Antonio Carlos de Andrade Campello Junior

Reticulados, Projeções e Aplicações à Teoria da Informação

Campinas

2014

Universidade Estadual de Campinas

Instituto de Matemática, Estatística
e Computação Científica

Antonio Carlos de Andrade Campello Junior

Reticulados, Projeções e Aplicações à Teoria da Informação

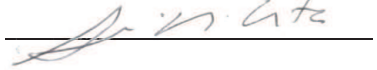
Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática Aplicada

Orientador: Sueli Irene Rodrigues Costa

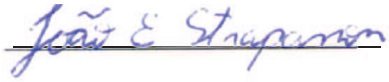
Coorientador: João Eloir Strapasson

Este exemplar corresponde à versão final da tese defendida pelo aluno Antonio Carlos de Andrade Campello Junior e orientada pela Prof. Dra. Sueli Irene Rodrigues Costa

Assinatura da Orientadora



Assinatura do Coorientador



Campinas

2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

C153r

Campello, A., 1988-
Reticulados, projeções e aplicações à teoria da informação / Antonio Carlos de Andrade Campello Junior. – Campinas, SP : [s.n.], 2014.

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

1. Teoria de reticulados. 2. Teoria da Informação. 3. Geometria discreta. I. Costa, Sueli Irene Rodrigues,1949-. II. Strapasson, João Eloir,1979-. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Lattices, projections, and applications to information theory
Palavras-chave em inglês:
Lattice theory
Information theory
Discrete geometry
Área de concentração: Matemática Aplicada
Titulação: Doutor em Matemática Aplicada
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
Jean-Claude Belfiore
Renato Portugal
Marcelo Muniz Silva Alves
Danilo Silva
Data de defesa: 24-03-2014
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 24 de março de 2014 e aprovada

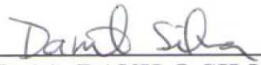
Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). JEAN-CLAUDE BELFIORE

Prof(a). Dr(a). RENATO PORTUGAL

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES



Prof(a). Dr(a). DANILO SILVA

Abstract

The contents of this thesis lie in the interface between Discrete Mathematics (particularly lattices) and Information Theory. The original contributions of this work are organized so that the first two chapters are devoted to theoretical results on q-ary and projection lattices, whereas the last ones are related to the construction of continuous source-channel codes.

In the first chapters, we exhibit results on decoding q-ary lattices and on finding tilings associated to perfect error-correcting codes in the l_p norm. Regarding projection lattices, our contributions include the study of sequences of projections of a given n-dimensional lattice converging to any k-dimensional target lattice, as well as a convergence analysis of such sequences. These new results on projections extend and improve recent works on the topic and serve as building blocks for the applications to be developed throughout the last part of the thesis.

In the last two chapters, we consider the problem of constructing mappings for the transmission of a continuous alphabet source over a Gaussian channel, when the channel dimension, n, is strictly greater than the source dimension, k. For one-dimensional sources, we exhibit codes based on curves on flat tori with performance significantly superior to the previous proposals in the literature with respect to the mean squared error achieved. For $k > 1$, we show how to apply projections of lattices to obtain codes whose mean squared error decays optimally with respect to the signal-to-noise ratio of the channel (referred to as *asymptotically optimal* codes). Through techniques from the rich theory of *dissections of polyhedra*, we present the first constructions of provenly asymptotically optimal codes for sources with dimension greater than 1.

Resumo

O conteúdo desta tese reside na interface entre Matemática Discreta (particularmente reticulados) e Teoria da Informação. Dividimos as contribuições originais do trabalho em quatro capítulos, de modo que os dois primeiros são relativos a resultados teóricos acerca de duas importantes classes de reticulados (os reticulados q-ários e os reticulados projeção), e os dois últimos referem-se a aplicações em codificação contínua fonte-canal.

Nos primeiros capítulos, exibimos resultados sobre decodificação de reticulados q-ários e sobre ladrilhamentos associados a códigos corretores de erros perfeitos na norma l_p. No que tange a reticulados projeção, nossas contribuições

incluem o estudo de sequências de projeção de um dado reticulado n-dimensional convergindo para qualquer reticulado k-dimensional fixado, $k < n$, incluindo uma análise de convergência de tais sequências. Esses novos resultados relativos a projeções estendem e aprimoram recentes trabalhos no tema e são elementos de base para as aplicações consideradas no restante da tese.

Nos dois últimos capítulos, consideramos o problema de transmitir uma fonte com alfabeto contínuo através de um canal gaussiano no caso em que a dimensão da fonte, k, é menor que a dimensão do canal, n. Para fontes unidimensionais, exibimos códigos baseados em curvas na superfície de toros planares com performance significativamente superior aos propostos anteriormente na literatura no que diz respeito ao erro quadrático médio atingido. Para $k > 1$, mostramos como aplicar projeções de reticulados para obter códigos cujo erro quadrático médio possui decaimento ótimo com respeito à relação sinal-ruído do canal (chamados de *assintoticamente ótimos*). Através de técnicas provenientes da bela teoria de *dissecção de poliedros*, apresentamos as primeiras construções de códigos assintoticamente ótimos para fontes com dimensão maior do que 1.

Sumário

A Dona Léa e Seu Antonio,
que me ensinaram a resolver os primeiros problemas

I wasn't much of a petty thief. I wanted the whole world or nothing.

- Charles Bukowski, *Post Office*

Agradecimentos

As noites mal dormidas procedentes de uma semana de trabalho árduo representam, não raras vezes, a verdade sobre a vida um estudante de doutorado. Em muitas dessas noites, o trabalho não está acompanhado de uma perspectiva real de retorno. Trabalha-se, sobretudo, pela grande vontade de trabalhar e pela busca por fazer algo novo; por investigar algum ramo inexplorado da ciência com a certeza de que o assunto buscado interessa à construção de uma nova verdade, não necessariamente disruptiva, mas pelo menos aprimorada. Porém, trabalhar incessantemente no caminho do ineditismo parece tão inquietante quanto procurar avidamente por algo que não se sabe o que é, como entrar em um processo jurídico sem saber a pauta nem as implicações de tal. E nesse delírio kafkiano, seguimos contrastando a cogitação sobre a verdade do universo com as contas a pagar. Para auxiliar com ambas as tarefas, bem como com a inevitável necessidade de esporadicamente esquecê-las, precisamos de boas pessoas. São a essas que dedico esta tese. Uma parcela delas está contemplada na lista abaixo.

Em primeiro lugar, ratifico a homenagem feita em forma de dedicatória a meus pais Antonio Carlos e Léa. Se eles não houvessem me ensinado a resolver os primeiros problemas (e a dar um jeito nos problemas insolúveis) esta tese não seria possível. Ainda em um âmbito maternal, agradeço à minha orientadora Profa. Sueli Costa por, além de orientar meus primeiros passos no meio acadêmico, mostrar-me que um pesquisador em Matemática não necessita deixar de lado a sua parte humana.

Agradeço ao meu co-orientador Prof. João Strapasson e ao Prof. Cristiano Torezzan pelos trabalhos conjuntos e pelas diversas discussões. À então colega de doutorado e agora professora Grasiele Jorge por parcerias frutíferas. Agradeço também aos membros da banca examinadora pelas sugestões muito pertinentes, que certamente ajudaram a aprimorar a versão final do trabalho.

Não é exagerado dizer que a elaboração desta tese iniciou-se em 2006, ano em que ingressei na graudação da UNICAMP, a qual considero verdadeiramente minha *alma mater*. Gostaria de agradecer a todos os professores e amigos que foram marcantes desde então. Uma ínfima lista que certamente contém omissões importantes inclui o Prof. Aurélio, Prof. Moretti, os amigos João Tiago, Seifer, Nove, Lemense, Bixo, Ju, e, é claro, minha parceira de todos os momentos, Ana.

Durante o meu estágio no AT&T Shannon Laboratory, tive a honra de discutir e colaborar com pesquisadores exepcionais, como meu supervisor Dr. Vinay Vaishampayan, o Dr. Neil Sloane e o Dr. Vaneet Aggarwal, aos quais agradeço pelas frutíferas conversas nos *bump spaces* do laboratório. Agradeço também a Igor Carboni por me prover moradia nos fins de semana e pela amizade durante o inverno gelado de Nova York.

Agradeço aos diversos companheiros de laboratório, entre eles Bruno, Marcos, Elen, Jerry, Chris, Cláudio, Prof. Marcelo Firer, Prof. Carlile Lavor, e todas as outras pessoas que tornaram este ambiente de trabalho mais divertido e interessante.

Por último, mas não menos importante, agradeço (alguns *in memoriam*) a Amy Winehouse, Muse, Cat Power, The Strokes, The Beatles e Raul Seixas, entre muitos outros, por me acompanharem durante o processo de redação final desta tese.

A pesquisa desenvolvida durante este doutorado beneficiou-se da ajuda financeira da FAPESP, através das bolsas DD 2009/18337-6, DD 2011/22044-4 e BEPE 2012/09167-2.

Introdução

Como anunciado categoricamente por Ram Zamir no título de [Zam09], reticulados estão em toda parte. Além das utilizações mais prosaicas da sua estrutura, como o empacotamento de compras na feira ou a fabricação de colmeias por abelhas, reticulados são notáveis por desempenharem um importante papel na Teoria da Informação, nome dado ao ramo do conhecimento cujo marco inicial é o artigo seminal de Claude Shannon [Sha48] que estabelece as bases teóricas para o estudo de esquemas de transmissão de informação eficientes e seguros. No contexto de transmissão eficiente, citamos particularmente o uso de reticulados em canais gaussianos [Zam09], canais com desvanecimento [BVRB96], a construção de códigos esféricos [TCV09, SC08] e a relação entre sistemas de codificação contínua fonte-canal e reticulados projeção densos [VC03, SVC09, SVC10]. Na esfera da segurança de informação, por sua vez, podemos localizar em diversos trabalhos a utilização de problemas computacionalmente intratáveis envolvendo reticulados como pressupostos de segurança para protocolos criptográficos. Alguns exemplos são as propostas de criptossistemas, os esquemas de assinatura digital, as funções *hash* e os protocolos de identificação, encontrados no livro [BBD08].

Não obstante as aplicações, questionamentos puramente teóricos associados a reticulados e empacotamentos vêm intrigando matemáticos desde o século XVI, envolvendo expoentes como Johannes Kepler, Isaac Newton, Carl Gauss, Joseph-Louis Lagrange e Hermann Minkowski. Seu escopo abrange, além das áreas já citadas, o cálculo numérico de integrais, a solução aproximada de equações diofantinas e a otimização inteira, entre outros. Além disso, a versão n-dimensional da segunda parte do 18º problema proposto por David Hilbert no Congresso Internacional de Matemática (1900) perguntando pelo empacotamento de esferas

mais denso encontra-se, em sua generalidade, em aberto.

Os temas tratados nesta tese residem na interface entre reticulados e Teoria da Informação. Uma maneira econômica, em número de palavras, de definirmos um reticulado é como um subgrupo aditivo e discreto do $\mathbb{R}^n$. Assim, um reticulado é qualquer subconjunto discreto $\Lambda \subset \mathbb{R}^n$ com a propriedade de que se $\boldsymbol{x}$ e $\boldsymbol{y}$ pertencem a Λ, então $\boldsymbol{x} + \boldsymbol{y}$ e $-\boldsymbol{x}$ também pertencem a Λ. Os pontos de um reticulado posicionam-se de maneira bastante regular e simétrica no espaço, como ilustrado na Figura 1.

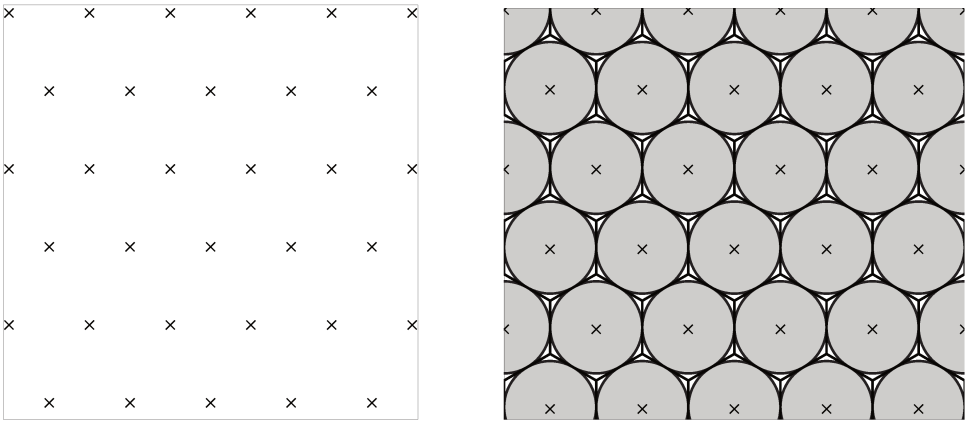
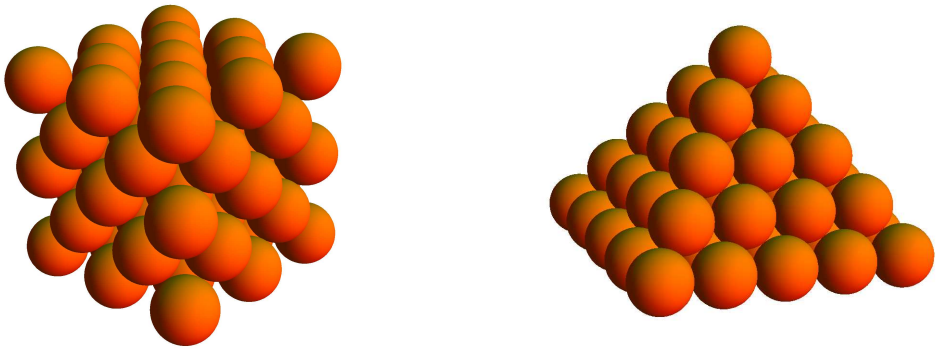


Figura 1: Pontos de um reticulado restrito a um quadrado e o empacotamento de esferas associado

Uma boa parte da pesquisa de reticulados é impulsionada pela busca por uma resposta à seguinte pergunta: qual a maneira de dispormos esferas de mesmo raio em $\mathbb{R}^n$, sem sobreposição, de modo a cobrir a maior parte possível do espaço? A solução no plano e no espaço tridimensional é bastante intuitiva: a maneira com que as abelhas fazem as suas colmeias (ilustrada na Figura 1) provém a maior eficiência no plano, enquanto em $\mathbb{R}^3$ o reticulado conhecido como cúbico de face centrada (ou "pilha de laranjas", Figura 2) nos diz onde devem estar posicionados os centros das esferas de modo a minimizar os espaços vazios. Para dimensões maiores, o problema torna-se significativamente mais complexo.

A Teoria da Informação, por sua vez, é uma abstração matemática utilizada



(a) (b)

Figura 2: (a) Empacotamento de esferas associado ao reticulado cúbico de face centrada e (b) uma "pilha de laranjas" retirada do empacotamento

para modelar sistemas de comunicação. Um modelo simplificado, porém relevante, encontra-se ilustrado no diagrama de blocos abaixo. O objetivo é transmitir uma *mensagem* através de um meio de comunicação ruidoso para um receptor.

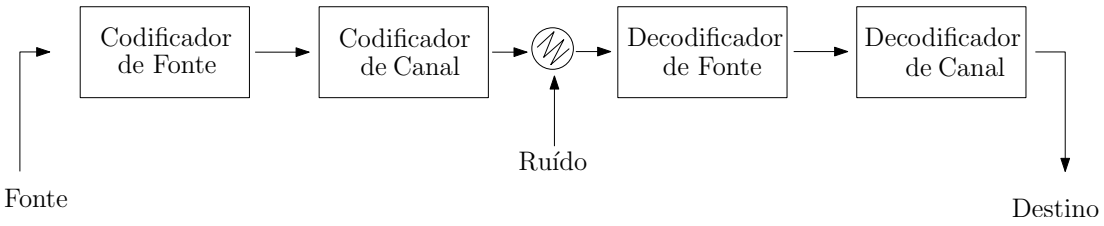


Figura 3: Modelo de transmissão de informação

Uma maneira abstrata de descrever a *fonte de informação* é através de uma variável aleatória, que pode ser contínua ou discreta. As possíveis mensagens a serem enviadas são representadas por amostras desta variável aleatória. Um *codificador de fonte* associa a cada possível amostra da fonte, uma sequência de símbolos (por exemplo, um conjunto de bits). Os símbolos são escolhidos de acordo com a estatística da fonte, de modo que o menor número de símbolos sejam utilizados em média, minimizando os custos e o tempo de transmissão.

Matematicamente, um *canal* recebe como entrada um símbolo e aplica uma transformação de modo a distorcê-lo, e o receptor observa apenas a versão dis-

torcida. Por exemplo, um modelo largamente estudado é o canal Gaussiano no qual, para cada símbolo real x enviado, o ruído age aditivamente, produzindo uma saída $y = x + z$, onde z é uma amostra retirada de uma variável aleatória com distribuição normal. O *codificador de canal* aplica uma transformação nas saídas do codificador de fonte, de modo a amenizar os efeitos do ruído. Os *decodificadores* (de canal e fonte) utilizam a saída do canal para tentar estimar a mensagem enviada.

Um modelo analisado nesta tese assume que a fonte possui distribuição contínua e os blocos relativos à fonte e ao canal colapsam, isto é, as codificações são feitas de uma só vez. Essa estratégia é conhecida por vezes como codificação conjunta fonte-canal.

Organização da Tese

Os problemas aqui tratados envolvem estruturas como reticulados q-ários (Capítulo 2), reticulados projeção (Capítulo 3) e as aplicações desses últimos ao problema de codificação contínua fonte-canal (capítulos 4 e 5). A tese está dividida de modo que os primeiros capítulos são destinados a questões mais teóricas, enquanto os últimos referem-se a aplicações em Teoria da Informação e codificação. O Capítulo 1 destina-se a estabelecer as bases da teoria utilizada, e portanto é necessário para a compreensão do restante da tese. Os capítulos 4 e 5 dependem apenas dos resultados acerca de projeção contidos no Capítulo 3 e podem ser lidos independentemente do Capítulo 2. A seguir, descrevemos brevemente cada conteúdo e contribuição original da tese.

Reticulados q-ários na Norma l_p

Chamamos de código corretor de erros q-ário um subconjunto de $\mathbb{Z}_q^n$, onde $\mathbb{Z}_q$ é o anel de inteiros módulo q[1]. Para tornar códigos corretores de erros aplicáveis

[1]Na literatura, a denominação "código q-ário" pode referir-se também a um subconjunto do espaço vetorial $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é um corpo com q elementos

a comunicações é necessário munir $\mathbb{Z}_q^n$ de uma métrica. A métrica usual nesse contexto é a métrica de Hamming, que possui aplicações no desenvolvimento de códigos para o Canal Binário Simétrico (BSC), um modelo ubíquo de transmissão de informação. Uma alternativa a essa métrica foi proposta por Lee em [Lee58], a qual coincide com métrica de Hamming quando $q = 2, 3$, mas nos provém uma geometria mais "fina" quando $q > 3$. Dentre as aplicações mais recentes da métrica de Lee está o desenvolvimento de códigos para memórias *flash* [JB10].

Podemos utilizar a estrutura de códigos corretores de erros para construir reticulados em $\mathbb{R}^n$ através, por exemplo, da chamada Construção A [CS98]. Esses reticulados, aos quais nos referimos por *reticulados q-ários* herdam muitas propriedades dos códigos subjacentes e são largamente utilizados em Teoria da Informação [Zam09]. No Capítulo 2 estudamos reticulados *q-ários* munindo o código associado de uma generalização da métrica de Lee (a qual chamamos p-Lee). Estudamos questões como algoritmos de decodificação e códigos perfeitos. Os resultados desse capítulo foram publicados em [CJC11] e [JCC13].

Reticulados Projeção

Apesar de a motivação inicial para nosso estudo de projeção de reticulados haver sido aplicações em codificação contínua fonte-canal, o tópico possui interesse próprio, e os resultados sustentam-se por si só. Por exemplo, a teoria de projeções de reticulados pode ser encontrada previamente na literatura associada a aproximações diofantinas e ao problema clássico de encontrar empacotamentos de esferas denso no $\mathbb{R}^n$ [CS98]. De fato, muitos reticulados notáveis como E_6, E_7, E_8, A_n, bem como os seus duais, possuem caracterizações naturais a partir de projeções e intersecções de reticulados com hiperplanos.

Um resultado notável e relativamente recente, devido a Sloane et. al [SVC11], é o de que qualquer reticulado de dimensão $(n-1)$ está arbitrariamente próximo, a menos de equivalência, de uma projeção do reticulado cúbico $\mathbb{Z}^n$ ao longo de um vetor $\boldsymbol{v} \in \mathbb{Z}^n$. Isso significa que muitos problemas importantes envolvendo

reticulados arbitrários (por exemplo, encontrar o empacotamento de esferas mais denso) podem ser tratados, ao menos aproximadamente, via projeções de $\mathbb{Z}^n$.

Um inconveniente do método descrito em [SVC11] é o de que necessitamos crescer muito a norma do vetor no qual estamos projetando para obter boas aproximações, o que dificulta aplicações práticas do resultado. No trabalho [CS13], provemos uma análise de convergência das sequências de projeções e mostramos como construir sequências quadraticamente melhores que aquelas em [SVC11], bem como construções explícitas para importantes famílias de reticulados. Em [CSC13], mostramos que o resultado de [SVC11] vale em uma generalidade muito maior. De fato, qualquer reticulado k-dimensional Λ_1 pode ser aproximado por projeções de qualquer reticulado n-dimensional Λ_2. Esses novos resultados estão descritos no Capítulo 3.

Codificação Contínua Fonte-Canal

Qual aplicação de uma fonte com suporte contínuo e dimensão k para um canal n-dimensional minimiza uma dada função de distorção? Shannon, o pai da Teoria da Informação, foi o primeiro a levantar esse questionamento [Sha49]. Quando a fonte e o canal possuem distribuição Gaussiana, $n = k$, e a função de distorção é o erro quadrático médio, é sabido que uma aplicação *linear* (às vezes referida na literatura como transmissão "sem codificação") é suficiente para atingir distorção ótima. Entretanto, no caso de outras distribuições de fonte relevantes (como a distribuição uniforme) e quando $k \neq n$, o problema torna-se significativamente mais complexo. Existe uma variedade de construções *ad hoc* na literatura, em baixa dimensão (e.g. [Chu00, WSR09, KR10, SV03]). Apesar de estas construções comportarem-se bem para a dimensão a qual foram projetadas, sua generalização e análise de erro são bastante complicadas. O estudo de aplicações para estes propósitos é também chamado de codificação contínua fonte-canal, ou mesmo codificação analógica.

Quando $k = 1$, podemos visualizar o desenvolvimento de códigos analógicos

como um problema de *empacotamento de curvas* [Sak70]. Construímos tais códigos em [CTC13] baseados em objetos geométricos chamados *toros planares*. Surpreendentemente, a maximização de certos parâmetros desses códigos contínuos está relacionada com o problema discreto de encontrar projeções do reticulado retangular $c_1\mathbb{Z} \oplus \ldots \oplus c_n\mathbb{Z}$ com boa densidade de empacotamento. Utilizando uma construção por camadas, exibimos códigos cuja performance aprimora significativamente os existentes na literatura. Esse é o tema do Capítulo 4.

O assunto do Capítulo 5 é o desenvolvimento de códigos para o regime $k < n$, conhecido como regime de expansão de largura de banda. Em [CVC13], mostramos como obter aplicações no caso $k > 1$ com comportamento assintoticamente ótimo no sentido dos limitantes apropriados advindos da Teoria de Informação. Uma conexão entre estes mapas e a teoria matemática da *dissecção de poliedros* é também exibida. Esperamos que os resultados dos capítulos 4 e 5 estimulem novas aplicações da rica teoria de dissecções de poliedros.

Notação

Como usual, utilizamos as letras $\mathbb{N}, \mathbb{Z}$ e $\mathbb{R}$ para denotar os números naturais, inteiros e reais. Escrevemos vetores do $\mathbb{R}^n$ com letras minúsculas em negrito e os interpretamos matricialmente como vetores-linha. Assim, por exemplo, o produto interno euclidiano usual entre dois vetores é dado por $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{x}\boldsymbol{y}^t$, onde $\boldsymbol{y}^t$ é o vetor transposto de $\boldsymbol{y}$. Matrizes são escritas em maiúsculo e os seus elementos em subscrito (e.g., o elemento da linha i e coluna j de uma matriz A é denotado por A_{ij}). A matriz identidade de ordem $n \times n$ é denotada por I_n, ou simplesmente I quando não houver ambiguidade. O vetor $\mathbf{0} \in \mathbb{R}^n$ é o vetor com todas as coordenadas nulas. A distância euclidiana usual entre dois vetores $\boldsymbol{x}$ e $\boldsymbol{y}$ de $\mathbb{R}^n$ é denotada por

$$d_2(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|_2 = \sqrt{(x_1 - y_1)^2 + \ldots + (x_n - y_n)^2}.$$

Para complexidade de funções, utilizamos as notações assintóticas $O(\cdot)$ e $\Theta(\cdot)$.

Se f e g são ambas funções reais (inteiras ou naturais), dizemos que $f(x) = O(g(x))$ se existem x_0 e $c > 0$ tais que, para qualquer $x \geq x_0$, vale que $|f(x)| \leq c|g(x)|$. Se $f(x) = O(g(x))$ e $g(x) = O(f(x))$, dizemos que $f(x) = \Theta(g(x))$ ($\Leftrightarrow g(x) = \Theta(f(x))$). O símbolos $\lfloor x \rfloor$ e $\lfloor x \rceil$ denotam, respectivamente, o maior inteiro que não ultrapassa x e o inteiro mais próximo de x (com empates decididos arbitrariamente).

Capítulo 1

Reticulados

At one point while working on this book we even considered adopting a special abbreviation for "It is a remarkable fact that", since this phrase seemed to occur so often.

- John Conway e Neil Sloane em [CS98], sobre como reticulados são fascinantes

Apesar de problemas relacionados a reticulados serem estudados pelo menos desde o século XVII, a formalização da teoria da maneira como a conhecemos é relativamente recente, devido aos trabalhos de matemáticos como Fejes Tóth e Rogers, de meados do século XX. Antes disso, a maioria das referências no tema trata de construções *ad hoc* para problemas específicos e não é raro encontrar resultados relevantes acerca de reticulados enunciados em outros contextos como equações diofantinas, formas quadráticas e teoria dos números [Lag75].

Neste capítulo discutimos noções e propriedades iniciais de reticulados, essenciais ao desenvolvimento do restante do trabalho. Longe de tentar cobrir exaustivamente o tema, nosso objetivo é estabelecer a notação e o ferramental teórico necessários para a compreensão do conteúdo do restante da tese. Nenhum dos resultados deste capítulo introdutório é original, e a maioria das proposições e demonstrações aqui contidas podem ser encontradas nas excelentes referências [Rog64], [Cas97] e [CS98]. Entretanto demos preferência por exibir a demonstração de alguns dos resultados, de modo a enfatizar pontos que serão importantes ao decorrer do trabalho.

1.1 Definições Iniciais

Sejam $m \leq n$ vetores linearmente independentes $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$. Um *reticulado* Λ com base $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ é o conjunto de todas as combinações lineares inteiras de $\boldsymbol{b}_i$, $i = 1, \ldots, m$, isto é:

$$\Lambda = \{u_1\boldsymbol{b}_1 + \ldots + u_m\boldsymbol{b}_m : u_1, \ldots, u_m \in \mathbb{Z}\}. \tag{1.1}$$

O conjunto $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ é denominado uma *base* de Λ. A matriz B cujas linhas são os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ é dita uma *matriz geradora* de Λ. Durante o texto, representaremos também um reticulado gerado pela matriz B por $\Lambda(B) = \Lambda$, intercambiando livremente ambas as notações quando não houver ambiguidade. O número de vetores de uma base de Λ é chamado de *posto* ou *dimensão*. Caso $m = n$, dizemos que Λ possui *posto completo*. Podemos re-escrever (1.1) matricialmente como

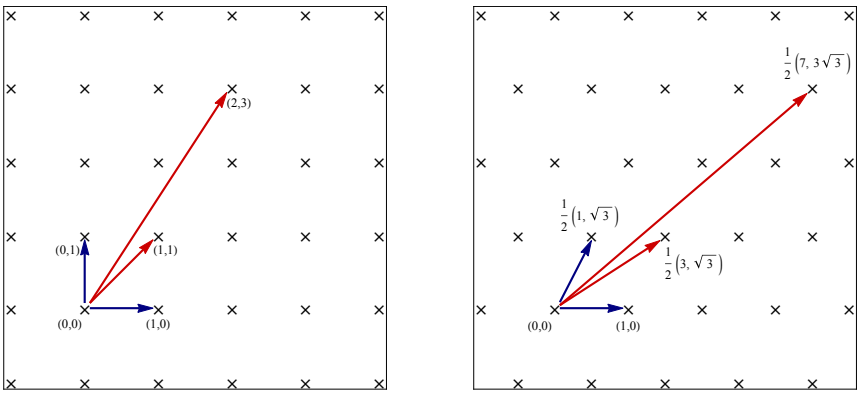
$$\Lambda = \{\boldsymbol{u}B : \boldsymbol{u} \in \mathbb{Z}^m\}, \tag{1.2}$$

onde $\mathbb{Z}^m$ é o conjunto de todos os vetores m-dimensionais com entradas inteiras (ou o reticulado gerado pela matriz identidade $m \times m$). Isso nos mostra que um reticulado pode ser visto como a imagem de $\mathbb{Z}^m$ por uma transformação linear. O *vetor de coordenadas* de um ponto $\boldsymbol{x} \in \Lambda$ com respeito à matriz B é o vetor $\boldsymbol{u} \in \mathbb{Z}^m$ tal que $\boldsymbol{u}B = \boldsymbol{x}$. Denotamos por $\text{span}(B) = \{\boldsymbol{u}B : \boldsymbol{u} \in \mathbb{R}^m\}$ o espaço vetorial gerado pelas linhas da matriz B.

Segue imediatamente da definição que um reticulado é um subgrupo aditivo e discreto do $\mathbb{R}^n$. Menos diretamente, pode-se provar o seguinte resultado, que nos provém uma definição alternativa de reticulado:

Teorema 1.1.1 ([Cas97, p.78])**.** *Um conjunto $\Lambda \subset \mathbb{R}^n$ é um reticulado se, e somente se, é um subgrupo aditivo discreto de $\mathbb{R}^n$.*

Um reticulado $\Lambda(B)$ possui infinitas bases, como ilustrado na Figura 1.1. A caracterização de bases distintas é feita a partir de matrizes especiais, conhecidas



(a) Reticulado $\mathbb{Z}^2$ (b) Reticulado Hexagonal

Figura 1.1: Bases distintas para o mesmo reticulado em cada figura

como unimodulares. Uma matriz U de ordem $m \times m$ é dita *unimodular* se possui entradas inteiras e determinante igual a $+1$ ou -1.

Proposição 1.1.2 ([Cas97, p.10])**.** *Sejam B e $\overline{B}$ matrizes $m \times n$ de posto completo. Temos que $\Lambda(B) = \Lambda(\overline{B})$ se, e somente se, existe uma matriz unimodular U tal que $\overline{B} = UB$.*

Exemplo 1.1.3. *Na Figura 1.1 estão ilustrados dois reticulados contidos no plano e duas bases distintas para cada um deles. As matrizes geradoras associadas às diferentes bases do reticulado $\mathbb{Z}^2 = \{(u_1, u_2) : u_1, u_2 \in \mathbb{Z}\}$ em 1.1a são*

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e } \overline{B} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

No caso do reticulado hexagonal,1.1b, temos

$$B = \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix} \text{ e } \overline{B} = \begin{pmatrix} 3/2 & \sqrt{3}/2 \\ 7/2 & 3\sqrt{3}/2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}.$$

Em ambos os casos, a matriz mudança de base unimodular U é dada por

$$U = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

A matriz $G = BB^t$ é chamada de *matriz de Gram* de $\Lambda = \Lambda(B)$ e essencialmente nos diz os ângulos entre os vetores de uma base e as suas normas. O *determinante* ou *discriminante* de Λ é definido como $\det \Lambda = \det G$. Note que o determinante de um reticulado é um invariante por mudança de base. Para dar um significado geométrico à grandeza $\det \Lambda$, definimos primeiramente o *paralelotopo fundamental* $\mathcal{P}(B)$ como

$$\mathcal{P}(B) = \{\alpha_1 \boldsymbol{b_1} + \ldots + \alpha_m \boldsymbol{b_m} : 0 \leq \alpha_i < 1, i = 1, \ldots m\}. \tag{1.3}$$

Temos que o volume (m-dimensional) de $\mathcal{P}(B)$ é igual a $\sqrt{\det \Lambda}$. É fácil verificar que o paralelotopo $\mathcal{P}(B)$ possui as seguintes propriedades:

(i) Se $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, $\boldsymbol{x} \neq \boldsymbol{y}$, então $(\boldsymbol{x} + \mathcal{P}(B)) \bigcap (\boldsymbol{y} + \mathcal{P}(B)) = \emptyset$ e

(ii) $\bigcup_{\boldsymbol{x} \in \Lambda} (\boldsymbol{x} + \mathcal{P}(B)) = \text{span}(B)$.

Em outras palavras, a união disjunta de translações de $\mathcal{P}(B)$ por pontos de Λ *ladrilha* o espaço $\text{span}(B)$. Qualquer região que satisfaz as propriedades (i) e (ii) é chamada de *região fundamental* de Λ. Um fato interessante é o de que qualquer região fundamental de Λ possui volume $\sqrt{\det \Lambda}$ (veja Teorema 1.6. [Rog64, p.28]). Para regiões fundamentais poliedrais, isto pode ser visto como uma consequência do Teorema dos Dois Ladrilhos, enunciado na Seção 5.3.1. Uma outra região fundamental importante é a *região de Voronoi* dada por $\mathcal{V}_\Lambda(\boldsymbol{x}) = \{\boldsymbol{y} \in \text{span}(B) : \|\boldsymbol{x} - \boldsymbol{y}\|_2 \leq \|\boldsymbol{z} - \boldsymbol{y}\|_2, \text{for all } \boldsymbol{z} \in \Lambda\}$. A região de Voronoi corresponde aos pontos em $\text{span}(B)$ que estão mais próximos de $\boldsymbol{x}$ que de qualquer outro ponto de Λ.

Em diversas aplicações, estamos interessados em contar (ou ao menos aproxi-

mar) a quantidade de pontos da intersecção de um reticulado com algum conjunto, usualmente um corpo convexo (e.g., um politopo ou uma esfera euclidiana). A proposição a seguir nos diz que, assintoticamente, a quantidade de pontos de um reticulado por unidade de volume é $\sqrt{(\det \Lambda)^{-1}}$, provendo uma outra motivação para a definição de determinante. Denotaremos daqui em diante a bola euclidiana fechada, de raio R, centrada em um ponto $\boldsymbol{x}$, por $B_2(\boldsymbol{x}, R)$, i.e.,

$$B_2(\boldsymbol{x}, R) = \left\{ \boldsymbol{x} \in \mathbb{R}^n : x_1^2 + \ldots + x_n^2 \leq R^2 \right\}.$$

Por simplificação, a bola centrada na origem, $B_2(\mathbf{0}, R)$, será denotada por $B_2(R)$.

Proposição 1.1.4. *Seja Λ um reticulado de posto completo e seja $S(R) = \Lambda \cap B_2(R)$ o conjunto dos pontos de Λ contidos em $B_2(R)$. Temos:*

$$\sqrt{\det \Lambda} = \lim_{R \to \infty} \frac{\mathrm{vol}(B_2(R))}{|S(R)|}.$$

Demonstração. Considere o paralelotopo $\mathcal{P} = \mathcal{P}(B)$ associado a alguma matriz geradora B de Λ e o conjunto $\bigcup_{\boldsymbol{x} \in S(R)} (\boldsymbol{x} + \mathcal{P})$. Seja $L = \sup \{ \|\boldsymbol{x}\|_2 : \boldsymbol{x} \in \mathcal{P} \}$. Para $R > L$, temos:

$$B_2(R - L) \subset \bigcup_{\boldsymbol{x} \in S(R)} (\boldsymbol{x} + \mathcal{P}) \subset B_2(R + L)$$

e portanto

$$\mathrm{vol}(B_2(R - L)) \leq \mathrm{vol}\left(\bigcup_{\boldsymbol{x} \in S(R)} (\boldsymbol{x} + \mathcal{P}) \right) \leq \mathrm{vol}(B_2(R + L)) \Rightarrow$$

$$\mathrm{vol}(B_2(R - L)) \leq |S(R)| \sqrt{\det \Lambda} \leq \mathrm{vol}(B_2(R + L)) \Rightarrow$$

$$\frac{\mathrm{vol}(B_2(R - L))}{\mathrm{vol}(B_2(R))} \leq \frac{|S(R)| \sqrt{\det \Lambda}}{\mathrm{vol}(B_2(R))} \leq \frac{\mathrm{vol}(B_2(R + L))}{\mathrm{vol}(B_2(R))}.$$

Tomando o limite para $R \to \infty$ concluimos a demonstração. □

Observação 1.1.5. *O teorema acima pode ser facilmente estendido para reticulados de posto incompleto, tomando alguns cuidados adicionais, como considerar a intersecção de $B_2(R)$ com o subspaço vetorial gerado pelas linhas de B e calcular o volume m-dimensional desta intersecção. Neste caso, sendo $\tilde{B}_2(R) = B_2(R) \cap \operatorname{span}(B)$, vale que*

$$\sqrt{\det \Lambda} = \lim_{R\to\infty} \frac{\operatorname{vol}(\tilde{B}_2(R))}{|S(R)|}.$$

Sejam $\Lambda, \Lambda' \subset \mathbb{R}^n$ dois reticulados de mesmo posto. Se $\Lambda' \subseteq \Lambda$, dizemos que Λ' é um *sub-reticulado* de Λ. O *índice* de Λ' em Λ é definido como a razão $\sqrt{\det \Lambda'}/\sqrt{\det \Lambda}$. Como qualquer ponto de Λ' é também um ponto de Λ, segue que se $\Lambda = \Lambda(B)$ e $\Lambda' = \Lambda(B')$, então as suas respectivas matrizes geradoras estão relacionadas por $MB = B'$, onde M é uma matriz inteira de ordem $m \times m$, mostrando que o índice de Λ' em Λ é sempre um número inteiro.

Utilizando a caracterização de Λ' e Λ como grupos abelianos, é possível definir o quociente Λ/Λ' . Dizemos que $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$ estão na mesma classe de equivalência se $\boldsymbol{x} - \boldsymbol{y} \in \Lambda'$. A cardinalidade do grupo quociente $|\Lambda/\Lambda'|$ é igual ao número de classes de equivalências distintas em Λ com respeito a Λ'. Temos o seguinte resultado:

Proposição 1.1.6 ([Cas97, p.14])**.** *A cardinalidade do grupo quociente Λ/Λ' é igual ao índice de Λ' em Λ.*

Observação 1.1.7. *Na definição de sub-reticulado, exigimos que Λ' possua o mesmo posto que Λ, pois caso contrário a cardinalidade do grupo quociente não é finita, e a caracterização 1.1.6 não é válida.*

Dizemos que dois reticulados Λ_1 e Λ_2 são equivalentes (e escrevemos $\Lambda_1 \sim \Lambda_2$) se podemos obter Λ_1 de Λ_2 através de uma composição de rotações, reflexões e mudança de escala. Mais formalmente, dizemos que $\Lambda_1(B_1) \sim \Lambda_2(B_2)$ se existem uma matriz unimodular U, uma matriz ortogonal Q e um número real $k \neq 0$ tais que $kUB_1Q = B_2$. Neste caso, temos que $\det \Lambda_2 = k^{2m} \det \Lambda_1$. Reticulados equi-

valentes são idênticos no que tange a propriedades relativas à métrica euclidana. Em outras métricas, é necessário utilizar outras noções de equivalência.

Algumas vezes é mais conveniente visualizar um reticulado $\Lambda(B) \subset \mathbb{R}^n$ imerso isometricamente em $\mathbb{R}^k$, $k > n$. Podemos fazer isso de infinitas maneiras. A mais simples é provavelmente adicionar $k - n$ colunas de zeros à matriz B. Dois reticulados equivalentes, ou imersos isometricamente em espaços distintos, são também chamados de duas *representações* do mesmo reticulado.

1.1.1 Conjuntos Primitivos de Vetores

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de posto m. Dizemos que conjunto $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\} \subset \Lambda$ é um *conjunto primitivo* (de vetores de Λ) se existem $\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{x}_m \in \Lambda$ tais que $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{x}_{k+1}, \ldots \boldsymbol{x}_m\}$ é uma base para Λ. Em outras palavras, um conjunto é primitivo em Λ se podemos completá-lo até formarmos uma base para Λ.

Exemplo 1.1.8. *Está claro da definição que nem todo vetor $\boldsymbol{x} \in \Lambda$ é primitivo. Para ver isso, considere, por exemplo, o reticulado $\mathbb{Z}^2$ (Exemplo 1.1.3), e seja o vetor $\boldsymbol{x} = (2, 0) \in \mathbb{Z}^2$. Suponha que existe um vetor $\boldsymbol{y}$ tal que $\{\boldsymbol{x}, \boldsymbol{y}\}$ é uma base para Λ. O determinante da matriz cujas linhas são $\boldsymbol{x}$ e $\boldsymbol{y}$ é certamente maior que 2, em módulo, o que contradiz o fato do determinante de $\mathbb{Z}^2$ ser 1. Isso nos mostra que não pode existir nenhuma base de $\mathbb{Z}^2$ que contém o vetor $(2, 0)$. De fato, não é difícil ver que qualquer vetor cujo mdc das coordenadas é diferente de 1 não é primitivo em $\mathbb{Z}^2$. Veremos a seguir que esta condição necessária para primitividade é também suficiente, ou seja, qualquer vetor cujo mdc das coordenadas é igual a 1 faz parte de alguma base de $\mathbb{Z}^n$*

Pode-se encontrar na literatura diversas definições distintas para conjuntos primitivos de vetores, todas elas equivalentes. O teorema abaixo descreve algumas delas.

Teorema 1.1.9. *Seja $\Lambda(B) \subset \mathbb{R}^n$ um reticulado de posto m e considere os vetores $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \in \Lambda(B)$, tais que $\boldsymbol{x}_i = \boldsymbol{u}_i B, \boldsymbol{u}_i \in \mathbb{Z}^n, i = 1, \ldots k$. Denotemos por U*

a matriz cujas linhas são os vetores de coordenadas $\boldsymbol{u}_i$*. As seguintes afirmações são equivalentes:*

(i) $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ *é um conjunto primitivo de* $\Lambda(B)$

(ii) *O mdc dos menores* $k \times k$ *da matriz* U *é igual a* 1*.*

(iii) *O paralelotopo*

$$\mathcal{P}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k) = \{\alpha_1 \boldsymbol{x}_1 + \ldots + \alpha_k \boldsymbol{x}_k : 0 \leq \alpha_i < 1, i = 1, \ldots m\}$$

não possui nenhum ponto de $\Lambda(B)$*, exceto a origem.*

Demonstração. A demonstração da equivalência (i) $\Leftrightarrow$ (ii) pode ser encontrada em [Cas97, p.15, Lem.2]. Já a demonstração de que (iii) $\Rightarrow$ (i) pode ser encontrada em [GL87, p.21, Teo. 5]. Para conectar as caracterizações, provamos aqui que (i) $\Rightarrow$ (iii). Seja uma base $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{x}_{k+1}, \ldots \boldsymbol{x}_m$ para $\Lambda(B)$. Suponhamos, por absurdo, que existe um ponto não nulo $\boldsymbol{y} \in \Lambda(B)$ tal que $\boldsymbol{y} = \alpha_1 \boldsymbol{x}_1 + \ldots + \alpha_k \boldsymbol{x}_k, 0 \leq \alpha_i < 1$. Isso quer dizer que se escrevermos $\boldsymbol{y} = u_1 \boldsymbol{x}_1 + \ldots + u_k \boldsymbol{x}_k + u_{k+1} \boldsymbol{x}_{k+1} + \ldots + u_m \boldsymbol{x}_m$ temos necessariamente $u_i = \alpha_i$, para $i \leq k$ e $u_i = 0$, para $i \geq k + 1$. Assim, se algum $\alpha_i \neq 0$, $\boldsymbol{y}$ é um ponto do reticulado $\Lambda(B)$ que não pode ser escrito como combinação inteira dos vetores de uma base para $\Lambda(B)$, o que é um absurdo e portanto $\boldsymbol{y}$ não pode existir, finalizando a demonstração. □

Corolário 1.1.10. *Um vetor* $\boldsymbol{x} \in \Lambda$ *é primitivo se, e somente se, o mdc das entradas do seu vetor de coordenadas é igual a* 1*.*

1.1.2 O Reticulado Dual

Um conceito central para os resultados acerca de projeções de reticulados é o de dualidade. O reticulado *dual* de $\Lambda = \Lambda(B)$, denotado por $\Lambda^* = \Lambda^*(B)$, é definido como

$$\Lambda^* = \{\boldsymbol{y} \in \text{span}(B) \mid \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ para qualquer } \boldsymbol{x} \in \Lambda\}. \tag{1.4}$$

Reticulados duais são por vezes chamados de *polares* ou *recíprocos* e surgem em contextos tão distintos como Teoria Algébrica dos Números e Cristalografia. Formalmente, ainda não podemos dizer que Λ^* é um reticulado - a demonstração deste fato será adiada para a Proposição 1.1.11. Contudo, mostraremos a seguir uma motivação algébrica e uma interpretação geométrica da definição acima.

