empacotamento de tubos.

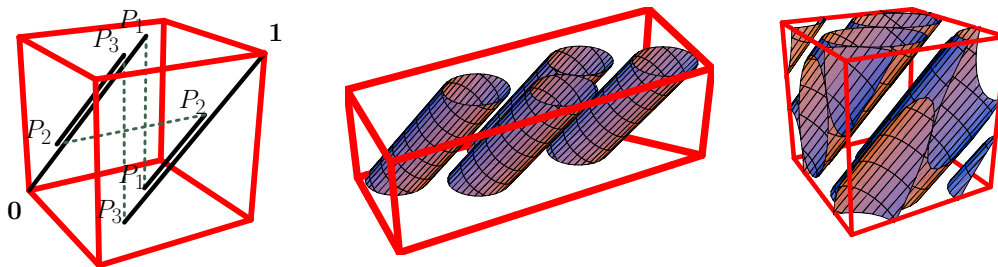


Figura 2.2: Caso $n = 3$: Ilustramos, à esquerda, a curva dada pelo o vetor $\mathbf{v} = (1, 2, 3)$ no toro tridimensional, ao centro, o empacotamento de tubos com eixo suportado em pontos de \mathbb{Z}^3 com inclinação na direção de \mathbf{v} e, à direita, o mesmo empacotamento restrito ao toro tridimensional.

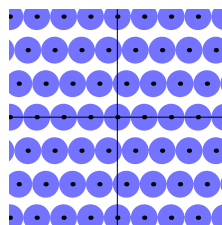


Figura 2.3: Caso $n = 3$: Ilustramos a secção ortogonal, empacotamento de tubos da Figura 2.2.

2.2 Formulação do Problema da Projeção

Estamos interessados em encontrar reticulados que sejam projeção do reticulado \mathbb{Z}^n e que tenham densidade de empacotamento boa, entretanto nem todas as direções de projeção resultam em reticulados. Por exemplo, tomando $\mathbf{v} \in \mathbb{R}^n$ com algumas coordenadas irracionais, o resultado desta projeção é um \mathbb{Z} -módulo do \mathbb{R}^n , gerado pela projeção dos vetores canônicos \mathbf{e}_i . Temos que os \mathbf{e}_i 's associados às entradas racionais geram um reticulado e os demais \mathbf{e}_j geram um sub-módulo de \mathbb{R}^n denso em algum subespaço do espaço vetorial real gerado pela projeção de \mathbb{Z}^n . Portanto só consideraremos projeções sobre vetores \mathbf{v} de entradas inteiras, já que as projeções nas direções de \mathbf{v} e $m\mathbf{v}$ resultam no mesmo conjunto. Além disso, quando o vetor da projeção tem entradas inteiras e o máximo divisor comum das entradas é 1, a norma do vetor \mathbf{v} é o comprimento da curva na superfície quociente associada ao problema.

Sem perda de generalidade, podemos supor que todas coordenadas de \mathbf{v} são positivas, pois, se alguma delas for negativa aplicamos uma reflexão através do plano ortogonal a essa coordenada tornando-a positiva. Visto que esta transformação é uma isometria, obtemos um reticulado equivalente. Da mesma forma, como a troca de coordenadas também é uma isometria, podemos supor que $0 < a_1 \leq a_2 \leq \dots \leq a_n$. Então seja $\mathbf{v} = (a_1, \dots, a_n) \in \mathbb{Z}^n$, nestas condições. A função projeção é dada por:

$$\begin{aligned} \varphi : \mathbb{Z}^n &\longrightarrow \mathbb{R}^n \\ \mathbf{x} &\longmapsto \mathbf{x} - \frac{\langle \mathbf{x}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} \mathbf{v} \end{aligned} \quad (2.2)$$

Como $\text{mdc}(a_1, \dots, a_n) = 1$, existem vetores $\mathbf{v}_2, \dots, \mathbf{v}_n \in \mathbb{Z}^n$ tais que $\{\mathbf{v}_1 = \mathbf{v}, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ geram \mathbb{Z}^n . Para isto basta considerar os vetores colunas de seguinte matriz:

$$G = \begin{bmatrix} a_1 & -y_1 & -y_2 \frac{a_1}{d_1} & \cdots & -y_{n-2} \frac{a_1}{d_{n-3}} & -y_{n-1} \frac{a_1}{d_{n-2}} \\ a_2 & x_1 & -y_2 \frac{a_2}{d_1} & \cdots & -y_{n-2} \frac{a_2}{d_{n-3}} & -y_{n-1} \frac{a_2}{d_{n-2}} \\ a_3 & 0 & x_2 & \cdots & -y_{n-2} \frac{a_3}{d_{n-3}} & -y_{n-1} \frac{a_3}{d_{n-2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & 0 & 0 & \cdots & x_{n-2} & -y_{n-1} \frac{a_3}{d_{n-2}} \\ a_n & 0 & 0 & \cdots & 0 & x_{n-1} \end{bmatrix} \quad (2.3)$$

onde $d_i = \text{mdc}(a_1, \dots, a_{i+1})$ e o par (x_i, y_i) é tal que $\langle (x_i, y_i), (d_{i-1}, a_{i+1}) \rangle = x_i d_{i-1} + y_i a_{i+1} = d_i \forall i = 1, \dots, n-1$, defina também $d_0 = a_1$. Não é difícil mostrar por indução que $\det(G) = \text{mdc}(a_1, \dots, a_n) = 1$

Logo, $\varphi(\mathbb{Z}^n)$ é um reticulado $(n-1)$ -dimensional gerado por $\{\varphi(\mathbf{v}_2), \dots, \varphi(\mathbf{v}_n)\}$, já que a projeção ortogonal do vetor \mathbf{v} na direção de \mathbf{v} é nula.

A menos de uma dilatação de $\|\mathbf{v}\|^2$, associamos $\varphi(\mathbb{Z}^n)$ ao sub-reticulado $\mathcal{L}_{\mathbf{v}} = \|\mathbf{v}\|^2 \varphi(\mathbb{Z}^n)$ do reticulado \mathbb{Z}^n e denotamos por ψ a função $\|\mathbf{v}\|^2 \varphi(\cdot)$.

Vamos analisar a densidade de empacotamento do reticulado $\mathcal{L}_{\mathbf{v}}$. Não é difícil mostrar que $\text{vol}(\varphi(\mathbb{Z}^n)) = \|\mathbf{v}\|^{-1}$. *Idéia da prova:* como volume do prisma gerado pelos vetores $\{\mathbf{v}, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ é 1, ao projetarmos ortogonalmente este prisma na direção de \mathbf{v} , o volume da projeção do prisma corresponde ao volume do reticulado-projeção. Este número multiplicado pela altura $\|\mathbf{v}\|$ tem que ser 1 (volume do prisma original). Assim, o volume da projeção do prisma é $\|\mathbf{v}\|^{-1}$ e logo $\text{vol}(\mathcal{L}_{\mathbf{v}}) = \|\mathbf{v}\|^{2n-3}$. Para calcular a densidade de empacotamento (ρ) dada por:

$$\rho = \frac{\mathcal{N}(\mathcal{L}_{\mathbf{v}})}{2^n \text{vol}(\mathcal{L}_{\mathbf{v}})}, \quad (2.4)$$

falta calcularmos $d_{\min}(\mathcal{L}_{\mathbf{v}})$.

2.3 Como Obter $\mathcal{N}(\mathcal{L}_{\mathbf{v}})$

Sabemos que o reticulado-projeção é equivalente a $\mathcal{L}_{\mathbf{v}}$, por ser uma dilatação deste, e que $\mathcal{L}_{\mathbf{v}}$ é imagem de \mathbb{Z}^n pela ψ , isto é, gerado por $\{\psi(\mathbf{e}_1), \dots, \psi(\mathbf{e}_n)\}$. A condição $a_1 \leq a_2 \leq \dots \leq a_n$ permite provar que $\|\psi(\mathbf{e}_i)\| \geq \|\psi(\mathbf{e}_j)\|$ se $i < j$ e que o conjunto $\{\psi(\mathbf{e}_1), \dots, \psi(\mathbf{e}_{n-1})\}$ está na forma (1.3) (Minkowski-reduzida, $n \leq 5$). Logo, encontrar o vetor de norma mínima de $\mathcal{L}_{\mathbf{v}}$ é achar qual o menor valor das distâncias: $d(\psi(a \mathbf{e}_n), \mathcal{L}')$, onde $a = 1, \dots, \lfloor a_n/2 \rfloor$ e \mathcal{L}' é o reticulado gerado por $\{\psi(\mathbf{e}_1), \dots, \psi(\mathbf{e}_{n-1})\}$, sendo $\{\psi(\mathbf{e}_1), \dots, \psi(\mathbf{e}_{n-1})\}$ uma base Minkowski-reduzida. Para determinar $d(\psi(a \mathbf{e}_n), \mathcal{L}')$ identificamos em que região fundamental se encontra o vetor $a \psi(\mathbf{e}_n)$, calculamos a sua distância aos vértices desta região e tomamos o menor valor.

Teorema 2.3.1. *Seja ψ como acima descrito. Então $\{\psi(\mathbf{e}_1), \dots, \psi(\mathbf{e}_{n-1})\}$ satisfaz as condições de (1.3) (Minkowski-reduzida), restritas aos inteiros $\epsilon_s \in \{-1, 0, 1\}$*

Demonstração: Antes de iniciar a prova observemos que:

$$\psi(\mathbf{e}_i) = (-a_i a_1, -a_i a_2, \dots, -a_i a_{i-1}, \underbrace{\|\mathbf{v}\|^2 - a_i^2}_{i^{\text{a}} \text{ coordenada}}, -a_i a_{i+1}, \dots, -a_i a_n). \quad (2.5)$$

$$a_{ii} = \|\psi(\mathbf{e}_i)\|^2 = \|\mathbf{v}\|^2 (\|\mathbf{v}\|^2 - a_i^2). \quad (2.6)$$

$$a_{ij} = \langle \psi(\mathbf{e}_i), \psi(\mathbf{e}_j) \rangle = -a_i a_j \|\mathbf{v}\|^2. \quad (2.7)$$

Provemos que $\{\psi(\mathbf{e}_{n-1}), \dots, \psi(\mathbf{e}_1)\}$ é Minkowski-reduzida.

Para que $\{\psi(\mathbf{e}_{n-1}), \dots, \psi(\mathbf{e}_{n-k-1})\}$ seja Minkowski-reduzida precisamos garantir que todo $S \subseteq \{n-1, n-2, \dots, n-k\}$. Temos:

$$H = 2 \left(\sum_{s \in S} \epsilon_s a_{s l} - \sum_{\substack{r, s \in S \\ r < s}} \epsilon_r \epsilon_s a_{r s} \right) \leq \sum_{s \in S} a_{s s}$$

Como o produto interno dois a dois, neste caso, é sempre negativo, isso significa que podemos considerar que $\epsilon_i = -1, \forall i$. Em outras palavras H assume seu maior valor quando $\epsilon_i = -1, \forall i$.

Seja $t = \#S, l = n - k - 1$ e $S = \{s_1, \dots, s_t\}$.

$$\begin{aligned} H &= 2 \left(- \sum_{s \in S} a_{s l} - \sum_{\substack{r, s \in S \\ r < s}} a_{r s} \right) \\ &= 2 \left(\sum_{s \in S} a_s a_l \|\mathbf{v}\|^2 + \sum_{\substack{r, s \in S \\ r < s}} a_r a_s \|\mathbf{v}\|^2 \right) && \text{pela equação (2.7)} \\ &= \|\mathbf{v}\|^2 \left(\sum_{s \in S} 2 a_s a_l + \sum_{\substack{r, s \in S \\ r < s}} 2 a_r a_s \right) \\ &\leq \|\mathbf{v}\|^2 \left(\sum_{s \in S} (a_s^2 + a_l^2) + \sum_{\substack{r \in S \\ r < s}} (a_r^2 + a_s^2) \right) && \text{desigualdade de Cauchy-Schwartz} \\ &= \|\mathbf{v}\|^2 \left(t a_l^2 + \sum_{s \in S} a_s^2 + (t-1) \sum_{s \in S} a_s^2 \right) \\ &= \|\mathbf{v}\|^2 \left(t a_l^2 + \sum_{s \in S} a_s^2 + \sum_{s \in S} \sum_{\substack{r \in S \\ r < s}} (a_r^2 + a_s^2) \right) && t = \#S \\ &= \|\mathbf{v}\|^2 \left(t a_l^2 + t \sum_{s \in S} a_s^2 \right) \\ &\leq \|\mathbf{v}\|^2 (t \|\mathbf{v}\|^2 - t a_n^2) && a_n \notin S \cup \{l\} \\ &\leq \|\mathbf{v}\|^2 (t \|\mathbf{v}\|^2 - (a_{s_1}^2 + a_{s_2}^2 + \dots + a_{s_{t-1}}^2 + a_{s_t}^2)) && a_n \geq a_{s_t} \forall s_t \in S \\ &= \sum_{s \in S} \|\mathbf{v}\|^2 (\|\mathbf{v}\|^2 - a_s^2) \\ &= \sum_{s \in S} a_{s s} && \text{pela equação (2.6)} \end{aligned} \tag{2.8}$$

Como queríamos demonstrar. ■

O resultado acima garante o conjunto $\{\psi(\mathbf{e}_1), \dots, \psi(\mathbf{e}_{n-1})\}$ é Minkowski-reduzido para $n - 1 \leq 4$, ou seja, $n \leq 5$. O teorema acima pode ser melhorado se, na definição equivalente de Minkowski-reduzida, for suficiente nos restringirmos a inteiros $|\epsilon_s| \leq 1$. Conjecturamos que isto seja válido.

2.4 Projeção de \mathbb{Z}^3

O problema do empacotamento do reticulado-projeção faz sentido apenas para $n \geq 3$, uma vez que para $n = 2$ o reticulado é unidimensional, a densidade de empacotamento não depende do vetor \mathbf{v} e portanto sua densidade é sempre máxima. É importante notar que a densidade de empacotamento de reticulados-projeção já na dimensão seguinte (de dimensão 3 para 2) pode mudar radicalmente mesmo com variações mínimas do vetor \mathbf{v} . Isto já mostra a complexidade que iremos constatar neste problema. Este fato é ilustrado no exemplo da Tabela 2.1, onde listamos os vetores que dão a direção de projeção e as respectivas densidades dos reticulados bidimensionais resultantes.

\mathbf{v}	$\Delta(\mathcal{L}_{\mathbf{v}})$	\mathbf{v}	$\Delta(\mathcal{L}_{\mathbf{v}})$
(51, 53, 4680)	0.67976	(55, 57, 5429)	0.68131
(51, 53, 4681)	0.90022	(55, 57, 5430)	0.87744
(51, 53, 4682)	0.67980	(55, 57, 5431)	0.68048
(51, 53, 4683)	0.89581	(55, 57, 5432)	0.89302
(51, 53, 4684)	0.68052	(55, 57, 5433)	0.68023
(51, 53, 4685)	0.87934	(55, 57, 5434)	0.90483
(51, 53, 4686)	0.68190	(55, 57, 5435)	0.68056
(51, 53, 4687)	0.86355	(55, 57, 5436)	0.88929
(51, 53, 4688)	0.68396	(55, 57, 5437)	0.68146
(51, 53, 4689)	0.84844	(55, 57, 5438)	0.87413
(51, 53, 4690)	0.68668	(55, 57, 5439)	0.68295
(51, 53, 4691)	0.83402	(55, 57, 5440)	0.85966
(51, 53, 4692)	0.69007	(55, 57, 5441)	0.68500
(51, 53, 4693)	0.82027	(55, 57, 5442)	0.84578
(51, 53, 4694)	0.69412	(55, 57, 5443)	0.68764
(51, 53, 4695)	0.80721	(55, 57, 5444)	0.83249

Tabela 2.1: A tabela ilustra que alterações mínimas na maior coordenada podem alterar significativamente a densidade do reticulado-projeção.

Começaremos analisando o caso dos vetores do tipo $\mathbf{v} = (1, a, b(a))$ usando resultados obtidos em [48].

2.4.1 Vetores do Tipo $\mathbf{v} = (1, a, b)$

Apresentamos aqui a análise feita sobre o caso do vetor da forma $\mathbf{v} = (1, a, b)$, apresentado em [48], adaptando à nossa notação para compatibilizar com a extensão deste resultado que faremos. Precisamos dos vetores que geram o reticulado-projeção para analisarmos qual é o vetor mínimo e assim, conhecermos a densidade de empacotamento do reticulado. Consideremos os vetores $\mathbf{u} = (0, -1, 0)$ e $\mathbf{w} = (0, 0, 1)$. É claro que $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ gera \mathbb{Z}^3 e portanto $\psi(\{\mathbf{u}, \mathbf{v}, \mathbf{w}\})$ gera o reticulado-projeção, ou seja, o reticulado-projeção é gerado pelos vetores: $(a, -1 - b^2, ab)$ e $(-b, -ab, 1 + a^2)$ e então a matriz de Gram de $\varphi_{\mathbf{v}}(\mathbb{Z}^3)$ é:

$$\mathcal{A}_{\mathbf{v}} = \frac{1}{1 + a^2 + b^2} \begin{bmatrix} 1 + a^2 & ab \\ ab & 1 + b^2 \end{bmatrix}. \quad (2.9)$$

O fator $\frac{1}{1 + a^2 + b^2}$ não interfere no processo de redução e portanto vamos deixá-lo de lado. Supondo uma redução simples temos:

$$\begin{aligned} \mathcal{A}'_{\mathbf{v}} &= \begin{bmatrix} 1 & 0 \\ -\alpha & 1 \end{bmatrix} \mathcal{A}_{\mathbf{v}} \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 + a^2 & ab - (1 + a^2)\alpha \\ ab - (1 + a^2)\alpha & 1 + b^2 - 2ab\alpha + (1 + a^2)\alpha^2 \end{bmatrix}. \end{aligned}$$

Esta redução corresponde a troca de \mathbf{u} por $\mathbf{u} - \alpha \mathbf{w}$. Ou seja, se a matriz geradora é $\mathcal{M} = \begin{bmatrix} \mathbf{w}^t & \mathbf{u}^t \end{bmatrix}$ e $\mathcal{U} = \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix}$. A nova matriz geradora passa ser $\mathcal{M}\mathcal{U}$ e a nova matriz de Gram é $\mathcal{A}' = (\mathcal{M}\mathcal{U})^t \mathcal{M}\mathcal{U} = \mathcal{U}^t \mathcal{M}^t \mathcal{M}\mathcal{U} = \mathcal{U}^t \mathcal{A}\mathcal{U}$.

Queremos que $\mathcal{A}'_{\mathbf{v}}$ esteja próxima, a menos de escala, da matriz de Gram do reticulado hexagonal que é dada por:

$$\mathcal{A}_{\text{hex}} = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}. \quad (2.10)$$

Ou equivalentemente, que $\mathcal{A}' = \frac{1}{1 + a^2} \mathcal{A}'_{\mathbf{v}}$ esteja próxima da matriz \mathcal{A}_{hex} , ou ainda, que

$$\mathcal{A}' = \begin{bmatrix} 1 & \frac{1}{2} + \xi_1 \\ \frac{1}{2} + \xi_1 & 1 - 2\alpha\xi_1 + \xi_2 \end{bmatrix}, \quad (2.11)$$

com as condições:

$$\begin{aligned}
\xi_1 &\leq 0 \\
\xi_2 - 2\alpha\xi_1 &> 2\xi_1 \\
|\xi_1| &\lll 1 \\
|\xi_2 - 2\alpha\xi_1| &\lll 1.
\end{aligned} \tag{2.12}$$

As duas primeiras desigualdades em (2.12) são condições para que a matriz esteja na forma (1.3) (Minkowski), já as outras duas é que de fato garantem que a matriz é uma pequena perturbação da matriz de Gram do reticulado hexagonal, a notação \lll significa muito menor.

Resolvendo as equações dadas em (2.11) tem-se:

Teorema 2.4.1 ([48]). *Dado $a \in \mathbb{Z}$, sejam*

$$\alpha = \left\lfloor \frac{1}{2} \left(-1 + \frac{a\sqrt{3a^2-1}}{\sqrt{1+a^2}} \right) \right\rfloor \quad e \quad b = \left\lfloor \frac{(1+a^2)(1+2\alpha)}{2a} \right\rfloor. \tag{2.13}$$

Então, quando a é grande, a matriz A' (2.11) satisfaz as seguintes desigualdades:

$$\frac{-a}{1+a^2} \leq \xi_1 < 0, \quad \xi_2 - 2\alpha\xi_1 \leq \frac{\sqrt{3}}{a} + \frac{\sqrt{3}}{a^2} \quad e \quad \xi_2 - 2\alpha\xi_1 > 2\xi_1. \tag{2.14}$$

Observação 2.4.1. Para α e b , como no teorema, acima temos: $\lim_{a \rightarrow +\infty} \xi_1 = 0$ e $\lim_{a \rightarrow +\infty} (\xi_2 - 2\alpha\xi_1) = 0$ e então \mathcal{L}_v aproxima-se do reticulado hexagonal para a grande.

A prova deste teorema pode ser obtida em [48]. Este resultado é sub-ótimo como mostra o seguinte resultado, apresentado neste mesmo artigo:

Teorema 2.4.2 ([48]). *Dado $a \in \mathbb{Z}$, o valor de $b \in \mathbb{Z}$ que dá a melhor densidade de empacotamento para o reticulado associado a matrix A' (2.11) é*

$$b = \left\lfloor \frac{\sqrt{3}}{2} a \right\rfloor a + \left\lfloor \frac{a}{2} \right\rfloor + 1.$$

O resultado do Teorema 2.4.1 exige que o reticulado-projeção tenha matriz de Gram com as condições (2.12), e com isso despreza os inteiros b tais que:

$$\begin{aligned}
\xi_1 &\geq -1 \\
\xi_2 - 2\alpha\xi_1 &> -2(1 + \xi_1) \\
|\xi_1 + 1| &\lll 1 \\
|\xi_2 - 2\alpha\xi_1| &\lll 1
\end{aligned} \tag{2.15}$$

A terceira desigualdade em (2.15) significa que estamos considerando outra base para o reticulado hexagonal, a base dada pelos vetores $(1, 0)$ e $(-1/2, \sqrt{3}/2)$, a qual determina a matriz de Gram

$$\begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix}. \quad (2.16)$$

Se no Teorema 2.4.1 trocarmos a matriz por esta, obteremos um teorema dual satisfazendo as restrições (2.15).

Teorema 2.4.3. *Dado $a \in \mathbb{Z}$, sejam*

$$\alpha = \left\lfloor \frac{1}{2} \left(-1 + \frac{a \sqrt{3a^2 - 1}}{\sqrt{1 + a^2}} \right) \right\rfloor \quad e \quad b = \left\lceil \frac{(1 + a^2)(-1 + 2\alpha)}{2a} \right\rceil. \quad (2.17)$$

Então, quando a é grande, a matriz \mathcal{A}' (2.11) satisfaz as seguintes desigualdades:

$$-1 < \xi_1 \leq -1 + \frac{a}{1 + a^2}, \quad \xi_2 - 2\alpha \xi_1 \leq \frac{\sqrt{3}}{a} + \frac{\sqrt{3}}{a^2} \quad e \quad \xi_2 - 2\alpha \xi_1 > -2(1 + \xi_1). \quad (2.18)$$

Ainda como corolário da demonstração do Teorema 2.4.1 segue o teorema:

Teorema 2.4.4. *Dado $a \in \mathbb{Z}$, seja*

$$\alpha = \left\lfloor \frac{1}{2} \left(-1 + \frac{a \sqrt{3(1 + a^2) - 4}}{\sqrt{1 + a^2}} \right) \right\rfloor \quad e \quad b = \left\lceil \frac{(1 + a^2)(-1 + 2\alpha)}{2a} \right\rceil. \quad (2.19)$$

Então, a matriz \mathcal{A}' (2.11) satisfaz:

$$|\xi_2 - 2\alpha \xi_1| \xrightarrow{a \rightarrow +\infty} 0 \quad e \quad \xi_1 \xrightarrow{a \rightarrow +\infty} 0. \quad (2.20)$$

Observação 2.4.2. A Tabela 2.2 ilustra as diferenças entre esses 4 teoremas acima. Note a semelhança no desempenho das duas últimas colunas. Baseado neste excelente desempenho adotaremos o enfoque do Teorema 2.4.4 na próxima seção.

