



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



Códigos esféricos em toros planares

Cristiano Torezzan

torezzan@gmail.com

Tese de Doutorado

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

Co-orientador: **Prof. Dr. José Plínio de Oliveira Santos**

Junho de 2009

Campinas - SP

Este trabalho contou com apoio financeiro da FAPESP - processo 05/58102-7.


Códigos esféricos em camadas de toros

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Cristiano Torezzan** e aprovada pela comissão julgadora.

Campinas, agosto de 2009.



Profa. Dra. Sueli Irene Rodrigues Costa
Orientadora



Prof. Dr. José Plínio de O. Santos
Co-orientador

Banca Examinadora:

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

Prof. Dr. José Mario Martinez (IMECC - UNICAMP)

Prof. Dr. Reginaldo Palazzo Junior (FEEC - UNICAMP)

Prof. Dr. Vilmar Trevisan (DMPA - UFRGS)

Prof. Dr. Weiler Alves Finamore (CETUC - PUC RJ)

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

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

Bibliotecária: Crislene Queiroz Custódio – CRB8 / 7966

Torezzan, Cristiano

T631c Códigos esféricos em toros planares / Cristiano Torezzan -- Campinas,
[S.P. : s.n.], 2009.

Orientador : Sueli Irene Rodrigues Costa

Co-orientador: José Plínio de Oliveira Santos

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

1. Empacotamento de esferas. 2. Teoria da codificação. 3. Teoria dos
reticulados. 4. Geometria discreta. 5. Grupos abelianos. 6. Otimização. I.
Costa, Sueli Irene Rodrigues. II. Santos, José Plínio de Oliveira. III.
Universidade Estadual de Campinas. Instituto de Matemática, Estatística e
Computação Científica. IV. Título.

Título em inglês: Spherical codes on flat torus

Palavras-chave em inglês (Keywords): 1. Sphere packings. 2. Codification theory. 3. Lattice theory. 4. Discrete
geometry. 5. Abelian groups. 6. Optimization.

Área de concentração: Matemática Aplicada

Titulação: Doutor em Matemática Aplicada

Banca examinadora: Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)
Prof. Dr. José Mario Martinez (IMECC-UNICAMP)
Prof. Dr. Reginaldo Palazzo Junior (FEEC-UNICAMP)
Profa. Dra. Vilmar Trevisan (UFRGS)
Prof. Dr. Weiler Alves Finamore (PUC-RJ)

Data da defesa: 21/07/2009

Programa de Pós-Graduação: Doutorado em Matemática Aplicada

Tese de Doutorado defendida em 21 de julho de 2009 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.



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



Prof(a). Dr(a). JOSÉ MARIO MARTÍNEZ PÉREZ



Prof(a). Dr(a). REGINALDO PALAZZO JUNIOR



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



Prof(a). Dr(a). WEILER ALVES FINAMORE

A meu pai Jaci Antonio Torezzan

in memoriam.

Dedico.

Agradecimentos

Embora a solidão seja uma companheira inevitável de um estudante, não se termina um doutorado sozinho. Não se chega a um doutorado sozinho. Muitas pessoas me ajudaram a chegar aqui, outras a concluir o curso. Devo muito a elas, muito mais que esse modesto tributo. Quero dizer a todos que, em cada palavra, vai um abraço de gratidão.

Gostaria de fazer algumas menções especiais de agradecimento à:

Minha mãe, Lúcia, a senhora me possibilitou chegar até aqui. Seu incentivo constante, seus cuidados e esforços incansáveis para nos dar educação, desde o berço, venceram todas as dificuldades do trajeto e nos fizeram acreditar que esta seria *o* caminho.

Minha esposa Gláucia. Não teria conseguido terminar este projeto sem teu apoio e seu entusiasmo contantes. Você é meu ponto de equilíbrio. Este doutorado é compartilhado contigo.

Não há como exagerar a contribuição de minha orientadora Sueli I. R. Costa. O que você me ensinou está muito além do que pode ser escrito numa tese de matemática. Como uma maneira de lhe retribuir, tentarei repetir seus gestos durante minha carreira. Você é um exemplo para todos os que passam pelo *laboratório*.

Toda minha família, em especial meus irmãos Daniela, Fernando e Eduardo. Tenho comigo muito mais de vocês do que possam imaginar.

João E. Strapasson, meu companheiro de pesquisa, que colaborou durante toda a realização deste trabalho.

Rogério M. Siqueira, quem me apresentou os códigos esféricos e me fez as perguntas iniciais sobre o tema.