A motivação algébrica para a dualidade de reticulados pode ser feita por analogia com a definição para espaços vetoriais. Lembramos que o espaço dual de um espaço vetorial V sobre um corpo $\mathbb{F}$ é definido de maneira usual como o conjunto de todos os funcionais lineares de V em $\mathbb{F}$. De maneira análoga, o espaço dual de um reticulado Λ é o espaço de funcionais lineares de Λ em $\mathbb{Z}$. Assim como no caso de espaços vetoriais, pode-se mostrar que cada funcional linear $\phi : \Lambda \to \mathbb{Z}$ é da forma $\phi(\boldsymbol{x}) = \phi_{\boldsymbol{a}}(\boldsymbol{x}) = \langle \boldsymbol{x}, \boldsymbol{a} \rangle$ para um único $\boldsymbol{a} \in \text{span}(B)$. Desse modo, o espaço Λ^* (1.4) é o espaço de funcionais lineares de Λ em $\mathbb{Z}$ representados como vetores em $\text{span}(B)$.

Do ponto de vista da interpretação geométrica, notemos primeiro que a condição $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}$ para qualquer $\boldsymbol{x} \in \Lambda$ é equivalente à condiçao $\langle \boldsymbol{b}_i, \boldsymbol{y} \rangle \in \mathbb{Z}$, $i = 1, \ldots, m$, onde $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ é uma base para Λ. Cada conjunto

$$H_i = \{\boldsymbol{y} \in \text{span}(B) : \langle \boldsymbol{b}_i, \boldsymbol{y} \rangle = 0, \pm 1, \pm 2, \ldots\}$$

corresponde à união de hiperplanos separados de uma distância $1/\left\|\boldsymbol{b}_i\right\|$, como ilustrado na Figura 1.2 no caso em que H_i é constituído por retas no $\mathbb{R}^2$. Assim, o reticulado dual é dado pela intersecção dos conjuntos H_i. Essa caracterização de dualidade através de intersecções com hiperplanos será crucial no Capítulo 3.

A seguinte proposição coleta algumas propriedades úteis de reticulados duais.

Proposição 1.1.11. *Seja $\Lambda(B)$ um reticulado gerado pela matriz de posto completo B, $m \times n$, $m \leq n$. Valem as seguintes propriedades:*

(i) $\Lambda^*(B) = \Lambda(B^\dagger)$, onde $B^\dagger = (BB^t)^{-1}B$ é a transposta da matriz pseudo-

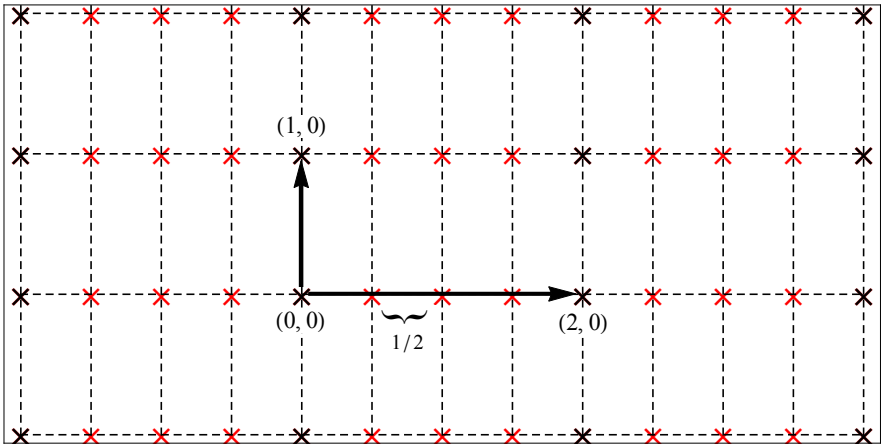


Figura 1.2: Ilustração do reticulado com base $\{\boldsymbol{b}_1, \boldsymbol{b}_2\} = \{(2,0),(0,1)\}$ e seu dual, que possui como base o conjunto $\{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*\} = \{(1/2,0),(0,1)\}$.

inversa de B. Em particular, se $m = n$, $\Lambda^*(B)$ é gerado por B^{-t} (a transposta da inversa da matriz B).

(ii) *Se G é uma matriz de Gram de Λ então G^{-1} é uma matriz de Gram de Λ^{-1}*

(iii) $\det \Lambda^*(B) = (\det \Lambda(B))^{-1}$.

(iv) $(\Lambda^*)^* = \Lambda$

(v) *Se $\Lambda_1 \sim \Lambda_2$, então $\Lambda_1^* \sim \Lambda_2^*$.*

Demonstração. Notemos primeiro que as propriedades (ii)-(v) decorrem imediatamente de (i). Para demonstrar (i), consideremos primeiro a inclusão $\Lambda(B^\dagger) \subset \Lambda^*(B)$. Se $\boldsymbol{y} \in \Lambda(B^\dagger)$, então $\boldsymbol{y} = \boldsymbol{u}B^\dagger$ para algum $\boldsymbol{u} \in \mathbb{Z}^n$. Realizando o produto interno de $\boldsymbol{y}$ com qualquer elemento $\boldsymbol{x} = \boldsymbol{v}B \in \Lambda(B)$, $\boldsymbol{v} \in \mathbb{Z}^n$, temos $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{u}B^\dagger B^t \boldsymbol{v}^t = \boldsymbol{u}\boldsymbol{v}^t \in \mathbb{Z}$, mostrando que $\boldsymbol{y} \in \Lambda^*(B)$. Consideremos agora a inclusão $\Lambda^*(B) \subset \Lambda(B^\dagger)$. Como $\operatorname{span}(B) = \operatorname{span}(B^\dagger)$, podemos escrever qualquer elemento $\boldsymbol{y} \in \Lambda^*(B)$ como $\boldsymbol{y} = \boldsymbol{u}B^\dagger$, para algum $\boldsymbol{u} \in \mathbb{R}^n$. Para provar a inclusão, é suficiente mostrar que $\boldsymbol{u} \in \mathbb{Z}^n$. Como $\boldsymbol{y} = \boldsymbol{u}B^\dagger \in \Lambda^*(B)$, então $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}$ para qualquer $\boldsymbol{x} \in \Lambda(B)$. Escolhendo $\boldsymbol{x} = \boldsymbol{b}_i$ como a i-ésima linha de B, temos que $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{u}_i \in \mathbb{Z}$, mostrando que $\boldsymbol{u} \in \mathbb{Z}^n$ e portanto $\boldsymbol{x} \in \Lambda(B^\dagger)$. □

Exemplo 1.1.12. *Denotamos por $D = diag(c_1, \ldots, c_n)$ a matriz diagonal tal que $D_{ii} = c_i$. O reticulado $\Lambda = \Lambda(D)$ possui malha retangular e é denotado por $c_1\mathbb{Z} \oplus \ldots \oplus c_n\mathbb{Z}$. Vemos da Proposição 1.1.11 que uma matriz geradora para $\Lambda^*(D)$ é a matriz $D^{-1} = diag(1/c_1, \ldots, 1/c_n)$. Se c_i são números inteiros positivos, então $\Lambda \subset \Lambda^*$. Na Figura 1.2 ilustramos o caso $n = 2$, $c_1 = 2$ e $c_2 = 1$.*

Se $\Lambda = \Lambda^*$, dizemos que Λ é *auto-dual*. Caso $\Lambda \sim \Lambda^*$, dizemos que Λ é *isodual*.

1.2 Empacotamentos de Esferas

Nas seções anteriores consideramos majoritariamente propriedades algébricas da teoria de reticulados. A razão pela qual reticulados despertam tanto interesse da comunidade matemática, entretanto, está provavelmente nas suas propriedades geométricas e na associação com o difícil problema de encontrar empacotamentos densos no espaço. A *norma mínima* de um reticulado é definida como

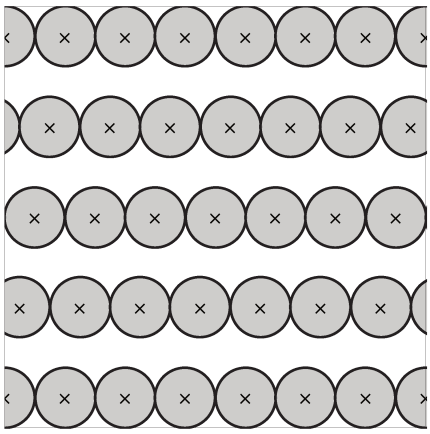
$$\lambda(\Lambda) = \min_{\mathbf{0} \neq \boldsymbol{x} \in \Lambda} \|\boldsymbol{x}\|_2 , \tag{1.5}$$

isto é, $\lambda(\Lambda)$ é o o mínimo entre todas as normas de vetores de não nulos de Λ. É fácil ver que $\rho = \lambda/2$ é o maior valor para o qual as bolas $B_2(\boldsymbol{x}, \rho)$ centradas em $\boldsymbol{x} \in \Lambda$ possuem interiores disjuntos. Definimos assim um *empacotamento reticulado* como a união de translações da bola $B_2(\rho)$ por pontos de Λ. Chamamos $\rho = \lambda/2$ de *raio de empacotamento* de Λ e definimos a *densidade* de empacotamento de um reticulado de posto completo Λ como

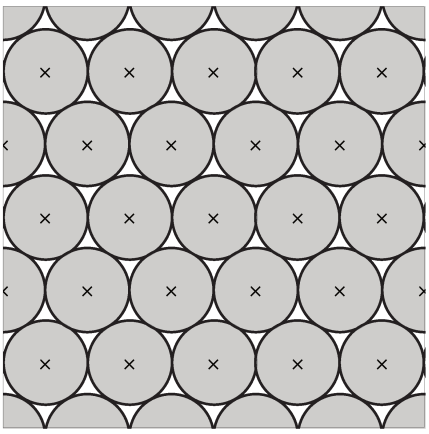
$$\Delta(\Lambda) = \frac{\text{vol } B_2(\rho)}{\sqrt{\det \Lambda}}. \tag{1.6}$$

O volume de $B_2(\rho)$ pode ser calculado através da fórmula

$$\text{vol}(B_2(\boldsymbol{x}, \rho)) = \frac{\rho^n \pi^n}{(n/2)!}, \tag{1.7}$$



(a) Reticulado gerado pelos vetores $(1, 0)$ e $(1/4, 3/2)$, cuja densidade é aproximadamente 0.523599



(b) Reticulado hexagonal, cuja densidade de é aproximadamente 0.906899

Figura 1.3: Dois reticulados com densidade de

onde $(n/2)!$ deverá ser entendido como a função gama, $(n/2)! = \Gamma(n/2 + 1) = \int_0^\infty e^{-t} t^{n/2} \mathrm{d}t$. Para evitar a utilização da função gama, é comum definir-se a *densidade de centro* de Λ como

$$\delta(\Lambda) = \frac{\Delta(\Lambda)}{\text{vol } B_2(1)} = \frac{\rho^n}{\sqrt{\det \Lambda}}. \tag{1.8}$$

Na Figura 1.3 estão ilustrados alguns reticulados e as suas respectivas densidades de empacotamento. Intuitivamente, a densidade mede a porção do espaço coberta por bolas com maior valor possível de raio. Da definição de densidade, temos diretamente:

Proposição 1.2.1. *Se* $\Lambda_1 \sim \Lambda_2$*, então* $\Delta(\Lambda_1) = \Delta(\Lambda_2)$.

Observação 1.2.2. *Para definirmos a densidade de reticulados que não possuem posto completo, basta substituirmos* vol $B_2(\rho)$ *na fórmula* (1.6) *pelo volume da bola de raio* ρ *com dimensão igual à dimensão de* Λ*. Alternativamente, podemos calcular a densidade de* Λ *achando uma representação de posto completo e utilizando a fórmula* (1.6)*.*

A teoria de empacotamentos é muito mais geral do que trataremos aqui. Para

entender porque a densidade como definida anteriormente corresponde à noção intuitiva de preenchimento do espaço por esferas[1], precisamos adentrar em algumas tecnicalidades da teoria, as quais podem ser encontradas em [Rog64]. Aqui daremos apenas uma ideia dos conceitos.

Primeiramente, notemos que se $M \subset N$ são dois conjuntos com volume finito, é natural definir a densidade de M em N (isto é, a porção de N ocupada por M) como (vol N)/(vol M). A dificuldade em definir a densidade de um empacotamento reticulado surge do fato de que vol $\mathbb{R}^n = \infty$. Para contornar este problema, calculamos a densidade do reticulado restrita a uma esfera e tendemos o raio desta esfera para infinito.

Formalmente, seja um reticulado Λ com raio de empacotamento ρ. Considere o conjunto $S(R) = \Lambda \cap B_2(R)$ como definido na Proposição 1.1.4, com $R > \rho$. Sejam também

$$S^+(R) = \{\boldsymbol{x} \in \Lambda : B_2(\boldsymbol{x}, \rho) \cap B_2(\boldsymbol{x}, R) \neq \emptyset\} \text{ e}$$

$$S^-(R) = \{\boldsymbol{x} \in \Lambda : B_2(\boldsymbol{x}, \rho) \subset B_2(\boldsymbol{x}, R)\},$$

tais que $S^-(R) \subset S(R) \subset S^+(R)$. Se calcularmos as razões

$$\Delta^+(R) = \frac{|S^+(R)|\text{vol } B_2(\rho)}{\text{vol } B_2(R)},\ \Delta^-(R) = \frac{|S^-(R)|\text{vol } B_2(\rho)}{\text{vol } B_2(R)}$$

teremos limitantes superiores e inferiores para a porção da esfera maior $B_2(R)$ coberta pela união de esferas menores $B_2(\rho)$ (ambos conjuntos de volume finito). À medida que aumentamos o raio R, temos a noção de preenchimento do espaço desejada. Segue diretamente da Proposição 1.1.4 que

$$\lim_{R\to\infty} \frac{|S(R)|\text{vol } B_2(\rho)}{\text{vol } B_2(R)} = \Delta(\Lambda).$$

[1]Estritamente falando, o termo esfera refere-se à superfície de uma bola euclidiana. Deste modo, o espaço é preenchido por bolas euclidianas e não esferas. Para ser consistente com a literatura, entretanto, utilizamos a expressão menos precisa "empacotamento de esferas".

Modificando sutilmente os argumentos da demonstração de 1.1.4, podemos demonstrar também que $\lim_{R\to\infty} \Delta^-(R) = \lim_{R\to\infty} \Delta^+(R) = \Delta(\Lambda)$ e portanto ambos os limitantes convergem para o mesmo valor. É natural, então, que definamos $\Delta(\Lambda)$ como a densidade do reticulado Λ.

Observação 1.2.3. *Uma maneira mais simples de interpretar a densidade de Λ é a partir da região de Voronoi. O raio de empacotamento ρ é o maior raio tal que $B_2(\rho) \subset \mathcal{V}_\Lambda(\mathbf{0})$. Portanto, a densidade de empacotamento de Λ restrita a uma região de Voronoi é dada por* vol $B_2(\rho)$/vol $\mathcal{V}_\Lambda(\mathbf{0})$. *Por periodicidade, essa é também a densidade de Λ em $\mathbb{R}^n$. Esta abordagem, entretanto, não se estende para empacotamentos mais gerais.*

Seja Δ_n o supremo de $\Delta(\Lambda)$ tomado sobre todos os reticulados de posto n. Segue do Teorema da Compacidade de Mahler [Cas97, Cap. 4] que existe pelo menos um reticulado em $\mathbb{R}^n$ cuja densidade corresponde a Δ_n. Encontrar tal reticulado é o Santo Graal da teoria de empacotamentos e está relacionado com o 18^o problema de Hilbert. Em [CS98, p.xxix] encontra-se uma tabela dos reticulados mais densos conhecidos, bem como mais referências acerca do tema. Até o momento em que esta tese foi escrita, conhecia-se o empacotamento reticulado *provadamente* mais denso apenas nas dimensões $n = 1$ a 8 e $n = 24$. Em altas dimensões, o melhor resultado assintótico é o Limitante de Minkowski-Hlawka, dado por

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

onde $\zeta(n) = \sum_{i=1}^{\infty} 1/i^n$ é a função zeta de Riemman. Uma demonstração simples e auto-contida de uma versão sutilmente mais fraca do limitante ($\Delta_n \geq 1/2^{n-1}$) pode ser encontrada em [Rog64, Cap. 4].

É claro que não precisamos limitar-nos a empacotamentos reticulados. Um *empacotamento de esferas*, de maneira geral, é simplesmente a união de translações de uma esfera cujos interiores não se interesctam. Utilizando a mesma ideia de $\Delta^+(R)$ e $\Delta^-(R)$ podemos definir a densidade de empacotamentos mais gerais

[Rog64, Cap. 1]. Podemos então perguntar qual o supremo de todas as densidades para um empacotamento *qualquer* em $\mathbb{R}^n$. Esse problema é significativamente mais difícil que a sua restrição a reticulados, e sabe-se a resposta apenas até o $\mathbb{R}^3$ [Hal05]. Não consideraremos, nesta tese, o problema geral de empacotamentos. Entretanto, é interessante notar que o problema geral pode ser aproximado utilizando reticulados e o conceito de sistemas periódicos. De maneira geral, um sistema de translações periódico $\mathcal{L}$ é um conjunto do tipo

$$\mathcal{L} = \bigcup_{i=1}^{k} (\Lambda + \boldsymbol{x}_i)\,, \tag{1.9}$$

com $\Lambda \subset \mathbb{R}^n$ um reticulado e $\boldsymbol{x}_i \in \mathbb{R}^n$. Um *empacotamento periódico* é a união finita de translações de um empacotamento reticulado. Em [Rog64, p.29] é demonstrado que existe uma sequência de empacotamentos periódicos com densidades arbitrariamente próximas da melhor densidade de empacotamento. Em [CE03], empacotamentos períodicos são empregados para estabelecer os melhores limitantes superiores para a densidade de empacotamentos gerais nas dimensões 4 até 36 conhecidos até hoje.

1.2.1 Extensões

O problema de empacotamentos pode ser facilmente estendido para outros corpos convexos e para outras métricas que não a euclidiana. No Capítulo 2 consideraremos a família das métricas l_p , dada por

$$d_p(\boldsymbol{x}, \boldsymbol{y}) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p}. \tag{1.10}$$

Para essa família, todas as definições vistas anteriormente (norma mínima, densidade, e densidade de centro), bem como uma generalização da Proposição 1.1.4, são completamente análogas. No caso $p = 1$, as bolas na norma l_p são conhecidas como *politopos cruz*. Para $n = 2$, um politopo cruz é um losango, e é fácil

ver que a melhor densidade de empacotamento é 1, isto é, losangos preenchem completamente o plano. Para $n = 3$, Minkowski demonstrou que a melhor densidade de empacotamento é 18/19 [Min04]. Em dimensões maiores, pouco se sabe sobre o melhor empacotamento. Um resultado assintótico para empacotamentos de esferas na norma l_p comparável ao Limitante de Minkowski-Hlawka é exibido por Rush e Sloane em [RS87].

1.3 Zoológico de Reticulados

Certos reticulados são particularmente importantes por possuírem grande simetria e outras propriedades especiais. Listamos aqui alguns deles:

O Reticulado $\mathbb{Z}^n$

O reticulado cúbico $\mathbb{Z}^n$ definido como $\mathbb{Z}^n = \{(u_1, \ldots, u_n) : u_i \in \mathbb{Z}, i = 1, \ldots, n\}$ corresponde a todos os pontos inteiros em $\mathbb{R}^n$. Como possível matriz geradora, podemos tomar simplesmente a matriz identidade de ordem $n \times n$. Por esta razão, deduzimos que $\mathbb{Z}^n$ é auto-dual, sua norma mínima é $\lambda(\mathbb{Z}^n) = 1$ e sua densidade de centro é dada por $\delta(\mathbb{Z}^n) = 2^{-n}$. É interessante notar que qualquer matriz unimodular também gera $\mathbb{Z}^n$. O reticulado $\mathbb{Z}^n$ é um importante elemento de base da teoria, já que qualquer outro reticulado é uma transformação linear dele.

O Reticulado A_n

O reticulado A_n é dado pela intersecção de $\mathbb{Z}^{n+1}$ com o hiperplano perpendicular ao vetor $\boldsymbol{e} = (1, \ldots, 1)$, isto é

$$A_n = \mathbb{Z}^{n+1} \cap \boldsymbol{e}^{\perp} = \left\{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} : x_1 + \ldots + x_{n+1} = 0\right\}.$$

Uma possível matriz geradora é dada por

$$\begin{pmatrix} -1 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}. \tag{1.11}$$

Daí deduzimos que $\lambda(A_n) = \sqrt{2}$ e $\delta(A_n) = 2^{-n/2}(n+1)^{-1/2}$. O dual de A_n, A_n^*, é a projeção de $\mathbb{Z}^{n+1}$ no hiperplano ortogonal ao vetor $\boldsymbol{e}$, o que pode ser visto como uma consequência da Proposição 3.1.4 do Capítulo 3.

O reticulado hexagonal ilustrado no Exemplo 1.1.3 é uma representação em $\mathbb{R}^2$ de A_2. Assim como A_2, o reticulado hexagonal é isodual. A_2 possui a melhor densidade entre qualquer empacotamento no plano (não necessariamente reticulado).

O Reticulado D_n

O reticulado D_n é o conjunto de todos os vetores inteiros em $\mathbb{R}^n$ cuja soma das suas coordenadas é par. Em outras palavras,

$$D_n = \{(x_1, \dots, x_n) \in \mathbb{Z}^n : x_1 + \dots + x_n = 0 \pmod 2\}.$$

Uma matriz geradora para D_n é

$$\begin{pmatrix} 2 & 0 & 0 & \dots & 0 & 0 \\ 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}, \tag{1.12}$$

de onde concluímos que $\lambda(D_n) = \sqrt{2}$ e $\delta(D_n) = 2^{-(n+2)/2}$. Na linguagem do Capítulo 2, D_n pode ser visto como a Construção A binária de um código consistindo de todos os elementos de $\mathbb{Z}_2^n$ cuja soma das suas coordenadas é par. O

reticulado D_n^* possui matriz geradora

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 1/2 & 1/2 & 1/2 & \dots & 1/2 & 1/2 \end{pmatrix}, \tag{1.13}$$

norma mínima $\lambda(D_n^*) = 1$, se $n \geq 4$ e $\lambda(D_3^*) = \sqrt{3}/2$, densidade de centro $\delta(D_n^*) = 2^{-(n-1)}$ se $n \geq 4$ e $\delta(D_3^*) = 2^{-5}\sqrt{27}$. O reticulado $D_3 \sim A_3$ é também chamado de *cúbico de face centrada* e é o empacotamento mais denso em $\mathbb{R}^3$ (não necessariamente reticulado). O sistema periódico D_n^+ é definido como

$$D_n^+ = D_n \bigcup \left(D_n + \left(\frac{1}{2}, \dots, \frac{1}{2} \right) \right). \tag{1.14}$$

É fácil ver que D_n^+ é um reticulado se, e somente se, n é par. D_3^+ é também conhecido como empacotamento *tetraedral* ou *diamante*.

Os reticulados E_6, E_7 e E_8

Chamamos de $E_8 = D_8^+$ o reticulado constituído pelos pontos $(x_1, \dots, x_8)$ tais que todo $x_i \in \mathbb{Z}$ ou todo $x_i \in \mathbb{Z} + 1/2$. Este é o reticulado mais denso em dimensão 8. Uma matriz geradora para E_8 é dada por

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}, \tag{1.15}$$

sua norma mínima é $\lambda(E_8) = \sqrt{2}$ e sua densidade de centro é $\delta(E_8) = 1/16$. Pode-se mostrar que $E_8 = E_8^*$. Os reticulados E_6 e E_7 são definidos como:

$$E_7 = E_8 \cap (1, \ldots, 1)^\perp \text{ e } E_6 = E_8 \cap H^\perp,$$

onde H é o sub-espaço vetorial gerado por $(1, 0, \ldots, 0, 1)$ e $(1/2, \ldots, 1/2)$. Similarmente ao caso de A_n, esta definição caracteriza E_6^* e E_7^* como projeções de E_8 nos subespaços $(1, \ldots, 1)^\perp$ e $H^\perp$, pela Proposição 3.1.4.

Finalizamos esta seção com uma tabela dos empacotamentos reticulados mais densos em dimensão $n = 1$ até 8. Estes são também os empacotamentos (gerais) *conhecidamente* mais densos nestas dimensões, e apenas demonstradamente mais densos para $n = 1, 2$, e 3.

Dimensão	1	2	3	4	5	6	7	8
Reticulado	$\mathbb{Z}$	A_2	D_3	D_4	D_5	E_6	E_7	E_8

Tabela 1.1: Empacotamentos reticulados mais densos em dimensões 1 até 8

1.4 Decodificação

Como uma regra geral, problemas envolvendo propriedade algébricas de reticulados (como encontrar matrizes geradoras com estrutura especial ou determinar o determinante de um reticulado) costumam ser computacionalmente mais simples, enquanto problemas geométricos são mais complexos.

Um problema geométrico foi visto na seção anterior: dado um inteiro $n > 1$, encontrar o reticulado de dimensão n mais denso. Outra questão, relacionada a esta, é a seguinte. Dado um reticulado Λ, descrito pela sua matriz geradora B, quanto vale $\delta(\Lambda)$? Para responder a esta pergunta, necessitamos calcular

$$\lambda(\Lambda) = \min_{\boldsymbol{x} \in \Lambda} \|\boldsymbol{x}\|_2 .$$

O problema de encontrar $\lambda(\Lambda)$ é conhecido com o problema do vetor mais curto (SVP, do inglês *shortest vector problem*). Tanto o problema acima, como as suas variantes aproximadas, são computacionalmente difíceis (na linguagem de Teoria de Complexidade, o SVP é NP-difícil sob certas hipóteses de aleatorização [MG02, Cap. 4])

Nesta tese, damos especial atenção a um outro problema geométrico, o de *decodificação*, que recebe este nome devido a sua aplicação em sistemas de transmissão de informação. Para a noção de proximidade, trabalharemos no Capítulo 2 com métricas que não são a euclidiana. De maneira bastante geral, seja $d : \mathbb{R}^n \times \mathbb{R}^n \to [0, \infty)$ uma métrica qualquer, $\Lambda \subset \mathbb{R}^n$ um reticulado e $\boldsymbol{r} \in \mathbb{R}^n$ um ponto qualquer. O problema de decodificação pergunta qual o ponto de Λ mais próximo de $\boldsymbol{r}$, isto é, qual o valor de

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}\in\Lambda} d(\boldsymbol{x}, \boldsymbol{r}).$$

Algoritmos para encontrar o ponto mais próximo dos reticulados D_n, E_6, E_7, E_8 e A_n são descritos em [CS98, Cap. 20]. Para reticulados gerais, não há um algoritmo eficiente que resolva o problema acima [MG02, Cap. 3]. Apesar disso, existem algoritmos universais que comportam-se bem na prática. No *survey* [AEVZ02] é feito um estudo comparativo dos métodos de decodificação mais populares até então.

Capítulo 2

Reticulados q-ários na Métrica l_p

"If you look for perfection, you will never be content."

- Leon Tolstoi, *Anna Karenina*

De todas as construções envolvendo códigos corretores de erros e reticulados, uma das mais utilizadas é a Construção A, que relaciona um código corretor de erro em $\mathbb{Z}_q^n$ e um reticulado em $\mathbb{Z}^n$. Reticulados advindos da Construção A são também chamados de q-ários e possuem diversas aplicações em Teoria da Informação e Criptografia. De fato, grande parte dos reticulados utilizados em esquemas criptográficos são q-ários [MG02]. Isso deve-se ao fato de que, apesar da sua aparente estrutura mais simples, essa classe preserva a dificuldade de diversos problemas computacionais envolvendo reticulados gerais. Do ponto de vista da Teoria da Informação, a Construção A é utilizada para construir bons códigos para o canal gaussiano e para uma boa gama de canais com informação lateral [Zam09].

Neste capítulo, abordamos problemas de reticulados q-ários na métrica l_p. Em geral, não há uma literatura extensa sobre reticulados nessas métricas para $p \neq 1, 2$. Peikert estuda em [Pei08] a complexidade de importantes problemas computacionais para esta classe de reticulados no caso $2 < p \leq \infty$. Em [TYK10], os autores mostram algoritmos ótimos para a busca pelo ponto mais próximo na norma l_p para as famílias $\mathbb{Z}^n$, D_n, A_n, E_6, E_7 e E_8, entretanto não abordam o problema de reticulados q-ários de maneira geral. Em [RS87] são estudados empacotamentos reticulados de bolas na norma l_p com boa densidade.

Ao lidarmos com reticulados q-ários na norma l_p, na tentativa de generalizar um recente resultado sobre a busca pelo ponto mais próximo na métrica de Lee [CJC11], uma nova métrica é naturalmente induzida no espaço $\mathbb{Z}_q^n$ (que também pode ser vista como uma métrica no quociente $\mathbb{Z}^n/q\mathbb{Z}^n$), a qual chamamos p-Lee. Mostramos que a decodificação em um reticulado q-ário na métrica l_pé equialente à decodificação no código associado na métrica p-Lee. Estudamos ao fim do capítulo códigos perfeitos na norma p-Lee e a sua conexão com a famosa Conjectura de Golomb-Welch para códigos na métrica de Lee tradicional.

Os resultados contidos aqui foram parcialmente apresentados no *IEEE Information Theory Workshop*, Paraty-RJ (2011), no *XXX Simpósio Brasileiro de Telecomunicações*, Fortaleza-CE (2012), no *Workshop on Coding and Cryptography*, Bergen, Noruega (2013), e podem ser encontrados em [CJC11] e [JCC13].

2.1 Códigos q-ários na métrica de Lee

O ambiente que utilizaremos para estudar códigos corretores de erro é o espaço $\mathbb{Z}_q^n$, produto cartesiano do anel $\mathbb{Z}_q$ de inteiros módulo q munido da operação de adição usual elemento a elemento. Se q é primo, $\mathbb{Z}_q$ é um corpo e portanto $\mathbb{Z}_q^n$ é um espaço vetorial (sobre $\mathbb{Z}_q$). Caso contrário, $\mathbb{Z}_q^n$ é apenas um $\mathbb{Z}_q$-módulo. Para evitar ambiguidades, denotaremos os elementos de $\mathbb{Z}_q$ por $\left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{q-1}\right\}$ e os vetores de $\mathbb{Z}_q$ através de símbolos em negrito com uma barra, isto é, um elemento de $\mathbb{Z}_q^n$ é tipicamente dado por $\overline{\boldsymbol{x}} = (\overline{x}_1, \ldots, \overline{x}_n)$.

Um *código* (corretor de erros) q-ário $\mathcal{C}$ é um subconjunto de $\mathbb{Z}_q^n$. Dizemos que $\mathcal{C} \subset \mathbb{Z}_q^n$ é linear se ele é fechado para adição e subtração[1]. Códigos lineares são particularmente importantes por possuírem estrutura que facilita sua decodificação e análise. Daqui para frente, trataremos apenas de códigos lineares. Por conta do jargão relacionado a aplicações em Teoria de Informação, vetores de $\mathbb{Z}_q^n$ são também chamados de *palavras* e vetores de um código $\mathcal{C}$ são também

[1] A rigor, necessitamos apenas que $\mathcal{C}$ seja fechado apenas para a adição. Além disso, um subgrupo de $\mathbb{Z}_q^n$ é também um $\mathbb{Z}_q$-submódulo.

chamados de *palavras-código*

Se q é primo, um código linear é um subespaço vetorial de $\mathbb{Z}_q^n$, e podemos encontrar uma base, isto é, vetores linearmente independentes (sobre $\mathbb{Z}_q$) $\boldsymbol{c}_i, i = 1, \ldots, k$, $k \leq n$, que geram todos os vetores de $\mathcal{C}$. Caso contrário, podemos apenas garantir a existência de um conjunto minimal de geradores, não necessariamente linearmente independentes. Uma *matriz geradora* de um código $\mathcal{C}$ é uma matriz cujas linhas formam um conjunto gerador de $\mathcal{C}$. Se q é primo, sempre existe uma matriz geradora da forma sistemática

$$(I_k \ M_{k\times n-k}) .$$

Com o intuito de tornar códigos corretores de erro aplicáveis em Teoria de Informação, é necessário munir $\mathbb{Z}_q^n$ de uma métrica. Sejam $\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}} \in \mathbb{Z}_q^n$. A métrica usual é a de Hamming, definida como:

$$d_H(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = |\{i : \overline{x}_i \neq \overline{y}_i\}| ,$$

isto é, $d_H(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}})$ é a quantidade de coordenadas distintas entre os vetores $\overline{\boldsymbol{x}}$ e $\overline{\boldsymbol{y}}$. Uma das aplicações da métrica de Hamming é o desenvolvimento de códigos para o Canal Binário Simétrico (BSC) e para o Canal de Apagamento (BEC), dois modelos de transmissão de informação largamente utilizados na prática. A literatura da métrica de Hamming é extremamente extensa, e existem diversas boas referências para o seu estudo (por exemplo, os livros [HP03] e [SM77]). Trataremos aqui de outra métrica, alternativa à de Hamming, proposta por Lee em [Lee58].

Sejam $\overline{x}, \overline{y} \in \mathbb{Z}_q$. Sejam x e y os valores inteiros não negativos entre 0 e $q-1$ associados a $\overline{x}$ e $\overline{y}$ na imersão natural de $\mathbb{Z}_q$ em $\mathbb{Z}$ (isto é, x e y são os menores valores não-negativos tais que $x\overline{1} = \overline{x}$ e $y\overline{1} = \overline{y}$, respectivamente). A *distância de*

Lee entre $\overline{x}$ e $\overline{y}$ é definida como

$$d_{Lee}(\overline{x},\overline{y}) = \min\{|x-y|, q-|x-y|\}. \tag{2.1}$$

A distância de Lee entre dois vetores $\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_q^n$ é definida naturalmente como:

$$d_{Lee}(\overline{\boldsymbol{x}},\overline{\boldsymbol{y}}) = \sum_{i=0}^{n} \min\{|x_i-y_i|, q-|x_i-y_i|\} = \sum_{i=0}^{n} d_{Lee}(\overline{x}_i,\overline{y}_i). \tag{2.2}$$

A fórmula (2.1) corresponde ao número de arestas do menor caminho entre $\overline{x}$ e $\overline{y}$ no grafo cujos vértices estão rotulados por $0,\ldots,q-1$ e tal que existe uma aresta entre $\overline{x}$ e $\overline{y}$ se, e somente se, $\overline{x}-\overline{y}=\overline{1}$. Com esta caracterização, mostra-se facilmente que a a distância de Lee é efetivamente uma função de distância.

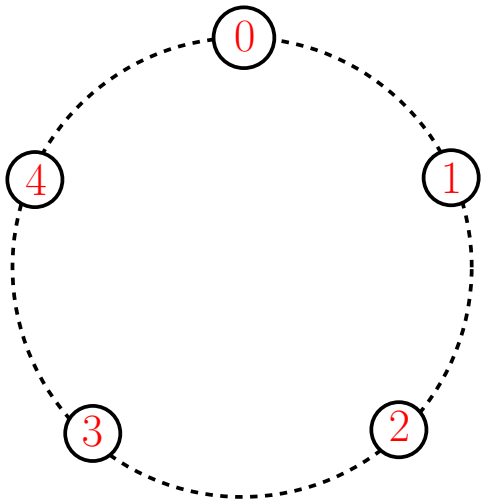


Figura 2.1: Grafo representando a distância de Lee em $\mathbb{Z}_5$

Observação 2.1.1. *Para $q=2,3$, a métrica de Lee coincide com a métrica de Hamming.*

2.1.1 Reticulados q-ários: Construção A

A chamada Construção A estendida para códigos q-ários é provavelmente a maneira mais natural de associarmos um código $\mathcal{C} \subset \mathbb{Z}_q^n$ a um reticulado inteiro (isto

é, um reticulado $\Lambda \subset \mathbb{Z}^n$) e pode ser descrita conforme mostrado a seguir. Seja ϕ a aplicação sobrejetiva

$$\begin{aligned} \phi : \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, \ldots, x_n) &\longmapsto (\overline{x_1}, \ldots, \overline{x_n}), \end{aligned} \tag{2.3}$$

onde $\overline{x_i} = x_i \pmod q$ para $i = 1, \ldots, n$. Dado um código $\mathcal{C} \in \mathbb{Z}_q^n$, definimos $\Lambda_A(\mathcal{C})$ como a imagem inversa de $\mathcal{C}$ por ϕ, isto é $\Lambda_A(\mathcal{C}) = \phi^{-1}(\mathcal{C})$. É fácil ver que $\Lambda_A(\mathcal{C})$ é um reticulado se, e somente se, $\mathcal{C}$ é um código linear. Com efeito, se $\mathcal{C}$ é um código linear, como ϕ é um homomorfismo de grupos, $\phi^{-1}(\mathcal{C})$ é fechado para adição/subtração e é discreto (pois é um subconjunto de $\mathbb{Z}^n$), portanto $\Lambda_A(\mathcal{C})$ é um reticulado. Por outro lado, se $\mathcal{C}$ não é linear, então existem $\overline{x} = \phi(x)$ e $\overline{y} = \phi(y)$ tais que $\overline{x}, \overline{y} \in \mathcal{C}$ mas $\overline{x} + \overline{y} = \phi(x + y) \notin \mathcal{C}$. Isso implica que $x + y \notin \phi^{-1}(\mathcal{C}) = \Lambda_A(\mathcal{C})$, ou seja $\Lambda_A(\mathcal{C})$ não é fechado para adição e portanto não é um reticulado.

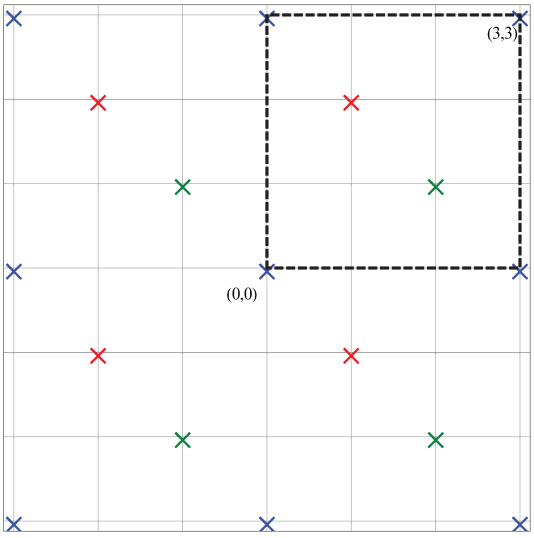


Figura 2.2: Construção A do código 3-ário $\mathcal{C} = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{2}), (\overline{2}, \overline{1})\}$. Os pontos com mesma cor são representantes de classes idênticas em $\Lambda_A(\mathcal{C})/3\mathbb{Z}^2$

Dizemos que $\Lambda_A(\mathcal{C})$ é o *reticulado q-ário* associado a $\mathcal{C}$. Como $\ker \phi = \phi^{-1}(\{\overline{\mathbf{0}}\}) = q\mathbb{Z}^n$, todos os reticulados q-ários contém $q\mathbb{Z}^n$ como sub-reticulado e o quociente $\Lambda_A(\mathcal{C})/q\mathbb{Z}^n$ é isomorfo a $\mathcal{C}$. $\Lambda_A(\mathcal{C})$ é sempre um reticulado de posto

completo e pode ser visto como o conjunto de translações do código $\mathcal{C}$ (imerso em $\mathbb{R}^n$) por vetores com coordenadas múltiplas de q, como mostrado na Figura 2.2. Uma condição necessária e suficiente para que um reticulado Λ seja q-ário é a de que $\mathbb{Z}^n \subset \Lambda \subset q\mathbb{Z}^n$, para algum q.

Algumas propriedades da Construção A utilizadas neste trabalho são dadas na seguinte proposição:

Proposição 2.1.2. *Seja $\Lambda_A(\mathcal{C})$ o reticulado q-ário associado a um código $\mathcal{C} \subset \mathbb{Z}_q^n$. Valem as seguintes propriedades:*

(i) O número de palavras de $\mathcal{C}$ é dado por

$$|\mathcal{C}| = \left|\frac{\Lambda_A(\mathcal{C})}{q\mathbb{Z}^n}\right| = \frac{q^n}{\sqrt{\det(\Lambda_A(\mathcal{C}))}}.$$

(ii) Se $\mathcal{C}$ é gerado pela matriz $\begin{pmatrix} I_{k\times k} & M_{k\times(n-k)} \end{pmatrix}$, então

$$B = \begin{pmatrix} I_{k\times k} & M_{k\times(n-k)} \\ 0_{(n-k)\times k} & qI_{(n-k)\times(n-k)} \end{pmatrix} \tag{2.4}$$

é uma matriz geradora para $\Lambda_A(\mathcal{C})$.

(iii) Todo reticulado $\Lambda \subset \mathbb{Z}^n$ é q-ário, para algum q, $1 \leq q \leq \sqrt{\det \Lambda}$.

Demonstração. A propriedade (i) segue diretamente do isomorfismo entre $\mathcal{C}$ e $\Lambda_A(\mathcal{C})/q\mathbb{Z}^n$ e da Proposição 1.1.6.

(ii) Seja $\boldsymbol{u}B = \boldsymbol{x} \in \Lambda(B)$, para $\boldsymbol{u} \in \mathbb{Z}^n$. Particionando $\boldsymbol{u} = (\boldsymbol{u}_1\ \boldsymbol{u}_2)$, onde $\boldsymbol{u}_1$ é constituído pelas k primeiras coordenadas de $\boldsymbol{u}$, segue que $\boldsymbol{u}B = (\boldsymbol{u}_1\ \boldsymbol{u}_1M) + (0\ q\boldsymbol{u}_2)$, e portanto temos diretamente que $\phi(\boldsymbol{x}) = \overline{\boldsymbol{u}_1}(I\ M) \in \mathcal{C}$, assim $\boldsymbol{x} \in \Lambda_A(\mathcal{C})$. Reciprocamente, se $\boldsymbol{x} \in \Lambda_A(\mathcal{C})$, então $\boldsymbol{x} = \boldsymbol{u}_1(I\ M) + q\boldsymbol{y} = (\boldsymbol{u}_1 + q\boldsymbol{y}_1\ \boldsymbol{u}_1M + q\boldsymbol{y}_2)$, onde $\boldsymbol{y} = (\boldsymbol{y}_1\ \boldsymbol{y}_2) \in \mathbb{Z}^n$. Tomando $\hat{\boldsymbol{u}}_1 = \boldsymbol{u}_1 + q\boldsymbol{y}_1$ e $\hat{\boldsymbol{u}}_2 = -\boldsymbol{y}_1M + \boldsymbol{y}_1$, segue que $\boldsymbol{x} = (\hat{\boldsymbol{u}}_1\ \ \hat{\boldsymbol{u}}_2)B$, ou seja, $\boldsymbol{x} \in \Lambda(B)$.

(iii) A terceira propriedade vem do fato de que $\Lambda \subset \mathbb{Z}^n$ possui matriz geradora B com todas as entradas inteiras, e portanto $|\det B| = \sqrt{\det \Lambda}$ também é inteiro. Tome $q = \sqrt{\det \Lambda}$ e considere o sistema linear $\boldsymbol{x}B = q\boldsymbol{z}$. O sistema sempre possui solução, dada por

$$\boldsymbol{x} = q\boldsymbol{z}B^{-1} = q\boldsymbol{z}\,\frac{\mathrm{adj}(B)}{\det B} = \pm\boldsymbol{z}\ \mathrm{adj}(B),$$

onde $\mathrm{adj}(B)$ é a matriz adjunta de B (isto é, $(-1)^{i+j}(\mathrm{adj}B)_{ij}$ é o determinante da matriz excluindo a linha j e coluna i de B). Isso nos mostra mostrando que $q\mathbb{Z}^n \subset \Lambda$ e portanto Λ é um reticulado q-ário. □

A última propriedade da proposição acima nos mostra que qualquer reticulado inteiro é q-ário. Como qualquer reticulado racional (isto é, contido em $\mathbb{Q}^n$) é, através de uma mudança de escala, equivalente a um reticulado inteiro, então é intuitivo que qualquer reticulado no $\mathbb{R}^n$ esteja arbitrariamente próximo de algum reticulado q-ário (noções mais precisas de proximidade serão dadas no Capítulo 3). Assim, é intuitivo pensar que os reticulados q-ários são de uma certa forma densos na classe de reticulados, a menos de equivalências.

Exemplo 2.1.3 (Reticulado E_8)**.** *Revisitamos aqui o Reticulado E_8 descrito na Seção 1.3. Seja $\mathcal{H}_8$ o código de Hamming estendido descrito em [CS98, p.80], que possui matriz geradora equivalente na forma sistemática dada por*

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

De acordo com a proposição acima, obtemos como matriz geradora para $\Lambda_A(\mathcal{H}_8)$:

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

$\Lambda_A(\mathcal{H}_8)$ *é, a menos de rotações e uma mudança de escala, o reticulado* E_8.

2.2 A Métrica p-Lee

Consideramos a partir de agora uma extensão da métrica de Lee. Sejam dois vetores $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^n$. A distância l_p, $p \geq 1$, usual entre $\boldsymbol{x}$ e $\boldsymbol{y}$ é dada por:

$$d_p(\boldsymbol{x}, \boldsymbol{y}) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p}.$$

No caso $p = \infty$, a distância l_∞ é definida como:

$$d_\infty(\boldsymbol{x}, \boldsymbol{y}) = \max\{|x_i - y_i|;\ i = 1, \ldots, n\}.$$

A métrica de Lee (2.2) pode ser vista como a distância induzida pela métrica l_1 no quociente $\mathbb{Z}^n/q\mathbb{Z}^n$. A generalização da métrica de Lee considerada aqui é a aplicação $d_{p,Lee} : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \to \mathbb{R}$,

$$d_{p,Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{y}_i))^p \right)^{1/p}, \tag{2.5}$$

onde $d_{Lee}(\overline{x}, \overline{y})$ é dado por (2.1). Tal aplicação define uma métrica em $\mathbb{Z}_q^n$, a qual chamamos de métrica p-Lee. A demonstração deste fato segue do resultado mais

geral a seguir.