Observação 2.4.3. O $b(a)$ obtido em 2.4.2 não é em geral o melhor b para qual a densidade de empacotamento de $\varphi_v(\mathbb{Z}^3)$, como mostra próximo exemplo, mas esse $b(a)$ serve como um limitante superior para a procura de b de tal forma que a densidade de empacotamento seja boa. E para b menores que $b(a)$, devemos supor que a redução não seja simples como mencionamos anteriormente.

Exemplo 2.4.1. Suponha que $a = 75$, pelo Teorema 2.4.2 devemos escolher $b(a) = 4838$, mas veja uma tabela abaixo as densidades para outros b 's:

a	$b(a)$ (2.4.1)	ρ	$b(a)$ (2.4.3)	ρ	$b(a)$ (2.4.2)	ρ	$b(a)$ (2.4.4)	ρ
3	5	0.796539	9	0.823321	8	0.821706	8	0.821706
4	10	0.653491	15	0.858284	15	0.858284	15	0.858284
5	18	0.797645	24	0.832271	23	0.866796	23	0.866796
6	27	0.737817	34	0.84134	34	0.84134	34	0.84134
7	39	0.832245	47	0.826232	46	0.843783	39	0.832245
8	52	0.791051	61	0.829684	53	0.864368	53	0.864368
9	68	0.858668	78	0.820166	68	0.858668	68	0.858668
10	85	0.825846	96	0.821813	86	0.888939	86	0.888939
11	94	0.838119	106	0.862233	105	0.877795	105	0.877795
12	114	0.808458	127	0.892711	127	0.892711	127	0.892711
13	137	0.856057	151	0.880945	150	0.886774	150	0.886774
14	161	0.831029	176	0.876328	176	0.876328	176	0.876328
15	188	0.870351	204	0.867745	188	0.870351	188	0.870351
16	216	0.848514	233	0.864254	217	0.887939	217	0.887939
17	247	0.881877	265	0.857723	247	0.881877	247	0.881877
18	279	0.862421	298	0.854995	280	0.898542	280	0.898542
19	295	0.866132	315	0.881032	314	0.891318	314	0.891318
20	330	0.848098	351	0.895822	351	0.895822	351	0.895822
21	368	0.875742	390	0.888827	389	0.891106	389	0.891106
22	407	0.8594	430	0.884697	430	0.884697	430	0.884697
23	449	0.883942	473	0.879004	449	0.883942	449	0.883942
24	492	0.868969	517	0.875602	493	0.895852	493	0.895852
25	538	0.891004	564	0.87088	538	0.891004	538	0.891004
26	559	0.85753	586	0.902453	586	0.902453	586	0.902453
27	608	0.87883	636	0.889563	635	0.89714	635	0.89714
28	658	0.865779	687	0.896689	687	0.896689	687	0.896689
29	711	0.885183	741	0.891766	740	0.892969	740	0.892969
30	765	0.87302	796	0.888368	766	0.894421	766	0.894421
31	822	0.890822	854	0.88414	822	0.890822	822	0.890822
32	880	0.879421	913	0.881203	881	0.899806	881	0.899806
33	941	0.895854	975	0.877532	941	0.895854	941	0.895854
34	969	0.869967	1004	0.904566	1004	0.904566	1004	0.904566
35	1033	0.88601	1069	0.894389	1068	0.900371	1068	0.900371
36	1098	0.87577	1135	0.897048	1135	0.897048	1135	0.897048
37	1166	0.890702	1204	0.893262	1203	0.894004	1203	0.894004
38	1235	0.881009	1274	0.89042	1236	0.898081	1236	0.898081
39	1307	0.894967	1347	0.887064	1307	0.894967	1307	0.894967
40	1380	0.885762	1421	0.884535	1381	0.902175	1381	0.902175
41	1415	0.8866	1457	0.893394	1456	0.89886	1456	0.89886
42	1491	0.877759	1534	0.90333	1534	0.90333	1534	0.90333
43	1570	0.890618	1614	0.897488	1613	0.900478	1613	0.900478
44	1650	0.882188	1695	0.897229	1695	0.897229	1695	0.897229
45	1733	0.894318	1779	0.894158	1733	0.894318	1733	0.894318
46	1817	0.886261	1864	0.891728	1818	0.900457	1818	0.900457
47	1904	0.897737	1952	0.888948	1904	0.897737	1904	0.897737
48	1992	0.890017	2041	0.886743	1993	0.903754	1993	0.903754
49	2034	0.890554	2084	0.896327	2083	0.900904	2083	0.900904
50	2125	0.883097	2176	0.902464	2176	0.902464	2176	0.902464

Tabela 2.2: Comparando as densidades de empacotamento tomando os $b(a)$ sugeridos pelos Teoremas: 2.4.1, 2.4.3, 2.4.2 e 2.4.4 (respectivamente).

b	ρ
702	0.896650
1613	0.901771
4763	0.892635
4838	0.899415
4839	0.891450
4912	0.894501

Tabela 2.3: Tabela densidades para vetores $\mathbf{v} = (1, 75, b)$

Para $b = 1613$, uma redução simples não produzirá uma base Minkowski-reduzida.

2.4.2 Vetores do Tipo $\mathbf{v} = (a, b, c)$

Vamos tentar resolver o problema para a, b arbitrários e analisar o que podemos garantir.

Suponha que $\text{mdc}(a, b) = d$, sejam $x, y \in \mathbb{Z}$ tal que $ax + by = d$ e sejam $z, t \in \mathbb{Z}$ tal que $zd + tc = 1$.

$$A = \begin{bmatrix} a & -y & -t \frac{a}{d} \\ b & x & -t \frac{b}{d} \\ c & 0 & z \end{bmatrix} \quad (2.21)$$

Temos que $\det(A) = 1$, logo $\{\mathbf{v}, \mathbf{v}_2, \mathbf{v}_3\}$ gera \mathbb{Z}^3 e portanto $\{\varphi(\mathbf{v}_2), \varphi(\mathbf{v}_3)\}$ gera o reticulado-projeção. Após alguns cálculos chegamos que:

$$\begin{aligned} \varphi(\mathbf{v}_2) &= \frac{1}{a^2 + b^2 + c^2} (-bd - c^2 y, ad + c^2 x, c(-bx + ay)) \\ \varphi(\mathbf{v}_3) &= \frac{1}{a^2 + b^2 + c^2} \left(-\frac{ac}{d}, -\frac{bc}{d}, \frac{a^2 + b^2}{d} \right). \end{aligned}$$

E portanto, a matriz de Gram G do reticulado-projeção tem a seguinte forma:

$$G = \frac{1}{a^2 + b^2 + c^2} \begin{bmatrix} \frac{a^2 + b^2}{d^2} & \frac{-c(bx - ay)}{d} \\ \frac{-c(bx - ay)}{d} & d^2 + c^2(x^2 + y^2) \end{bmatrix}. \quad (2.22)$$

Que é equivalente ao reticulado cuja matriz de Gram é:

$$\begin{bmatrix} \frac{a^2 + b^2}{d^2} & \frac{-c(bx - ay)}{d} \\ \frac{-c(bx - ay)}{d} & d^2 + c^2(x^2 + y^2) \end{bmatrix}. \quad (2.23)$$

Seja $\mathbf{u} = \sqrt{a^2 + b^2 + c^2} \varphi(\mathbf{v}_3)$ e $\mathbf{w} = \sqrt{a^2 + b^2 + c^2} \varphi(\mathbf{v}_2)$, então

$$\|\mathbf{u}\|^2 = \frac{a^2 + b^2}{d^2} < d^2 + c^2(x^2 + y^2) = \|\mathbf{w}\|^2.$$

Suponha que exista $\alpha \in \mathbb{Z}$ tal que o vetor que realiza o mínimo esteja em $\{\mathbf{u}, \mathbf{w} - \alpha \mathbf{u}, \mathbf{w} - (\alpha + 1) \mathbf{u}\}$. Vamos determinar para qual $c = c(a, b)$ isso ocorre e além disso mostrar que para quais $c(a, b)$ a densidade de empacotamento dos reticulados-projeção converge para a densidade de empacotamento do reticulado hexagonal.

Neste novo reticulado, obtemos a matriz de Gram (G')

$$G' = \frac{a^2 + b^2}{d^2} \begin{bmatrix} 1 & 0 \\ -\alpha & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{-cd(bx - ay)}{a^2 + b^2} \\ \frac{-cd(bx - ay)}{a^2 + b^2} & \frac{d^2(d^2 + c^2(x^2 + y^2))}{a^2 + b^2} \end{bmatrix} \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix}, \quad (2.24)$$

a qual queremos que tenha o seguinte formato:

$$G'' = \frac{a^2 + b^2}{d^2} \begin{bmatrix} 1 & \frac{1}{2} + \xi_1 \\ \frac{1}{2} + \xi_1 & 1 - 2\alpha\xi_1 + \xi_2 \end{bmatrix}. \quad (2.25)$$

Com as seguintes restrições:

$$\begin{aligned} |\xi_1| &\lll 1 \\ |\xi_2 - 2\alpha\xi_1| &\lll 1 \end{aligned} \quad (2.26)$$

Estas restrições é que garantem a existência de 3 vetores com praticamente a mesma norma e tal que os ângulos dois a dois sejam $\frac{\pi}{3}$ ou $\frac{2\pi}{3}$, o que caracteriza uma pequena perturbação do reticulado hexagonal.

Logo da imposição que $G'' = G'$, temos as seguintes equações:

$$-\frac{1}{2} + \frac{cd(-bx + ay)}{a^2 + b^2} - \alpha - \xi_1 = 0 \quad (2.27)$$

$$-1 + \frac{d^4 + c^2 d^2(x^2 + y^2) + 2cd(bx - ay)\alpha + (a^2 + b^2)\alpha^2}{a^2 + b^2} + 2\alpha\xi_1 - \xi_2 = 0. \quad (2.28)$$

Esta última equação pode ser reescrita da forma abaixo completando quadrados:

$$-1 + \frac{d^4}{a^2 + b^2} + \frac{c^2 d^4}{(a^2 + b^2)^2} + \left(\frac{cd(bx - ay)}{a^2 + b^2} + \alpha \right)^2 + 2\alpha\xi_1 - \xi_2 = 0 \quad (2.29)$$

Resolvendo a equação (2.27) em c obtemos que:

$$c = -\frac{(a^2 + b^2)(1 + 2\alpha + 2\xi_1)}{2d(bx - ay)} \quad (2.30)$$

Como queremos que ξ_1 seja pequeno, vamos desprezá-lo, mas como não sabemos o seu sinal não podemos tomar o chão (maior inteiro menor que) de c se $\xi_1 < 0$ ou o teto (menor inteiro maior que) de c se $\xi_1 > 0$. Além disso, o valor escolhido para c deverá ser coprimo com d . Logo, vamos tomar o inteiro mais próximo (arredondando) e, que seja coprimo com d , denotaremos tal escolha pela função $[\cdot]_d$ (observamos que, para $d = 1$, a função $[\cdot]_d$ é a mesma função $[\cdot]$). Assim temos que:

$$c \sim \left[-\frac{(a^2 + b^2)(1 + 2\alpha)}{2d(bx - ay)} \right]_d. \quad (2.31)$$

Substituindo essa aproximação em (2.29) e desprezando ξ_1 e $\xi_2 - 2\alpha\xi_1$ temos:

$$\alpha \sim \left[-\frac{1}{2} - \frac{\sqrt{3(a^2 + b^2) - 4d^4}(bx - ay)}{2d\sqrt{a^2 + b^2}} \right]. \quad (2.32)$$

Note que o problema pode não ter solução real, como no caso em que $a = n$ e $b = 2n$, onde temos que:

$$\sqrt{3(a^2 + b^2) - 4d^4} = \sqrt{3(n^2 + 4n^2) - 4n^4} = \sqrt{15n^2 - 4n^4} \quad (2.33)$$

Para $n \geq 4$, este número passar a ser imaginário, portanto não haverá uma solução c boa para o problema, e dentre os c possíveis não é difícil concluir que a melhor solução será:

$$c = -\frac{(a^2 + b^2)(1 + 2\Re(\alpha))}{2d(bx - ay)}, \quad (2.34)$$

onde $\Re(\alpha)$ é a parte real do número complexo α .

Assumiremos daqui por diante que $3(a^2 + b^2) \gg 4d^4$.

Seja

$$\delta_c = -\frac{(a^2 + b^2)(1 + 2\alpha)}{2d(bx - ay)} - c$$

e

$$\delta_\alpha = -\frac{1}{2} - \frac{\sqrt{3(a^2 + b^2) - 4d^4}(bx - ay)}{2d\sqrt{a^2 + b^2}} - \alpha.$$

Vamos estimar os valores ξ_1 e $2\alpha\xi_1 - \xi_2$.

Substituindo os valores supra mencionados em (2.27) e após algumas contas simples obtemos:

$$\xi_1 = \frac{d(bx - ay)\delta_c}{a^2 + b^2}, \quad (2.35)$$

valor que gostaríamos que fosse muito pequeno. Entretanto isto nem sempre ocorre, como por

exemplo para $a = 2n - 1$ e $b = 2n + 1$, nestas condições $x = n$ e $y = 1 - n$ e assim temos:

$$\begin{aligned}
 \xi_1 &= \frac{d(bx - ay)\delta_c}{a^2 + b^2} \\
 &= \frac{d((2n+1)n - (2n-1)(1-n))\delta_c}{(2n-1)^2 + (2n+1)^2} \\
 &= \frac{d(1 - 2n + 4n^2)\delta_c}{2 + 8n^2} \\
 &\xrightarrow{n \rightarrow +\infty} \frac{d\delta_c}{2}.
 \end{aligned} \tag{2.36}$$

Tal número é majorado por $\frac{d}{2}$ e portanto se a e b forem arbitrários ξ_1 não será necessariamente pequeno, salvo se δ_c o for. Assim suponhamos que ξ_1 seja desprezível.

Vamos substituir os valores de α e c acima em (2.29). Para facilitar substituiremos primeiro só o valor de c , obtendo a seguinte equação:

$$\xi_2 - 2\alpha\xi_1 = -1 + \frac{d^4}{a^2 + b^2} + \frac{\left(-\frac{(a^2 + b^2)(1 + 2\alpha)}{2d(bx - ay)} - \delta_c\right)^2 d^4}{(a^2 + b^2)^2} + \left(\frac{1}{2} + \xi_1\right)^2. \tag{2.37}$$

Simplificando temos:

$$\xi_2 - 2\alpha\xi_1 = -1 + \frac{d^4}{a^2 + b^2} + \left(\frac{(1/2 + \alpha)}{d(bx - ay)} + \frac{\delta_c}{a^2 + b^2}\right)^2 d^4 + \left(\frac{1}{2} + \xi_1\right)^2. \tag{2.38}$$

Substituindo α temos:

$$\begin{aligned}
 \xi_2 - 2\alpha\xi_1 &= -1 + \frac{d^4}{a^2 + b^2} + \left(\frac{1}{2} + \xi_1\right)^2 + \\
 &\quad \left(\frac{\left(-\delta_\alpha - \frac{\sqrt{3(a^2 + b^2) - 4d^4}(bx - ay)}{2d\sqrt{a^2 + b^2}}\right)}{d(bx - ay)} + \frac{\delta_c}{a^2 + b^2}\right)^2 d^4
 \end{aligned} \tag{2.39}$$

Simplificando novamente:

$$\begin{aligned}
 \xi_2 - 2\alpha\xi_1 &= -1 + \frac{d^4}{a^2 + b^2} + \left(\frac{1}{2} + \xi_1\right)^2 \\
 &\quad + \left(\frac{\delta_\alpha}{2d(bx - ay)} + \frac{\sqrt{3(a^2 + b^2) - 4d^4}}{2d^2\sqrt{a^2 + b^2}} - \frac{\delta_c}{a^2 + b^2}\right)^2 d^4
 \end{aligned} \tag{2.40}$$

$$\begin{aligned}
\xi_2 - 2\alpha\xi_1 &= -1 + \frac{d^4}{a^2 + b^2} + \left(\frac{1}{2} + \xi_1\right)^2 + \left(\frac{\delta_\alpha}{2d(bx - ay)} - \frac{\delta_c}{a^2 + b^2}\right)^2 d^4 \\
&+ 2 \left(\frac{\delta_\alpha}{2d(bx - ay)} - \frac{\delta_c}{a^2 + b^2}\right) \left(\frac{\sqrt{3(a^2 + b^2) - 4d^4}}{2d^2\sqrt{a^2 + b^2}}\right) d^4 \\
&+ \frac{3(a^2 + b^2) - 4d^4}{4d^4(a^2 + b^2)} d^4.
\end{aligned} \tag{2.41}$$

Para a e b suficientemente grandes e d fixo temos que

$$\left(\frac{\delta_\alpha}{2d(bx - ay)} - \frac{\delta_c}{a^2 + b^2}\right) \xrightarrow{\|(a,b)\| \rightarrow +\infty} 0 \tag{2.42}$$

e

$$\left(\frac{\sqrt{3(a^2 + b^2) - 4d^4}}{2d^2\sqrt{a^2 + b^2}}\right) \xrightarrow{\|(a,b)\| \rightarrow +\infty} \frac{\sqrt{3}}{2d^2}. \tag{2.43}$$

Das equações (2.42) e (2.43), o lado direito da equação (2.41) converge, quando $\|(a, b)\|$ vai para o infinito, para:

$$\begin{aligned}
\xi_2 - 2\alpha\xi_1 &\xrightarrow{\|(a,b)\| \rightarrow +\infty} -1 + \left(\frac{1}{2} + \xi_1\right)^2 + \frac{d^4}{a^2 + b^2} + \frac{3(a^2 + b^2) - 4d^4}{4d^4(a^2 + b^2)} d^4 \\
&= -1 + \left(\frac{1}{2} + \xi_1\right)^2 + \frac{d^4}{a^2 + b^2} + \frac{3}{4} - \frac{d^4}{a^2 + b^2} \\
&= \left(\frac{1}{2} + \xi_1\right)^2 - \frac{1}{4}.
\end{aligned} \tag{2.44}$$

Observemos que, esta última expressão tenderá a 0 se, e só se, $\xi_1 = 0$ ou -1 . Isto reforça a nossa idéia inicial de que não há necessidade de nos restringirmos apenas ao caso $\xi_1 = 0$ que produz a matriz de Gram $\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$ e devemos analisar $\xi_1 = -1$, que resulta na matriz de Gram $\begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix}$. Esta escolha é feita de forma automática quando trabalhamos com a função arredondamento ($\lceil \cdot \rceil$).

Concluimos portanto a demonstração do seguinte teorema:

Teorema 2.4.5. *Fixados inteiros x, y, d , com x e y coprimos. Sejam*

$$c = \left\lceil -\frac{(a^2 + b^2)(1 + 2\alpha)}{2d(bx - ay)} \right\rceil \quad e \quad \alpha = \left\lceil -\frac{1}{2} - \frac{\sqrt{3(a^2 + b^2) - 4d^4}(bx - ay)}{2d\sqrt{a^2 + b^2}} \right\rceil.$$

Se $\frac{d(bx - ay)\delta_c}{a^2 + b^2}$, com $\delta_c = -\frac{(a^2 + b^2)(1 + 2\alpha)}{2d(bx - ay)} - c$ e $ax + by = d$, converge a 0, quando a norma de (a, b) vai para o infinito. Então, o reticulado-projeção se aproxima do hexagonal().*

Observação 2.4.4. (*) Em outras palavras, os erros cometidos da aproximação da matriz do reticulado hexagonal convergem para zero, da mesma forma do Teorema 2.4.4. Os erros estarem convergindo para zero garantem que, após a redução simples, um dos vetores $\varphi(\mathbf{v}_2)$, $\varphi(\mathbf{v}_3)$ ou $\varphi(\mathbf{v}_2) - \varphi(\mathbf{v}_3)$ é o menor vetor não nulo do reticulado. Quando $\xi_2 - 2\alpha\xi_1 \rightarrow 0$ estamos garantindo que $\|\varphi(\mathbf{v}_2)\| \rightarrow c$ e $\|\varphi(\mathbf{v}_3)\| \rightarrow c$. Quando $\xi_1 \rightarrow 0$ estamos garantindo que $\langle \varphi(\mathbf{v}_2), \varphi(\mathbf{v}_3) \rangle \rightarrow c^2/2$. Assim temos:

$$\|\varphi(\mathbf{v}_2) - \varphi(\mathbf{v}_3)\|^2 = \|\varphi(\mathbf{v}_2)\|^2 + \|\varphi(\mathbf{v}_3)\|^2 - 2\langle \varphi(\mathbf{v}_2), \varphi(\mathbf{v}_3) \rangle \rightarrow c^2 + c^2 - c^2 = c^2.$$

Ou seja, a norma mínima convergirá para c e o determinante da matriz de Gram convergirá para $\frac{3}{4}c^4$, resultando que a densidade de centro converge para a densidade de centro do reticulado hexagonal. Geometricamente o reticulado está convergindo ao reticulado que é uma dilatação do hexagonal e portanto equivalente ao hexagonal.

Observação 2.4.5. O fato crucial para garantir a convergência dos reticulados-projeção para o reticulado hexagonal está em garantir que $\left| \frac{(bx - ay)\delta_c}{a^2 + b^2} \right| \xrightarrow{|(a,b)| \rightarrow +\infty} 0$. Isto é o que impede garantir a convergência dos reticulados-projeção dados pelo vetor $\mathbf{v} = (2a - 1, 2a + 1, c(a))$, uma vez que $\left| \frac{(bx - ay)\delta_c}{a^2 + b^2} \right| \xrightarrow{|(a,b)| \rightarrow +\infty} \left| \frac{\delta_c}{2} \right|$ que só podemos assegurar que é menor que $1/4$.

Corolário 2.4.1. *O reticulado-projeção determinado pelo vetor*

$$\mathbf{v} = (d(a_0 - ny), d(b_0 + nx), c),$$

com $a_0x + b_0y = 1$ e c dado pelo Teorema 2.4.5, se aproxima do reticulado hexagonal quando n tende ao infinito.

Demonstração: Note que o numerador de $\frac{d(bx - ay)\delta_c}{a^2 + b^2}$ é linear enquanto o denominador é quadrático em n , logo pelo teorema anterior segue o resultado. ■

Observação 2.4.6. O Corolário 2.4.1 gera para cada (x, y) uma família a um parâmetro de vetores $\mathbf{v} = (a, b, c) \in \mathbb{Z}^3$ (reticulado unidimensional), que corresponde a uma reta ortogonal a (x, y) passando pelo ponto $\frac{d(x, y)}{x^2 + y^2}$.

Por exemplo para $d = 1$:

1. Seja $(x, y) = (1, 0)$, consideramos $(a_0, b_0) = (1, 0)$. Logo, a família de vetores corresponde $\mathbf{v} = (1, n, c(n))$, onde $c(n) = \left[-\frac{(1 + n^2)(1 + 2\alpha)}{2n} \right]$ e $\alpha = \left[-\frac{1}{2} - \frac{\sqrt{3(1 + n^2) - 4(n)}}{2\sqrt{1 + n^2}} \right]$. A Figura 2.4, ilustra a interseção da reta

$a = 1$ ($ax + by = 1$) com \mathbb{Z}^2 . Neste caso, o erro $\xi_1 = \frac{(bx - ay)\delta_c}{a^2 + b^2}$ é majorado por $\frac{n+1}{1+(n+1)^2} = \frac{b}{1+b^2}$.

2. Seja $(x, y) = (1, -1)$, consideramos $(a_0, b_0) = (0, 1)$. Logo, a família de vetores corresponde $\mathbf{v} = (n, n+1, c(n))$, onde $c = \left[-\frac{(n^2 + (n+1)^2)(1+2\alpha)}{2(1+2n)} \right]$ e $\alpha = \left[-\frac{1}{2} - \frac{\sqrt{3(n^2 + (n+1)^2) - 4(1+2n)}}{2\sqrt{n^2 + (n+1)^2}} \right]$. A Figura 2.5, ilustra a interseção da

reta $a + b = 1$ ($ax + by = 1$) com \mathbb{Z}^2 . Neste caso, o erro $\xi_1 = \frac{(bx - ay)\delta_c}{a^2 + b^2}$ é majorado por $\frac{1+2n}{n^2 + (n+1)^2} = \frac{1+2n}{2n^2 + 2n + 1}$.

