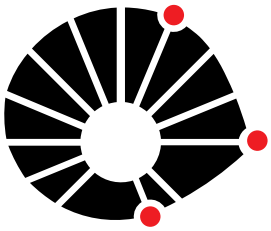


UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

MAKSON MILLER ALVES RIBEIRO

Sobre a densidade de empacotamento de reticulados obtidos através da Construção A

Campinas

2020

Makson Miller Alves Ribeiro

Sobre a densidade de empacotamento de reticulados obtidos através da Construção A

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

Orientadora: Sueli Irene Rodrigues Costa

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Makson Miller Alves Ribeiro e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.

Campinas

2020

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

R354s

Ribeiro, Makson Miller Alves, 1993-
Sobre a densidade de empacotamento de reticulados obtidos através da Construção A / Makson Miller Alves Ribeiro. – Campinas, SP : [s.n.], 2020.

Orientador: Sueli Irene Rodrigues Costa.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos corretores de erros (Teoria da informação). 2. Problemas de empacotamento. 3. Teoria dos reticulados. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: On packing density of Construction A lattices
Palavras-chave em inglês:
Error-correcting codes (Information theory)
Packing problems
Lattice theory
Área de concentração: Matemática Aplicada e Computacional
Titulação: Mestre em Matemática Aplicada e Computacional
Banca examinadora:
Sueli Irene Rodrigues Costa
Fabiano Boaventura de Miranda
Agnaldo José Ferrari
Data de defesa: 13-03-2020
Programa de Pós-Graduação: Matemática Aplicada e Computacional

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0003-0291-9996
- Currículo Lattes do autor: http://lattes.cnpq.br/7492327798440341

Dissertação de Mestrado Profissional defendida em 13 de março de 2020 e aprovada pela banca examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). FABIANO BOAVENTURA DE MIRANDA

Prof(a). Dr(a). AGNALDO JOSÉ FERRARI

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

A minha MÃE que sempre será minha professora da vida.

Agradecimentos

Agradecer pode parecer uma tarefa simples, mas não é. Para registrar aqui alguns agradecimentos, temos algumas limitações. Ao deixarmos de citar algo ou alguém (não menos importante), não reduz a gratidão por estes que fizeram parte desta conquista. A gratidão por conseguir finalizar esta etapa surge com bastante naturalidade, sendo assim, faz-se necessário destacar algumas pessoas que motivaram, apoiaram, ajudaram e de certa forma foram essenciais para a conclusão deste trabalho. Registro assim meus agradecimentos:

- Primeiramente à Deus, por ter me proporcionado condições para concluir esta etapa.

- Aos meus pais e meus irmãos, Miriam e Jorge, Thiago e Mariely, por todo apoio e sabedoria em me orientar e incentivar nos estudos até hoje.

- À minha orientadora Dra. Sueli, pelos momentos de ensino e aprendizagem, pelas conversas e principalmente pela paciência em mostrar caminhos de estudos. A experiência dos momentos compartilhados é, sem demagogia, extraordinária.

- Aos professores e coordenadores do programa que contribuíram para que eu chegasse até aqui e foram acolhedores, e principalmente, nos agregaram valores para a carreira docente. Um agradecimento também, não menos importante, aos funcionários do IMECC, particularmente os da secretaria de pós-graduação e da biblioteca.

- Agradeço ao pessoal do Buena Vista, em especial à direção e ao corpo docente, por terem paciência de se organizarem nas datas em que estive nas aulas do mestrado. Particularmente à diretora Elenir por me apoiar sempre, às coordenadoras Cristiane Maria e Critiane Jacome, sempre me ajudando e dando força para continuar os estudos a Zenaide pelos sorrisos e animação nas manhãs de preocupações.

- Aos amigos que a Unicamp me fez conhecer, em especial, Andrei, Camila, Enio, Gil e Suellen e o casal com uma família exemplar e exemplos de vida, Rafa e Dani Peres. Meu muito obrigado a todos vocês, pois não chegamos a esta fase sozinhos e às pessoas da república G8 que me acolheram no início desta caminhada e sempre foram solícitos.

- A Ju, quem me ajudou com os estudos, dúvidas no *Mathematica* e LaTeX, e por todo carinho e paciência demonstrado no fim desta dissertação, uma referência de pessoa, amiga, estudante, mãe e mulher.

- Aos professores que compõem a banca desta dissertação, Dr. Agnaldo José e Dr. Fabiano Boaventura meu muito obrigado. Em especial ao Fabiano, que me motivou durante a graduação na UEG, despertando meu interesse para estudar teoria de códigos.

- A todos que de certa forma, me apoiaram e se importaram com esta fase da minha vida, meu sincero agradecimento.

O sonho é que leva a gente para a frente.
Se a gente for seguir a razão, fica aquietado, acomodado.
Ariano Suassuna

Resumo

Códigos corretores de erros compõem uma das subáreas da teoria da informação. Códigos lineares sobre corpos finitos ou anéis tem propriedades especiais e podem ser utilizados para se obter reticulados via a chamada Construção A. Reticulados são subconjuntos discretos do espaço euclidiano n-dimensional formados por combinações inteiras de vetores independentes e vem sendo utilizados em diversas aplicações como em codificação para transmissão em canais Gaussianos ou com desvanecimento e em criptografia. Neste trabalho apresentamos uma breve introdução a códigos e reticulados e analisamos a densidade de empacotamento de alguns reticulados obtidos de códigos lineares sobre anéis finitos através da Construção A.

Palavras-chave: Códigos Lineares. Construção A. Densidade de Empacotamento. Reticulados.

Abstract

Error correcting codes compose one of the subareas of information theory. Linear codes over finite fields or rings have special properties and can be used to obtains lattices via the so called Construction A. Lattices are discrete subsets of the n-dimensional Euclidean space described as integer linear combinations of independent vectors and have been used in several applications such as coding for transmission over Gaussian or fading channels and cryptography. In this work we present a brief introduction to codes and lattices and analyze the packing density of some lattices obtained from linear codes over finite rings via the Construction A.

Keywords: Linear Codes. Construction A. Packing Density. Lattices.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

Na transmissão de uma mensagem, consideramos um emissor, um receptor e o canal por onde esta mensagem irá passar. Vamos supor que duas pessoas, A e B estejam se comunicando com uma certa distância entre elas em um parque. Se A diz uma frase para B, dizemos que A é o emissor, B o receptor e o ar é o canal por onde a mensagem passa (onde o som se propaga). Agora imaginemos que haja neste parque uma construção com várias máquinas emitindo sons de alta potência, e que tais sons não permitam a B entender por completo o que A está dizendo. Neste caso dizemos que houve ruído na entrega da mensagem.

A teoria da informação busca criar métodos para garantir que erros cometidos na transmissão e/ou armazenamento de dados possam ser detectados e corrigidos. Corrigir erros de transmissão de informação faz parte da teoria da informação, a qual usa bastante estruturas algébricas para embasar sua teoria. O capítulo 1 deste trabalho é dedicado a uma introdução à teoria de códigos, explorando resultados e exemplos já consolidados. As principais referências utilizadas foram [Hefez e Villela 2008], [Lavor et al. 2006, vol.21], [Hamming 1986] e [Boldrini et al. 1980].

No capítulo 2 abordamos a teoria de reticulados, que são oriundos de combinações lineares inteiras de um conjunto de vetores linearmente independentes no espaço euclidiano n-dimensional. Exibimos conceitos e resultados pertinentes, apresentando exemplos particulares e também reticulados bastante conhecidos como os reticulados raízes (A_n, D_n, E_n). As ilustrações e os cálculos foram feitos com o programa *Wolfram Mathematica 11.3* [Wolfram]. Apresentamos também neste capítulo o conceito de densidade de empacotamento de esferas, no caso em que os centros destas são pontos de um reticulado, e comentamos dois problemas clássicos que fazem reticulados serem ferramenta na área de informação, particularmente em criptografia, os quais são o problema do vetor mais curto e o do vetor mais próximo. As principais referências para este capítulo são [Costa et al. 2017], [Conway e Sloane 2013] e [Zong 1999].

O Capítulo 3 é dedicado à relacão entre códigos e reticulados q-ários cujos reticulados associados possuam densidade de empacotamento que se aproxime da máxima possível para uma dada dimensão. Este processo é abordado em dimensão dois, podendo ser estendido à outras dimensões, utilizando um código que possui um longo alfabeto. Analisamos também a densidade de vários reticulados obtidos via Construção A, a qual depende da distância euclidiana mínima do código envolvido. As referências principais para este capítulo são [Conway e Sloane 2013] e [Costa et al. 2017].

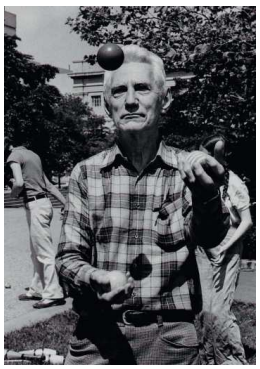
1 Códigos Corretores de Erros

"Information is the resolution of uncertainty."

Claude Shannon

Códigos corretores de erros compõem uma subárea da Teoria da Informação, a qual tem como marco o artigo de 1948 "*A mathematical theory of communication*" [Shannon 1948] do matemático e engenheiro eletrônico Claude Elwood Shannon (1916-2001) que integrava o corpo de pesquisadores do laboratório Bell (EUA). Este trabalho foi publicado logo depois (1949) em forma de livro [Shannon e Weaver 1949], com um capítulo adicional de W. Weaver que discute a teoria para um público mais geral.

Figura 1 – Claude Shannon



Fonte: Retirada da internet[1].

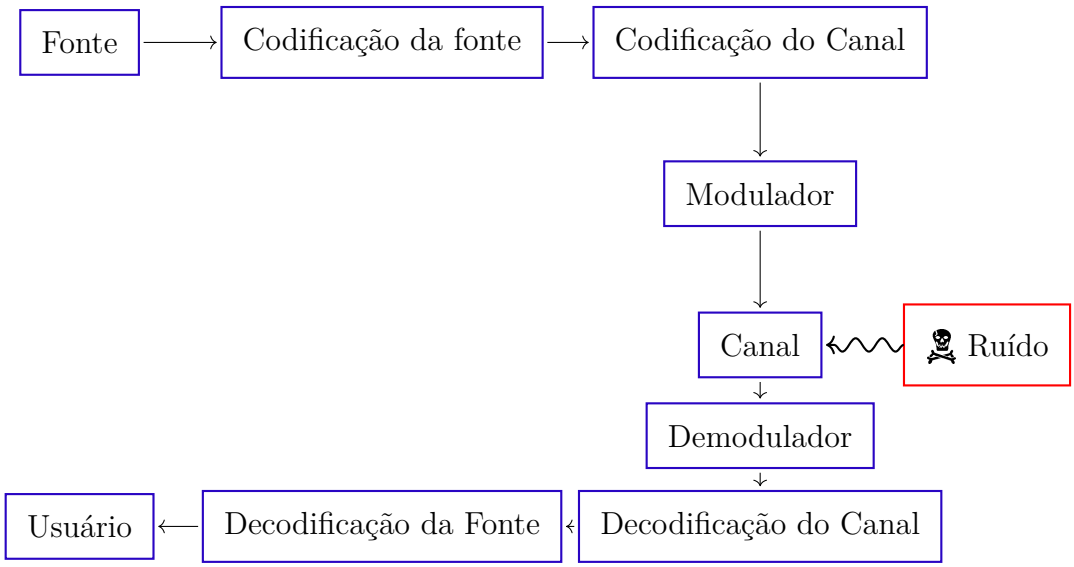
O processo de comunicação entre dois interlocutores baseia-se resumidamente entre um **emissor** que deseja enviar uma **mensagem** para um **receptor**, utilizando um **canal de comunicação** e dispondo de um **código**. Na teoria da informação o grande interesse é enviar mensagens eletrônicas, e portanto devemos utilizar a linguagem pelos quais os dispositivos eletrônicos (computatores e smartphones por exemplo) compreendem uma mensagem.

Boa parte dos computadores utilizam a linguagem binária como forma de enviar/armazenar uma mensagem, isto quer dizer que ao escolhermos uma determinada mensagem e a enviar por um computador, este a transformará em uma sequência (vetor) finita, com cada entrada sendo 0 ou 1.

[1] Disponivel em: <https://www.juggle.org/claude-shannon-mathematician-engineer-genius-juggler/>. Acessado em agosto de 2019.

O processo de transmissão está representado no esquema a seguir, onde uma fonte deseja enviar uma mensagem, e esta deve ser convertida, passando para linguagem do equipamento eletrônico em questão. Para receber a mensagem com máxima precisão, é necessário realizar a codificação de canal (geralmente acrescenta-se redundâncias no Código-fonte), em seguida tal mensagem deve passar por um modulador, o qual transforma a mensagem para sua forma digital (ondas). O canal será o meio por onde esta onda (sinal) transitará, finalmente para completar o processo de transmissão de sinais, deve-se demodular o sinal, decodificar o canal e por fim decodificar a fonte. Espera-se que a mensagem contida no receptor esteja de acorda com a transmitida pela fonte, caracterizando a mensagem como sem erros de transmissão.

Esquema de transmissão de sinais



1.1 Código corretor de erros

Como ilustrado no esquema anterior, um sinal (mensagem) usa o canal para sair da fonte e chegar até o usuário, e assume-se um canal ruidoso, isto é, ele é capaz de distorcer ligeiramente a mensagem (troca os bits) em questão. Sendo assim, faz-se necessário utilizar artifícios para que se por algum motivo, ocorrer algum erro na transmissão, o código criado seja capaz de identificar e se possível corrigí-lo.

Um código corretor de erros é basicamente uma técnica utilizada sobre as palavras do alfabeto (código fonte), que foram codificadas geralmente acrescentando redundâncias (código canal), para que assim seja possível detectar e se este for eficiente, também corrigir.

1.1.0.1 Algumas terminologias da Teoria da Informação

1. O Alfabeto $\mathbb{A}$ (finito) é formado por todos os símbolos nos quais se pode utilizar para o processo de codificação. Via de regra ultiliza-se $\mathbb{A} = \mathbb{Z}_q$ (inteiros módulo q).

2. Palavras são sequências (finitas) utilizando elementos do alfabeto $\mathbb{A}$.

3. Comprimento é quantidade de símbolos (entradas) utilizados para escrever uma palavra.

Definição 1.1.1. *Um código corretor de erros C , tendo $\mathbb{A}$ como alfabeto, é um subconjunto de $\mathbb{A}^n$, isto é, $C \subset \mathbb{A}^n$.*

Os computadores trabalham geralmentes na linguagem binária, isto é, o alfabeto $\mathbb{A} = \mathbb{Z}_2 = \{0, 1\}$, logo qualquer operação proposta à este equipamento é reduzida à uma operação sobre os binários. exibimos abaixo a tábua das operações de soma e multiplicação (módulo 2) respectivamente

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Exemplo 1.1.1. *Operações entre palavras do código.*
Considere $C = \{(0,0,0,0,0,0)\,;(0,1,0,1,0,1)\,;(1,0,1,0,1,0);(1,1,1,1,1,1)\} \subset \mathbb{Z}_2^6$. *Podemos então somar duas palavras quaisquer deste código, por exemeplo:*

$$(1,1,1,1,1,1) \;+\; (0,1,0,1,0,1) = (1,0,1,0,1,0).$$

1.2 Entropia

Em teoria da informação, o conceito de entropia [Cover e Thomas 2012, pg.5] surgiu no artigo de Shannon (1948), e esta é uma função capaz de determinar a incerteza da informação recebida ou de uma variável aleatória. Esta ideia se deve ao fato de que o processo de transmissão de sinais (ou informação) é caracterizado como não determinístico. De fato, ao se transmitir uma mensagem não se sabe qual é a mensagem que chegará ao receptor. Shannon percebeu que poderia relacionar este processo como um processo de Markov, definindo assim a entropia ou ainda em sua homenagem, a **entropia de Shannon**, como

$$H = \sum_{i=1}^{n} p_i \cdot \log \frac{1}{p_i} = -\sum_{i=1}^{n} p_i \cdot \log p_i, \tag{1.1}$$

onde p_i é a probabilidade do i-ésimo resultado dos n possíveis.