Proposição 2.2.1. *Considere (X, d) um espaço métrico e X^n o produto cartesiano de X, $n \in \mathbb{N}$. A aplicação $\tilde{d} : X^n \times X^n \to [0, \infty)$ dada por*

$$\tilde{d}(\boldsymbol{x}, \boldsymbol{y}) = \left(\sum_{i=1}^{n} d(x_i, y_i)^p \right)^{1/p}.$$

é uma métrica em X^n (em outras palavras, $(X^n, \tilde{d})$ é um espaço métrico).

Demonstração. As condições de simetria e positividade são imediatas. Para a desigualdade triangular, sejam $\boldsymbol{x}, \boldsymbol{y}$ e $\boldsymbol{z} \in X^n$. Como a métrica d satisfaz a desigualdade triangular, temos

$$d(x_i, y_i)^p \leq (d(x_i, z_i) + d(z_i, y_i))^p.$$

Assim

$$\begin{aligned} \tilde{d}(\boldsymbol{x}, \boldsymbol{y}) = \left(\sum_{i=1}^{n} d(x_i, y_i)^p \right)^{1/p} &\leq \left(\sum_{i=1}^{n} (d(x_i, z_i) + d(z_i, y_i))^p \right)^{1/p} \\ &\overset{(a)}{\leq} \left(\sum_{i=1}^{n} d(x_i, z_i)^p \right)^{1/p} + \left(\sum_{i=1}^{n} d(z_i, y_i)^p \right)^{1/p} \\ &= \tilde{d}(\boldsymbol{x}, \boldsymbol{z}) + \tilde{d}(\boldsymbol{z}, \boldsymbol{y}), \end{aligned}$$

em que (a) segue da Desigualdade de Minkowski para espaços l_p. □

Tomando $\tilde{d} = d_{p,Lee}$ e $X = \mathbb{Z}_q$ na proposição acima, segue imediatamente:

Proposição 2.2.2. *Sejam $1 \leq p < \infty$ e $\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}} \in \mathbb{Z}_q^n$. A aplicação $d_{p,Lee} : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \to \mathbb{R}$ dada por*

$$d_{p,Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{y}_i))^p \right)^{1/p},$$

onde $d_{Lee}(\overline{x}, \overline{y})$ define uma métrica em $\mathbb{Z}_q^n$.

Chamamos a métrica descrita acima de *métrica p-Lee*. Note que a métrica de Lee é a métrica p-Lee para $p = 1$. No caso em que $p = \infty$, temos uma proposição similar, definindo

$$d_\infty(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \max\{d_{Lee}(x_i, y_i);\ i = 1, \ldots, n\}.$$

A seguir, mostramos uma outra maneira de provar que $d_{p,Lee}$ é uma métrica, um pouco mais esclarecedora. A *distância induzida* entre $\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}$ vistos como elementos do quociente $\mathbb{Z}^n/q\mathbb{Z}^n$ é definida como a menor distância entre representantes da classe de $\bar{\boldsymbol{x}}$ e de $\bar{\boldsymbol{y}}$, isto é:

$$d_{ind}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \inf\{d_p(\boldsymbol{x}^*, \boldsymbol{y}^*);\ \ \boldsymbol{x}^* = \boldsymbol{x} + q\boldsymbol{t},\ \boldsymbol{y}^* = \boldsymbol{y} + q\boldsymbol{w};\ \ \boldsymbol{t}, \boldsymbol{w} \in \mathbb{Z}^n\}. \tag{2.6}$$

O seguinte resultado é válido:

Proposição 2.2.3. *Se $\overline{\boldsymbol{x}}$ e $\overline{\boldsymbol{y}}$ são dois elementos em $\mathbb{Z}_q^n \simeq \mathbb{Z}^n/q\mathbb{Z}^n$, então:*

$$d_{p,Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = d_{ind}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}). \tag{2.7}$$

Demonstração.

$$\begin{aligned} d(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) &= \inf\{d_p(\boldsymbol{x}^*, \boldsymbol{y}^*);\ \ \boldsymbol{x}^* = \boldsymbol{x} + q\boldsymbol{t},\ \boldsymbol{y}^* = \boldsymbol{y} + q\boldsymbol{w};\ \ \boldsymbol{t}, \boldsymbol{w} \in \mathbb{Z}^n\} \\ &= \inf\left\{ \left(\sum_{i=1}^{n} |x_i - y_i - q(w_i - t_i)|^p \right)^{\frac{1}{p}};\ \ \boldsymbol{t}, \boldsymbol{w} \in \mathbb{Z}^n \right\} \\ &= \left(\sum_{i=1}^{n} \left| x_i - y_i - q \left\lceil \frac{x_i - y_i}{q} \right\rfloor \right|^p \right)^{\frac{1}{p}}, \end{aligned}$$

onde a última igualdade segue do fato de que $\displaystyle\sum_{i=1}^{n} |x_i - y_i - qs_i|^p$ assume valor mínimo quando $s_i = \left\lceil \frac{x_i - y_i}{q} \right\rfloor$.

Seja $\alpha_i = \left\lceil \dfrac{x_i - y_i}{q} \right\rfloor$, $i = 1, \cdots, n$. Como $0 \leq |x_i - y_i| < q$, segue que $\alpha_i \in \{-1, 0, 1\}$. Analisando os três casos:

- Se $\alpha_i = 0$ para algum i, então $-q/2 \leq x_i - y_i \leq q/2$, o que implica $\min\{|x_i - y_i|, q - |x_i - y_i|\} = |x_i - y_i|$.
- Se $\alpha_i = 1$ para algum i, então $q/2 < x_i - y_i \leq q$ e portanto $\min\{|x_i - y_i|, q - |x_i - y_i|\} = q - |x_i - y_i|$ e $|x_i - y_i| = x_i - y_i$.
- Se $\alpha_i = -1$ para algum i, então $-q \leq x_i - y_i < -q/2$ e portanto $\min\{|x_i - y_i|, q - |x_i - y_i|\} = q - |x_i - y_i|$ and $|x_i - y_i| = -(x_i - y_i)$.

Assim, nos três casos $|x_i - y_i - q\alpha_i| = d_{Lee}(\overline{x_i}, \overline{y_i})$, e o resultado segue. □

A distância mínima de um código na métrica p-Lee é definida como

$$d_{p,Lee}(\mathcal{C}) = \min_{\substack{\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}} \in \mathcal{C} \\ \overline{\boldsymbol{x}} \neq \overline{\boldsymbol{y}}}} d_{p,Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}).$$

Na métrica de Lee, o raio de empacotamento de um código é definido com o maior valor inteiro tal que as bolas centradas em palavra-código são, duas a duas, disjuntas. Para estender essa definição para a métrica p-Lee precisamos de algumas sutilezas, já que a distância $d_{p,Lee}(\boldsymbol{x}, \boldsymbol{y})$ entre duas palavras, em geral, pode não ser inteira (ainda que $d_{p,Lee}(\boldsymbol{x}, \boldsymbol{y})^p$ seja sempre inteiro inteiro). Tendo em vista isso, seja

$$B_{p,Lee}(\overline{\boldsymbol{x}}, R) = \left\{ \overline{\boldsymbol{y}} \in \mathbb{Z}_q^n : d_{p,Lee}(\overline{\boldsymbol{y}}, \overline{\boldsymbol{x}}) \leq R \right\}$$

a bola centrada em $\boldsymbol{x}$ na métrica p-Lee. O raio de empacotamento de $\mathcal{C}$ é dado pelo maior R tal que:

(i) $B_{p,Lee}(\overline{\boldsymbol{x}}, R) \bigcap B_{p,Lee}(\overline{\boldsymbol{y}}, R) = \emptyset$, para quaisquer $\boldsymbol{x} \neq \boldsymbol{y}$, $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$.

(ii) Existe $\overline{\boldsymbol{x}} \in \mathcal{C}$ e $\overline{\boldsymbol{y}} \in \mathbb{Z}_q^n$, tais que $d_{p,Lee}(\boldsymbol{y}, \boldsymbol{x}) = R$.

Note que R^p é sempre um inteiro que pode ser escrito como soma de inteiros elevados a p. O objetivo da condição (ii) é evitar ambiguidades já que, a priori, poderia haver mais que um valor de R com R^p inteiro tal que a condição (i) seja satisfeita. Além disso, a condição (ii) evita que utilizemos raios desnecessariamente grandes. No caso da métrica de Lee, é um resultado clássico o fato de que

$$R = \left\lfloor \frac{d_{Lee} - 1}{2} \right\rfloor .$$

Para a métrica p-Lee este resultado não é válido, como pode ser visto no exemplo abaixo:

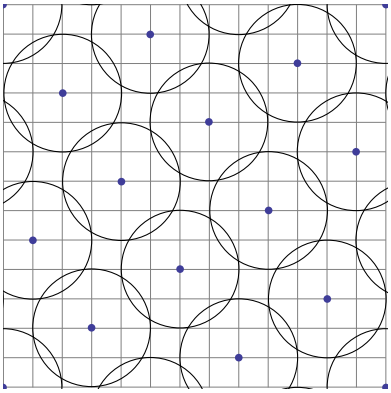


Figura 2.3: Raio de empacotamento na métrica 2-Lee

Exemplo 2.2.4. *Considere o código* 13*-ário* $C = \langle(\overline{1}, \overline{5})\rangle$*. Para* $p = 2$*,* $d_{2,Lee}(\mathcal{C}) = \sqrt{13}$ *e* $\lfloor (d_{2,Lee}(\mathcal{C}) - 1)/2 \rfloor = 1$*, mas o raio de empacotamento* $R = 2$*, (Fig. 2.3). Além disso* R *é estritamente maior que* $d_{Lee,2}/2 \simeq 1.8$*.*

Um resultado útil para as construções de códigos perfeitos no fim deste capítulo é o de que a norma l_p mínima de um reticulado q-ário $\Lambda_A(\mathcal{C})$ satisfaz [RS87]

$$\lambda_p = \min\{d_{p,Lee}(\mathcal{C}), q\}. \tag{2.8}$$

2.2.1 Decodificação de reticulados na métrica l_p

Nesta seção mostraremos que encontrar o ponto $\boldsymbol{z}$ mais próximo de $\boldsymbol{x} \in \Lambda_A(\mathcal{C})$ é equivalente a encontrar o ponto mais próximo de $\overline{\boldsymbol{x}} \in \mathcal{C}$, isto é, decodificar em um reticulado q-ário é equivalente a decodificar no código q-ário associado. Isso nos dá um algoritmo para decodificar em $\Lambda_A(\mathcal{C})$ utilizando como sub-rotina um decodificador em $\mathcal{C}$, e é particularmente útil quando o código possui um algoritmo de decodificação eficiente (por exemplo quando a dimensão de $\mathcal{C}$ é pequena, ou em classes de códigos conhecidas, como é o caso da métrica de Lee, para $p = 1$).

Proposição 2.2.5. *[JCC13] Seja $\Lambda_A(\mathcal{C})$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{Z}^n$. Suponhamos que $\overline{\boldsymbol{c}} \in \mathcal{C}$ seja uma palavra mais próxima de $\overline{\boldsymbol{r}}$ na métrica p-Lee. Um elemento $\boldsymbol{z} \in \Lambda_A(\mathcal{C})$ mais próximo de $\boldsymbol{r}$ na distância l_p é dado por $\boldsymbol{z} = (z_1, \cdots, z_n)$, onde*

$$z_i = c_i + qw_i \text{ e } w_i = \left\lceil \frac{r_i - c_i}{q} \right\rfloor, i = 1, \ldots n$$

Demonstração. Faremos a demonstração para $1 \leq p < \infty$ (o caso $p = \infty$ é análogo). Considere a classe de equivalência de $\overline{\boldsymbol{x}}$ dada por $\{\boldsymbol{x} + q\boldsymbol{w},\ \boldsymbol{w} \in \mathbb{Z}^n\}$. Pelos mesmos argumentos da Proposição 2.2.3, o ponto mais próximo de $\boldsymbol{r}$ nesta classe é obtido quando

$$w_i = \left\lceil \frac{r_i - x_i}{q} \right\rfloor, i = 1, \ldots, n.$$

e sua distância até $\boldsymbol{x}$ é dada por

$$\begin{aligned} d_p(\boldsymbol{r}, \boldsymbol{z}) &= \left(\sum_{i=1}^{n} \left| {r_i}^* + qt_i - x_i - q \left\lceil \frac{r_i - x_i}{q} \right\rfloor \right|^p \right)^{\frac{1}{p}} \\ &= \left(\sum_{i=1}^{n} \left| {r_i}^* - x_i - q \left(\left\lceil \frac{r_i^* - x_i}{q} + t_i \right\rfloor - t_i \right) \right|^p \right)^{\frac{1}{p}} \end{aligned}$$

$$= \left(\sum_{i=1}^{n} \left| {r_i}^* - x_i - q \left(\left\lceil \frac{r_i^* - x_i}{q} \right\rfloor \right) \right|^p \right)^{\frac{1}{p}}$$
$$= d_{p,Lee}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{z}}).$$

Por hipótese, $\overline{\boldsymbol{c}} \in \mathcal{C}$ satisfaz $d_{p,Lee}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{c}}) = \min\{d_{p,Lee}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{x}}), \overline{\boldsymbol{x}} \in \mathcal{C}\}$. Para $w_i = \left\lceil \frac{r_i - c_i}{q} \right\rfloor$ segue que $d_p(\boldsymbol{r}, \boldsymbol{c} + q\boldsymbol{w}) = d_{p,Lee}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{c}}) \leq \min\{d_p(\boldsymbol{r}, \boldsymbol{x} + q\boldsymbol{t}), \overline{\boldsymbol{x}} \in \mathcal{C}, \boldsymbol{t} \in \mathbb{Z}^n\}$, ou seja $\boldsymbol{c} + q\boldsymbol{w}$ é o elemento de $\Lambda_A(\mathcal{C})$ mais próximo de $\boldsymbol{r}$ na distância l_p. □

Observação 2.2.6. *A proposição acima só nos mostra como decodificar pontos com todas as coordenadas inteiras. Para decodificar qualquer $\boldsymbol{r} \in \mathbb{R}^n$, necessitaríamos de um algoritmo em $\mathcal{C}$ que fosse capaz de decodificar qualquer ponto no quociente $\mathbb{R}^n/q\mathbb{Z}^n$, que é isomorfo à caixa $[0, q)^n$. Para $q = 2$ e a métrica de Hamming, tais algoritmos são conhecidos como Soft-decoding (cf. [CS98, Ch. 12]).*

Algoritmo 1 Encontrar o ponto mais próximo em $\Lambda_A(\mathcal{C})$

1: AchaMaisProximo($\Lambda_A(\mathcal{C}), \boldsymbol{r} = (r_1, \ldots, r_n)$)
2: $\overline{\boldsymbol{r}} \leftarrow \boldsymbol{r}$ (mod q)
3: Encontre $\overline{\boldsymbol{c}} = (x_1, \ldots, x_n) \in C$ mais próximo a $\overline{\boldsymbol{r}}$ na métrica p-Lee
4: **para** $i : 1, \ldots, n$ **faça**
5:
6: $w_i \leftarrow \left\lceil \frac{r_i - x_i}{q} \right\rfloor$
7: **fim para**
8: **retorna** $z_i = x_i + qw_i$.
9: **fim**

A Proposição 2.2.5 nos permite descrever o algoritmo de decodificação 2. Além da decodificação em $\mathcal{C}$, o custo do algoritmo acima envolve $\Theta(n)$ operações aritméticas e portanto, de uma maneira geral, o procedimento mais caro é decodificar em $\mathcal{C}$.

Exemplo 2.2.7. *Seja o código cíclico 13-ário em $\mathbb{Z}_{13}^2$, gerado pelo vetor $(\overline{1}, \overline{5})$, isto é:*

$$\mathcal{C} = \left\{ j(\overline{1}, \overline{5}), j = 0, \ldots, 12 \right\}.$$

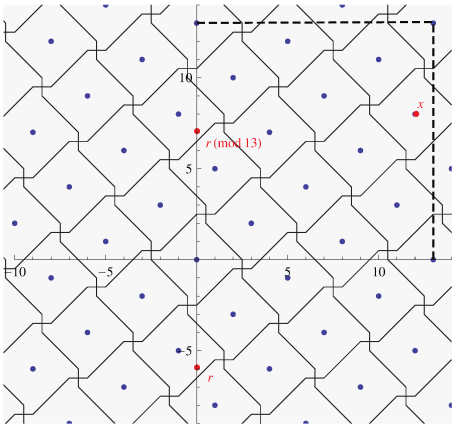


Figura 2.4: Decodificação na Métrica de Lee

A distância mínima de $\mathcal{C}$ vale $d_{p,Lee}(\mathcal{C}) = (2^p + 3^p)^{1/p}$. Seja $\boldsymbol{r} = (0, -6)$. A palavra-código mais próxima a $\overline{\boldsymbol{r}} = (\overline{0}, \overline{7})$ é $(\overline{12}, \overline{8})$. Assim, na notação da Proposição 2.2.5, $w_1 = w_2 = -1$ e o ponto de $\Lambda_A(\mathcal{C})$ mais próximo de $\boldsymbol{r}$ é $\boldsymbol{z} = (-1, -5)$. A Figura 2.4 ilustra esse processo.

Exemplo 2.2.8. *Considere $\mathcal{C}$ o código BCH na métrica de Lee (ou 1-Lee) definido no anel $\dfrac{\mathbb{Z}_4[x]}{\langle f(x)\rangle}$, onde $f(x) = x^3 + x + 1$ [AIPJ03], com matriz de paridade*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha^5 & \alpha & 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^4 \end{pmatrix}^t,$$

onde $\alpha = \beta^2$ e β é uma raiz de $f(x)$. A partir da matriz geradora do código [AIPJ03], podemos derivar uma matriz geradora para o reticulado 4-ário $\Lambda_A(\mathcal{C})$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 3 & 4 & 0 & 0 & 0 \\ 1 & 3 & 2 & 0 & 4 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 4 & 0 \\ 3 & 2 & 1 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

Seja $\boldsymbol{r} = (0, 7, 4, 8, 0, 12, 0)^t$. *Utilizando o algoritmo em [AIPJ03], obtemos que o ponto de* $\mathcal{C}$ *mais próximo de* $\overline{\boldsymbol{r}} = (\overline{0}, \overline{3}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0})$ *é* $\overline{\boldsymbol{x}} = (\overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0})$. *Assim, na notação da Proposição 2.2.5,*

$$w_i = 0, \text{ para } i = 1, 5, 7,$$

$$w_2 = \left\lceil \frac{7}{4} \right\rceil = 2, w_3 = \left\lfloor \frac{4}{4} \right\rceil = 1, w_4 = \left\lfloor \frac{8}{4} \right\rceil = 2, \text{ e } w_6 = \left\lfloor \frac{12}{4} \right\rceil = 3.$$

Deste modo, $\boldsymbol{z} = (0, 0, 0, 0, 0, 0, 0)^t + 4(0, 2, 1, 2, 0, 3, 0) = (0, 8, 4, 8, 0, 12, 0)$ *é o ponto mais próximo de* $\boldsymbol{r}$ *no reticulado q-ário.*

2.2.2 Códigos perfeitos na métrica p-Lee

Alguns códigos possuem a propriedade de que as bolas centradas em palavras-código com raio igual ao seu raio de empacotamento preenchem todo o espaço $\mathbb{Z}_q^n$, e portanto possuem a maior cardinalidade possível, fixado este raio. Esses códigos são chamados de códigos perfeitos e vêm sendo vastamente estudados na literatura, com respeito a diversas métricas.

Formalmente, seja d uma métrica em $\mathbb{Z}_q^n$ e $\mathcal{C}$ um código. Se $\mathcal{C}$ possui a propriedade de que, para quaisquer $\overline{\boldsymbol{x}} \in \mathbb{Z}_q^n$ existe uma e apenas uma palavra-código $\overline{\boldsymbol{y}} \in \mathcal{C}$ tal que $d(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) \leq R$, dizemos que $\mathcal{C}$ é um *código perfeito* com raio R. Os códigos perfeitos triviais são constituídos pelo espaço inteiro ($\mathcal{C} = \mathbb{Z}_q^n$) e apenas pelo vetor nulo ($\mathcal{C} = \{\overline{\boldsymbol{0}}\}$).

A caracterização de códigos perfeitos está completamente resolvida no caso da métrica de Hamming [VL75]: os únicos códigos perfeitos além dos triviais e dos códigos de repetição possuem os mesmos parâmetros da família do chamados códigos de Hamming, e os códigos de Golay. No caso da métrica de Lee, por outro lado, o problema encontra-se em aberto, e a Conjectura de Golomb-Welch [GW70] propõe uma solução.

Definimos, de maneira análoga, códigos perfeitos em $\mathbb{Z}^n$, dada uma métrica

d. O raio de empacotamento é definido da mesma maneira que para a métrica p-Lee. Um subconjunto $\Lambda \subset \mathbb{Z}^n$ é um código perfeito com raio R se, para cada ponto $\boldsymbol{x} \in \mathbb{Z}^n$, existe um e apenas um $\boldsymbol{y} \in \Lambda$ tal que $d(\boldsymbol{x}, \boldsymbol{y}) \leq R$. Se Λ é um reticulado, dizemos que ele é *código perfeito linear*. Tais códigos perfeitos são também chamados de *ladrilhamentos* de $\mathbb{Z}^n$.

A seguinte conjectura sobre códigos perfeitos encontra-se em aberto por quase 45 anos:

Conjectura 2.2.9 ([GW70])**.** *Não existem códigos perfeitos em $\mathbb{Z}^n$ na métrica l_1 para $n > 2$ e $R > 1$.*

Na literatura, geralmente encontramos a Conjectura de Golomb-Welch relacionada à métrica de Lee. Apesar disso, num sentido estrito, a conjectura refere-se a códigos perfeitos na métrica l_1 (também chamada por alguns autores de métrica de Lee em $\mathbb{Z}^n$).

Voltemos nossa atenção às métricas p-Lee. Se $\mathcal{C} \subset \mathbb{Z}_q^n$ é um código perfeito na métrica p-Lee com distância mínima suficientemente pequena (relativamente a q) é intuitivo que $\Lambda_A(\mathcal{C}) \subset \mathbb{Z}^n$ também seja um código perfeito (na métrica l_p). Esse fato encontra-se demonstrado na Prop. 2.2.11. Entretanto, podem existir outros códigos perfeitos em $\mathbb{Z}_q^n$ com distância pequena que não produzem ladrilhamentos de $\mathbb{Z}^n$, como ilustrado no exemplo a seguir.

Exemplo 2.2.10. *O código binário $\mathcal{C} = \{(\overline{0},\overline{0},\overline{0},\overline{0},\overline{0},\overline{0},\overline{0}), (\overline{1},\overline{1},\overline{1},\overline{1},\overline{1},\overline{1},\overline{1})\} \subset \mathbb{Z}_2^7$ é perfeito na métrica de Lee (Hamming), mas o reticulado 2-ário associado não ladrilha $\mathbb{Z}^7$. Para ver isto, basta perceber que a norma mínima de $\Lambda_A(\mathcal{C})$ vale $\lambda(\Lambda_A(\mathcal{C})) = 2$ (e é atingida, por exemplo, por $(2,0,0,0,0,0,0)$). Assim, por exemplo, o vetor $(1,1,1,0,0,0)$ não está em nenhuma das bolas na métrica l_1 centradas em palavras do reticulado.*

Proposição 2.2.11. *Seja $\mathcal{C} \subset \mathbb{Z}_q^n$ um código perfeito na métrica p-Lee com raio de empacotamento R e distância mínima $d_{p,Lee}(\mathcal{C})$. Se $\max\{d_{p,Lee}(\mathcal{C}), 2R\} < q$, então $\Lambda_A(\mathcal{C}) \subset \mathbb{Z}^n$ é um código perfeito na métrica l_p.*

Demonstração. Seja $\boldsymbol{x} \in \mathbb{Z}^n$. Existe um único $\overline{\boldsymbol{c}} \in \mathcal{C}$ tal que $d_{p,Lee}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{c}}) \leq R$. Assim, pelos mesmos argumentos da Proposição 2.2.5, existe $\boldsymbol{c} \in \Lambda_A(\mathcal{C})$ tal que $d_p(\boldsymbol{x}, \boldsymbol{c}) \leq R$. Vamos mostrar que $\boldsymbol{c}$ é único. Suponha o contrário, isto é, que existe $\boldsymbol{c}' \in \mathbb{Z}^n$ tal que $d_p(\boldsymbol{x}, \boldsymbol{c}') \leq R$. Como $\overline{\boldsymbol{c}}$ é único, segue que $\overline{\boldsymbol{c}} = \overline{\boldsymbol{c}}'$, ou seja $\boldsymbol{c} = \boldsymbol{c}' + q\boldsymbol{z}$, $\boldsymbol{z} \in \mathbb{Z}$, o que implica que $d_p(\boldsymbol{c}, \boldsymbol{c}') = d_p(q\boldsymbol{z}, 0) \in q\mathbb{Z}$. Por outro lado,

$$d_p(\boldsymbol{c}, \boldsymbol{c}') \leq d_p(\boldsymbol{c}, \boldsymbol{x}) + d_p(\boldsymbol{y}, \boldsymbol{c}') \leq 2R < q,$$

e portanto $\boldsymbol{c} = \boldsymbol{c}'$. Assim, para qualquer $\boldsymbol{x} \in \mathbb{Z}^n$ existe $\boldsymbol{c} \in \Lambda_A(\mathcal{C})$ tal que $d_p(\boldsymbol{c}, \boldsymbol{x}) \leq R$, ou seja, $\Lambda_A(\mathcal{C})$ é um código perfeito (ou ladrilhamento) em $\mathbb{Z}^n$. □

A condição acima é estrita, no sentido de que se $\max\{d_{p,Lee}(\mathcal{C}), 2R\} = q$ é possível encontrar códigos perfeitos em $\mathbb{Z}_q^n$ que não produzem ladrilhamentos de $\mathbb{Z}^n$. Para $d_{p,Lee}(\mathcal{C}) > q$, isso foi visto no Exemplo 2.2.10. A necessidade de pedirmos também que $2R < q$ é mostrada no simples exemplo abaixo

Exemplo 2.2.12. *Seja $\mathcal{C} = \{(\overline{0}, \overline{0}, \overline{0}), (\overline{1}, \overline{1}, \overline{1}) \in \mathbb{Z}_2^3\}$ na métrica 2-Lee. Temos $d_{2,Lee}(\mathcal{C}) = \sqrt{3} < q$, mas as bolas de raio 1 centradas em palavras-código são disjuntas. Assim, $\mathcal{C}$ é perfeito com $R = 1$, e $2R \geq q > d_{2,Lee}(\mathcal{C})$. O reticulado q-ário associado, $\Lambda_A(\mathcal{C})$, claramente não é um ladrilhamento de $\mathbb{Z}^n$ com $R = 1$. Por exemplo, o vetor $(1, 0, 0)$ está à distância $R = 1$ dos elementos $(0, 0, 0)$ e $(2, 0, 0)$, ambos em $\Lambda_A(\mathcal{C})$.*

Observação 2.2.13. *Na métrica de Lee, $d_{1,Lee}(\mathcal{C}) > 2R$, assim, a condição da Proposição 2.2.11 reduz-se a $d_{1,Lee}(\mathcal{C}) < q$. Uma maneira de simplificar as hipóteses é pedirmos apenas que $2R + 1 > q$.*

Neste capítulo, estamos interessados no estudo de códigos perfeitos com distância mínima menor que q, aos quais estão associados ladrilhamentos de $\mathbb{Z}^n$.

Seja $\mu_p(n, R)$ o número de pontos inteiros na bola da distância l_p com raio R, isto é

$$\mu_p(n, R) = \mathbb{Z}^n \bigcap \{\boldsymbol{x} \in \mathbb{R}^n : d_p(\boldsymbol{x}, \boldsymbol{0}) \leq R\}.$$

Para $p = 1$ [GW70] e $p = \infty$, $\mu_p(n, R)$ possui formas fechadas:

$$\mu_1(n, R) = \sum_{i=0}^{\min\{n,R\}} 2^i \binom{n}{i} \binom{R}{i} \tag{2.9}$$

e

$$\mu_\infty(n, R) = (2R + 1)^n. \tag{2.10}$$

Se $\mathcal{C}$ é um código com raio de empacotamento R, vale o seguinte Limitante do Empacotamento Esférico (e.g., [Etz11, Teo. 1]):

$$|\mathcal{C}|\mu_p(n, R) \leq q^n.$$

A equação acima vale de maneira bastante geral, para qualquer métrica invariante por translação e vem do fato de que

$$\bigcup_{\overline{\boldsymbol{x}} \in C} B_{p,Lee}(\overline{\boldsymbol{x}}, R) \subset \mathbb{Z}_q^n. \tag{2.11}$$

Códigos para os quais vale a igualdade no Limitante do Empacotamento Esférico são perfeitos.

Nos casos restantes da Conjectura de Golomb-Welch, isto é, quando $R = 1$ ou $n = 2$ é fácil exibir códigos perfeitos na métrica de Lee [GW70]. Para $n = 2$, considere o alfabeto $q = R^2 + (R + 1)^2$. A construção A do código q-ário

$$\mathcal{C} = \{(j, (2R + 1)j) : j = 0, 1 \ldots, q - 1\} \subset \mathbb{Z}_q^2$$

é um código perfeito em $\mathbb{Z}^2$ com raio R. Para $R = 1$ e $n > 2$, tome

$$\mathcal{C} = \left\{ (\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_n) : \sum_{i=1}^{n} i c_i \equiv 0 \bmod q \right\} \subset \mathbb{Z}_{2n+1}^n.$$

O reticulado $\Lambda_A(\mathcal{C})$ é um código perfeito na métrica de Lee em $\mathbb{Z}^n$ com raio 1. De fato, $\Lambda_A(\mathcal{C})$ também é perfeito na norma l_p.

Proposição 2.2.14. *[JCC13] Existem códigos perfeitos em $\mathbb{Z}^n$ na distância l_p, $1 \leq p < \infty$, com raio $R = 1$.*

Demonstração. O caso $p = 1$ é um resultado clássico e encontra-se provado em [GW70, Thm. 3] que os códigos exibidos acima são perfeitos. Para $1 < p < \infty$ a equação $|x_1|^p + \ldots + |x_n|^p \leq 1$ tem exatamente $2n+1$ soluções inteiras. Portanto $\mu_p(n,1) = 2n+1 = \mu_1(n,1)$. Como existe um código perfeito na métrica l_1, então esse código também é perfeito na métrica p-Lee, $\leq p < \infty$, pois $|\mathcal{C}|\mu_p(n,1) = |\mathcal{C}|\mu_1(n,1) = q^n$. □

Corolário 2.2.15. *Para $1 \leq p < \infty$, existem códigos perfeitos em $\mathbb{Z}^n_{2n+1}$ na métrica p-Lee para $R = 1$.*

Os valores de q para os quais existem códigos perfeitos em $\mathbb{Z}^n_q$ na métrica ∞-Lee podem ser completamente caracterizados através da seguinte proposição.

Proposição 2.2.16. *[JCC13] Existem códigos perfeitos não triviais em $\mathbb{Z}^n_q$ na métrica ∞-Lee se, e somente se, $q = bm$, com $b > 1$ um inteiro ímpar e $m > 1$ um inteiro.*

Demonstração. Um código $\mathcal{C} \subset \mathbb{Z}^n_q$ com raio de empacotamento R é perfeito na métrica ∞-Lee se, e somente se

$$|\mathcal{C}|(2R+1)^n = q^n. \tag{2.12}$$

(i) Condição necessária: De acordo com a equação acima, se existe um código perfeito $\mathcal{C}$, então $|\mathcal{C}| = \left(\frac{q}{2R+1}\right)^n$. Portanto, $2R+1$ deve dividir q. Excluindo os códigos triviais, q deve ter um fator ímpar maior que 1, mostrando que $q = 2^a$ é impossível. Se q é primo, como $(2R+1)|q$, segue que $2R+1 = q$, o que nos dá um código trivial. Isso mostra que q não pode ser primo nem uma potência de 2, e portanto deve ser da forma dada pela proposição.

(ii) Condição suficiente: seja $q = bm$ com $b > 1$ um inteiro ímpar e $m > 1$ um inteiro. Tomando o código $\mathcal{C}$ gerado pelos vetores

$$\{(\overline{b}, \overline{0}, \ldots, \overline{0}), (\overline{0}, \overline{b}, \ldots, \overline{0}) \ldots, (\overline{0}, \ldots, \overline{0}, \overline{b})\} \subset \mathbb{Z}_q^n$$

temos $|\mathcal{C}| = m^n$. De fato, se $\overline{t} \in \mathbb{Z}_q$ e $\overline{t} = \overline{am} + \overline{r}$ com $\overline{0} \leq \overline{r} < \overline{m}$ então $\overline{t}(\overline{0}, \ldots, \overline{b}, \ldots, \overline{0}) = \overline{r}(\overline{0}, \ldots, \overline{b}, \ldots, \overline{0})$. Para este código, $R = (b-1)/2$. Como $\mu_\infty(n, R) = (2R+1)^n = b^n$, segue que $|\mathcal{C}|\mu_\infty(n, R) = m^n b^n = q^n$, $1 < |\mathcal{C}| < q^n$ e esse código é perfeito e não trivial.

□

Na proposição anterior mostramos códigos na métrica ∞-Lee que são produtos cartesianos. O próximo exemplo nos mostra que existem outras famílias de códigos perfeitos em tais métricas.

Exemplo 2.2.17. *Seja $q = p^2$, onde p é um primo maior que 2. O grupo $\mathbb{Z}_{p^2}^2$ tem p^4 elementos e possui subgrupos não triviais de ordem p, p^2 e p^3. Da igualdade $|\mathcal{C}|(2R+1)^2 = p^4$, uma condição necessária para obter um código perfeito é $|\mathcal{C}| = p^2$. Os códigos $\mathcal{C} = \langle(\overline{1}, \overline{p\,a})\rangle$, $\overline{a} \neq \overline{0}$, satisfazem $|\mathcal{C}| = p^2$ e são perfeitos. A Figura 2.2.17 mostra o código $\mathcal{C} = \langle(\overline{1}, \overline{7})\rangle \subset \mathbb{Z}_{49}^2$.*

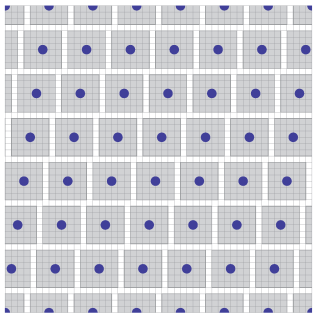


Figura 2.5: Códigos perfeitos não cartesianos na métrica ∞-Lee

Observação 2.2.18. *Se $q = 2^a$ para algum $a \in \mathbb{N}$, então não existem códigos $\mathcal{C} \subset \mathbb{Z}_q^n$ não triviais na métrica p-Lee para $1 \leq p \leq \infty$. De fato, para cada $1 \leq p \leq \infty$ e raio de empacotamento R, $\mu_p(n, R)$ é ímpar, assim $|\mathcal{C}|\mu_p(n, R) \neq 2^{an}$.*

Na Proposição 2.2.15, mostramos que os códigos perfeitos exibidos em [GW70] são também perfeitos na métrica p-Lee para $p < \infty$ com os mesmo paramêtros, $n > 2$ e $R = 1$. Para $n > 2$, sabemos que é conjecturado que estes são os únicos parâmetros possíveis para que existam códigos perfeitos. A seguir, mostramos que isso não é necessariamente verdade para as métricas p-Lee.

Proposição 2.2.19. *Seja $\mathcal{C} \subset \mathbb{Z}_q^n$ um código perfeito na métrica ∞-Lee com raio de empacotamento R. Se $p > \dfrac{\ln(n)}{\ln\left(1+\frac{1}{R}\right)}$, então $\mathcal{C}$ é também perfeito na métrica p-Lee com raio $R_p = Rn^{1/p}$.*

Demonstração. Se $\mathcal{C}$ é perfeito na métrica p-Lee, então para algum valor de p, existe um raio de empacotamento R_p (R_p^p inteiro) tal que

$$B_{\infty,Lee}(\overline{0}, R) \subset B_{p,Lee}(\overline{0}, R_p) \subset B_{\infty,Lee}(\overline{0}, R+1). \tag{2.13}$$

Para a primeira inclusão note que das desigualdades de normas l_p no $\mathbb{R}^n$, temos $\|\boldsymbol{x}\|_{p,Lee} \leq n^{1/p}\|\boldsymbol{x}\|_{\infty,Lee} \leq Rn^{1/p}$. Portanto $Rn^{1/p} \leq R_p$. Da segunda inclusão $R_p < R+1$.

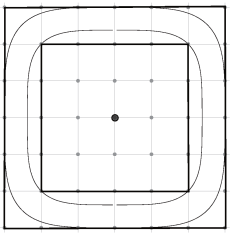


Figura 2.6: $B_{\infty,Lee}(\overline{0}, 2) \subset B_{p,Lee}(\overline{0}, R_p) \subset B_{p,Lee}(\overline{0}, 3) \subset B_{\infty,Lee}(\overline{0}, 3)$

Como R_p^p deve ser inteiro, $Rn^{1/p} = R_p < R+1$. Agora, $Rn^{1/p} < R+1$ se, e somente se, $n^{1/p} < 1 + \dfrac{1}{R}$, isto é, $p > \dfrac{\ln(n)}{\ln\left(1+\frac{1}{R}\right)}$. Portanto, para $p > \dfrac{\ln(n)}{\ln\left(1+\frac{1}{R}\right)}$, as bolas de raio $Rn^{1/p}$ centradas em palavras de $\mathcal{C}$ são disjuntas e cobrem $\mathbb{Z}_q^n$, o que significa que este código é perfeito. □

Corolário 2.2.20. *Para qualquer $R > 0$ e p suficientemente grande, existem*

códigos perfeitos em $\mathbb{Z}^n$ na norma l_p com raio de empacotamento maior ou igual a R.

Exemplo 2.2.21. *Considere o código $\mathcal{C} = \langle(\overline{5},\overline{0}),(\overline{0},\overline{5})\rangle \subset \mathbb{Z}_{15}^2$. Esse código é perfeito na métrica ∞-Lee e para $p \geq 2$ ele também é perfeito na metrica p-Lee. Note que $\mathcal{C}$ não é perfeito na métrica 1-Lee.*

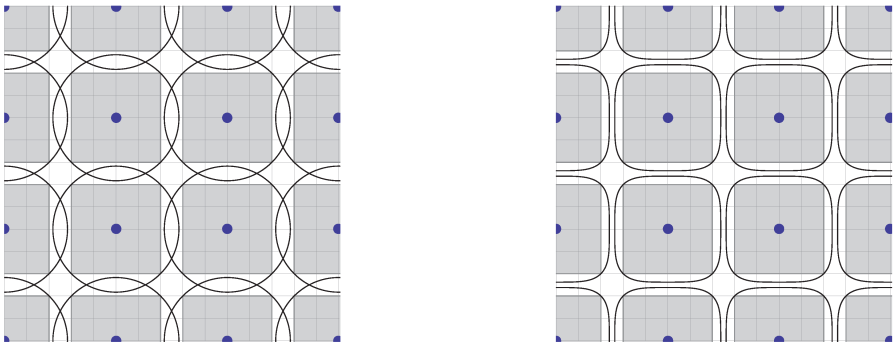


Figura 2.7: Um código perfeito na métrica p-Lee, $2 \leq p \leq \infty$. À direita, $p = 2$ e à esquerda, $p = 4$.

Exemplo 2.2.22. *Seja $q = 10$. Da Proposição 2.2.16, o código*

$$\mathcal{C} = \langle(\overline{5},\overline{0},\cdots,\overline{0}),\cdots,(\overline{0},\overline{0},\cdots,\overline{5})\rangle \subset \mathbb{Z}_q^n$$

é perfeito na métrica ∞-Lee, com raio 2. Da Proposição 2.2.19, para qualquer n o código $\mathcal{C}$ é perfeito na métrica p-Lee para todo $p > \dfrac{\ln(n)}{\ln\left(1+\frac{1}{2}\right)} = \dfrac{\ln(n)}{0.405}$. A tabela abaixo mostra alguns valores de n e o menor p que satisfaz $p > \dfrac{\ln(n)}{\ln\left(1+\frac{1}{2}\right)} = \dfrac{\ln(n)}{0.405}$.

n	10	25	50	100	250	500	1000	5000	10000
p	6	8	10	12	14	16	18	22	23

Tabela 2.1: Menores valores de p tais que a Proposição 2.2.19 garante que há códigos perfeitos na métrica p-Lee em $\mathbb{Z}_{10}^n$

Do que vimos até agora, para n fixo e R fixo, podemos crescer o valor de p de modo a obtermos um ladrilhamento de $\mathbb{Z}^n$ na norma l_p. Mostraremos agora que, para n fixo e p fixo, existe um certo raio limite R tal que não há nenhum ladrilhamento de $\mathbb{Z}^n$ na norma l_p com raio maior que R. A técnica para demonstrar isso é via associação de ladrilhamentos com os chamados poliominós, proposta por Golomb e Welch em [GW70, Teo. 7] e recentemente revisitada por Grosek e Horak em [HG14, Teo. 7].

Seja $B_p(R) \subset \mathbb{R}^n$ a bola de raio R na distância l_p centrada na origem, isto é

$$B_p(R) = \{\boldsymbol{x} \in \mathbb{R}^n : d_p(\boldsymbol{x}, \mathbf{0}) \leq R\}.$$

A união de cubos de raio $1/2$ centrados em pontos inteiros $B_p(R)$ é denotada por $L_p(n, R)$ e é chamada de um *poliominó*. Claramente, um ladrilhamento de $\mathbb{Z}^n$ através do reticulado Λ induz um ladrilhamento de $\mathbb{R}^n$ por poliominós, tomando alguns cuidados com os bordos. Abaixo estão ilustrados alguns poliominós em $\mathbb{R}^2$.

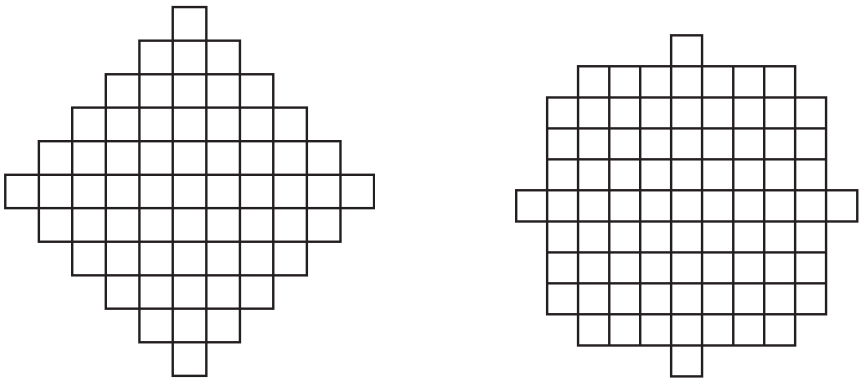


Figura 2.8: À esquerda, o poliminó $L_1(2, 5)$ e à direita $L_2(2, 5)$.

A conjectura de Golomb-Welch pode ser re-escrita como: para $n > 2$ e $R > 1$, translações do poliominó $L_1(n, R)$ não ladrilham $\mathbb{R}^n$.

Proposição 2.2.23. *[JCC13] Seja $n > 2$ e $1 \leq p < \infty$. Existe $\bar{R}_{n,p} > 0$ tal que para $R > \bar{R}_{n,p}$ não há códigos perfeitos lineares $\Lambda \subset \mathbb{Z}^n$ com raio R.*

Demonstração. Suponhamos, por absurdo, que existe um código perfeito com raio R. O volume do poliominó $L_p(n, R)$ é igual a $\mu_p(n, R)$ e as cópias de $L_p(n, R)$ por pontos de Λ ladrilham $\mathbb{R}^n$. Por outro lado, o raio de empacotamento do reticulado Λ na norma l_p é certamente maior ou igual a R e portanto possui densidade:

$$\delta \geq \frac{\mathrm{vol}(B_p(R))}{\mathrm{vol}(L_p(n, R))} = \frac{\mathrm{vol}(B_p(R))}{\mu_p(n, R)}. \tag{2.14}$$

Sabemos que o lado direito da desigualdade acima tende a $\det \mathbb{Z}^n = 1$ quando R tende a infinito (Proposição 1.1.4 modificada para a norma l_p). Mas também sabemos que a densidade de empacotamento de qualquer reticulado em $\mathbb{R}^n$ na norma l_p é limitada superiormente por algum $\alpha < 1$. Assim, para R suficientemente grande, construímos um empacotamento que ultrapassa a melhor densidade de empacotamento em $\mathbb{R}^n$, o que é um absurdo. Portanto, deve existir um raio limite $\bar{R}_{n,p}$, tal que não há códigos perfeitos para $R > \bar{R}_{n,p}$. □

2.3 Referências Futuras

A despeito de distintas nomenclaturas, a métrica p-Lee aparece naturalmente na literatura associada a reticulados. Um limitante do tipo Gilbert-Varshamov para códigos na métrica p-Lee é exibido em [RS87], a partir do qual pode-se demonstrar a existência de reticulados q-ários com boa densidade de empacotamento (com respeito à norma l_p). Duas referências mais recentes são [FSK13] e [SB13]. Em [FSK13], no contexto de codificação de rede na camada física, é definido o "peso euclidiano" de uma palavra-código $\boldsymbol{c}$, que é precisamente a raiz da distância 2-Lee aqui discutida. Em [SB13] é exibida uma construção de códigos esféricos com boas taxas, utilizandos códigos em $\mathbb{Z}_q^n$ munidos da "distância Euclidiana". A menos de rotulamento, a distância considerada em [SB13] é precisamente a distância 2-Lee estudada neste capítulo. Como apontado pelos autores, códigos perfeitos na métrica 2-Lee podem ser utilizados como base para a construção de bons códigos esféricos, o que provém uma outra motivação para o estudo de

códigos perfeitos nas métricas p-Lee. Infelizmente na métrica 2-Lee os poliominós parecem possuir forma mais proibitiva a códigos perfeitos que na métrica de Lee, como ilustrado na Figura 2.8.