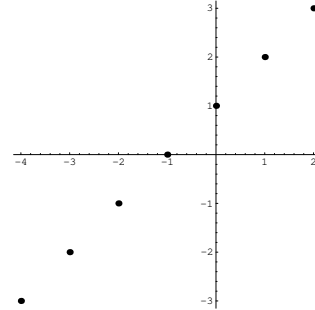
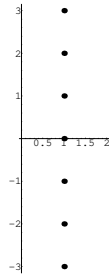


Figura 2.4: Interseção da reta $a = 1$ com \mathbb{Z}^2 . Figura 2.5: Interseção da reta $a + b = 1$ com \mathbb{Z}^2 .

Observação 2.4.7. No caso geral, fixados o par (x, y) e d , o erro $\xi_1 = \frac{(bx - ay)\delta_c}{a^2 + b^2}$ é majorado por: $\frac{d(bx - ay)\delta_c}{a^2 + b^2} = \frac{1}{\sqrt{a^2 + b^2}} \frac{d \langle (a, b), (-y, x) \rangle}{\sqrt{a^2 + b^2}} \leq \frac{d}{\sqrt{a^2 + b^2}} \|(-y, x)\|$. Portanto considerar vetor (x, y) com norma pequena, d pequeno e (a, b) com norma grande garantem erros bem pequenos, ou seja, convergência mais rápida ao reticulado hexagonal.

2.5 Projeção de \mathbb{Z}^4

Como no caso anterior, gostaríamos de exibir uma seqüência de vetores cuja densidade de empacotamento (ou de centro), do reticulado-projeção associado, converge para a densidade de empacotamento (ou de centro) do reticulado mais denso na dimensão três: o (*fcc*) cujo valor é $\Delta = \text{vol}(S^3) \frac{1}{4\sqrt{2}} = \frac{1}{4\sqrt{2}} \frac{4\pi}{3} (\approx 0.74048)$ e densidade de centro aproximadamente igual a 0.176777. Empiricamente, observamos que a densidade de centro dos reticulados-projeção fica bem aquém do valor acima, dando a impressão de que densidade de centro fosse inferior ao número 0.16238, que corresponde à densidade de centro do reticulado-projeção na direção do vetor $\mathbf{v} =$

$(1, 1, 1, 1)$, à semelhança do que ocorre na dimensão três onde a projeção na direção do vetor $\mathbf{v} = (1, 1, 1)$ resulta no reticulado hexagonal. Felizmente isso não é verdade.

Vimos na dimensão três que não há um ganho significativo em supor que o máximo divisor comum das duas primeiras coordenadas seja diferente de 1. Desta forma, trabalharemos por simplicidade apenas com hipótese de que o máximo divisor comum das duas primeiras coordenadas seja 1.

A principal dificuldade nesta dimensão começa na escolha de uma base conveniente do reticulado fcc para aproximarmos os reticulados-projeção. Como vimos na seção anterior, podemos descartar soluções boas ao ficarmos restritos a uma única base. Entretanto, dada a complexidade do problema consideraremos apenas bases tais que a matriz de Gram seja da forma:

$$G_{fcc} = \begin{bmatrix} 1 & 0 & \pm\frac{1}{2} \\ 0 & 1 & \pm\frac{1}{2} \\ \pm\frac{1}{2} & \pm\frac{1}{2} & 1 \end{bmatrix} \quad (2.45)$$

Iniciamos nossa análise supondo que $\mathbf{v} = (a_4, a_3, a_2, a_1)$, $\text{mdc}(a_4, a_3) = 1$ e $a_i < a_j$ se $j < i$.

A seguir discutiremos em várias etapas condições necessárias sobre estas coordenadas que possibilitem a convergência de $\mathcal{L}_{\mathbf{v}}$, para valores crescentes de $\|\mathbf{v}\|$, a um reticulado com a densidade do fcc . Estas condições serão sintetizadas no Teorema 2.5.1. O Corolário 2.5.1 dá as condições suficientes para a convergência ótima.

Tomamos x, y inteiros de tal forma que: $a_4 x + a_3 y = 1$. Nestas condições temos que a matriz:

$$A = \begin{bmatrix} a_4 & -y & 0 & 0 \\ a_3 & x & 0 & 0 \\ a_2 & 0 & 1 & 0 \\ a_1 & 0 & 0 & 1 \end{bmatrix}, \quad (2.46)$$

tem determinante igual a 1 e portanto suas colunas geram \mathbb{Z}^4 . Assim, o reticulado-projeção é gerado pela projeção dos vetores:

$$\mathbf{v}_2 = (-y, x, 0, 0), \mathbf{v}_3 = (0, 0, 1, 0) \text{ e } \mathbf{v}_4 = (0, 0, 0, 1), \quad (2.47)$$

ou seja,

$$\begin{aligned} \psi(\mathbf{v}_2) &= (-y (a_1^2 + a_2^2 + a_3^2) - x a_3 a_4, y a_3 a_4 + x (a_1^2 + a_2^2 + a_4^2), \\ &\quad a_2 (-x a_3 + y a_4), a_1 (-x a_3 + y a_4)) \\ \psi(\mathbf{v}_3) &= (-a_2 a_4, -a_2 a_3, a_1^2 + a_3^2 + a_4^2, -a_1 a_2) \\ \psi(\mathbf{v}_4) &= (-a_1 a_4, -a_1 a_3, -a_1 a_2, a_2^2 + a_3^2 + a_4^2) \end{aligned} \quad (2.48)$$

Uma conta simples mostra que $\|\psi(\mathbf{v}_4)\| \leq \|\psi(\mathbf{v}_3)\| \leq \|\psi(\mathbf{v}_2)\|$.

De forma análoga ao caso tridimensional, desejamos através de um número mínimo de reduções conseguir um reticulado cuja densidade de centro esteja próxima a de um reticulado equivalente ao *fcc*. Vamos impor que o reticulado-projeção seja uma perturbação do reticulado *fcc*.

A matriz do reticulado-projeção, a menos de dilatação é dada por:

$$G_{\mathbf{v}} = \begin{bmatrix} 1 & \frac{-a_1 a_2}{a_2^2 + a_3^2 + a_4^2} & \frac{a_1 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} \\ \frac{-a_1 a_2}{a_2^2 + a_3^2 + a_4^2} & \frac{a_1^2 + a_3^2 + a_4^2}{a_2^2 + a_3^2 + a_4^2} & \frac{a_2 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} \\ \frac{a_1 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} & \frac{a_2 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} & \frac{(x^2 + y^2)(a_1^2 + a_2^2) + 1}{a_2^2 + a_3^2 + a_4^2} \end{bmatrix}. \quad (2.49)$$

Sejam $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ os vetores geradores que determinam essa matriz de Gram. Suponhamos que através de uma redução da forma: troca de \mathbf{u}_2 por $\mathbf{u}'_2 = \mathbf{u}_2 - \alpha \mathbf{u}_1$, produza um sub-reticulado que é aproximadamente um \mathbb{Z}^2 , i.e., \mathbf{u}_2 e \mathbf{u}_1 são aproximadamente ortogonais e que $\|\mathbf{u}_2\| \approx \|\mathbf{u}_1\|$. Isto resultará numa matriz da forma:

$$G_{\mathbf{v}}(\alpha) = \begin{bmatrix} 1 & -\alpha - \frac{a_1 a_2}{a_2^2 + a_3^2 + a_4^2} & \frac{a_1 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} \\ -\alpha - \frac{a_1 a_2}{a_2^2 + a_3^2 + a_4^2} & 1 + \alpha^2 + \frac{a_1^2 + 2\alpha a_1 a_2 - a_2^2}{a_2^2 + a_3^2 + a_4^2} & \frac{(\alpha a_1 - a_2)(-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} \\ \frac{a_1 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} & \frac{(\alpha a_1 - a_2)(-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} & \frac{1 + (x^2 + y^2)(a_1^2 + a_2^2)}{a_2^2 + a_3^2 + a_4^2} \end{bmatrix}$$

desejamos que

$$G_{\mathbf{v}}(\alpha) = \begin{bmatrix} 1 & \xi_1 & \frac{a_1 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} \\ \xi_1 & 1 + \xi_2 & \frac{(\alpha a_1 - a_2)(-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} \\ \frac{a_1 (-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} & \frac{(\alpha a_1 - a_2)(-x a_3 + y a_4)}{a_2^2 + a_3^2 + a_4^2} & \frac{1 + (x^2 + y^2)(a_1^2 + a_2^2)}{a_2^2 + a_3^2 + a_4^2} \end{bmatrix}$$

onde $|\xi_1|, |\xi_2| \lll 1$, isto nos dá duas equações:

$$-\alpha - \frac{a_1 a_2}{a_2^2 + a_3^2 + a_4^2} = \xi_1 \quad (2.50)$$

$$1 + \alpha^2 + \frac{a_1^2 + 2\alpha a_1 a_2 - a_2^2}{a_2^2 + a_3^2 + a_4^2} = 1 + \xi_2, \quad (2.51)$$

as quais resultam em, se supusermos ξ_1, ξ_2 muito pequenos:

$$a_1 = -\frac{\alpha (a_2^2 + a_3^2 + a_4^2)}{a_2} \quad (2.52)$$

$$\alpha = -\frac{a_2^2}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}}. \quad (2.53)$$

Como a_1 e α são inteiros, vamos tomar:

$$a_1 = \left[-\frac{\alpha (a_2^2 + a_3^2 + a_4^2)}{a_2} \right] \quad (2.54)$$

$$\alpha = \left[-\frac{a_2^2}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \right]. \quad (2.55)$$

Vamos ver se garantimos as afirmações (2.50) e (2.51) com erros pequenos. Sejam

$$a_1 = -\frac{\alpha (a_2^2 + a_3^2 + a_4^2)}{a_2} + \delta_{a_1} \quad (2.56)$$

$$\alpha = -\frac{a_2^2}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} + \delta_\alpha. \quad (2.57)$$

Vamos estimar os erros ξ_1 e ξ_2 . Primeiro obtemos que:

$$\xi_1 = -\frac{a_2 \delta_{a_1}}{a_2^2 + a_3^2 + a_4^2}, \quad (2.58)$$

ξ_1 se torna muito pequeno para a_2 suficientemente grande o que é plausível quando a_3, a_4 vão para o infinito dado que $a_2 \geq a_3, a_4$. Vamos estimar ξ_2 , primeiro completando quadrados a equação (2.51) resulta em:

$$\xi_2 = \frac{a_1^2 (a_3^2 + a_4^2)}{(a_2^2 + a_3^2 + a_4^2)^2} - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \left(\alpha + \frac{a_1 a_2}{a_2^2 + a_3^2 + a_4^2} \right)^2 \quad (2.59)$$

$$\xi_2 = \frac{a_1^2 (a_3^2 + a_4^2)}{(a_2^2 + a_3^2 + a_4^2)^2} - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2 \quad (2.60)$$

substituindo o valor de a_1 temos:

$$\begin{aligned}
\xi_2 &= \frac{(a_3^2 + a_4^2) \left(-\frac{\alpha(a_2^2 + a_3^2 + a_4^2)}{a_2} + \delta_{a_1} \right)^2}{(a_2^2 + a_3^2 + a_4^2)^2} - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2 \\
&= (a_3^2 + a_4^2) \left(-\frac{\alpha}{a_2} + \frac{\delta_{a_1}}{a_2^2 + a_3^2 + a_4^2} \right)^2 - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2
\end{aligned} \tag{2.61}$$

substituindo o valor de α temos:

$$\begin{aligned}
\xi_2 &= (a_3^2 + a_4^2) \left(\frac{a_2}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} - \frac{\delta_\alpha}{a_2} + \frac{\delta_{a_1}}{a_2^2 + a_3^2 + a_4^2} \right)^2 \\
&\quad - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2 \\
&= \left(\frac{a_2}{\sqrt{a_2^2 + a_3^2 + a_4^2}} - \frac{\sqrt{a_3^2 + a_4^2} \delta_\alpha}{a_2} + \frac{\sqrt{a_3^2 + a_4^2} \delta_{a_1}}{a_2^2 + a_3^2 + a_4^2} \right)^2 \\
&\quad - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2 \\
&= \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} \left(1 - \frac{\sqrt{a_2^2 + a_3^2 + a_4^2} \sqrt{a_3^2 + a_4^2} \delta_\alpha}{a_2^2} + \frac{\sqrt{a_3^2 + a_4^2} \delta_{a_1}}{a_2 \sqrt{a_2^2 + a_3^2 + a_4^2}} \right)^2 \\
&\quad - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2
\end{aligned} \tag{2.62}$$

é claro que

$$\frac{\sqrt{a_3^2 + a_4^2} \delta_{a_1}}{a_2 \sqrt{a_2^2 + a_3^2 + a_4^2}} \xrightarrow{a_2 \rightarrow +\infty} 0, \tag{2.63}$$

logo

$$\xi_2 = \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} \left(1 - \frac{\sqrt{a_2^2 + a_3^2 + a_4^2} \sqrt{a_3^2 + a_4^2} \delta_\alpha}{a_2^2} \right)^2 - \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \xi_1^2. \tag{2.64}$$

Como ξ_1^2 fica pequeno quando a_2 é grande, para que esta última equação convirja a 0 é necessário que

$$\frac{\sqrt{a_2^2 + a_3^2 + a_4^2} \sqrt{a_3^2 + a_4^2} \delta_\alpha}{a_2^2} \xrightarrow{a_2 \rightarrow +\infty} 0 \tag{2.65}$$

e só podemos garantir isso se

$$\frac{a_3^2 + a_4^2}{a_2^2} \xrightarrow{a_2 \rightarrow +\infty} 0 \text{ ou } \delta_\alpha \rightarrow 0. \tag{2.66}$$

Suponhamos isso por enquanto.

Após esta primeira etapa da redução estamos com uma matriz de Gram $G_v(\alpha)$ no formato, a menos dos erros de aproximação:

$$\begin{bmatrix} 1 & 0 & \frac{a_2(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \\ 0 & 1 & \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \\ \frac{a_2(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} & \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} & 1 + 2(x^2 + y^2) \frac{a_2^2}{a_2^2 + a_3^2 + a_4^2} + \frac{(x^2 + y^2) a_2^4}{a_3^2 + a_4^2} \end{bmatrix}.$$

Os vetores que produzem tal matriz são $\mathbf{u}_1, \mathbf{u}'_2, \mathbf{u}_3$. Suponha que através de uma redução da forma: troca de \mathbf{u}_3 por $\mathbf{u}'_3 = \gamma \mathbf{u}'_2 - \beta \mathbf{u}_1$, produza um reticulado próximo ao reticulado *fcc*, i.e., $\langle \mathbf{u}'_3, \mathbf{u}_1 \rangle \cong \frac{1}{2}$, $\langle \mathbf{u}'_3, \mathbf{u}'_2 \rangle \cong \frac{1}{2}$ e $\|\mathbf{u}_1\| \cong \|\mathbf{u}'_2\| \cong \|\mathbf{u}'_3\|$.

Infelizmente não conseguimos garantir $\langle \mathbf{u}'_3, \mathbf{u}_1 \rangle \cong \frac{1}{2}$ para todos a_4, a_3, a_2, x, y . Na seqüência veremos como contornar esse problema ao trabalhar com famílias específicas. Admitamos que $\langle \mathbf{u}'_3, \mathbf{u}_1 \rangle = t$, onde $|t| \leq \frac{1}{2}$ e depois tentaremos achar famílias as quais $|t| \cong \frac{1}{2}$, mesmo que não consigamos isso veremos que é possível aproximarmos de um reticulado cuja matriz de Gram é:

$$G_t = \begin{bmatrix} 1 & 0 & t \\ 0 & 1 & \frac{1}{2} \\ t & \frac{1}{2} & 1 \end{bmatrix}. \quad (2.67)$$

Esse reticulado é relativamente denso pois, sua densidade de centro é dada por:

$$\delta(t) = \frac{1}{2\sqrt{3-4t^2}}, \quad (2.68)$$

vide figura 2.6.

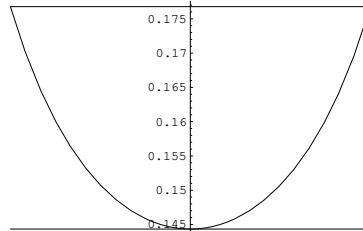


Figura 2.6: Gráfico $\delta(t)$, $t \in [-0.5, 0.5]$

A função $\delta(t)$ possui mínimo em $\delta(0) = \frac{1}{4\sqrt{3}} = 0.144338$, que corresponde a densidade de centro do reticulado denso $A_2 \times \mathbb{Z}$ e máximo em $\delta(\pm 0.5) = \frac{1}{4\sqrt{2}} = 0.176777$, que corresponde a do desejado fcc .

Após a redução, correspondente a troca \mathbf{u}_3 por $\mathbf{u}'_3 = \gamma \mathbf{u}'_2 - \beta \mathbf{u}_1$ obtemos a matriz de Gram $G(\beta, \gamma)$:

$$\begin{bmatrix} 1 & 0 & -\beta + \frac{a_2(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \\ * & 1 & -\gamma + \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \\ * & * & \frac{a_2^2 + a_3^2 + a_4^2}{(a_3^2 + a_4^2)^2} + \left(\gamma - \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \right)^2 + \left(\beta - \frac{a_2(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \right)^2 \end{bmatrix}.$$

Queremos que $G(\beta, \gamma) = G_t$, isto resulta em três equações:

$$t = -\beta + \frac{a_2(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \quad (2.69)$$

$$\frac{1}{2} = -\gamma + \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \quad (2.70)$$

$$1 = \frac{a_2^2 + a_3^2 + a_4^2}{(a_3^2 + a_4^2)^2} + \left(\gamma - \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \right)^2 + \left(\beta - \frac{a_2(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \right)^2 \quad (2.71)$$

Impondo a condição na primeira equação corresponde $\langle \mathbf{u}'_3, \mathbf{u}_1 \rangle = t$, reduzimos o sistema de equações acima para:

$$\frac{1}{2} = -\gamma + \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \quad (2.72)$$

$$1 = \frac{a_2^2 + a_3^2 + a_4^2}{(a_3^2 + a_4^2)^2} + \left(\gamma - \frac{a_2(-x a_3 + y a_4)}{a_3^2 + a_4^2} \right)^2 + t^2. \quad (2.73)$$

Resolvendo a equação (2.72) em relação a_2 temos:

$$a_2 = -\frac{(1 + 2\gamma)(a_3^2 + a_4^2)}{2x a_3 - 2y a_4} \quad (2.74)$$

e com esse valor de a_2 resolvemos a equação (2.73) em relação γ obtendo:

$$\gamma = -\frac{1}{2} - \frac{(x a_3 - y a_4) \sqrt{-4 + (3 - 4t^2)(a_3^2 + a_4^2)}}{2\sqrt{a_3^2 + a_4^2}} \quad (2.75)$$

mas γ e a_2 devem ser inteiros então tomaremos o arredondamento dos resultados obtidos acima, logo:

$$a_2 = -\frac{(1+2\gamma)(a_3^2+a_4^2)}{2xa_3-2ya_4} + \delta_{a_2} \quad (2.76)$$

e

$$\gamma = -\frac{1}{2} - \frac{(xa_3-ya_4)\sqrt{-4+(3-4t^2)(a_3^2+a_4^2)}}{2\sqrt{a_3^2+a_4^2}} + \delta_\gamma \quad (2.77)$$

Queremos garantir que os erros dados pelas equações (2.72) e (2.73) sejam muito pequenos. Denotaremos esses erros por ξ_3 e ξ_4 , ou seja:

$$\xi_3 = -\gamma + \frac{a_2(-xa_3+ya_4)}{a_3^2+a_4^2} - \frac{1}{2} \quad (2.78)$$

e

$$\xi_4 = \frac{a_2^2+a_3^2+a_4^2}{(a_3^2+a_4^2)^2} + \left(\gamma - \frac{a_2(-xa_3+ya_4)}{a_3^2+a_4^2}\right)^2 + t^2 - 1 \quad (2.79)$$

Substituindo os valores de a_2 e γ nestas equações temos:

$$\xi_3 = \frac{(-xa_3+ya_4)\delta_{a_2}}{a_3^2+a_4^2} \quad (2.80)$$

ξ_3 deve estar suficientemente próximo de 0 desde que $\|(a_3, a_4)\|$ seja suficientemente grande e x e y fixos. Já o erro ξ_4 é dado por:

$$\begin{aligned} \xi_4 &= \frac{a_2^2+a_3^2+a_4^2}{(a_3^2+a_4^2)^2} + \left(\gamma - \frac{a_2(-xa_3+ya_4)}{a_3^2+a_4^2}\right)^2 + t^2 - 1 \\ &= \frac{a_2^2+a_3^2+a_4^2}{(a_3^2+a_4^2)^2} + \left(\frac{1}{2} + \xi_3\right)^2 + t^2 - 1 \end{aligned}$$

substituindo o valor de a_2 temos:

$$\begin{aligned} \xi_4 &= \frac{a_3^2+a_4^2 + \left(-\frac{(1+2\gamma)(a_3^2+a_4^2)}{2a_3x-2a_4y} + \delta_2\right)^2}{(a_3^2+a_4^2)^2} + \left(\frac{1}{2} + \xi_3\right)^2 + t^2 - 1 \\ &= \frac{1}{a_3^2+a_4^2} + \left(-\frac{(1/2+\gamma)}{a_3x-a_4y} + \frac{\delta_2}{a_3^2+a_4^2}\right)^2 + \left(\frac{1}{2} + \xi_3\right)^2 + t^2 - 1 \end{aligned}$$

substituindo o valor de γ temos:

$$\xi_4 = \left(\frac{\sqrt{-4 + (3 - 4t^2)(a_3^2 + a_4^2)}}{2\sqrt{a_3^2 + a_4^2}} - \frac{\delta_\gamma}{a_3 x - a_4 y} + \frac{\delta_2}{a_3^2 + a_4^2} \right)^2 + \frac{1}{a_3^2 + a_4^2} + \left(\frac{1}{2} + \xi_3 \right)^2 + t^2 - 1$$

como

$$\begin{aligned} & - \frac{\delta_\gamma}{a_3 x - a_4 y} + \frac{\delta_2}{a_3^2 + a_4^2} \xrightarrow{a_3, a_4 \rightarrow +\infty} 0 \\ \xi_4 \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} & \frac{1}{a_3^2 + a_4^2} + \left(\frac{\sqrt{-4 + (3 - 4t^2)(a_3^2 + a_4^2)}}{2\sqrt{a_3^2 + a_4^2}} \right)^2 + \left(\frac{1}{2} + \xi_3 \right)^2 + t^2 - 1 \\ \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} & \frac{1}{a_3^2 + a_4^2} + \frac{-1}{a_3^2 + a_4^2} + \frac{(3 - 4t^2)}{4} + \left(\frac{1}{2} + \xi_3 \right)^2 + t^2 - 1 \\ \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} & \frac{3}{4} - t^2 + \left(\frac{1}{2} + \xi_3 \right)^2 + t^2 - 1 \\ \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} & -\frac{1}{4} + \left(\frac{1}{2} + \xi_3 \right)^2 \end{aligned}$$

já vimos que $\xi_3 \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} 0$, assim

$$\xi_4 \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} 0. \quad (2.81)$$

Falta garantir que $\xi_2 \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} 0$. Para isso vamos mostrar que $\frac{a_3^2 + a_4^2}{a_2^2} \xrightarrow{a_2 \rightarrow +\infty} 0$. Note que:

$$\gamma \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} -\frac{1}{2} - \frac{(x a_3 - y a_4) \sqrt{3 - 4t^2}}{2} \quad (2.82)$$

logo

$$a_2 \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} \frac{\sqrt{3 - 4t^2} (a_3^2 + a_4^2)}{2}. \quad (2.83)$$

Assim

$$\frac{a_3^2 + a_4^2}{a_2^2} \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} \frac{4}{(3 - 4t^2)(a_3^2 + a_4^2)} \xrightarrow{\|(a_3, a_4)\| \rightarrow +\infty} 0 \quad (2.84)$$

Note a semelhança como no caso da projeção de \mathbb{Z}^3 , aqui também necessitamos garantir que uma razão, no caso $\frac{(-x a_3 + y a_4) \delta_{a_2}}{a_3^2 + a_4^2}$ seja pequena quando um certo par, (a_3, a_4) , tenha norma suficientemente grande. Isso não é um empecilho, pois, como vimos na seção anterior, basta fixar

x e y e tomar r e l os menores inteiros tais que $r x + l y = 1$ e assim temos, ao considerar $a_4 = r - n y$ e $a_3 = l + l x$, que esta razão fica pequena.