Observação 1.2.1. *Quando se utiliza base dois para o logaritmo em questão tal entropia será expressa em bits.*

1.2.1 Aplicações da Entropia de Shannon

Exemplo 1.2.1 (Quantidades de bits para codificar uma mensagem)**.** *Suponhamos que se queira codificar os resultados (eventos) de um lançamento de certo dado (honesto). Como estamos sobre um espaço amostral equiprovável, temos que* $p_i = \frac{1}{6}$ *para qualquer um dos seis resultados possíveis, daí temos que a entropia*

$$H = 6 \cdot \frac{1}{6} \cdot \log_2 \frac{1}{6} \simeq 2,6.$$

Como utilizamos uma quantidade inteira de bits, temos que será necessário três bits para a codificação dos seis possíveis resultados.

Exemplo 1.2.2 (Medida de diversidade em ecologia)**.** *Para se calcular a medida da diversidade em uma comunidade com várias espécies no mesmo ambiente, considera-se* $p_i = \frac{i}{\sum_{i=1}^{n} i}$*, donde* p_i *é a ocorrência da espécie* i *nesta comunidade [Masisi, Nelwamondo e Marwala 2008].*

A entropia é calculada em diversas bases, na ecologia, costuma-se empregar o logarítmo natural ou seja a base e*. Assim a entropia, de forma análoga ao exemplo anterior pode ser expressa como*

$$H = \sum_{i=1}^{n} p_i \cdot \ln \frac{1}{p_i} = -\sum_{i=1}^{n} p_i \cdot \ln p_i, \tag{1.2}$$

1.3 Alguns códigos bem conhecidos

1.3.1 Validação do cadastro de pessoa física (CPF)

Um código bastante popular é utilizado para saber se o CPF (uma sequência de nove algarismos seguidos de mais dois algarismos verificadores, haja vista que a Receita Federal reconhece cada cidadão brasileiro por este número) é válido ou não, estes dois dígitos verificadores são calculados a partir dos nove dígitos iniciais. Chamaremos neste caso n_i o valor do dígito na posição i.

$$n_{10} = \left[\left(\sum_{i=1}^{9} i \cdot n_i \right) \mod 11 \right] mod\ 10 \tag{1.3}$$

$$n_{11} = \left[\left(\sum_{i=0}^{9} i \cdot n_{i+1} \right) \mod 11 \right] mod\ 10. \tag{1.4}$$

Exemplo 1.3.1. *O portador de um CPF com os noves primeiros dígitos sendo* 010101010 *terá*

$$n_{10} = 20 \mod 11 \equiv 9$$
$$n_{11} = 97 \mod 11 \equiv 9$$

Gerando o CPF $010101010 - 99$.

1.3.2 Código de tripla repetição

Exemplo 1.3.2. *Suponhamos que em uma matéria, o professor estabeleceu quatro conceitos para avaliar seus alunos, A, B, C e D, sendo que D determina a reprovação na disciplina. Ao lançar um conceito (enviar uma informação), o professor usará um dispositivo eletrônico para digitar estes conceitos, por conveniência estas notas são mapeadas em* $\{0,1\} \times \{0,1\}$ *da seguinte maneira*

$$A \mapsto 00$$
$$B \mapsto 01$$
$$C \mapsto 10$$
$$D \mapsto 11$$

Estas notas passarão por um canal de transmisão, o qual está sujeito a erros. Para dificultar a ocorrência de um erro grave, utilizamos o código canal da tripla repetição, fazendo com que

$$A \mapsto 000000$$
$$B \mapsto 010101$$
$$C \mapsto 101010$$
$$D \mapsto 111111$$

Neste caso temos que o código canal $C = \{(0,0,0,0,0,0),(0,1,0,1,0,1),(1,0,1,0,1,0),(1,1,1,1,1,1)\}$. *Este código possibilita corrigir um erro. De fato, se apenas um dígito for corrompido. Por exemplo, recebe-se a palavra* $(1,1,0,1,0,1)$, *a qual não pertence ao código, é possível corrigir trocando o primeiro elemento por zero e assim entregar a mensagem correta, a saber* $(0,1,0,1,0,1)$.

Exemplo 1.3.3. *[Lavor et al. 2006, vol.21]. Consideremos agora, que um robô possa se mover num plano nas diagonais, e nas direções leste, oeste, norte e sul, observamos que a entropia (considerando os oito movimentos com mesma probabilidade) é três bits (três dígitos), sendo assim se faz necessário um código fonte binário com oito elementos e*

cada um com três bits (cada elemento mapeia um movimento). Consideramos então nosso código fonte como $\mathbb{Z}_2^3$. *Associado o código fonte*

$$\begin{aligned} N &\mapsto 000 \qquad & S &\mapsto 001 \\ L &\mapsto 010 \qquad & O &\mapsto 100 \\ NE &\mapsto 011 \qquad & SO &\mapsto 101 \\ SE &\mapsto 110 \qquad & NO &\mapsto 111. \end{aligned}$$

Conforme no exemplo 1.3.2, temos que qualquer bit distorcido por consequência de um canal ruidoso, faz com que o robô faça um movimento indesejado, necessitando assim do incremento de redundâncias para o código-canal. Em vez do tripla repetição propomos um código canal mais econômico, sendo

$$(x_1, x_2, x_3) \mapsto (x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3).$$

Com o seguinte mapeamento

$$\begin{aligned} N &\mapsto 000000 \qquad & S &\mapsto 001011 \\ L &\mapsto 010101 \qquad & O &\mapsto 100110 \\ NE &\mapsto 011110 \qquad & SO &\mapsto 101101 \\ SE &\mapsto 110011 \qquad & NO &\mapsto 111000. \end{aligned}$$

1.3.3 Função distância

Existem diversas maneiras de medir a distância entre dois objetos. Dada uma função distância ou métrica $d : \mathbb{A}^n \times \mathbb{A}^n \longrightarrow \mathbb{R}_+$, para qualquer $(x, y) \in \mathbb{A}^n \times \mathbb{A}^n$, temos:

i. $d(x, y) \geqslant 0$;

ii. $d(x, y) = 0 \Leftrightarrow x = y$;

iii. $d(x, y) = d(y, x)$;

iv. $d(x, z) \leqslant d(x, y) + d(y, z)$.

Algumas métricas são bastantes conhecidas como a **euclidiana**, a do **máximo** (ou Chebyshév) e da **soma**(ou métrica do taxista ou métrica de Manhattan). Na Teoria de Códigos é de interesse sabermos o quanto uma informação difere uma da outra e para isto se define as métricas abaixo.

Definição 1.3.1. *Dadas duas palavras* $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{A}^n$, *onde* $\mathbb{A}$ *é um conjunto finito, a distância de Hamming entre* x *e* y *é dada pelo número de coordenadas distintas entre* x *e* y*:*

$$d_H(x, y) = \mid i : x_i \neq y_i, 1 \leqslant i \leqslant n \mid .$$

É bem simples verificar que dado um conjunto finito $\mathbb{A}$, *a distância de Hamming satisfaz as quatro propriedades requeridas para ser uma distância.* De fato, as três primeiras são imeditamente verificadas e para verificar a quarta, isto é, $d_H(x,z) \leqslant d_H(x,y)+d_H(y,z)$, tomamos $A = \{i|x_i = z_i\}$, $B = \{i|x_i = y_i\}$ e $C = \{i|y_i = z_i\}$, temos que $B \cap C \subset A$, pois se tomarmos $\bar{i} \in B \cap C$ pela transitividade na relação de igualdade teremos que $\bar{i} \in A$, o que equivale para os conjuntos complementares em $\{0,\ldots,n\}$ $A^c \subset (B \cap C)^c = B^c \cup C^c$, como $|A^c| \leqslant |B^c \cup C^c| \leqslant |B^c| + |C^c|$, e temos $d_H(x,z) = |A^c|$, $d_H(x,y) = |B^c|$ e $d_H(y,z) = |C^c|$, segue daí que $d_H(x,z) \leqslant d_H(x,y) + d_H(y,z)$. Uma outra noção de distância que introduzimos a seguir é bastante utilizada no conjunto $\mathbb{Z}_q^n$, ela coincide com a distância de Hamming apenas para os casos $q = 2$ e $q = 3$.

Definição 1.3.2. *Dado $x, y \in \mathbb{Z}_q^n$ com $x = (x_1,\ldots,x_n)$, $y = (y_1,\ldots,y_n)$. A distância de Lee definida sobre $\mathbb{Z}_q^n$, é dada por*

$$d_{Lee}(x,y) = \sum_{i=1}^{n} \min\{|\ x_i - y_i\ |, q - |\ x_i - y_i\ |\}.$$

Exemplo 1.3.4. *Considerando $\mathbb{Z}_{11}$ e as classes residuais $\overline{2}$, $\overline{6}$ e $\overline{10}$, a distâcia de Lee será:*

$$d_{Lee}(\overline{2},\overline{6}) = 4,\ d_L(\overline{2},\overline{10}) = 3\ \ e\ \ d_L(\overline{6},\overline{10}) = 4.$$

Uma noção geométrica para a métrica de Lee é que se estivermos trabalhando sobre o anel $\mathbb{Z}_q$ e colocarmos cada classe residual sobre um vértice (orientando sua enumeração) de um polígono regular que possui q lados. A distância de Lee é interpretada como o menor caminho de arestas que será utilizado para conectar os dois vértices. Observe o Exemplo 1.3.4 e a Figura 2.

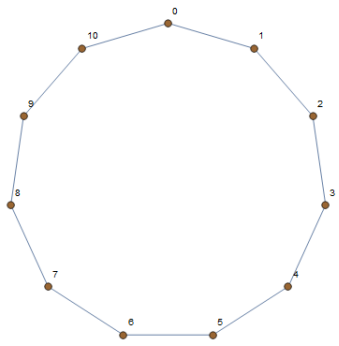


Figura 2 – $\mathbb{Z}_{11}$ na métrica de Lee

Definição 1.3.3. *Seja $x \in \mathbb{A}^n$ e $r \in \mathbb{R}$, $r > 0$.Definimos a bola aberta, a bola fechada e a esfera de centro x e raio r, segundo a distância d, como os respectivos conjuntos*

$$B(x,r) = \{y \in \mathbb{A}^n; d(x,y) < r\}$$
$$B[x,r] = \{y \in \mathbb{A}^n; d(x,y) \leqslant r\}$$
$$S(x,r) = \{y \in \mathbb{A}^n; d(x,y) = r\}.$$

Definição 1.3.4. *Dado um código $C \subset \mathbb{A}^n$, definimos a distância mínima (na métrica de hamming) de C como sendo*

$$d(C) = min\{d_h(\boldsymbol{x},\boldsymbol{y}); \boldsymbol{x},\boldsymbol{y} \in C, \boldsymbol{x} \neq \boldsymbol{y}\}.$$

Teorema 1.3.1. *[Lavor et al. 2006, vol.21] Seja $C \subset \mathbb{Z}_2^n$ um código binário com distância mínima d e seja*

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Então é possível detectar $d-1$ erros e corrigir t erros.

O teorema acima nos diz que o quanto maior a distância mínima maior será a capacidade de correção deste código, isto equivale a encontrar t de tal forma que as bolas de centro em uma palavra do código e raio t, terão intersecção vazias. Caso uma palavra seja recebida com até $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros existirá uma única palavra do código com distância menor do que ou igual a t da recebida, este método é denominado correção por verossimilhança como ilustra a Figura 3 a seguir.

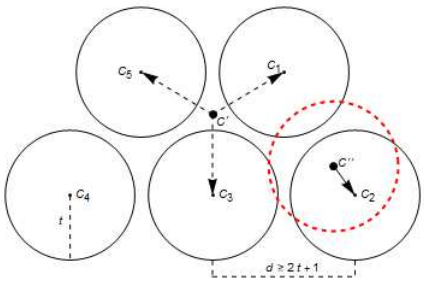


Figura 3 – Correção por verossimilhança.

Observamos que para outras distâncias com valores inteiros, como a de Lee, também teremos esta correção de até $\left\lfloor \frac{d_{Lee}-1}{2} \right\rfloor$ erros.
Os códigos cujas bolas de raio t, centradas em suas palavras, estejam mutuamente disjuntas e a união destas mesmas bolas seja todo conjunto $\mathbb{A}^n$ recebem uma nomenclatura especial, vejamos .

Definição 1.3.5. *Sejam d a distância mínima de um código $C \subset \mathbb{A}^n$ e $t = \left\lfloor \frac{d-1}{2} \right\rfloor$. Dizemos que C é um* ***código perfeito*** *se*

$$\bigcup_{c \in C} B[c,t] = \mathbb{A}^n.$$

Observação 1.3.1. *Um código pode ser perfeito em uma métrica d_1 e não ser perfeito para uma métrica d_2.*

Exemplo 1.3.5. *Seja o código $C = \{a \cdot (2,1)\}$ com $a \in \mathbb{Z}_5$, isto é, $C = \{(0,0);(2,1);(4,2);(1,3);(3,4)\} \subset \mathbb{Z}_5^2$. A distância mínima de Hamming para C é dois, enquanto na métrica de Lee, a distância mínima é três. Logo para esta métrica temos que o código é capaz de corrigir um erro. Tomando $t = 1$, temos que*

$$\begin{aligned}
B_1[(0,0),1] &= \{(0,0),(0,1),(0,4),(1,0),(4,0)\};\\
B_2[(2,1),1] &= \{(2,0),(2,1),(2,2),(1,1),(3,1)\};\\
B_3[(4,2),1] &= \{(4,1),(4,2),(4,3),(0,2),(3,2)\};\\
B_4[(1,3),1] &= \{(1,2),(1,3),(1,4),(0,3),(2,3)\};\\
B_5[(3,4),1] &= \{(3,0),(3,3),(3,4),(2,4),(4,4)\},
\end{aligned}$$

e portanto

$$B_i \cap B_j = \varnothing \; e \bigcup_{i=1}^{5} = \mathbb{Z}_5^2.$$

C é um código perfeito segundo a métrica de Lee, ou ainda C é dito 1-perfeito. Como pode ser notado, este código na métrica de Hamming não é perfeito, nem corrige um erro.

1.4 Códigos q-ários Lineares

Consideramos neste trabalho $\mathbb{A} = \mathbb{Z}_q$, conjunto dos inteiros módulo q com as operações usuais de soma e multiplicação. Um código $C \subset \mathbb{Z}_q^n$ é chamado um código q-ário.

Definição 1.4.1. *Um código $C \subset \mathbb{Z}_q^n$ será dito linear se C for um subgrupo aditivo de $\mathbb{Z}_q^n$.*

Veja que dada a condição de subgrupo, teremos para um código linear que $(0,0,\ldots,0) \in C$, e que para quaisquer u,v palavras de C e $\alpha \in \mathbb{Z}_q$ sempre teremos $-u$, $u+v$ e $\alpha \cdot v$ como elementos de C. O código do Exemplo 1.3.5 é 5-ário e linear. A menos de menção em contrário, ao nos referirmos a códigos q-ários, estaremos sempre assumindo que estes sejam lineares.

Observação 1.4.1. *Um caso muito especial é quando q for um número primo, portanto o alfabeto $\mathbb{Z}_q$ é um corpo ou ainda $\mathbb{Z}_q = \mathbb{F}_q$ (corpo de Galois). Neste caso especial, um código linear C será um subespaço vetorial de dimensão k do espaço vetorial $\mathbb{Z}_q^n$ e terá q^k palavras-código [Costa et al. 2017, pg.38].*

Observação 1.4.2. *Note que se $\mathbb{A}$ for um corpo finito e C um subespaço vetorial de dimensão k em $\mathbb{A}^n$, como $\mid C \mid = q^k$, daí $R(C) = \frac{k}{n}$.*[2]

Podemos definir códigos lineares como a imagem de uma transformação linear injetiva, da seguinte maneira

$$\begin{aligned} \Phi : \mathbb{Z}_q^k &\to \mathbb{Z}_q^n \\ (x_1, x_2, \ldots, x_k)^T &\mapsto G_{n\times k} \cdot (x_1, x_2, \ldots, x_k)^T. \end{aligned}$$

Neste caso dizemos que $\mathbb{Z}_q^k$ contém o Código-fonte e $\Phi(\mathbb{Z}_q^k)$ contém o código de canal. $G_{n\times k}$ é uma matriz cuja as entradas são elementos de $\mathbb{Z}_q$, e esta denomina-se **matriz geradora** do código C. Alertamos quanto a matriz geradora, que esta não é única. No caso em que q é primo a matriz geradora está condicionada à escolha de uma base do código C e tal base não é única. Um caso especial é quando a matriz geradora é uma matriz cuja as primeiras k linhas formam a matriz identidade de ordem k, esta matriz recebe nome de **matriz geradora na forma padrão ou sistemática**, ou seja

$$G = \begin{bmatrix} I_k \\ B_{(n-k)\times k} \end{bmatrix}.$$

Se uma matriz está na forma sistemática, então

$$\Phi(x_1, x_2, \ldots, x_k) = (x_1, x_2, \ldots, x_k, p_1, p_2, \ldots, p_{n-k}),$$

onde cada p_i é combinação linear das primeiras k entradas. Quando temos q primo, sempre poderemos considerar, a menos de trocas de coordenadas, uma matriz geradora do código na forma sistemática.