Capítulo 3

Projeções de Reticulados

"É uma complicação quando se tem de explicar que na maneira de perguntar já se escolhe o tipo de resposta."

- João Ubaldo Ribeiro, *Viva o Povo Brasileiro*

Este capítulo é devotado ao estudo de projeções de reticulados ao longo de subespaços vetoriais do $\mathbb{R}^n$. Como visto na Seção 1.3, muitos reticulados notáveis são naturalmente caracterizados através de projeções e intersecções com subespaços. Ademais, projeções estão fortemente presentes na literatura dos reticulados *perfeitos* [Mar03] e dos *laminados* [CS98, Cap. 6]. Estamos interessados aqui no caso em que a projeção de um reticulado ao longo de um subespaço produz um outro reticulado, de dimensão menor, com boa densidade de empacotamento.

Além do interesse puramente teórico, a principal motivação para o estudo mais recente de projeções do reticulado cúbico $\mathbb{Z}^n$ deve-se à sua aplicação na construção de códigos analógicos (trataremos mais detalhadamente de tal aplicação nos capítulos 4 e 5). Em [VC03], é mostrado que projeções de $\mathbb{Z}^n$ ao longo de um vetor primitivo $\boldsymbol{v} \in \mathbb{Z}^n$ podem ser utilizadas para o desenvolvimento de tais códigos. A figura de mérito nesse caso é a densidade de empacotamento; projeções com boa densidade implicam bons códigos. Surge então a seguinte pergunta: qual a melhor densidade atingível por uma projeção de $\mathbb{Z}^n$ ao longo de um vetor $\boldsymbol{v} \in \mathbb{Z}^n$? Resultados parciais em dimensões baixas acerca de boas projeções de $\mathbb{Z}^n$ ($n = 2, 3$, e 4) podem ser encontrados em [Str07], [SVC09], [SVC10]. Uma resposta definitiva à pergunta acima é dada, finalmente, em [SVC11]: *qualquer*

reticulado de dimensão $(n-1)$ pode ser aproximado, a menos de equivalência, por projeções de $\mathbb{Z}^n$. Como consequência, projeções do reticulado cúbico podem atingir, essencialmente, a melhor densidade de empacotamento de reticulados $(n-1)$ dimensionais.

Na Seção 3.2 descrevemos esses resultados sobre projeções de $\mathbb{Z}^n$. Uma desvantagem do método em [SVC11] é a de que, para conseguir boas aproximações, é necessário crescer significativamente a norma do vetor ao longo do qual estamos projetando (o que dificulta, por exemplo, a decodificação de tais reticulados). Através de uma análise de convergência cuidadosa, mostramos que é possível construir sequências quadraticamente melhores que aquelas em [SVC11] e exibimos construções explícitas para algumas das principais famílias de reticulados (a saber, D_n, D_n^*, E_7, E_8).

Na Seção 3.3, tratamos do estudo geral de projeções de um reticulado *qualquer* pré-fixado, exibindo um dos principais resultados desta tese, que generaliza [SVC11]. Apesar da construção que mostraremos na Seção 3.3 ser mais geral do que a exibida na Seção 3.2, decidimos por organizar o texto desta forma, de modo a seguir o curso histórico da teoria. Além disso, como dito anteriormente, projeções de $\mathbb{Z}^n$ são particularmente interessantes por suas aplicações em codificação contínua, e serão utilizadas diretamente nos capítulos 4 e 5.

Na Seção 3.4 discutimos algumas possíveis extensões dos resultados anteriores, incluindo o estudo de projeções de empacotamentos periódicos.

Os resultados contidos aqui podem ser encontrados em [CS13] e [CSC13], e foram parcialmente apresentados no *Workshop on Algebraic Coding Theory*, Lausanne, Suiça (2011) e no *Congresso Nacional de Matemática Aplicada e Computacional*, Águas de Lindóia, São Paulo (2012).

3.1 Resultados Preliminares

Seja V uma matriz de ordem $k \times n$, $k < n$, de posto completo. Denotamos por $\text{span}(V)^\perp$ o complemento ortogonal do espaço vetorial gerado pelas linhas de V, isto é:

$$\text{span}(V)^\perp = \{\boldsymbol{x} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \text{ para todo } \boldsymbol{y} \in \text{span}(V)\}.$$

Qualquer vetor $\boldsymbol{x} \in \mathbb{R}^n$ pode ser decomposto de maneira única como $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{v}^\perp$, onde $\boldsymbol{v} \in \text{span}(V)$ e $\boldsymbol{v}^\perp \in \text{span}(V)^\perp$. Dado $\boldsymbol{x} \in \mathbb{R}^n$, definimos a *projeção ortogonal* de $\boldsymbol{x}$ em $\text{span}(V)^\perp$ como $P_{V^\perp}(\boldsymbol{x}) = \boldsymbol{v}^\perp$. Pode-se mostrar (ver e.g. [Mey00, pp. 430]) que $P_{V^\perp}(\boldsymbol{x}) = \boldsymbol{x}P$, onde

$$P = (I - V^t(VV^t)^{-1}V).$$

Chamamos P de *projetor* (ou matriz de projeção) ortogonal em $\text{span}(V)^\perp$. Por abuso de notação quando V é um vetor-linha $\boldsymbol{v}$, denotamos $\text{span}(V)^\perp$ por $\boldsymbol{v}^\perp$.

Seja $\Lambda = \Lambda(B) \subset \mathbb{R}^n$ um reticulado de posto completo. A projeção de Λ em $\text{span}(V)^\perp$ é dada por

$$P_{V^\perp}(\Lambda) = \{\boldsymbol{x}P : \boldsymbol{x} \in \Lambda\} = \{\boldsymbol{u}BP : \boldsymbol{u} \in \mathbb{Z}^n\}. \tag{3.1}$$

Observação 3.1.1. *Por simplificação, consideraremos apenas projeções de reticulados de posto completo.*

Em princípio, a projeção de um reticulado ao longo de um subespaço vetorial pode não ser um conjunto discreto em $\mathbb{R}^n$, como nos mostra o exemplo abaixo.

Exemplo 3.1.2. *Seja $\Lambda = \mathbb{Z}^2$ e $\boldsymbol{v} = (1, \sqrt{2})$. O projetor ortogonal ao longo de $\boldsymbol{v}$ é dado por*

$$P = \begin{pmatrix} \frac{2}{3} & -\frac{\sqrt{2}}{3} \\ -\frac{\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}.$$

Aplicando a transformação ortogonal definida pela matriz

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

no conjunto projeção (3.1)*, obtemos*

$$P_{\boldsymbol{v}^\perp}(\mathbb{Z}^2)Q = \left\{\boldsymbol{x}PQ : \boldsymbol{x} \in \mathbb{Z}^2\right\} = \frac{1}{\sqrt{3}}\left\{(\sqrt{2}x_1 + x_2, 0) : x_1, x_2 \in \mathbb{Z}\right\}.$$

É um interessante exercício de combinatória utilizar o princípio da casa dos pombos para provar que, para qualquer $a \in \mathbb{R}$ e $\varepsilon > 0$, existe um elemento do conjunto arbitrariamente próximo de $(a, 0)$. Temos, assim, que o conjunto projeção não é discreto.

Levando em consideração o exemplo acima e a caracterização 1.1.1, vemos que $P_{V^\perp}(\Lambda)$ nem sempre é um reticulado. Isso pode parecer estranho à primeira vista, já que a Equação (3.1) parece prover-nos um conjunto de vetores cujas combinações inteiras geram $P_{V^\perp}(\Lambda)$ (ou seja, uma matriz geradora). Entretanto, como a matriz BP pode não ter posto completo, tal conjunto é não necessariamente uma base e, mais do que isso, pode não ser possível extrair uma base para $P_{V^\perp}(\Lambda)$ a partir das linhas de BP.

Para caracterizar conjuntos de vetores para os quais $P_{V^\perp}(\Lambda)$ é um reticulado, temos a seguinte proposição:

Proposição 3.1.3. *Seja V uma matriz de ordem $k \times n$ cujas linhas formam um conjunto primitivo de vetores de um reticulado $\Lambda \subset \mathbb{R}^n$. Valem as seguintes propriedades*

(i) *O conjunto $P_{V^\perp}(\Lambda)$ é um reticulado.*

(ii) *O discriminante de $P_{V^\perp}(\Lambda)$ é dado por*

$$\det P_{V^\perp}(\Lambda) = \frac{\det \Lambda}{\det VV^t}. \tag{3.2}$$

Demonstração. (i) Para mostrar que $P_{V^\perp}(\Lambda)$ é um reticulado, basta encontrar um conjunto linearmente independente de vetores cujas combinações lineares geram $P_{V^\perp}(\Lambda)$ (isto é, uma matriz geradora). Como as linhas de V são um conjunto primitivo, existe uma matriz $\bar{V}$ de ordem $(n-k)\times n$ e posto completo tal que

$$\hat{V} = \begin{pmatrix} V \\ \overline{V} \end{pmatrix} \tag{3.3}$$

é uma matriz geradora de Λ e qualquer elemento $\boldsymbol{x} \in \Lambda$ pode ser escrito como $\boldsymbol{x} = \boldsymbol{u}\hat{V}$, $\boldsymbol{u} \in \mathbb{Z}^m$. Projetando $\boldsymbol{x} \in \Lambda$ em $\mathrm{span}(V)^\perp$, temos:

$$\boldsymbol{x}P = \boldsymbol{u}\hat{V}P = \boldsymbol{u}\begin{pmatrix} \mathbf{0} \\ \overline{V}P \end{pmatrix}.$$

Assim, as linhas de $\overline{V}P$ formam um conjunto cujas combinações inteiras geram $P_{V^\perp}(\Lambda)$. Basta mostrar agora que $\overline{V}P$ tem posto completo. Com efeito, se $\boldsymbol{x}\overline{V}P = 0$, então $\boldsymbol{x}\overline{V} \in \mathrm{span}(V)$ e, portanto, $\boldsymbol{x}\overline{V} = \boldsymbol{y}V$. Entretanto como $\hat{V}$ é uma matriz geradora de Λ, suas linhas são LI, o que implica que $\boldsymbol{x} = \boldsymbol{y} = 0$, ou seja, o núcleo da matriz $\overline{V}P$ possui dimensão nula, concluindo a demonstração.

(ii) Da demonstração de (i), segue que $\overline{V}P$ é uma matriz geradora para V. Assim:

$$\det \Lambda = \det \hat{V}\hat{V}^t = \det \begin{pmatrix} VV^t & V\overline{V}^t \\ \overline{V}V^t & \overline{V}\overline{V}^t \end{pmatrix} \overset{(a)}{=} \det(VV^t)\det(\overline{V}\overline{V}^t - \overline{V}V^t(VV^t)^{-1}V\overline{V}^t)$$
$$\overset{(b)}{=} \det(VV^t)\det(\overline{V}P\overline{V}^t) = \det(VV^t)\det P_{V^\perp}(\Lambda),$$

onde a igualdade (a) segue do cálculo do determinante por blocos e a igualdade (b) segue do fato de que o projetor satisfaz $P = P^t = P^2$. □

Através de elementos de dualidade, podemos conectar projeções de reticulados e intersecções com hiperplanos. A conexão é feita a partir da seguinte proposição:

Proposição 3.1.4 ([Mar03])**.** *Se V é uma matriz de ordem $k \times n$ cujas linhas formam um conjunto primitivo de vetores de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$, então:*

$$P_{V^\perp}(\Lambda)^* = \Lambda^* \cap \operatorname{span}(V)^\perp.$$

Demonstração. Seja P um projetor em $\operatorname{span}(V)^\perp$. Vamos demonstrar primeiro a inclusão $P_{V^\perp}(\Lambda)^* \subset \Lambda^* \cap \operatorname{span}(V)^\perp$. Considere $\boldsymbol{x} \in P_{V^\perp}(\Lambda)^*$. Para qualquer $\boldsymbol{u} \in \Lambda$, temos $\boldsymbol{u}P = \boldsymbol{y} \in P_{V^\perp}(\Lambda)$, e portanto $\langle \boldsymbol{u}P, \boldsymbol{x} \rangle \in \mathbb{Z}$. Mas como P é uma matriz simétrica e $\boldsymbol{x} \in V^\perp$:

$$\langle \boldsymbol{u}P, \boldsymbol{x} \rangle = \langle \boldsymbol{u}, \boldsymbol{x}P \rangle = \langle \boldsymbol{u}, \boldsymbol{x} \rangle \in \mathbb{Z},$$

mostrando que $\boldsymbol{x} \in \Lambda^* \cap \operatorname{span}(V)^\perp$. Consideremos agora a inclusão contrária. Se $\boldsymbol{x} \in \Lambda^* \cap \operatorname{span}(V)^\perp$, então $\boldsymbol{x} \in V^\perp$ e $\langle \boldsymbol{x}, \boldsymbol{u} \rangle \in \mathbb{Z}$ para qualquer $\boldsymbol{u} \in \Lambda$. De maneira similar ao primeiro caso, temos $\langle \boldsymbol{x}, \boldsymbol{u}P \rangle = \langle \boldsymbol{x}P, \boldsymbol{u} \rangle = \langle \boldsymbol{x}, \boldsymbol{u} \rangle \in \mathbb{Z}$, e assim para qualquer $\boldsymbol{y} = \boldsymbol{u}P \in P_{V^\perp}(\Lambda)$, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}$, ou seja, $\boldsymbol{x} \in P_{V^\perp}(\Lambda)^*$. □

Exemplo 3.1.5. *Como visto em 1.3, o reticulado A_n é definido como $\mathbb{Z}^{n+1} \cap \boldsymbol{e}^\perp$, onde $\boldsymbol{e} = (1, \ldots, 1)$. Segue imediatamente do teorema acima e da auto-dualidade do reticulado $\mathbb{Z}^{n+1}$ que $P_{\boldsymbol{e}^\perp}(\mathbb{Z}^{n+1}) = A_n^*$.*

Uma consequência das proposições 3.1.3 e 3.1.4 é a chamada Desigualdade de Mordell .

Teorema 3.1.6 (Desigualdade de Mordell, [CS98, p.167])**.** *Seja δ_n a maior densidade de centro possível entre todos os reticulados de dimensão n. Temos então*

$$\delta_{n-1} \geq \frac{1}{2} \delta_n^{(n-2)/n}.$$

Demonstração. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de dimensão n com densidade máxima e determinante igual a 1. Considere um vetor de norma mínima $\boldsymbol{v} \in \Lambda^*$, $\boldsymbol{v} \neq \mathbf{0}$. Utilizando as fórmulas da densidade de centro (1.8) e da norma mínima de um reticulado (1.5):

$$\delta(\Lambda \cap \boldsymbol{v}^\perp) = \frac{\lambda(\Lambda \cap \boldsymbol{v}^\perp)^{n-1}}{2^{n-1}\sqrt{\det(\Lambda \cap \boldsymbol{v}^\perp)}} \geq \frac{\lambda(\Lambda)^{n-1}}{2^{n-1}\sqrt{\det(\Lambda \cap \boldsymbol{v}^\perp)}} \overset{(a)}{=} \frac{\lambda(\Lambda)^{n-1}}{2^{n-1}\sqrt{\det(P_{\boldsymbol{v}^\perp}(\Lambda^*)^*)}}$$
$$\overset{(b)}{=} \frac{\lambda_1(\Lambda)^{n-1}}{2^{n-1}\lambda(\Lambda^*)} \overset{(c)}{\geq} \frac{\lambda(\Lambda)^{n-2}}{2^{n-1}} = \frac{1}{2}\delta_n^{(n-2)/n},$$

onde: (a) segue da Proposição 3.1.4, (b) segue da Proposição 3.1.3 e (c) é uma consequência de $\lambda_1(\Lambda^*) \leq \lambda_1(\Lambda)$, o que, por sua vez, segue da otimalidade da densidade de Λ. □

Uma consequência da desigualdade é que a otimalidade da densidade dos reticulados D_4 e E_8 segue imediatamente da otimalidade de D_3 e E_7, respectivamente.

A demonstração da Desigualdade de Mordell 3.1.6 nos diz que é possível obter reticulados de dimensão $(n-1)$ com boa densidade a partir de projeções de reticulados de dimensão n com boa densidade. Entretanto, não sabemos a priori qual o reticulado de dimensão n mais denso. Gostaríamos, portanto, de caracterizar quais as melhores densidades de projeção de algum reticulado $\Lambda \subset \mathbb{R}^n$ *fixado* previamente. O reticulado mais simples é provavelmente $\Lambda = \mathbb{Z}^n$, e este será o tema da próxima seção.

3.2 Projeções do Reticulado Cúbico

Como vimos anteriormente, o reticulado A_n^* pode ser definido como a projeção de $\mathbb{Z}^{n+1}$ no hiperplano $(1, \ldots, 1)^\perp$. No caso $n = 2$, temos que $A_2 \sim A_2^*$, e portanto a melhor densidade de empacotamento no plano pode ser atingida através de projeções de $\mathbb{Z}^3$. O próximo passo natural seria considerarmos projeções de $\mathbb{Z}^4$ cuja densidade seja igual à do reticulado D_3. Este problema só faz sentido *a*

menos de equivalência já que, como vimos no Capítulo 1, reticulados equivalentes possuem mesma densidade. Tais equivalências, entretanto, introduzem graus de liberdade, o que torna o problema mais complexo. Precisamos então considerar *sequências* de projeções que *aproximam* o reticulado de melhor densidade. De fato, os resultados apresentados aqui são mais gerais: mostraremos como construir sequências de projeções que aproximam *qualquer* reticulado.

Para enunciar formalmente os resultados, necessitamos de uma noção de proximidade entre dois reticulados. Seja $\|.\|$ alguma norma de matrizes. Usualmente na literatura (e.g. [GL87]), diz-se que um reticulado Λ_1 está na ε-vizinhança de $\Lambda_2 = \Lambda_2(B_2)$ (com respeito à matriz geradora B_2) se existe B_1 tal que $\Lambda_1 = \Lambda_1(B_1)$ e $\|B_1 - B_2\| \leq \varepsilon$. Com essa noção de vizinhança, pode-se definir uma topologia no espaço de reticulados, conjuntos compactos e uma gama de outras propriedades que fogem ao escopo deste trabalho.

Aqui utilizaremos uma noção um pouco diferente, que não distingue reticulados equivalentes conforme a proximidade. Dizemos que Λ_1 está na ε-vizinhança de Λ_2 (com respeito à matriz de Gram A_1 para Λ_1) se existe matriz Gram A_2 para Λ_2 tal que $\|A_1 - A_2\| \leq \varepsilon$.

Para convergência de sequências de reticulados, gostaríamos de uma noção que também não distinguisse mudança de escala. Assim, dizemos que uma sequência de reticulados $\Lambda_w, w = 1, 2, \ldots$ converge para Λ, a menos de equivalência, se, para qualquer $\varepsilon > 0$, existe w_0 tal que, para $w > w_0$, $c_w\Lambda_w$ está na ε vizinhança de Λ para algum fator de escala c_w (possivelmente dependendo de w). Daqui para frente, a notação $\Lambda_w \to \Lambda$ será usada para indicar que uma sequência de reticulados Λ_w converge para Λ, a menos de equivalência. Está claro que a convergência não depende da matriz de Gram escolhida para Λ. Por simplificação, utilizaremos a norma de matrizes definida por $\|A\|_\infty = \max_{i,j} |A_{ij}|$, salvo explicitado o contrário.

Observação 3.2.1. *Como a densidade é uma função contínua das entradas da matriz de Gram (ver e.g. [SVC11]), se $\Lambda_w \to \Lambda$, então a sequência de densidades $\delta_w = \delta(\Lambda_w)$ converge para $\delta(\Lambda)$.*

Observação 3.2.2. *Se $\Lambda_w \to \Lambda$, então $\Lambda_w^* \to \Lambda^*$. Com efeito, seja A_w uma sequência de matrizes de Gram para Λ_w tal que $c_w A_w \to A$. Como A_w é definida-positiva, temos que a sua inversa existe, e vale que $(1/c_w)A_w^{-1} \to A^{-1}$, ou seja, $\Lambda_w^* \to \Lambda^*$.*

Descrevemos a seguir Construção *Lifting* de [SVC10, SVC11]. O objetivo dessa construção é exibir sequências de reticulados projeção de $\mathbb{Z}^n$ que convergem, a menos de equivalência, para qualquer reticulado de posto $(n-1)$ dado.

3.2.1 A Construção *Lifting*

Seja o vetor primitivo $\boldsymbol{v} = (1, v_1, \ldots, v_{n-1}) \in \mathbb{Z}^n$. Uma matriz geradora para $\boldsymbol{v}^\perp \cap \mathbb{Z}^n = P_{\boldsymbol{v}^\perp}(\mathbb{Z}^n)^*$ é dada por $M = (-\hat{\boldsymbol{v}}^t \; I)$, onde $\hat{\boldsymbol{v}} = (v_1, \ldots, v_{n-1})$ e I é a matriz identidade de ordem $(n-1) \times (n-1)$.

Considere agora um reticulado Λ de posto $(n-1)$ e seja A^* uma matriz de Gram para Λ^*. Podemos sempre encontrar $\tilde{L}^*$ triangular inferior tal que $A^* = \tilde{L}^* \tilde{L}^{*t}$ (por exemplo, utilizando a fatoração de Cholesky). Seja $L^* = (\tilde{L}^* \; \mathbf{0})$, onde a matriz de $\mathbf{0}$ possui ordem $(n-1) \times 1$. Construímos a sequência de matrizes

$$
\begin{aligned}
L_w^* &= -\lfloor wL^* \rfloor + (\mathbf{0} \; I) \\
&= \begin{pmatrix}
-\lfloor wL_{11}^* \rfloor & 1 & 0 & \ldots & 0 \\
-\lfloor wL_{21}^* \rfloor & -\lfloor wL_{22}^* \rfloor & 1 & \ldots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
-\lfloor wL_{(n-1),1}^* \rfloor & -\lfloor wL_{(n-1),2}^* \rfloor & \ldots & -\lfloor wL_{(n-1),(n-1)}^* \rfloor & 1
\end{pmatrix}
\end{aligned}
\tag{3.4}
$$

e consideramos a sequência de reticulados $\Lambda_w^* = \Lambda(L_w^*)$. A matriz

$$H_w = \begin{pmatrix} 1 & 0 & \dots & 0 \\ -\lfloor wL_{22}^* \rfloor & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ -\lfloor wL_{(n-1),2}^* \rfloor & \dots & -\lfloor wL_{(n-1),(n-1)}^* \rfloor & 1 \end{pmatrix}$$

composta pelas últimas $(n-1)$ colunas de L_w^* possui entradas inteiras e determinante 1. Desta maneira, o reticulado Λ_w^* é também gerado pela matriz $H_w^{-1}L_w^*$. Mas $H_w^{-1}L_w^*$ é da forma $(-\hat{\boldsymbol{v}}^t\ I)$ para algum $\hat{\boldsymbol{v}}$, e portanto corresponde à intersecção de $\mathbb{Z}^n$ com algum hiperplano $\boldsymbol{v}^\perp$. Assim, $\Lambda(L_w^*) = P_{\boldsymbol{v}^\perp}(\mathbb{Z}^n)^*$, para algum $\boldsymbol{v} \in \mathbb{Z}^n$. Por outro lado, temos

$$(1/w^2)L_w^* L_w^{*t} \to L^* L^{*t},$$

o que mostra que $\Lambda_w^* \to \Lambda^*$. Por conta da Observação 3.2.2, temos que $\Lambda_w \to \Lambda$. Provamos assim o seguinte:

Teorema 3.2.3 ([SVC11])**.** *Seja Λ um reticulado de posto $(n-1)$. Existe uma sequência de vetores $\boldsymbol{v}_w \in \mathbb{Z}^n$ tal que $P_{\boldsymbol{v}_w^\perp}(\mathbb{Z}^n) \to \Lambda$, quando $w \to \infty$. Em outras palavras, a sequência de projeções de $\mathbb{Z}^n$ nos hiperplanos $\boldsymbol{v}_w^\perp$ converge, a menos de equivalência, para Λ.*

Exemplo 3.2.4. *Seja $\Lambda = D_3$ o reticulado cúbico de face centrada. Uma matriz geradora triangular inferior para D_3^* é*

$$\overline{L}^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1/2 & 1/2 & 1/2 \end{pmatrix}.$$

Por simplificação, consideraremos $L^* = 2\overline{L}^*$, isto é, considerarmos uma matriz

geradora para o reticulado escalado $2D_3^*$*. Da Construção Lifting, temos*

$$L_w^* = \begin{pmatrix} -2w & 1 & 0 & 0 \\ 0 & -2w & 1 & 0 \\ -w & -w & -w & 1 \end{pmatrix} \text{ e } H_w = \begin{pmatrix} 1 & 0 & 0 \\ -2w & 1 & 0 \\ -w & -w & 1 \end{pmatrix}.$$

Aplicando $H_w^{-1}L_w^*$*, obtemos* $\boldsymbol{v}_w = (1, 2w, 4w^2, 4w^3 + 2w^2 + w)$*. À medida que* w *cresce (ou* $\|\boldsymbol{v}_w\|_\infty$ *cresce), temos que* $P_{\boldsymbol{v}_w^\perp}(\mathbb{Z}^n)$ *aproxima-se de um reticulado equivalente a* D_3*. Na Figura 3.1, exibimos a densidade de* $P_{\boldsymbol{v}_w^\perp}(\mathbb{Z}^n)$ *em função da norma do vetor projeção. Vemos que para obter boas densidades necessitamos crescer significativamente a norma de* $\|\boldsymbol{v}_w\|_\infty$*.*

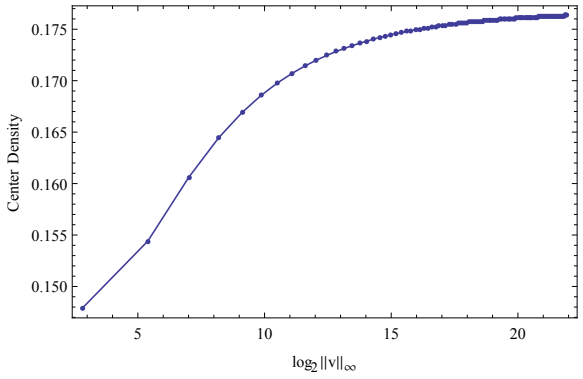


Figura 3.1: Densidade de centro de $P_{\boldsymbol{v}_w^\perp}(\mathbb{Z}^n)$ em função da norma do vetor projeção. No topo, temos $\delta(D_3) \approx 0.1767$.

Em [VC03] e [Str07, Capítulo 2], é mostrado um algoritmo para a decodificação em reticulados projeção de $\mathbb{Z}^n$. Ambos os algoritmos são eficientes quando o vetor $\boldsymbol{v}$ possui norma pequena. De fato, em [VC03] é mostrado que podemos decodificar em $P_{\boldsymbol{v}}(\mathbb{Z}^n)$ utilizando $\Theta(\|\boldsymbol{v}\|_1)$ operações. Portanto, um parâmetro bastante relevante a se considerar nas sequências de projeção produzidas pela Construção *Lifting* é a norma do vetor projeção. A análise de convergência feita a seguir levará em consideração esta relação entre a norma de $\boldsymbol{v}$ e proximidade entre $P_{\boldsymbol{v}^\perp}(\mathbb{Z}^n)$ e Λ.

3.2.2 Análise de Convergência

Consideremos a sequência v_w do Exemplo 3.2.4. O quarto vetor desta sequência, $v_4 = (1, 8, 64, 292)$, produz um reticulado projeção de $\mathbb{Z}^4$ cuja densidade de centro é 0.164452. Fazendo uma busca exaustiva por todos os vetores de norma até 292, vemos que é possível encontrar muitos vetores de menor norma cujo reticulado projeção possui densidade melhor que $P_{\boldsymbol{v}_4^{\perp}}(\mathbb{Z}^n)$, como exemplificado na Tabela 3.1.

Vetor Projeção $\boldsymbol{v}$	Densidade de Centro	Norma Mínima	$\|\boldsymbol{v}\|_\infty$
$(1, 29, 37, 268)$	0.17351	0.172147	268
$(1, 56, 185, 196)$	0.16502	0.168637	196
$(1, 121, 163, 187)$	0.17059	0.170362	187
$(1, 33, 80, 265)$	0.16473	0.16783	265
$(1, 98, 125, 230)$	0.16803	0.168793	230
$(1, 107, 141, 222)$	0.16670	0.167472	222
$(1, 42, 181, 215)$	0.16642	0.167331	215
$(1, 8, 110, 265)$	0.16572	0.166535	265
$(1, 12, 84, 282)$	0.16420	0.164612	282
$(1, 91, 153, 236)$	0.16619	0.165065	236
$(1, 119, 152, 224)$	0.16556	0.16484	224
$(1, 88, 121, 256)$	0.16497	0.164493	256
$(1, 8, 64, 292)$	0.16445	0.163858	292

Tabela 3.1: Reticulados $P_{\boldsymbol{v}^{\perp}}(\mathbb{Z}^4)$ densos, para $187 \leq \|\boldsymbol{v}\| \leq 292$.

Vemos assim que existe bastante espaço para melhorar as sequências da Construção *Lifting*. No que segue, proporemos uma modificação da construção que nos dê graus de liberdade a serem convenientemente escolhidos de modo a obter uma convergência acelerada.

Seja Λ um reticulado de posto $(n-1)$ cujo dual possui matriz geradora inteira $\tilde{L}^*$. Consideremos $L^* = (\tilde{L}^* \ \mathbf{0})$, onde a matriz de zeros $\mathbf{0}$ possui ordem $(n-1)\times 1$. Seja P uma matriz com entradas inteiras e ordem $(n-1)\times n$, a qual chamaremos

matriz de perturbação. Consideramos as sequências de matrizes

$$L_w^* = wL^* + P,$$

e a sequência de reticulados $\Lambda_w^* = \Lambda(L_w^*)$. As matrizes de Gram de $\Lambda(L_w^*)$ correspondentes são

$$A_w^* = w^2 A^* + w(L^* P^t + P L^{*t}) + P P^t = w^2 A^* + w Q_1 + Q_0, \tag{3.5}$$

Segue que $(1/w^2)A_w^* \to A^*$ quando $w \to \infty$. Como vimos anteriormente, se escolhermos $P = (\mathbf{0}\ I)$, cada elemento Λ_w^* corresponde à intersecção de $\mathbb{Z}^n$ com $\boldsymbol{v}^\perp$ para algum vetor $\boldsymbol{v}$. Considere $H_w = (L_w^*)_{(1,\ldots,n-1),(2,\ldots,n)}$ a matriz construída pelas $(n-1)$ últimas colunas de L_w^*. O seguinte lema generaliza o resultado 3.2.3 para qualquer matriz de perturbação P.

Lema 3.2.5 ([CS13])**.** *Sejam L_w^* e H_w as matrizes definidas acima. Se H_w é unimodular para qualquer $w \in \mathbb{N}$ então os reticulados Λ_w, duais de $\Lambda(L_w^*)$, são projeções de $\mathbb{Z}^n$.*

Demonstração. Como H_w é unimodular, a sua inversa também é, e portanto Λ_w^* é também gerado por $H_w^{-1} L_w^*$. Por outro lado, $H_w^{-1} L_w^* = \begin{pmatrix} \hat{\boldsymbol{v}}_w^t \\ I \end{pmatrix}$, e pelos mesmos argumentos da Seção 3.2.1, $\Lambda_w^* = \mathbb{Z}^n \cap \boldsymbol{v}_w^\perp$, onde $\boldsymbol{v}_w = (1\ -\hat{\boldsymbol{v}}_w^t)$. Pela Proposição 3.1.4, temos que $\Lambda_w = P_{\boldsymbol{v}_w^\perp}(\mathbb{Z}^n)$. □

A matriz de perturbação P nos dará o grau de liberdade desejado para encontrarmos boas sequências de projeções. Claramente se $P = (\mathbf{0}\ I)$, H_w será unimodular. Entretanto, há diversas outras matrizes que satisfazem a condição dada pelo Lema 3.2.5. Por exemplo, a condição é trivialmente satisfeita por qualquer P cujas últimas $(n-1)$ colunas formam uma matriz triangular inferior com diagonal unitária.

Procedemos agora com a análise de convergência das sequências 3.2.2. Para tal, iremos analisar

(i) A distância entre as matrizes de Gram de Λ_w e de Λ, em função de w.

(ii) A norma do vetor projeção $\boldsymbol{v}_w$, em função de w.

Para o item (i), notemos primeiramente que a ordem de convergência da sequência de duais de projeções Λ_w^* é dada por

$$\left\|A^* - (1/w^2)A_w^*\right\|_\infty = \left\|\frac{Q_1}{w} + \frac{Q_0}{w^2}\right\|_\infty = O\left(\frac{1}{w}\right).$$

Entretanto, estamos interessados na sequência de matrizes de gram A_w, associada aos reticulados projeção Λ_w. Para analisar esta sequência, precisamos do lema:

Lema 3.2.6 ([CS13])**.** *Seja A_w^* a matriz de Gram de Λ_w^* dada pela Equação* (3.5)*. Existe w_o tal que, para $w \geq w_o$, os reticulados projeção Λ_w possuem matriz de Gram*

$$A_w = \sum_{k=0}^{\infty} \left(\frac{A}{w^2}\left(-wQ_1 - Q_0\right)\right)^k \frac{A}{w^2}. \tag{3.6}$$

Demonstração. De acordo com a série de Neumman para matrizes [Mey00, Ch. 3, Eq. (3.8.5)], se M e N são matrizes quadradas de mesmas dimensões tais que N^{-1} existe e $\lim_{w\to\infty}(N^{-1}M)^k = \mathbf{0}_{n\times n}$, então

$$(M+N)^{-1} = \sum_{w=0}^{\infty}(-N^{-1}B)^w N^{-1}.$$

Aplicando este resultado para $N = w^2A^*$ (cuja inversa é $(1/w^2A)$) e $M = wQ_1 + Q_0$, temos que, se

$$\lim_{k\to\infty}\left\|\left((w^2A^*)^{-1}(wQ_1+Q_0)\right)^k\right\|_\infty = 0, \text{ então}$$

$$A_w = (A_w^*)^{-1} = (w^2A^* + wQ_1 + Q_0)^{-1} = \sum_{k=0}^{\infty} \left(\frac{A}{w^2} (-wQ_1 - Q_0) \right)^k \frac{A}{w^2}. \quad (3.7)$$

Provemos que para w suficientemente grande, o limite acima é sempre zero. Com efeito, como todas as entradas de $(wQ_1 + Q_0)$ e de $(w^2A^*)^{-1}$ possuem ordem $\Theta(w)$ e $\Theta(w^2)$, existe w_o tal que, para $w \geq w_o$, a matriz $(w^2A^*)^{-1}(wQ_1 + Q_0)$ está arbitrariamente próxima da matriz nula. Assim, para qualquer ε, podemos escolher w tal que as entradas de $\left((w^2A^*)^{-1}(wQ_1 + Q_0)\right)^k$ são menores que ε, e o resultado segue. □

Como consequência do Lema 3.2.6, temos

$$\begin{aligned} \left\| A - w^2A_w \right\| &= \left\| \sum_{k=1}^{\infty} \left(\frac{A}{w^2} (-wQ_1 - Q_0) \right)^k A \right\| \approx \\ &\approx \left\| \frac{AQ_1A}{w} + \frac{AQ_0A}{w^2} \right\| = O\left(\frac{1}{w} \right). \end{aligned} \quad (3.8)$$

Assim, de uma maneira geral a proximidade entre as matrizes de Gram de Λ_w e de Λ é $O(1/w)$. Entretanto, se conseguirmos uma perturbação P tal que $Q_1 = \alpha A^*$ ($\Leftrightarrow AQ_1A = \alpha A$), obtemos uma sequência cuja ordem de convergência é $O(1/w^2)$, pois

$$\frac{A}{w^2} - \frac{\alpha A}{w^3} + \frac{AQ_0A}{w^4} = A\left(\frac{1}{w} - \frac{\alpha}{2w^2} \right)^2 + \frac{\alpha^2 A}{4w^4} + \frac{AQ_0A}{w^4} \quad (3.9)$$

e portanto a distância entre $A_w / \left(1/w - \alpha/2w^2\right)^2$ e A possui ordem $O(1/w^2)$.

Com relação ao item (ii), notemos que $\boldsymbol{v}_w$ pode ser dado, a menos de sinal, pelo produto vetorial generalizado (ver e.g. [Spi71]) das linhas de L_w^*. Com efeito, seja $(\overline{\boldsymbol{v}}_w)_i = (-1)^{n+i} \, |\overline{(L_w^*)_i}|$, onde $|\overline{(L_w^*)_i}|$ denota o determinante da matriz obtida excluindo-se a i-ésima coluna de L_w^*. De acordo com o Lema 3.2.5, o vetor projeção $\boldsymbol{v}_w$ é dado por $\boldsymbol{v}_w = (1, -\hat{\boldsymbol{v}}_w)$, onde

$$\hat{\boldsymbol{v}}_w = (L_w^*)_1^t (H_w)^{-t} \Rightarrow (L_w^*)_1^t = \hat{\boldsymbol{v}}_w H_w = -\sum_{j=2}^{n} (\boldsymbol{v}_w)_j (L_w^*)_j^t.$$

Portanto

$$\begin{aligned}|\overline{(L_w^*)_i}| &= \det\left(-\sum_{j=2}^{n}(\boldsymbol{v}_w)_j(L_w^*)_j \mid (L_w^*)_2 \mid \ldots \mid \widehat{(L_w^*)_i} \mid \ldots \mid (L_w^*)_n\right)\\ &= \det\left(-(\boldsymbol{v}_w)_i(L_w^*)_i \mid (L_w^*)_2 \mid \ldots \mid \widehat{(L_w^*)_i} \mid \ldots \mid (L_w^*)_n\right)\\ &= (-1)^i\,|H_w|\,(\boldsymbol{v}_w)_i.\end{aligned}$$

onde $\widehat{(L_w^*)_i}$ significa a exclusão da i-ésima coluna. Considerando esta caracterização, temos que cada entrada $(\boldsymbol{v}_w)_i$, $i = 1, \ldots, n-1$ é um polinômio cujo grau é no máximo $n-1$, e $(\boldsymbol{v}_w)_n = |\det \overline{(L_w^*)}_n| = |\det \overline{(wL^* + P)_n}| = |w^n \det \tilde{L}^* + O(w^{n-1})|$.

Pelas análises de (i) e (ii), concluímos que de uma maneira geral a distância entre Λ_w e Λ e a norma do vetor projeção satisfaz

$$\left\|A - w^2 A_w\right\| = O\left(\frac{1}{w}\right) = O\left(\frac{1}{\|\boldsymbol{v}_w\|^{1/(n-1)}}\right).$$

Entretanto, vimos também que sob certas condições entre as matrizes Q_1 e A, podemos acelerar esta convergência. Em suma, temos o seguinte:

Teorema 3.2.7. *[CS13] Seja Λ_w^* a sequência de reticulados com matrizes geradoras* (3.2.2) *e considere H_w, Q_0 e Q_1 como definidos em* (3.5)*. Suponha que as condições abaixo são satisfeitas*

$$\det(H_w) = \pm 1, \forall w \in \mathbb{N} \text{ e} \tag{3.10}$$

$$\exists \alpha \text{ tal que } Q_1 = \alpha A^*, \tag{3.11}$$

Temos então que cada reticulado da sequência $\Lambda_w = (\Lambda_w^*)^*$ é projeção de $\mathbb{Z}^n$ no hiperplano ortogonal a um vetor $\boldsymbol{v}_w \in \mathbb{Z}^n$ cuja norma satisfaz

$$\|\boldsymbol{v}_w\|_\infty = \left|\sqrt{\det \Lambda^*} w^{n-1} + O(w^{n-2})\right| \tag{3.12}$$

para w suficientemente grande. Além disso, existe $c_w \in \mathbb{R}$ tal que

$$\|A - c_w A_w\|_\infty = O\left(\frac{1}{w^2}\right) = O\left(\frac{1}{\|\boldsymbol{v}_w\|_\infty^{2/(n-1)}}\right) \to 0, \text{ quando } w \to \infty. \quad (3.13)$$

É fácil notar que utilizando a estrutura (3.2.2) não é possível conseguirmos sequências com uma ordem de convergência melhor que $O\left(\|\boldsymbol{v}_w\|_\infty^{-2/(n-1)}\right)$. Deste modo, daqui para frente nos referiremos a tais sequências como *ótimas*, entendendo que este termo refere-se apenas a projeções com a estrutura (3.2.2). Exibiremos construções explícitas de sequências ótimas de projeções.

Observação 3.2.8. *Um exemplo de uma sequência de projeções ótima convergindo para $\Lambda = D_3$ pode ser encontrado em [SVC11, Seção 4], como uma construção ad hoc. Veremos em breve que tal exemplo encaixa-se nas condições do Teorema 3.2.7.*

Observamos que quando não há matriz de perturbação tal que $Q_1 = \alpha A^*$, a convergência da sequência de reticulados Λ_w é dominada pelo coeficiente $A(Q_1 - \alpha A^*)A$ (Equação (3.8)). Podemos, portanto, produzir boas sequências de projeção através a solução do problema de minimização

$$\begin{aligned} &\min \left\| A(L^* P^t + P L^{*t} - \alpha A^*)A \right\|_\infty \\ &\text{s. t.} \quad |\det H_w| = 1 \ , \forall w \in \mathbb{N} \\ &P \in \mathbb{Z}^{n\times(n+1)} \\ &\alpha \in \mathbb{Z} \end{aligned} \quad (3.14)$$

que é um problema não linear com $n^2 + n$ variáveis inteiras. A maior complexidade do problema está na restrição $|\det H_w| = 1$. Portanto, algumas vezes é interessante considerarmos soluções sub-ótimas. Uma possibilidade é escolhermos uma matriz L^* triangular inferior e considerarmos

$$\min \left\| A(L^* P^t + P L^{*t} - \alpha A^*)A \right\|_\infty$$

$$\text{s. t.} \quad P \in \mathbb{Z}^{n\times(n+1)} \tag{3.15}$$

$$P_{ij} = 1, \text{ if } j = i+1$$

$$P_{ij} = 0, \text{ if } j > i+1,$$

$$\alpha \in \mathbb{Z}$$

Neste caso, a restrição $|H_w| = 1$ é trivialmente satisfeita. Se trabalharmos com a norma de Fröbenius dada por $\|A|_F = \sqrt{\text{tr}(AA^t)}$, temos um problema de programação quadrática inteira (IQP).

3.2.3 Construções explícitas

No que segue, empregamos diferentes estratégias para gerar sequências ótimas/subótimas de reticulados projeção, a depender da estrutura de cada reticulado Λ e da factibilidade em encontrar soluções inteiras satisfazendo as condições (3.10) e (3.11), ou em resolver o problema não-linear (3.15).

O reticulado $a\mathbb{Z} \oplus b\mathbb{Z}$

Como exemplo inicial ilustrativo, seja o reticulado $a\mathbb{Z} \oplus b\mathbb{Z}$, com a e b inteiros não nulos tais que $\text{mdc}(a, b) = 1$. Como uma matriz geradora para um reticulado equivalente ao seu dual, escolhemos $\tilde{L}^* = \text{diag}(a, b)$. Assim, dada um perturbação geral P, temos

$$L_w^* = \begin{pmatrix} aw + P_{11} & P_{12} & P_{13} \\ P_{21} & bw + P_{22} & P_{23} \end{pmatrix} \tag{3.16}$$

Neste caso, a condição (3.11) é equivalente a:

$$P_{11} = \frac{a\alpha}{2}, P_{21} = -\frac{bP_{12}}{a} \text{ e } P_{22} = \frac{\alpha b}{2} \tag{3.17}$$

Como a e b não possuem fatores comuns, α deve ser par ($\alpha = 2\beta$, para $\beta \in \mathbb{Z}$) e P_{12} deve ser múltiplo de a ($P_{12} = ka$). Sob estas condições o determinante de H_w é dado por

$$\det(H_w) = akP_{23} - b\beta P_{13} - bwP_{13} \tag{3.18}$$

e a condição (3.10) será satisfeita para todo d se, e somente se

$$P_{13} = 0 \text{ and } akP_{23} = \pm 1. \tag{3.19}$$

Portanto, pelo teorema 3.2.7, para qualquer β a família de vetores

$$\boldsymbol{v}_w = (1, -w - \beta, bw^2 + 2b\beta w + b\beta^2 + b)$$

está associada a sequências de projeções ótimas que convergem para $\mathbb{Z} \oplus b\mathbb{Z}$. Por outro lado, para $a \neq 1$ não é possível achar uma matriz de perturbação tal que as condições de 3.2.7 sejam satisfeitas. Isso nos mostra que representações equivalentes distintas de um mesmo reticulado podem ser mais convenientes ao trabalharmos com sequências de projeção.