Ainda não sabemos o comportamento de t e portanto não sabemos ao certo para qual reticulado esta seqüência de vetores converge. Façamos isso agora, lembrando que β é inteiro e t é dado por:

$$t = -\beta + \frac{a_2 (-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}}. \quad (2.85)$$

Queremos o comportamento em termos da convergência. Assim, temos que analisar a expressão para a_3 e a_4 suficientemente grandes. Nestas condições, como a_2 é de ordem quadrática em relação a norma do vetor (a_4, a_3) , é fácil ver que a expressão acima aproxima-se assintoticamente da expressão:

$$t \xrightarrow{a_2 \rightarrow \infty} -\beta + \frac{(-x a_3 + y a_4)}{\sqrt{a_3^2 + a_4^2}}. \quad (2.86)$$

Vamos estimar o comportamento dessa expressão supondo $a_4 = r - n y$ e $a_3 = l + n x$, já que estes valores garantem erros pequenos, quando n vai ao infinito.

$$t = -\beta + \frac{-l x + r y - n (x^2 + y^2)}{\sqrt{l^2 + r^2 + 2 n (l x - r y) + n^2 (x^2 + y^2)}} \xrightarrow{n \rightarrow \infty} -\beta - \sqrt{x^2 + y^2}. \quad (2.87)$$

Tomando $\beta = [-\sqrt{x^2 + y^2}]$ temos que $|t| \leq 1/2$.

Como conseqüência destes cálculos fica demonstrado o próximo resultado:

Teorema 2.5.1. *Dados x, y inteiros coprimos, sejam $a_4 = r - n y$, $a_3 = l + n x$, com $r x + l y = 1$ e $t = [\sqrt{x^2 + y^2}] - \sqrt{x^2 + y^2}$. Definimos*

$$a_1 = \left[-\frac{\alpha (a_2^2 + a_3^2 + a_4^2)}{a_2} \right] \quad (2.88)$$

$$\alpha = \left[-\frac{a_2^2}{\sqrt{a_3^2 + a_4^2} \sqrt{a_2^2 + a_3^2 + a_4^2}} \right] \quad (2.89)$$

$$a_2 = \left[\frac{(1 + 2 \gamma) (a_3^2 + a_4^2)}{2 x a_3 - 2 y a_4} \right] \quad (2.90)$$

$$\gamma = \left[-\frac{1}{2} - \frac{(x a_3 - y a_4) \sqrt{-4 + (3 - 4 t^2) (a_3^2 + a_4^2)}}{2 \sqrt{a_3^2 + a_4^2}} \right] \quad (2.91)$$

Então o reticulado-projeção determinado por $\mathbf{v} = (a_4, a_3, a_2, a_1)$ converge, quando n tende ao infinito, para o reticulado \mathcal{L}_t , cuja matriz de Gram é dada por:

$$G_t = \begin{bmatrix} 1 & 0 & t \\ 0 & 1 & \frac{1}{2} \\ t & \frac{1}{2} & 1 \end{bmatrix}. \quad (2.92)$$

Gostaríamos que a convergência acima resultasse no reticulado fcc . Não podemos garantir isso porque a convergência acima está na dependência do valor fracionário de $\sqrt{x^2 + y^2}$. Por exemplo, para ternas pitagóricas da forma $(x, y, -\beta)$ isto implica para n grande, $t \rightarrow 0$. Logo, só conseguiremos aproximarmos do reticulado $\mathcal{A}_2 \times \mathbb{Z}$.

Uma pergunta conveniente agora é a seguinte: Existe uma seqüência de vetores cujos reticulados-projeção convergem para o reticulado fcc ? A resposta disso está na dependência de encontrarmos um par de inteiros coprimos (x, y) com a seguinte propriedade $\|(x, y)\| - \lfloor \|(x, y)\| \rfloor = \pm \frac{1}{2}$. Logo, vamos procurar tais inteiros, empiricamente, fixado y , o valor conveniente para x é y^2 . Como y e y^2 não são coprimos (salvo se $y = \pm 1$) consideraremos $x = y^2 \pm 1$ como a solução boa para o problema:

$$\sqrt{y^2 + (y^2 - 1)^2} = \sqrt{y^4 - y^2 + 1} = \sqrt{\left(y^2 - \frac{1}{2}\right)^2 + \frac{3}{4}}. \quad (2.93)$$

Esta última expressão aproxima assintoticamente do valor $y^2 - \frac{1}{2}$.

Corolário 2.5.1. *Nas mesmas condições do Teorema (2.5.1). Se $x = y^2 - 1$ então o reticulado-projeção está próximo do reticulado fcc quando y e n forem suficientemente grandes.*

Na seqüência, mostramos na Tabela 2.4 o resultado do cálculo de t quando $x = y^2 - 1$.

y	t	y	t	y	t	y	t	y	t
2	0.394449	11	0.496888	20	0.499061	29	0.499554	68	0.499919
3	0.455996	12	0.497387	21	0.499149	30	0.499583	69	0.499921
4	0.475825	13	0.497774	22	0.499224	31	0.499610	70	0.499923
5	0.484699	14	0.498082	23	0.499290	32	0.499634	71	0.499926
6	0.489438	15	0.498330	24	0.499348	33	0.499655	72	0.499928
7	0.492269	16	0.498532	25	0.499400	34	0.499675	73	0.499930
8	0.494095	17	0.498700	26	0.499445	35	0.499694	74	0.499932
9	0.495342	18	0.498841	27	0.499485	36	0.499711	75	0.499933
10	0.496231	19	0.498960	28	0.499521	37	0.499726	76	0.499935

Tabela 2.4: Ilustração dos valores de $t = \lceil \sqrt{y^2 + (y^2 - 1)^2} \rceil - \sqrt{x^2 + y^2}$.

Vamos comparar algumas performances.

\mathbf{v}	δ	\mathbf{v}	δ	\mathbf{v}	δ
(1, 14, 176, 2125)	0.13391	(1, 26, 586, 12917)	0.14049	(1, 38, 1236, 39589)	0.13938
(1, 15, 188, 2270)	0.12933	(1, 27, 635, 14631)	0.13979	(1, 39, 1307, 43169)	0.13903
(1, 16, 217, 2836)	0.13417	(1, 28, 687, 16515)	0.13980	(1, 40, 1381, 46993)	0.14103
(1, 17, 247, 3474)	0.13380	(1, 29, 740, 18528)	0.13943	(1, 41, 1456, 51000)	0.14060
(1, 18, 280, 4217)	0.13833	(1, 30, 766, 19179)	0.13764	(1, 42, 1534, 55265)	0.14180
(1, 19, 314, 5042)	0.13749	(1, 31, 822, 21402)	0.13732	(1, 43, 1613, 59723)	0.14145
(1, 20, 351, 5986)	0.13851	(1, 32, 881, 23818)	0.13981	(1, 44, 1695, 64453)	0.14095
(1, 21, 389, 7022)	0.13817	(1, 33, 941, 26380)	0.13933	(1, 45, 1733, 65898)	0.13883
(1, 22, 430, 8191)	0.13720	(1, 34, 1004, 29149)	0.14153	(1, 46, 1818, 70947)	0.14054
(1, 23, 449, 8553)	0.13454	(1, 35, 1068, 32074)	0.14113	(1, 47, 1904, 76206)	0.14020
(1, 24, 493, 9883)	0.13783	(1, 36, 1135, 35220)	0.14051	(1, 48, 1993, 81760)	0.14187
(1, 25, 538, 11322)	0.13734	(1, 37, 1203, 38532)	0.14016	(1, 49, 2083, 87534)	0.14147

Tabela 2.5: Considerando $x = 1$ e $y = 0$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.144338

\mathbf{v}	δ	\mathbf{v}	δ
(14, 13, 277, 3896)	0.14427	(32, 31, 1497, 50943)	0.16166
(15, 14, 327, 5253)	0.15871	(33, 32, 1609, 56361)	0.16376
(16, 15, 365, 6227)	0.15707	(34, 33, 1692, 60960)	0.16300
(17, 16, 421, 7601)	0.16028	(35, 34, 1812, 67093)	0.16283
(18, 17, 464, 8841)	0.16000	(36, 35, 1900, 72250)	0.15986
(19, 18, 528, 10586)	0.15892	(37, 36, 2026, 79065)	0.15957
(20, 19, 576, 12124)	0.16270	(38, 37, 2157, 88490)	0.16025
(21, 20, 646, 14241)	0.16072	(39, 38, 2253, 92427)	0.15887
(22, 21, 699, 16107)	0.15854	(40, 39, 2390, 102826)	0.16144
(23, 22, 777, 18679)	0.15307	(41, 40, 2491, 107170)	0.16108
(24, 23, 835, 20908)	0.15740	(42, 41, 2636, 118679)	0.16259
(25, 24, 919, 23928)	0.15698	(43, 42, 2742, 126193)	0.16186
(26, 25, 982, 26550)	0.16108	(44, 43, 2893, 136032)	0.16182
(27, 26, 1074, 31184)	0.15934	(45, 44, 3004, 144255)	0.16287
(28, 27, 1142, 33156)	0.15285	(46, 45, 3163, 155051)	0.16113
(29, 28, 1240, 38481)	0.16103	(47, 46, 3279, 164016)	0.16331
(30, 29, 1313, 40744)	0.15628	(48, 47, 3444, 175711)	0.16293
(31, 30, 1419, 46870)	0.16111	(49, 48, 3565, 185449)	0.16471

Tabela 2.6: Considerando $x = 1$ e $y = -1$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.164356

\mathbf{v}	δ	\mathbf{v}	δ
(35, 93, 7275, 531174)	0.16916	(92, 245, 50433, 9733831)	0.16387
(38, 101, 8570, 677137)	0.16462	(95, 253, 53755, 10697515)	0.16822
(41, 109, 9984, 858741)	0.15967	(98, 261, 57217, 11729763)	0.16961
(44, 117, 11507, 1058769)	0.16326	(101, 269, 60786, 12886920)	0.16190
(47, 125, 13137, 1287559)	0.16905	(104, 277, 64464, 14053448)	0.16896
(50, 133, 14859, 1560338)	0.15768	(107, 285, 68214, 15280240)	0.16976
(53, 141, 16705, 1854406)	0.15909	(110, 293, 72106, 16584692)	0.16951
(56, 149, 18658, 2183145)	0.16943	(113, 301, 76107, 18037681)	0.16665
(59, 157, 20720, 2569448)	0.16204	(116, 309, 80215, 19492575)	0.16694
(62, 165, 22869, 2973147)	0.15629	(119, 317, 84392, 21013946)	0.16966
(65, 173, 25145, 3419905)	0.16720	(122, 325, 88716, 22711644)	0.16460
(68, 181, 27530, 3909453)	0.16860	(125, 333, 93147, 24404870)	0.16543
(71, 189, 30022, 4473480)	0.16787	(128, 341, 97687, 26180480)	0.16963
(74, 197, 32598, 5052901)	0.16464	(131, 349, 102291, 28028106)	0.16956
(77, 205, 35306, 5684485)	0.16493	(134, 357, 107045, 30080027)	0.16416
(80, 213, 38121, 6404556)	0.16548	(137, 365, 111908, 32117986)	0.16864
(83, 221, 41017, 7137194)	0.16934	(140, 373, 116878, 34245652)	0.16935
(86, 229, 44047, 7928705)	0.16256	(143, 381, 121909, 36573108)	0.16308
(89, 237, 47186, 8776849)	0.16943	(146, 389, 127095, 38891486)	0.16676

Tabela 2.7: Considerando $x = 8$ e $y = -3$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.169779

\mathbf{v}	δ	\mathbf{v}	δ
(19, 188, 25341, 3395883)	0.14568	(179, 1772, 2251363, 2845724613)	0.17518
(29, 287, 59057, 12106974)	0.13655	(189, 1871, 2509948, 3350782461)	0.16772
(39, 386, 106831, 29378912)	0.11164	(199, 1970, 2782607, 3909564815)	0.17035
(49, 485, 168655, 58355117)	0.13575	(209, 2069, 3069300, 4530288880)	0.16668
(59, 584, 244534, 101971266)	0.13196	(219, 2168, 3370048, 5213466436)	0.16430
(69, 683, 334474, 162889524)	0.15658	(229, 2267, 3684873, 5958441919)	0.16918
(79, 782, 438462, 244662582)	0.16434	(239, 2366, 4013730, 6775178618)	0.17141
(89, 881, 556503, 349484769)	0.15300	(249, 2465, 4356640, 7658975597)	0.16935
(99, 980, 688609, 481338676)	0.17332	(259, 2564, 4713631, 8621233676)	0.17611
(109, 1079, 834760, 642766285)	0.16152	(269, 2663, 5084651, 9660839577)	0.16936
(119, 1178, 994965, 835771784)	0.16833	(279, 2762, 5469725, 10775361026)	0.17214
(129, 1277, 1169236, 1065175280)	0.16031	(289, 2861, 5868852, 11978329808)	0.16961
(139, 1376, 1357550, 1333115484)	0.15739	(299, 2960, 6282064, 13267722144)	0.16790
(149, 1475, 1559918, 1641035218)	0.16699	(309, 3059, 6709301, 14639697856)	0.17109
(159, 1574, 1776356, 1994849370)	0.16883	(319, 3158, 7150592, 16110286950)	0.17271
(169, 1673, 2006832, 2394152257)	0.16562	(329, 3257, 7605969, 17668669260)	0.17209

Tabela 2.8: Considerando $x = 99$ e $y = -10$ no Teorema 2.5.1, a densidade de centro converge para o valor 0.176117

Notamos, nesta última tabela, que para o o vetor $(259, 2564, 4713631, 8621233676)$ atingimos a densidade 0.17611, que está muito próxima da máxima 0.17677.

2.6 Algoritmo para Encontrar Mínimo em Reticulados-projeção

2.6.1 Distância de um Conjunto Discreto a uma Reta

A primeira idéia para encontrar o mínimo do reticulado-projeção é calcular a distância entre: todos os pontos de coordenadas inteiras, contidos no paralelepípedo de diagonal $\mathbf{v} = (a_1, \dots, a_n)$ e a reta gerada por \mathbf{v} . Isso resulta no cálculo de $\prod_i a_i$ normas e este número é significativamente grande para projeção de vetores com coordenadas grandes, ou em dimensões altas. Por simetria, esse número pode ser reduzido a $\prod_{i, a_i \neq 1} \lfloor \frac{a_i}{2} \rfloor$, mesmo assim os cálculos envolvidos serão muito numerosos. Por exemplo, para $\mathbf{v} = (1, 2^k, 2^{k+1})$ necessita-se o cálculo de $2^{k-1} 2^k = 2^{2k-1}$ normas e se $\mathbf{v} = (1, 4, \dots, 4) \in \mathbb{R}^{k+1}$ necessita-se o cálculo de 2^k normas.

O algoritmo citado no início do capítulo faz o cálculo de $c 2^{n-1}$ normas onde $c = \max_i \lfloor \frac{a_i}{2} \rfloor$ e $\mathbf{v} \in \mathbb{Z}^n$. Esse número é bem menor que o número acima já que este procedimento equivale a tomar caixas com vértices inteiros contendo o segmento de reta ligando $\mathbf{0}$ a $\mathbf{v}/2$ e calcular a distância de seus vértices a este segmento; logo, temos que tomar o cuidado de retirar os eventuais pontos de \mathbb{Z}^n que tenham as i -ésima coordenada maior que $\frac{a_i}{2}$, vide figuras 2.7 e 2.8. Mesmo esse algoritmo é muito custoso.

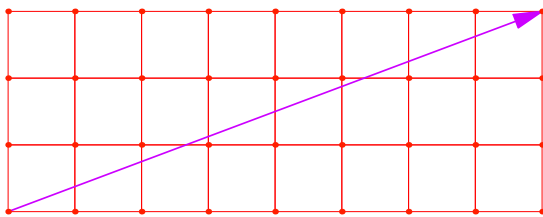


Figura 2.7: Vetor $\mathbf{v} = (3, 8)$.

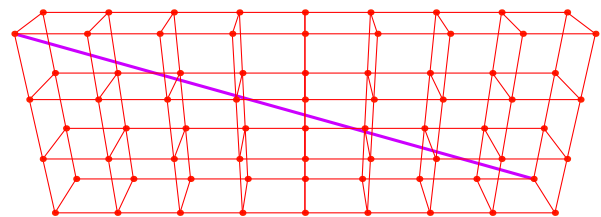


Figura 2.8: Vetor $\mathbf{v} = (1, 3, 8)$.

Nesse sentido seria interessante achar um algoritmo mais eficiente. Com esse objetivo conseguimos a implementação de um algoritmo para obtenção da base de Minkowski, mencionado no Capítulo, 1 o qual tem uma performance muito melhor que os algoritmos acima em dimensões baixas. No entanto, a geometria do problema levava a crer que deveria existir uma maneira mais eficiente que dependesse mais do vetor \mathbf{v} do que da dimensão e de fato existe como mostraremos a seguir.

2.6.2 Utilizando as Regiões de Voronoi (Algoritmo RV).

Esta seção visa descrever um algoritmo, proposto em [48], para busca do vetor mínimo em reticulados-projeção.

Uma forma muito eficiente de se determinar o mínimo é considerar apenas os pontos $\mathbf{u} \in \mathbb{Z}^n$ tais que o vetor \mathbf{v} perfura a região de Voronoi de \mathbf{u} .

Consideremos $P \neq \mathbf{0}$ o ponto da reta que realiza a distância entre reta e a caixa contendo $\mathbf{v}/2$. Como P está mais perto de um ponto \mathbf{u} do que qualquer outro ponto de \mathbb{Z}^n ele deve pertencer a região de Voronoi de \mathbf{u} , ou seja, basta considerar vetores $\mathbf{u} \in \mathbb{Z}^n$ cujas regiões de Voronoi são interceptadas pelo segmento de reta ligando $\mathbf{0}$ e $\mathbf{v}/2$ (figuras 2.9 e 2.6.2). Assim, temos o algoritmo:

Esquemmatizando o algoritmo RV:

- 1 Entrada: $\mathbf{v} = (a_1, \dots, a_n)$;
- 2 $L = 1, T = \emptyset$;
- 3 Enquanto $L \leq n$ faça
 - $T \cup \{t \in (0, \frac{1}{2}); \text{Fr}(t a_L) = \frac{1}{2}\}$, onde $\text{Fr}(x) = \text{parte fracionária de } x$;
 - Faça $L = L + 1$;
- 4 Faça $d = \min(\{d([\![t \mathbf{v}]\!], \mathbf{v}); t \in T\})$;
- 5 Saída d .

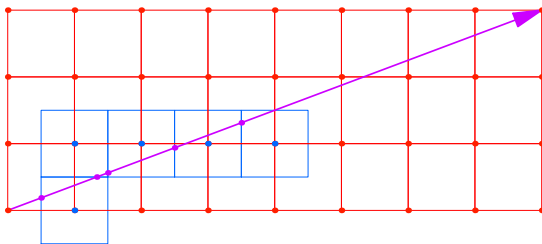


Figura 2.9: Regiões de Voronoi dos pontos \mathbf{u} que são atingidas pelo vetor $\mathbf{v} = (3, 8)$.

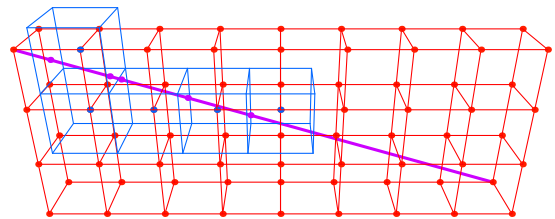


Figura 2.10: Regiões de Voronoi dos pontos \mathbf{u} que são atingidas pelo vetor $\mathbf{v} = (1, 3, 8)$.

Vamos estimar o número de normas a ser calculado por este algoritmo.

Para que o segmento de reta $t \mathbf{v}$, $t \in [0, 0.5]$ mude de região de Voronoi é necessário encontrar os valores $t \in [0, 0.5]$ tais que $t a_i$ tenha parte fracionária igual a $\frac{1}{2}$, vide as figuras 2.7 e 2.8. Ou

seja, cada índice i contribui com exatamente $\frac{a_i}{2}$ valores de t . Totalizando um número no máximo igual a

$$\sum_i \left\lfloor \frac{v_i}{2} \right\rfloor. \quad (2.94)$$

Este número pode ser bem menor caso os conjuntos dos valores t encontrados para índices distintos i e j tenham uma interseção não nula.

Este cálculo é bem mais econômico se comparado aos algoritmos citados no início da seção.

A próxima tabela compara a velocidade que este algoritmo encontra o mínimo em dimensões altas comparando com o algoritmo LLL que é muito rápido mas que não foi feito para encontrar o mínimo. Os tempos são dados em segundos, e os programas foram executados no mesmo computador.

Vetores	LLL	$k \times LLL$	RV	$\mathcal{N}(\mathcal{L})$	$\mathcal{N}(\mathcal{L})^*$
$\mathbf{v}_7 \in \mathbb{Z}^{30}$	0.234*	0.619*	1.765	0.8861	0.8980
$\mathbf{v}_8 \in \mathbb{Z}^{45}$	0.859	4.109	3.546	0.9481	—
$\mathbf{v}_9 \in \mathbb{Z}^{60}$	1.937	26.813	5.125	0.9585	—
$\mathbf{v}_{10} \in \mathbb{Z}^{75}$	5.219	29.875	5.938	0.9580	—
$\mathbf{v}_{11} \in \mathbb{Z}^{90}$	9.953	67.250	8.187	0.9677	—
$\mathbf{v}_{12} \in \mathbb{Z}^{100}$	16.344	159.453	8.344	0.9010	—

(2.95)

Nestes exemplos as reduções do algoritmo LLL e do $k \times LLL$ continham o vetor que realizava o mínimo exceto no caso (*). Os vetores utilizados na conta acima foram gerados aleatoriamente com a restrição que apenas o tamanho da maior coordenada que não excedesse 10000. Tais vetores são:

$$\begin{aligned} \mathbf{v}_7 &= (560, 868, 1069, 1351, 1513, 1529, 1550, 1618, 1771, 1890, 1954, 2231, 2819, 3033, 3556, 3881, 3941, \\ &\quad 3963, 5456, 6221, 6614, 7160, 7432, 7919, 8234, 8488, 8660, 8795, 8877, 9276), \\ \mathbf{v}_8 &= (151, 813, 839, 1373, 1511, 1909, 2046, 2726, 3049, 3112, 3498, 3733, 3780, 3919, 4209, 4501, 5006, 5049, \\ &\quad 5147, 5888, 6234, 6366, 6372, 6372, 6448, 6802, 6851, 6971, 7256, 7530, 7579, 7588, 7652, 7979, 8215, \\ &\quad 8529, 8740, 9637, 9699, 9770, 9797, 9804, 9908, 9934, 9991), \\ \mathbf{v}_9 &= (392, 1046, 1162, 1233, 1649, 1828, 1982, 2197, 2289, 2574, 2637, 2711, 2758, 2822, 2859, 3182, 3328, \\ &\quad 3679, 3762, 3816, 3985, 4153, 4195, 4473, 4481, 4544, 4710, 4740, 5046, 5164, 5190, 5663, 5970, 6030, \\ &\quad 6111, 6218, 6354, 7210, 7247, 7377, 7698, 7745, 7849, 7900, 8089, 8199, 8220, 8284, 8330, 8474, 8668, \\ &\quad 8717, 8807, 8923, 8952, 9010, 9116, 9242, 9396, 9594), \end{aligned}$$

$$\begin{aligned} \mathbf{v}_{10} &= (69, 141, 214, 266, 275, 459, 609, 774, 819, 860, 894, 913, 1163, 1198, 1233, 1668, 1861, 2024, 2060, 2198, \\ &2321, 2491, 2534, 2886, 3368, 3483, 3527, 3832, 3928, 3986, 4170, 4282, 4373, 4460, 4625, 4687, 4764, \\ &4988, 4996, 5018, 5023, 5164, 5351, 5620, 5720, 5801, 5984, 6056, 6091, 6133, 6230, 6285, 6346, 6593, \\ &6919, 6988, 7002, 7118, 7422, 7550, 7943, 8055, 8182, 8513, 8547, 8628, 8770, 9019, 9190, 9295, 9334, \\ &9451, 9588, 9706, 9937), \\ \mathbf{v}_{11} &= (68, 77, 275, 351, 370, 664, 1041, 1176, 1305, 1334, 1642, 1835, 1961, 2291, 2301, 2639, 2755, 2813, 2820, \\ &2879, 3052, 3064, 3328, 3341, 3411, 3436, 3629, 3765, 3830, 3995, 4022, 4093, 4287, 4292, 4374, 4428, \\ &4597, 4766, 4858, 4969, 5009, 5394, 5401, 5411, 5450, 5564, 5664, 5714, 5884, 6002, 6059, 6134, 6225, \\ &6282, 6298, 6371, 6512, 6553, 6614, 6622, 6862, 6928, 6932, 7081, 7121, 7128, 7152, 7220, 7237, 7309, \\ &7465, 7490, 7626, 7770, 7892, 7944, 7979, 8113, 8340, 8343, 8373, 8482, 8574, 9059, 9195, 9281, 9370, \\ &9541, 9613, 9965), \\ \mathbf{v}_{12} &= (26, 131, 374, 418, 595, 610, 613, 765, 868, 876, 906, 1094, 1114, 1211, 1538, 1855, 1889, 1987, 2007, \\ &2073, 2521, 2630, 2964, 3035, 3122, 3145, 3159, 3419, 3459, 3534, 3585, 3659, 3741, 3752, 3785, 3896, \\ &3941, 4013, 4029, 4064, 4072, 4154, 4317, 4732, 4799, 4897, 4949, 5172, 5258, 5413, 5431, 5486, 5608, \\ &5640, 5689, 5791, 5855, 5901, 5929, 5998, 6178, 6277, 6430, 6438, 6497, 6541, 6596, 6612, 6777, 6819, \\ &6919, 7086, 7100, 7197, 7232, 7377, 7480, 7549, 7786, 7866, 7871, 7966, 8116, 8123, 8273, 8336, 8456, \\ &8490, 8615, 8669, 8814, 8911, 9125, 9178, 9253, 9283, 9470, 9512, 9697, 9869). \end{aligned}$$

Parte II

Grafos Circulantes

Capítulo 3

Grafos e Grafos Circulantes

Inicialmente, introduzimos os conceitos da teoria de grafos e apresentamos os grafos em toros k -dimensionais obtidos de quocientes de reticulados, utilizando para isto os resultados do artigo [14]. Descrevemos os grafos circulantes e sua realização como grafos obtidos do quociente de reticulados. O principal resultado deste capítulo estabelece uma conexão entre grafos circulantes, quocientes de reticulados e códigos esféricos. Cada grafo circulante pode ser visto como um código esférico. Um resultado recíproco também é demonstrado: um código esférico gerado por um grupo cíclico de matrizes ortogonais está associado a único grafo circulante a menos de um isomorfismo. Fechamos o capítulo falando a respeito de conexidade dos grafos circulantes.