Todos os colegas de doutorado, pela convivência, pelas conversas no café, pelos debates, produtivos ou fúteis. Vocês dão sentido à frase “não se termina um doutorado

sozinho”. Uma menção especial, aos do dia-a-dia: Alan, Agnaldo, Andréia, Carina, Felipe, Grasielle, João Paulo, Mael, Nolmar, Rosane, Tatiana.

Professor Nelo Alan, que me ajudou no preparo para um curso de pós-graduação em matemática e disponibilizou sua casa para que morássemos durante o primeiro semestre do doutorado.

Instituto de Matemática, Estatística e Computação Científica da Unicamp, seus professores e funcionários. Em especial aos professores José Plínio de O. Santos - meu co-orientador, Aurélio R. L. Oliveira, Carlile C. Lavor, Marcelo Firer, Sandra A. Santos. Sinto-me honrado em dizer que estudei *aqui*.

Aos membros da banca, por várias sugestões pertinentes que tornaram melhor a versão final deste trabalho.

Todos os meus professores, desde a infância, e meus alunos. Obrigado pelos ensinamentos, trago um pouco de cada um de vocês.

AT&T Shannon Laboratory, pela oportunidade de estudar no exterior. Em especial ao Dr. Vinay Vaishampayan e ao Dr. Neil A. J. Sloane, pelas frutíferas conversas sobre códigos e reticulados.

A Fapesp, pelo imprescindível apoio financeiro. Processos: 05/58102-7 e 07/00514-3.

Marcos, Rita, Alceu, Mazilio, Miguel, Zoraide, Argüello, Tulio, Edson, Ermerita (*in memoriam*), Carlão, Baju, Marcelão, representam uma lista enorme de amigos que infelizmente não posso citar por completo, vocês sabem quem são e eu não sei como lhes agradecer.

Resumo

Códigos esféricos em espaços euclidianos n -dimensionais são conjuntos finitos de pontos sobre superfícies esféricas e têm sido amplamente estudados em conexão com a transmissão de sinais sobre um canal Gaussiano. Para este propósito deseja-se maximizar a distância mínima entre dois pontos quaisquer do código, o que está fortemente relacionado com o problema mais geral do empacotamento em esferas, o qual contempla aplicações em outras áreas.

Na primeira parte deste trabalho estudamos códigos esféricos gerados como órbita de um vetor unitário sob a ação de um grupo comutativo de matrizes ortogonais, os denominados códigos de grupo comutativo. Propomos um método para obter o melhor código de grupo comutativo n -dimensional de ordem M , que baseia-se na associação entre tais códigos em dimensão $2k$ e reticulados k -dimensionais. Utilizando fatorações matriciais conhecidas, como as formas normais de Hermite e Smith, demonstramos que é possível reduzir o número de casos a serem analisados através da identificação de códigos isométricos que podem ser descartados. O problema da busca do vetor inicial ótimo para códigos de grupo comutativo é formalmente estabelecido com um problema de programação linear e utilizado em uma das etapas do método. Apresentamos resultados numéricos, incluindo tabelas com códigos de grupo comutativo ótimos em várias dimensões.

Outra contribuição deste trabalho é a introdução de uma nova família de códigos esféricos, na qual os pontos são alocados sobre a superfície da esfera unitária $2k$ -dimensional em camadas de toros planares. Em cada uma das camadas deste código, pode-se estabelecer um código de grupo para a geração dos sinais e utilizar os resultados acima mencionados. Além de limitantes, inferior e superior, para o número de pontos, um método para construção destes códigos é apresentado explicitamente e alguns exemplos são construídos. Os resultados mostram que tais códigos têm desempe-

nho comparável aos melhores códigos esféricos estruturados conhecidos, com destaque para uma potencial vantagem no processo de codificação/decodificação, decorrente da homogeneidade, estrutura de grupo e associação a reticulados na metade da dimensão.

Abstract

Spherical codes in Euclidean spaces are finite sets of points on the surface of a multidimensional sphere and have been widely studied in connection with the signal transmission over a Gaussian channel. For this purpose one fundamental issue is to maximize the minimum distance between two code points, what is strongly related to the more general problem of sphere packing.