Exemplo 1.4.1. *As matrizes geradoras para os códigos dos exemplos 1.3.2 e 1.3.3, são*

[2] $R(C)$ denota a taxa de informação do código C, esta é dada por $R(C) = \frac{\log_q m}{n}$ com $m = |C|$.

respectivamente:

$$G_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad G_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Definição 1.4.2. *Dado p primo, um código $C \subset \mathbb{Z}_p^n = \mathbb{F}_p^n$ de dimensão k, possuindo G como matriz geradora, chama-se* ***matriz de paridade*** *ou* ***matriz de verificação****, a matriz $H_{(n-k)\times n}$ tal que:*

$$H \cdot \boldsymbol{w}^T = 0 \Leftrightarrow \boldsymbol{w} \in C \subset \mathbb{A}^n.$$

Definição 1.4.3. *Seja C um [n-k] código linear sobre o corpo $\mathbb{F}_p = \mathbb{Z}_p$, p primo. Definimos o códgio* ***ortogonal*** *ou* ***dual*** *$C^\perp$ da seguinte forma*

$$C^\perp = \{u | < u, v >= 0 \, \forall \, v \in C\}.$$

Observação 1.4.3. *Observamos que neste caso estamos definindo o código C como núcleo de uma transformação que tem H como matriz.*

Exemplo 1.4.2. *Seja $C = \{(0,0,0);(0,1,1);(1,0,1);(1,1,0)\} \subset \mathbb{Z}_2^3$, então seu código dual será $C^\perp = \{(0,0,0);(1,1,1)\}$. Note que $\left(C^\perp\right)^\perp = C$.*

Proposição 1.4.1. *[Lavor et al. 2006, vol.21, pg.17]. Dada G uma matriz geradora na forma padrão para um código $C \subset \mathbb{Z}_p^n$, então a matriz de paridade H assume a seguinte forma*

$$H = \begin{bmatrix} -B & I_{(n-k)\times(n-k)} \end{bmatrix}.$$

Exemplo 1.4.3. *Como no exemplo 1.4.1 as matrizes geradoras G_1 e G_2 estão na forma padrão, temos que as matrizes de paridade H_1 e H_2 são respectivamente*

$$H_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad H_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Ao receber uma mensagem (palavra) w é possível verificar se houve ou não erros de transmisão, este procedimento é feito aplicando w à matriz de paridade. Temos que $H \cdot w \in \mathbb{Z}_p^{n-k}$, e este vetor é chamado de **síndrome**. Concluimos assim que uma palavra pertence ao código se e somente se a síndrome for nula.

1.5 Código de Hamming

Richard Hamming através de conversas com Shannon se interessou pela Teoria de Códigos Corretores de Erros, e desenvolveu um trabalho de fundamental importância nesta área. Os códigos que levam seu nome tem destaque na Teoria da Informação e são utilizados em muitas aplicações. Nestes códigos $n = 2^r - 1$, com $r \geqslant 2$ e a matriz de paridade de ordem $r \times (2^r - 1)$ denotada por H_r tem por colunas todos os vetores não nulos de $\mathbb{Z}_2^r = \mathbb{F}_2^r$. Como o número mínimo de vetores-coluna desta matriz que forma uma coluna linearmente dependende é três, podemos afirmar [Lavor et al. 2006, vol.21, prop.1.3] que um o código binário que tem esta matriz de paridade, tem distância de Hamming mínima igual a três, e portanto corrige um erro. Este $[2^r - 1, 2^r - r - 1]$código linear binário $\mathcal{H}_r$ é conhecido como código de Hamming.

Teorema 1.5.1. *O código $\mathcal{H}_r$ é um código perfeito que corrige um erro.*

Demonstração. Usaremos o fato que todo código de Hamming possui distância mínima três então $t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$. Vamos calcular a cardinalidade da união das bolas de raio um centradas nas palavras de $\mathcal{H}_r$. Inicialmente observamos que

$$|B_{d_h}[x, 1]| = \binom{2^r - 1}{0} + \binom{2^r - 1}{1} = 2^r.$$

Esta cardinalidade é para cada palavra x do código, agora observando que a cardinalidade do código é $2^{2^r - r - 1}$, obtemos que a quantidade de elementos na união das bolas será

$$2^r \cdot 2^{2^r - r - 1} = 2^{2^r - 1} = \left|\mathbb{Z}_2^{2^r - 1}\right|.$$

□

1.5.1 O código de Hamming 7-4

Se considerarmos $r = 3$, a matriz de paridade H contendo todos os vetores não nulos de $\mathbb{Z}_2^3$ e ordenados de forma a termos uma matriz identidade 3×3 nas três últimas colunas e uma matriz 3×4 nas quatro primeiras, teremos como vimos na seção anterior que a matriz geradora associada ao código de Hamming é de ordem 7×4, tendo a matriz identidade 4×4 nas primeiras linhas e a matriz $-B = B$ nas três últimas. Assim teremos o código, $C = \{(x_1, x_2, x_3, x_4, x_5, x_6, x_7)\}$ com matriz geradora

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

2 Reticulados

A teoria de reticulados tem relação com diversas áreas de pesquisa e aplicações, como cristalografia, criptografia, telecomunicações e álgebra booleana. Existem relatos de problemas propostos no século XVII relacionados à reticulados, entretanto tal teoria foi formalizada apenas no século XX com os trabalhos iniciais como os de Hermann Minkowski, C. Rogers e Fejes Tóth. Neste capítulo resumimos conceitos e propriedades que formam a base de nosso estudo sendo que as principais referências utilizadas foram ([Lavor et al. 2006, vol.21], [Costa et al. 2017], [Conway e Sloane 2013] e [Zong 1999]).

2.1 Conceitos e definições

Definição 2.1.1. *Dado um conjunto de vetores linearmente independentes* $\beta = \{b_1, b_2, \ldots, b_m\} \in \mathbb{R}^n$[1]*, chamamos de reticulado* Λ*, o conjunto de todas as combinações lineares* ***inteiras*** *de* b_i*, ou seja :*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i \cdot b_i : \ \lambda_i \in \mathbb{Z} \right\}.$$

Definição 2.1.2. *O conjunto* β *acima é denominado uma base do reticulado* Λ *e a matriz* $B = B(\beta)$ *que tem os vetores de* β *como colunas é uma matriz geradora do reticulado.*

Observação 2.1.1. *Um vetor* $v \in \mathbb{R}^n$ *pertence ao reticulado se e somente se puder ser escrito na forma coluna como* $v = B \cdot z$ *onde* z *é um vetor coluna com coordenadas inteiras.*

Exemplo 2.1.1. *Definindo* $b_1 = \left(\frac{1+\sqrt{5}}{2}, 0\right)$ *e* $b_2 = \left(1, \frac{3-\sqrt{5}}{2}\right)$*, o reticulado gerado por esta base possui como matriz geradora*

$$B = \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 1 \\ 0 & \frac{3-\sqrt{5}}{2} \end{bmatrix},$$

e sua representação geométrica no plano pode ser vista na Figura 4.

[1] Quando $m = n$ dizemos que o reticulado é de posto completo.

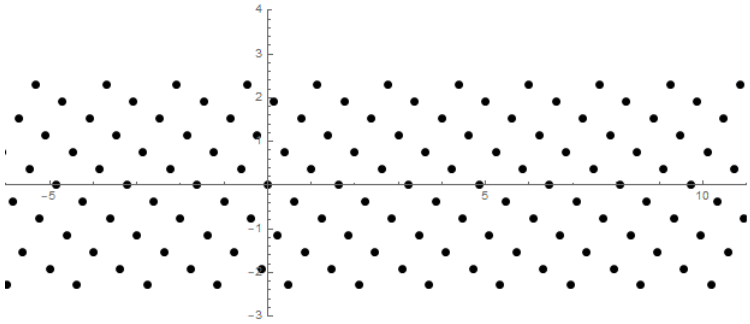
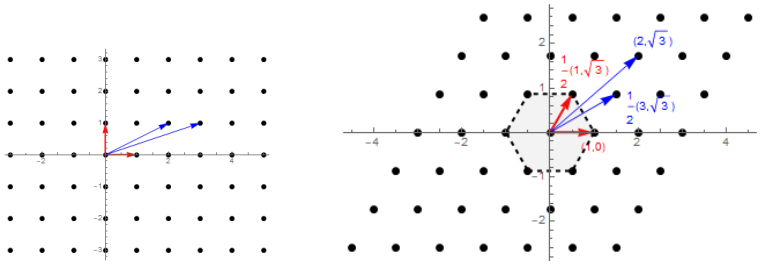


Figura 4 – Reticulado gerado pela matriz B restrito à um retângulo.

Observação 2.1.2. *Um reticulado gerado por uma matriz B, $\Lambda(B)$, pode também ser gerado por uma outra matriz B'. Isto significa que a base (consequentemente a matriz geradora) de um reticulado não é única. A Figura 5 ilustra que o reticulado $\mathbb{Z}^2$ pode ser construído utilizando a base $\{(1,0);(0,1)\}$ ou a base $\{(3,1);(4,1)\}$, enquanto o reticulado hexagonal pode ser contruído tomando a base $\left\{(1,0);\left(\frac{1}{2};\frac{\sqrt{3}}{2}\right)\right\}$ ou a base $\left\{\left(\frac{3}{2},\frac{\sqrt{3}}{2}\right),\left(2,\sqrt{3}\right)\right\}$.*



(a) Reticulado $\mathbb{Z}^2$ restrito à um retângulo.

(b) Reticulado hexagonal restrito à um retângulo.

Figura 5 – Reticulados gerados por duas bases distintas

Proposição 2.1.1. *[Costa et al. 2017] Duas matrizes A e B geradoras $n \times k$ de posto $k \leqslant n$ geram o mesmo reticulado se e somente se $A = B \cdot U$ onde U é uma matriz $k \times k$ unimodular, isto é, com entradas inteiras e determinante ± 1.*

Podemos caracterizar reticulados de um outro modo, mas antes, vale lembrar que um conjunto é discreto quando não possui pontos de acumulação, ou seja, todo ponto do conjunto é classificado como um ponto isolado [Elon 2015, Pg.21]. Em outras palavras, para um conjunto ser discreto há a necessidade da existência de um $\epsilon > 0$ tal que quando tomarmos a intersecção da bola de raio ϵ centrada em um elemento qualquer do conjunto, com o próprio conjunto o resultado deve ser somente o centro da bola.

Em [Cassel 2012, Pg.78] encontra-se uma condição necessária e suficiente para que um conjunto de pontos, seja classificado como um reticulado, enuciamos o teorema abaixo cuja demonstração pode ser vista nesta mesma referência.

Teorema 2.1.1. *Dado um subconjunto do $\mathbb{R}^n$ este será um reticulado se, e somente se, for um* ***subgrupo aditivo discreto****.*

Exemplo 2.1.2. *Em $\mathbb{R}^3$ um reticulado clássico é o $\mathbb{Z}^3$, onde temos a base canônica $\{b_1, b_2, b_3\}$, $b_1 = (1, 0, 0)$, $b_2 = (0, 1, 0)$ e $b_3 = (0, 0, 1)$ cuja a matriz geradora, B, é dada por*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

e sua representação gráfica pode ser vista na figura abaixo.

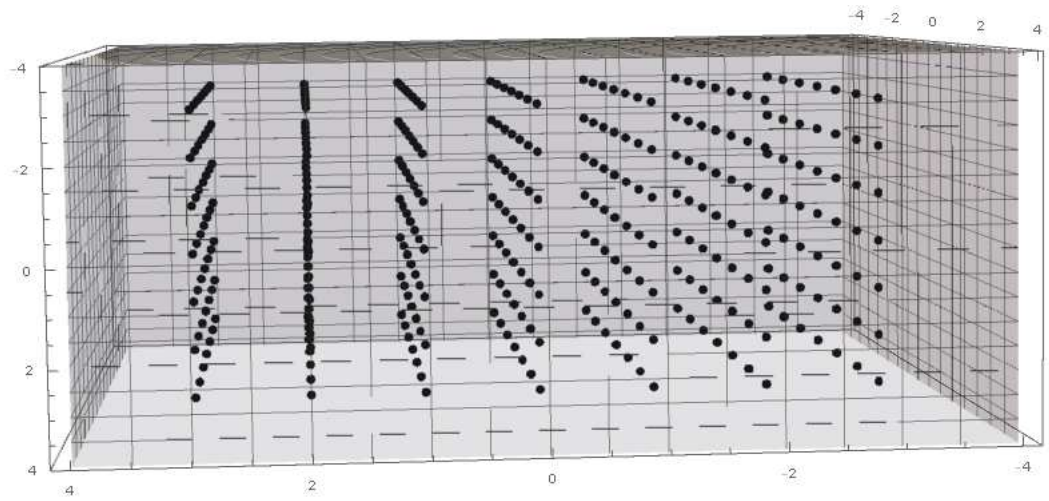


Figura 6 – Reticulado $\mathbb{Z}^3$ gerado pela base canônica restrito à uma caixa.

Observamos que, pela Proposicão 2.1.1 por exemplo, $v_1 = (899, 30, 0), v_2 = (30, 1, 0)\, e\, v_3 = (0, 0, 1)$ também compõem uma base para o reticulado $\mathbb{Z}^3$.

2.1.1 Matriz de Gram

A matriz de Gram de um reticulado, introduzida a seguir, fornece algumas informações sobre um reticulado, tais como os ângulos e as normas dos vetores da base. Seu determinante caracteriza o volume de uma região fundamental, definida a seguir.

Definição 2.1.3. *Dado um reticulado Λ gerado por uma matriz B, chama-se* ***matriz de Gram****, a matriz G obtida por*

$$G = B^T \cdot B.$$

Observamos que da definição acima temos que se considerarmos $G = [g_{ij}]$, cada entrada da matriz é dada por $g_{ij} = \langle b_i, b_j \rangle$ e estes produtos internos, como já mencionado, fornecem informações sobre a norma dos vetores da base escolhida para o reticulado e seus respectivos ângulos.

Definição 2.1.4. *Dado um reticulado Λ, com matriz geradora B, o determinante do reticulado Λ é definido como*

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

Com esta definição de determinante de reticulado, e com a caracterização entre bases de um mesmo reticulado, podemos observar que o determinante de um reticulado é invariante à mudança de base. De fato, Considerando B e B' duas matrizes geradoras, com bases distintas, para um reticulado, e admitindo que $B = B' \cdot U$ com U unimodular $m \times m$ temos que $det\,(G) = det\left(B^T \cdot B\right) = det\left(U^T \cdot B'^T \cdot B' \cdot U\right)$, fazendo $B'^T \cdot B' = G'$ (matriz de Gram para base B') temos que $det(G) = det(G')$, pois U é unimodular, logo $det(\Lambda) = det\Lambda(B) = det(\Lambda(B'))$.
Existe uma interpretação geométrica associada ao determinante de um reticulado, relacionada ao paralelotopo fundamental, associado à uma matriz geradora B do reticulado.