3.1 Grafos: Definições e Terminologia

Consideramos neste trabalho a seguinte definição de grafo (não-direcionado) [19]: Um *grafo* \mathcal{G} é um par ordenado $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ satisfazendo as seguintes condições:

- \mathcal{V} é um conjunto enumerável e não vazio chamado de conjunto dos *vértices*;
- \mathcal{A} é um conjunto de subconjuntos de \mathcal{V} com dois elementos, chamado de conjunto de *arestas*.

A partir de agora $\mathfrak{v}(\mathcal{G})$ (ou simplesmente \mathfrak{v} , quando não houver confusão entre grafos) representa a quantidade de vértices do grafo \mathcal{G} . Essa cardinalidade também é conhecida como *ordem*. Analogamente, $\mathfrak{a}(\mathcal{G})$ (ou \mathfrak{a}) denota o número de arestas do grafo \mathcal{G} .

Os vértices v_i e v_j são ditos *adjacentes* (ou *vizinhos*) se existir uma aresta $a = \{v_i, v_j\}$ em \mathcal{A} . Esta aresta é dita ser *incidente* a ambos, v_i e v_j .

Em cada vértice podem existir várias arestas incidentes, a quantidade destas arestas é chamada de *grau* de um vértice.

Definição 3.1.1. Um grafo é dito ser *regular* quando todos os seus vértices têm o mesmo grau.

Definição 3.1.2. Uma *cadeia* é uma seqüência qualquer de vértices adjacentes.

- Uma cadeia é dita ser *elementar* se não passa duas vezes pelo mesmo vértice, e é dita ser *simples*, se não passa duas vezes pela mesma aresta.
- O comprimento de uma cadeia é o número de arestas que a compõe.

Um *ciclo* é uma cadeia simples, elementar e fechada (o vértice inicial é o mesmo que o vértice final), com comprimento maior ou igual a 3 vértices.

Definição 3.1.3. Um grafo $\mathcal{G}_s = (\mathcal{V}_s, \mathcal{A}_s)$ é dito *subgrafo* de um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ quando $\mathcal{V}_s \subseteq \mathcal{V}$ e $\mathcal{A}_s \subseteq \mathcal{A}$. E, neste caso, $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ é dito *supergrafo* de $\mathcal{G}_s = (\mathcal{V}_s, \mathcal{A}_s)$.

Definição 3.1.4. Um grafo $\mathcal{G}(\mathcal{V}, \mathcal{A})$ é dito ser *conexo* se houver pelo menos uma cadeia ligando cada par de vértices deste grafo \mathcal{G} .

Um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ é dito ser *desconexo* se não for conexo. Um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ desconexo é formado por pelo menos dois subgrafos conexos, disjuntos em relação aos vértices e maximais em relação à inclusão. Cada um destes subgrafos conexos é chamado de *componente conexa* de \mathcal{G} .

Definição 3.1.5. Um vértice é dito ser um *vértice de corte* se sua remoção (juntamente com as arestas a ele conectadas) provoca um aumento no número de componentes conexas.

Definição 3.1.6. Uma aresta é dita ser uma *ponte* se sua remoção provoca um aumento no número de componentes conexas.

Definição 3.1.7. Sejam dois grafos $\mathcal{G}_1 = (\mathcal{V}_1, \mathcal{A}_1)$ e $\mathcal{G}_2 = (\mathcal{V}_2, \mathcal{A}_2)$. Um *isomorfismo* de \mathcal{G}_1 sobre \mathcal{G}_2 é um mapeamento bijetivo $f : \mathcal{V}_1 \rightarrow \mathcal{V}_2$ tal que $(v_i, v_j) \in \mathcal{A}_1$ se, e somente se, $(f(v_i), f(v_j)) \in \mathcal{A}_2$, para todo $v_i, v_j \in \mathcal{V}_1$.

3.2 Exemplos de Grafos

***n*-cadeia:** consiste de uma seqüência de n vértices $1, \dots, n$ e cada vértice i é ligado ao seu sucessor $i + 1$, como mostra a figura 3.1.



Figura 3.1: *n*-cadeia

n -cíclico: consiste de um polígono com n lados, vide figura 3.2.

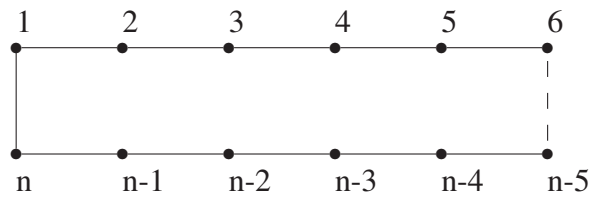


Figura 3.2: n -cíclico

completo: é um grafo com a propriedade de que para todo par de vértices v_i, v_j do grafo existe a aresta $a = \{v_i, v_j\}$. Este grafo é denotado por \mathcal{K}_n , onde n é a ordem do grafo. A figura 3.3 ilustra um grafo completo com 5 vértices.

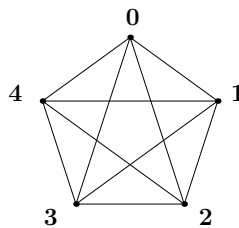


Figura 3.3: \mathcal{K}_5

bipartido: consiste em um grafo cujo conjunto de vértices \mathcal{V} pode ser particionado em dois subconjuntos \mathcal{V}_1 e \mathcal{V}_2 , tais que toda aresta de \mathcal{G} une um vértice de \mathcal{V}_1 a outro de \mathcal{V}_2 . O grafo é dito bipartido completo quando todos os vértices de \mathcal{V}_1 estão unidos com os vértices \mathcal{V}_2 , e, neste caso, o denotaremos por $\mathcal{K}_{m,n}$, onde m e n são respectivamente as cardinalidade de \mathcal{V}_1 e \mathcal{V}_2 . A figura 3.4 ilustra um grafo bipartido famoso, o Utility Graph (UG), ou $\mathcal{K}_{3,3}$.

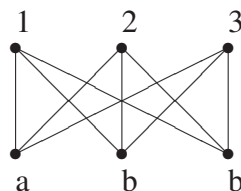


Figura 3.4: Utility graph (UG)

3.3 Grafos sobre o Toro Plano

Esta seção é baseada no artigo [14]. Dada uma base $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ de \mathbb{R}^k , o toro planar $\mathcal{T}_{\mathcal{B}}$ é algebricamente definido como o espaço quociente $\mathcal{T}_{\mathcal{B}} = \mathbb{R}^k / \mathcal{L}_{\mathcal{B}}$, onde $\mathcal{L}_{\mathcal{B}}$ é o reticulado gerado por \mathcal{B} .

Dois vetores \mathbf{x} e \mathbf{y} de \mathbb{R}^k estão na mesma classe se, e somente se, $\mathbf{x} - \mathbf{y} = \sum_{i=1}^k m_i \mathbf{u}_i$, $m_i \in \mathbb{Z}$.

A distância euclidiana d em \mathbb{R}^k induz a distância $d_{\mathcal{B}}$ sobre o toro planar $\mathcal{T}_{\mathcal{B}}$ de forma natural [24]. A distância medida no toro planar entre duas classes $\bar{\mathbf{x}}$ e $\bar{\mathbf{y}}$ de \mathbf{x} e \mathbf{y} , com $\mathbf{x}, \mathbf{y} \in \mathbb{R}^k$, é

$$d_{\mathcal{B}}(\bar{\mathbf{x}}, \bar{\mathbf{y}}) = \min\{d(\mathbf{z}, \mathbf{w}) = \|\mathbf{z} - \mathbf{w}\|; \mathbf{z} \in \bar{\mathbf{x}}, \mathbf{w} \in \bar{\mathbf{y}}\}, \quad (3.1)$$

onde $\|\mathbf{x}\| = \sqrt{\sum_{i=1}^k x_i^2}$ é a norma euclidiana em \mathbb{R}^k .

Geometricamente, o toro planar \mathcal{T} pode ser caracterizado pelo quociente de \mathbb{R}^k pelo grupo de translações gerado por \mathcal{B} , também denotado por $\mathcal{L}_{\mathcal{B}}$. Para $k = 2$ e $\mathcal{B} = \{\mathbf{u}, \mathbf{v}\}$, esse quociente $\mathcal{T}_{\mathcal{B}}$ pode ser visto como o paralelogramo gerado por \mathbf{u} e \mathbf{v} em que os lados opostos são identificados (esse paralelogramo contém representante para todas as classes com redundância no bordo).

3.3.1 Ladrilhamento e Grafos em Toros

Considere o ladrilhamento do plano \mathbb{R}^2 pelo reticulado \mathbb{Z}^2 e a base $\mathcal{B} = \{\mathbf{u}, \mathbf{v}\}$, onde $\mathbf{u} = (a, b)$, $\mathbf{v} = (c, d)$, a, b, c, d inteiros, e o sub-reticulado $\mathcal{L}_{\mathcal{B}}$ gerado por \mathbf{u} e \mathbf{v} . O quociente $\mathbb{Z}^2 / \mathcal{L}_{\mathcal{B}}$ induz um grafo com $n = \left| \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \right|$ vértices e um ladrilhamento quadrado sobre o toro planar $\mathcal{T}_{\mathcal{B}}$ ([14]).

Por exemplo, para $\mathbf{u} = (3, 2)$ e $\mathbf{v} = (-2, 3)$, temos o grafo $\mathcal{G}_{\mathbf{u}, \mathbf{v}}$ no toro planar com $n = \det \begin{bmatrix} 3 & -2 \\ 2 & 3 \end{bmatrix} = 13$ vértices e o ladrilhamento por 13 quadrados associados (Figura 3.5).

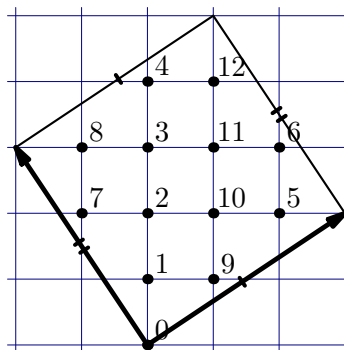


Figura 3.5: Toro planar $\mathcal{T}_{\mathbf{u}, \mathbf{v}}$ ladrilhado por 13 quadrados.

A translação vertical pelo vetor $\mathbf{w} = (0, 1)$ induz um rotulamento cíclico em $\mathcal{G}_{\mathbf{u}, \mathbf{v}}$. Note que os segmentos verticais do grafo são conectados quando identificamos os lados opostos do paralelogramo e os vértices do grafo são colocados numa curva sobre a superfície do toro. Visto no toro padrão do \mathbb{R}^3 , essa curva fechada é conhecida (nó trefoil).

Seja $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ uma base de \mathbb{R}^k com coordenadas inteiras e $\mathcal{T}_{\mathcal{B}}$ o toro planar associado. A existência de um grafo e o ladrilhamento de $\mathcal{T}_{\mathcal{B}}$ por hipercubos é assegurado pela próxima proposição. Mas, antes, vamos definir a aplicação quociente $\bar{\mu}_{\mathcal{B}} : \mathbb{R}^k \rightarrow \mathbb{R}^k$,

$$\bar{\mu}_{\mathcal{B}}(\mathbf{x}) = \mathbf{x} \bmod \mathcal{L}_{\mathcal{B}} = \mathbf{x} - \sum_{i=1}^k [x_i] \mathbf{u}_i. \quad (3.2)$$

Proposição 3.3.1 ([14]). *Seja $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ uma base de \mathbb{R}^k com coordenadas inteiras, $\mathcal{L}_{\mathcal{B}}$ o reticulado gerado por \mathcal{B} e $\mathcal{T}_{\mathcal{B}}$ o toro planar associado. $\mathbb{Z}^k \subset \mathbb{R}^k$ induz, através da aplicação quociente $\bar{\mu}_{\mathcal{B}}$, um grafo regular $\mathcal{G}_{\mathcal{B}} = \frac{\mathbb{Z}^k}{\mathcal{L}_{\mathcal{B}}}$ e um ladrilhamento de $\mathcal{T}_{\mathcal{B}}$ por hipercubos unitários onde*

- a) $\bar{\mu}_{\mathcal{B}}(\mathbb{Z}^k)$ são os vértices de $\mathcal{G}_{\mathcal{B}}$;
- b) $\bar{\mu}_{\mathcal{B}}([i_1, i_1 + 1] \times \mathbb{Z}^{k-1}) \cup \bar{\mu}_{\mathcal{B}}(\mathbb{Z} \times [i_2, i_2 + 1] \times \mathbb{Z}^{k-2}) \cup \dots \cup \bar{\mu}_{\mathcal{B}}(\mathbb{Z}^{k-1} \times [i_k, i_k + 1])$, i_j inteiro, é união de arestas;
- c) $\bar{\mu}_{\mathcal{B}}([i_1, i_1 + 1] \times [i_2, i_2 + 1] \times \dots \times [i_k, i_k + 1])$, i_j inteiro, são hipercubos;
- d) O número de vértices, \mathbf{v} , e o número de hipercubos, \mathcal{F} , de $\mathcal{G}_{\mathcal{B}}$, são ambos iguais a $|\det[\mathbf{u}_1, \dots, \mathbf{u}_k]|$.

O resultado seguinte é obtido como consequência da Proposição 23 de [14].

Proposição 3.3.2 ([14]). *Sob as hipóteses da Proposição 3.3.1, $\Gamma_{\mathcal{B}} = \frac{\mathbb{Z}^k}{\mathcal{L}_{\mathcal{B}}}$ é cíclico se, e somente se, existe um vetor $\mathbf{w} = (w_1, \dots, w_k) \in \mathbb{Z}^k$ e inteiros h_1, \dots, h_{k+1} tais que:*

$$M = \left[\begin{array}{ccc|c} & & & w_1 \\ & A & & \vdots \\ & & & w_k \\ \hline h_1 & \cdots & h_k & h_{k+1} \end{array} \right] \quad (3.3)$$

tem determinante 1, onde A é a matriz cujas colunas são os vetores \mathbf{u}_i . Neste caso, $\langle \bar{\mathbf{w}} \rangle = \Gamma_{\mathcal{B}}$.

Demonstração: Para $\mathbf{u}, \mathbf{w} \in \mathbb{Z}^k$, $\bar{\mathbf{u}} = \bar{\mathbf{w}}$ em $\Gamma_{\mathcal{B}}$ se, e somente se, $\mathbf{u} - \mathbf{w} \in \mathcal{L}_{\mathcal{B}}$. Em outras palavras, existe $\mathbf{x} \in \mathbb{Z}^k$ tal que $A\mathbf{x} = \mathbf{u} - \mathbf{w}$. Portanto, a ordem de $\bar{\mathbf{w}}$ é o menor inteiro r tal que o sistema $A\mathbf{x} = r\mathbf{w}$ tem solução \mathbf{x} com coordenadas inteiras.

Assim, A é invertível e pela fórmula de Cramer o sistema $A\mathbf{x} = \mathbf{w}$ tem uma única solução dada por $\mathbf{x} = |A|^{-1}(|A_1|, \dots, |A_k|)$, onde a matriz A_i é a matriz A com a i -ésima coluna trocada por \mathbf{w} e $|A| = |\det(A)|$. Isso significa que $A\mathbf{x}_0 = |A|\mathbf{w}$ tem solução $\mathbf{x}_0 = (|A_1|, \dots, |A_k|) \in \mathbb{Z}^k$.

Assim, $|A| = |\mathbb{Z}^k/\mathcal{L}_B|$. Se r é a ordem de $\bar{\mathbf{w}} = \mathbf{w} + \mathcal{L}_B$, então r divide $|A|$. Isso implica que $|A| = rl$, e a única solução de $A\mathbf{x} = r\mathbf{w}$ é dada por $\mathbf{x} = (1/l)\mathbf{x}_0$. Então, l divide cada $|A_i|$. Agora, para cada inteiro l_1 tal que l_1 divide $|A|, |A_1|, \dots, |A_k|$, seja r_1 dado por $|A| = r_1 l_1$. Então, $r|r_1$, o que implica que $l_1|l$. Isto mostra que $l = \text{mdc}\{|A|, |A_1|, \dots, |A_k|\}$ e que $r = |A|/\text{mdc}\{|A|, |A_1|, \dots, |A_k|\}$.

Γ_B é cíclico se, e somente se, existe $\bar{\mathbf{w}}$ com ordem $|A|$, o que pelos cálculos acima significa que $\text{mdc}\{|A|, |A_1|, \dots, |A_k|\} = 1$. Isso é equivalente a existir constantes inteiras h_1, \dots, h_{k+1} tais que

$$h_1 |A_1| + \dots + h_k |A_k| + h_{k+1} |A| = 1. \quad (3.4)$$

Em outras palavras, Γ_B é cíclico se, e somente se, existem h_1, \dots, h_{k+1} tais que, pelo desenvolvimento por Laplace aplicado na $(k+1)$ -ésima linha de M , $\det(M)$ é igual a

$$\begin{aligned} &= (-1)^{k+1} h_1 (-1)^{k-1} |A_1| + \dots + (-1)^{k+k} h_k (-1)^{k-k} |A_k| + (-1)^{2k+2} h_{k+1} |A| \\ &= h_1 |A_1| + \dots + h_k |A_k| + h_{k+1} |A| = 1. \end{aligned} \quad \blacksquare$$

3.4 Grafos Circulantes

Esta seção é uma versão com pequenas modificações do artigo [16] (em fase de conclusão).

Definição 3.4.1. Um grafo circulante com n vértices $\{v_0, \dots, v_{n-1}\}$ e saltos a_1, \dots, a_m é um grafo não direcionado em que cada vértice $v_j, 0 \leq j \leq n-1$, é adjacente a todos os vértices v_k , onde $k = i \pm a_i \pmod n$ e $1 \leq i \leq m$. Denotaremos esse grafo por $\mathcal{C}_n(a_1, \dots, a_m)$.

A figura 3.6 mostra uma figura padrão para o grafo circulante $\mathcal{C}_{13}(1, 5)$.

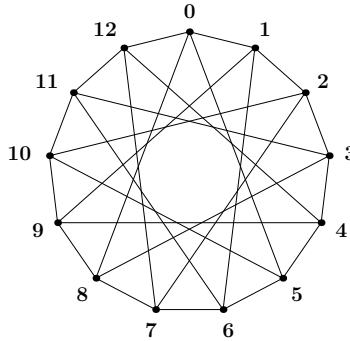


Figura 3.6: Grafo Circulante $\mathcal{C}_{13}(1, 5)$.

O grafo n -cíclico e o grafo completo de n vértices são exemplos de grafos circulantes denotados por $\mathcal{C}_n(1)$ e $\mathcal{K}_n = \mathcal{C}_n(1, \dots, \lfloor n/2 \rfloor)$.

Um importante resultado sobre isomorfismo de grafos circulantes é que, se existe $r \in \mathbb{Z}$, $\text{mdc}(r, n) = 1$, tal que $(a_1, \dots, a_m) = r(\tilde{a}_1, \dots, \tilde{a}_m) \bmod n$, então $\mathcal{C}_n(a_1, \dots, a_m)$ é isomorfo a $\mathcal{C}_n(\tilde{a}_1, \dots, \tilde{a}_m)$ ([36]). Essa condição é chamada de *propriedade de Ádám*.

A recíproca desse resultado foi conjecturada para grafos circulantes por Ádám [1]. A conjectura é falsa para grafos gerais. No entanto, é válida para $m = 2$ [21].

Um grafo circulante $\mathcal{C}_n(a_1, \dots, a_m)$ é conexo se, e somente se, $\text{mdc}(a_1, \dots, a_m, n) = 1$ ([7]). Todos os grafos considerados a partir de agora são conexos, salvo menção em contrário.

O próximo resultado descreve \mathcal{G}_B^w (=grafo \mathcal{G}_B rotulado por w) como um grafo circulante, quando as condições da Proposição 3.3.2 são satisfeitas.

Proposição 3.4.1 ([16]). *Sob as condições da Proposição 3.3.2, o rotulamento dado por w induz um isomorfismo de grafos*

$$\mathcal{G}_B^w \approx \mathcal{C}_n(s_1, \dots, s_k), \quad (3.5)$$

onde $n = |\det A|$,

$$s_i = \min\{M_{i, k+1} \bmod n, n - M_{i, k+1} \bmod n\} \quad (3.6)$$

e $M_{i, k+1}$ é o cofator associado à entrada $\{i, k+1\}$ de M .