O reticulado D_n (n ímpar)

Como matriz geradora para um reticulado equivalente a D_n^* escolhemos

$$L^* = \begin{bmatrix} 2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 2 & 0 & 0 \\ 1 & 1 & \cdots & 1 & 1 & 0 \end{bmatrix}$$

Temos a seguinte proposição

Proposição 3.2.9. *Seja n um número ímpar. Existe uma sequência ótima de reticulados projeção de $\mathbb{Z}^{n+1}$ que converge para D_n.*

Demonstração. A demonstração segue escolhendo uma matriz de perturbação conveniente. Neste caso, tome P tal que

$$P_{ij} = \begin{cases} (-1)^i & \text{se } j = n - i \text{ e } 1 \leq i \leq n, \\ (-1)^{i+1} & \text{se } j = n - i + 2 \text{ e } 2 \leq i \leq n - 1, \\ 1 & \text{se } (i,j) \in \{(n-1, n+1), (n, n+1)\} \\ 1 & \text{se } (i,j) = (1,n) \\ 0 & \text{caso contrário} \end{cases} \tag{3.20}$$

Por multiplicação direta, mostra-se que $Q_0 = L^* P^t + P L^{*t} = 0$ e, através de operações elementares na matriz H_w, temos que $\det H_w = 1 \; \forall w$ se n for um número par. Assim, ambas as condições do Teorema 3.2.7 são satisfeitas e temos uma sequência ótima de vetores. □

Observação 3.2.10. *Para n par, com um pouco de álgebra, pode-se mostrar que $L^* P^t + P L^{*t} \neq 0$ e $\det H_w = 1 \pm w$, e assim as sequências obtidas não satifazem as hipóteses do Teorema 3.2.7. De fato, para $n = 4$ e uma busca computacional exaustiva por soluções, é possível provar que não há matriz de perturbação que satisfaza tais hipóteses. Assim, para encontrar boas sequências neste caso, seriam necessárias técnicas diferentes das apresentadas aqui.*

Para $n = 5$, temos que a sequência de projeções do $\mathbb{Z}^6$ associada às matrizes abaixo converge para o reticulado D_5, o mais denso em $\mathbb{R}^5$.

$$L_w^* = \begin{pmatrix} 2w & 0 & 0 & -1 & 1 & 0 \\ 0 & 2w & 1 & 0 & -1 & 0 \\ 0 & -1 & 2w & 1 & 0 & 0 \\ 1 & 0 & -1 & 2w & 0 & 1 \\ w & w & w & w & w & 1 \end{pmatrix} \tag{3.21}$$

$$A_w^* = \begin{pmatrix} 4w^2+2 & -1 & -1 & 0 & 2w^2 \\ -1 & 4w^2+2 & 0 & -1 & 2w^2 \\ -1 & 0 & 4w^2+2 & 0 & 2w^2 \\ 0 & -1 & 0 & 4w^2+3 & 2w^2+1 \\ 2w^2 & 2w^2 & 2w^2 & 2w^2+1 & 5w^2+1 \end{pmatrix},$$

$$P = \begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ e } \boldsymbol{v}_w = \begin{pmatrix} 1 \\ 4w^3+2w^2+3w+1 \\ -4w^3+2w^2-3w+1 \\ 8w^4+8w^2+w+1 \\ 8w^4+8w^2-w+1 \\ 16w^5+20w^3+5w \end{pmatrix}$$

Observação 3.2.11. *Para $n = 3$ e uma mudança de base conveniente, a perturbação dada por* (3.21) *é precisamente a mesma obtida como uma construção ad hoc em [SVC11, Sec. 4].*

O reticulado D_n^*

A família de reticulados D_n^* representa um caso em que é necessátrio tomar $\alpha \neq 0$ na condição (3.11). Seja a matriz geradora para $(D_3^*)^* = D_3$ dada abaixo.

$$L^* = \begin{pmatrix} -2 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}, \tag{3.22}$$

Gostariamos de encontrar uma perturbação P inteira de ordem 3×4 que satisfaça as hipóteses do Teorema (3.2.7). A condição (3.10) com $\alpha = 0$ é equivalente às

equações

$$\begin{aligned} &P_{11} = 0, P_{12} = -2P_{23} + 2P_{31} - 2P_{33}, P_{21} = P_{23} - P_{31} + P_{33}, \\ &P_{22} = P_{23} - P_{31} + P_{33}, P_{13} = -2P_{23} - 2P_{33}, P_{32} = P_{33}. \end{aligned} \tag{3.23}$$

Além disso, vemos que o coeficiente de w^2 na expansão polinomial do determinante de H_w é igual a $P_{1,4}$, e portanto temos que ter $P_{1,4} = 0$ para assegurar (3.11). Sob estas condições, temos:

$$H_w = \begin{pmatrix} -2P_{23} + 2P_{31} - 2P_{33} & -2P_{23} - 2P_{33} & 0 \\ -w + P_{23} - P_{31} + P_{33} & P_{23} & P_{24} \\ w + P_{33} & P_{33} - w & P_{34} \end{pmatrix}. \tag{3.24}$$

e claramente $\det H_w$ é par i.e., não há como satisfazer a condição (3.11). Entretanto, seguindo uma mesma linha de argumentação, encontramos facilmente a perturbação que produz sequências ótimas

$$P = \begin{pmatrix} -1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & -2 \end{pmatrix}. \tag{3.25}$$

Estendendo esta construção para qualquer n, temos a seguinte proposição:

Proposição 3.2.12. *Existe uma sequência ótima de reticulados projeção de $\mathbb{Z}^{n+1}$ que converge para D_n^*.*

Demonstração. Seja a matriz de perturbação dada por

$$P_{ij} = \begin{cases} (-1)^i \binom{n-1}{i-1} & \text{se } j = n+1 \text{ e } i \geq 2, \\ -1 & \text{se } i = j, \\ 1 & \text{se } i = 1 \text{ e } j \leq n, \\ 0 & \text{caso contrário.} \end{cases}. \tag{3.26}$$

Por multiplicação direta, vemos que $G^* P^t + P G^{*t} = A^*$ ($\alpha = 1$) e através de

operações elementares em H_w vemos que $\det H_w = (-1)^{n+1}$, o que demonstra a proposição. □

Para $n = 3$, a sequência ótima de projeções associada aos vetores

$$\boldsymbol{v}_w = \left(1, -2w^2 + w + 1, -2w^2 - 3w - 2, 2w^3 + 3w^2 + 3w + 1\right)$$

converge para o reticulado cúbico de face centrada, de maior densidade de cobertura em $\mathbb{R}^3$ [CS98].

O reticulado E_8

Para o reticulado E_8, o mais denso em 8 dimensões, o problema de encontrar uma matriz de perturbação associada a uma sequência ótima possui 72 variáveis inteiras. Após algumas simplificações, podemos reduzir este problema a 36 variáveis inteiras e 7 restrições não lineares. Para diminuir a complexidade computacional do problema, trabalhamos com o IQP (3.15). Comparamos também diferentes representações do reticulado E_8. Mostramos abaixo que mesmo soluções associadas a sequências sub-ótimas podem nos prover grandes ganhos em termos da relação entre densidade de centro do reticulado produzido e a norma do vetor projeção.

A primeira representação de $\Lambda^* = E_8$ utilizada é a matriz (1.15), para a qual utilizamos a perturbação P_1 abaixo. A segunda, é a representação obtida aplicando a Construção A do Capítulo 2 ao código de Hamming estendido $\mathcal{H}(8, 4)$, e neste caso utilizamos P_2 como matriz de perturbação. Abaixo estão as respectivas matrizes de perturbação. Na Figura 3.2 um gráfico com as diferentes sequências geradas pelas perturbações P_1 e P_2. As duas primeiras curvas, de baixo para cima, foram otidas com a primeira representação para E_8 e matrizes de perturbação $(0\ I)$ (Construção *Lifting*) e P_1, respectivamente. As duas últimas curvas correspondem à segunda representação de E_8 e matrizes de pertrubação

$(0\ I)$ e P_2.

$$P_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$P_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0 & 1 \end{pmatrix}.$$

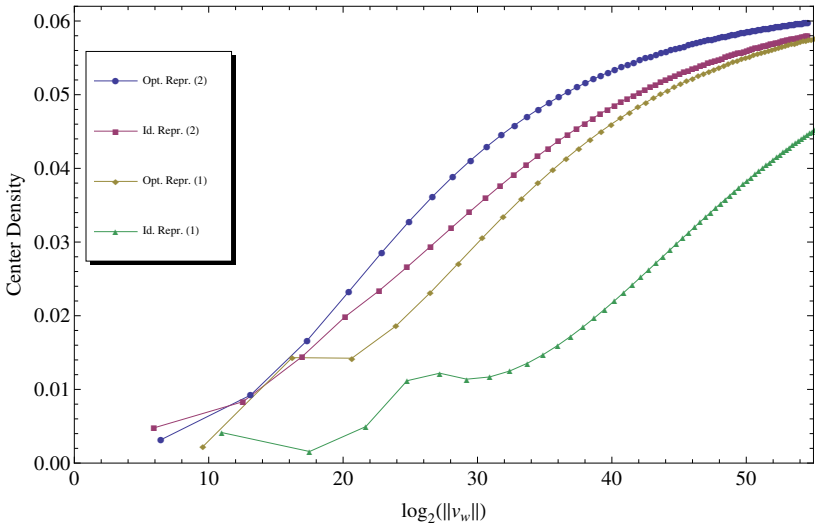


Figura 3.2: Comparação entre diferentes sequências de projeções convergindo para o reticulado E_8.

Finalizamos esta seção exibindo uma tabela de vetores associado às melhores sequências de reticulados projeção no sentido de norma do vetor versus densidade em dimensões $n = 3, 4, 5, 6, 7$ e 8. No $\mathbb{R}^6$, não é de nosso conhecimento uma matriz geradora inteira para alguma representação do E_6, assim as técnicas vistas para convergência acelerada não se aplicam. Abaixo, mostramos uma sequência de vetores associados a projeções que convergem para D_6. Para uma sequência não-ótima que converge para E_6 podemos utilizar diretamente a Construção *Lifting*.

n (Λ)	**Vetor**
3 (D_3)	$(1, 2w^2 + w + 1, 2w^2 - w + 1, -4w^3 - 3w)$
4 (D_4)	$(1, -1 + 2w, 4w^2 - 2w + 1, 8w^3 - 4w^2 + 1, 8w^4 - 8w^3 + 4w^2)$
5 (D_5)	$(1, 4w^3 + 2w^2 + 3w + 1, -4w^3 + 2w^2 - 3w + 1$ $8w^4 + 8w^2 + w + 1, 8w^4 + 8w^2 - w + 1, 16w^5 + 20w^3 + 5w)$
6 (D_6)	$(1, 2w - 1, 4w^2 - 2w + 1, 8w^3 - 4w^2 + 1, 16w^4 - 8w^3 + 4w^2 + 1$ $32w^5 - 16w^4 + 4w^2 + 2w - 1, 32w^6 - 32w^5 + 16w^4 + 2w^2 - 2w + 1)$
7 (E_7)	$(1, 1 - 2w, 4w^2 - 4w + 2, -8w^3 + 12w^2 - 10w + 3,$ $8w^4 - 16w^3 + 18w^2 - 10w + 2$ $-8w^5 + 16w^4 - 30w^3 + 28w^2 - 16w + 4$ $8w^6 - 16w^5 + 38w^4 - 44w^3 + 36w^2 - 16w + 3$ $-8w^7 + 16w^6 - 46w^5 + 60w^4 - 70w^3 + 50w^2 - 24w + 5)$
8 (E_8)	$(1, -2w, 4w^2, -8w^3, 16w^4 + 8w^3 - 2w, -16w^5 - 8w^4 - 4w^3 + 4w^2 + w$ $16w^6 + 8w^5 + 12w^4 - 3w^2, -16w^7 - 8w^6 - 28w^5 + 7w^3 + 6w^2$ $16w^8 + 8w^7 + 44w^6 + 8w^5 - 3w^4 - 10w^3 - 3w^2 + w)$

Tabela 3.2: Famílias ótimas de reticulado projeção.

3.3 Projeções de Reticulados Gerais

Apesar do reticulado cúbico $\mathbb{Z}^n$ possuir propriedades bastante especiais, como auto-dualidade e base ortonormal, nenhuma delas foi de fato fortemente utilizada na Construção *Lifting* da Seção 3.2. Assim, uma questão natural é se o Teorema 3.2.3 ainda permanece válido ao substutímos $\mathbb{Z}^n$ por algum outro reticulado. Nesta seção, responderemos a esta pergunta em completa generalidade. Mostraremos o seguinte:

Teorema 3.3.1 ([CSC13])**.** *Sejam Λ_1 e Λ_2 reticulados de posto n e $(n-k)$, respectivamente. Existe uma sequência de matrizes V_w cujas linhas formam um conjunto primitivo de vetores de Λ_1 tal que $P_{V_w^{\perp}}(\Lambda_1) \to \Lambda_2$, quando $w \to \infty$.*

Para nossa construção geral, necessitamos de alguns elementos. Assumimos, sem perda de generalidade, que Λ_1 possui matriz geradora B triangular superior e a dividimos por blocos conforme a equação abaixo:

$$B = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}, \tag{3.27}$$

onde B_1 e B_3 são matrizes quadradas triangulares superiores de ordem $k \times k$ e $(n-k) \times (n-k)$, respectivamente. Qualquer matriz geradora para Λ_1 pode ser colocada nesta forma através de uma transformação de equivalência. Com efeito, seja $\tilde{B}$ uma outra matriz geradora para Λ_1. Através de uma fatoração RQ [Mey00] (ou ortogonalização de Gram-Schmidt nas linhas de $\tilde{B}$ começando pela última), encontramos uma matriz ortogonal Q e uma triangular superior R tais que $\tilde{B} = RQ$. Desta maneira, os reticulados gerados por R e $\tilde{B}$ são equivalentes e podemos tomar $B = R$, na forma (3.27).

Consideremos agora, uma matriz A inteira de ordem $k \times n$ da forma

$$A = \begin{pmatrix} I & \hat{A} \end{pmatrix}.$$

Seja $V = AB = \begin{pmatrix} B_1 & B_2 + \hat{A}B_3 \end{pmatrix}$. Como o primeiro determinante menor $k \times k$ de A é igual a 1, temos que as linhas de V formam um conjunto primitivo de vetores de Λ_1, pela caracterização (ii) do Teorema 1.1.9. Para facilitar nossa discussão, introduzimos as matrizes

$$\hat{V} = B_2 + \hat{A}B_3 \text{ e}$$

$$M = \begin{pmatrix} -B_3^{-t}\hat{V}^t B_1^{-t} & B_3^{-t} \end{pmatrix}. \tag{3.28}$$

Lema 3.3.2. *Seja $\Lambda_1 = \Lambda_1(B)$ um reticulado gerado por uma matriz B na forma (3.27). Sejam as matrizes V e M definidas acima. Temos:*

$$\Lambda(M) = \Lambda_1^* \cap \operatorname{span}(V)^\perp = P_{V^\perp}(\Lambda_1)^*. \tag{3.29}$$

Demonstração. A segunda igualdade do lema nada mais é que a Proposição 3.1.4 aplicada à matriz V. Para a primeira igualdade, provemos a inclusão $\Lambda(M) \subseteq \Lambda_1^* \cap \operatorname{span}(V)^\perp$. Seja $\boldsymbol{x} \in \Lambda(M)$, $\boldsymbol{x} = \boldsymbol{u}M$ com $\boldsymbol{u} \in \mathbb{Z}^k$. Por multiplicação direta, vemos que $\boldsymbol{x}V^t = \boldsymbol{0}$. Além disso, se $\boldsymbol{y} = \boldsymbol{w}B$ é um elemento de Λ_1, então

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{w}BM^t\boldsymbol{u}^t = \boldsymbol{w} \begin{pmatrix} -\hat{V}B_3^{-1} + B_2B_3^{-1} \\ I_{n-k} \end{pmatrix} \boldsymbol{u}^t = \boldsymbol{w} \begin{pmatrix} \hat{A} \\ I_{n-k} \end{pmatrix} \boldsymbol{u}^t \in \mathbb{Z},$$

portanto $\boldsymbol{x} \in \Lambda_1^*$, demonstrando a inclusão. Para provar que a inclusão é de fato uma igualdade, basta mostrar que $\Lambda(M)$ e $P_{V^\perp}(\Lambda_1)^*$ possuem mesmo determinante. De fato:

$$\begin{aligned} \det \Lambda(M) &= \det MM^t = \det(B_3^{-t}\hat{V}^t B_1^{-t} B_1^{-1}\hat{V}B_3^{-1} + B_3^{-t}B_3^{-1}) \\ &= \det(B_3^{-t}B_3^{-1}) \det(\hat{V}^t B_1^{-t}B_1^{-1}\hat{V} + I) \\ &= \det(B_3^{-t}B_3^{-1}) \det(B_1^{-1}\hat{V}\hat{V}^t B_1^{-t} + I) \\ &= \det(B_3^{-t}B_3^{-1}) \det(B_1^{-t}B_1^{-1}) \det(\hat{V}\hat{V}^t + B_1B_1^t) = \frac{\det(VV^t)}{\det \Lambda_1}. \end{aligned}$$

Comparando o resultado acima com a Proposição 3.1.3, concluímos a demonstração. □

Demonstração do Teorema 3.3.1: Assim como a demonstração no caso de projeções de $\mathbb{Z}^n$, vamos mostrar a versão dual de 3.3.1, ou seja, construir sequências de duais de projeções de Λ_1 que convergem, a menos de equivalência, para o dual de Λ_2.

Seja uma representação de Λ_2 cujo dual possui matriz geradora $\tilde{L}^*$ triangular inferior de ordem $(n-k)\times(n-k)$. Seja uma realização de Λ_2 em $\mathbb{R}^n$ obtida adicionando-se k colunas de zeros à matriz $\tilde{L}^*$, isto é

$$L^* = \left(\tilde{L}^* \quad \mathbf{0}\right), \tag{3.30}$$

onde L^* possui ordem $(n-k)\times n$. Consideramos também uma outra decomposição de L^*, da forma

$$L^* = \left(L_1^* \quad L_2^*\right), \tag{3.31}$$

em que L_1^* e L_2^* possuem ordem $(n-k)\times k$ e $(n-k)\times(n-k)$, respectivamente. Note que L_1^* e L^* possuem o mesmo número de colunas, correspondente ao posto do reticulado Λ. Seja $w \geq 1$ um número inteiro. Utilizando as notações (3.27) e (3.31), definimos as matrizes

$$H_w = \lfloor wL_2^* B_3^t \rfloor + I, \tag{3.32}$$

$$(L_w^*)_1 = \left(\lfloor wL_1^* B_1^t + H_w B_3^{-t} B_2^t \rfloor - H_w B_3^{-t} B_2^t\right) B_1^{-t},$$

$$(L_w^*)_2 = H_w B_3^{-t} \text{ e}$$

$$L_w^* = \left((L_w^*)_1 \quad (L_w^*)_2\right). \tag{3.33}$$

Seja a sequência de reticulados $\Lambda_w^* = \Lambda(L_w^*)$. No que segue, provaremos:

(i) Λ_w^* é equivalente a $P_{V_w^\perp}(\Lambda_1)^*$ para alguma matriz V_w cujas linhas são um conjunto primitivo de Λ_1.

(ii) Λ_w^* converge, a menos de equivalência, para Λ_2.

Para provar a primeira afirmação, observamos que, como L^* e B_3^t são matrizes

triangulares inferiores, e as entradas da diagonal de L_2^* são nulas, H_w é uma matriz triangular inferior com todos os elementos da diagonal iguais a um. Portanto, H_w é unimodular, assim como H_w^{-1}. Portanto, cada reticulado Λ_w^* é também gerado pela matriz $H_w^{-1}L_w^*$. Desenvolvendo o produto matricial, temos

$$\begin{aligned} H_w^{-1}L_w^* &= \begin{pmatrix} H_w^{-1}(L_w^*)_1 & B_3^{-t} \end{pmatrix} \\ &= \begin{pmatrix} \left(H_w^{-1}\lfloor wL_1^*B_1^t + H_wB_3^{-t}B_2^t\rfloor - B_3^{-t}B_2^t\right)B_1^{-t} & B_3^{-t} \end{pmatrix} \\ &= \begin{pmatrix} -\hat{A}^tB_1^{-t} - B_3^{-t}B_2^tB_1^{-t} & B_3^{-t} \end{pmatrix} \\ &= \begin{pmatrix} -B_3^{-t}\hat{V}^tB_1^{-t} & B_3^{-t} \end{pmatrix}, \end{aligned} \tag{3.34}$$

com $\hat{A}^t = -H_w^{-1}\lfloor wL_1^*B_1^t + H_wB_3^{-t}B_2^t\rfloor$ uma matriz inteira de ordem $(n-k)\times k$ e $\hat{V}^t = B_2^t + B_3^t\hat{A}^t$. Comparando estes resultados com a Equação (3.28) e com o Lema 3.3.2, concluímos (i) com V_w dado por

$$V_w = [B_1 \quad B_2 - (H_w^{-1}\lfloor wL_1^*B_1^t + H_wB_3^{-t}B_2^t\rfloor)^tB_3]. \tag{3.35}$$

Para demonstrar (ii), começamos com as seguintes desigualdades simples sobre a operação de chão

$$\begin{aligned} \frac{1}{w}(\lfloor wL_1^*B_1^t + H_wB_3^{-t}B_2^t\rfloor - H_wB_3^{-t}B_2^t)_{ij} &\geq (L_1^*B_1^t)_{ij} - \frac{1}{w} \\ \frac{1}{w}(\lfloor wL_1^*B_1^t + H_wB_3^{-t}B_2^t\rfloor - H_wB_3^{-t}B_2^t)_{ij} &\leq (L_1^*B_1^t)_{ij} \end{aligned}.$$

Daí, obtemos

$$\frac{1}{w}(\lfloor wL_1^*B_1^t + H_wB_3^{-t}B_2^t\rfloor - H_wB_3^{-t}B_2^t) \to L_1^*B_1^t \text{ as } w\to\infty,$$

e portanto $(L_w^*)_1/w \to L_1^*$. Analogamente, é possível provar que $(L_w)_2^*/w \to L_2^*$. Desta maneira:

$$\lim_{w\to\infty}\frac{L_w^*}{w} = (L^* \quad \mathbf{0}) \Rightarrow \lim_{w\to\infty}\frac{L_w^*L_w^{*t}}{w^2} = L^*L^{*t} \tag{3.36}$$

concluindo a demonstração. □

Uma consequência da demonstração acima é o seguinte corolário, que nos da uma análise de convergência da sequência dual Λ_w^* construída.

Corolário 3.3.3. *Na linguagem da demonstração do Teorema 3.3.1, temos:*

$$\left\|L^*L^{*t} - (1/w^2)L_w^*L_w^{*t}\right\|_\infty = \begin{cases} O(1/\left\|V_w\right\|_\infty^{1/(n-2k+1)}) & \text{se } k < n/2 \\ \\ O(1/\left\|V_w\right\|_\infty) & \text{se } k \geq n/2 \end{cases} \tag{3.37}$$

Demonstração. Da construção (3.33) está claro que:

$$\left\|L^*L^{*t} - \frac{1}{w^2}L_w^*L_w^{*t}\right\|_\infty = O\left(\frac{1}{w}\right)$$

Se $k \geq n/2$, então a matriz L_2^* é simplesmente a matriz nula, e portanto $H_w = H_w^{-1} = I_{n-k}$. Assim, pela Equação (3.35), $\left\|V_w\right\|_\infty = \Theta(w)$. Caso contrário, cada co-fator de H_w (e portanto cada elemento de H_w^{-1}) possui ordem w^{n-2k}. Assim, $\left\|V\right\|_\infty = \Theta(w^{n-2k+1})$ e o resultado segue. □

3.3.1 Exemplos

Para ilustrar o mecanismo construtivo da demonstração do Teorema 3.3.1, exibimos abaixo três exemplos.

Projeções de $\mathbb{Z}^n$ em subespaços de dimensão qualquer

Seja $\Lambda_1 = \mathbb{Z}^n$ e Λ_2 um reticulado qualquer, de posto $(n-k)$. Tome $B = I_n$, tal que $B_1 = I_k$, $B_3 = I_{n-k}$ e $B_2 = 0$. Seja $\tilde{L}^*$ uma matriz geradora triangular inferior para o reticulado Λ_2^*. Para $k \leq n/2$, a sequência de vetores produzida pela nossa construção é dada por:

$$V_w = \begin{pmatrix} I_k & \lfloor wL_1^{*t} \rfloor (\lfloor wL_2^* \rfloor + I_{n-k})^{-t} \end{pmatrix}, \tag{3.38}$$

com L_1^* e L_2^* definido como em (3.33). Se $k \geq n/2$, então

$$V_w = \begin{pmatrix} I_k & \begin{pmatrix} \lfloor w\tilde{L}^* \rfloor \\ \mathbf{0} \end{pmatrix} \end{pmatrix} \tag{3.39}$$

isto é, os últimos $2k-n$ vetores são simplesmentes o vetores canônicos $\boldsymbol{e}_i$, $i = n-k+1, \ldots, k$. Isso sugere graus de liberdade na construção, o que pode permitir uma melhora na taxa de convergência dada pelo Corolário 3.3.3.

Observação 3.3.4. *Para $k = 1$, a construção apresentada acima é exatamente a Construção Lifting.*

Projeções de reticulados retangulares

Projeções de reticulados retangulares $\Lambda_{\boldsymbol{c}} = c_1\mathbb{Z} \oplus \ldots \oplus c_n\mathbb{Z}$ em hiperplanos são de particular interesse devido a suas aplicações em comunicações, como será mostrado no Capítulo 4. Como usual, seja Λ_2 um reticulado alvo e L^* uma matriz geradora triangular inferior para alguma representação do seu dual. A sequência L_w^* produzida a partir da construção (3.33) é dada por:

$$L_w^* = \begin{pmatrix} \lfloor wL_{11}^* c_1 \rfloor / c_1 & 1/c_2 & \ldots & \ldots & 0 \\ \lfloor wL_{21}^* c_1 \rfloor / c_1 & \lfloor wL_{22}^* c_2 \rfloor / c_2 & \ldots & \ldots & 0 \\ \vdots & \vdots & \ddots & \ldots & 0 \\ \lfloor wL_{n1}^* c_1 \rfloor / c_1 & \lfloor wL_{n2}^* c_2 \rfloor / c_2 & \ldots & \lfloor c_{n-1} wL_{nn}^* \rfloor / c_{n-1} & 1/c_n \end{pmatrix}, w \in \mathbb{N}. \tag{3.40}$$

Para um exemplo numérico, mostremos como produzir o reticulado hexagonal A_2 através de projeções de $c_1\mathbb{Z} \oplus c_2\mathbb{Z} \oplus c_3\mathbb{Z}$. Utilizando a notação da construção (3.33):

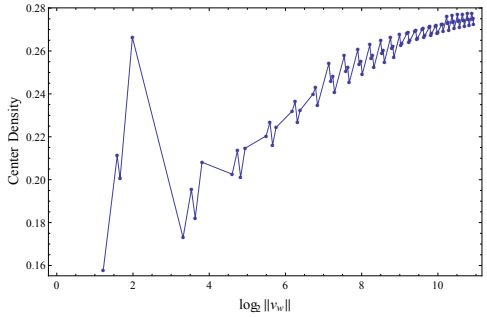
$$B = \begin{pmatrix} c_1 & 0 & 0 \\ 0 & c_2 & 0 \\ 0 & 0 & c_3 \end{pmatrix}, \; L_w^* = \begin{pmatrix} \lfloor wc_1 \rfloor / c_1 & 1/c_2 & 0 \\ \left\lfloor \frac{wc_2}{2} \right\rfloor / c_2 & \left\lfloor \frac{1}{2}\sqrt{3} wc_2 \right\rfloor / c_2 & 1/c_3 \end{pmatrix},$$

$$H_w = \begin{pmatrix} 1/c_2 & 0 \\ \left\lfloor \frac{1}{2}\sqrt{3}wc_2 \right\rfloor / c_2 & 1/c_3 \end{pmatrix},$$

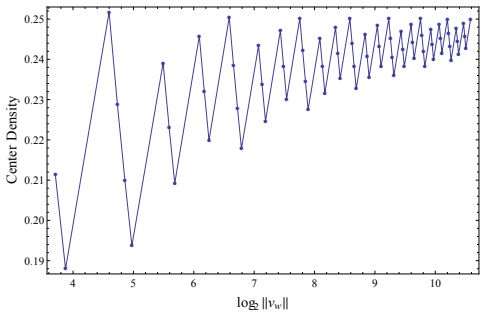
Realizando a multiplicação $H_w^{-1} L_w^*$ recuperamos a sequência de vetores:

$$\boldsymbol{v}_w = \begin{pmatrix} c_1 & -\lfloor wc_1 \rfloor c_2 & -\left(\left\lfloor \frac{wc_1}{2} \right\rfloor - \lfloor wc_1 \rfloor \left\lfloor \frac{1}{2}\sqrt{3}wc_2 \right\rfloor \right) c_3 \end{pmatrix}. \tag{3.41}$$

Na Figura 3.3(a) verificamos numericamente que a sequência de projeções de $c_1\mathbb{Z} \oplus c_2\mathbb{Z} \oplus c_3\mathbb{Z}$ em $v_w^{\perp}$ converge, a menos de equivalência, para o reticulado A_2. Na Figura 3.3(b), exibimos uma sequência de projeções de $c_1\mathbb{Z} \oplus c_2\mathbb{Z} \oplus c_3\mathbb{Z}$ convergindo para $\mathbb{Z}^2$.



(a) Reticulado hexagonal



(b) Reticulado $\mathbb{Z}^2$.

Figura 3.3: Exemplos numéricos de projeções de $c_1\mathbb{Z} \oplus c_2\mathbb{Z} \oplus c_3\mathbb{Z}$, $c_1 = 1$, $c_2 = 0.3$ e $c_3 = 0.8$

3.4 Extensões e Referências Futuras

Com um pouco de esforço adicional, o Teorema 3.3.1 pode ser estendido para projeções de sistemas periódicos. Seja $\mathcal{L}_2$ um sistema periódico.

$$\mathcal{L}_2 = \bigcup_{i=1}^{k} (\Lambda_2 + \boldsymbol{x}_i) \tag{3.42}$$

$\boldsymbol{x}_i \in \mathbb{R}^{n-k}$, e seja um reticulado de posto completo $\Lambda_1 \subset \mathbb{R}^n$. Da construção (3.33), podemos gerar uma sequência de reticulados Λ_w projeções de Λ_1 ao longo de sub-espaços de dimensão k tal que $\Lambda_w \to \Lambda_2$. Mais que isso, mostramos construtivamente que a sequência de matrizes $L_w = (L_w^*)^\dagger$ satisfaz

$$\Lambda(L_w) = P_{V_w^\perp}(\Lambda_1) \text{ e } wL_w \to \left(\tilde{L}^{-t} \;\; \mathbf{0}\right),$$

onde $\tilde{L}^{-t}$ é uma matriz geradora de Λ_2^*. Considere agora um sistema periódico da forma

$$\mathcal{L}_1 = \bigcup_{i=1}^{k} (\Lambda_1 + (1/w)\boldsymbol{y}_i). \tag{3.43}$$

onde $\boldsymbol{y}_i = (\boldsymbol{x}_i \;\; \mathbf{0}_{1\times k})$ é a imersão natural do vetor $\boldsymbol{x}_i$ em $\mathbb{R}^n$. Segue que

$$P_{V_w^\perp}(\mathcal{L}_1) = \bigcup_{i=1}^{k} \left(P_{V_w^\perp}(\Lambda_1) + (1/w)P_{V_w^\perp}(\boldsymbol{y}_i)\right). \tag{3.44}$$

Da nossa construção, temos que cada componente $P_{V_w^\perp}(\Lambda_1)$ está próxima (a menos de um fator de escala w) do reticulado Λ_2. Aplicando o fator de escala também em $(1/w)P_{V_w^\perp}(\boldsymbol{y}_i)$, e observando que $\lim_{w\to\infty} P_{V_w^\perp}(\boldsymbol{y}_i) = \boldsymbol{y}_i$, vemos que as projeções do sistema periódico $\mathcal{L}_1$ estão arbitrariamente próximas de $\mathcal{L}_2$.

Exemplo 3.4.1. *[Fabricando Diamantes] Considere a família de projeções de $\mathbb{Z}^4$ ao longo dos vetores:*

$$\boldsymbol{v}_w = (1, 2w, 4w^2, 4w^3 + 2w^2 + w).$$

Esta é a família obtida pela Construção Lifting com reticulado alvo D_3 do Exemplo 3.2.4. Calculando a pseudo-inversa de L_w^*, obtemos que os reticulados projeção Λ_w têm matriz geradora

$$L_w = \frac{1}{p(w)} \begin{pmatrix} -8w^5 & 0 & 8w^5 & 0 \\ 0 & -8w^5 & 8w^5 & 0 \\ 0 & 0 & -16w^5 & 0 \end{pmatrix} + M,$$

onde $p(w) = 16w^6+16w^5+28w^4+4w^3+5w^2+1$ *e* M *é uma matriz cujas entradas são todas da ordem de* $O(1/w^2)$*. Assim, vemos facilmente que*

$$\lim_{w\to\infty} wL_w = \begin{pmatrix} -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix},$$

sendo esta última uma matriz geradora para o reticulado escalonado $(1/2)D_3$*. Considere agora:*

$$\mathcal{L}_w = P_{\boldsymbol{v}_w^\perp}(\mathbb{Z}^4) \bigcup P_{\boldsymbol{v}_w^\perp}\left(\mathbb{Z}^4 + \left(\frac{1}{4w}, \frac{1}{4w}, \frac{1}{4w}, 0\right)\right).$$

À medida que w *cresce, o sistema periódico* $w\mathcal{L}_w$ *aproxima-se de uma realização no* $\mathbb{R}^4$ *do empacotamento diamante* D_3^+*.*

Por fim, a teoria de projeções de reticulados é muito rica e possui diversas outras nuances e aplicações além das consideradas nesta tese. Na tese de doutorado [McK10], McKilliam utiliza extensivamente intersecções de reticulados com hiperplanos para estudar os reticulados A_n e A_n^*, mostrando como obter eficientes algoritmos de decodificação para A_n^* e como calcular invariantes conhecidos como os momentos generalizados de A_n [MSVC12]. No recente trabalho [CSV13], são considerados algoritmos para encontrar vetores inteiros no hiperplano ortogonal a um vetor $\boldsymbol{x} \in \mathbb{R}^n$. Da mesma maneira que na Seção 3.3, encontrar uma base para $\Lambda \cap \operatorname{span}(V)^\perp$ é uma parte crucial para os resultados em [CSV13].

Indo além das técnicas estudadas aqui, projeções de reticulados estão presentes na bela teoria de quasicristais. Um exemplo são os ladrilhamentos de Penrose, descobertos pelo físico matemático Roger Penrose em [Pen74]. Através de caracterizações algébricas, De Bruijn [dB81] mostra que é possível produzir ladrilhamentos de Penrose através de intersecções de $\mathbb{Z}^5$ seguidas de projeções com certos subespaços de dimensão 2. O resultado são estruturas planas fascinantes

que não possuem simetria de translação, como a figura abaixo[1].

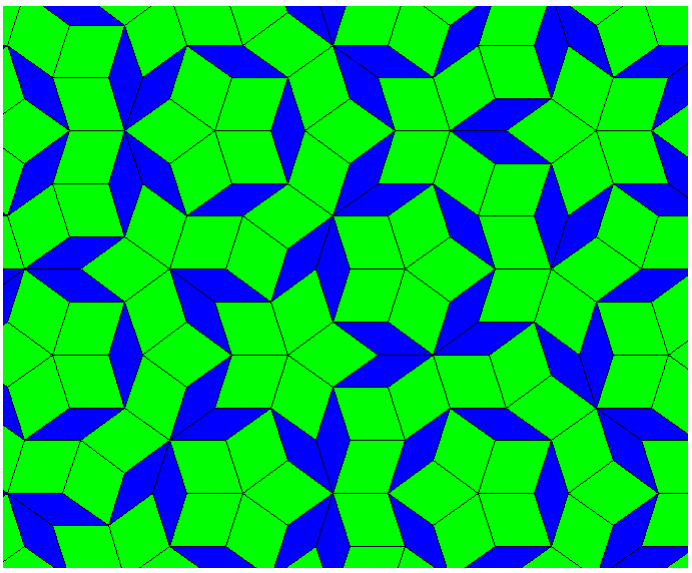


Figura 3.4: Ladrilhamento de Penrose

[1]Figura produzida utilizando o software "Bob - Penrose Tiling Generator and Explorer", disponível em http://stephencollins.net/penrose/

Capítulo 4

Curvas em Camadas de Toro

"Information theory does not handle the meaning of the information, it treats only the amount of information."

- Richard Hamming, *Coding and Information Theory*

Um fato notável da Teoria da Informação é o de que a maneira ótima de transmitirmos de uma fonte unidimensional com alfabeto contínuo e distribuição gaussiana através de um canal gaussiano unidimensional é o envio do sinal *sem* codificação (aplicando apenas um fator de escala de modo a respeitar a restrição de potência do canal) [Gob65]. Tal resultado nos mostra que técnicas digitais, apesar de atingirem otimalidade em diversos contextos, nem sempre representam a melhor estratégia de codificação/decodificação em termos de complexidade e *delay*.

Neste capítulo tratamos do problema da transmissão de uma fonte representada por uma variável aleatória real a ser transmitida através de um canal cujo ruído é aditivo, gaussiano e branco (definições mais precisas sobre o modelo de comunicação serão dadas na Seção 4.1). Como veremos adiante, se assumirmos que a dimensão do canal é maior que um, este problema reduz-se a encontrar curvas (aplicações de $\mathbb{R}$ em $\mathbb{R}^n$) satisfazendo certas restrições geométricas. Mostramos como construir tais curvas utilizando camadas de toro. Os elementos para nossa construção são códigos esféricos discretos e projeções de reticulados. Resultados do Capítulo 3 serão extensivamente utilizados.

Uma extensão natural desse problema é considerar fontes cujo suporte possui

dimensão maior que um (aplicações de $\mathbb{R}^k$ para $\mathbb{R}^n$), a qual será tratada no capítulo seguinte.

Shannon, o pai da Teoria de Informação, foi o primeiro a estudar aplicações contínuas entre fonte e canal. No seu artigo [Sha49], é mostrado uma curva espiral que mapeia uma fonte unidimensional a um canal bidimensional. Dentre os exemplos de esquemas de codificação analógica encontrados na literatura, incluindo análises de codificadores e de decodificadores ótimos, destacamos [KR10, Chu00, WSR09, VC03, SVC10]. Em [WSR09], os autores mostram como a teoria de polinômios ortogonais pode ser utilizada para a construção de curvas com o propósito de minimizar o erro quadrático médio (MSE) na transmissão. Em [VC03] é estabelecida a conexão entre códigos para fontes de alfabeto contínuo e projeções de reticulado aqui explorada. Nesse artigo, é apresentado um esquema explícito de codificação com boas propriedades assintóticas baseado em famílias de reticulados projeção de $\mathbb{Z}^n$ com boa densidade de empacotamento, tema extensivamente estudado no Capítulo 3 desta tese. Mostraremos que o esquema em [VC03] é um caso especial das nossas construções.

Os resultados deste capítulo foram parcialmente apresentados no *IEEE International Symposium on Information Theory*, Boston-MA, EUA (2012) [CTC12], e compõem o artigo [CTC13].

4.1 Modelo de Comunicação

O modelo de comunicação associado ao estudo de curvas feito neste capítulo está ilustrado no diagrama de blocos da Figura 4.1. O objetivo é transmitir um valor real x através de um canal de dimensão n com ruído gaussiano e restrição de potência média. Um *codificador* (ou aplicação de codificação) é uma aplicação injetiva $s(x)$ que leva cada possível mensagem x no espaço do canal $\mathbb{R}^n$. Um *decodificador* é uma função $g(\boldsymbol{y})$ que associa a cada possível vetor recebido $\boldsymbol{y} = \boldsymbol{s}(x) + \boldsymbol{z}$ uma estimativa $\hat{x}$ para o valor enviado. Em princípio a fonte pode ter

uma distribuição qualquer, mas nas nossas análises assumiremos que que x está uniformemente distribuído no intervalo unitário $[0, 1]$. Como usual, denotaremos por uma letra maiúscula uma variável aleatória e pela mesma letra, em minúsculo, uma amostra desta variável aleatória. O modelo de comunicação considerado possui, portanto, os seguintes elementos:

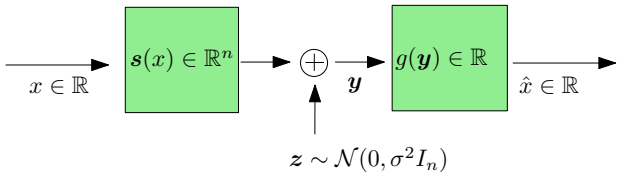


Figura 4.1: Modelo de comunicação

1. Uma variável aleatória X uniformemente distribuída em $[0, 1]$, associada à fonte.

2. Uma aplicação injetiva $\boldsymbol{s} : [0, 1] \to \mathbb{R}^n$ que associa cada possível mensagem x da fonte a um ponto no $\mathbb{R}^n$, de modo que a energia média dos pontos enviados seja menor que um valor P, isto é

$$E\left[\boldsymbol{s}(X)\boldsymbol{s}(X)^t\right] = \int_0^1 \|\boldsymbol{s}(x)\|_2^2 \, \mathrm{d}x \leq P \tag{4.1}$$

3. Um canal Gaussiano que distorce as mensagens enviadas de maneira que o vetor recebido seja $\boldsymbol{y} = \boldsymbol{s}(\boldsymbol{x}) + \boldsymbol{z}$, onde $\boldsymbol{z}$ está associado ao vetor aleatório $\boldsymbol{Z} = (Z_1, \ldots, Z_n)$, com Z_i independentes tais que $Z_i \sim \mathcal{N}(0, \sigma^2)$.

4. Um decodificador $\boldsymbol{g} : \mathbb{R}^n \to [0, 1]$ que associa cada possível vetor $\boldsymbol{y}$ a uma estimativa, $g(\boldsymbol{y}) = \hat{x}$.

Nossa figura de mérito será o erro quadrático médio (MSE). Em outras palavras, o esquema de comunicação será desenvolvido de modo a minimizar a variância do erro $E[(X - \hat{X})^2]$. A razão $P/\sigma^2 = \text{SNR}$ é chamada de relação sinal-ruído do canal. Nos referimos à imagem da aplicação $\boldsymbol{s}$ como o *local geométrico do sinal*.

Se $\boldsymbol{s}$ é uma aplicação contínua, o local geométrico é uma curva em $\mathbb{R}^n$. A extensão do modelo para fontes de dimensão maior que 1 será considerada no Capítulo 5, onde será também feita uma análise mais precisa das grandezas relevantes de um ponto de vista de teoria de informação.

O modelo de comunicação acima encontra-se cuidadosamente analisado em [Sak70, Cap. 4]. Dado um raio $\rho > 0$, denotemos por E_ρ o evento no qual o ruído está concentrado em uma bola de raio ρ, isto é $E_\rho = \{\|\boldsymbol{Z}\|_2 < \rho\}$. O erro quadrático médio pode ser então dividido em dois termos, tal que:

$$\text{MSE} = E[(X - \hat{X})^2 | E_\rho] P(E_\rho) + E[(X - \hat{X})^2 | E_\rho^c] P(E_\rho^c). \tag{4.2}$$

Se a variância do ruído σ^2 é muito pequena (com relação ao raio ρ), temos que $P(E_\rho^c) \approx 0$ e portanto o erro quadrático médio é bem aproximado por $E[(X - \hat{X})^2 | E_\rho]$. Neste caso, chamado de *regime de ruído baixo*, aproximando $\boldsymbol{s}(x)$ pela sua reta tangente é possível mostrar que [Sak70, Ch. 4]:

$$E[(X - \hat{X})^2] \approx \sigma^2 \int_0^1 \|\dot{\boldsymbol{s}}(x)\|_2^{-2} \, dx = E_{\text{low}}[(X - \hat{X})^2], \tag{4.3}$$

onde $\dot{\boldsymbol{s}}(x)$ denota a derivada de $\boldsymbol{s}(x)$. Para esta análise, é necessário que $\boldsymbol{s}(x)$ seja diferenciável (ou ao menos diferenciável por partes). A maior parte da nossas análises será feita no regime de ruído baixo. Se a derivada de $\boldsymbol{s}$ é constante, temos que

$$E_{\text{low}}[(X - \hat{X})^2] = \frac{\sigma^2}{L^2}, \tag{4.4}$$

onde L é o comprimento da curva. Em [Sak70, Cap. 4] é mostrado também que, por conta da restrição de potência média (Equação (4.1)), se $n > 1$, aplicações lineares são necessariamente sub-ótimas. Assim, devemos necessariamente considerar aplicações não-lineares. Intuitivamente, isto quer dizer que o local geométrico do sinal terá que ter mais do que uma "volta" ou "dobra". Por este motivo, códigos para esse modelo de comunicação também são chamados de *modulação torcida* (*twisted modulation*).

Uma ilustração geométrica dos possíveis efeitos causados pelo ruído é dado pela Figura 4.2. No regime de baixo ruído, todos os cálculos podem ser feitos utilizando a Equação (4.3). Contudo, para ruídos com norma grande, não podemos utilizar a mesma análise, pois a estimativa $\hat{x}$ pode estar na "volta" incorreta da curva. Isso sugere que o local geométrico deve possuir duas propriedades básicas: (i) grande distância entre as voltas (ii) grande comprimento.

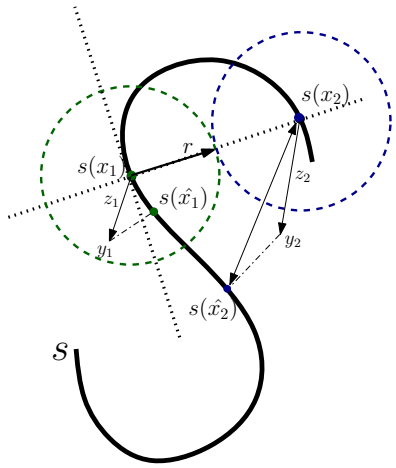


Figura 4.2: Erros pequenos e erros grandes.

Na próxima seção mostraremos nossa construção de curvas para o problema acima. Antes disso, vamos dar algumas definições mais precisas sobre as grandezas geométricas relevantes ao problema.