Definição 2.1.5. *Dado uma base de um reticulado $\beta = \{b_1, \ldots, b_m\}$ e sua respectiva matriz geradora B, o* ***paralelotopo fundamental*** *associado a esta base é dado por:*

$$\mathcal{P}(B) = \{\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_m b_m\},\ 0 \leqslant \alpha_j < 1, \forall\, j = 1, 2, \ldots, m\}.$$

Proposição 2.1.2. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado e T uma translação em $\mathbb{R}^n$, definida como $T(x) = x + u$, com $u \in \Lambda$. Então T é uma isometria que leva o reticulado nele mesmo.*

Demonstração. Por T ser uma translação (um movimento rígido), esta já é uma isometria. Agora tomemos $x \in \Lambda$, $x + u \in \Lambda$. De fato, se cosiderarmos uma base do reticulado sendo $\beta = \{b_1, b_2, \ldots, b_m\}$, temos que existem os inteiros $\alpha_1, \alpha_2, \ldots, \alpha_m, \theta_1, \theta_2, \ldots, \theta_m$, tal que

$$x = \sum_{i=1}^{m} \alpha_i b_i \ \ e \ \ u = \sum_{i=1}^{m} \theta_i b_i.$$

Como $x + u = \sum_{i=1}^{m} (\alpha_i + \theta_i)\, b_i$ e usando o fato que a soma de dois inteiros é um inteiro, segue então que $x + u \in \Lambda$. □

Teorema 2.1.2. *Seja Λ um reticulado em $\mathbb{R}^n$ de posto completo gerado por $\{b_1, \ldots, b_m\}$, cuja a matriz geradora é $B = [b_1\, b_2\, \ldots\, b_m]$. Então o volume do paralelotopo fundamental é*

$$V(\Lambda) = V\left(\mathcal{P}\left(B\right)\right) = \mid det\,(B) \mid = \sqrt{detG}.$$

Demonstração. Para calcularmos o volume do paralelotopo $\mathcal{P}(B)$, considerando $b_i = (b_{1i}, \ldots, b_{ni})^T$, basta integrarmos a unidade sobre esta região, ou seja,

$$V(\mathcal{P}(B)) = \int_{\mathcal{P}(B)} dx_1 \cdots dx_m.$$

Fazendo $z_i = \sum_{j=1}^{m} b_{ij}k_j$, com $0 \leqslant k_j < 1$, temos assim que o jacobiano desta transformação, é dado por $det(b_{ij})$. Note que $\mathcal{P}(B)$ é o conjunto dos pontos z_i, utilizando agora o teorema de mudança de variáveis [Elon 2015, pg.379], obtemos

$$\begin{aligned} V(\mathcal{P}(B)) &= \int_{\mathcal{P}(B)} \mid det(b_{ij}) \mid dk_1 \cdot dk_2 \cdots dk_m \\ &= \mid det(b_{ij}) \mid \int_0^1 dk_1 \cdot \int_0^1 dk_2 \cdots \int_0^1 dk_m \\ &= \mid det(b_{ij}) \mid = \mid det(B) \mid = \sqrt{det\,(B^T \cdot B)} = \sqrt{detG}. \end{aligned}$$

□

2.1.2 Região de Voronoi

Uma região fundamental $\mathcal{R}$ de um reticulado Λ de posto completo em $\mathbb{R}^n$ é um subconjunto $\mathcal{R} \subset \mathbb{R}^n$ que satisfaz as seguintes condições:

i) Para x e $y \in \Lambda$, $x \neq y$ $(x + \mathcal{R}) \cap (y + \mathcal{R}) = \varnothing$ ou esta intersecção contém apenas pontos do bordo destes conjuntos.

ii) $\bigcup_{x \in \Lambda} x + \mathcal{R} = \mathbb{R}^n$.

Dizemos então que a região $\mathcal{R}$ ladrilha o espaço $\mathbb{R}^n$ por translações dadas por vetores de λ. O paralelotopo fundamental associado a uma base de um reticulado Λ é uma região fundamental de Λ. Uma outra região fundamental de um reticulado Λ é a chamada região de Voronoi $\mathcal{V}_0$ da origem, composta por pontos do $\mathbb{R}^n$ que estão mais próximos da origem do que de qualquer outro ponto do reticulado.

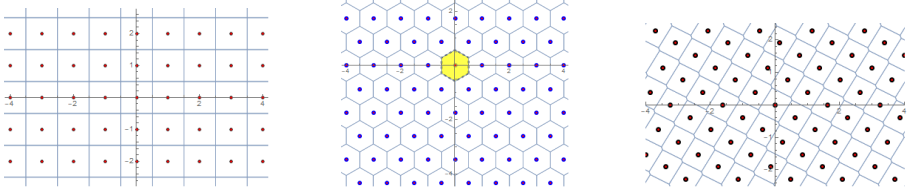
$$\mathcal{V}_0 = \{x \in \mathbb{R}^n;\ \| x \| \leqslant \| x - \lambda \|\ \forall\, \lambda \in \Lambda\}.$$

Observamos que esta região, ao contrário do paralelotpo fundamental, não depende da base do reticulado, e que

$$\mathcal{V}_\Lambda(\lambda_*) = \lambda_* + \mathcal{V}_0 = \{x \in \mathbb{R}^n; \| x - \lambda_* \| \leqslant \| x - \lambda \|\ \forall\, \lambda \in \Lambda\}$$

é a região de Voronoi associada a $\lambda_* \in \Lambda$, isto é, pontos do $\mathbb{R}^n$ que estão mais próximos de λ_* do que de outros pontos de Λ. Um ponto x do $\mathbb{R}^n$ na intersecção de duas regiões de Voronoi $\mathcal{V}_\Lambda(\lambda_1) \cap \mathcal{V}_\Lambda(\lambda_2)$ é equidistante de $\lambda_1 \, e \, \lambda_2$.
Como apontado em [Costa et al. 2017, pg. 11] um fato importante é que toda região fundamental de um reticulado de posto completo possui o mesmo volume, que é igual a $vol(B) = |det\, B|$, onde B é uma matriz geradora do reticulado. Este fato será usado na determinação das densidades de empacotamento e de cobertura de um reticulado.

Exemplo 2.1.3. *Como colocado, a região de Voronoi, diferentemente do paralelotopo, independe da base do reticulado. Abaixo estão ilustrados a regiões dos reticulados $\mathbb{Z}^2$, hexagononal, e do Exemplo 2.1.1.*



(a) Região de Voronoi do reticulado $\mathbb{Z}^2$ ladrilhando o plano.

(b) Região de Voronoi do reticulado hexagonal ladrilhando o plano.

(c) Região de Voronoi do reticulado do Exemplo2.1.1 ladrilhando o plano.

Figura 7 – Regiões de Voronoi associadas à reticulados distintos ladrilhando $\mathbb{R}^2$.

Para um reticulado com matriz geradora B e de posto completo, podemos definir o seu **volume** como sendo o volume da região de Voronoi (ou da região fundamental)

$$V(\Lambda) = V(\mathcal{V}_\Lambda(0)) = |det(B)| = \sqrt{[det(\Lambda)]}. \tag{2.1}$$

2.2 Reticulados Raízes

Alguns reticulados que são bastante explorados são os denominados reticulados raízes, que possuem alta simetria. Para mais detalhes e aplicações ver [Conway e Sloane 2013, Cap.4]. O nome também é sugestivo devido a tais reticulados estarem associados com o sistema de raízes de algumas álgebras de Lie [Jorge 2012].

Reticulado $\mathbb{Z}^n$

Chamado de reticulado cúbico, este tem por característica ser representado por todos os pontos com coordenadas inteiras do $\mathbb{R}^n$, sua matriz geradora pode ser considerada como qualquer matriz de entradas inteiras com determinante ± 1, ou seja , uma matriz

unimodular. Começar por este reticulado não é uma opção particular, pois todos os outros reticulados advém deste via uma transformação linear [Campello 2014].

Reticulado A_n

Definição 2.2.1. $A_n = \{(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} : x_1 + x_2 + \ldots + x_{n+1} = 0\}$.

Geometricamente descreve-se A_n como a intersecção do hiperplano que possui vetor normal $N = \underbrace{(1, 1, \ldots, 1)}_{n+1\, vezes}$ com $\mathbb{Z}^{n+1}$. Uma base a se considerar para A_n com a associada matriz geradora (que não é quadrada) e sua matriz de Gram são:

$$B = \begin{bmatrix} -1 & 0 & \ldots & 0 \\ 1 & -1 & \ldots & 0 \\ 0 & 1 & \ldots & \vdots \\ \vdots & \vdots & \ddots & -1 \\ 0 & 0 & \ldots & 1 \end{bmatrix} , G = \begin{bmatrix} 2 & -1 & 0 & \ldots & 0 & 0 \\ -1 & 2 & -1 & \ldots & 0 & 0 \\ 0 & -1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & -1 & 2 \end{bmatrix}.$$

Reticulado D_n

Definição 2.2.2. $D_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : x_1 + x_2 + \ldots + x_n = 0\,(mod\,2)\}$.

D_n pode ser descrito como os pontos com coordenadas inteiras de $\mathbb{R}^n$ cuja a soma é par, ou ainda tomando o reticulado $\mathbb{Z}^n$ e colorindo a partir da origem, todos os pontos alternadamente por duas cores distintas, conforme a soma das coordenadas seja par ou ímpar. Todos os pontos da primeira cor escolhida para o (0, 0, ..., 0) será o reticulado D_n. Por causa disto este é também chamado de reticulado *checkerboard*, olhando como um tabuleiro de xadrez. Uma matriz geradora para D_n e sua matriz de Gram associada são dadas por:

$$B = \begin{bmatrix} -1 & 1 & 0 & \ldots & 0 & 0 \\ -1 & -1 & 1 & \ldots & 0 & 0 \\ 0 & 0 & -1 & \ldots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & -1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & -1 \end{bmatrix} , G = \begin{bmatrix} 2 & 0 & -1 & \ldots & 0 & 0 \\ 0 & 2 & -1 & \ldots & 0 & 0 \\ -1 & -1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 2 & -1 \\ 0 & 0 & 0 & \ldots & -1 & 2 \end{bmatrix}.$$

Reticulados E_6, E_7 e E_8

Começamos definindo o reticulado E_8, que foi estudado inicialmente por T. Gosset, e então em algumas referências este aparece como reticulado de Gosset [Costa et al. 2017].

Definição 2.2.3. $E_8 = \{(x_1, x_2, \ldots, x_8) \in \mathbb{R}^8 : todo\, x_i \in \mathbb{Z}\ ou\ todo\, x_i \in \mathbb{Z} + \frac{1}{2}\, e\, x_1 + x_2 + \ldots + x_8 = 0\, (mod\, 2)$.

E_8 também chamado de reticulado diamante da dimensão oito, pode ter sua matriz geradora escrita como:

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -\frac{1}{2} \end{bmatrix}.$$

A matriz de Gram associada (que vamos utilizar no capítulo 3 para outra aplicação) é dada por

$$G_{E_8} = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & -1 & 2 \end{bmatrix}.$$

Com estas matrizes, geradora e de Gram expostas, visualizamos que:

i. $\langle e_i, e_i \rangle = 2$;

ii. $\langle e_i, e_{i+1} \rangle = -1\ \forall\ i \in \{1, 2, \ldots, 7\}$;

iii. $\langle e_i, e_j \rangle = 0$ se $\mid i - j \mid \geqslant 2$ e $i, j \neq 5, 8$;

iv. $\langle e_5, e_8 \rangle = -1$.

Os reticulados E_6 e E_7 são caracterizados como subreticulados de E_8.

Definição 2.2.4. $E_6 = \{(x_1, x_2, \ldots, x_8) \in\ E_8 : x_1 = x_2 = x_3\}$.

Definição 2.2.5. $E_7 = \{(x_1, x_2, \ldots, x_8) \in\ E_8 : x_1 + x_2 + \ldots + x_8 = 0\}$.

2.3 Reticulados Equivalentes

Definição 2.3.1. *Dada uma métrica d em $\mathbb{R}^n$, uma isometria é uma aplicação $\sigma_d : \mathbb{R}^n \to \mathbb{R}^n$, satisfazendo $d(x, y) = d(\sigma_d(x), \sigma_d(y))$, para quaisquer x e y em $\mathbb{R}^n$.*

Definição 2.3.2. *Dois reticulados Λ_1 e Λ_2 são equivalentes em uma métrica d, se existirem uma isometria σ_d e um valor real λ, tais que $\Lambda_2 = (\lambda\sigma_d)(\Lambda_1)$. Neste caso λ é chamado de fator de dilatação e quando $\lambda = 1$ os reticulados Λ_1 e Λ_2 serão ditos congruentes.*

Neste trabalho estamos considerando a métrica euclidiana em $\mathbb{R}^n$. O que a definição 2.3.2 nos diz é que dado dois reticulados Λ_1 e Λ_2 com as respectivas matrizes geradoras B_1 e B_2, se os reticulados forem equivalentes na métrica euclidiana usual, teremos que $B_2 = \lambda \cdot O \cdot B_1 \cdot U$, onde O é uma matriz ortogonal e U uma matriz unimodular.

Exemplo 2.3.1. *Os reticulados gerados pelas matrizes B_1 e B_2 a seguir são equivalentes*

$$B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad , B_2 = \begin{bmatrix} 1 & 0 \\ 3 & 5 \end{bmatrix}.$$

Neste caso temos a seguinte reescrita de B_2:

$$\begin{bmatrix} 1 & 0 \\ 3 & 5 \end{bmatrix} = \sqrt{5} \cdot \underbrace{\begin{bmatrix} \frac{2\sqrt{5}}{5} & \frac{-\sqrt{5}}{5} \\ \frac{\sqrt{5}}{5} & \frac{2\sqrt{5}}{5} \end{bmatrix}}_{O} \cdot \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{B_1} \cdot \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}}_{U}.$$

Observe que O é uma matriz de rotação, sendo assim interpretamos o reticulado gerado por B_2 como sendo o reticulado $\mathbb{Z}^2$ rotacionado $\theta = \arcsin\left(\frac{\sqrt{5}}{5}\right)$ e expandido pelo fator $\sqrt{5}$.

Reticulados equivalentes podem ser relacionados por rotações, reflexões e ainda serem dilatados ou contraídos. Dois reticulados equivalentes não diferem nos parâmetros de densidades (empacotamento e cobertura), entretanto o parâmetro volume é múltiplicado por $(\lambda^n)^2$ e o raio de empacotamento e de cobertura serão multiplicados pelo fator de dilatação, estes parâmentros serão definidos posteriormente neste trabalho. É possível ainda considerar a equivalência de reticulados em dimensões distintas. Um exemplo é o reticulado hexagonal em $\mathbb{R}^2$ que é equivalente ao reticulado A_2 em $\mathbb{R}^3$.

2.3.1 Sub-reticulados e Reticulados Quocientes

Definição 2.3.3. *Sejam Λ um reticulado e $\Lambda' \subseteq \Lambda$. Dizemos que Λ' é sub-reticulado de Λ se Λ' é um reticulado.*

[2] Dada uma matriz quadrada A de ordem n, o $det(\lambda \cdot A) = \lambda^n \cdot det(A)$.

Reticulados têm estrutura de grupo comutativo e admitem quociente por sub-reticulados. O quociente de dois reticulados é um grupo finito, que pode ser representado por um conjunto finito de pontos (classes laterais). A quantidade de pontos obtidos ao quocientar dois reticulados é dada por $\frac{V(\Lambda')}{V(\Lambda)}$. Para efeito ilustrativo, consideremos o reticulado $\mathbb{Z}^2$ e o reticulado $3\mathbb{Z}^2$ ($\mathbb{Z}^2$ dilatado pelo fator três), então teremos nove (resultado de $\frac{V(3\mathbb{Z}^2)}{V(\mathbb{Z}^2)} = \frac{3^2}{1}$) no reticulado quociente, como segue a Figura 8.

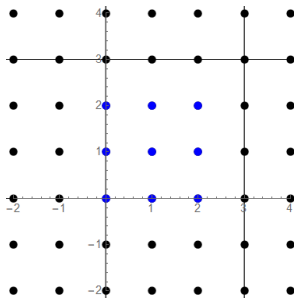


Figura 8 – Pontos do reticulado quociente $\frac{\mathbb{Z}^2}{3\mathbb{Z}^2}$ identificados no quadrado $[0,3)^2$.

Observação 2.3.1. *Na Figura 8, os pontos espelhados nas fronteiras paralelas se encontram na mesma classe de equivalência.*

2.4 Empacotamento, Cobertura e Kissing Number de reticulados

Definição 2.4.1. *A norma mínima (λ) de um reticulado Λ é a menor norma dentre os elementos não nulos de Λ, isto é:*

$$\lambda = \min_{0 \neq x \in \Lambda} \| x \| .$$

Quando pensamos em um reticulado sob a definição de subgrupo aditivo, é possível garantir a existência de um vetor de norma mínima [Costa et al. 2017, Pg.12]. Diante disto, usando a definição de bola fechada, podemos assumir que o maior raio que estas bolas podem assumir quando centradas em pontos de um reticulado de tal forma que seus interiores tenham intersecção vazia é $\rho = \frac{\lambda}{2}$. A teoria de emapacotamento de esferas é bastante estudada e com diversas aplicações, neste trabalho nos limitamos a definições e resultados iniciais já conhecidos.