Demonstração: A relação de adjacência em \mathcal{G}_B é induzida por \mathbb{Z}^k . Então, os vértices adjacentes a $\bar{0}$ são $\pm \mathbf{e}_i$'s. Necessitamos mostrar que

$$\begin{aligned} s_i \mathbf{w} \equiv \mp \mathbf{e}_i &\iff \exists r_1, \dots, r_k \in \mathbb{Z} \text{ tal que } s_i \mathbf{w} \pm \mathbf{e}_i = r_1 \mathbf{u}_1 + \dots + r_k \mathbf{u}_k \\ &\iff r_1 \mathbf{u}_1 + \dots + r_k \mathbf{u}_k - s_i \mathbf{w} = \pm \mathbf{e}_i \iff \end{aligned}$$

$$\begin{cases} r_1 a_{11} + \dots + r_k a_{1k} - s_i w_1 = 0 \\ \vdots \\ r_1 a_{i1} + \dots + r_k a_{ik} - s_i w_i = \pm 1 \\ \vdots \\ r_1 a_{k1} + \dots + r_k a_{kk} - s_i w_k = 0 \end{cases} \quad (3.7)$$

Temos que $r_1 = \pm(-1)^{i+1} M_{i,1}, \dots, \pm(-1)^{i+k} r_k = M_{i,k}$ e $s_i = \pm(-1)^{i+k} M_{i, k+1}$ é a solução para o sistema (3.7). De fato, a i -ésima equação pode ser vista como o desenvolvimento por Laplace de M , dado em (3.3) pela i -ésima linha. As outras equações podem ser vistas como o determinante

de uma matriz com duas linhas iguais. Portanto, $\overline{s_i w}$ é vizinho (adjacente a) de $\overline{0}$. Então, \mathcal{G}_B^w , o grafo \mathcal{G}_B rotulado por w , é isomorfo ao grafo circulante $\mathcal{C}_n(\overline{s_1}, \dots, \overline{s_k})$,

$$\overline{s_i} = \min\{M_{i, k+1} \bmod n, n - M_{i, k+1} \bmod n\}. \quad \blacksquare$$

Observação 3.4.1. A distância no grafo \mathcal{G}_B^w é induzida pela distância em \mathbb{Z}^k . Para $\overline{x}, \overline{y} \in \mathcal{G}_B = \frac{\mathbb{Z}^k}{\mathcal{L}_B}$, temos:

$$d_{\mathcal{G}_B}(\overline{x}, \overline{y}) = \min \left\{ \sum_{i=1}^k |x_i - y_i|, \mathbf{x} = (x_1, \dots, x_k) \in \overline{x} \text{ e } \mathbf{y} = (y_1, \dots, y_k) \in \overline{y} \right\} \quad (3.8)$$

Para outros w' e h'_1, \dots, h'_{k+1} satisfazendo (3.3), obteremos, pela Proposição 3.3.2 um grafo circulante diferente $\mathcal{C}_n(s'_1, \dots, s'_k)$, mas ambos devem ser isomorfos, como veremos a seguir.

Proposição 3.4.2 ([16]). *Se existirem outros w' e h' satisfazendo a Proposição 3.3.2 para a mesma submatriz A de M (3.3), então*

$$\mathcal{C}_n(a_1, \dots, a_k) \approx \mathcal{C}_n(a'_1, \dots, a'_k). \quad (3.9)$$

Demonstração: Pela Proposição 3.3.2, Γ_B^w e $\Gamma_B^{w'}$ são cíclicos e gerados por \overline{w} e $\overline{w'}$, respectivamente. Então $\langle \overline{w} \rangle = \langle \overline{w'} \rangle$, o que significa que existem inteiros r, t relativamente primos com n tais que $\overline{w} = r \overline{w'}$ e $\overline{w'} = t \overline{w}$. Em outras palavras,

$$\overline{w} = r \overline{w'} = r t \overline{w} \iff r t \equiv 1 \pmod{n}. \quad (3.10)$$

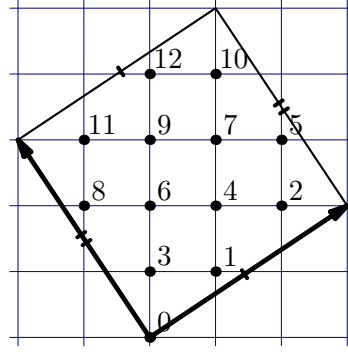
Portanto, $e_i \equiv a_i w \equiv a_i r w'$ e $e_i \equiv a'_i w'$, o que implica que $\overline{a'_i w'} = \overline{a_i r w'}$. Assim $a'_i \equiv a_i r \pmod{n}$ e, então,

$$\mathcal{C}_n(a_1, \dots, a_k) \approx \mathcal{C}_n(a'_1, \dots, a'_k). \quad \blacksquare$$

Exemplo 3.4.1. A figura 3.5 mostra o grafo circulante $\mathcal{C}_{13}(1, 5)$ visto sobre o toro planar gerado por $v_1 = (3, 2)$ e $v_2 = (-2, 3)$, e rotulado por $w = (0, 1)$ ($h_1 = 1, h_2 = -1, h_3 = 0$). Se consideramos o rotulamento por $w' = (1, 1)$ ($h_1 = h_3 = 0$ e $h_2 = -1$), temos, pela Proposição 3.3.2, $\mathcal{C}_{13}(2, 3)$ sobre o toro planar com o mesmo conjunto de vértices (vide a figura 3.7). Conforme assegurado pela Proposição 3.4.2, esses grafos circulantes são isomorfos.

3.4.1 Grafos circulantes realizados como grafos sobre o toro planar

Pela Proposição 3.4.1, vemos que todos os grafos que ladrilham o toro planar por hipercubos dão um grafo circulante. A recíproca é verdadeira, como veremos na próxima proposição. A prova deste resultado é baseada no resultado obtido na Proposição 10 de [33], adaptada ao nosso contexto.

Figura 3.7: Grafo Circulante $\mathcal{C}_{13}(2, 3)$.

Proposição 3.4.3 ([16]). *Qualquer grafo circulante conexo $\mathcal{C}_n(a_1, \dots, a_k)$ de grau $2k$ ou $2k - 1$ (cada vértice tem grau $2k$ ou $2k - 1$) com vértices $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ é isomorfo a um grafo $\mathcal{G}_{\mathcal{B}}$, que ladrilha um toro planar k -dimensional $\mathcal{T}_{\mathcal{B}}$ por hipercubos. Isto é, existe uma base $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ de \mathbb{R}^k com $\mathbf{u}_i \in \mathbb{Z}^k$ e um vetor $\mathbf{w} \in \mathbb{Z}^k$ tal que, para o reticulado $\mathcal{L}_{\mathcal{B}} = \langle \mathbf{u}_1, \dots, \mathbf{u}_k \rangle$,*

$$\Gamma_{\mathcal{B}}^{\mathbf{w}} = \frac{\mathbb{Z}^k}{\mathcal{L}_{\mathcal{B}}} = \langle \overline{\mathbf{w}} \rangle \cong \mathbb{Z}_n \text{ e } \Psi(\mathbf{v}_i) = i \overline{\mathbf{w}} \text{ é um isomorfismo de grafos.} \quad (3.11)$$

Demonstração: Inicialmente, notamos que $\mathcal{C}_n(a_1, \dots, a_k)$ é conexo e $\text{mdc}(a_1, \dots, a_k, n) = 1$. Portanto, existem inteiros w_1, \dots, w_{k+1} tal que

$$w_1 a_1 + \dots + w_k a_k + n w_{k+1} = 1. \quad (3.12)$$

Seja $\tilde{\mathbf{w}} = (w_1, \dots, w_{k+1})$. Para $\mathbf{s} = (a_1, \dots, a_k, n)$, considere a base $\tilde{\mathcal{B}} = \{\tilde{\mathbf{u}}_1, \dots, \tilde{\mathbf{u}}_k\}$, $\tilde{\mathbf{u}}_i = (u_{1i}, \dots, u_{k+1i}) \in \mathbb{Z}^{k+1}$, do subreticulado de \mathbb{Z}^{k+1} definido pelo hiperplano \mathbf{s}^\perp ortogonal a \mathbf{s} em \mathbb{R}^{k+1} e $A = \{u_{ij}\}$. Mostraremos a seguir que a matriz M $(k+1) \times (k+1)$, cujas colunas são $\tilde{\mathbf{u}}_1, \dots, \tilde{\mathbf{u}}_k$ e $\tilde{\mathbf{w}}$, tem determinante igual a um e a submatriz A $k \times k$, do canto superior esquerdo, tem determinante n :

$$M = \left[\begin{array}{ccc|c} u_{11} & \cdots & u_{1k} & w_1 \\ \vdots & \ddots & \vdots & \vdots \\ u_{k1} & \cdots & u_{kk} & w_k \\ \hline u_{k+11} & \cdots & u_{k+1k} & w_{k+1} \end{array} \right], \det(M) = 1. \quad (3.13)$$

A afirmação desta proposição pode então ser derivada da Proposição 3.3.2, tomando $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ e \mathbf{w} , onde \mathbf{u}_i e \mathbf{w} são obtidos de $\tilde{\mathbf{u}}_i$ e $\tilde{\mathbf{w}}$, eliminando a última coordenada.

Segundo [33], considere a aplicação:

$$\begin{aligned} \varphi : \quad \mathbb{Z}^k &\longrightarrow \mathbb{Z}_n \\ (x_1, \dots, x_k) &\longmapsto \overline{x_1 a_1 + \dots + x_k a_k}, \end{aligned} \quad (3.14)$$

que é um homomorfismo de grupos. Então, por (3.12), $\varphi(\mathbf{w}) = \varphi(w_1, w_2, \dots, w_k) = \bar{1}$ e φ é sobrejetora. O núcleo é um reticulado \mathcal{L} em \mathbb{R}^k satisfazendo

$$\text{vol}(\mathcal{L}) = \left| \frac{\mathbb{Z}^k}{\mathcal{L}} \right| = |\mathbb{Z}_n| = n. \quad (3.15)$$

Note que $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$, definida como acima, é uma base para esse núcleo. Assim, $\mathbf{v} \in \mathcal{L} \iff \exists \lambda \in \mathbb{Z}; (\mathbf{v}, \lambda) \in s^\perp \cap \mathbb{Z}^k$. Isso implica que

$$|\det(A)| = \text{vol}(\mathcal{L}) = n. \quad (3.16)$$

(Consideramos $\det(A) = n$ permutando dois vetores nesta base, se necessário).

Voltando a \mathbb{R}^{k+1} , tomamos $\mathbf{m} = (m_1, \dots, m_{k+1})$ como o produto vetorial $\mathbf{u}_1 \wedge \dots \wedge \mathbf{u}_k$, que é o único vetor tal que

$$\mathbf{u} \cdot \mathbf{m} = \det[\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{u}], \quad (3.17)$$

para todo $\mathbf{u} \in \mathbb{R}^{k+1}$. As coordenadas desse produto de vetores podem ser escritas usando os cofatores da última coluna da matriz M dada acima: $m_i = M_{i, k+1}$ [43]:

$$m_i = \mathbf{e}_i \cdot \mathbf{m} = \det[\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{e}_i] = M_{j, k+1} \quad (3.18)$$

e, em particular, $m_{k+1} = \det(A) = n$. Além disso,

$$\mathbf{u}_i \cdot \mathbf{m} = \det[\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{u}_i] = 0; \quad (3.19)$$

assim os \mathbf{u}_i 's formam uma base para o hiperplano ortogonal a \mathbf{s} e concluímos que $\mathbf{m} = \lambda \mathbf{s}$, para algum $\lambda \in \mathbb{R}$. Portanto, de (3.13), garantimos que $m_{k+1} = \det(A) = \lambda \det(A)$, i.e., $\lambda = 1$ e $\mathbf{m} = \mathbf{s}$, desenvolvendo o determinante de $M = [\tilde{\mathbf{u}}_1, \dots, \tilde{\mathbf{u}}_k, \tilde{\mathbf{w}}]$, pela última coluna. Temos, então,

$$\det(M) = \tilde{\mathbf{w}} \cdot \mathbf{m} = \tilde{\mathbf{w}} \cdot \mathbf{s} = 1, \quad (3.20)$$

o que conclui a prova. ■

Exemplo 3.4.2. Para \mathcal{G}_B^w isomorfo a $\mathcal{C}_{13}(3, 5)$, devemos encontrar uma base para o reticulado

Proposição 3.5.1 ([17]). *Seja $\mathcal{C}_n(r a_1, \dots, r a_k)$ com $\text{mdc}(a_1, \dots, a_k) = 1$ e $\text{mdc}(r, n) = 1$. Então, existe uma base de vetores $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_k\} \subset \mathbb{R}^k$ tais que $\mathcal{C}_n(r a_1, \dots, r a_k) \approx \mathcal{G}_{\mathcal{B}} = \frac{\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle}{(n\mathbb{Z})^k}$.*

Demonstração: Considere $\mathbf{w} = (a_1, \dots, a_k)$. É conhecido que, para inteiros satisfazendo $\text{mdc}(a_1, \dots, a_k) = 1$, existe uma matriz unimodular $M \in M_{k \times k}(\mathbb{Z})$, cuja primeira coluna é a_1, \dots, a_m , i.e.,

$$M = \begin{bmatrix} a_1 & u_{12} & \dots & u_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ a_k & u_{k2} & \dots & u_{kk} \end{bmatrix}. \quad (3.22)$$

Afirmamos que $\mathcal{C}_n(a_1, \dots, a_k) \approx \mathcal{G}_{\mathcal{B}}$, onde $\mathbf{v}_i = (v_{1i}, \dots, v_{ki})$ é a i -ésima coluna de $M P$ e P é a matriz

$$P = \begin{bmatrix} a_1 & \dots & a_k \\ n u_{12} & \dots & n u_{k2} \\ \vdots & \ddots & \vdots \\ n u_{1k} & \dots & n u_{kk} \end{bmatrix}. \quad (3.23)$$

Mostraremos primeiramente que $\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle \supseteq (n\mathbb{Z})^k$. Em outras palavras, exibiremos $\mathbf{x} = \{x_1, \dots, x_k\} \in \mathbb{Z}^k$ tal que $M P \mathbf{x}^t = n \mathbf{e}_i^t$. Como a solução existe, é suficiente mostrar que a solução x tem coordenadas inteiras. Resolvendo o sistema, obtemos:

$$\begin{aligned} M P \mathbf{x}^t &= n \mathbf{e}_i^t \\ \underbrace{\text{adj}(M) M}_{=\text{Id}_k} P \mathbf{x}^t &= n \text{adj}(M) \mathbf{e}_i^t \\ \underbrace{\text{adj}(P) P}_{=n^{k-1}\text{Id}_k} \mathbf{x}^t &= n \text{adj}(P) \text{adj}(M) \mathbf{e}_i^t. \end{aligned}$$

Note que n^{k-2} é fator de cada elemento em $\text{adj}(P)$, o que implica que podemos dividir ambos os lados da igualdade por n^{k-1} e

$$\mathbf{x}^t = \frac{\text{adj}(P)}{n^{k-2}} \text{adj}(M) \mathbf{e}_i^t.$$

Portanto, $\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle \supseteq (n\mathbb{Z})^k$. Além disso, $\text{vol}(\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle) = |\det(M P)| = \underbrace{\det(M)}_{=1} \det(P) = n^{k-1} \underbrace{\det(M^t)}_{=1} = n^{k-1}$. Logo $\left| \frac{\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle}{(n\mathbb{Z})^k} \right| = n$.

A seguir, mostraremos que $\bar{\mathbf{w}}$ gera esse quociente. Seja $\mathbf{u}_i = (u_{1i}, \dots, u_{ki})$ a i -ésima coluna de

M , então $\mathbf{v}_i = a_i \mathbf{w} + n \sum_{j=2}^k u_{ij} \mathbf{u}_j$. Como existem inteiros x_1, \dots, x_k tais que $\sum_{t=1}^k x_t a_t = 1$, então $\mathbf{w} = \sum_{t=1}^k x_t a_t \mathbf{w} = \sum_{t=1}^k x_t (\mathbf{v}_t - n \sum_{j=2}^k u_{tj} \mathbf{u}_j)$. Logo, \mathbf{w} pertence a $\langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle$. Como, $\bar{\mathbf{v}}_i = a_i \bar{\mathbf{w}}$ concluímos que $\bar{\mathbf{w}}$ gera o quociente $\Gamma = \frac{\langle v_1, \dots, v_k \rangle}{(n\mathbb{Z})^k}$.

Agora, mostraremos as relações de adjacência para concluir o isomorfismo, isto é, $\pm a_i w$ são os vizinhos de $\mathbf{0}$ com a métrica do grafo em β_k . Como $\mathbf{v}_i = a_i \mathbf{w} + n \sum_{j=1}^k u_{ij} \mathbf{u}_j \equiv a_i \mathbf{w} \pmod{n\mathbb{Z}^k}$, $\pm \mathbf{v}_i$ conecta dois vizinhos, portanto a relação de adjacência é $i \bar{\mathbf{w}} \sim j \bar{\mathbf{w}}$ se, e somente se, $i \bar{\mathbf{w}} - j \bar{\mathbf{w}} = \bar{\mathbf{v}}_t$ ou, equivalentemente, $i - j = a_t \pmod{n}$ para algum t . Isto conclui a prova. ■

Conseguimos, através da proposição acima, uma função que associa cada grafo circulante a um quociente de reticulados. A figura 3.9 ilustra este mergulho para o grafo $C_6(2, 3)$. Como comentamos, este quociente corresponderá a um código esférico em \mathbb{R}^{2k} . Uma questão natural é saber se há uma espécie de recíproca, i.e., dado um quociente $\Gamma = \frac{\Lambda}{(n\mathbb{Z})^k}$, existe um grafo circulante que é levado pela função da Proposição 3.5.1 em Γ ? A próxima proposição mostrará que a recíproca é verdadeira.

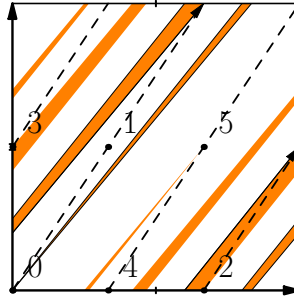


Figura 3.9: O grafo circulante $C_6(2, 3)$ mergulhado no toro planar: vértices, rotulamento e região fundamental da base $\{(10, 12), (12, 15)\}$ que definem a relação de adjacência.

Proposição 3.5.2 ([17]). *Seja $\mathcal{L} = \langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle$ tal que $(n\mathbb{Z})^k \subset \Lambda \subset \mathbb{Z}^k$ e o quociente $\Gamma = \frac{\Lambda}{(n\mathbb{Z})^k}$ como grupo é cíclico de ordem n gerado por $\mathbf{b} = (b_1, \dots, b_k)$. Então, existe uma base $\alpha = \{\mathbf{w}_1, \dots, \mathbf{w}_k\}$ de \mathcal{L} e um vetor \mathbf{a} tal que $C_n(b_1, \dots, b_k)$ é isomorfo a $\mathcal{G}_B = \frac{\Lambda_c \mathbf{b}}{(n\mathbb{Z})^k}$, onde:*

(i) $\Gamma_n^{\mathbf{a}} = \{i \mathbf{a} \pmod{(n\mathbb{Z})^k}; i = 0, \dots, n-1, \mathbf{a} = (\gcd(b_1, \dots, b_k))^{-1} \mathbf{b}\}$ é o conjunto de vértices;

(ii) as arestas são determinadas pela base α : $i \bar{a}$ está conectado a $j \bar{a}$ se, e somente se, $(i - j) \mathbf{a} = \pm \mathbf{w}_i$.

Demonstração: Seja $d = \gcd(b_1, \dots, b_k)$, como \mathbf{b} gera o grupo cíclico, Γ . Então. $\gcd(d, n) = 1$. Temos então que $\mathbf{a} = d^{-1} \mathbf{b}$ também gera Γ . Como $\mathbf{b} = d \mathbf{a}$, $C_n(\mathbf{b})$ é isomorfo a $C_n(\mathbf{a})$, podemos assumir a construção da Proposição 3.5.1, que se traduz nas condições (i) e (ii). ■

A proposição acima estabelece uma função que leva um código esférico em um único grafo circulante, a menos de isomorfismo. De fato, se tivéssemos partido de outros geradores para o quociente de reticulados, esta escolha produziria, a menos de isomorfismo de grafos, o mesmo grafo circulante. Isto se deve ao fato de que a nova matriz geradora G' , do reticulado, diferiria da outra matriz geradora G por uma matriz unimodular U ($G' = GU$) e U realiza o isomorfismo.

Para estabelecer uma bijeção entre grafos circulantes e códigos esféricos, a menos de isometrias e isomorfismos, seria necessário mostrar que grafos isomorfos são levados em reticulados equivalentes. Entretanto, isso não ocorre como mostra o exemplo a seguir.

Exemplo 3.5.1. Sejam $\mathcal{G}_1 = \mathcal{C}_{16}(1, 2, 7)$ e $\mathcal{G}_2 = \mathcal{C}_{16}(1, 6, 7)$. Considere o isomorfismo de grafo $f : \mathcal{G}_1 \longrightarrow \mathcal{G}_2$:

$$f(i) = \begin{cases} -5i - 4 \pmod{16} & \text{se } i \text{ par.} \\ -5i \pmod{16} & \text{se } i \text{ ímpar.} \end{cases} \quad (3.24)$$

Os reticulados associados aos grafos acima têm, respectivamente, como matrizes geradoras:

$$G_1 = \begin{bmatrix} 1 & 2 & 7 \\ 2 & 20 & 14 \\ 7 & 14 & 65 \end{bmatrix} \text{ e } G_2 = \begin{bmatrix} 1 & 6 & 7 \\ 6 & 52 & 42 \\ 7 & 42 & 65 \end{bmatrix}. \quad (3.25)$$

Aplicando a redução de Minkowski, temos:

$$\hat{G}_1 = \begin{bmatrix} -2 & 1 & -7 \\ -4 & 2 & 2 \\ 2 & 7 & -1 \end{bmatrix} \text{ e } \hat{G}_2 = \begin{bmatrix} -2 & 5 & 6 \\ 4 & -2 & 4 \\ 2 & 3 & -6 \end{bmatrix}, \quad (3.26)$$

cujas matrizes de Gram são dadas pelas respectivas matrizes:

$$\hat{A}_1 = \begin{bmatrix} 24 & 4 & 4 \\ 4 & 54 & -10 \\ 4 & -10 & 54 \end{bmatrix} \text{ e } \hat{A}_2 = \begin{bmatrix} 24 & -12 & -8 \\ -12 & 38 & 4 \\ -8 & 4 & 88 \end{bmatrix}. \quad (3.27)$$

Esses reticulados não podem ser congruentes pelo fato do primeiro reticulado não conter nenhum elemento com norma ao quadrado igual a 38.

Os grafos do exemplo acima não são Ádám isomorfos. Este tipo de isomorfismo garante que os reticulados são congruentes [17].

3.6 Conexidade dos Grafos Circulantes

Considere o grafo circulante $\mathcal{G} = \mathcal{C}_n(a_1, \dots, a_k)$ com $\text{mdc}(a_1, \dots, a_k, n) = d$. Vamos mostrar que \mathcal{G} é um grafo com d componentes conexas em que cada componente contém apenas um vértice de rótulo r , com $0 \leq r < d$. Seja v_j um vértice de \mathcal{G} . Como o grafo \mathcal{G} é rotulado pelo grupo \mathbb{Z}_n , temos que $v_j \in \mathbb{Z}_n$.

Dados dois vértices v_i e v_j do grafo circulante \mathcal{G} , existe uma cadeia conectando-os se, e somente se, existe uma seqüência de vértices $v_i = v_{i_0}, \dots, v_{i_l} = v_j$ com v_r vizinho de v_{r+1} , para todo $r = i_0, \dots, i_{l-1}$. Mas v_r é vizinho de v_{r+1} se, e somente se, $v_{r+1} = v_r + a_s$, para algum $s \in \{\pm a_1, \dots, \pm a_k\}$. Logo, v_i e v_j estão na mesma componente conexa se, e somente se, $v_j = v_i + \sum_s p_s a_s$, onde $p_s \in \mathbb{Z}$. Então, $v_j - v_i = \sum_k p_s a_s \pmod{n}$, o que equivale a $v_j - v_i = \sum_k p_s a_s + l n$. Esta equação é linear dentro do anel dos inteiros e terá solução se, e somente se, d dividir $v_i - v_j$. Portanto, concluímos que existem d componentes conexas, onde $\mathcal{C}(r)$ é a componente que contém o vértice r , $0 \leq r < d$.

A componente $\mathcal{C}(r)$, que é um subgrafo de \mathcal{G} , pode ser vista como o grafo circulante $\mathcal{C}_{n/d}(a_1/d, \dots, a_k/d)$ através do isomorfismo de grafos dado por:

$$\begin{aligned} \phi_r : \mathcal{C}(r) &\longrightarrow \mathcal{C}_{n/d}(a_1/d, \dots, a_k/d) \\ x &\longmapsto (x - r)/d \end{aligned} \quad (3.28)$$

Se $x, y \in \mathcal{C}(r)$ são vizinhos, então $x - y = \pm a_s$. Logo, dividindo ambos os lados por d temos que $\frac{x - y}{d} = \pm \frac{a_s}{d}$, isto é, $\frac{(x - r) - (y - r)}{d} = \pm \frac{a_s}{d}$. Portanto, $\frac{x - r}{d}$ é vizinho de $\frac{y - r}{d}$.

Um corolário imediato é que $\mathcal{C}_n(a_1, \dots, a_k)$ é conexo se, e só se, $\text{gcd}(n, a_1, \dots, a_k) = 1$.