Dada uma aplicação $\boldsymbol{s} : [0,1] \mapsto \mathbb{R}^n$, a região de Voronoi $V(x)$ de um ponto $\boldsymbol{s}(x)$ é o conjunto de todos os pontos em $\mathbb{R}^n$ que estão mais próximos de $\boldsymbol{s}(x)$ do que qualquer outro ponto da curva. Seja $H(x)$ o hiperplano ortogonal à curva no ponto $\boldsymbol{x}(x)$. O maior raio $R > 0$ tal que $B(\boldsymbol{s}(x), R) \cap H(x) \subset V(x)$ é chamado de *raio de empacotamento* da curva. Intuitivamente, R é o maior valor tal que o "tubo" ao longo da curva $\boldsymbol{s}$ não se auto-intersecta. O *stretch* de uma curva é a função $\mathcal{S}(x) = \|\dot{\boldsymbol{s}}(x)\|_2$. O *stretch* nos dá uma medida de quão "alongado" está o intervalo $[0,1]$ quando mapeado no $\mathbb{R}^n$. O *comprimento* de uma curva é dado por $\int_0^1 \mathcal{S}(x)\mathrm{d}x$. Nosso objetivo será, fixado um raio de empacotamento, construir curvas com o maior comprimento possível.

4.2 Construção e Propriedades

4.2.1 Folheação da Esfera

Seja $\mathcal{S}^{2n-1}$ a esfera unitária do $\mathbb{R}^{2n}$, isto é

$$\mathcal{S}^{2n-1} = \left\{(x_1, \ldots, x_n) \in \mathbb{R}^{2n} : x_1^2 + \ldots + x_{2n}^2 = 1\right\}.$$

Consideraremos apenas curvas cujo local geométrico do sinal reside em $\mathcal{S}^{2n-1}$, de modo que para satisfazer a restrição de potência necessitamos aplicar apenas um fator de escala $\sqrt{P}$.

Um elemento importante para nossas construções será a folheação da esfera por toros planares, descrita a seguir. A ideia de folhear a esfera por toros para aplicações em comunicações pode ser encontrada previamente na literatura em [TCV09].

Para cada vetor unitário $\boldsymbol{c} = (c_1, c_2, .., c_n) \in \mathbb{R}^n, c_i > 0$ e $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{R}^n$, seja $\Phi_{\boldsymbol{c}} : \mathbb{R}^n \to \mathbb{R}^{2n}$ a aplicação definida por

$$\Phi_{\boldsymbol{c}}(\boldsymbol{u}) = \left(c_1 \left(\cos\frac{u_1}{c_1}, \sin\frac{u_1}{c_1}\right), \ldots, c_n \left(\cos\frac{u_n}{c_n}, \sin\frac{u_n}{c_n}\right)\right). \tag{4.5}$$

Segue diretamente que

$$\left\langle \frac{\partial \Phi_{\boldsymbol{c}}}{\partial u_i}, \frac{\partial \Phi_{\boldsymbol{c}}}{\partial u_j} \right\rangle = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

e portanto $\Phi_{\boldsymbol{c}}$ é uma isometria local na sua imagem. Seja $\mathcal{P}_{\boldsymbol{c}}$ o hiperretângulo

$$\mathcal{P}_{\boldsymbol{c}} = \{\boldsymbol{u} \in \mathbb{R}^n; 0 \leq u_i < 2\pi c_i, \quad 1 \leq i \leq n\}. \tag{4.6}$$

Temos que $\Phi_{\boldsymbol{c}}(\mathcal{P}_{\boldsymbol{c}}) = \Phi_{\boldsymbol{c}}(\mathbb{R}^n)$, o que mostra que a função $\Phi_{\boldsymbol{c}}$ é periódica, e portanto podemos trabalhar apenas com a sua restrição a $\mathcal{P}_{\boldsymbol{c}}$. Denotamos por $T_{\boldsymbol{c}} = \Phi_{\boldsymbol{c}}(\mathcal{P}_{\boldsymbol{c}})$ a imagem de $\Phi_{\boldsymbol{c}}$. O objeto $T_{\boldsymbol{c}}$ é uma subvariedade n-dimensional do $\mathbb{R}^{2n}$, contida em $\mathcal{S}^{2n-1}$, chamada de *toro planar*.

Note que cada vetor de $\mathcal{S}^{2n-1}$ pertence a um e apenas um destes toros planares, se considerarmos também os casos degenerados, em que algumas das componentes do vetor $\boldsymbol{c}$ é igual a zero. Dizemos portanto que a família de toros $T_{\boldsymbol{c}}$ e suas degenerações *folheia* a esfera unitária $\mathcal{S}^{2n-1} \subset \mathbb{R}^n$. Um estudo detalhado destes toros pode ser encontrado em [Tor09]. Para nossas construções, necessitaremos apenas das proposições abaixo. A primeira delas diz respeito à distância mínima entre pontos em dois toros distintos $T_{\boldsymbol{b}}$ e $T_{\boldsymbol{c}}$. A segunda está relacionada com a distância entre dois pontos em um mesmo toro.

Proposição 4.2.1. *[TCV09]A distância entre os toros $T_{\boldsymbol{b}}$ e $T_{\boldsymbol{c}}$ é dada por*

$$d(T_{\boldsymbol{c}}, T_{\boldsymbol{b}}) = \|\boldsymbol{c} - \boldsymbol{b}\|_2 = \left(\sum_{i=1}^{n} (c_i - b_i)^2 \right)^{1/2}. \tag{4.7}$$

Da Equação (4.5), temos que a distância entre dois pontos em um mesmo toro é dada por

$$\|\Phi_{\boldsymbol{c}}(\boldsymbol{u}) - \Phi_{\boldsymbol{c}}(\boldsymbol{v})\|_2 = 2\sqrt{\sum c_i^2 \sin^2\left(\frac{u_i - v_i}{2c_i}\right)}.$$

Podemos limitar a equação acima através do resultado abaixo.

Proposição 4.2.2. *[TCV09] Considere um vetor unitário $\boldsymbol{c} = (c_1, c_2, .., c_n), c_i > 0$ e $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{P}_{\boldsymbol{c}}$. Sejam $P = \|\Phi_{\boldsymbol{c}}(\boldsymbol{u}) - \Phi_{\boldsymbol{c}}(\boldsymbol{v})\|_2$ e $Q = \|\boldsymbol{u} - \boldsymbol{v}\|_2$. As seguintes desigualdades são válidas:*

$$\frac{2}{\pi}P \leq \frac{\sin\frac{P}{2c_\xi}}{\frac{P}{2c_\xi}}P \leq Q \leq \frac{\sin\frac{P}{2}}{\frac{P}{2}}P \leq P, \tag{4.8}$$

onde $c_\xi = \min c_i$.

4.2.2 Curvas em Camadas de Toro

Nas nossas construções, o local geométrico do sinal será constituído por uma coleção de curvas em $\mathcal{S}^{2n-1} \subset \mathbb{R}^{2n}$, cada uma delas em um toro $T_{\boldsymbol{c}}$ (o que pode ser visto como uma "curva contínua por partes"). Através da funcão (4.5) e das proposições 4.2.1 e 4.2.2 controlaremos o raio de empacotamento de cada curva e o raio de empacotamento da coleção final.

Para garantirmos que o conjunto final tenha raio de empacotamento pelo menos $\rho > 0$, necessitamos de dois elementos:

(i) Uma coleção de M toros $\{T_1, \ldots, T_M\} \subset \mathcal{S}^{2n-1}$, sendo M o maior valor possível tal que a distância entre quaisquer dois toros distintos da coleção seja pelo menos 2ρ.

(ii) Uma coleção de M curvas, cada uma delas contida em um toro T_i, com raio de empacotamento seja maior que ρ.

Abordaremos o item (i) acima através de técnicas de códigos esféricos esféricos clássicos e o item (ii) através de projeções de reticulados. Definidos os elementos acima, descreveremos como utilizá-los para construir uma aplicação $\boldsymbol{s} : [0, 1] \to \mathbb{R}^n$ com boa performance em termos do modelo de comunicação descrito anteriormente.

(i) Camadas de Toro: Códigos Esféricos

Um código esférico discreto é um conjunto finito de pontos na esfera $\mathcal{S}^{2n-1}$. O principal problema de códigos esféricos discretos consiste em, fixada uma distância d, encontrar a maior quantidade possível de pontos na esfera $\mathcal{S}^{2N-1}$ que distem pelo menos d entre eles. A relação deste problema com o item (i) se dá de maneira natural, através da Proposição 4.2.1.

Dado um raio de empacotamento ρ, queremos encontrar uma coleção de toros planares $\{T_1, \ldots, T_M\} \subset \mathcal{S}^{2n-1}$ tal que $d(T_i, T_j) > 2\rho$ para qualquer $i \neq j$. Pela

Proposição 4.2.1, a distância entre os toros T_i e T_j é precisamente a distância entre os dois vetores que os determinam (digamos, $\boldsymbol{c}_i$ e $\boldsymbol{c}_j$). Queremos, então, encontrar a maior quantidade possível de pontos $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ com todas as componentes positivas tais que

$$\|\boldsymbol{c}_i\|_2 = 1 \text{ e } \|\boldsymbol{c}_i - \boldsymbol{c}_j\|_2 > 2\rho, \forall i \neq j.$$

Esse é precisamente o problema de códigos esféricos restrito ao octante positivo da esfera $\mathcal{S}^{n-1}$. Denotamos por $\mathcal{SC}_+$ o código esférico $\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\}$.

Existe uma varidade de construções de códigos esféricos que podem ser utilizadas aqui, por exemplo [EZ01, HZ97], ou até mesmo as estratégias utilizando toros planares vistas em [TCV09]. Para uma boa referência em português sobre o tema, sugerimos a tese de doutorado [Tor09]. Citamos abaixo uma família de códigos esféricos que será utilizada nas nossas simulações computacionais:

Exemplo 4.2.3. *Seja*

$$\boldsymbol{c}(t) = \frac{(1, 1+t, 1+2t, \cdots, 1+(n-1)t)}{\sqrt{\sum_{i=0}^{n-1}(1+it)^2}},\ t > 0 \tag{4.9}$$

O conjunto $\mathcal{SC}_{c(t)} = \{\sigma(\boldsymbol{c}(t)) : \sigma \in S_n\}$ *de todas as permutações de* $\boldsymbol{c}(t)$ *define um código esférico de cardinalidade* $M = n!$ *em que cada vetor possui coordenadas positivas. A menor distância entre dois elementos de* $\mathcal{SC}_{c(t)}$ *é*

$$d(t) = \frac{t\sqrt{2}}{\sqrt{\sum_{i=0}^{N-1}(1+it)^2}}.$$

Note que

$$\lim_{t\to 0} \boldsymbol{c}(t) = \frac{1}{\sqrt{N}}(1, \ldots, 1) = \hat{\boldsymbol{e}}, \tag{4.10}$$

e, para cada $t > 0$*, os elementos de* $\mathcal{SC}_{c(t)}$ *são equidistantes do vetor* $\hat{\boldsymbol{e}}$*. Além disso, para qualquer* n *fixo e* $d_0 > 0$ *suficientemente pequeno, existe* $t > 0$ *tal que*

$d(t) = d_0$. *Esse resultado segue da observação de que a equação*

$$d_0 = \frac{t\sqrt{2}}{\sqrt{\sum_{i=0}^{N-1}(1+it)^2}}$$

possui raiz positiva para

$$0 < d_0 < \frac{2\sqrt{3}}{\sqrt{(N-1)N(2N-1)}}.$$

Apesar de a construção acima não ser a melhor em termos de números de pontos, fixada uma distância, ela possui a vantagem de ser altamente simétrica e de ser possível deduzir uma forma fechada para a distância mínima do código esférico.

(ii) Curvas em Cada Toro

Seja um toro $T_{\boldsymbol{c}}$ determinado pelo vetor $\boldsymbol{c}$, e sejam os vetores $\boldsymbol{u} \in \mathbb{Z}^n$ e $\boldsymbol{v} = \boldsymbol{u}C$, onde $C = \mathrm{diag}(c_1, \ldots, c_n)$. Considere o conjunto de retas paralelas

$$W = \{\boldsymbol{v}x + \hat{\boldsymbol{n}} : \boldsymbol{n} \in \Lambda_{\boldsymbol{c}}\},$$

onde $\Lambda_{\boldsymbol{c}} = \Lambda(C)$. Considere também $2\pi W \cap \mathcal{P}_{\boldsymbol{c}}$ a intersecção entre este conjunto de retas, após aplicarmos uma escala de 2π, e o hiperretângulo $\mathcal{P}_{\boldsymbol{c}}$. As curvas que estudaremos serão a imagem da função $\Phi_{\boldsymbol{c}}$ restrita a $2\pi W \cap \mathcal{P}_{\boldsymbol{c}}$. Levando em consideração a periodicidade de $\Phi_{\boldsymbol{c}}$, definimos a curva[1]:

$$\boldsymbol{s}_{T_c} : [0,1) \to \mathbb{R}$$

$$\boldsymbol{s}_{T_c}(x) = \Phi_{\boldsymbol{c}}(x 2\pi \boldsymbol{v}). \tag{4.11}$$

[1] Apesar de que no modelo de comunicação o suporte da fonte é o intervalo $[0,1]$, tecnicamente necessitamos excluir um dos extremos para que nossa função seja injetiva, o que não altera nenhuma das considerações feitas anteriormente

Para que $\boldsymbol{s}_{T_c}$ seja uma aplicação injetiva, necessitamos que o vetor $\boldsymbol{v} \in \mathbb{Z}$ seja primitivo. A curva acima é fechada, está contida em $\mathcal{S}^{2n-1}$, é completamente determinada pelo vetor $\boldsymbol{v}$ e possui comprimento igual a $2\pi \left\|\boldsymbol{v}\right\|_2$. Podemos encontrar limitantes para o seu raio de empacotamento a partir da distância mínima $r_{\boldsymbol{c}}(\boldsymbol{v})$ entre duas retas distintas do conjunto W. Temos

$$\begin{aligned} r_{\boldsymbol{c}}(\boldsymbol{v}) &= \min_{\hat{\boldsymbol{n}} \neq k\boldsymbol{v}, k\in\mathbb{Z}} \min_{\hat{x},x} \left\|\boldsymbol{v}x - (\boldsymbol{v}\hat{x} + \boldsymbol{n})\right\|_2 \\ &= \min_{\boldsymbol{n} \neq k\boldsymbol{v}, k\in\mathbb{Z}} \min_{x} \left\|\boldsymbol{v}x - \boldsymbol{n}\right\|_2 \\ &= \min_{\boldsymbol{n} \neq k\boldsymbol{v}, k\in\mathbb{Z}} \left\|P_{\boldsymbol{v}^\perp}(\boldsymbol{n})\right\|_2 \\ &= \min_{\boldsymbol{n} \notin \boldsymbol{v}^\perp} \left\|P_{\boldsymbol{v}^\perp}(\boldsymbol{n})\right\|_2 , \end{aligned} \tag{4.12}$$

onde $P_{\boldsymbol{v}^\perp}(\boldsymbol{n})$ denota a projeção ortogonal de $\boldsymbol{n}$ em $\boldsymbol{v}^\perp$, como no Capítulo 3. A equação acima nos diz que $r_{\boldsymbol{c}}(\boldsymbol{v})$ é comprimento do menor vetor não nulo da projeção de $\Lambda_{\boldsymbol{c}}$ em $\boldsymbol{v}^\perp$. Isso estabelece a relação desejada entre as curvas em camadas de toro e as estruturas de projeção de reticulados estudadas previamente. Por conta da Proposição 4.2.2, o raio de empacotamento $\rho_{\boldsymbol{v},\boldsymbol{c}}$ de $\boldsymbol{s}_{T_c}$ pode ser limitado em termos de $r_{\boldsymbol{c}}(\boldsymbol{v})$ da seguinte maneira:

$$2c_\xi \sin\left(\frac{\pi r_{\boldsymbol{c}}(\boldsymbol{v})}{2c_\xi}\right) \leq \rho_{\boldsymbol{v},\boldsymbol{c}} \leq 2\sin\left(\frac{\pi r_{\boldsymbol{c}}(\boldsymbol{v})}{2}\right), \tag{4.13}$$

onde $c_\xi = \min_i c_i$ e $c_i > 0$ para todo i. Assim, para valores pequenos de $\rho_{\boldsymbol{v},\boldsymbol{c}}$, temos $\rho_{\boldsymbol{v},\boldsymbol{c}} \approx \pi r_{\boldsymbol{c}}(\boldsymbol{v})$. Nosso objetivo, é portanto, escolher vetores $\boldsymbol{v}$ de modo a maximizar $r_{\boldsymbol{c}}(\boldsymbol{v})$. Entretanto, temos também o objetivo de maximizar o comprimento $2\pi \left\|\boldsymbol{v}\right\|_2$ de $\boldsymbol{s}_{T_c}$. Estas duas grandezas estão relacionadas pela densidade do reticulado projeção de $\Lambda_{\boldsymbol{c}}$ em $\boldsymbol{v}^\perp$:

$$\delta(P_{\boldsymbol{v}^\perp}(\Lambda_{\boldsymbol{c}})) = \frac{r_{\boldsymbol{c}}(\boldsymbol{v})^{n-1} \left\|\boldsymbol{v}\right\|_2}{2^{n-1}\prod_{i=1}^n c_i} \leq \delta_{n-1}, \tag{4.14}$$

lembrando que δ_{n-1} é a densidade de centro do melhor reticulado de dimensão $(n-1)$.

Dado um raio de empacotamento ρ, encontrar a curva de maior comprimento equivale a encontrar o reticulado projeção mais denso. A construção geral da Seção 3.3 nos provê uma solução para este problema.

Exemplo 4.2.4. *Seja $N = 2$. Considere a isometria local*

$$\Phi_{\boldsymbol{c}}(\boldsymbol{u}) = \left(c_1 \cos\frac{u_1}{c_1}, c_1 \sin\frac{u_1}{c_1}, c_2 \cos\frac{u_2}{c_2}, c_2 \sin\frac{u_2}{c_2} \right) \tag{4.15}$$

e o segmento de reta dado por $\boldsymbol{v}(x) = x(2\pi u_1 c_1, 2\pi u_2 c_2)$, $x \in [0,1)$, $u_1, u_2 \in \mathbb{Z}$. A curva $\boldsymbol{s}_{T_c}(x)$ será a composição $\Phi(\boldsymbol{v}(x))$. Como o reticulado projeção, neste caso, é unidimensional, temos:

$$r_{\boldsymbol{c}}(\boldsymbol{v}) \left\|\boldsymbol{v}\right\|_2 = 2\pi c_1 c_2 \Rightarrow r_{\boldsymbol{c}}(\boldsymbol{v}) = \frac{c_1 c_2}{\sqrt{u_1^2 c_1^2 + u_2^2 c_2^2}} \tag{4.16}$$

Esta curva em $\mathbb{R}^4$ dá u_1 voltas em torno do círculo obtido pela sua projeção nas duas primeiras coordenadas e u_2 voltas em torno do círculo de raio c_2 dado pelas suas duas últimas coordenadas, produzindo o que é chamado de nó do tipo (u_1, u_2) no toro planar $T_{\boldsymbol{c}}$. Na Figura 4.3 ilustramos esta curva para $(u_1, u_2) = (4, 5)$, e a sua projeção estereográfica no $\mathbb{R}^3$.

Observação 4.2.5. *A família de curvas "exponencial" (também chamada de código shift) descrita no artigo [VC03] é um caso especial das aqui consideradas, tomando*

$$\boldsymbol{c} = \hat{\boldsymbol{e}} = (1/\sqrt{n})(1, \ldots, 1) \text{ e } \boldsymbol{v} = (1/\sqrt{n})(1, a, a^2, \ldots, a^{n-1}),$$

para um valor inteiro $a \geq 1$. Vale notar que o toro determinado pelo vetor $\hat{\boldsymbol{e}}$ possui maior volume entre todos os toros planares $T_{\boldsymbol{c}}$ e menor distorção de distâncias, no sentido da Proposição 4.2.2. Em [SVC10], são mostradas curvas com melhor desempenho do que as dadas pelo vetor $\boldsymbol{v}$ acima, baseadas na Construção Lifting e em técnicas de projeções de reticulados.

Com os elementos (i) e (ii) em mãos, estamos aptos a descrever nossa proposta para esquema de codificação e decodificação.

Codificação

Seja $T = \{T_1, \ldots, T_M\}$ uma coleção de M toros planares. Para cada toro T_k, consideramos a curva $\boldsymbol{s}_{T_k}(x) = \Phi(x2\pi\boldsymbol{v}_k), (k = 1, 2, \ldots, M)$ determinada pelo vetor $\boldsymbol{v}_k$. Seja

$$L = \sum_{j=1}^{M} L_j,$$

onde L_k é o comprimento de $\boldsymbol{s}_{T_k}$.

Dividimos o intervalo $[0, 1)$ em M partes de acordo com o comprimento de cada curva, de modo que

$$[0, 1) = I_1 \cup I_2, \ldots \cup I_M, \text{ onde}$$

$$I_k = \left[\frac{\sum_{j=1}^{k-1} L_j}{L}, \frac{\sum_{j=1}^{k} L_j}{L} \right), \text{ para } k = 1, \ldots, M.$$

Para cada intervalo, consideramos a aplicação bijetiva que leva I_k em $[0, 1)$ dada por

$$f_k : I_k \to [0, 1)$$
$$f_k(x) = \frac{x - \sum_{j=1}^{k-1} L_j/L}{L_k/L}.$$

A aplicação de codificação $\boldsymbol{s}$ pode ser então definida como

$$\boldsymbol{s}(x) = \boldsymbol{s}_{T_k}(f_k(x)), \text{ se } x \in I_k. \tag{4.17}$$

O *stretch* de $\boldsymbol{s}$ é constante e igual ao seu comprimento total L. O seu raio de empacotamento é o menor raio ρ dentre as curvas $\boldsymbol{s}_{T_k}$, contanto que escolhamos uma coleção de toros separados, dois a dois, por uma distância maior que 2ρ.

Para codificar um valor x entre $[0, 1)$, aplicamos a função (4.17), com um fator

de escala $\sqrt{P}$, de modo que a potência de transmissão seja P. O lugar geométrico do sinal será então uma coleção de M curvas fechadas, cada uma em um toro T_k, definido por um vetor $\boldsymbol{v}_k$. O processo completo de decodificação está descrito na Figura 4.3.

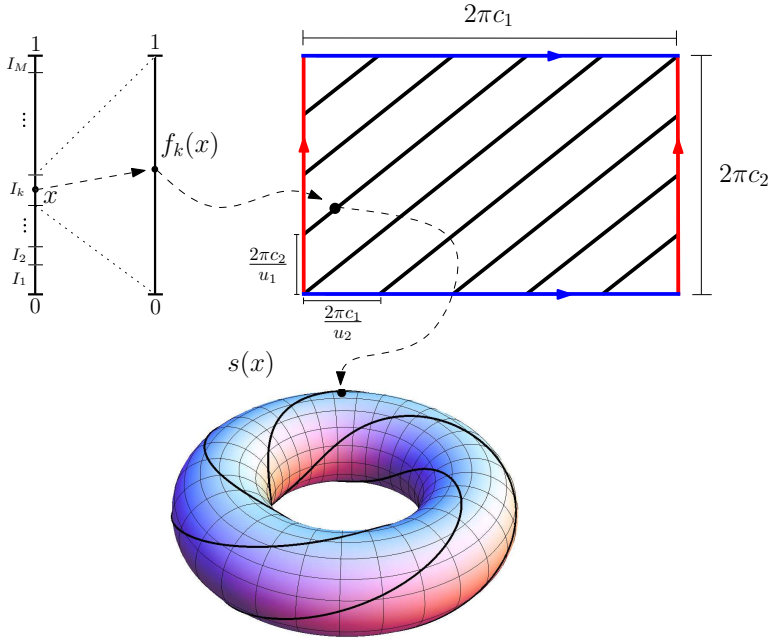


Figura 4.3: Processo de codificação

Como dito anteriormente, assumiremos que a fonte está uniformemente distribuída em $[0, 1]$. Desta maneira, a divisão de intervalos feita aqui é ótima em termos do erro quadrático médio, pois todos os subintervalos são igualmente "esticados" (uma demonstração formal deste fato será dada na Seção 4.3). Se a fonte não tiver distribuição uniforme, é necessário considerar outros tipos de partição. Para fontes Gaussianas, mostramos um exemplo de divisão eficiente em na Seção 4.4.

Decodificação

O processo de decodificação que descreveremos a seguir é a junção de dois algoritmos: o decodificador esférico proposto em [TCV09] e o algoritmo SHIFTDEMOD

em [VC03, Seção VI].

Para determinar a função de decodificação $g(\boldsymbol{y})$, consideraremos os chamados *decodificadores de máxima verossimilhança*. No caso do nosso modelo de comunicação, dado um vetor recebido $\boldsymbol{y} \in \mathbb{R}^{2n}$, a estimativa $\hat{x}$ de máxima verossimilhança é dada por [Sak70, Ch. 4]:

$$\hat{x} = \arg \min_{x \in [0,1)} \|\boldsymbol{y} - \boldsymbol{s}(x)\|_2 .$$

O problema de minimização acima é computacionalmente bastante complexo, com diversos mínimos locais. Focamos portanto, em um decodificador sub-ótimo. Seja $0 \neq \gamma_i = \sqrt{y_{2i-1}^2 + y_{2i}^2}$. Podemos escrever $\boldsymbol{y}$ como

$$\begin{aligned} \boldsymbol{y} &= \left(\gamma_1 \left(\frac{y_1}{\gamma_1}, \frac{y_2}{\gamma_1}\right), \ldots, \gamma_n \left(\frac{y_{2n-1}}{\gamma_n}, \frac{y_{2n}}{\gamma_n}\right)\right) \\ &= \left(\gamma_1 \left(\cos\frac{\theta_1}{\gamma_1}, \sin\frac{\theta_1}{\gamma_1}\right), \ldots, \gamma_n \left(\cos\frac{\theta_n}{\gamma_n}, \sin\frac{\theta_n}{\gamma_N}\right)\right), \end{aligned}$$

onde

$$\theta_i = \arccos\left(\frac{y_{2i-1}}{\gamma_i}\right)\gamma_i, \quad 1 \leq i \leq N.$$

A decodificação procede em dois passos: encontrar a camada correta e, dentro de cada camada, encontrar o ponto da curva corresponde mais próximo do vetor recebido.

O processo de encontrar a camada mais próxima envolve encontrar o ponto do código esférico $\mathcal{SC}_+ \subset \mathcal{S}^{n-1}$ mais próximo de $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \cdots, \gamma_n)$. Um algoritmo para resolver este problema possui complexidade, no pior caso, $O(nM)$ (o que pode ser feito, por exemplo, calculando todas as distâncias possíveis e encontrando a menor).

Seja agora $\boldsymbol{c}_i = (c_{i1}, c_{i2}, \cdots, c_{in})$ o ponto em $\mathcal{SC}_+$ mais próximo de $\boldsymbol{\gamma}$ e considere

$$\bar{\boldsymbol{y}}_i = \left(c_{i1} \left(\cos\frac{\theta_1}{\gamma_1}, \sin\frac{\theta_1}{\gamma_1}\right), \ldots, c_{in} \left(\cos\frac{\theta_n}{\gamma_n}, \sin\frac{\theta_n}{\gamma_n}\right)\right)$$

a projeção de $\boldsymbol{y}$ no toro T_{c_i}, isto é:

$$||\boldsymbol{y} - \bar{\boldsymbol{y}}_i|| \leq ||\boldsymbol{y} - \boldsymbol{x}||, \forall\, \boldsymbol{x} \in T_{c_i}.$$

O algoritmo SHIFTDEMOD [VC03] nos mostra como encontrar o ponto mais próximo de $\bar{\boldsymbol{y}}_i$ com número de operações $\Theta(N \|\boldsymbol{u}_i\|_1)$, onde $\boldsymbol{u}_i$ é o vetor de coordenadas do vetor $\boldsymbol{v}_i$ que determina a curva $\boldsymbol{s}_{T_i}$. Portanto, se o número de toros não for muito grande, a complexidade será dominada pela norma do vetor projeção. Mais formalmente, se $M = O(\max_i \|\boldsymbol{u}_i\|_1)$, a complexidade do algoritmo descrito nessa seção é $O(N \max_i \|\boldsymbol{u}_i\|_1)$.

Observação 4.2.6. *A discussão sobre a complexidade da decodificação feita acima justifica a figura de mérito das sequências de projeções geradas no Capítulo 3, onde analisamos a relação entre norma do vetor projeção e densidade obtida. A densidade está relacionada com o desempenho das curvas em termos do erro quadrático médio, enquanto a norma do vetor projeção relaciona-se com a complexidade de decodificação. Assim, dados dois reticulados projeção com mesma densidade, o que possui vetor projeção de menor norma está associado a curvas com decodificação computacionalmente mais fácil.*

Para finalizar a seção, mostramos comparações numéricas da nossas curvas com as construídas em [VC03] e [SVC10], em termos de comprimento e raio de empacotamento. Dado $\rho > 0$, consideramos um conjunto de toros determinado por um código esférico em $\mathcal{S}^2$ com distância mínima 2ρ [TCV09]. Utilizando a primeira desigualdade de (4.13) para cada toro, encontramos $r_{\boldsymbol{c}}$ de maneira a garantir que cada curva possui raio de empacotamento pelo menos ρ. Consideramos, então, a sequência de projeções de $\Lambda_{\boldsymbol{c}}$ que converge para o reticulado mais denso em duas dimensões, A_2, e buscamos pelo vetor mais longo que produz uma projeção com distância mínima pelo menos $r_{\boldsymbol{c}}$. O resultado encontra-se ilustrado no gráfico abaixo.

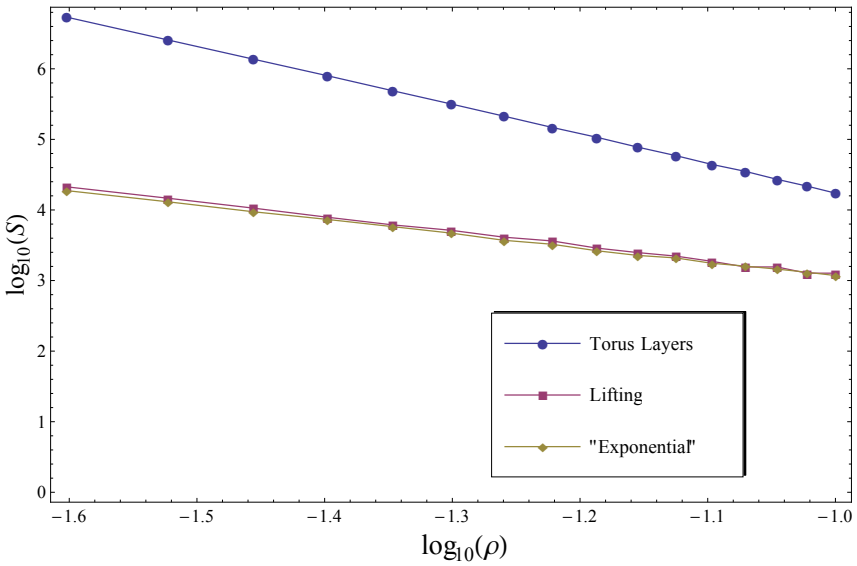


Figura 4.4: Comparação entre diferentes abordagens em termos de raio de empacotamento ρ e comprimento total L (igual ao stretch $\mathcal{S}$). De baixo para cima, vemos as curvas exponenciais em [VC03], as curvas da Construção Lifting em [SVC10] e as curvas propostas aqui

4.3 Análise

Nos referiremos à nossas curvas e ao processo de codificação/decodificação descritos anteriormente como o Esquema de Camadas de Toros. A análise será feita baseada no comportamento do MSE em termos da relação sinal-ruído. Os resultados exibidos mostram que nosso esquema é assintoticamente superior aos popostos anteriormente na literatura.

O primeiro passo no processo de codificação envolve a escolha de uma partição do intervalo unitário $[0, 1]$. Se a fonte tiver distribuição uniforme, é intuitivo que a melhor escolha de partição em termos de erro quadrático médio é a que possui *stretch* constant, ou seja, que todos os intervalos são igualmente "esticados". Esse fato encontra-se formalizado no teorema abaixo:

Teorema 4.3.1. *[CTC13]Seja $I_1, \ldots, I_M$ uma partição do intervalo $[0, 1)$. Seja $\{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_M\}$ uma coleção de curvas disjuntas duas a duas em $\mathcal{S}^{2n-1}$ com comprimentos $L_1, \ldots, L_M$, respectivamente, e domínio $[0, 1)$. Suponha que a regra de*

codificação (4.17) *é utilizada. Sob o regime de baixo ruído, temos que o mínimo* ϵ^* *de* $E_{low}[(X-\hat{X})^2]$ *sobre todas as partições* $\{I_1,\ldots,I_m\}$ *vale* $\epsilon^* = \sigma^2/L^2$ *e é atingido quando os tamanhos dos intervalos satisfazem*

$$|I_j| = \frac{L_j}{\sum_{j=1}^{M} L_j} = \frac{L_j}{L}. \tag{4.18}$$

Demonstração. Utilizando o lado direito da Equação (4.3), notemos que

$$\begin{aligned} E_{\text{low}}[(X-\hat{X})^2] &= \sum_{j=1}^{M} E_{\text{low}}[(X-\hat{X})^2 | X \in I_j] P(X \in I_j) \\ &= \sum_{j=1}^{M} E_{\text{low}}[(X-\hat{X})^2 | X \in I_j] |I_j| \end{aligned}$$

onde, $E_{\text{low}}[(X-\hat{X})^2|X\in I_j] = \sigma^2|I_j|^2/L_j^2$. Portanto

$$\begin{aligned} E_{\text{low}}[(X-\hat{X})^2] &= \sigma^2 \sum_{j=1}^{M} \frac{|I_j|^3}{L_j^2} = \sigma^2 L \sum_{j=1}^{M} \left(\frac{|I_j|}{L_j}\right)^3 \left(\frac{L_j}{L}\right) \\ &\overset{(a)}{\geq} \sigma^2 L \left(\sum_{j=1}^{M} \frac{|I_j|}{L}\right)^3 = \frac{\sigma^2}{L^2}, \end{aligned}$$

onde (a) é devido à convexidade da função $g(x) = x^3, x > 0$, e portanto a igualdade só é satisfeita quando $|I_j|/L_j = |I_k|/L_k, \forall k, j$. Essa condição e o fato de que $\sum_{j=1}^{n} |I_j| = 1$, implicam a Equação (4.18). □

Para a análise do MSE, procederemos como em [VC03, Seção VI.b]. Nesse artigo, os autores mostram que, fixados n e σ^2, o MSE da família de curvas proposta satisfaz

$$E[(X-\hat{X})^2)] = O\left(P^{-n}\right),$$

ou seja, o erro quadrático médio decai com a potência elevada à *metade* da dimensão (lembrando que as curvas estão contidas em $\mathbb{R}^{2n}$).

No que segue, exibiremos dois resultados:

1. Um resultado construtivo, baseado no Exemplo 4.2.3, mostrando curvas cujo comprimento é $n!$ vezes maior que o do esquema proposto em [VC03], mesmo com as melhorias assintóticas provenientes da Construção *Lifting* [SVC10]. Isso implica um comportamento assintótico comparável a $O(P^{-n})$, mas com melhor performance à medida que aumentamos n.

2. Um resultado assintótico não-construtivo mostrando que é possível "recuperar" as $(n-1)$ dimensões perdidas em [VC03] e atingir ordem de decaimento $O(P^{-(2n-1)})$.

Para o primeiro resultado, seja $\boldsymbol{c}(t)$ dado pela Equação 4.9. Para $\rho > 0$ suficientemente pequeno, existe $t > 0$ tal que os toros no conjunto $\mathcal{SC}_{c(t)}$ possuem, dois a dois, distância mínima maior ou igual a 2ρ. Além disso, existe $\boldsymbol{v} \in \Lambda_{\boldsymbol{c}(t)}$ arbitrariamente próximo ao limitante (4.14), pela nossa construção de projeções dada na Seção 3.3. O mesmo vetor $\boldsymbol{v}$ pode ser utilizado para todos os toros, permutando as suas coordenadas. Como temos $n!$ toros no conjunto $\mathcal{SC}_{\boldsymbol{c}(t)}$, o comprimento total L_{TL} produzido pela nossa construção é:

$$L_{TL} = (n!)L_{\boldsymbol{c}(t)} = n!\ \frac{(2\pi)^n}{\rho^{n-1}} \prod_{i=1}^{n} c_i(t)\,(\delta_n - \varepsilon_1)\,, \tag{4.19}$$

para algum ε_1. No caso das curvas da Construção *Lifting* com mesmo raio de empacotamento, temos [VC03]:

$$L_{LC} = L_{\hat{\boldsymbol{e}}} = 2\pi \|\hat{\boldsymbol{u}}\|_2 = \frac{(2\pi)^n}{\rho^{n-1} n^{n/2}}\,(\delta_n - \varepsilon_2)\,.$$

À medida que $\rho \to 0$, podemos fazer com que ambos ε_1 e ε_2 tendam a zero, e portanto:

$$\frac{L_{TL}}{L_{LC}} \to n!\ n^{n/2} \prod_{i=1}^{n} c_i(t).$$

Tomando t suficientemente pequeno (mas mantendo o raio de empacotamento

maior que ρ), temos

$$\lim_{t\to 0} \frac{L_{TL}}{L_{LC}} = n!$$

.

Em outras palavras, à luz da Equação (4.3):

$$E^{TL}_{\text{low}}[(X - \hat{X})^2] \approx \frac{1}{(n!)^2} E^{LC}_{\text{low}}[(X - \hat{X})^2].$$

onde a aproximação é tão boa quanto o raio de empacotamento seja pequeno (este é o caso quando a relação sinal-ruído é alta).

O próximo teorema nos mostra que é possível encontrar parâmetros de códigos esféricos e curvas tais que o MSE tenha ordem de decaimento $O(P^{-(2n-1)})$. Contudo, a sua demonstração é não construtiva, baseada em argumentos existenciais devido a Chabauty, Shannon e Wyner [EZ01, Seção 1.6]. A ideia intuitiva é de que as construções anteriores [VC03, SVC10] utilizam apenas um toro (um objeto n-dimensional) em $\mathcal{S}^{2n-1}$, enquanto utilizando a folheação podemos preencher uma parte maior da superfície da esfera.

Teorema 4.3.2. *[CTC13] Existe uma escolha de parâmetros M, $\boldsymbol{c}_i$ e $\boldsymbol{v}_i$ para os quais o erro quadrático médio do Esquema de Camadas de Toros satisfaz $E[(X - \hat{X})^2] = O(P^{-(2n-1)+\mu})$, para qualquer $\mu > 0$ e P suficientemente grande.*

Demonstração. Ver Apêndice A. □

4.4 Simulações

Apresentaremos resultados numéricos provenientes de simulações para ilustrar o desempenho do Esquema de Camada de Toros. O estudo comparativo será feito com o esquema [VC03], ao qual nos referiremos por V&C, e com uma simples modulação linear (isto é, quando $s(x) = \sqrt{P}(x, \ldots, x)$). Os resultados de simulação correspondem a 50000 amostras com $n = 3$ (isto é, dimensão do canal igual a

6), e o desempenho é medido através da relação entre o sinal ruído SNR $= P/\sigma^2$ e o erro quadrático médio. Mostraremos também como adaptar o Esquema de Camada de Toros para fontes gaussianas, isto é, quando a variável aleatória X possui distribuição normal com variância σ_s^2.

Uma outra possível construção para comparação em $\mathbb{R}^6$ seriam as curvas polinomiais de [WSR09]. Entretanto, o decodificador proposto para tais curvas possui alta complexidade computacional (um dos passos é encontrar o mínimo global de de polinômios de grau arbitrariamente alto), de modo que torna-se infactível realizar todas as amostras computacionalmente. Além disso, como demonstrado no próprio artigo [WSR09], o esquema V&C supera as curvas polinomiais para fontes uniformes e é bastante comparável a estas para fontes gaussianas. Outras construções na literatura, como o trabalho de [Chu00] só envolvem curvas em $\mathbb{R}^2$ e $\mathbb{R}^3$.

O comportamento típico das simulações evidencia um efeito *threshold*: para valores de SNR muito baixos, uma boa parte dos vetores é decodificado na camada de toro incorreta. Acima de um certo SNR limite, o sistema é regido pela Equação (4.3) correspondente ao regime de baixo ruído. Esse efeito *threshold* é característico a qualquer sistema de modulação analógica (veja por exemplo [Sak70, Capítulo 4]).

Fontes Uniformes

Na Figura 4.5, à esquerda, o desempenho do Esquema de Camadas de Toros (TL) é exibida, para $M = 6$ toros como do Exemplo 4.2.3 com $t = 0.6$ (raio de empacotamento 0.29277) e vetor projeção com coordenadas $\boldsymbol{u} = (1, 2, 198)$. O esquema V&C foi simulado para $a = 18$ (isto é, com as curvas associada aos vetores $\boldsymbol{u} = (1, 18, 324)$. Escolhemos estes parâmetros de modo que os dois esquemas atingem a assíntota para o mesmo valor de SNR (isto é, possuem aproximadamente o mesmo raio de empacotamento). Como esperado, o esquema TL apresenta um

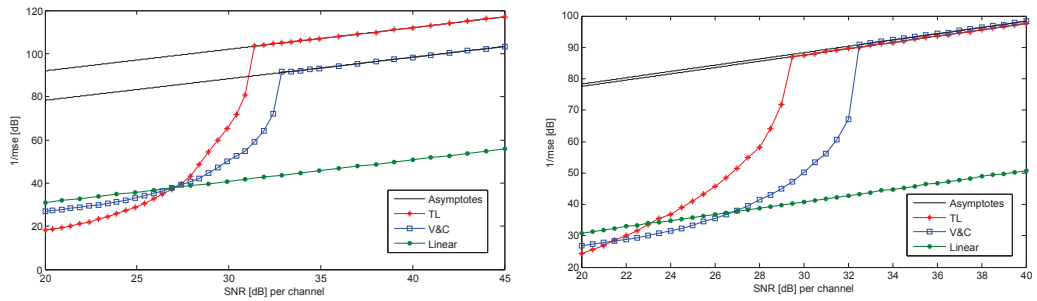


Figura 4.5: Simulações computacionais no caso de fontes uniformes.

melhor desempenho assintótico (aproximadamente 13dB maior neste exemplo).

A Figura 4.5 mostra, à direita, resultados de simulação também para $M = 6$ toros como no Exemplo 4.2.3. Neste caso, $t = 1.75$ (raio de empacotamento 0.46107) e o vetor projeção possui coordenadas $\boldsymbol{u} = (1, 4, 34)$. O código V&C foi simulado novamente para $a = 18$. Os parâmetros, neste caso, foram escolhidos de modo que ambos os esquemas tenham mesmo comportamento assintótico (isto é, as curvas possuem comprimento igual). Neste caso, o esquema TL atinge a assíntota para um valor de sinal-ruído muito menor (5db neste exemplo)

Fontes Gaussianas

Apesar de a teoria ter sido apropriadamente desenvolvida para fontes uniformes, apresentamos a seguir uma possível extensão para fontes gaussianas, acompanhada de resultados de simulação.

Considere x retirado de uma distribuição normal $\mathcal{N}(0, \sigma_s^2)$ e seja $p(x)$ a função densidade de probabilidade da distribuição. Para usar o Esquema de Camadas de Toros, precisamos primeiramente mapear a reta real no intervalo $[0, 1]$. Existem infinitas maneiras de fazê-lo - mostraremos a seguir uma delas - utilizando uma técnica chamada de *companding* [Sak70]. A técnica propõe um mapeamento da reta real em um intervalo finito, mudando o suporte de uma variável aleatória, de modo que a distorção produzida seja pequena. Uma função *companding* ótima

para a variável Gaussiana foi empregada no trabalho [WSR09], para curvas polinomiais.

Seja $T = \{T_1, \ldots, T_M\}$ uma coleção de M toros projetados como no caso uniforme. Para cada um desses toros, temos uma curva $\boldsymbol{s}_{T_k}(x)$ com comprimento L_k, tal que o comprimento total é $L = \sum_{k=1}^{M} L_k$. Particionamos o intervalo real em M sub-intervalos tais que a área abaixo de $p(x)$ restrita a Q_k é igual a $\frac{L_k}{L}$. Sejam $\{x_1, x_2, \cdots, x_{M-1}\}$ os extremos destes intervalos, de modo que

$$Q_1 = (-\infty, x_1],\ Q_k = (x_{k-1}, x_k],\ Q_M = (x_{M-1}, \infty).$$

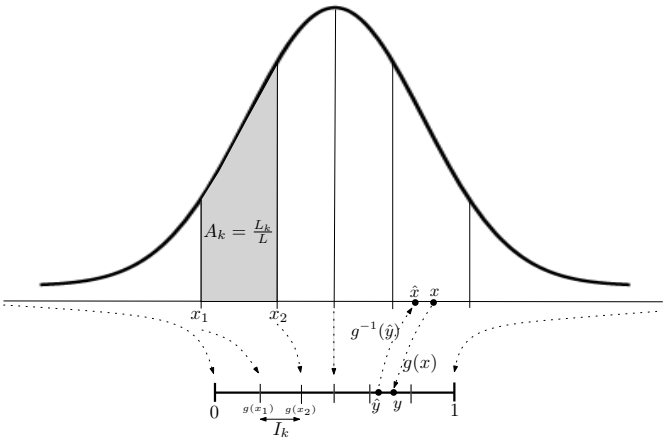


Figura 4.6: Divisão de intervalos para a variável Gaussiana

Aplicamos então a função *companding* [Sak70]:

$$g : \mathbb{R} \to [0, 1]$$

$$g(x) = \frac{\int_{-\infty}^{x} p(u)^{\frac{1}{3}}\, du}{\int_{-\infty}^{\infty} p(u)^{\frac{1}{3}}\, du} \tag{4.20}$$

para mapear a reta real em $[0, 1]$. As imagens $\{g(x_1), g(x_2), \cdots, g(x_{M-1})\}$ induzem uma partição de $[0, 1]$ em M pedaços $\{I_1, I_2, \cdots, I_M\}$, com

$$I_1 = [0, g(x_1)],\ I_k = (g(x_{k-1}), g(x_k)],\ I_M = (g(x_{M-1}), 1],$$

com tamanhos $|I_1|, |I_2|, \cdots, |I_M|$ e podemos definir a nossa função bijetiva entre I_k e $[0, 1)$ como

$$f_k : I_k \to [0, 1)$$
$$f_k(y) = \frac{y - \sum_{j=1}^{k-1} L_{I_j}}{L_{I_k}} \ , \text{ where } y = g(x).$$

O aplicação de codificação $\boldsymbol{s}(x)$, bem como o processo de decodificação são similares ao caso uniforme. Uma vez que tenhamos uma estimativa $\hat{y} \in [0, 1)$, precisamos inverter a função $g(x)$ para obtermos $\hat{x} = g^{-1}(\hat{y})$ e então computar o MSE. A codificação está ilustrado na Figura 4.6.