Definição 2.4.2. *O **raio de empacotamento** do reticulado Λ é definido como sendo*

$$\rho = \frac{\lambda}{2}.$$

Definição 2.4.3. *Quando os centros das bolas de raio ρ forem todos pontos do reticulado Λ (translada-se a bola de raio ρ por pontos de Λ), estaremos diante de um empacotamento de reticulado.*

Definição 2.4.4. *Considere $volB^n(\rho)$ como o volume da bola n-dimensional de raio ρ centrada na origem. A densidade de empacotamento de um reticulado $\Lambda(B)$ de posto completo e matriz geradora B é definida como:*

$$\Delta(\Lambda) = \frac{volB^n(\rho)}{V(\Lambda)} = \frac{volB^n(\rho)}{|det(B)|}. \tag{2.2}$$

Para $n = 2$ e $n = 3$ temos fórmulas bem usuais, entretanto quando tomamos dimensões maiores do que as citadas, a fórmula para o volume das hiperesferas não é tão conhecida. Utilizamos a relação $volB^n(\rho) = \rho^n volB^n(1)$, onde o volume da bola unitária é explicitado por [Costa et al. 2017, Pg.13]:

$$volB^n(1) = \begin{cases} \dfrac{\pi^{\frac{n}{2}}}{(\frac{n}{2})!}, & se\ n\ for\ par, e \\ \\ \dfrac{2^n \cdot \pi^{\frac{n-1}{2}} \cdot (\frac{n-1}{2})!}{n!}, & se\ n\ for\ ímpar. \end{cases} \tag{2.3}$$

Como alternativa utiliza-se também a densidade de centro definida como

$$\delta(\Lambda) = \frac{\Delta(\Lambda)}{volB^n(1)} = \frac{\rho^n}{V(\Lambda)}, \tag{2.4}$$

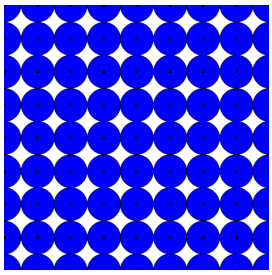
a qual permite comparar densidades de reticulados na mesma dimensão.

Exemplo 2.4.1. *Na Figura 9 indentificamos o empacotamento dos reticulados, detalhando a norma mínima (λ), o raio de empacotamento (ρ) e a densidade do empacotamento (Δ) de cada um deles. É possível observar ainda que, a proporção que a reunião das bolas de empacotamento do reticulado hexagonal ocupa do plano é maior que as dos demais. Notamos ainda que no hexagonal, temos 6 bolas de empacotamento tangentes a cada bola, enquanto que o reticulado $\mathbb{Z}^2$ possui quatro e do reticulado do Exemplo 2.1.1 apenas duas. Para a dimensão dois as únicas configurações para quantidade de bolas tangentes são estas.*

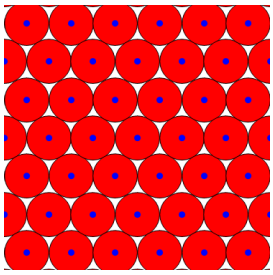
O reticulado hexagonal apresenta a maior densidade de empacotamento (até mesmo sobre estruturas não reticuladas), este resultado é apresentado e demonstrado em [Zong 1999, pg.8] como **teorema de Lagrange e Thue**. No espaço $\mathbb{R}^3$ ilustramos o empacotamentos do reticulado $\mathbb{Z}^3$ do Exemplo 2.1.2. Temos seu empacotamento representado na Figura 10.

Exemplo 2.4.2. *Outros reticulados que são importantes em dimensão três, são o reticulado de corpo centrado (BCC) e de face centrada (FCC), com as respectivas bases [Costa et al. 2017], $\beta_1 = \{(2,0,0);(0,2,0);(1,1,1)\}$, $\beta_2 = \{(2,0,0);(1,1,0);(1,0,1)\}$ e densidades.*

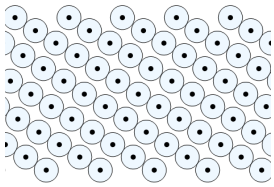
Observamos que o FCC, como definido acima, é o reticulado D_3, e este representa o reticulado mais denso no $\mathbb{R}^3$. Podemos visualizar estes dois reticulados e seus respectivos empacotamentos na seguinte figura.



(a) Empacotamento do reticulado $\mathbb{Z}^2$, com $\lambda = 1; \rho = 1/2; \Delta = 0.785$



(b) Empacotamento do reticulado hexagonal, com $\lambda = 1; \rho = 1/2; \Delta = 0.906$.



(c) Empacotamento do reticulado do Exemplo 2.1.1, com $\lambda = \sqrt{5-2\sqrt{5}}$; $\rho = \dfrac{\sqrt{5-2\sqrt{5}}}{2}$; $\Delta = 0.670$.

Figura 9 – Os empacotamentos de reticulados com suas respectivas densidades Δ.

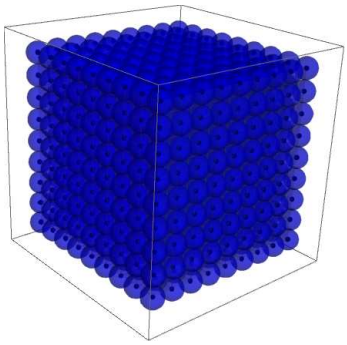
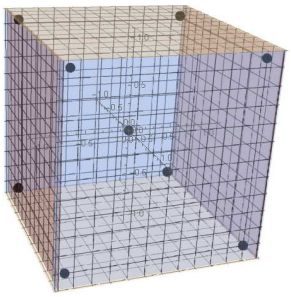


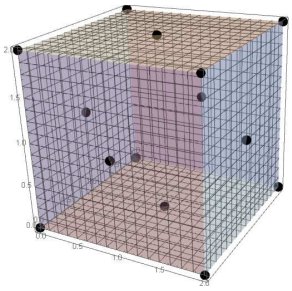
Figura 10 – Empacotamento do reticulado $\mathbb{Z}^3$ com $\lambda = 1$; $\rho = \dfrac{1}{2}$ e $\Delta = 0.523$.

Em 1611 com o advento da expansão marítima, os navios em alto mar portavam canhões e sua munição eram esferas sólidas que ficavam no convés (parte superior) do navio. Um explorador inglês chamado Sir Walter Raleigh, colocou um problema sobre qual seria **a melhor forma de empilhar balas de canhão** (existem variantes do problema). O problema despertou interesse do matemático Thomas Harriot, que também era inglês. Harriot por sua vez trocou cartas com Johannes Kepler. Kepler respondeu a Harriot, propondo a ele uma conjectura que o empilhamento com maior densidade, poderia ser feito análogo ao empilhamento de laranjas em uma feira. Este problema ficou conhecido como **conjectura de Kepler** (para mais detalhes ver [Hales 2005] e [Souza 2019]).

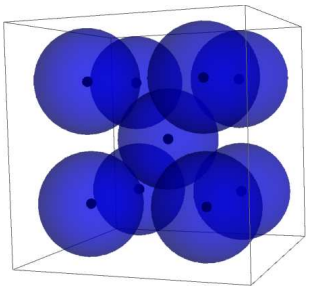
Esta conjectura mostrou-se correta. Em 1831 Carl F. Gauss demonstrou que a conjectura era válida para empacotamentos reticulados. Entretanto, foi necessário passar 400 anos para mostrar que a conjectura original estava correta. Thomas Hales [Hales 2005] apresentou uma prova que leva ao final resultados computacionais, mas já é universalmente aceita.



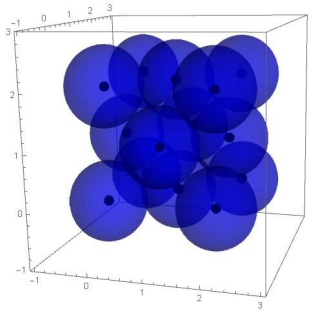
(a) Reticulado cúbico de corpo centrado



(b) Reticulado cúbico de face centrada



(c) Empacotamento esférico do reticulado de corpo centrado, com $\lambda = \sqrt{3}$, $\rho = \dfrac{\sqrt{3}}{2}$, $\Delta = 0.680$



(d) Empacotamento esférico do reticulado de face centrada, com $\lambda = \sqrt{2}$, $\rho = \dfrac{\sqrt{2}}{2}$, $\Delta = 0.740$

Figura 11 – Reticulados BCC e FCC com seus respectivos empacotamentos

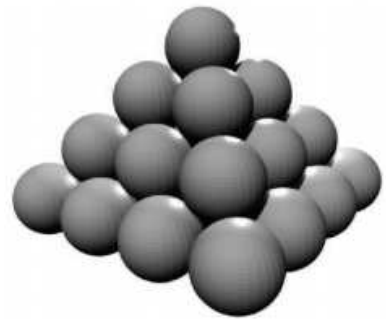


Figura 12 – Emplilhamento de bolas de canhão

2.4.1 Kissing Number

Empacotar esferas em um espaço de dimensão qualquer é um amplo tópico de pesquisa que se relaciona com o tema a seguir. Durante um jogo de bilhar, quando uma bola toca outra utiliza-se o termo em inglês *kiss* e daí vem o termo *kissing number*. Dada uma dimensão n saber quantas esferas ou hiperesferas de de raio p podem tocar simultaneamente uma esfera de raio r o que caracteriza o problema do ***"kissing number"***.

Denotamos por $\tau(n, p, r)$ o número máximo de esferas que tocam. Na teoria de reticulados estamos interessados em saber este *kissing number* para $p = r$, e neste caso

denotamos somente por $\tau(n)$. Em dimensão dois estamos procurando número máximo de esferas (discos) que tocam outra de mesmo raio. A resolução deste problema equivale a distribuir os pontos de tangência sobre o bordo de um disco, notamos que tomando ao mesmo tempo dois discos tangentes à esfera, ao unirmos o centro destes discos mutuamente tangentes e unirmos cada centro ao disco em questão forma-se um triangulo equilátero de lado $2r$, o mesmo possui ângulo interno igual a $\frac{\pi}{3}$ então conseguimos um total de $\frac{2\pi}{\frac{\pi}{3}} = 6$ pontos sobre o disco, logo $\tau(2) = 6$.

Em dimensão três o problema fica mais sofisticado e desafiador, este também é conhecido como o *problema da* 13^a *esfera*. Como bem descrito em [Souza 2019], Newton já discutia tal problema em dimensão três com David Gregory em maio de 1694. Enquanto Newton desconfiava que seriam doze, Gregory acreditava que a resposta seria treze o número máximo de esferas. A prova de que Newton estava certo só foi feita em 1953 por Schűtte e Van Der Waerden [Musin 2003]. Em dimensão três, a melhor configuração para $\tau(3)$ é dispor os centros das esferas sobre os vértices de um icosaedro, com uma esfera fixa e de mesmo raio como ilustrado na Figura 13.

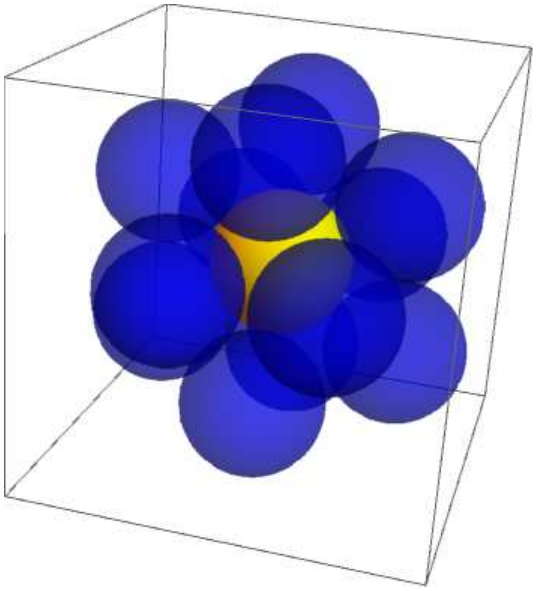


Figura 13 – Kissing number em dimensão 3.

2.5 O problema de cobertura

Estudar a melhor forma de empacotar esferas de tal forma que elas no máximo se tangenciam é o que busca a teoria de empacotamentos. O problema dual relacionado a este é o de cobrir todo o espaço por esferas sobrepostas que tenham o menor raio possível. Neste trabalho estamos sempre considerando os centro destas esferas como pontos de um reticulado. Assim podemos definir este menor raio se segue.

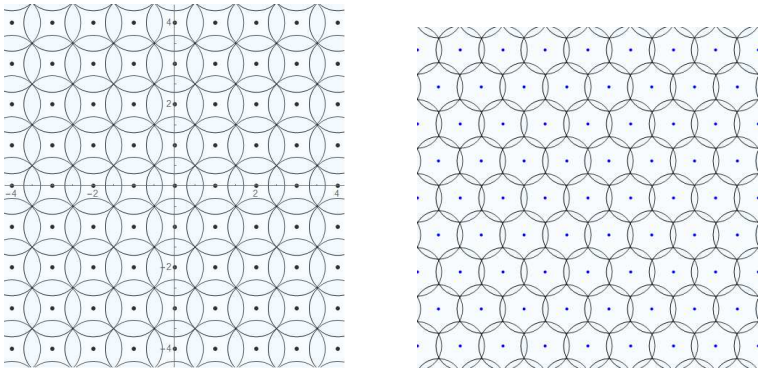
Definição 2.5.1. *Dado um reticulado* Λ*, define-se o seu* ***raio de cobertura*** *como sendo o menor valor* μ *tal que as translações da bola* $B^n[\mu]$ *por pontos de* Λ *cobrem todo o* $\mathbb{R}^n$*, ou seja:*

$$\bigcup_{x\in\Lambda}(B^n(\mu)+x)=\mathbb{R}^n.$$

Assim como medimos qual a melhor densidade de empacotamento de reticulados, no caso de coberturas também estamos interessados em medir a densidade de cobertura. Repare que enquanto a densidade de empacotamento é um real positivo menor do que ou igual a um, a densidade de cobertura será um real positivo maior do que ou igual a um. Enquanto nos empacontamento de esferas buscamos a maior densidade, no problema de cobertura buscamos a cobertura com menor densidade, e tal cobertura é calculada por

$$\Theta=\frac{volB^n(\mu)}{V(\Lambda)}=\frac{\mu^n volB^n(1)}{[det(\Lambda)]^{\frac{1}{2}}}. \tag{2.5}$$

O reticulado BCC apresenta a melhor densidade cobertura em $\mathbb{R}^3$, enquanto o reticulado FCC possui a melhor densidade de empacotamento, até mesmo entre estruturas não reticuladas. Para mais detalhes ver [Souza 2019].



(a) Cobertura de $\mathbb{R}^2$ pelo reticulado $\mathbb{Z}^2$.

(b) Cobertura de $\mathbb{R}^2$ pelo reticulado hexagonal.

Figura 14 – Coberturas de $\mathbb{R}^2$

2.6 Decodificação em reticulados

Existem problemas envolvendo reticulados que se tornam difíceis com o aumento da dimensão dos mesmos. Para mais detalhes e aplicações (com exemplos práticos) ver [Gouvêa 2011]. Vejamos os dois problemas clássicos envolvendo reticulados.

- Problema 1 (**SVP**). O problema do vetor mais curto (*shortest vector problem*). Consiste em encontrar um vetor $v \neq 0 \in \Lambda$, tal que a norma (comprimento) seja a menor possível. Isto é encontrar $v \in \Lambda$ que minimiza a norma euclidiana $\| v \|$.
- Problema 2 (**CVP**). O problema do vetor mais próximo (*closest vector problem*). Dado um vetor $z \in \mathbb{R}^n$, encontrar $v \in \Lambda$ tal que a norma $\| z - v \|$ seja minimizada.

Ambos os problemas são considerados difíceis do ponto de vista da teoria da complexidade computacional, sendo que o CVP é comprovadamente NP-difícil [Micciancio e Goldwasser 2012]. O problema de decodificação condicionado à reticulados resume-se no problema CVP. Em [Conway e Sloane 2013] são apresentados algoritmos para este problema considerando os reticulados raízes.

Quando estamos à procura da densidade de empacotamento de um reticulado, automaticamente precisamos do volume da região fundamental (simples de se calcular se tivermos a matriz geradora) e o vetor de norma mínima, que agora sabemos que se trata de um problema do tipo SVP. Apresentaremos um método na seção 2.8 que oferece, pela matriz de Gram, a menor norma ao quadrado de um vetor do reticulado, mas que também tem uma complexidade computacional grande para dimensões altas.