Capítulo 4

Gênero de Grafos Circulantes

Dedicamos este capítulo ao problema do gênero de um grafo circulante, o qual é uma importante medida de sua complexidade. Iniciamos introduzindo a definição de gênero e exibindo alguns resultados conhecidos na literatura a respeito do gênero de grafos. Apresentamos o resultado do artigo [33], que classifica todos os grafos circulantes planares. Salvo os casos em que o grafo circulante é um grafo planar, um grafo completo ou um grafo bipartido completo, o gênero de um grafo circulante não era conhecido. Conseguimos estabelecer a classificação dos grafos circulantes toroidais (gênero 1). Impondo algumas condições no grafo circulante, o seu gênero g deve satisfazer $g \geq \frac{nk-2n+4}{4}$. Provamos um teorema (4.3.2) que estabelece uma classe relativamente grande de grafos circulantes que satisfazem à igualdade para k arbitrário.

4.1 Gênero de um Grafo

Definição 4.1.1 ([46]). O gênero de um grafo \mathcal{G} é o menor g , gênero de uma superfície, na qual o grafo \mathcal{G} possa ser desenhado em uma superfície \mathcal{M}_g (de gênero g), de modo que nenhum par de arestas se cruze.

No caso particular do gênero 0, o grafo é chamado de planar pois, através de uma projeção estereográfica, poderá ser também mergulhado no plano.

Quando mergulhamos um grafo em superfície de gênero g (mínimo), o grafo divide a superfície em regiões, chamadas de *faces*. A quantidade de faces determinadas por esse grafo é denotada por $f(\mathcal{G})$ (ou simplesmente f) ([46]).

O primeiro teorema que destacamos é o referente à segunda fórmula de Euler, dado a seguir.

Teorema 4.1.1 (Segunda fórmula de Euler [46]). *Seja \mathcal{G} um grafo conexo. Então,*

$$v + f - a = 2 - 2g. \quad (4.1)$$

Lema 4.1.1 ([46]). *Se \mathcal{G} é um grafo de gênero g com $v \geq l$ e toda face tem mais que l lados, então $lf \leq 2a$.*

Demonstração: Vamos dar uma idéia desta prova. Como face de \mathcal{G} é limitada por l ou mais arestas, temos:

$$\begin{aligned} l &\leq \text{o número de lados da face 1} \\ l &\leq \text{o número de lados da face 2} \\ &\vdots \\ l &\leq \text{o número de lados da face } f \end{aligned}$$

Somando as desigualdades acima, temos que lf (soma do primeiro lado) é menor ou igual D (soma do segundo lado), i.e., $lf \leq D$. Além disso, como cada aresta de uma face é contada duas vezes, temos que $D = 2a$. Portanto vale que $lf \leq 2a$. ■

Lema 4.1.2. *Se \mathcal{G} é um grafo de gênero g com $v \geq l$, se toda face tem mais que l lados, então $g \geq \frac{l-2}{2l} a - \frac{1}{2}(v-2)$.*

Demonstração: Da relação de Euler, temos que $v + f - a = 2 - 2g$. Isolando f e multiplicando por l , temos $lf = l(a - v + 2 - 2g)$. Usando o lema anterior, temos que $l(a - v + 2 - 2g) \leq 2a$, o que implica que $g \geq \frac{l-2}{2l} a - \frac{1}{2}(v-2)$. ■

Na verdade, vale a igualdade quando temos apenas faces com l lados.

4.1.1 Exemplo de gênero de grafos

Relacionamos exemplos que têm o seu gênero conhecido [46].

\mathcal{K}_n : Como consequência do Lema 4.1.2, podemos concluir que o gênero g do grafo \mathcal{K}_n satisfaz:

$$g \geq \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil. \quad (4.2)$$

Heawood conjecturou, em 1890, que valia a igualdade e, na década de 70, foi demonstrada a outra desigualdade passo a passo por vários pesquisadores.

bipartido completo $\mathcal{K}_{m,n}$: O gênero desta classe de grafos é

$$g = \left\lceil \frac{(m-2)(n-2)}{4} \right\rceil.$$

4.1.2 Limitantes para o Gênero

Na seção anterior, já colocamos um limitante inferior para o gênero de um grafo. Nesta seção, estabeleceremos outros limitantes para o gênero de um grafo.

Definição 4.1.2. Dizemos que um grafo \mathcal{G} é uma expansão, de \mathcal{H} se \mathcal{G} é o grafo \mathcal{H} com a adição de vértices sobre alguma aresta (subdivisão de arestas).

Um exemplo simples de expansão seria olhar um polígono de $n + 1$ lados como a expansão do polígono de n lados. Idem para uma n cadeia.

Vamos enunciar alguns teoremas que estabelecem alguns limitantes para o gênero de um grafo.

Teorema 4.1.2 ([46]). *Se um grafo \mathcal{G} tem gênero g , então \mathcal{G} pode ser desenhado sem cruzamentos em toda superfície de gênero n com $n \geq g$.*

Lema 4.1.3 ([46]). *Se \mathcal{G} é supergrafo de \mathcal{H} , então $g_{\mathcal{G}} \geq g_{\mathcal{H}}$.*

Corolário 4.1.1 ([46]). *Se \mathcal{G} tem $v \geq 3$ e gênero g , então*

$$g \leq \left\lceil \frac{(v-3)(v-4)}{12} \right\rceil. \quad (4.3)$$

Demonstração: Como \mathcal{G} é subgrafo de \mathcal{K}_v , pelo lema acima, segue o resultado. ■

Corolário 4.1.2 ([46]). *Se \mathcal{G} é um grafo conexo com $v \geq 3$ e gênero g , então*

$$\lceil \alpha/6 - (v-2)/2 \rceil \leq g \leq \left\lceil \frac{(v-3)(v-4)}{12} \right\rceil. \quad (4.4)$$

4.2 Grafos Circulantes

Do fato de um grafo circulante $\mathcal{C}_n(a_1, \dots, a_k)$ ter a estrutura algébrica do grupo \mathbb{Z}_n , é razoável esperar que consigamos determinar para alguns casos o seu gênero. Entretanto, sabe-se muito pouco sobre os gênero desses grafos. Basicamente, o que foi publicado sobre o assunto é: i) a classificação de todos os grafos circulantes planares ([33]-2003); ii) gênero 1 de alguns grafos circulantes e; iii) gênero dos grafos circulantes que são n -completos ($\mathcal{C}_n(1, \dots, \lfloor \frac{n}{2} \rfloor)$) ou $2n$ -bipartido completos ($\mathcal{C}_{2n}(1, 3, \dots, 2 \lfloor \frac{n-1}{2} \rfloor + 1)$).

Nas subseções que seguem, comentamos a classificação dos grafos planares e classificamos todos os grafos circulantes de gênero 1 (toroidais).

4.2.1 Grafos Circulantes Planares

Heubeger, em [33], mostra quais são os grafos circulantes de gênero zero (planares).

Teorema 4.2.1 ([33]). *Um grafo circulante conexo $\mathcal{C}_n(a_1, \dots, a_m)$ tem gênero zero se, e somente se, as seguintes condições são satisfeitas:*

1. $m = 2, a_2 = \pm 2 a_1 \text{ mod } n, e 2|n,$
2. $m = 2, a_2 = n/2, 2|a_1,$
3. $m = 1.$

A Figura 4.1 abaixo ilustra o mergulho do grafo $\mathcal{C}_n(1, 2)$, que pertence à classe dos grafos dados por 1 da proposição acima num cilindro.

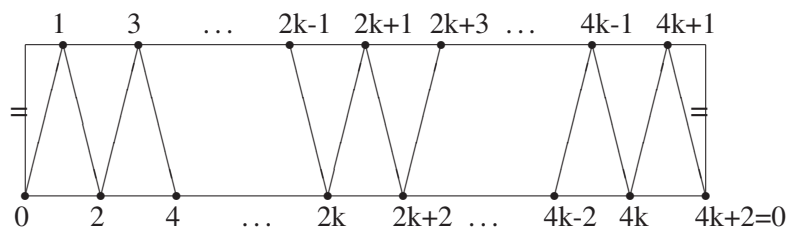


Figura 4.1: Anti-prisma.

A Figura 4.2 abaixo ilustra o mergulho do grafo $\mathcal{C}_{4k+2}(2, 2k+1)$, que pertence à classe dos grafos dados por 2 da proposição acima num cilindro.

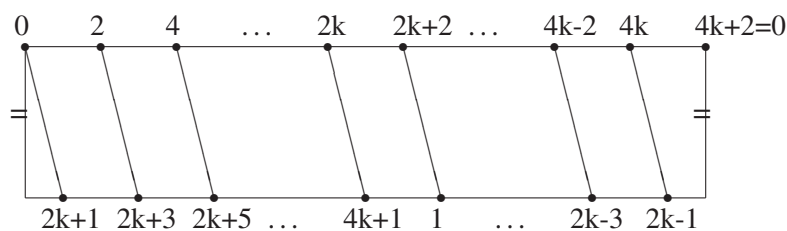


Figura 4.2: Prisma.

4.2.2 Grafos Circulantes Toroidais

A seguir, exibimos a classificação completa dos grafos toroidais que são dados pelos próximos teoremas.

Teorema 4.2.2 ([16]). *Todo grafo circulante $\mathcal{C}_n(a_1, a_2)$, $a_1 < a_2$, tem gênero 1, exceto os casos: i) $a_2 = \pm 2 a_1 \pmod n$ e $2|n$, ii) $a_2 = n/2$, $2|a_2$, que são planares.*

Demonstração: Pela Proposição 3.4.3, todo grafo circulante $\mathcal{C}_n(a_1, a_2)$ pode ser mergulhado em um toro planar bidimensional que tem gênero um. Assim, o gênero é menor que um. Por outro lado [33], o Teorema 4.2.1 mostra que os únicos grafos circulantes planares são os grafos $\mathcal{C}_n(a_1)$ ou $\mathcal{C}_n(a_1, a_2)$, onde i) $m = 2$, $a_2 = \pm 2 a_1 \pmod n$, e $2|n$ ou ii) $a_2 = n/2$ e $2|a_2$. Isto completa a prova. ■

Para $k = 3$ podemos assegurar que o gênero de $\mathcal{C}_n(a_1, a_2, a_3)$ satisfaz:

$$1 \leq g \leq \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil.$$

Uma questão interessante que surge é saber quais destes grafos circulantes têm gênero um e saber o quão alto o gênero pode ser. O próximo teorema completa a classificação dos grafos circulantes de gênero um.

Teorema 4.2.3. *O gênero g de um grafo circulante $\mathcal{C}_n(a_1, a_2, a_3)$ de grau 5 ou 6, $0 < a_1 < a_2 < a_3$, satisfaz:*

1. $g \geq 1$, $\forall a_1, a_2, a_3$;
2. $g = 1$ se, e somente se,
 - (a) $a_3 = a_1 + a_2$; ou
 - (b) $a_2 = 2 a_1$, $n = 2 a_3$ para a_1 e a_3 ímpares; ou
 - (c) $\mathcal{C}_n(a_1, a_2, a_3) \approx \mathcal{C}_8(1, 2, 4)$.

Demonstração: O item (1) foi provado em [33], como mencionado no último teorema.

Mostremos, inicialmente, que todas as condições implicam em um grafo de gênero 1.

(a) Podemos afirmar que $\mathcal{C}_n(a_1, a_2, a_1 + a_2)$ tem gênero um, pois ele é isomorfo a um supergrafo de $\mathcal{C}_n(a_1, a_2)$, onde os vértices são preservados e novos lados adicionados correspondem às diagonais principais dos quadriláteros que ladrilham o toro planar definido pelo mergulho de $\mathcal{C}_n(a_1, a_2)$ (Proposição 3.4.3). Portanto, $\mathcal{C}_n(a_1, a_2, a_1 + a_2)$ ladrilha o mesmo toro planar por triângulos, se $n \neq 2 a_3$ ou triângulos e quadrados, se $n = 2 a_3$.

(b) Como $1 = \text{mdc}(a_1, a_2, \frac{n}{2}, n) = \text{mdc}(a_1, 2 a_1, \frac{n}{2})$ e a_1 é ímpar, $\text{mdc}(a_1, n) = 1$. O grafo circulante (b) é isomorfo a $\mathcal{C}_n(1, 2, a_3)$ ($\approx \mathcal{C}_n(a_1(1, 2, n/2))$ com a_1 invertível e ímpar), que é um supergrafo do grafo antiprisma $\mathcal{C}_n(1, 2)$. Os novos lados podem ser adicionados por um tubo

conectando os $n/2$ polígonos, que são as bases inferior e superior do antiprisma. A figura 4.3 ilustra o grafo $\mathcal{C}_n(1, 2, a_3)$ no toro planar.

(c) Os grafos da forma $\mathcal{C}_8(a_1, a_2, 4)$, que são isomorfos ao grafo $\mathcal{C}_8(1, 2, 4)$, são toroidais, pois são um supergrafo do grafo planar $\mathcal{C}_8(1, 2)$ e podem ser vistos como antiprisma colocado no cilindro. Na figura 4.4, os vértices do quadrado superior deste antiprisma são rotulados pelos números pares, enquanto os vértices do quadrado inferior são rotulados pelos números ímpares. Como podemos ver, os novos lados correspondentes a $a_3 = 4$ podem ser adicionados no toro, como mostra a figura.

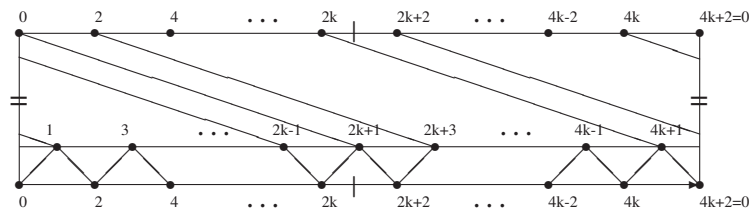


Figura 4.3: Mergulho do grafo circulante $\mathcal{C}_{4k+2}(1, 2, 2k + 1)$ em um toro planar.

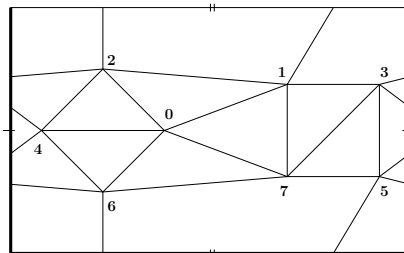


Figura 4.4: Mergulho do grafo circulante $\mathcal{C}_8(1, 2, 4)$ em um toro planar.

Reciprocamente: para ver que nenhum outro grafo circulante $\mathcal{C}_n(a_1, a_2, a_3)$ pode ser mergulhado num toro, consideraremos dois casos:

- I. $\mathcal{C}_n(a_1, a_2, a_3)$ tem grau 6 ($a_3 \neq n/2$). Neste caso, o subgrafo $\mathcal{C}_n(a_1, a_2)$ ou o subgrafo $\mathcal{C}_n(a_1, a_3)$ deve ladrilhar um toro por quadrados (Proposição 3.4.3). A única possibilidade para $\mathcal{C}_n(a_1, a_2, a_3)$ ser um supergrafo obtido de $\mathcal{C}_n(a_1, a_2)$ é adicionando lados correspondentes às diagonais principais dos quadrados ($a_3 = a_1 + a_2$) ou, partindo de $\mathcal{C}_n(a_1, a_3)$ adicionando lados correspondentes às diagonais secundárias dos quadrados ($a_2 = a_3 - a_1$). Em ambos os casos, temos (a).

II. $\mathcal{C}_n(a_1, a_2, a_3)$ tem grau 5 ($a_3 = n/2$). Se $\mathcal{C}_n(a_1, a_2)$ ladrilha um toro por quadrados (o gênero é um), a prova é como em (a). Se $\mathcal{C}_n(a_1, a_2)$ é planar, pelo Teorema 4.2.2, devemos ter $a_2 = 2a_1$ e II.1) a_1 é par ou II.2) $\text{mdc}(a_1, n) = 1$, o que implica $\mathcal{C}_n(a_1, 2a_1, n/2) \approx \mathcal{C}_n(1, 2, n/2)$. No primeiro caso II.1), $\text{mdc}(a_1, n) = 2$ e então $\text{mdc}(a_1/2, n) = 1$, que implica $\mathcal{C}_n(a_1, 2a_1, n/2) \approx \mathcal{C}_n(2, 4, n/2)$, onde $n/2 = 2u + 1$. Então, $\mathcal{C}_n(2, 4)$ é um grafo desconexo, onde cada componente conexa é isomorfa ao grafo $\mathcal{C}_{n/2}(1, 2)$ que tem gênero um (Teorema 4.2.2). Portanto, concluímos que o gênero $\mathcal{C}_n(2, 4)$ é no mínimo dois e o mesmo vale para o supergrafo $\mathcal{C}_n(2, 4, n/2)$. No caso II.2), consideramos $n = 4u$, pois para $n = 4u + 2$, temos (b), $\mathcal{C}_{4u}(1, 2, 2u)$ é um supergrafo de $\mathcal{C}_{4u}(2, 2u)$ que tem duas componentes conexas, ambas isomorfas a $\mathcal{C}_{2u}(1, u)$, e cada componente é não planar, exceto para $u = 2$ ([33]), onde temos (c). Por outro lado, o caso $u > 2$ não pode, ocorrer pois $\mathcal{C}_{4u}(1, 2, 2u)$ deve ter gênero no mínimo dois, uma vez que é um supergrafo de dois subgrafos desconexos de gênero um. Isto completa a prova. ■

Este teorema, em conjunto com o teorema anterior, dá a classificação completa dos grafos circulantes de gênero um, dado que grafos circulantes com $k > 3$, pelo Corolário 4.1.2, devem satisfazer:

$$\begin{aligned}
g &\geq \left\lceil \frac{a}{6} - \frac{v-2}{2} \right\rceil \\
&\geq \left\lceil \frac{(2k-1)n}{12} - \frac{n-2}{2} \right\rceil \\
&\geq \left\lceil \frac{7n}{12} - \frac{n-2}{2} \right\rceil \\
&\geq \left\lceil \frac{n}{12} + 1 \right\rceil \\
&\geq 2.
\end{aligned} \tag{4.5}$$

4.3 Gênero de Grafos Circulantes Quadriláteros

Em geral, nos grafos circulantes, $\mathcal{C}_n(a_1, \dots, a_k)$, a maioria das faces é composta por 4 lados, com vértices: $P, P + a_i, P + a_i + a_j, P + a_j$, salvo exceções onde: $a_i = \pm 2a_j$, $a_i = \pm(a_j \pm a_m)$. Ambas as situações podem ser resumidas na seguinte fórmula: existem combinações de forma $a_i + a_j + a_m = 0$, onde a_i, a_j e $a_m \in \{\pm a_1, \dots, \pm a_k\}$. Esses grafos circulantes devem ser analisados com mais calma, uma vez que as seqüências $0, a_i, a_i + a_j, a_i + a_j + a_m = 0$ podem representar triângulos, quando mergulhamos o grafo numa superfície, como mostram os Teoremas 4.2.2 e 4.2.3 da seção anterior.

Assim, desconsiderando estes casos supra mencionados, o gênero é superior a $\frac{nk-2n+4}{4}$, pois $g \geq \frac{l-2}{2l} a - \frac{v-2}{2} = \frac{2}{8} nk - \frac{n-2}{2} = \frac{nk-2n+4}{4}$. Obtemos, assim de forma direta, o seguinte lema.

Lema 4.3.1. *O gênero do grafo circulante $\mathcal{C}_n(a_1, \dots, a_k)$ tal que $a_i \neq \pm(a_j \pm a_l)$, $\forall i, j, l \leq k$ e $n \neq 2a_i$, $\forall i$ satisfaz*

$$g \geq \frac{nk - 2n + 4}{4}.$$

Nos dois teoremas a seguir, construímos famílias de grafos circulantes que efetivamente atingem o limitante inferior dado pelo lema. O que terá como consequência, ao contrário do que ocorre para $k = 2$, que o gênero pode ser arbitrariamente grande conforme o valor de n , mesmo com k fixado.

Mostraremos primeiro para o caso $k = 3$.

Teorema 4.3.1. *Seja $\mathcal{G} = \mathcal{C}_n(a_1, a_2, a_3) = \mathcal{C}_{2^l u}(2^{l-i_1} a'_1, 2^{l-i_2} a'_2, a_3)$, com $0 < i_1 < i_2 < l$ e $0 \neq a_i + a_j + a_k, \forall a_i, a_j, a_k \in \{0, \pm a_1, \pm a_2, \pm a_3\}$. Então, o gênero de G é $\frac{n+4}{4}$.*

Demonstração: Suponhamos que $0 \neq a_i + a_j + a_k, \forall a_i, a_j, a_k \in \{0, \pm a_1, \pm a_2, \pm a_3\}$. Pelo que vimos anteriormente, o grafo \mathcal{G} não possui triângulos, assim seu gênero deve ser maior ou igual a $\frac{n+4}{4}$. Por outro lado, se exibirmos um mergulho em uma superfície de gênero $\frac{n+4}{4}$, o gênero de \mathcal{G} deve ser menor ou igual a $\frac{n+4}{4}$ e, portanto, é exatamente $\frac{n+4}{4}$. Vamos construir tal mergulho, lembrando que devemos ter todas as faces com 4 lados. Seja $d = \text{mdc}(a_1, a_2) = 2^{l-i_2} \text{mdc}(a'_1, a'_2)$. Pela Seção 3.6, $\mathcal{G} = \mathcal{C}_n(a_1, a_2)$ é um grafo circulante com d componentes conexas, cada qual isomorfa a $\mathcal{H} = \mathcal{C}_{\frac{n}{d}}(a_1 d^{-1}, a_2 d^{-1})$. Já vimos que cada uma das componentes conexas é um ladrilhamento do toro com ladrilhos quadriláteros (Proposição 3.4.3). Denotamos por \mathcal{T}_r , $0 \leq r < d$, o toro que contém o vértice r . Vamos adicionar tubos, para podermos acrescentar as arestas correspondentes a $\pm a_3$. Primeiro, observamos que, da forma que mergulhamos cada componente conexa não apropriada vide figura 4.5.

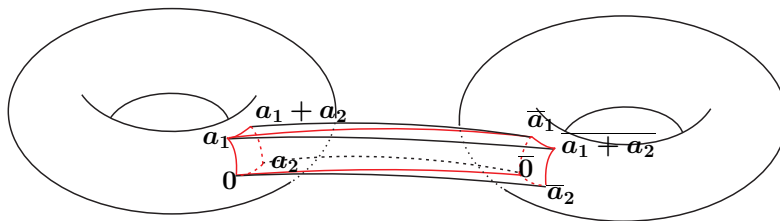


Figura 4.5: Mergulho não ideal de grafo circulante de grau 6 (\bar{x} denota o vértice $x + a_3$).

Se o mergulho for como acima, obrigatoriamente teremos faces com 6 lados e não atingiremos o limitante do teorema. Entretanto, se pudermos inverter a orientação do toro $\mathcal{T}_{r \pm a_3}$, as faces adicionadas possuem 4 lados como mostra a figura 4.6.

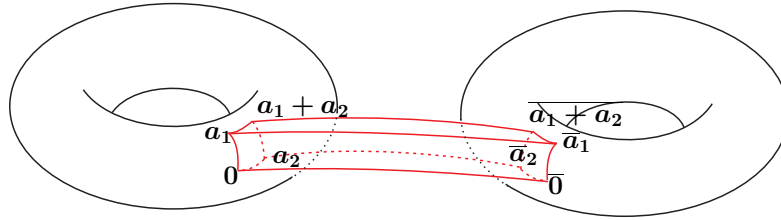


Figura 4.6: Mergulho ideal de grafo circulante de grau 6 (\bar{x} denota o vértice $x + a_3$).

Assim, invertemos a orientação de todas as componentes que contêm os múltiplos ímpares de a_3 que correspondem aos toros \mathcal{T}_r com r ímpar, isto é possível pelo fato de d ser par.

Acrescentamos os tubos que podem ser vistos como prismas de bases quadradas. Por convenção, escolhemos como base inferior do prisma uma face do toro \mathcal{T}_r com r par, ou seja, os vértices da base inferior têm rótulos pares da forma $P, P + a_1, P + a_1 + a_2, P + a_2$ e, portanto, os vértices da base superior têm rótulos ímpares da forma $I, I + a_1, I + a_1 + a_2, I + a_2$, com $I = P \pm a_3$. Devemos ser cuidadosos na escolha das faces que serão bases desses prismas, pelo fato de estarmos olhando os toros como quocientes de reticulados.