Na Figura 4.7, mostramos resultados de simulação para uma fonte gaussiana com variância $\sigma_s^2 = 0.5$. Os parâmetros foram os mesmos que os simulados no caso uniforme (Figura 4.5 à esquerda). Como podemos ver, necessitamos de um SNR muito mais alto para atingir o *threshold*, mas o esquema TL ainda mantem uma vantagem com relação a V&C.

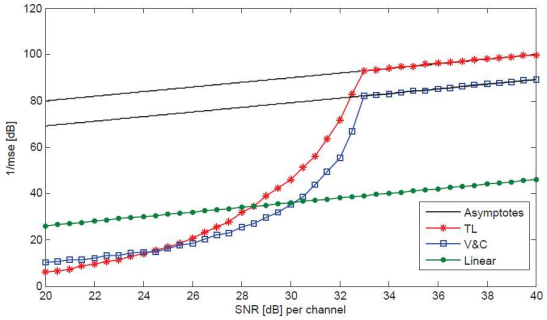


Figura 4.7: Simulações para uma fonte gaussiana

.

Finalizamos esta seção com uma observação sobre a implementação. Como as curvas construídas pelo nosso método são fechadas, se o valor enviado estiver próximo de algum dos extremos do intervalo $I_j = [L_{j-1}/L, L_j/L]$, isto é, se $L_{j-1}/L + \varepsilon$ é enviado, o decodificador poderá gerar como saída um valor próximo de L_j/L, produzindo um erro muito grande. Esse efeito, que assintoticamente é negligenciável, pode deteriorar bastante o comportamento prático do nosso es-

quema. Para prever tais erros, na prática, o codificador deve "comprimir" o intervalo I_j por um fator $\alpha \in (0, 1)$, de modo a "abrir" a curva, separando os valores dos extremos. Por outro lado, essa técnica deteriora a performance acima do *threshold*, de modo que devemos calibrar α cuidadosamente. Nos nossos exemplos, precisamos tomar $\alpha \in (0.7, 0.8)$.

4.5 Referências Futuras

Como exibido na análise assintótica e nas simulações, as curvas em camadas de toro possuem um bom desempenho em termos do MSE como função da razão sinal-ruído do canal. Além disso, um recente trabalho de Almeida et. al [ATB13] mostra como aplicar nossas construções para o canal *wiretap* (uma espécie de canal gaussiano grampeado em que um receptor ilegítmo tenta obter informação da transmissão). Se convenientemente parametrizados, os códigos em camadas de toro provém naturalmente segurança para a transmissão, forçando o receptor não-autorizado a operar em regimes de alto ruído. Em [TMZ13], os autores estudam como otimizar os parâmetros dos nossos códigos de modo a melhorar o desempenho no regime de alto ruído, sem comprometer o comportamento assintótico, incluindo um estudo analítico do decodificador de máxima verossimilhança.

Capítulo 5

Aplicações de Expansão de Largura de Banda

No capítulo anterior, consideramos aplicações utilizadas para transmitirmos uma fonte unidimensional através de um canal gaussiano n-dimensional. Aqui, consideraremos uma extensão natural deste problema, dada pelo modelo de comunicação abaixo: Estamos interessados no caso $k < n$, conhecido como regime

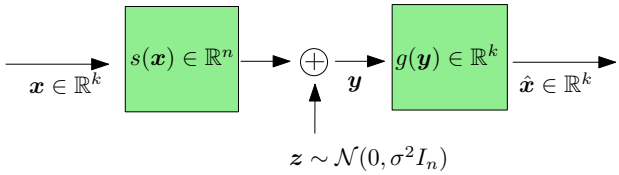


Figura 5.1: Modelo de Comunicação

de expansão de largura de banda. A teoria da taxa *versus* distorção estabelece que o erro quadrático médio do sistema não pode decair a uma taxa melhor que $\text{MSE} = O(\text{SNR}^{-n/k})$ (ver Seção 5.1). Diz-se que um esquema de codificação que atinge essa taxa possui *expoente ótimo*. Esquemas com expoente ótimo foram estudados previamente por Santhi e Vardy [SV03], Kleiner e Rimoldi [KR10] e Bhattad e Narayanan [BN10]. Todas essas referências estudam apenas o caso $k = 1$. Limitantes que vão além do expoente do MSE podem ser encontrados em [ILZF08].

Para o caso $k = 1$, vimos que este problema está associado a encontrar curvas esféricas de comprimento grande. Como é de se esperar, para $k > 1$, códigos para

esse modelo de comunicação estão relacionados com variedades de dimensão k no $\mathbb{R}^n$ com certas propriedades geométricas.

Apesar de a formulação do problema ser completamente análoga à do capítulo anterior, veremos mais para frente que a figura de mérito para o modelo de comunicação acima guarda algumas particularidades as quais torna não trivial a generalização para fontes de dimensão superior. Isso explica em parte porque referências anteriores na literatura consideraram apenas o caso unidimensional.

Os resultados deste capítulo foram parcialmente apresentados no *IEEE Information Theory Workshop*, Sevilha, Espanha (2013), e podem ser encontrados em [CVC13].

5.1 Limitantes Fundamentais

A formulação do problema é completamente análoga ao caso unidimensional. Um vetor $\boldsymbol{x} \in \mathbb{R}^k$ retirado de uma distribuição contínua deve ser transimitido através de um canal gaussiano n-dimensional. Um receptor estima o vetor enviado como $\hat{\boldsymbol{x}}$ de modo a minimizar o erro quadrático médio por dimensão da fonte, dado por

$$\text{MSE} = \frac{1}{k} E\left[\left\|\boldsymbol{X} - \hat{\boldsymbol{X}}\right\|_2^2\right].$$

5.1.1 Limitante de Cramér-Rao

O Limitante de Cramér-Rao [Sak70] é provavelmente o limitante inferior mais geral para o MSE e resulta em boas estimativas quando o ruído é particularmente baixo. Dado um vetor desconhecido $\boldsymbol{x}$ com vetor de observação $y(\boldsymbol{x})$, o limitante de Cramér-Rao nos diz que

$$E\left[\left\|\boldsymbol{X} - \hat{\boldsymbol{X}}\right\|_2^2 \mid \boldsymbol{X} = \boldsymbol{x}\right] \geq \text{tr}(I(\boldsymbol{x})^{-1}), \tag{5.1}$$

onde $I(\boldsymbol{x})$ é a Matriz de Informação de Fisher dada por

$$[I(\boldsymbol{x})]_{ij} = E_{\boldsymbol{y}}\left[\frac{\partial \ln f(\boldsymbol{y};\boldsymbol{x})}{\partial x_i}\frac{\partial \ln f(\boldsymbol{y};\boldsymbol{x})}{\partial x_j}\right],$$

e $f(\boldsymbol{y};\boldsymbol{x})$ é a função densidade de probabilidade das observações $\boldsymbol{y}$ com respeito ao parâmetro $\boldsymbol{x}$. Consideremos agora o nosso modelo de comunicação. Suponhamos que a aplicação que leva $\boldsymbol{x}$ na saída do canal é dada por $\boldsymbol{s} : \Omega \to \mathbb{R}^n$, onde Ω é o suporte da fonte, e $p(\boldsymbol{x})$ é sua a função distribuição de probabilidade. Fixado um vetor desconhecido, as observações são dadas por

$$\boldsymbol{Y} = \boldsymbol{s}(\boldsymbol{x}) + \boldsymbol{Z}, \text{tal que } \boldsymbol{Z} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2 I_n),$$

Assim, temos que

$$f(\boldsymbol{y};\boldsymbol{x}) = \frac{e^{-\|\boldsymbol{y}-\boldsymbol{s}(\boldsymbol{x})\|_2^2/2\sigma^2}}{\left(\sqrt{2\pi\sigma^2}\right)^n}. \tag{5.2}$$

$$\begin{aligned}\frac{\partial \ln f}{\partial x_i} &= \frac{1}{\sigma^2}\left\langle \boldsymbol{y} - \boldsymbol{s}(\boldsymbol{x}), \frac{\partial \boldsymbol{s}(\boldsymbol{x})}{\partial x_i}\right\rangle. \\ &= (\boldsymbol{y} - \boldsymbol{s}(\boldsymbol{x}))[J_s(\boldsymbol{x})]_i,\end{aligned}$$

onde $[J_s(\boldsymbol{x})]_i$ representa a i-ésima coluna do jacobiano de $\boldsymbol{s}$, definido como

$$[J_s(\boldsymbol{x})]_{ij} = \partial s_i/\partial x_j.$$

Tomando a esperança de ambos os termos, temos que

$$[I(\boldsymbol{x})]_{ij} = \frac{1}{\sigma^2}\left\langle [J_s(\boldsymbol{x})]_i, [J_s(\boldsymbol{x})]_j \right\rangle,$$

o que nos dá o limitante

$$\text{MSE} = \frac{1}{k}E\left[\left\|\boldsymbol{X} - \hat{\boldsymbol{X}}\right\|_2^2\right] \geq \frac{\sigma^2}{k}\int_\Omega \text{tr}((J(\boldsymbol{x})J(\boldsymbol{x})^t)^{-1})p(\boldsymbol{x})\text{d}\boldsymbol{x}. \tag{5.3}$$

Note que quando $k = 1$, esta fórmula especializa-se para

$$E[(X - \hat{X})^2] \geq \sigma^2 \int_\Omega \frac{p(x)}{\|\dot{s}(x)\|_2^2} \mathrm{d}x, \tag{5.4}$$

que é precisamente o erro quadrático médio do regime de ruído baixo discutido no capítulo anterior (4.3). Nas nossas construções, focaremos novamente em fontes uniformes, de modo que daqui para frente $p(\boldsymbol{x}) = 1$ e $\Omega = [0, 1)^k$.

5.1.2 Limitante da Taxa *versus* Distorção

Aqui utilizamos extensivamente os resultados de [CT06, Cap. 12], sem definir formalmente a terminologia de Teoria da Informação.

Dada uma fonte sem memória com entropia diferencial $h(X) < \infty$, a função de taxa *versus* distorção com respeito ao erro quadrático médio satisfaz

$$R(D) \geq h(X) - \frac{1}{2} \log 2\pi e D.$$

Por outro lado, a capacidade do canal gaussiano é dada por

$$C = \frac{1}{2} \log \left(1 + \frac{P}{\sigma_c^2}\right) \text{ bits/uso do canal,}$$

onde σ_c é a variância do ruído. No nosso modelo, estamos utilizando k amostras da fonte para n usos do canal, e portanto $kR(D) \leq nC$, o que implica

$$\mathrm{MSE} \geq \frac{1}{2\pi e}(1 + \mathrm{SNR})^{-n/k}. \tag{5.5}$$

Isso nos mostra que o MSE não pode decair a uma taxa melhor que $O(\mathrm{SNR}^{-n/k})$. O lado direito da desigualdade acima é também chamado de OPTA (*Optimum Performance Theoretically Attainable*).

Observamos que limitantes derivados da teoria de taxa *versus* distorção são atingíveis invocando o Princípio da Separação de Shannon, através de códigos

digitais com bloco arbtirariamente longos. Ao invés disso, aqui estamos interessados em aplicações para blocos significativamente pequenos (como $k = 1$, no capítulo anterior). Neste caso, um resultado relativamente recente de Ingber et. al [ILZF08] aprimora as constantes no limitante acima. De fato, os resultados em [ILZF08] nos mostram que a diferença entre a constante atingível por blocos finitos e o lado direito de (5.5) cresce significativamente à medida que a dimensão do canal aumenta.

5.2 A aplicação mod-1

Seja A uma matriz com entradas inteiras de ordem $k \times n$, $k < n$. A aplicação mod-1 é definida da seguinte maneira:

$$s_1(\boldsymbol{x}) = (\boldsymbol{x}A)_1 = \boldsymbol{x}A \pmod 1 = \boldsymbol{x}A \ - \lfloor \boldsymbol{x}A \rceil \,, \tag{5.6}$$

em que $\lfloor \boldsymbol{y} \rceil$ é o vetor obtido arredondando cada entrada de $\boldsymbol{y}$ para o inteiro mais próximos. Para $k = 1$, essa função linear por partes leva os pontos do intervalo $[0, 1)$ em um conjunto de segmentos de reta em $\mathbb{R}^n$, e é similar ao conjunto de retas que produz as curvas em toros estudadas em 4.2. Para $k \geq 2$, analogamente, a imagem de $\boldsymbol{s}_1(\boldsymbol{x})$ é a intersecção dos espaços afins $\{\boldsymbol{x}A + \boldsymbol{n} : \boldsymbol{x} \in \mathbb{R}^k\}$, $\boldsymbol{n} \in \mathbb{Z}^n$, dentro da caixa $[-1/2, 1/2)^n$. De maneira mais formal, temos:

$$s_1(\mathbb{R}^k) = s_1([0,1)^k) = \bigcup_{n \in \mathbb{Z}} (\text{span}(A) + \boldsymbol{n}) \cap [-1/2, 1/2)^n. \tag{5.7}$$

Com o proposito de empregar a aplicação mod-1 para codificação contínua, necessitamos de algumas propriedades de $\boldsymbol{s}_1(\boldsymbol{x})$, descritas na proposição a seguir.

Proposição 5.2.1. *Seja $\boldsymbol{s}_1 : [0,1)^k \to [-1/2, 1/2)^n$ a aplicação mod-1 (5.6), com A uma matriz inteira de ordem $k \times n$ e posto k. As seguintes propriedades são válidas:*

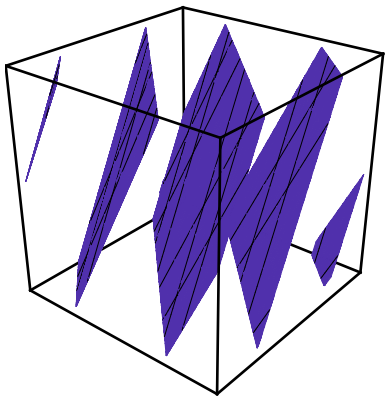


Figura 5.2: Imagem de $\boldsymbol{s}_1(\boldsymbol{x})$, com $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}$

(i) *$\boldsymbol{s}_1$ é injetiva se, e somente se, as linhas de A formam um conjunto primitivo de vetores de $\mathbb{Z}^n$*

(ii) *A energia média de $\boldsymbol{s}_1(\boldsymbol{x})$ para $\boldsymbol{x}$ uniformemente distribuído no cubo $[0,1)^k$ é dada por $E\left[\|\boldsymbol{s}_1(\boldsymbol{X})\|_2^2\right] = n/12$.*

(iii) *A distância mínima entre os planos que compõem a imagem de $\boldsymbol{s}_1(\boldsymbol{x})$ é igual à norma mínima do reticulado $P_{A^\perp}(\mathbb{Z}^n)$.*

Demonstração. (i) Pela caracterização (iii) do Teorema 1.1.9 com $A = V$, as linhas de A são um conjunto primitivo de vetores em $\mathbb{Z}^n$ se, e somente se, $\left\{\boldsymbol{x}A : \boldsymbol{x} \in [0,1)^k\right\} \cap \mathbb{Z}^n = \{\boldsymbol{0}\}$. É claro que essa condição pode ser substituída por $\left\{\boldsymbol{x}A : \boldsymbol{x} \in (-1,1)^k\right\} \cap \mathbb{Z}^n = \{\boldsymbol{0}\}$, já que qualquer ponto de $(-1,1)^k$ pode ser transladado por uma direção inteira para $[0,1)^k$. Suponha que $\boldsymbol{x}$ e $\tilde{\boldsymbol{x}}$ são tais que

$$\boldsymbol{x}A - \lfloor \boldsymbol{x}A \rceil = \tilde{\boldsymbol{x}}A - \lfloor \tilde{\boldsymbol{x}}A \rceil \therefore (\boldsymbol{x} - \tilde{\boldsymbol{x}})A = \lfloor \tilde{\boldsymbol{x}}A \rceil - \lfloor \boldsymbol{x}A \rceil = \boldsymbol{n} \in \mathbb{Z}^n.$$

Como $\boldsymbol{x} - \tilde{\boldsymbol{x}} \in (-1,1)^k$, $\boldsymbol{n}$ deve ser o vetor nulo e assim, $\boldsymbol{x} = \tilde{\boldsymbol{x}}$ e portanto $\boldsymbol{s}_1$ é injetiva. Reciprocamente, se $\boldsymbol{s}_1$ é injetiva, então para qualquer $\boldsymbol{x} \in [0,1)^k$ tal que $\boldsymbol{x}A$ é inteiro, temos $\boldsymbol{x} = \boldsymbol{0}$, provando que as linhas de A são um conjunto primitivo de vetores.

(ii) Para qualquer inteiro não-nulo a, vale que

$$\int_{-1/2}^{1/2}(ax - \lfloor ax \rceil)^2 \mathrm{d}x = \frac{1}{12}.$$

A energia média dos pontos de $\boldsymbol{s}_1(\boldsymbol{x})$ é dada por

$$\begin{aligned} E\left[\|\boldsymbol{s}_1(\boldsymbol{X})\|_2^2\right] &= \int_0^1 \cdots \int_0^1 \sum_{j=1}^{n} \left(\sum_{i=1}^{k} x_i A_{ij} - \lfloor x_i A_{ij} \rceil \right)^2 \mathrm{d}x_1 \ldots \mathrm{d}x_n \\ &= \sum_{j=1}^{n} \int_0^1 \cdots \int_0^1 \left(\sum_{i=1}^{k} x_i A_{ij} - \lfloor x_i A_{ij} \rceil \right)^2 \mathrm{d}x_1 \ldots \mathrm{d}x_n \qquad (5.8) \\ &= \sum_{j=1}^{n} \int_0^1 \cdots \int_0^1 \frac{1}{12} \mathrm{d}x_2 \ldots \mathrm{d}x_n = \frac{n}{12} \end{aligned}$$

(iii) Observe que pela caracterização (5.7), a distância mínima $\overline{\rho}$ entre dois planos em $\boldsymbol{s}_1([0,1)^k)$ pode ser calculada como

$$\overline{\rho} = \min_{\boldsymbol{n}\in\mathbb{R}^n, \boldsymbol{n}\notin A^\perp} \min_{\boldsymbol{x}\in\mathbb{Z}^k} \|\boldsymbol{x}A - \boldsymbol{n}\|_2 .$$

A solução para o mínimo interior é obtida projetando de $\boldsymbol{n}$ em $A^\perp$, de modo que

$$\min_{\boldsymbol{x}\in\mathbb{R}^k} \|\boldsymbol{x}A - \boldsymbol{n}\|_2 = \|P_{A^\perp}(\boldsymbol{n})\|_2 .$$

Temos portanto:

$$\overline{\rho} = \min_{\boldsymbol{0}\neq\boldsymbol{y}\in P_{A^\perp}(\mathbb{Z}^n)} \|\boldsymbol{y}\|_2 , \qquad (5.9)$$

ou seja, $\overline{\rho}$ é igual ao menor vetor não nulo em $P_{A^\perp}(\mathbb{Z}^n)$, concluindo a demonstração. □

O item (ii) acima nos diz que normalizando $\boldsymbol{s}_1(\boldsymbol{x})$ por um fator $\alpha = 2\sqrt{3P}/\sqrt{n}$, a aplicação $\boldsymbol{s}(\boldsymbol{x}) = \alpha s_1(\boldsymbol{x})$ respeita a restrição de potência. De agora em diante, consideraremos sempre a aplicação $s(\boldsymbol{x})$ (normalizada pelo fator α) como função de codificação.

Similarmente ao Capítulo 4, uma grandeza relevante para nossas análises será o raio de empacotamento do local geométrico do sinal, definido de maneira análoga ao caso de curvas como o maior valor tal que os "tubos" ao redor dos segmentos que compõem a imagem de $\boldsymbol{s}(\boldsymbol{x})$ não se sobrepõem. Aplicando a Proposição 3.1.3 (com $V = A$) e a definição de densidade de centro, vemos que esse raio possui relação com o $\det A$ através da equação

$$\rho = \frac{4\sqrt{3P}\delta^{1/(n-k)}}{\sqrt{n}\det\left(AA^t\right)^{1/2(n-k)}}, \tag{5.10}$$

onde δ é a densidade de centro de $P_{A^\perp}(\mathbb{Z}^n)$. Assim, um critério para escolher as aplicações é escolher A primitivo de modo que $\det(AA^t)$ seja pequeno.

Exemplo 5.2.2. *Seja $w \in \mathbb{N}$. Considere a família de matrizes de ordem $(n-1)$ por n dada por*

$$A_w = \begin{pmatrix} 1 & w & 0 & \cdots & 0 & 0 \\ 0 & 1 & w & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & w \end{pmatrix}, \tag{5.11}$$

Como o determinante da matriz constituída pelas $(n-1)$ primeiras colunas de A_w é igual a 1, as linhas de A_w formam um conjunto primitivo de vetores em $\mathbb{Z}^n$. É fácil ver que

$$\det(A_w A_w^t) = \sum_{i=1}^{n-1} w^{2i}.$$

Como $P_{A^\perp}(\mathbb{Z}^n)$ é sempre um reticulado unidimensional ($\delta = 1/2$) temos

$$\overline{\rho} = \frac{1}{\sqrt{\det(A_w A_w^t)}} = \frac{1}{(\sum_{i=1}^{n-1} w^{2i})^{1/2}}. \tag{5.12}$$

5.2.1 Análise do MSE

As técnicas para a análise do MSE utilizadas aqui podem ser encontradas em [VC03, Sec. VI B]. Suponha que utilizamos $\boldsymbol{s}(\boldsymbol{x})$ como função de codificação e que o vetor recebido $\boldsymbol{y} = \boldsymbol{s}(\boldsymbol{x}) + \boldsymbol{z}$. Por simplicidade, assumimos que σ^2 é fixo, analisando como o MSE se comporta à medida que aumentamos P. Mostraremos também como escolher a matriz A (ou a família de matrizes A_w) de acordo com a potência do canal para minimizar o MSE.

Seja $\rho = \overline{\rho}/2$ a *metade* da distância mínima entre os segmentos que compõem a imagem de $\boldsymbol{s}$. Considere o evento $E_\rho = \{\|\boldsymbol{Z}\|_2 < \rho\}$. O MSE pode ser limitado por

$$\begin{aligned} \text{MSE} &= \frac{1}{k} E\left[\left\|\boldsymbol{X} - \hat{\boldsymbol{X}}\right\|_2^2 \mid E_\rho\right] P\left(E_\rho\right) + \frac{1}{k} E\left[\left\|\boldsymbol{X} - \hat{\boldsymbol{X}}\right\|_2^2 \mid E_\rho^c\right] P\left(E_\rho^c\right) \\ &\leq \frac{1}{k} E\left[\left\|\boldsymbol{X} - \hat{\boldsymbol{X}}\right\|_2^2 \mid E_\rho\right] + P\left(E_\rho^c\right) \end{aligned} \tag{5.13}$$

O primeiro termo da desigualdade acima é o MSE em regime de ruído baixo (isto é, quando $\hat{\boldsymbol{x}}$ é decodificado no mesmo segmento que $\boldsymbol{x}$) e aproxima-se do Limitante de Cramér-Rao (5.1) à medida que a potência cresce. O termo $P\left(E_\rho^c\right)$ é a probabilidade que um vetor com distribuição gaussiana possua norma maior que ρ, e vale portanto

$$P\left(\|\boldsymbol{Z}\|_2 \geq \rho\right) = e^{-\rho^2/2\sigma^2} \sum_{i=0}^{n-1} \frac{(\rho^2/2\sigma^2)^i}{i!}.$$

Assim, em geral, se utilizamos uma família de matrizes A_w, com w um parâmetro de projeto a ser escolhido convenientemente, o MSE satisfaz

$$\text{MSE} \leq \frac{\sigma^2 n \text{tr}(A_w A_w^t)^{-1}}{12kP} + e^{-\rho_w^2/2\sigma^2} \sum_{i=0}^{n-1} \frac{(\rho_w^2/2\sigma^2)^i}{i!}. \tag{5.14}$$

Para que o primeiro termo atinja ordem de decaimento $O(1/P^{n/k})$ é necessário (e suficiente) que $\text{tr}(A_w A_w^t)^{-1} = O(1/P^{(n-k)/k})$. Além disso, precisamos garantir

que $P\left(\|\boldsymbol{Z}\|_2 \geq \rho_w\right)$ não domina a equação acima. Para tal propósito, é suficiente garantir que a distância entre os segmentos da imagem de $\boldsymbol{s}(\boldsymbol{x})$ seja suficientemente grande. Da equação (5.10), precisamos que a densidade dos reticulados $P_{A_w^{\perp}}(\mathbb{Z}^n$ tenda a um número não-nulo, o que implica que $\det(A_w A_w^t)^{1/(n-k)+\mu}$ para algum $\mu > 0$. Se estas condições forem satisfeitas, o termo $P\left(\|\boldsymbol{Z}\|_2 \geq \rho_w\right)$ será exponencialmente pequeno, e o MSE total atingirá o expoente ótimo.

Os argumentos acima impõem uma condição entre o traço e o determinante de $(A_w A_w^t)^{-1}$, a saber $\mathrm{tr}(A_w A_w^t)^{-1} = O(1/P^{(n-k)/k})$. Em suma, se as três condições abaixo forem satisfeitas para a família de matrizes A_w obteremos uma família de esquemas de codificação com expoente ótimo.

(i) (Injetividade) As colunas de A_w são um conjunto primitivo de vetores de $\mathbb{Z}^n$.

(ii) (Distância mínima) A densidade de $P_{A_w^{\perp}}(\mathbb{Z}^n)$ está afastada de zero à medida que w cresce. (De fato, quanto maior a densidade, melhor a aproximação feita em (5.14)).

(iii) (Expoente do MSE)

$$\mathrm{tr}(A_w A_w^t)^{-1} = O(\det\left(A_w A_w^t\right)^{-1/k}) \tag{5.15}$$

As condições (i) e (ii) podem ser resolvidas utilizando as construções de projeção do Capítulo 3. De fato, para atingir apenas o expoente ótimo, não necessitamos projeções que aproximem o melhor reticulado $(n-k)$-dimensional, mas apenas alguma construção cujo limite seja um reticulado com densidade não-nula. A maior complexidade está na condição (iii), a qual nos referiremos como condição traço-determinante. Utilizando argumentos do tipo média aritmética *versus* média geométrica não é difícil mostrar que para qualquer matriz de posto completo a

$$\mathrm{tr}(AA^t)^{-1} \geq k \det\left(AA^t\right)^{-1/k},$$

com igualdade satisfeita se, e somente se, as colunas de A são ortogonais e possuem

mesma norma. Portanto, a condição (iii) é bastante restrita, levando em conta que também precisamos que as linhas de A sejam um conjunto primitivo de vetores.

Exemplo 5.2.3 (Otimalidade da aplicação $(n-1):n$)**.** *Sejam A_w as matrizes como no Exemplo 5.2.2. Como mostrado no exemplo,* $\det(A_w A_w^t) = \Theta(w^{2(n-1)})$. *Além disso, é fácil ver que $[(A_w A_w^t)^{-1}]_{ii} = \Theta(1/w^2)$, e deste modo a condição traço-determinante é satisfeita. Da análise anterior, se escolhermos o parâmetro w de modo que $P = \Theta(w^{2n-2+\mu})$ para algum $\mu > 0$ arbitrariamente pequeno, o MSE da aplicação mod-1 $\boldsymbol{s}(\boldsymbol{x})$ decairá com expoente ótimo.*

Exemplo 5.2.4 (Otimalidade dos Códigos *Shift* [VC03])**.** *Para $k = 1$, foram propostos códigos baseados na aplicação shift em [VC03]. Na linguagem deste capítulo, os códigos shift são dados pela aplicação mod-1* (5.6)*, cujas matrizes A_w possuem uma única linha dada pelo vetor primitivo*

$$(1, w, w^2, \ldots, w^{n-1}).$$

Neste caso, a condição traço-determinante é trivialmente satisfeita. Além disso, pode-se demonstrar que a densidade dos reticulados projeção de $\mathbb{Z}^n$ associados convergem para a densidade de $\mathbb{Z}^{n-1}$, e assim a condição de distância mínima também é satisfeita. Segue que os códigos shift possuem expoente ótimo.

Observação 5.2.5. *Um outro exemplo de códigos com expoente ótimo baseado em ideias similares à da aplicação mod-1 é descrito [KR10].*

Exemplo 5.2.6. *Seja $A_w, w \in \mathbb{N}$, a sequência de matrizes dada por*

$$(A_w)_{ij} = \begin{cases} w^{\lfloor (i-1)/2 \rfloor} & \text{if } (i,j) = (1, \text{ímpar}) \text{ ou } (2, \text{par}) \\ 0 & \text{caso contrário} \end{cases}$$

Por exemplo, para $n = 2m+1$ ímpar, a imagem de A_w é gerada pelos vetores $(1, 0, w, 0, w^2, \ldots, 0, w^m)$ e $(0, 1, 0, w, \ldots, w^{m-1}, 0)$. Argumentando como na Seção 3.2, podemos mostrar que as projeções de $\mathbb{Z}^n$ em $A_w^{\perp}$ estão, a menos de equivalência, próximas do reticulado $\mathbb{Z}^{n-2}$ à medida que w cresce. A Figura 5.3

exibe a densidade de centro dos reticulados projeção à medida que w aumenta e $n = 5$. Se n é par, as linhas de A_w possuem mesma norma e são ortogonais, portanto a condição traço-determinante é garantida, e desde modo obtemos códigos com expoente ótimo (observe que estes são precisamente os códigos shift acima utilizados sincronizadamente para cada saída da fonte). Se $n = 2m + 1$ é ímpar, temos

$$A_w A_w^t = \begin{pmatrix} p_m(w) & 0 \\ 0 & p_{m-1}(w) \end{pmatrix},$$

onde $p_m(w) = 1 + w + \cdots + w^m = O(w^m)$. Assim, $\det(A_w A_w^t)$ é um polinômio com termo de maior grau w^{2m-1}. Além disso, $tr((A_w A_w^t)^{-1}) = \Theta(w^{1-m})$, de onde vemos que $tr(A_w A_w^t)^{-1} = O(\det(A_w A_w^t)^{-1/2+1/4(2m-1)})$, ou seja, a condição traço-determinante não é satisfeita. De fato, argumentando da mesma maneira acima, pode-se mostrar que o melhor expoente possível do MSE no caso ímpar é dado por $P^{-m} = P^{-(n-1)/2}$ (o mesmo expoente se tivéssemos "desistido" de uma dimensão do canal).

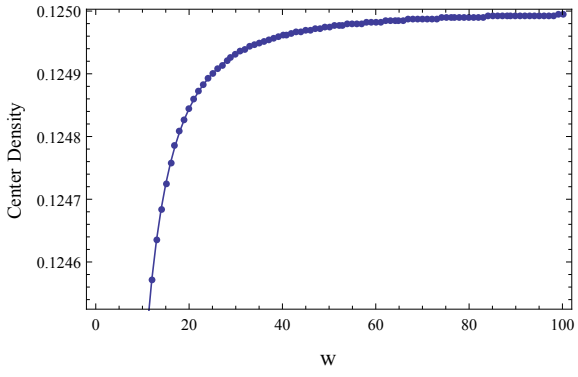


Figura 5.3: Densidade de centro de $P_{A_w^\perp}(\mathbb{Z}^5)$ em função de w.

5.2.2 Decodificação

Para o esquema de comunicação considerado, o melhor decodificador em termos do erro quadrático médio (MMSE), dado um vetor recebido $\boldsymbol{y}$ é dado por [Sak70]:

$$\hat{\boldsymbol{x}}(\boldsymbol{y}) = E\left[\boldsymbol{x}|\boldsymbol{y}\right].$$

Na prática, entretanto, tal decodificador possui grande complexidade de implementação. Focamos, portanto no decodificador de máxima verossimilhança que é dado pelo valor que maximiza $\log f(\boldsymbol{y};\boldsymbol{x})$ (Equação (5.2)). Assim, mostra-se facilmente que

$$\hat{\boldsymbol{x}}(\boldsymbol{y}) = \arg\min_{\boldsymbol{x}} \left\|\boldsymbol{y} - s(\boldsymbol{x})\right\|_2.$$

Em outras palavras, $\hat{\boldsymbol{x}}(\boldsymbol{y})$ é a distância do ponto recebido até a imagem de $s(\boldsymbol{x})$. Baseado na caracterização da imagem de $s(\boldsymbol{x})$ dada pela equação (5.7), desenvolvemos um algoritmo eficiente para a decodificação por máxima verossimilhança, dado em pseudo-código ProjDecod. A ideia do algoritmo é, dado um ponto recebido $\boldsymbol{y}$, projetá-lo em $A^{\perp}$ e efetuar uma decodificação no reticulado $P_{A^{\perp}}(\mathbb{Z}^n)$ de modo a encontrar o ponto mais próximo do projetado. Por conta de (5.7), as coordenadas inteiras do ponto mais próximo da projeção dirão exatamente qual das translações de span(A) minimiza a distância até o vetor recebido. A partir daí, projetamos no plano correspondente e encontramos a coordenada do vetor projetado, que será a estimativa $\hat{\boldsymbol{x}}$. No pseudo-código abaixo, assumimos que existe uma procedimento capaz de executar a decodificação no reticulado $P_{A^{\perp}}(\mathbb{Z}^n)$. Alguns algoritmos de decodificação universais que podem ser empregados aqui encontram-se descritos em [AEVZ02].

A complexidade do algoritmo é dominada pela decodificação no reticulado $P_{A^{\perp}}(\mathbb{Z}^n)$. De maneira geral, decodificar em reticulados arbitrários possui complexidade exponencial [AEVZ02], apesar de existirem algoritmos aproximados com complexidade polinomial. Excetuando a decodificação, a operação mais cara efetuada é resolução de sistemas linear/inversão de matrizes, cujo custo é de $O(n^3)$

operações aritméticas.

Algoritmo 2 Decodificação por projeções

1: PROJDECOD(A, $\boldsymbol{y}, \alpha = 2\sqrt{3P}/n$)
2: $\quad P \leftarrow I_n - A^t(AA^t)^{-1}A$
3: $\quad \bar{\boldsymbol{y}} \leftarrow P\boldsymbol{y}/\alpha$
4: $\quad$ Encontre $\hat{\boldsymbol{z}} = \arg \min_{\boldsymbol{z} \in P_{A^\perp}(\mathbb{Z}^n)} \|\boldsymbol{z} - \bar{\boldsymbol{y}}\|_2$
5: $\quad \hat{\boldsymbol{x}} \leftarrow (\alpha\boldsymbol{y} - \hat{\boldsymbol{z}})A(AA^t)^{-1}$
6: $\quad \hat{\boldsymbol{x}} \leftarrow \hat{\boldsymbol{x}} - \lfloor \hat{\boldsymbol{x}} \rceil$
7: **return** $\hat{\boldsymbol{x}}$
8: **fim**

Simulações

O algoritmo acima foi utilizado para fazermos simulações de como comporta-se o mapa $(n-1) : n$ ótimo do Exemplo 5.2.2. Para critério de comparação, escolhemos as matrizes A_w e B_w dadas por

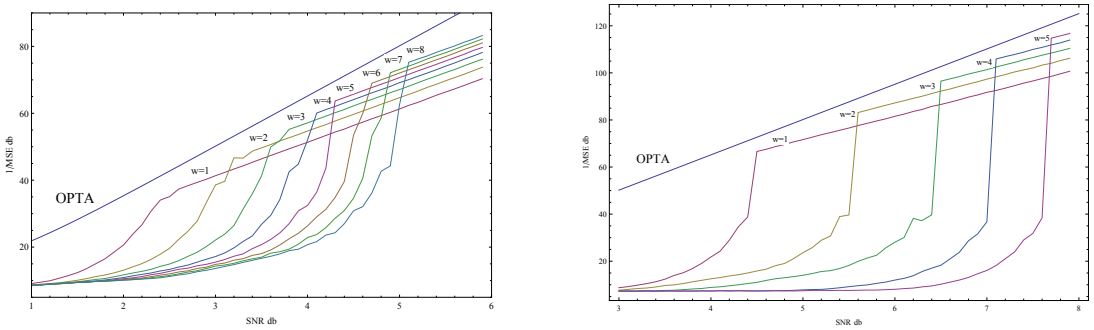
$$A_w = \begin{pmatrix} 1 & w & 0 \\ 0 & 1 & w \end{pmatrix} \tag{5.16}$$

$$B_w = \begin{pmatrix} w(w+1) & w & w+1 \\ 1-w & (w+1)w & -w \end{pmatrix}. \tag{5.17}$$

No segundo caso, é também fácil ver que B_w satisfazem as três condições de otimalidade da Seção 5.2.1. As aplicações correspondentes são

$$s_A(\boldsymbol{x}) = \alpha(\boldsymbol{x}A_w)_1 \text{ e } s_B(\boldsymbol{x}) = \alpha(\boldsymbol{x}B)_1.$$

As famílias consideradas nas simulações correspondem a expansão de largura de banda $2 : 3$, isto é, $k = 2$ e $n = 3$ dados pelas matrizes acima. Para ambos os



(a) Simulações para as matrizes A_w (b) Simulações para as matrizes B_w

Figura 5.4: Simulações de aplicações de expansão de largura de banda $(n-1) : n$ Acima do *threshold*, o sistema aproxima-se da Eq. (5.3)

esquemas, se utilizarmos limitantes de taxa-versus distorção, obtemos:

$$\text{MSE} \geq \frac{1}{2\pi e(1+\text{SNR})^{3/2}} = \text{OPTA}.$$

As simulações mostram um comportamento próximo da curva ótima. De fato, se w for escolhido de acordo com a relação sinal-ruído, obtemos uma curva paralela à OPTA, indicando que o expoente de decaimento do MSE está próximo do ótimo (-3/2). Para diferentes valores de n, se escolhermos matrizes de maneira análoga a A_w, encontramos expoentes próximos do ótimo $\text{SNR}^{-n/(n-1)}$. Cada simulação foi baseada em 15000 amostras independentes e uniformemente distribuídas em $[0,1)^2$ com valores de sinal-ruído variando entre 1 e 6db em um passo de 0.1. Nas simulações observamos que abaixo do *threshold*, a família A_w comporta-se melhor que a família B_w e esse comportamento inverte-se no regime de baixo ruído. Em comparação com o limitante OPTA, a família B_w apresenta um melhor desempenho, sugerindo que é preferível codificarmos com vetores ortogonais, ainda que com norma ligeiramente distintas.

5.3 Aplicação mod-1 Modificada

Como foi visto, a matriz A determina a imagem da aplicação $\boldsymbol{s}(\boldsymbol{x})$ (ou o local geométrico do sinal). Entretanto, existem diversas outras aplicações que que

produzem a mesma imagem. Apesar de a condição de distância mínima entre os segmentos de $\boldsymbol{s}([0,1)^k)$ ser inerente à imagem do cubo $[0,1)^k$ pela função $\boldsymbol{s}$, o traço da matriz AA^t é uma característica inerente apenas à aplicação. Como já temos técnicas de garantir a condição geométrica da distância entre os segmentos de $[0,1)^k$, faz sentido considerarmos aplicações diferentes que produzem a mesma imagem que $(A\boldsymbol{x})_1$. No que segue, apresentaremos uma aplicação alternativa a $(A\boldsymbol{x})_1$ que atinge a condição traço-determinante, com o custo de modificar o suporte da fonte.

Dada uma sequência de matrizes $A_w, w \in \mathbb{N}$, é sempre possível ortogonalizar as suas linhas (via fatoração RQ, por exemplo), de tal maneira que $A_w = R'_w Q'_w$, onde Q'_w é uma matriz ortogonal em R'_w é triangular superior. Após aplicarmos um fator de escala, obtemos $A_w = R_w Q_w$, onde $Q_w = \beta Q'_w$, $R_w = (1/\beta_w)R'_w$ e $\beta_w = (\det(A_w A_w^t)^{1/2k})$, e assim $\det R_w = 1$. Portanto, a imagem do cubo $[0,1)^k)$ pela aplicação $(\boldsymbol{x}A_w)_1$ é a mesma que a imagem do paralelepípedo $\mathcal{S}_w = R_w[0,1)^k$ pela aplicação $(\boldsymbol{x}Q_w)_1$, com a propriedade adicional de que $Q_w Q_w^t = \beta_w^2 I_k$, assegurando portanto a condição traço-determinante. Como R_w é uma transformação que preserva volume, para uma fonte uniformemente distribuída em $\mathcal{S}_w$ a mesma análise de MSE das seções anteriores e válida, substituindo A_w por Q_w. Portanto, se A_w satisfaz as condições de distância mínima e injetividade, a aplicação

$$s_Q : \mathcal{S}_w \to \mathbb{R}^n$$

$$s_Q(\boldsymbol{x}_2) = \alpha(Q_w \boldsymbol{x}_2 \pmod 1). \tag{5.18}$$

satisfará também ambas as condições e a condição do traço-determinante, atingindo assim expoente ótimo. Note, entretanto, que agora necessitamos que a fonte possua suporte "artificial" convenientemente escolhido $\mathcal{S}_w \neq [0,1)^k$. Para voltar ao problema original, precisamos de um método para mapear S_w de volta em $[0,1)^k$ de maneira a não deteriorar o erro quadrático médio. Tal método deve ser o mais próximo possível de uma isometria, mas sabemos que de uma maneira geral não há isometrias entre cubos e paralelepípedos. A seguir, mostraremos

uma abordagem para mapear $\mathcal{S}_w$ em $[0,1)^k$ através da teoria de *dissecções de poliedros*.

5.3.1 Dissecções de Poliedros

Seja $P \subset \mathbb{R}^n$ um politopo (ou poliedro). Uma *dissecção* de P em k diferentes poliedros é uma decomposição da forma

$$P = \bigcup_{i=1}^{k} P_i,$$

tal que os interiores de P_i e P_j são disjuntos para $i \neq j$. Os elementos P_i são chamados de *peças* da dissecção. Seja agora $Q \subset \mathbb{R}^n$ um outro poliedro e suponhamos que exista uma dissecção

$$Q = \bigcup_{i=1}^{k} Q_i,$$

tal que Q_i pode ser obtido de P_i por uma isometria de $\mathbb{R}^n$. Dizemos que Q e P são *equidissecáveis*. Poliedros equidissecáveis possuem o mesmo volume n-dimensional, mas a recíproca só é verdadeira para $n = 1, 2$[1]. Em termos gerais, uma dissecção pode ser vista como uma "isometria por partes", em que cada peça de um poliedro é levada em outra por isometrias. Existem diversas construções para exemplos específicos, principalmente em $\mathbb{R}^2$ e $\mathbb{R}^3$ (veja, por exemplo, o livro [Fre03]), e o objetivo principal é minimizar o número de peças da dissecção. Um método geral para realizar dissecções é o Teorema dos Dois Ladrilhos, cuja versão a qual utilizaremos aqui pode ser encontrada em [SV09].

Seja G um grupo de isometrias de $\mathbb{R}^n$, P um politopo em $\mathbb{R}^n$, e $\Omega \subset \mathbb{R}^n$. Se as imagens de P pela ação de G possuem interiores disjuntos e $\Omega = \bigcup_{g \in G} gP$, dizemos

[1] A recíproca desta afirmação no caso tridimensional constitui o 3º Problema de Hilbert. Um ano depois de posto o problema, Max Dehn demonstrou que o cubo e o tetraedro regular de mesmo volume não são equidissecáveis.

que P é um G-ladrilho de Ω.

Teorema 5.3.1 (dos Dois Ladrilhos [SV09])**.** *Se para algum conjunto $\Omega \subset \mathbb{R}^n$, dois politopos P e Q são G-ladrilhos de Ω, então P e Q são equidissecáveis.*

Um corolário ao teorema acima é o de que duas regiões fundamentais poliedrais (e.g., a região de Voronoï e um paralelotopo fundamental) de um reticulado possuem mesmo volume.

Corolário 5.3.2. *Se Q é um poliedro que ladrilha $\mathbb{R}^n$ por um reticulado $\Lambda \subset \mathcal{R}^n$, então* vol $Q = \sqrt{\det \Lambda}$.

Demonstração. Sabemos que o paralelotopo fundamental $\mathcal{P}(B)$ com respeito a alguma matriz geradora B de Λ é um Λ-ladrilho de $\mathcal{R}^n$ e possui volume $\sqrt{\det \Lambda}$. Interpretando Λ como um grupo de translações, tome $\Lambda = G$, $P = \mathcal{P}(B)$ e $\Omega = \mathbb{R}^n$ no teorema acima. □

Uma dissecção particularmente importante para nós será a dissecção do quadrado para o retângulo, descoberta por Jean Etienne Montucla no século XVIII. Ela é descrita em [Fre03, p. 221] da seguinte forma. Seja um quadrado Q e um retângulo Q'. Estenda a base de Q para a direita, desenhando linhas perpendiculares à base com distância igual ao comprimento do lado de Q entre elas. Rotacione Q' e posicione-o de modo que o seu canto esquerdo superior coincida com o do quadrado e o seu canto direito superior esteja na extensão da base, conforme a Figura 5.5. Os cortes da dissecção são as partes do retângulo cruzadas pelas linhas desenhadas e pela extensão da base.