2.7 Alguns Reticulados Introduzidos No Século XX

2.7.1 O Reticulado de Coxeter-Tood K_{12}

Coxeter e Tood em 1954 descreveram o reticulado K_{12}, um reticulado em $\mathbb{R}^{12}$ que apresentava os seguintes parâmetros $det(G) = 729$, portanto o determinante da matriz geradora é vinte e sete, o vetor com menor norma apresenta $\lambda = 2$. Portanto, $\rho = 1$, a densidade de empacotamento é $\Delta = \dfrac{\pi^6}{19440} \cong 0.04945$, este reticulado possui *kissing number* $\tau = 756$. Apresentamos a seguir uma matriz geradora deste reticulado.

$$G_{K_{12}} = \begin{bmatrix}
2 & 0 & 0 & 0 & 1 & \frac{-1}{2} & -1 & 0 & 0 & 0 & \frac{-1}{2} & \frac{-1}{2} \\
0 & 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \sqrt{3} & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{-\sqrt{3}}{2} \\
0 & 2 & 0 & 1 & 0 & \frac{-1}{2} & 0 & -1 & 0 & \frac{-1}{2} & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & \frac{-\sqrt{3}}{2} & 0 & \sqrt{3} & 0 & \frac{\sqrt{3}}{2} & 0 & 0 \\
0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & \frac{-1}{2} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{3} & 0 & \frac{\sqrt{3}}{2} & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & \frac{-1}{2} & 0 & \frac{-1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{2} & 0 & \frac{\sqrt{3}}{2} \\
0 & 0 & 0 & \frac{-1}{2} & \frac{-1}{2} & 0 & 0 & 0 & 0 & \frac{-1}{2} & \frac{-1}{2} & 0 \\
0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 & \frac{-\sqrt{3}}{2} & \sqrt{3} & 0 \\
0 & 0 & 0 & \frac{-1}{2} & \frac{-1}{2} & 1 & 0 & 0 & 0 & 1 & 1 & \frac{-1}{2} \\
0 & 0 & 0 & \frac{-\sqrt{3}}{2} & \frac{-\sqrt{3}}{2} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2}
\end{bmatrix}.$$

2.7.2 O Reticulado de Barnes-Wall Λ_{16}

Este é um reticulado em dimensão dezesseis, foi construído em 1959 por E.S. Barnes e G.E. Wall, tal reticulado apresenta $det(\Lambda_{16}) = 256$, fazendo com que sua matriz geradora possua determinante igual a dezesseis, seu vetor de menor norma possui $\lambda = 2$, consequentemente o raio de empacotamento $\rho = 1$. Desta forma sua densidade de empacotamento fica determinada e vale $\Delta = \dfrac{\pi^8}{645.120} \cong 0.0147$, seu *kissing number* vale $\tau = 4320$. Uma matriz geradora para este reticulada pode ser exibida da seguinte forma:

$$G_{\Lambda_{16}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

2.7.3 O Reticulado de Leech Λ_{24}

Em 1965 Leech apresentou um reticulado em dimensão vinte e quatro que, em sua homenagem, é chamado de reticulado de Leech. Seus parâmetros são $det(\Lambda_{24}) = 1$, $\lambda = 2$, raio de empacotamento $\rho = 1$, fazendo com que sua densidade de empacotamento $\Delta = \frac{\pi^{12}}{12!} \cong 0.0019$ e seu *kissing number* $\tau = 196.560$. Uma matriz geradora para o reticulado de Leech é apresentada a seguir. Este é o reticulado mais denso em sua dimensão. Foi provado também em 2017 (detalhes em [Souza 2019]) que este tem o melhor empacotamento nesta dimensão mesmo entre constelações que não são reticulados.

$$G_{\Lambda_{24}} = \frac{1}{\sqrt{2}} \begin{bmatrix}
4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \frac{-3}{2} \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & \frac{1}{2} \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}
\end{bmatrix}.$$

Tabela de reticulados de melhor densidade e seus outros parâmetros

A tabela abaixo (adaptada de [Costa et al. 2017]) mostra reticulados que são provados serem os mais densos nas dimensões de 1 a 8 e dimensão 24 e o mais denso conhecido em dimensão 16. Outros parâmetros são exibidos para os mesmos reticulados.

Dimensão	Reticulado	Densidade de empacotamento	Densidade de cobertura	*Kissing Number*
1	$\mathbb{Z}$	1	1	2
2	A_2	0.9069	1.2092	6
3	A_3 D_3	0.7450	1.4635	12
4	D_4	0.6169	1.7655	24
5	D_5	0.4653	2.1243	40
6	E_6	0.3730	2.4648	72
7	E_7	0.2953	2.900	126
8	E_8	0.2537	3.2013	240
16	Λ_{16}	0.0147	15.3109	4320
24	Λ_{24}	0.0019	7.9035	196560

Tabela 1 – Reticulados mais densos e seus parâmetros

2.8 Redução de Minkowski

Dada uma base B de um reticulado, calcular o vetor de norma mínima nem sempre é simples (como já vimos é o problema SVP). Por exemplo, o reticulado hexagonal gerado por B, $x = B \cdot u$ com $u \in \mathbb{Z}^2$. Para ponto do reticulado hexagonal, logo temos

$$B = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}; \quad x = \begin{bmatrix} u_1 + \frac{u_2}{2} \\ \frac{\sqrt{3}u_2}{2} \end{bmatrix} \Longrightarrow \| x \|^2 = u_1^2 + u_1 u_2 + u_2^2.$$

Como u_1 e u_2 são inteiros temos que esta norma é mínima quando assumir o valor 1, que é o que ocorre se considerarmos $(u_1, u_2) = \{(\pm, 0), (0, \pm 1), \pm(-1, 1)\}$, como já sabemos. Observamos o reticulado hexagonal possui *kissing number* seis, que é justamente a quantidade de vetores de norma mínima que A_2 possui. Se considerarmos $H = BU$ uma outra matriz geradora para o reticulado hexagonal por exemplo, com $U = \{\{50, 9\}, \{11, 2\}\}$ chegaremos a uma expressão

$$\| x \|^2 = 3031u_1^2 + 1335u_1 u_2 + 147u_2^2.$$

Assim, para alguém que apenas conhecesse esta matriz geradora, associada a uma base "ruim", e não soubesse que este era o reticulado hexagonal iria ficar bem mais difícil determinar um vetor de norma mínima.

Um método a se considerar é a redução de Minkowski, que gera uma base (reduzida de Minkowski). Com a matriz de Gram satisfazendo algumas propriedades este método garante que o primeiro elemento desta matriz é justamente o quadrado da norma do vetor mais curto do reticulado. Existem algoritmos como o apresentado em [Strapasson 2007], para trasformar uma base dada numa "base Minkowiski reduzida", mas eles são computacionalmente "caros".

Definição 2.8.1. *[Costa et al. 2017, Pg.32] Uma base* $\{b_1, b_2, \ldots, b_n\}$ *de um reticulado* Λ *é dita uma base* ***Minkowski reduzida*** *se:*

- *(i)* b_1 *é o vetor mais curto em* Λ*;*

- *(ii) Para todo* $i = 1, 2, \ldots, n-1$, b_{i+1}*é um vetor mais curto em* Λ *tal que* $\{b_1, b_2, \ldots, b_i, b_{i+1}\}$ *pode ser estendido à uma base de* Λ*.*

A matriz de Gram $G = [b_{ij}]$, onde $b_{ij} = \langle b_i, b_j \rangle$, associada a uma base de Minkowski satisfaz várias propriedades ([Conway e Sloane 2013], [Costa et al. 2017]). Listamos três delas aqui que serão utilizadas no próximo capítulo:

P1) $0 \leqslant b_{11} \leqslant b_{22} \ldots \leqslant b_{nn}$;

P2) $2 \mid b_{ij} \mid \leqslant b_{ii}$, $(i < j)$

P3) $2 \mid b_{ij} \pm b_{ik} \pm b_{jk} \mid \leqslant b_{ii} + b_{jj}$, $(i < j < k)$;

Mostra-se que, em dimensões 2 e 3 as condições (P1 e P2) e (P1, P2 e P3) também são suficientes respectivamente, para garantir que a base do reticulado seja de Minkowiski. Uma condição que caracteriza base de Mikowiski em dimensão 4 é apresentada em [Conway e Sloane 2013] e para dimensões maiores que quatro, as condições sobre a matriz de Gram que caracterizam uma base de Minkowiski vão se tornando complexas.

3 Reticulados Construídos a partir de Códigos q-ários

Neste capítulo estudamos reticulados que são obtidos de códigos lineares q-ários através da chamada construção A. Esta construção associa de forma natural um código linear em $\mathbb{Z}_q^n$ a um reticulado contido em $\mathbb{Z}^n$. Introduzimos inicialmente conceitos e propriedades que complementam o que foi exposto nos capítulos anteriores e analisamos então parâmetros de alguns reticulados obtidos via a construção A, particularmente a densidade de empacotamento. As principais referências utilizadas neste capítulo foram [Lavor et al. 2006, vol.21], [Costa et al. 2017] e [Zong 1999].

3.1 Construção A

A ideia da Construção A é obter um reticulado "replicando"um código contido na "caixa" $\mathbb{Z}_q^n$, para todo $\mathbb{Z}^n$. Consideramos então a redução módulo q, $\Psi(x)$ é feita componente a componente:

$$\Psi : \mathbb{Z}^n \to \mathbb{Z}_q^n.$$

Tomando $S \subset \mathbb{Z}_q^n$, podemos considerar a pré-imagem $\Psi^{-1}(S)$(pontos de $\mathbb{Z}^n$ que são levados aos pontos de S via Ψ).
Observamos que Ψ é sobrejetora e também é um **homomorfismo** de grupos, pois é válida a relação $\Psi(x+y) = \Psi(x) + \Psi(y)$ e $\Psi(-x) = -\Psi(x)$. A proposição a seguir é que garante a construção A.

Proposição 3.1.1. *[Costa et al. 2017, Pg.39]Dado um subconjunto $S \subset \mathbb{Z}_q^n$ então $\Psi^{-1}(S)$ é um reticulado em $\mathbb{R}^n$ se, e somente se, S é um código linear em $\mathbb{Z}_q^n$.*

Definição 3.1.1. *[Costa et al. 2017, Pg. 40] Seja C um código linear em $\mathbb{Z}_q^n$ com $q \geqslant 2$ e o homomorfismo Ψ dado por*

$$\begin{aligned} \Psi :& \mathbb{Z}^n \to \mathbb{Z}_q^n \\ (x_1, x_2, \ldots, x_n) &\mapsto (x_1 (mod\, q), x_2 (mod\, q), \ldots, x_n (mod\, q)), \end{aligned}$$

Então o reticulado $\Lambda_C = \Psi^{-1}(C)$ é dito obtido via construção A ou ainda reticulado q-ário associado ao código C.

Observação 3.1.1. *Como $q\mathbb{Z}^n = \Psi^{-1}(\boldsymbol{0})$ temos então $q\mathbb{Z}^n \subset \Lambda(C) \subset \mathbb{Z}^n$, o que implica que $\Lambda(C)$ é um reticulado de posto completo que contém $q\mathbb{Z}^n$ como subreticulado.*

Proposição 3.1.2. *[Costa et al. 2017] (a)Se Λ_C é um reticulado q-ário associado ao código linear $C \subseteq \mathbb{Z}_q^n$, então $\left|\frac{\Lambda_C}{q\mathbb{Z}^n}\right| = \frac{q^n}{V(\Lambda_C)} = |C|$, onde $|C|$ denota a quantidade de palavras do código C.*
(b) Qualquer reticulado de posto completo com coordenadas inteiras ($\Lambda \subseteq \mathbb{Z}^n$) é q-ário para $q = V(\Lambda)$.

Demonstração. (a) Observamos que o quociente de reticulados $\frac{\Lambda(C)}{q\mathbb{Z}^n}$ é isomorfo ao grupo $C \subset \mathbb{Z}_q^n$ e que as classes laterais deste quociente estão representadas pelos pontos do reticulado $\Lambda(C)$ que estão contidos no cubo n-dimensional $[0, q)^n$, isto é $\left|\frac{\Lambda_C}{q\mathbb{Z}^n}\right| = \frac{q^n}{V(\Lambda_C)} = |C|$.

(b) Dado um reticulado de posto completo, $\Lambda \subset \mathbb{Z}^n$, seja B uma matriz geradora deste, que portanto terá entradas inteiras, e $q = V(\Lambda) = |det(B)|$. Dado qz, $z \in \mathbb{Z}^n$ queremos ver se existe x com coordenadas inteiras tal que $Bx = qz$. Considerando então a matriz dos cofatores $cofat(B)$, temos $x = B^{-1}qz = \frac{cofat(B)^T}{det(B)} \cdot qz = \frac{cofat(B)^T}{\pm q} \cdot qz = \pm cofat(B)^T z \in \mathbb{Z}^n$. Tomando agora o código $C = \Psi(\Lambda) \subset \mathbb{Z}_q^n$ onde Ψ é a redução módulo q em cada coordenada, temos então que $\Lambda = \Lambda_C$. □

Observação 3.1.2. *Sabemos que se q for um número primo, o código C possuirá a estrutura de subespaço vetorial de dimensão $k \leqslant n$, então $\mathbb{Z}_q^n = \mathbb{F}_q^n$, este código possui então q^k palavras código. Segue da proposição 3.1.2 que $V(\Lambda_C) = q^{(n-k)}$.*

Exemplo 3.1.1. *Seja $C = \langle(1, 3)\rangle \subset \mathbb{Z}_5^2$. Pela simplicidade do código podemos listar cada uma de suas palavras que o formam, a saber $C = \{(0, 0), (1, 3), (2, 1), (3, 4), (4, 2)\}$. Como $|C| = 5$ e $q = 5$ o qual é primo e temos a dimensão $k = 1$, segue que $V(\Lambda_C) = 5^{(2-1)} = 5$, daí temos que $\left|\frac{\Lambda_C}{5\mathbb{Z}^n}\right| = \frac{5^2}{5} = 5$. o reticulado associado a C está representado na Figura 15 .*

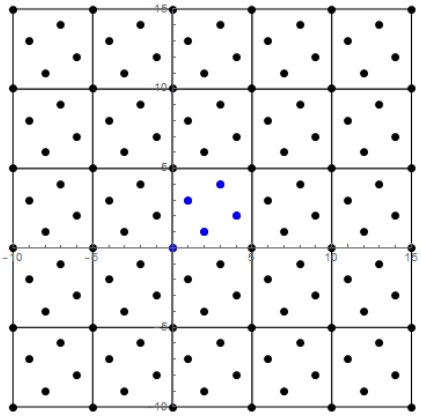


Figura 15 – Reticulado associado ao código C e pontos de $\frac{\Lambda_C}{5\mathbb{Z}^n}$ em azul.

3.1.1 Matriz geradora de um reticulado obtido via construção A

Exibir a matriz geradora de um reticulado associado à um código nem sempre é direto e simples, sob certas condições esta matriz é calculada computando a forma normal de Hermite da matriz dos vetores geradores do reticulado acrescido dos vetores canônicos de $\mathbb{R}^n$ multiplicados pelo escalar q, para mais detalhes ver [Costa et al. 2017]. Porém se o código for linear e sua matriz geradora estiver na forma padrão (ou sistemática), a proposição seguinte nos dá uma estrutra da matriz geradora do reticulado.

Proposição 3.1.3. *[Costa et al. 2017, pg.43], [Jorge 2012] Seja C um código linear, com a matriz geradora na forma sistemática. Então a matriz geradora de Λ_C é dado por:*

$$B = \begin{bmatrix} I_{k\times k} & 0_{k\times(n-k)} \\ A_{(n-k)\times k} & qI_{(n-k)\times(n-k)} \end{bmatrix}.$$

Demonstração. Temos que mostrar que $\Lambda_C = \Lambda(B)$. Então devemos mostrar as duas inclusões e por hipótese a matriz geradora do código é dada por:

$$G = \begin{bmatrix} I_{k\times k} \\ A_{(n-k)\times k} \end{bmatrix}.$$

Observamos que $\Lambda(B) \subset \Lambda_C$ pois todos os vetores coluna de B módulo q pertencem ao código e portanto estes vetores e o conjunto das combinações lineares inteiras destes, que é $\Lambda(B)$, está contida em Λ_C.
Pela definição da Construção A o reticulado Λ_C é gerado pelos vetores colunas, $v_1, \ldots, v_k$ de G mais os vetores da forma qe_i, onde $\{e_1, \ldots e_n\}$ é a base canônica de $\mathbb{R}^n$. Mas os vetores $qe_1, qe_2, \ldots, qe_k$ podem ser escritos como combinação linear dos demais. Para $i \leqslant j \leqslant k$ temos que $qe_j = qv_j - a_{1j}e_1 - a_{2j}e_2 - \ldots - a_{(n-k)j}e_k$, portanto o conjunto $\{v_1, \ldots, v_k, qe_{j+1}, \ldots, qe_n\}$ é uma base para Λ_C, ou seja $\Lambda_C = \Lambda(B)$.