Afirmamos que todos os vértices pares do grafo estão nos quadrados $\{P, P + a_1, P + a_1 + a_2, P + a_2\}$, onde P é da forma:

$$P = r + 2Q_1 a_1 + 2Q_2 a_2, \quad (4.6)$$

onde r é par, $0 \leq Q_1 < o(2a_1)$ (ordem de $2a_1$) e $0 \leq 2Q_2 < L$, $L = \min\{x \in \mathbb{N}; x a_2 \in \langle a_1 \rangle\}$.

Assim, as bases inferiores para os prismas associados à soma de a_3 são $P, P + a_1, P + a_1 + a_2, P + a_2$ e, para os associados à soma de $-a_3$, são $P, P - a_1, P - a_1 - a_2, P - a_2$.

Devemos mostrar que qualquer vértice Q do grafo \mathcal{G} está conectado com o vértice $Q \pm a_3$. Vamos mostrar que Q está conectado a $Q + a_3$. Se Q é vértice de \mathcal{G} , então existe um toro \mathcal{T}_r que o contém. Se r for par, tomamos Q'_1 e Q'_2 os menores inteiros positivos tais que $Q = r + Q'_1 a_1 + Q'_2 a_2$. Seja $Q_i = \lceil Q'_i / 2 \rceil$, então Q é um elemento de $\{P, P + a_1, P + a_1 + a_2, P + a_2\}$, onde P é da forma (4.6). Caso r seja ímpar, fazemos o mesmo procedimento para $Q - a_3$, ou seja, concluiremos que Q é um elemento de $\{I, I + a_1, I + a_1 + a_2, I + a_2\}$.

É claro que isto só faz sentido se tomarmos $Q_1 < o(2a_1)$ e, além disso, é fácil ver que existe um índice L tal que $L a_2 \in \langle a_1 \rangle$. Assim, só é necessário que $2Q_2 < L$.

Portanto, todo vértice Q do toro \mathcal{T}_r está conectado ao vizinho da forma $Q + a_3$. De modo análogo, vale que Q está conectado com vizinho $Q - a_3$. O valor do gênero desta superfície decorre do fato de todas as faces serem quadriláteros, o que encerra a prova. ■

Exemplo 4.3.1. O grafo $\mathcal{C}_{32}(8, 2, 3)$ é mergulhado num 9-toro ($k = 3$), gerando um ladrilhamento só por quadrados, como é ilustrado na Figura 4.7.

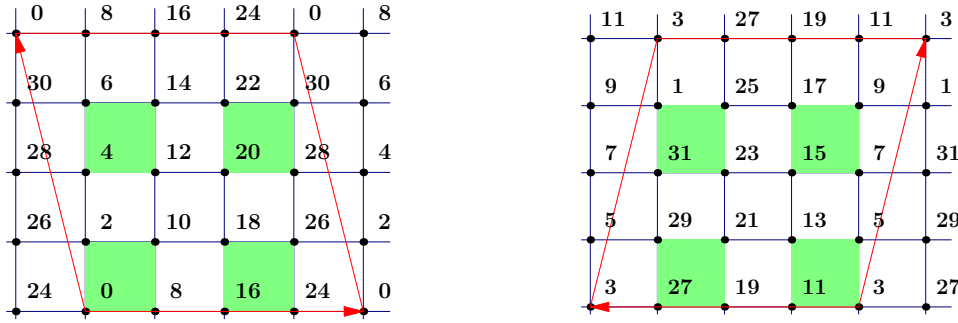


Figura 4.7: A figura mostra as duas componentes conexas do grafo $\mathcal{C}_{32}(8, 2)$. Utilizando o mergulho dado por 3.4.3, invertemos a orientação da segunda componente.

Gostaríamos de generalizar esse teorema para $k > 3$. Para $k = 3$, utilizamos o mergulho de quadriláteros do subgrafo $\mathcal{C}_n(a_1, a_2)$. É razoável esperar que isso valha também para $k > 3$.

Teorema 4.3.2. *Seja $\mathcal{G} = \mathcal{C}_n(a_1, \dots, a_k) = \mathcal{C}_{2^l u}(2^{l-i_1} a'_1, \dots, 2^{l-i_{k-1}} a'_{k-1}, a'_k)$, com $0 < i_1 < i_2 < \dots < i_{k-1} < l$. Então o gênero de G é $\frac{nk - 2n + 4}{4}$.*

Demonstração: A prova será feita por indução em k . Para $k = 2$, o resultado é válido pelo Teorema 4.2.2 e, para $k = 3$ é o Teorema 4.3.1 acima. Suponhamos que o resultado valha para $k - 1$. O grafo $\mathcal{H} = \mathcal{C}_n(a_1, \dots, a_{k-1})$ é um grafo circulante desconexo com um número par de componentes conexas, como vimos na Seção 3.6. Cada componente pode ser mergulhada em uma superfície na qual as faces possuem quatro lados. Como no teorema anterior, optamos pela inversão da orientação das componentes que contêm os múltiplos ímpares de a_k .

Desejamos acrescentar tubos que, topologicamente, são prismas com base quadrada. Definimos a base inferior desses tubos com sendo a seqüência de vértices $P, P \pm a_{k-1}, P \pm a_{k-1} \pm a_j, P \pm a_j$, onde $0 < j < k - 1$, e P :

$$P = r + \sum_{\substack{s=1 \\ s \neq j}} (p_s a_s) + 2p_j a_j + 2p_{k-1} a_{k-1}, \quad (4.7)$$

com r par, caracterizando as diferentes componentes de \mathcal{H} , $2p_j < l_j$, $2p_{k-1} < l_{k-1}$ e $p_s < l_s$, $s \neq j, k - 1$, onde $l_s = \min\{r \in \mathbb{Z}; r a_s \in \langle a_1, \dots, a_{s-1} \rangle\}$. Por definição, $l_1 = o(a_1)$ (ordem de a_1). Observe que, pela hipótese, cada l_s é par.

É claro que a base superior é dada por $I, I \pm a_{k-1}, I \pm a_{k-1} \pm a_j, I \pm a_j$, onde $I = P \pm a_k$. A nossa escolha define a soma a_k para a seqüência $P, P + a_{k-1}, P + a_{k-1} + a_j, P + a_j$ e a subtração de a_k para $P, P - a_{k-1}, P - a_{k-1} - a_j, P - a_j$.

Para concluir a prova, devemos garantir que todo vértice Q está conectado a $Q \pm a_k$. É suficiente provar apenas para a soma $Q + a_k$. Seja Q vértice de \mathcal{G} . Como os vértices de \mathcal{G} coincidem com os vértices de \mathcal{H} , o vértice Q está em alguma componente conexa de \mathcal{H} . Se Q está em uma componente par, devemos achar P tal que $Q \in \{P, P + a_{k-1}, P + a_{k-1} + a_j, P + a_j\}$, P como em (4.7). De forma análoga, concluiremos que $Q \in \{I, I - a_{k-1}, I - a_{k-1} - a_j, I - a_j\}$ se a componente for ímpar.

Podemos decompor Q como uma soma da forma $r + \sum_{s=1}^k \tilde{p}_s a_s$. Esta decomposição é única, pois $0 \leq r < \text{mdc}(a_1, \dots, a_{k-1}, n)$ e cada \tilde{p}_s é o menor inteiro, considerando-se todos os $\tilde{p}_t, t > s$ com os quais podemos escrever $Q = r + \sum_{s=1}^k \tilde{p}_s a_s$. Assim, tomamos $p_s = \tilde{p}_s, s \neq j, k-1$, $p_s = \lfloor a_s/2 \rfloor, s = j, k-1$. Logo $Q = P + \lceil \text{frac}(a_j/2) \rceil + \lceil \text{frac}(a_{k-1}/2) \rceil$, onde $\text{frac}(x)$ é a parte fracionária de x ($\text{frac}(x) = x - \lfloor x \rfloor$).

Portanto, $Q \in \{P, P + a_{k-1}, P + a_{k-1} + a_j, P + a_j\}$. Falta determinar o gênero da superfície construída, mas o gênero decorre do fato de que a superfície é ladrilhada por quadriláteros. Isso conclui a prova. ■

Voltando ao Teorema 4.2.3, concluímos que quando existia uma situação de soma ($a_l = a_i \pm a_k$), o gênero do grafo $\mathcal{C}_n(a_i, a_j, a_l)$ coincidia com o gênero da superfície na qual conseguimos mergulhar $\mathcal{C}(a_i, a_j)$ com faces quadradas. Podemos estender esse resultado? Isto é, dado um grafo $\mathcal{C}_n(a_1, \dots, a_k, a_i + a_j)$, o gênero é dado pelo mergulho de $\mathcal{C}_n(a_1, \dots, a_k)$ em uma superfície na qual os ladrilhos são quadrados? Dependendo dos índices, já conseguimos concluir que sim, como mostra o Corolário abaixo.

Corolário 4.3.1. *Seja $\mathcal{G} = \mathcal{C}_n(a_1, \dots, a_k)$ como no Teorema 4.3.2 e sejam $I = \{i_1, \dots, i_{k-1}\}$ os índices j escolhidos para exclusão da face determinada pelos vértices $P, P + a_i, P + a_i + a_j, P + a_j$ e $S = \{a_i \pm a_l; l < i, l \neq i_{i-1}\}$. Então o gênero de $\mathcal{H} = \mathcal{C}_n(a_1, \dots, a_k, b_1, \dots, b_m)$ é igual ao gênero de $\mathcal{C}_n(a_1, \dots, a_k)$, se $b_i \in S, \forall i = 1, \dots, m$.*

Demonstração: Pelo fato de \mathcal{H} ser um supergrafo de \mathcal{G} , seu gênero é maior que o gênero de \mathcal{G} o qual determinamos acima. Notamos que no mergulho dado pelo Teorema 4.3.2, as seqüências $P, P \pm a_j, P \pm a_j \pm a_k, P \pm a_k$ são faces. Assim, podemos acrescentar arestas que ligam o vértice P ao vértice $P \pm a_j \pm a_k$ (não simultaneamente), para todo $0 < j < k$. Logo, existe um mergulho satisfazendo o limitante inferior e, portanto, segue a igualdade. ■

Notamos que a escolha dos pontos P , da forma 4.7, pode ser modificada, ou seja, esta não é a única maneira de escolher um ponto base dos quadriláteros a serem excluídos para o acréscimo de tubos. Sendo assim, o resultado do Corolário acima pode ser melhorado escolhendo diferentes índices para determinar as diferentes faces com ponto base P possíveis, e, é claro, o índice mais

Perspectivas Futuras

A perspectiva natural é a de obter resultados que são extensões dos resultados obtidos durante este trabalho.

Reticulados-projeção: Os resultados conhecidos e os obtidos durante o doutorado restringem-se à projeções de \mathbb{Z}^n para $n \leq 4$. Desejamos estender estes resultados para dimensões $n \geq 5$. Já sabemos ser possível encontrar direções \mathbf{v} tais que o reticulado obtido da projeção de \mathbb{Z}^n seja uma pequena perturbação de \mathbb{Z}^{n-1} (a menos de escala). Mas o desejável é encontrar direções em que os reticulados-projeção sejam pequenas perturbações dos reticulados laminados Λ_{n-1} , que são os mais densos para a maioria das dimensões ([12]) onde o reticulado mais denso é conhecido. Para dimensão 5 testes preliminares mostram que é possível encontrar um reticulado intermediário que é mais denso que \mathbb{Z}^4 e menos denso que Λ_4 , uma espécie de $\mathbb{Z} \oplus \Lambda_3$. No artigo [40], Santhi e Vardy questionam a performance de codificações contínuas fonte/canal conhecidas e isto fortalece a necessidade de se encontrar direções de projeção com alta densidade de empacotamento para dimensões mais altas, o que não ocorre para a classe de vetores do artigo [47].

Grafos Circulantes: O gênero de um grafo circulante $\mathcal{C}_n(a_1, \dots, a_k)$, mesmo com grau $(2k)$ baixo como 6 ($k = 3$), pode ser arbitrariamente grande. A existência de uma classe de grafos circulantes com gênero dado pela fórmula $\frac{nk - 2n + 4}{4}$ está ligada a grafos com $2k$ conexões e cujo mergulho tem faces com quatro lados (“quadradas”). Grafos com esse perfil têm gêneros pequenos, perdendo apenas para os grafos circulantes em que haja triangularização dada pela conexão através de diagonais dessas faces. Nosso propósito é o de encontrar uma classificação para tais grafos circulantes. Também propomos investigar limitações para o número de vértices para grafos circulantes de diâmetro fixo, problema associado ao de se buscar bons códigos q-ários na métrica de Lee.

Geometria Hiperbólica e Métrica de Fisher: Como superfícies de gênero $g \geq 2$ são obtidas por quocientes do plano hiperbólico, uma das possibilidades de abordagem de questões gerais sobre o gênero de grafos circulantes é associada a ladrilhamentos deste plano. Um outro problema de

natureza distinta, também ligado à geometria hiperbólica, em que já temos alguns resultados e que não constam neste trabalho é associado à medida da distância entre duas distribuições gaussianas. As distribuições gaussianas de probabilidade no caso mais geral são dadas por um par (M, Σ) onde $M \in \mathbb{R}^n$ e $\Sigma \in M(n, n)$ é uma matriz simétrica não-singular. Dos cálculos preliminares para $n = 2$, ([15]) constatamos que este espaço com a métrica dada pela matriz de informação de Fisher não é exatamente um espaço hiperbólico mas possui subvariedades com curvaturas seccionais constantes. Se estas subvariedades forem completas, o seu recobrimento universal será o espaço euclidiano, hiperbólico ou esférico, dependendo do sinal da curvatura. O objetivo é determinar qual é o espaço que compõe o espaço destas distribuições e obter uma maneira de encontrar geodésicas deste espaço e a distância entre duas distribuições. Os artigos [13] e [18] dão uma perspectiva de aplicação destes resultados em teoria da informação.

Referências Bibliográficas

- [1] A. Ádám. Research problem 2-10. *J. Combinatorial Theory*, 1967.
- [2] E. Agrell, T. Eriksson, A. Vardy, e K. Zeger. Closest point search in lattices. *IEEE Trans. Inform. Theory*, 48(8):2201–2214, 2002.
- [3] E. Agustini. *Constelações de sinais em espaços hiperbólicos*. Tese de Doutorado, IMECC-Unicamp, 2002.
- [4] I. V. Bajić e J. W. Woods. Maximum minimal distance partitioning of the \mathbb{Z}^2 lattice. *IEEE Trans. Inform. Theory*, 49(4):981–992, 2003.
- [5] A. F. Beardon. *The geometry of discrete groups*, volume 91 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. Corrected reprint of the 1983 original.
- [6] E. Biglieri e M. Elia. Cyclic-group codes for the Gaussian channel. *IEEE Trans. Information Theory*, IT-22(5):624–629, 1976.
- [7] F. Boesch e R. Tindell. Circulants and their connectivities. *J. Graph Theory*, 8(4):487–499, 1984.
- [8] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.
- [9] J. W. S. Cassels. Rational quadratic forms. In *Proceedings of the International Mathematical Conference, Singapore 1981 (Singapore, 1981)*, volume 74 of *North-Holland Math. Stud.*, pages 9–26, Amsterdam, 1982. North-Holland.
- [10] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [11] H. Cohn. *Advanced number theory*. Dover Publications Inc., New York, 1980. Reprint of *A second course in number theory*, 1962, Dover Books on Advanced Mathematics.

- [12] J. H. Conway e N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen e B. B. Venkov.
- [13] M. H. M. Costa e T. C. Cover. On the similarity of the entropy power inequality and the brunn-minkowski inequality. *IEEE Trans. Inform. Theory*, 1984.
- [14] S. I. R. Costa, M. Muniz, E. Agustini, e R. Palazzo. Graphs, tessellations, and perfect codes on flat tori. *IEEE Trans. Inform. Theory*, 50(10):2363–2377, 2004.
- [15] S. I. R. Costa, S. A. Santos, e J. E. Strapasson. Fisher information theory e hyperbolic geometry. In *IEEE- Workshop in Information Theory- Coding and Complexity*, 2004.
- [16] S. I. R. Costa, J. E. Strapasson, M. Muniz, e T. B. Carlos. Circulant graphs viewed as graphs on flat tori. Pre-Print.
- [17] S. I. R. Costa, J. E. Strapasson, R. M. Siqueira, e M. Muniz. Circulant graphs, lattices and spherical codes (aceito). *Int. Journal of Applied Mathematics*, 2007.
- [18] A. Dembo e T. M. Cover. Information theoretic inequalities. *IEEE Trans. Inform. Theory*, 1991.
- [19] R. Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 2005.
- [20] R. Dougherty e V. Faber. The degree-diameter problem for several varieties of Cayley graphs. I. The abelian case. *SIAM J. Discrete Math.*, 17(3):478–519 (electronic), 2004.
- [21] B. Elspas e J. Turner. Graphs with circulant adjacency matrices. *J. Combinatorial Theory*, 9:297–307, 1970.
- [22] U. Fincke e M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.
- [23] G. David Forney, Jr. Geometrically uniform codes. *IEEE Trans. Inform. Theory*, 37(5):1241–1260, 1991.
- [24] S. Gallot, D. Hulin, e J. Lafontaine. *Riemannian geometry*. Universitext. Springer-Verlag, Berlin, 1987.

- [25] J. E. Goodman e J. O'Rourke, editors. *Handbook of discrete and computational geometry*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2004.
- [26] J. E. Gross e T. W. Tucker *Topological graph theory* Dover Publications Inc., Mineola, NY, 2001
- [27] T. C. Hales. Sphere packings. I. *Discrete Comput. Geom.*, 17(1):1–51, 1997.
- [28] T. C. Hales. Sphere packings. II. *Discrete Comput. Geom.*, 18(2):135–149, 1997.
- [29] T. C. Hales. A proof of the Kepler conjecture. *Ann. of Math. (2)*, 162(3):1065–1185, 2005.
- [30] T. C. Hales. Sphere packings. III. Extremal cases. *Discrete Comput. Geom.*, 36(1):71–110, 2006.
- [31] T. C. Hales. Sphere packings. IV. Detailed bounds. *Discrete Comput. Geom.*, 36(1):111–166, 2006.
- [32] Thomas C. Hales. A computer verification of the Kepler conjecture. In *Proceedings of the International Congress of Mathematicians, Vol. III (Beijing, 2002)*, pages 795–804, Beijing, 2002. Higher Ed. Press.
- [33] C. Heuberger. On planarity and colorability of circulant graphs. *Discrete Math.*, 268(1-3):153–169, 2003.
- [34] S. Katok. *Fuchsian groups*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.
- [35] B. A. LaMacchia. *Basis Reduction Algorithms and Subset Sum Problems*. Tese de Doutorado, Massachusetts Institute of Technology, 1991.
- [36] V. Liskovets e R. Pöschel. Counting circulant graphs of prime-power order by decomposing into orbit enumeration problems. *Discrete Math.*, 214(1-3):173–191, 2000.
- [37] D. Micciancio e S. Goldwasser. *Complexity of lattice problems*. The Kluwer International Series in Engineering and Computer Science, 671. Kluwer Academic Publishers, Boston, MA, 2002. A cryptographic perspective.
- [38] J. R. Munkres. *Topology: a first course*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1975.
- [39] T. D. Parsons. Circulant graph imbeddings. *J. Combin. Theory Ser. B*, 29(3):310–320, 1980.

-
- [40] N. Santhi e A. Vardy. Analog codes on graphs. arxiv.org and IEEE Transactions on Information Theory, 2006. (submetido).
- [41] R. M. Siqueira. *Códigos Esféricos com Simetrias Cíclicas*. Tese de Doutorado, UNICAMP, 2006.
- [42] D. Slepian. Group codes for the Gaussian channel. *Bell System Tech. J.*, 47:575–602, 1968.
- [43] M. Spivak. *Calculus on manifolds. A modern approach to classical theorems of advanced calculus*. W. A. Benjamin, Inc., New York-Amsterdam, 1965.
- [44] J. Stillwell. *Geometry of surfaces*. Universitext. Springer-Verlag, New York, 1992.
- [45] J. E Strapasson, S. I. R Costa, e M. Muniz. Genus of class circulant graphs. Pre-Print.
- [46] R. J. Trudeau. *Introduction to graph theory*. Dover Publications Inc., New York, 1993. Corrected reprint of the 1976 original.
- [47] V. A. Vaishampayan e S. I. R. R. Costa. Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. *IEEE Trans. Inform. Theory*, 49(7):1658–1672, 2003.
- [48] V. A. Vaishampayan, N. J. A. Sloane, e S. I. R. R. Costa. Dynamical systems, curves and coding for continuous alphabet sources. In *Proceedings International Telecommunications Symposium*. ITW2002, Bangalore, 2002.

Índice Remissivo

- Adjacentes, 55
- Algoritmo, xxv, 10, 48
 - RV, 49
- Anti-prisma, 74
- Arestas, 8, 55
- Cadeia, 56
- Codificação contínua
 - fonte/canal, xxvi, 19
 - na esfera, xxv
- Conjectura de Kepler, 6
- Códigos de grupos, xxv
- Códigos esféricos, xxvii, 8
 - vistos como Grafos Circulantes, 65
- Densidade
 - de centro, 8
 - de empacotamento, xxvi, 7
 - empacotamento, 21
- Distância mínima, xxv
- Empacotamento
 - de esferas, xxv, 6
 - reticulado, 6
- Euler
 - Segunda fórmula de, 71
- Expansão de grafos, 73
- Faces, 71
- fcc, xxvii, 37, 45
- Geometria Hiperbólica, 83
- Grafo, xxv, 8, 55
 - n -cadeia, 56
 - n -cíclico, 57, 61
 - Bipartido completo, xxvii, 57, 73
 - Completo, xxvii, 57, 61, 72
 - conexo, 56
 - desconexo, 56
 - planar, xxvii
 - regular, 56
 - sobre o toro plano, 58
 - toroidal, xxvii
- Grafos Circulantes, xxvi, xxvii, 60, 83
 - conexidade, 69
 - de gênero dados por $g = \frac{nk-2n+4}{4}$, 77
 - gênero de, 73
 - isomorfismo, 61
 - planares, 74
 - propriedade de Ádám, 61
 - sobre o toro plano, 62
 - toroidais, 74
 - vistos como Códigos esféricos, 65
- Grau, 56
- Gênero
 - de um grafo, 71
 - exemplos, 72
 - limitantes, 73
- Hermite
 - forma normal de, 65

- Isomorfismo, xxvii
- KZ, xxvi
- LLL, xxvi, 14, 15
- Matriz
 - de Gram, 5
 - geradora, 4
 - unimolular, 4
- Minkowski, xxvi
- Minkowski-reduzida, xxvi, 9, 11, 12, 22
- Métrica de Fisher, 83
- Norma Mínima, 7
- NP-completo, xxvi
- Paralelepípedo fundamental, xxvi, 4
- Prisma, 74
- Propriedade de Ádám, 61
- Quocientes de Reticulados, 8
- Redução
 - de Korkin-Zolotarev, 14, 15
 - de Lenstra-Lenstra-Lovász, 14
 - de Minkowski, 9, 15
 - LLL, 14
- Redução de base, xxvi
- Região
 - de Voronoi, xxvi, 4, 11, 12
 - fundamental, 4, 12
- Reticulado, xxv
 - base de um, 3
 - definição, 3
 - determinante de um, 5
 - discriminante de um, 4
 - equivalentes, 5
 - fcc, 6, 7
 - Hexagonal, 7
 - Reticulado-projeção, xxv, xxvi, 22, 37, 83
 - de \mathbb{Z}^3 , 24
 - de \mathbb{Z}^3 por $\mathbf{v} = (1, a, b(a))$, 25
 - de \mathbb{Z}^3 por $\mathbf{v} = (a, b, c(a, b))$, 29
 - de \mathbb{Z}^4 , 35
 - de \mathbb{Z}^4 por $\mathbf{v} = (a_4, a_3, a_2, a_1)$
 - $a_2 = a_2(a_4, a_3)$, $a_1 = a_1(a_4, a_3, a_2)$, 36
 - Rotulamento cíclico, 59
 - Sub-reticulado, 8
 - Subgrafo, 56
 - Teoria de códigos, xxv
 - Toro plano, 58
 - Vizinhos, 55
 - Vértices, xxvi, 8, 55