Apesar de geometricamente atraente, a dissecção de Montucla da maneira descrita acima é pouco esclarecedora, e não nos dá nenhuma informação sobre possíveis generalizações para dimensões superiores. Abaixo, mostramos que a dissecção de Montucla é uma aplicação do Teorema dos Dois Ladrilhos. Por simplicidade, vamos mostrar como dissecar um retângulo e rearranjar as peças de modo a formar um quadrado de lado 1.

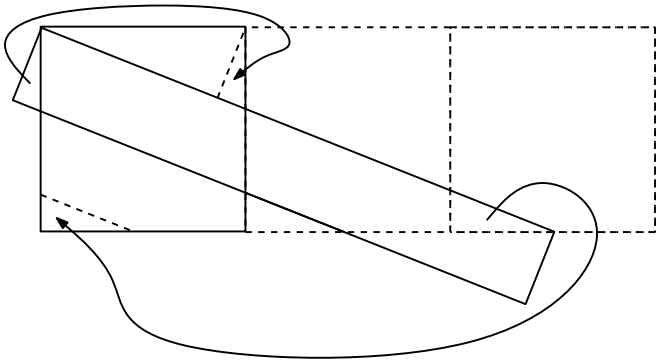


Figura 5.5: Dissecção de Montucla

Suponha que queremos transformar um retângulo de lados $l \times 1/l$, $l > 1$, em um quadrado de lado unitário. Seja $x = \sqrt{l^2 - 1}$. Considere o reticulado (grupo de translações) $\Lambda = \{u_1 + u_2 x : u_1, u_2 \in \mathbb{Z}\}$ i.e., o reticulado com matriz geradora

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

Considere agora o quadrado $Q = [0,1)^2 = \{(\alpha_1, \alpha_2) : 0 \leq \alpha_1 \leq 1, 0 \leq \alpha_2 \leq 1\}$ e o retângulo $Q' = \mathcal{P}(\boldsymbol{v}_1, \boldsymbol{v}_2) = \{\alpha \boldsymbol{v}_1 + \alpha \boldsymbol{v}_2 : 0 \leq \alpha_1 \leq 1, 0 \leq \alpha_2 \leq 1\}$, onde

$$\boldsymbol{v}_1 = \left(\frac{1}{1+x^2}, \frac{-x}{1+x^2} \right) \text{ e } \boldsymbol{v}_2 = (x, 1).$$

Temos a seguinte proposição

Proposição 5.3.3. *Q e Q' são Λ-ladrilhos de $\mathbb{R}^2$.*

Demonstração. (i) Q é um Λ-ladrilho de $\mathbb{R}^2$. Se os interiores de translações distintas de Q não fossem disjuntos, existiriam translações distintas de pontos de Q tais que $\boldsymbol{u}_1 B + (\alpha_1, \alpha_2) = \boldsymbol{u}_2 B + (\tilde{\alpha}_1, \tilde{\alpha}_2)$. Mas se isso ocorrer, então $(\boldsymbol{u}_1 - \boldsymbol{u}_2)B \in \Lambda \cap (-1, 1)^2$, ou seja $\boldsymbol{u}_1 = \boldsymbol{u}_2$ e $\alpha_i = \tilde{\alpha}_i$, provando que os interiores são disjuntos. Além disso, qualquer ponto $\boldsymbol{y} \in \mathbb{R}^n$ pode ser escrito como $\boldsymbol{y} = \boldsymbol{u}B + (\alpha_1, \alpha_2)$, com

$$u_2 = \lfloor y_2 \rfloor, u_1 = \lfloor y_1 - u_2 x \rfloor,$$

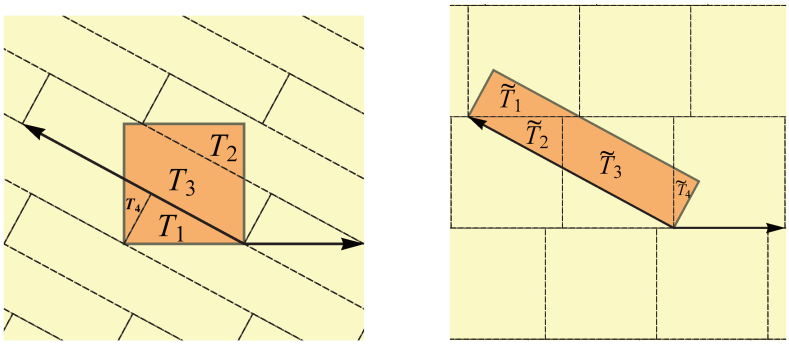


Figura 5.6: Dissecção de Montucla em termos do Teorema dos Dois Ladrilhos

$$\alpha_2 = y_2 - u_2, \alpha_1 = y_2 - (u_1 + u_2 x),$$

de tal modo que $0 \leq \alpha_1, \alpha_2 \leq 1$ e $u_1, u_2 \in \mathbb{Z}$. Assim Q é um Λ-ladrilho de $\mathbb{R}^2$. (ii) Q' é um Λ-ladrilho de $\mathbb{R}^2$. Novamente, não é difícil ver que dois pontos no interior de translações distintas de Q' não podem existir e que qualquer ponto do $\mathbb{R}^2$ pode ser escrito como $\boldsymbol{u}B + \alpha\boldsymbol{v}_1 + \alpha\boldsymbol{v}_2$ e assim Q' é um Λ-ladrilho de $\mathbb{R}^n$. $\square$

Uma ilustração da dissecção de Montucla nos termos da proposição acima pode ser vista na Figura 5.6. A ideia intuitiva é que podemos dissecar o quadrado sobrepondo-o com o ladrilhamento por retângulos, ou vice-versa.

Com esta interpretação da dissecção, podemos contar o número de peças formalmente. Com efeito, fixemos o retãngulo Q'. Seja $\boldsymbol{y} = u_1(1,0) + u_2(-\sqrt{l^2-1}, 1)$ um vetor de translação. Se $u_2 > 1$ ou $u_2 < 0$, então claramente a translação do quadrado tem intersecção vazia com Q'. Para a faixa equivalente a $u_2 = 1$, a única intersecção não vazia é quando $u_1 = 0$, dando-nos a primeira peça. Agora para a camada $u_2 = 0$, se $u_1 < -\sqrt{l^2-1}$, cada ponto da translação do quadrado tem coordenada no eixo horizontal igual a $-\sqrt{l^2-1}$, e portanto não intersecta Q'. Isso nos dá os possíveis valores $u_1 = -\left\lceil \sqrt{l^2-1} \right\rceil, \ldots, 0$. O número total de peças é portanto $2 + \left\lceil \sqrt{l^2-1} \right\rceil \leq \lceil l \rceil + 2$.

5.3.2 Esquema de Dissecções

Voltando ao problema de aplicações de expansão de largura de banda, nosso objetivo é construir uma bijecção entre $[0,1)^k$ e $\mathcal{S}_w$ como definido na Seção 5.3. Para isso, realizamos os seguintes passos:

(i) *Dissecamos* $[0,1)^k$ em m poliedros $T_1, T_2, \ldots, T_m$ cujos interiores são disjuntos dois a dois e $[0,1)^k = \bigcup_{i=1}^{m} T_i$;

(ii) *Dissecamos* $\mathcal{S}_w$ em m poliedros $\tilde{T}_1, \tilde{T}_2, \ldots, \tilde{T}_m$, cujos interiores são disjuntos dois a dois e $\mathcal{S}_w = \bigcup_{i=1}^{m} \tilde{T}_i$.

de tal maneira que T_i e $\tilde{T}_i$ estão relacionada por uma isometria. Isso nos permite estabelecer a bijeção Φ, onde

$$\boldsymbol{x}_2 = \Phi(\boldsymbol{x}) = \phi_i(\boldsymbol{x}),\ \boldsymbol{x} \in T_i,\ i = 1, 2, \ldots, m$$

.

Para montar o esquema de codificação por dissecções não podemos utilizar diretamente a bijeção acima. Para ver isso, suponha que $\boldsymbol{x}_2 \in \tilde{T}_i$ é transmitido. É possivel que um evento de ruído baixo resulte em uma estimativa que reside em $\tilde{T}_j$, $j \neq i$. As descontinuidades em Φ causarão assim um aumento não controlável do MSE entre $\boldsymbol{x}$ e $\boldsymbol{y}$, como ilustrado na Figura 5.7(a). Controlamos a degradação do MSE modificando a bijeção de maneira a encolher e separar cada peça da dissecção, reduzindo assim a probabilidade de decodificar na peça incorreta. A bijeção modificada está descrita a seguir.

Codificação: O codificador encontra i tal que $\boldsymbol{x} \in T_i$ e aplica $s(\boldsymbol{x}) = s_Q((1-\varepsilon)\phi_i(\boldsymbol{x}) + \boldsymbol{t_i})$ onde $\varepsilon > 0$ e $\boldsymbol{t_i}$ são tais que cada peça de $\mathcal{S}_w$ está encolhida de um fator $(1-\varepsilon)$ e separada, como na Figura 5.7(b).

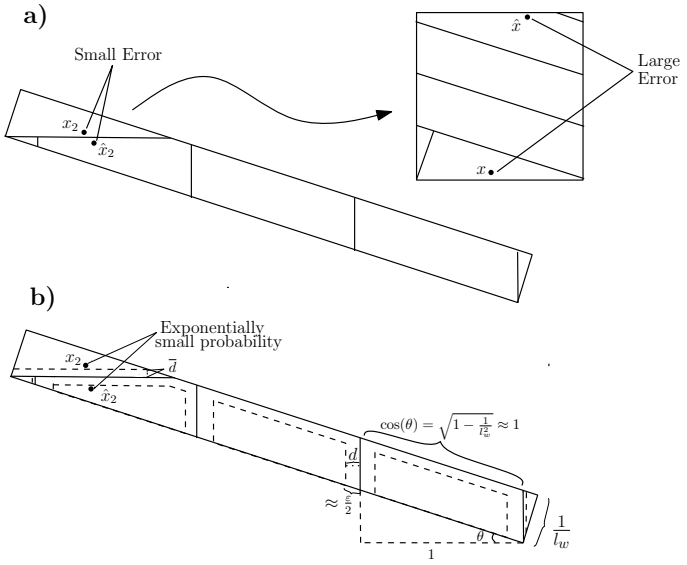


Figura 5.7: Ilustração da técnica de encolher/separar cada peça da dissecção

Decodificação: Dado $\boldsymbol{y} = s(\boldsymbol{x}) + \boldsymbol{z} = s_Q(\boldsymbol{x_2}) + \boldsymbol{z}$, onde $\boldsymbol{x_2} = (1-\varepsilon)\phi_i(\boldsymbol{x}) + \boldsymbol{t_i}$, o receptor decodifica $\boldsymbol{y}$ para recuperar $\hat{\boldsymbol{x}}_{\boldsymbol{2}} \in \mathcal{S}_w$ (isso pode ser feito com o Algoritmo 2) e então computa $\hat{\boldsymbol{x}} = \phi_i^{-1}(\hat{\boldsymbol{x}}_{\boldsymbol{2}} - \boldsymbol{t_i})/(1-\varepsilon)$.

Análise do MSE: Dentro das peças T_i, a análise assintótica do erro quadrático médio é essencialmente a mesma para $\boldsymbol{s}_Q(\boldsymbol{x})$ e $\boldsymbol{s}(\boldsymbol{x})$, pois ϕ_i é uma isometria. A complicação ocorre quando a estimativa $\hat{\boldsymbol{x}}_2$ "salta" de uma peça para outra, tal que durante o reagrupamento para formar o cubo original, um erro grande ocorre. A perda de MSE é, portanto, essencialmente produzida pelos eventos de "salto". Seja $\rho > 0$ metade da distância entre os segmentos de $s_Q(\mathcal{S}_w)$, e E_ρ o evento de ruído baixo. Se definimos "jump" como o evento quando $\boldsymbol{x} \in T_i$ e $\hat{\boldsymbol{x}} \in T_j$, $i \neq j$ e "no jump" o seu complementar. O MSE pode ser limitado por

$$\begin{aligned}
&\frac{1}{k}E\left[\|\boldsymbol{x}-\hat{\boldsymbol{x}}\|_2^2\right] \leq \frac{1}{k}E\left[\|\boldsymbol{x}-\hat{\boldsymbol{x}}\|_2^2 \,|\, \|\boldsymbol{z}\|_2 < \rho, \text{“no jump”}\right] \\
&+ P(\text{“jump”} \,|\, \|\boldsymbol{z}\|_2 \leq \rho) + P(\|\boldsymbol{z}\|_2 > \rho) = \\
&\frac{1}{k(1-\varepsilon)^2}E\left[\|\boldsymbol{x}_2-\hat{\boldsymbol{x}}_2\|_2^2 \,|\, \|\boldsymbol{z}\|_2 < \rho, \text{“no jump”}\right] \\
&+ P(\text{“jump”} \,|\, \|\boldsymbol{z}\|_2 \leq \rho) + P(\|\boldsymbol{z}\|_2 > \rho)
\end{aligned}$$

Se o ruído for menor que a distância entre os segmentos da imagem de $\boldsymbol{s}(\boldsymbol{x})$, então $\hat{\boldsymbol{x}}_{\boldsymbol{2}}$ será dado pela projeção no segmento correto. Neste caso, o erro será $\hat{\boldsymbol{x}}_2 - \boldsymbol{x}_2 = Q_w \boldsymbol{z}/(\alpha\beta_w^2) = \boldsymbol{z}' \sim \mathcal{N}(0, \sigma^2/\alpha\beta_w I_k)$. Suponhamos agora que o vetor de translação $\boldsymbol{t}_i$ e o fator ε foram escolhidos de tal maneira que cada peça está separada pelo menos d dos seus vizinhos. Um salto ocorrerá se a projeção de $\boldsymbol{z}'$ ortogonal ao plano que determina um corte tiver norma maior que d. Como a projeção de uma variável normal é também uma variável normal, pode-se mostrar que $P(\hat{\boldsymbol{x}} \in T_j | \boldsymbol{x} \in T_i) \leq Q(d\alpha\beta_w/\sigma)$, onde $Q(x)$ é a mesma função utilizada no Apêndice A, que denota a "cauda" de uma distribuição normal, isto é

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-x^2/2} \mathrm{dx}.$$

Proposição 5.3.4. *Se cada peça $\tilde{T}_i$ da dissecção possui no máximo r vizinhos, então:*

$$P(\text{"jump"} \,|\, \|\boldsymbol{z}\|_2 < \rho) \leq rQ(d\alpha\beta/\sigma). \tag{5.19}$$

O número de vizinhos pode ser subsequentemente limitado pelo número total de peças da dissecção, menos um. Portanto, se escolhermos ε de modo que $\varepsilon \to 0$ e $d\alpha\beta_w$ cresce com ordem pelo menos P^μ, para algum $\mu > 0$, os eventos "jump" terão probabilidade exponencialmente pequena e essencialmente a mesma análise assintótica valerá para $\boldsymbol{s}$ e $\boldsymbol{s}_Q$. O objetivo da próxima seção é mostrar que a dissecção de Montucla do quadrado para o cubo, junto com uma aplicação mod-1 conveniente, satisfazem estes requisitos. O mapa alternativo $\boldsymbol{s}_Q$ pode ser visto como um esquema de comunicação modificado, conforme a Figura 5.8.

5.3.3 Construção $2 : n$

Seja aplicação mod-1 com matrizes A_w descritas no Exemplo 5.2.6, a qual não possui expoente ótimo para $n = 2m + 1$. Mostramos que a aplicação mod-1

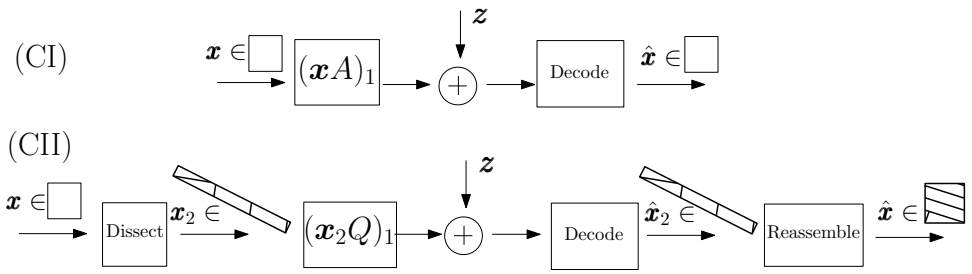


Figura 5.8: Esquemas de comunicação

modificada, junto com a dissecção de Montucla, podem "corrigir" o expoente do MSE de tal modo a atingir o decaimento ótimo $P^{-n/2}$.

No caso ímpar $n = 2m + 1$, as matrizes A_w são dadas por

$$A_w \begin{pmatrix} 1 & 0 & w & \dots & 0 & w^m \\ 0 & 1 & 0 & \dots & w^{m-1} & 0 \end{pmatrix}$$

Notemos primeiro que, do exemplo, temos $\det(A_w A_w^t) = \Theta(w^{4m-2})$. Usando a notação da subseção anterior, podemos escrever $A_w = R_w Q_w$, onde Q_w é uma matriz de ordem $2 \times n$ cujas linhas são ortogonais e R_w é uma matriz diagonal com determinante 1,

$$R_w = \begin{pmatrix} l_w & 0 \\ 0 & 1/l_w \end{pmatrix},$$

com $l_w = \Theta(\sqrt{w})$. Além disso, $\beta_w = \Theta(w^{m-1/2})$. Da análise do MSE, temos que se escolhermos $P = \Theta(\det(A_w A_w^t)^{1/(n-2)+\mu}) = \Theta(w^{2+\mu(4m-2)})$, o evento de erros grandes E_ρ^c terá probabilidade exponencialmente baixa, e o MSE dados que não há erros grandes pode ser aproximado por

$$\begin{aligned} \text{MSE} &\approx \frac{\sigma^2}{\alpha^2 k} \int_{R_w[0,1)^2} \text{tr}((Q_w Q_w^t))^{-1} \mathrm{d}\boldsymbol{x} \\ &= \frac{n\sigma^2}{12 P \beta_w^2} = O\left(\frac{1}{P w^{2m-1}}\right) \approx O\left(P^{-\frac{n}{2}}\right). \end{aligned} \tag{5.20}$$

Portanto, a aplicação $s_Q(\boldsymbol{x})$ (modelo de comunicação CII, após dissecarmos a

fonte e antes de reagruparmos as peças) possui expoente ótimo para uma fonte com distribuição no retângulo.

Para a etapa de dissecção, utilizamos a dissecção de Montucla. Note que para cortar o retângulo, utilizamos $M-2$ cortes verticais e 1 corte horizontal, onde $M \leq \lceil l \rceil + 2$ é o número de peças da dissecção (ver Figura 5.7(b)). Está claro que podemos separar os semi-planos correspondentes aos cortes verticais transladando um dos vértices da peça para o orgiem, aplicando um fator de escala $(1-\varepsilon)$, e então transladando-o de volta para a posição original do vértice. Neste caso, cada peça está a uma distância $d = \dfrac{\varepsilon}{2}$ dos seus vizinhos. O triângulo provido pelo único corte horizontal pode ser transladado tal que o vértice correspondente ao lado do retângulo seja levado na origem, escalado, e então transladado de volta, dando-nos uma distância até os seus vizinhos $\bar{d} \approx \varepsilon / l_w \leq d$. Portanto, se escolhermos $\varepsilon = \Theta(w^{-m+\mu})$, da Proposição 5.3.4, os "saltos" entre peças diferentes na fase de reagrupamento terão probabilidade exponencialmente pequena, e $\varepsilon \to 0$ quando $w \to \infty$.

Em suma, como todas as peças possuem no máximo $r = 3$ vizinhos e cada uma delas está separada de uma distância pelo menos $\bar{d}$, temos:

$$\begin{aligned} \text{MSE} \leq \frac{1}{k(1-\varepsilon)^2} \overbrace{E[\|\boldsymbol{x_2} - \hat{\boldsymbol{x}}_{\boldsymbol{2}}\|_2^2 \,|\, \text{“no jump”}, \|\boldsymbol{z}\|_2 \leq \rho]}^{O(P^{-n/2}) \text{ de (5.20)}} + \\ + \underbrace{P(\|z\|_2 \geq \rho)}_{\substack{\text{exponencialmente pequeno} \\ \text{de (5.14)}}} + \underbrace{P(\text{“jump”} \,||\, \|\boldsymbol{z}\|_2 < \rho)}_{\substack{\text{exponencialmente pequeno} \\ \text{da Proposição 5.3.4}}} = O(P^{-n/2}). \end{aligned} \tag{5.21}$$

Isso nos mostra que o MSE possui expoente ótimo.

5.4 Extensões e Referências Futuras

Nas seções anteriores mostramos como utilizar a dissecção de Montucla para obter códigos com expoente ótimo para fontes uniformes bi-dimensionais. Como vimos, a dissecção de Montucla é uma manifestação do Teorema dos Dois Ladrilhos 5.3.1. Através dessa caracterização, podemos generalizar a dissecção para qualquer hipercubo e qualquer hiperretângulo de mesmo volume em $\mathbb{R}^n$, conforme mostrado a seguir.

Seja L uma matriz de ordem $n \times n$ triangular *inferior*, tal que $L_{ii} = 1$. Utilizando argumentos como na Prop. 5.3.3 não é difícil mostrar que o cubo $[0,1)^n$ é um $\Lambda(L)$-ladrilho para $\mathbb{R}^n$. Também pode-se mostrar que se U é triangular *superior* com $U_{ii} = 1$, então o parallelogramo $\mathcal{R} = \{UL\boldsymbol{x} : \boldsymbol{x} \in [0,1)^n\}$ é um $\Lambda(L)$-ladrilho para $\mathbb{R}^n$. Considere agora os vetores ortogonalizados pelo processo Gram-Schmidt aplicado às linhas de L, i.e.,

$$\boldsymbol{r}_n = \boldsymbol{l}_n$$

$$\boldsymbol{r}_i = \boldsymbol{l}_i - \sum_{j=i+1}^{n} \frac{\langle \boldsymbol{l}_i, \boldsymbol{r}_j \rangle}{\langle \boldsymbol{r}_j, \boldsymbol{r}_j \rangle} \boldsymbol{r}_j, \text{ for } i = n-1, \ldots, 1.$$

Tomando U como a matriz que ortogonaliza $\boldsymbol{l}_1, \ldots, \boldsymbol{l}_n$, vemos que, pelo teorema dos dois ladrilhos, o hiperretângulo $\{\alpha_1 \boldsymbol{r}_1 + \ldots + \alpha_n \boldsymbol{r}_n : 0 \leq \alpha_i < 1\}$ é um $\Lambda(L)$-ladrilho para $\mathbb{R}^n$, e portanto é equidissecável com o o cubo $[0,1)^n$. Basta mostrar que *qualquer* hiperretângulo pode ser produzido através deste processo para uma matriz L convenientemente escolhida. Seja um retângulo de lados $a_1 \times a_2 \ldots \times a_n$. Ademais, suponhamos que $a_1 \leq a_2 \leq \ldots \leq a_n$ (o que pode ser obtido por uma transformação ortogonal), e $a_1 \times a_2 \times \ldots a_n = 1$. Considere a matriz dada por

$$L_{ij} = \begin{cases} 1 & \text{if } i = j \\ \dfrac{\sqrt{\prod_{k=j}^{n} a_k^2 - 1}}{\prod_{k=j+1}^{n} a_k} & \text{if } i = j+1 \\ 0 & \text{caso contrário} \end{cases} \tag{5.22}$$

Aplicando ortogonalização de Gram-Schmidt nas linhas de L, a começar pela última, produziremos vetores ortogonais tais que $\|\boldsymbol{r}_i\|_2 = a_i$. Assim, a realização do retângulo de lados $a_1 \leq a_2 \leq \ldots \leq a_n$ ao longo desses vetores, bem como o cubo $[0,1)^n$ são $\Lambda(L)$-ladrilhos para $\mathbb{R}^n$, e deste modo, pelo Teorema 5.3.1, são equidissecáveis. Por exemplo, no $\mathbb{R}^4$, podemos dissecar um hipercubo e um hiperretângulo de lados $a_1 \times a_2 \times a_3 \times a_4$ através do Teorema dos Dois Ladrilhos utilizando o reticulado gerado por

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \dfrac{\sqrt{a_2^2 a_3^2 a_4^2 - 1}}{a_3 a_4} & 1 & 0 & 0 \\ 0 & \dfrac{\sqrt{a_3^2 a_4^2 - 1}}{a_4} & 1 & 0 \\ 0 & 0 & \sqrt{a_4^2 - 1} & 1 \end{pmatrix}. \tag{5.23}$$

A utilização dessa dissecção para o desenvolvimento de códigos analógicos com expoente ótimo para fontes com dimensão k arbitrária é deixada para investigação futura.

Capítulo 6

Conclusões e Perspectivas Futuras

He took his time coming over. "You boys going to get somewhere, or just going?" We didn't understand his question, and it was a damned good question.

- Jack Kerouac, *On the Road*

Abaixo resumimos brevemente os resultados apresentados e listamos algumas perspectivas futuras.

No Capítulo 2, estudamos a classe de reticulados q-ários, mostrando algumas relações entre algoritmos de decodificação para reticulados e códigos corretores de erros q-ários. Analisamos a estrutura combinatória de códigos perfeitos associados a reticulados na norma l_p. Mostramos uma completa caracterização de códigos perfeitos no caso $p = \infty$ e teoremas acerca da impossibilidade/possibilidade de existência de tais códigos para alguns parâmetros de raio de empacotamento e dimensão. O problema geral de determinar quais parâmetros admitem códigos perfeitos na norma l_p (e efetivamente encontrá-los) está longe de ser completamente resolvido. Uma solução geral para as normas l_p implicaria uma prova ou contra-exemplo para a Conjectura de Golomb-Welch [GW70] sobre códigos perfeitos na métrica de Lee (ou l_1), em aberto por cerca de 45 anos. É natural, portanto, investigar se o estudo de métricas l_p de maneira geral nos dá alguma informação adicional para a compreensão da conjectura. Além disso, códigos na

métrica 2-Lee considerada no Capítulo 2 possuem potenciais aplicações em teoria da informação [FSK13] e na construção de códigos esféricos [SB13]. É possível encontrar códigos perfeitos na métrica 2-Lee que não sejam os triviais nem os herdados da métrica de Lee?

No Capítulo 3 consideramos projeções de reticulados. Apresentamos sequências de projeções do reticulado cúbico $\mathbb{Z}^n$ com boa taxa de convergência, as quais podem ser aplicadas à construção de códigos analógicos. Mostramos também um resultado geral acerca de projeções de qualquer reticulado n-dimensional convergindo para qualquer reticulado k-dimensional pré-fixado. Uma boa perspectiva de pesquisa futura é a utilização da estrutura de projeções para abordar dois problemas centrais da teoria: desenvolver algoritmos aproximados de decodificação de reticulados e encontrar o empacotamento de esfera mais denso. Com relação ao primeiro, ideias iniciais podem ser encontradas em [VC03] e [Str07], onde algoritmos de decodificação para projeções de $\mathbb{Z}^n$ dependem da norma do vetor ao longo do qual se está projetando. No que tange ao problema de empacotamentos gerais, podemos estudar como obter sequências de projeções com boas densidades quando não sabemos qual o reticulado mais denso, a priori.

Nos capítulos finais 4 e 5 desenvolvemos códigos analógicos para transmitir uma variável contínua através de um canal gaussiano no regime de expansão de largura de banda. Através de ferramentas matemáticas como a folheação da esfera por toros planares, e as projeções de reticulados, mostramos garantias para o desempenho dos códigos desenvolvidos que aprimoram significativamente as propostas anteriores na literatura. Nossas análises consideram que há um receptor e um transmissor. Uma direção de pesquisa futura é analisar como se comporta o problema de empacotamento de curvas no caso de canais com mais do que um usuário (receptor ou transmissor), tema de bastante interesse da comunidade de Teoria da Informação na atualidade. Canais famosos incluem os canais de *broadcast* e de múltiplo acesso. O artigo [FKW$^+$12] apresenta um estudo preliminar nesta direção para o canal de múltiplo acesso.

Em suma, de uma maneira bastante abrangente, nosso interesse para direções

futuras de pesquisa está na aplicação de estruturas de Matemática Discreta (e em particular Geometria Discreta) em ambientes com potencial aplicação a telecomunicações. Uma outra vertente de trabalho, cujo desenvolvimento foi feito em paralelo com os temas considerados aqui, é a aplicação de técnicas de geometria poliedral (cálculo de volume de regiões determinadas por desigualdades) ao cálculo de probabilidade de erro de sistemas de armazenamento de informação em [CV13], assuntoq ue não está no escopo e nos objetivos desta tese. Deixamos a realização de uma versão estendida de [CV13] como trabalho futuro.

Apêndice A

Este apêndice é devotado à demonstração do Teorema 4.3.2. Temos os seguintes lemas técnicos

Lema A.0.1. *Considere uma família de aplicações dadas pela Equação* (4.17)*, normalizada de modo a ter potência média P. Suponha que à medida que o raio de empacotamento $\rho \to 0$, o comprimento total e o raio de empacotamento da família satisfaça $L = \Theta(\rho^{-(k-1)})$ para algum $k > 1$. Para qualquer $\mu > 0$ arbitrariamente pequeno, existe uma escolha de parâmetros tal que o* MSE *decai com ordem $O(P^{-k+\mu})$.*

Demonstração. A demonstração é uma aplicação da recente técnica [TK12, Appendix A], que descrevemos brevemente por razão de completude. Denotemos $P(\text{“jump”})$ a probabilidade de que a estimativa $\hat{x}$ seja decodificada na “volta” incorreta da curva. Isto ocorrerá se o ruído for maior que o raio de empacotamento ρ da curva, e portanto podemos limitar esta probabilidade por $Q(\sqrt{P}\rho/\sigma)$, onde $Q(x)$ denota a função Q:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-x^2/2} \mathrm{dx}.$$

Por outro lado, se estimativa $\hat{x}$ e o valor enviado x estiverem na mesma “volta” da curva, então fazendo a projeção do vetor recebido $\boldsymbol{y}$ no local geométrico, temos que o MSE é proporcional a $\sigma^2/\alpha^2 L^2$, onde L é o comprimento total e $\alpha = \sqrt{P}$. Dado P escolhemos nossas curvas de modo que o raio de empacotamento

ρ satisfaça $\rho = \Theta(P^{-1/2+\bar{\mu}})$, para algum $\bar{\mu} > 0$ arbitrariamente pequeno (isto pode ser feito, por exemplo, crescendo a norma do vetor projeção suficientemente). Assim, tomando $\bar{\mu} = \mu/(2k-2)$, temos que $\sqrt{P}\rho = \Theta(P^{\bar{\mu}})$ de onde segue que

$$\begin{aligned}
\text{MSE} &= E[(x-\hat{x})^2|\text{“no jump”}]P(\text{“no jump”}) + E[(x-\hat{x})^2|\text{“jump”}]P(\text{“jump”}) \\
&\leq E[(x-\hat{x})^2|\text{“no jump”}] + P(\text{”jump”}) \\
&\leq \underbrace{\frac{\sigma^2}{PL^2}}_{O(P^{-k+\mu})} + \underbrace{Q\left(\frac{\sqrt{P}\rho}{\sigma}\right)}_{\text{exponencialmente pequeno}},
\end{aligned} \tag{A.1}$$

e isso conclui a prova. □

Lema A.0.2. *Para $\rho > 0$ suficientemente pequeno e $\mu > 0$, existe um código esférico $SC_+ = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\} \subset S^{n-1}$ com distância mínima 2ρ satisfazendo:*

$$\sum_{i=1}^{M}\prod_{j=1}^{n} c_{ij} = \Theta(\rho^{-(n-1)+\mu}), \tag{A.2}$$

onde c_{ij} denota a j-ésima coordenada do vetor $\boldsymbol{c}_i$.

Demonstração. Do Limitante de Chabauty-Shannon-Wyner [EZ01, Thm. 1.6.2], aplicado ao octante positivo de S^{n-1}, existe um código esférico com distância mínima 2ρ e cardinalidade $M = |SC_+| = \Theta(\rho^{-(n-1)})$. Denotemos agora por SC_+^{ε} o subcódigo de SC_+ tal que $c_{ij} > \varepsilon$ para algum $\varepsilon > 0$. Temos

$$\sum_{i=1}^{M}\prod_{j=1}^{n} c_{ij} \geq \sum_{\boldsymbol{c}_i \in SC_+^{\varepsilon}}\prod_{j=1}^{n} c_{ij} \geq \varepsilon^n |SC_+^{\varepsilon}|.$$

À medida que $\varepsilon \to 0$, $|SC_+^{\varepsilon}| \to |SC_+| = \Theta(\rho^{-(n-1)})$, entretanto, se ε tender a zero muito rapidamente com respeito à distância mínima ρ, podemos estar deletando muitas coordenadas para construir SC_+^{ε}, e portanto não atingiremos o expoente

desejado. A escolha $\varepsilon = \rho^{\mu/n}$ para $\mu > 0$ arbitrariamente pequeno resolve este problema. □

Demonstração do Teorema 4.3.2: Se o código esférico $SC_+ = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\}$ possui M palavras e distância mínima 2ρ suficientemente pequena, é possível achar vetores projeção $\boldsymbol{v}_i$ tais que suas normas estão arbitrariamente próximas ao Limitante (4.14). Assim, para algum $\varepsilon > 0$, o comprimento total do Esquema de Camadas de Toros será

$$L = \sum_{i=1}^{M} 2\pi \|\boldsymbol{v}_i\| = \frac{(2\pi)^n}{\rho^{n-1}} \sum_{i=1}^{M} \prod_{j=1}^{n} c_{ij} \left(\delta_{n-1} - \varepsilon\right). \tag{A.3}$$

Desconsiderando o termo dentro da soma do produto, portanto, o comprimento iria crescer com ordem $\rho^{-(n-1)}$. Do Lemma A.0.2, podemos escolher $\boldsymbol{c}_i$ de forma que a soma do produto tenha ordem $\Theta(\rho^{-(n-1)})$, portanto, no total, teremos $L = \Theta(\rho^{-(2n-2)})$, e do Lema A.0.1 o resultado segue.

Referências Bibliográficas

[AEVZ02] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger. Closest point search in lattices. *IEEE Transactions on Information Theory,*, 48(8):2201–2214, 2002.

[AIPJ03] A.A. Andrade, J.C. Interlando, and R. Palazzo Jr. Alternant and BCH codes over certain rings. *Computational & Applied Mathematics*, 22:233 – 247, 00 2003.

[ATB13] J. Almeida, C. Torezzan, and J. Barros. Spherical codes for the Gaussian wiretap channel with continuous input alphabets. In *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 664–668, 2013.

[BBD08] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2008.

[BN10] K. Bhattad and K.R. Narayanan. A Note on the Rate of Decay of Mean-Squared Error With SNR for the AWGN Channel. *IEEE Transactions on Information Theory*, 56(1):332–335, 2010.

[BVRB96] J. Boutros, E. Viterbo, C. Rattelo, and J. C. Belfiore. Good Lattice Codes for Both Rayleigh and Gaussian Channels. *IEEE Transactions on Information Theory*, 42:502–517, 1996.

[Cas97] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1997.

[CE03] Henry Cohn and Noam Elkies. New Upper Bounds on Sphere Packings I. *The Annals of Mathematics*, 157(2):pp. 689–714, 2003.

[Chu00] S. Chung. *On the construction of some capacity-approaching coding schemes*. Ph.D. dissertation, Massachusetts Institute of Technology, 2000.

[CJC11] A. Campello, G. Jorge, and S. I R Costa. Decoding q-ary lattices in the Lee metric. In *IEEE Information Theory Workshop (ITW)*, pages 220–224, 2011.

[CS98] J. H. Conway and N. J. A. Sloane. *Sphere-packings, lattices, and groups*. Springer-Verlag, New York, NY, USA, 1998.

[CS13] A. Campello and J. Strapasson. On sequences of projections of the cubic lattice. *Computational and Applied Mathematics*, 32(1):57–69, 2013.

[CSC13] A. Campello, J. Strapasson, and S. I. R. Costa. On projections of arbitrary lattices. *Linear Algebra and its Applications*, 439(9):2577 – 2583, 2013.

[CSV13] J. Chen, D. Stehlé, and G. Villard. A New View on HJLS and PSLQ: Sums and Projections of Lattices. In *Proceedings of the 38th International Symposium on International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, pages 149–156, New York, NY, USA, 2013. ACM.

[CT06] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2 edition, 2006.

[CTC12] A. Campello, C. Torezzan, and S. I R Costa. Curves on Torus Layers and Coding for Continuous Alphabet Sources. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 2127–2131, 2012.

[CTC13] A. Campello, C. Torezzan, and S.I.R. Costa. Curves on Flat Tori and Analog Source-Channel Codes. *IEEE Transactions on Information Theory*, 59(10):6646–6654, 2013.

[CV13] A. Campello and V. A Vaishampayan. Reliability of Erasure Coded Storage Systems: A Geometric Approach. In *IEEE International Conference on BigData*, 2013.

[CVC13] A. Campello, V. A. Vaishampayan, and S. I . R. Costa. Projections, Dissections and Bandwidth Expansion Mappings. In *IEEE Information Theory Workshop (ITW)*, 2013.

[dB81] N. G. de Bruijn. Algebraic theory of Penrose's non-periodic tilings of the plane I, II. *Indagationes mathematicae*, 43(1):39–66, 1981.

[Etz11] T. Etzion. Product Constructions for Perfect Lee Codes. *Information Theory, IEEE Transactions on*, 57(11):7473–7481, 2011.

[EZ01] T Ericson and V Zinoviev. *Codes on Euclidean Spheres*. North-Holland Mathematical Library, 2001.

[FKW+12] P.A. Floor, A.N. Kim, N. Wernersson, T.A. Ramstad, M. Skoglund, and I. Balasingham. Zero-Delay Joint Source-Channel Coding for a Bivariate Gaussian on a Gaussian MAC. *IEEE Transactions on Communications*, 60(10):3091–3102, 2012.

[Fre03] G. N. Frederickson. *Dissections: Plane and Fancy*. Cambridge University Press, 2003.

[FSK13] Chen Feng, D. Silva, and F.R. Kschischang. An Algebraic Approach to Physical-Layer Network Coding. *IEEE Transactions on Information Theory*, 59(11):7576–7596, 2013.

[GL87] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland, 1987.

[Gob65] T. J. Goblick. Theoretical limitations on the transmission of data from analog sources. *IEEE Transactions on Information Theory*, 11(4):558–567, 1965.

[GW70] S.W. Golomb and L. R. Welch. Perfect Codes in the Lee Metric and the Packing of Polyominoes. *SIAM Journal on Applied Mathematics*, 18(2):302–317, 1970.

[Hal05] T. C. Hales. A proof of the Kepler conjecture. *Annals of Mathematics*, 162(3):1065–1185, 2005.

[HG14] Peter Horak and Otokar Grosek. A new approach towards the Golomb-Welch conjecture. *European Journal of Combinatorics*, 38(0):12 – 22, 2014.

[HP03] W. Cary Huffman and Vera Pless. *Fundamentals of Error Correcting Codes*. Cambridge University Press, Cambridge, U.K., 2003.

[HZ97] J. Hamkins and K. Zeger. Asymptotically dense spherical codes. I. Wrapped spherical codes. *IEEE Transactions on Information Theory*, 43(6):1774–1785, Nov. 1997.

[ILZF08] A. Ingber, I. Leibowitz, R. Zamir, and M. Feder. Distortion lower bounds for finite dimensional joint source-channel coding. In *IEEE International Symposium on Information Theory*, pages 1183–1187, 2008.

[JB10] A. Jiang and J. Bruck. Data representation for flash memories. *Data Storage, In-Tech Publisher*, 2010.

[JCC13] G. C. Jorge, A. Campello, and S. I. R. Costa. q-ary lattices in the l_p norm and a generalization of the Lee metric. In *Workshop on Coding and Cryptography (WCC), Bergen, Norway*, 2013.

[KR10] M. Kleiner and B. Rimoldi. A tight bound on the performance of a minimal-delay joint source-channel coding scheme. In *IEEE Interna-*

tional Symposium on Information Theory Proceedings (ISIT), pages 136–140, 2010.

[Lag75] J.L. Lagrange. *Recherches d'arithmétique*. C.F. Voss, 1775.

[Lee58] C. Lee. Some properties of nonbinary error-correcting codes. *IRE Transactions on Information Theory*, 4(2):77–82, 1958.

[Mar03] J. Martinet. *Perfect Lattices in Euclidean Space*. Springer-Verlag, Berlin Heidelberg New York, 2003.

[McK10] R. McKilliam. *Lattice Theory, Circual Statistics and Polynomial Phase Signals*. Tese de Doutorado, The University of Queensland, 2010.

[Mey00] C. D. Meyer. *Matrix Analysis and Applied Linear Algebra*. Society for Industrial Mathematics (SIAM), Philadelphia PA, USA, 2000.

[MG02] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*. Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

[Min04] H. Minkowski. Dichteste gitterförmige Lagerung kongruenter Körper. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, pages 311–355, 1904.

[MSVC12] R. G. McKilliam, R. Subramanian, E. Viterbo, and I. V. L. Clarkson. On the Error Performance of the A_n Lattices. *IEEE Transactions on Information Theory,*, 58(9):5941–5949, 2012.

[Pei08] Chris Peikert. Limits on the Hardness of Lattice Problems in l_p Norms. *computational complexity*, 17(2):300–351, 2008.

[Pen74] R. Penrose. The role of aesthetics in pure and applied mathematical research. *Bulletin of the Institute of Mathematics and its Applications*, 20(718):266–271, 1974.

[Rog64] C. A. Rogers. *Packing and Covering*. Cambridge University Press, March 1964.

[RS87] J. A. Rush and N. J. A. Sloane. An improvement to the Minkowski-Hlawka bound for packing superballs. *Mathematikal*, 34:8–18, 1987.

[Sak70] D. J. Sakrison. *Notes on analog communications*. New York: Van Nostrand Reinhold, 1970.

[SB13] P. Solé and J.-C. Belfiore. Constructive spherical codes near the Shannon bound. *Designs, Codes and Cryptography*, 66(1-3):17–26, 2013.

[SC08] R. M. Siqueira and S. I. R. Costa. Flat tori, lattices and bounds for commutative group codes. *Codes, Designs and Cryptography*, 20:76–91, 2008.

[Sha48] C. E. Shannon. A Mathematical Theory of Communication. *The Bell system technical journal*, 27:379–423, 1948.

[Sha49] C.E. Shannon. Communication in the Presence of Noise. *Proceedings of the IRE*, 37(1):10–21, 1949.

[SM77] N.J.A. Sloane and F.J. MacWilliams. *The Theory of Error-Correcting Codes*. North Holland, 1977.

[Spi71] M. Spivak. *Calculus on Manifolds: A modern approach to classical theorems of advanced calculus*. Westview Press, New York, NY, 1971.

[Str07] J. E. Strapasson. *Geometria Discreta e Códigos*. Tese de Doutorado, Universidade Estadual de Campinas, 2007.

[SV03] N. Santhi and A. Vardy. Analog codes on graphs. In *IEEE International Symposium on Information Theory*, pages 13–, 2003.

[SV09] N. J. A. Sloane and V. A. Vaishampayan. Generalizations of Schöbi's Tetrahedral Dissection. *Discrete & Computational Geometry*, 41(2):232–248, 2009.

[SVC09] N. J. A. Sloane, V. Vaishampayan, and S. I. R. Costa. Fat struts: Constructions and a bound. In *IEEE Information Theory Workshop (ITW)*, pages 333–337, 2009.

[SVC10] N. J. A. Sloane, V. A. Vaishampayan, and S. I. R. Costa. The lifting construction: A general solution for the fat strut problem. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 1037 –1041, 2010.

[SVC11] N. J. A. Sloane, V. Vaishampayan, and S. I. R. Costa. A Note on Projecting the Cubic Lattice. *Discrete and Computational Geometry*, 46:472–478, 2011.

[TCV09] C. Torezzan, S. I. R Costa, and V. Vaishampayan. Spherical codes on torus layers. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 2033–2037, 2009.

[TK12] M. Taherzadeh and A.K. Khandani. Single-Sample Robust Joint Source-Channel Coding: Achieving Asymptotically Optimum Scaling of SDR Versus SNR. *IEEE Transactions Information Theory*, 58(3):1565–1577, 2012.

[TMZ13] R.M. Taylor, L. Mili, and A. Zaghloul. Packing tubes on tori: An efficient method for low snr analog error correction. In *Information Theory Workshop (ITW), 2013 IEEE*, pages 1–5, Sept 2013.

[Tor09] C. Torezzan. *Códigos esféricos em toros planares*. Tese de Doutorado, Universidade Estadual de Campinas, 2009.

[TYK10] K. Takizawa, H. Yagi, and T. Kawabata. Closest point algorithms with lp norm for root lattices. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1042–1046, June 2010.

[VC03] V. A. Vaishampayan and S. I. R. Costa. Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. *IEEE Transactions on Information Theory*, 49:1658–1672, 2003.

[VL75] J. H. Van Lint. A survey of perfect codes. *Rocky Mountain J. Math*, 5:199–224, 1975.

[WSR09] N. Wernersson, M. Skoglund, and T. Ramstad. Polynomial based analog source-channel codes. *IEEE Transactions on Communications*, 57(9):2600 –2606, 2009.

[Zam09] R. Zamir. Lattices are everywhere. In *Information Theory and Applications Workshop*, pages 392 –421, 2009.

Índice Remissivo