□

Reticulados associados a códigos via Contrução A também podem ser considerados realizando uma pertubação na pré imagem da Definição 3.1.1, ou seja, $\Lambda_C = a \cdot \Psi^{-1}(C)$ com $a > 0$. Na construção do reticulado E_8 veremos a necessidade de usar $a \neq 1$.

3.2 Densidade de reticulados obtidos via Construção A

Vimos a ligação entre códigos e reticulados pela construção A, e agora estaremos interessados na análise da densidade de empacotamento destes reticulados. Um reticulado com alta densidade de empacotamento nos diz muito sobre a eficiência do código em questão.
No cálculo de densidade de empacotamento, um dado que é computacionalmente difícil de

se obter para um reticulado geral, particularmente em dimensões mais altas é a norma mínima do reticulado (SVP), como já comentamos no Capítulo 2.
Para reticulados obtidos via contrução A, esta norma mínima λ pode ser obtida a partir dos elementos do código q-ário ($C \neq 0$), que é um conjunto finito de pontos:

$$\lambda = d_{\min}(\Lambda_C) = \min\{d(C), q\} \tag{3.1}$$

onde $d(C)$ é a distância euclidiana mínima de pontos do código C até a origem [Costa et al. 2017, pg.50].
No caso especial em que C é um código linear binário, temos ainda um resultado mais específico:

Proposição 3.2.1. *[Lavor et al. 2006, vol.21, pg.40] Sejam C um código linear binário com parâmetros $[n, k, d]$ e $\Lambda_C = \Psi^{-1}(C)$. Então,*

i. Se $d < 4$, a norma mínima é $\sqrt{d}$ e os vetores de norma mínima de Λ_C são os vetores v, com $v \in C$ de peso menor ou igual a 4, bem como os vetores v', obtidos trocando-se alguns dos $1's$ por $-1's$.

ii. Se $d = 4$, a norma mínima é 2 e todos os vetores listados no item anterior são de norma mínima e possuem a única entrada não-nula igual a ± 2.

iii. Se $d > 4$, a norma mínima é 2 e os vetores de norma mínima são os vetores cuja única entrada não nula é ± 2.

3.2.1 Densidade de reticulados Λ_C em dimensão 2

Já foi dito anteriormente que a melhor densidade de empacotamento em dimensão dois é a do reticulado hexagonal ($\Delta \approx 0.9069$). Buscamos investigar se há a possibilidade de se obter um dado reticulado (através de um código) cuja a densidade se aproxima do hexagonal. Já foi mostrado que a densidade de empacotamento de $\mathbb{Z}^2$ é $\Delta \approx 0.7854$.

Exemplo 3.2.1. *Considere C o código linear em $\mathbb{Z}_2^2$ onde $C = \langle(1, 1)\rangle$. Uma maneira intuitiva de interpretar o reticulado Λ_C é pensar em todos os pontos de $\mathbb{Z}^2$ cuja a soma das coordenadas é par. A matriz deste reticulado dada pela construção A considerando $k = 1$, $n = 2$ e $q = 2$ é dada por:*

$$\Lambda_A(C) = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}.$$

Observamos que para este reticulado temos $\lambda = \sqrt{2}$ *conforme a Proposição 3.2.1, portanto o raio de empacotamento será* $\rho = \frac{2}{2}$. *O reticulado e seu empacotamento* $\Lambda_A(C)$*é mostrado na Figura 16, calculando sua densidade de empacotamento encontramos a mesma que a do reticulado* $\mathbb{Z}^2$, *a saber* $\Delta = \frac{\left(\frac{\sqrt{2}}{2}\right)^2 \cdot \pi}{2} = \frac{\pi}{4}$.

Ao atentarmos para a matriz de Λ_C *vemos que este reticulado é equivalente ao reticulado*

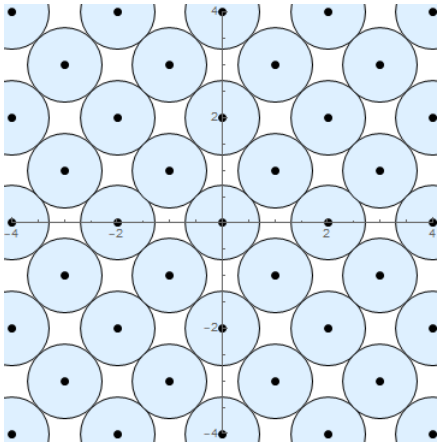


Figura 16 – Reticulado obdtido via construção A do código C e seu respectivo empacotamento.

$\mathbb{Z}^2$, *sendo uma dilatação pelo fator* $\sqrt{2}$ *e uma rotação de 45, ou seja*

$$\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} = \sqrt{2} \begin{bmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Veremos a seguir que não conseguimos densidade maior para reticulados em $\mathbb{R}^2$ construídos a partir de códigos binários.

Proposição 3.2.2. *O reticulado associado à um código* C *binário (alfabeto sendo* $\mathbb{Z}_2$*) não alcança uma densidade melhor que a de* $\mathbb{Z}^2$.

Demonstração. Os únicos códigos binários lineares em $\mathbb{Z}_2^2$ são $C_1 = \{(0,0)\}$, $C_2 = \{(0,0),(1,0)\}$,$C_3 = \{(0,0),(0,1)\}$,$C_4 = \{(0,0),(1,1)\}$ e $C_5 = \mathbb{Z}_2^2$. Para os reticulados associados a estes códigos temos respectivamente as matrizes geradoras

$$B_1 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix},\ B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\ B_3 = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix},\ B_4 = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \text{ e } B_5 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

As normas mínimas são $\lambda_1 = 2$,$\lambda_2 = 1$,$\lambda_3 = 1$,$\lambda_4 = \sqrt{2}$ e $\lambda_5 = 1$, conforme a Proposição 3.2.1. Portanto calculando as normas das desidades $\Delta_i = \frac{\pi \cdot \left(\frac{\lambda_i}{2}\right)^2}{det\, B_i}$, obtetmos $\Delta_1 = \frac{\pi}{4}$,$\Delta_2 = \frac{\pi}{8}$,$\Delta_3 = \frac{\pi}{8}$,$\Delta_4 = \frac{\pi}{4}$ e $\Delta_5 = \frac{\pi}{4}$.

Isto nos instiga a procurar novos alfabetos para encontrar códigos sobre estes alfabetos, de forma que o reticulado associado a estes códigos ultrapassem a densidade de $\mathbb{Z}^2$, como discutiremos posteriormente. □

3.2.2 Densidade de reticulados em dimensão 3

O reticulado gerado pelo código $C = \langle (1,0,0); (0,1,0) \rangle$

Sendo $C = \langle (1,0,0); (0,1,0) \rangle \subset \mathbb{Z}_2^3$, por se tratar de um código linear temos que sua matriz geradora é

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

Portanto, ao construir o reticulado associado à este código obtemos (via contrução A, $\Psi^{-1}(C)$) o seguinte reticulado

$$\Lambda_A(C) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

A norma mínima deste reticulado é $\lambda = 1$, portanto $\rho = \dfrac{1}{2}$, segue que

$$\Delta\left(\Lambda_A(C)\right) = \frac{\pi}{12},$$

que é uma densidade menor que a do reticulado cúbico ($\mathbb{Z}^3$).

3.2.2.1 Código cuja construção do reticulado alcança a densidade de empacotamento do BCC

Considere agora o código $C = \langle (1,1,1) \rangle \subset \mathbb{Z}_2^3$. O qual possui matriz geradora M sendo,

$$M = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

O reticulado gerado por este código linear via Construção A tem como matriz geradora

$$\Lambda_A(C) = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

Temos que para o reticulado $\Lambda_A(C)$ a menor norma é $\lambda = \sqrt{3}$ e raio de empacotamento do mesmo será $\rho = \dfrac{\sqrt{3}}{2}$, portanto segue que

$$\Delta\left(\Lambda_A(C)\right) = \frac{\sqrt{3}\cdot\pi}{8} \cong 0.680.$$

Observamos que este reticulado é, de fato o BCC.

3.2.2.2 Código cuja a construção do reticulado alcança a densidade do FCC

Considere $C = \langle(1,0,1);(0,1,1)\rangle \subset \mathbb{Z}_2^3$, note que a matriz geradora do código é dada por

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

A Construçã A deste código nos fornece a matriz geradora do reticulado associada ao código C, a saber

$$\Lambda_A(C) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix}.$$

Para este reticulado, temos $\lambda = \sqrt{2}$ logo $\rho = \frac{\sqrt{2}}{2}$, estes parâmetros nos fornece

$$\Delta = \frac{\sqrt{2}\cdot\pi}{6} \cong 0.740.$$

Novamente, observamos que este reticulado é o FCC.

Construção do reticulado D_n por códigos binários

Para construir inicialmente D_3, considere o código $C = \{(x_1,x_2,x_3) \in \mathbb{Z}_2^3; \sum_{i=1}^{3} x_i = 0\} = \{(1,1,0);(1,0,1);(0,1,1);(0,0,0)\}$. Como estamos interessados em realizar a Construção A do código C, observemos que uma matriz geradora do código é

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

Esta matriz está na forma padrão, então pela Proposição 3.1.3, a matriz geradora do reticulado Λ_C é

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix}.$$

Pela Proposição 3.2.1 tem-se $\lambda = \sqrt{2}$, tendo densidade de empacotamento igual a $\frac{\sqrt{2}\cdot\pi}{6}$.

Analogamente podemos construir D_4 (prosseguindo até D_n), estendendo a base de D_3, sendo a seguinte matriz geradora de D_4

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

Novamente pela Proposição 3.2.1 temos $\lambda = \sqrt{2}$, como determinante é também dois, a densidade de empacotamento para este reticulado será igual a $\frac{\pi^2}{16}$.

3.2.3 Reticulado obtido pelo código do robô com alfabeto em $\mathbb{Z}_4$

Vamos considerar agora o robô com os movimentos N, S, L e O, codidficados em $\mathbb{Z}_4$. Usando novamente a tripla repetição, então um código $C \subset \mathbb{Z}_4^3$ possui matriz geradora é

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Sendo assim, a matriz geradora de Λ_C associada é

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 4 & 0 \\ 1 & 0 & 4 \end{bmatrix}.$$

O $det\, B = 16$ e pela Equação 3.1 temos $\lambda = \sqrt{3}$, portanto, $\Delta(\Lambda_C) = \frac{\sqrt{3} \cdot \pi}{32} \approx 0.1700$, que é inferior a densidade de D_3.

3.2.4 Densidade de reticulados em dimensão 6

Densidade do reticulado construído a partir do código tripla repetição

O código de tripla repetição apresentado no Exemplo 1.3.2 possui matriz geradora sendo

$$C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix},$$

C está na forma sistemática, portanto a matriz geradora do reticulado é, segundo a Proposição: 3.1.3

$$\Lambda_A(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

Temos $det(\Lambda_A(C)) = 16$, observe que $\lambda = \sqrt{3}$ pela equação 3.1, logo $\rho = \dfrac{\sqrt{3}}{2}$, fazendo com que

$$\Delta(\Lambda_C) = \frac{\frac{\pi^3}{3!} \cdot \left(\frac{\sqrt{3}}{2}\right)^6}{16} \cong 0.1362 < \Delta(E_6).$$

3.2.5 Reticulado associado ao código do robô com 8 movimentos

O código apresentado no exemplo 1.3.3, possui matriz geradora

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

Como a matriz geradora esta na forma padrão, podemos exibir a matriz do reticulado associado, sendo esta

$$\Lambda_A(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 2 \end{bmatrix}.$$

Os parâmetros do reticulado gerado são $det\left(\Lambda_A(C)\right) = 8$, $\lambda = \sqrt{3}$, portanto $\rho = \dfrac{\sqrt{3}}{2}$ e desta forma a densidade de empacotamento será

$$\Delta = \frac{\frac{\pi^3}{3!} \cdot \left(\frac{\sqrt{3}}{2}\right)^6}{8} \cong 0.272.$$

Esta densidade está entre a densidade do reticulado cúbico $\mathbb{Z}^6$ e do E_6, que é mais denso nesta dimensão.

3.2.6 Densidade de reticulados em dimensão 8

Para a construção do reticulado E_8, vamos utilizar o código de Hamming estendido ao comprimento oito. Este código com mais detalhes pode ser visto em [Firer 2007] e [Lavor et al. 2006, vol.21]. O código de Hamming estendido pega o código de Hamming $\mathcal{H}_3$ e acrescenta uma coordenada de x_8, definindo um novo código da seguinte forma

$$\tilde{C} = \{(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) : (x_1, \ldots, x_7) \in \mathcal{H}_3 \; e \; x_8 = \sum_{i=1}^{7} x_i (mod\, 2)\}.$$

Lembrando que $x_5 = x_2 + x_3 + x_4$, $x_6 = x_1 + x_3 + x_4$ e $x_7 = x_1 + x_2 + x_4$. Para continuar a construção o seguinte lema tem bastante relevância.

Lema 3.2.1. *Dados x e y em $\mathbb{Z}_2^n$, sendo $\omega(x)$ o peso*[1] *de x e $\langle x, y\rangle$ o produto interno de x e y em $\mathbb{R}^n$, temos*

$$\omega(x + y) = \omega(x) + \omega(y) - 2\langle x, y\rangle .$$

Desta forma temos que $\tilde{C}$ tem os parâmetros $[8, 4, 4]$, e em algumas referências este código é denotado também por $\tilde{\mathcal{H}}_3$. Vale ressaltar que $\tilde{\mathcal{H}}_3$ possui 2^4 palavras código, dentre estas temos a palavra nula, a de peso oito e outras quatorze, sendo sete de peso quatro com $x_8 = 0$ e sete de peso quatro com $x_8 = 1$. Então pelo lema anterior, temos que se $\omega(b_i + b_j) = 8$ $\langle b_i, b_j\rangle = 0$, em contrapartida se $\omega(b_i + b_j) = 4$ temos $\langle b_i, b_j\rangle = 2$. Estamos interessados nos sete vetores cuja $x_8 = 1$, a saber

$$\begin{aligned}
b_1 &= (1, 0, 0, 1, 1, 0, 0, 1)\\
b_2 &= (0, 1, 0, 1, 0, 0, 1, 1)\\
b_3 &= (1, 0, 0, 0, 0, 1, 1, 1)\\
b_4 &= (1, 0, 0, 0, 0, 1, 1, 1)\\
b_5 &= (0, 1, 0, 1, 0, 1, 0, 1)\\
b_6 &= (0, 0, 1, 0, 1, 1, 0, 1)\\
b_7 &= (1, 1, 1, 0, 0, 0, 0, 1).
\end{aligned}$$

A construção A deste reticulado faz uma pertubação na pré imagem, utilizando o fator $\frac{1}{\sqrt{2}}$, isto se deve ao fato de utilizarmos os vetores acima para construir uma matriz de Gram do reticulado $\Lambda_A(\tilde{C})$ igual a do E_8, apresentada neste trabalho. Apresentamos a seguir a base procurada, definindo

$$f_i = \frac{1}{\sqrt{2}} \cdot b_i.$$

[1] Dado $x \in \mathbb{K}^n$, defini-se o peso de x sendo $\omega(x) =\mid \{i; x_i \neq 0\}$ ou $\omega(x) = d_H(x, 0)$.

Desta forma, temos as relações $\langle f_i, f_j \rangle = 1$ se $i \neq j$ e $\langle f_i, f_i \rangle = 2$ com $0 < i \leqslant 7$. Porém apenas esta mudança não satisfaz as condições da matriz de Gramm, definimos agora $e_i = f_{i+1} - f_i$ e $e_1 = f_1$, gerando

$$\begin{aligned}
e_1 = f_1 &= \frac{1}{\sqrt{2}}(1,0,0,1,1,0,0,1) \\
e_2 = f_2 - f_1 &= \frac{1}{\sqrt{2}}(-1,1,0,-1,0,0,1,0) \\
e_3 = f_3 - f_2 &= \frac{1}{\sqrt{2}}(0,-1,1,1,-1,0,0,0) \\
e_4 = f_4 - f_3 &= \frac{1}{\sqrt{2}}(1,0,-1,-1,0,1,0,0) \\
e_5 = f_5 - f_4 &= \frac{1}{\sqrt{2}}(-1,1,0,1,0,0,-1,0) \\
e_6 = f_6 - f_5 &= \frac{1}{\sqrt{2}}(0,-1,1,-1,1,0,0,0) \\
e_7 = f_7 - f_6 &= \frac{1}{\sqrt{2}}(1,1,0,0,-1,-1,0,0).
\end{aligned}$$

Com a base exposta acima, obtemos a seguinte relação

$$\begin{aligned}
\langle e_i, e_{i+1} \rangle &= -1 \ \ \forall\, i = \{1,2,\ldots,6\} \\
\langle e_i, e_j \rangle &= 0, \ \ \mid i-j \mid \geqslant 2.
\end{aligned}$$

Para completar a base precisamos definir e_8, nos atentando que $\langle e_8, e_8 \rangle = 2$, $\langle e_8, e_5 \rangle = -1$ e $\langle e_8, e_i \rangle = 0 \ \forall\, i \neq \{5,8\}$. A resoluçao do sistema linear nos fornece $e_8 = \frac{1}{\sqrt{2}}(0,-1,-1,0,0,-1,1,0)$, observamos que e_8 é um ponto do reticulado $\Lambda_A(\tilde{\mathcal{H}}_3)$, e como as matrizes de Gram entre E_8 e $\Lambda_A(\tilde{\mathcal{H}}_3$ coincidem (para a base construída) segue que $E_8 = \Lambda_A(\tilde{\mathcal{H}}_3)$.

Para o reticulado $\Lambda_A(\tilde{\mathcal{H}}_3)$, temos que o $det(\Lambda_A(\tilde{\mathcal{H}}_3) = -1$, $\lambda = \sqrt{2}$ e $\rho = \frac{\sqrt{2}}{2}$, fazendo assim com que $\Delta = \frac{\pi^4}{384} \cong 0.2537$, esta é a melhor densidade de empacotamento em dimensão oito.

3.2.6.1 Reticulado associado ao código Hamming 7-4

Como um contraste vamos analisar a seguir a construção A gerada pelo código de Hamming $[7,4,3]$, clássico em $\mathbb{R}^7$. Este código tem matriz geradora na forma sistemática,

portanto pela Proposição3.1.3 a matriz do reticulado associado é

$$\Lambda_{C\mathcal{H}_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 2 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 2 \end{bmatrix}$$

. Os parâmetros deste reticulado é $det\,\Lambda_{C\mathcal{H}_3} = 8$, e pela Proposição 3.2.1 temos $\lambda = \sqrt{3}$ e $\rho = \dfrac{\sqrt{3}}{2}$, portanto $\Delta(\Lambda_{\mathcal{H}_3}) = \dfrac{(\frac{\sqrt{3}}{2})^7 \cdot 2^7 \cdot \pi^3 \cdot 3!}{7! \cdot 8} \approx 0.2158$ que é uma boa densidade comparada à melhor densidade para reticulados nesta dimensão, que é a do E_7 (0.2953).

3.3 Reticulados q-ários cuja densidade se aproxima da maior conhecida

Esta seção destina-se a mostrar um processo de se obter um código q-ário cujo reticulado associado pela construção A possua densidade próxima da de um reiculado conhecido . Nossa abordagem, que é feita em dimensão dois, pode ser estendida para dimensões maiores. Vamos encontrar um código C tal que Λ_C tenha uma densidade próxima do reticulado hexagonal. A ideia aqui é fazer com que este reticulado a ser construído esteja contido no reticulado $\mathbb{Z}^2$ e então verificar a qual código q-ário este é associado. Já vimos (Proposição 3.2.2) que utilizando alfabeto $\mathbb{Z}_2$ não encontramos códigos C tais que a densidade de Λ_C seja maior do que a de $\mathbb{Z}^2$, isto nos leva busca de alfabetos maiores. Consideremos a matriz do reticulado hexagonal e uma aproximação desta:

$$\begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}, \; B = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & 0.86605 \end{bmatrix}.$$

Com esta aproximação $\dfrac{\sqrt{3}}{2} = 0.86605$, vamos dilatar o reticulado gerado por B utilizando o fator 100 com os elementos arredondados para o inteiro mais próximo:

$$\begin{bmatrix} 100 & 50 \\ 0 & 87 \end{bmatrix},$$

e a matriz de Gram associada:

$$G = \begin{bmatrix} 10000 & 5000 \\ 5000 & 10069 \end{bmatrix}.$$

Considerando $b_1 = (100, 0)$ e $b_2 = (50, 87)$, pela matriz de Gram observamos que $\| b_1 \|^2 = 10000$ e $\| b_2 \|^2 = 10069$, portanto $\| b_1 \| < \| b_2 \|$, ainda temos que $2 \mid 5000 \mid = 10000 = b_{11}$ o que faz esta base ser Minkowiski reduzida, daí teremos a norma mínima $\lambda = 100$. O reticulado possui determinante igual a 8700 e é de posto completo com entradas inteiras. Portanto pelo item b da proposição 3.1.2 temos que o presente reticulado é $q-$ário para $q = 8700$, e pode ser dado como Λ_C, onde o código $C \subset \mathbb{Z}_q^2$ é dado por $C = \langle (100, 0), (50, 87) \rangle$. A seguir apresentamos sua densidade de empacotamento e a ilustração do empacotamento

$$\Delta = \frac{\pi \cdot 50^2}{8700} \approx 0.9028.$$

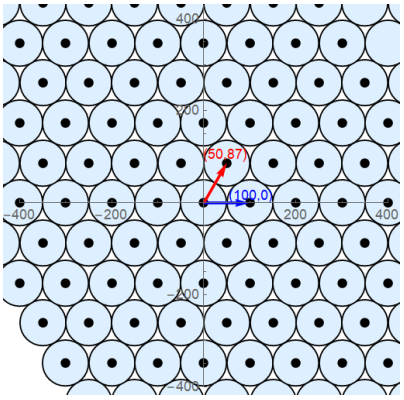


Figura 17 – Reticulado assocciado ao código em $\mathbb{Z}_{8700}^2$ $C = \langle (100, 0); (50, 87) \rangle$.

Neste processo foi feito um truncamento sobre a metade de raiz quadrada de três, uma dilatação pelo fator 100 na matriz aproximada do reticulado hexagonal e a aproximação pela matriz inteira mais próxima. Mas podemos avaliar, também, este processo com outros fatores, tomando o mesmo valor de aproximação para a metade de raiz quadrada de três. Analisamos a seguir, como pode variar a densidade obtida, se considerarmos diferentes fatores para a dilatação e os respectivos arredondamentos considerando os fatores 20,40, 60, 80, 100 (feito no exemplo acima), 120, 140, 160 e 180, gerando as respectivas matrizes geradoras

$$G_{20} = \begin{bmatrix} 20 & 10 \\ 0 & 17 \end{bmatrix} \quad G_{40} = \begin{bmatrix} 40 & 20 \\ 0 & 35 \end{bmatrix} \quad G_{60} = \begin{bmatrix} 60 & 30 \\ 0 & 52 \end{bmatrix} \quad G_{80} = \begin{bmatrix} 80 & 40 \\ 0 & 69 \end{bmatrix}$$

$$G_{120} = \begin{bmatrix} 120 & 6 \\ 0 & 104 \end{bmatrix} \quad G_{140} = \begin{bmatrix} 140 & 70 \\ 0 & 121 \end{bmatrix} \quad G_{160} = \begin{bmatrix} 160 & 80 \\ 0 & 139 \end{bmatrix}$$

$$G_{180} = \begin{bmatrix} 180 & 90 \\ 0 & 156 \end{bmatrix}.$$

Das matrizes apresentadas acima, somente G_{20}, G_{80} e G_{140} não satisfazem as condições para serem uma base Minkowski reduzida, entretanto em dimensão dois, o algoritmo que torna a base em uma Minkowski reduzida é simples (ver [Strapasson 2007]). A tabela a seguir mostra os resultados encontrados. Nota-se que uma dilatação pelo fator 60 já nos retorna um reticulado aproximado, com melhor densidade do que o dilatado pelo fator 100, enquanto neste utilizamos um código com o alfabeto $\mathbb{Z}_{8700}$, naquele consideramos o código sobre o alfabeto $\mathbb{Z}_{3120}$.

Fator de dilatação	Matriz geradora	Vetor de norma mínima	Densidade (Δ)
20	G_{20}	$\sqrt{389}$	0.8986
40	G_{40}	40	0.8976
60	G_{60}	60	0.9062
80	G_{80}	$\sqrt{6361}$	0.9051
100	G_{100}	100	0.9028
120	G_{120}	120	0.9062
140	G_{140}	$\sqrt{19541}$	0.9060
160	G_{160}	160	0.9041
180	G_{180}	160	0.9062

Tabela 2 – Densidade de empacotamento dos reticulados q-ários obtidos por dilatações aproximadas do reticulado hexagonal

Naturalmente, os diferentes valores ocorrem em função de uma maior ou menor aproximação inteira da matriz que é múltipla da matriz B. Lembrando que reticulados equivalentes (que incluem os múltiplos) tem a mesma densidade de empacotamento, para um fator maior ou igual a 10^6 teremos para os múltiplos", a densidade do reticulado gerado por B cujo o valor (0.906874) coincide com a densidade do hexagonal $\left(\frac{\pi\sqrt{3}}{6}\right)$ até a quarta casa.

Como comentamos, o apresentado pode ser estendido a dimensões maiores, lembrando que possivelmente haverá um alto custo computacional (devido a base de Minkowiski, etc) mas ilustra que podemos obter reticulados densos via Construção A de códigos q-ários. Por outro lado, há que se considerar que códigos em alfabetos muito grandes não são de muito interesse em aplicações.

3.4 Considerações Finais

Nesta dissertação resumimos inicialmente conceitos relacionados a códigos e reticulados (Capítulos 1 e 2) e abordamos no Capítulo 3 a Costrução A de reticulados a partir de códigos q-ários. O foco neste capítulo foi a análise da densidade de alguns destes reticulados. Perspectivas futuras de prosseguimento deste trabalho inicial, incluem um estudo mais detalhado de densidade de empacotamento destes reticulados bem como de outros parâmetros tais como densidade de cobertura e *kissing number*. Podem ainda ser analisados os casos de densidade de empacotamento e cobertura para reticulados obtidos da Construção A utilizando outras métricas, como a métrica de Lee e do máximo.

Uma outra proposta, é trabalhar com temas correlatos em construções de reticulados a partir de diferentes estruturas algébricas, omo reticulados ideiais a partir de corpos quadráticos e reticulados contruídos via teoria algébrica dos números [Flores 2000], [Jorge et al. 2015], [Bayer-Fluckiger 1999], [Bayer-Fluckiger 2002] e [Jorge, Ferrari e Costa 2011]

Referências

BAYER-FLUCKIGER, E. Lattices and number fields. *Contemp. Math.*, p. 69–84, 1999. Citado na página 64.

_____. *Ideal Lattices, proceedings of the conference Number Theory and Diophantine Geometry,(Zurich, 1999)*. [S.l.]: Cambridge Univ. Press, 2002. Citado na página 64.

BOLDRINI, J. L.; COSTA, S. I.; FIGUEREDO, V.; WETZLER, H. G. *Álgebra linear*. [S.l.]: Harper & Row, 1980. Citado na página 15.

CAMPELLO, A. Reticulados, projeções e aplicações à teoria da informação. *IMECC-UNICAMP*, 2014. Citado na página 35.

CASSEL, J. W. S. *An introduction to the geometry of numbers*. [S.l.]: Springer Science & Business Media, 2012. Citado na página 31.

CONWAY, J. H.; SLOANE, N. J. A. *Sphere packings, lattices and groups*. [S.l.]: Springer Science & Business Media, 2013. v. 290. Citado 5 vezes nas páginas 15, 29, 34, 44 e 49.

COSTA, S. I.; OGGIER, F.; CAMPELLO, A.; BELFIORE, J.-C.; VITERBO, E. *Lattices Applied to Coding for Reliable and Secure Communications*. [S.l.]: Springer, 2017. Citado 14 vezes nas páginas 15, 25, 29, 30, 34, 35, 38, 39, 48, 49, 50, 51, 52 e 53.

COVER, T. M.; THOMAS, J. A. *Elements of information theory*. [S.l.]: John Wiley & Sons, 2012. Citado na página 18.

ELON, L. L. *Curso de Analise vol. 2*. [S.l.]: Projeto Euclides IMPA,11.ed., 2015. Citado 2 vezes nas páginas 30 e 33.

FIRER, M. Códigos corretores de erros-notas de aula. *IMECC-UNICAMP*, 2007. Citado na página 59.

FLORES, A. L. Reticulados em corpos abelianos. *Tese de Doutorado-Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação*, 2000. Citado na página 64.

GOUVÊA, D. D. S. Um estudo sobre o problema do vetor mais próximo nos reticulados raízes zn, an e dn= algoritmos e simulações numéricas. *Dissertação–Universidade Estadual de Campinas,Instituto de Matemática, Estatística e Computação Científica*, 2011. Citado na página 44.

HALES, T. C. A proof of the kepler conjecture. *Annals of mathematics*, JSTOR, v. 162, n. 3, p. 1065–1185, 2005. Citado na página 40.

HAMMING, R. W. *Coding and Information Theory*. [S.l.]: Englewood Cliffs, NJ: Prentice Hall, 1986. Citado na página 15.

HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. [S.l.]: Instituto de Matematica Pura e Aplicada, 2008. Citado na página 15.

JORGE, G. C. Reticulados q-ários e algébricos. *IMECC-UNICAMP*, 2012. Citado 2 vezes nas páginas 34 e 52.

JORGE, G. C.; ANDRADE, A. A. de; COSTA, S. I.; STRAPASSON, J. E. Algebraic constructions of densest lattices. *Journal of Algebra*, Elsevier, v. 429, p. 218–235, 2015. Citado na página 64.

JORGE, G. C.; FERRARI, A. J.; COSTA, S. I. R. Rotated dn-lattices. *arXiv preprint arXiv:1111.3787*, 2011. Citado na página 64.

LAVOR, C. C.; ALVES, M. M. S.; SIQUEIRA, R. M. d.; COSTA, S. I. R. *Uma introdução a teoria de códigos*. [S.l.]: SBMAC, 2006, vol.21. Citado 9 vezes nas páginas 15, 20, 23, 26, 27, 29, 50, 53 e 59.

MASISI, L.; NELWAMONDO, V.; MARWALA, T. The use of entropy to measure structural diversity. In: IEEE. *2008 IEEE International Conference on Computational Cybernetics*. [S.l.], 2008. p. 41–45. Citado na página 19.

MICCIANCIO, D.; GOLDWASSER, S. *Complexity of lattice problems: a cryptographic perspective*. [S.l.]: Springer Science & Business Media, 2012. v. 671. Citado na página 44.

MUSIN, O. R. The kissing number in four dimensions. *arXiv preprint math/0309430*, 2003. Citado na página 42.

SHANNON, C. E. A mathematical theory of communication. *Bell system technical journal*, Wiley Online Library, v. 27, n. 3, p. 379–423, 1948. Citado na página 16.

SHANNON, C. E.; WEAVER, W. *The Mathematical Theory of Communication*. [S.l.]: University of Illinois Press, 1949. Citado na página 16.

SOUZA, J. G. F. d. O problema do empacotamento de esferas no espaço n-dimensional. *Dissertação–Universidade Estadual de Campinas,Instituto de Matemática, Estatística e Computação Científica*, 2019. Citado 4 vezes nas páginas 40, 42, 43 e 46.

STRAPASSON, J. E. Geometria discreta e códigos (tese de doutorado). *IMECC-UNICAMP*, 2007. Citado 2 vezes nas páginas 49 e 63.

WOLFRAM, R. *Wolfram Mathematica 11*. Citado na página 15.

ZONG, C. *Sphere packings*. [S.l.]: Springer Science & Business Media, 1999. Citado 4 vezes nas páginas 15, 29, 39 e 50.