In the first part of this work we study spherical codes generated as orbit of a initial vector under the action of a commutative group of orthogonal matrices, the so called commutative group codes. A method for searching the best n -dimensional commutative group code of order M is presented. Based on the well known Hermite and Smith normal form decomposition of matrices, and also on the relation between $2k$ -dimensional commutative group codes and k -dimensional lattices, we show that it is possible to reduce the number of cases to be analyzed through the identification of isometric codes which can be discarded. The initial vector problem for these codes is formally established as a linear programming problem and used as a sub-routine of the method. Numerical results are presented, including tables of good commutative groups codes in several dimensions.

Other contribution of this work is a new class of spherical codes, constructed by placing points on flat tori layers. The codebook on each torus can be generated by a commutative group of orthogonal matrices, using the results previously mentioned. Upper and lower bounds on performance are derived and a systematic method for constructing the codes is presented. Some examples are constructed and the results exhibit good performance when compared to the best known structured spherical codes, with some advantage in the encoding/decoding process, due to the homogeneity, group structure and the relation with lattices in the half of the dimension.

Sumário

Resumo	xi
Abstract	xiii
Introdução	1
1 Reticulados e códigos esféricos	13
1.1 Reticulados	13
1.1.1 Diagrama de treliça de reticulados	17
1.1.2 Alguns reticulados notáveis	21
1.1.3 Reticulados e empacotamentos esféricos	22
1.2 Construção de códigos esféricos	25
1.2.1 Limitantes superiores	26
1.2.2 Limitantes inferiores	31
1.2.3 Códigos esféricos obtidos via empacotamentos	31
1.2.4 Códigos esféricos obtidos de códigos binários	34
1.2.5 Códigos obtidos via métodos de otimização	35
1.3 Códigos esféricos com distâncias assintoticamente pequenas	37
1.3.1 Códigos esféricos <i>apple-peeling</i>	37
1.3.2 Códigos <i>wrapped</i>	39
1.3.3 Códigos esféricos laminados	42
2 Códigos de grupo comutativo	45
2.1 Códigos de grupo comutativo	46
2.2 Problema do vetor inicial em códigos de grupo comutativo	49
2.3 Códigos de grupo comutativo ótimos	51
2.4 Resultados computacionais	63

2.5	Códigos de grupo comutativo em dimensão ímpar	67
2.6	Decodificação em códigos de grupo comutativo	68
3	Códigos esféricos em camadas de toros	73
3.1	Toros planares	74
3.1.1	Distâncias em toros planares	76
3.2	Códigos esféricos em camadas de toros	78
3.2.1	A construção dos códigos esféricos em camadas de toros.	79
3.3	Limitantes para $\mathcal{C}_T(2k, d)$	80
3.3.1	Um limitante inferior para o número máximo de pontos	80
3.3.2	Um limitante superior	81
3.3.3	Códigos esféricos em camadas de toros nas dimensões ímpares	83
3.3.4	Densidade de um $\mathcal{C}_T(2k, d)$	83
3.4	Códigos esféricos quase comutativos	85
3.4.1	Códigos quase comutativos construídos a partir do reticulado A_2	87
3.4.2	Códigos esféricos quase cíclicos	92
3.4.3	Exemplo de um $\mathcal{C}_T(4, 0.3)$ quase cíclico	94
3.5	Decodificação de códigos esféricos em camadas de toros	97
	Considerações Finais e Perspectivas Futuras	101
	Referências Bibliográficas	105
A	Anexo1	111

Introdução

O assunto central desta tese é a construção de códigos esféricos. Um código esférico $\mathcal{C}(M, n)$ é um conjunto de M pontos sobre a superfície da esfera Euclidiana unitária n -dimensional $S^{n-1} \subset \mathbb{R}^n$, i.e.,

$$\mathcal{C}(M, n) = \{x_i \in S^{n-1} : \|x_i\| = 1, 1 \leq i \leq M\},$$

onde $\|x\|$, denota a norma Euclidiana de x .

O problema de alocar um conjunto finito de pontos sobre a superfície de uma esfera Euclidiana n -dimensional tem atraído a atenção de matemáticos, engenheiros e cientistas em geral, devido sua relevância em muitas áreas. As aplicações incluem desde transmissão de sinais [28, 32], quantização esférica [27], avaliação numérica de integrais sobre esferas [36], cálculo de distribuição de cargas de energia mínima sobre a esfera, aplicações em física, química [37], em arquitetura [54] e até aplicações inusitadas: a bola de golf, originalmente lisa, por razões aerodinâmicas recebeu pequenos círculos (em geral 336) correspondentes a um empacotamento sobre S^2 .



Figura 1: Uma bola de golf com 336 chapéus esféricos.

De modo geral, problemas envolvendo códigos esféricos buscam a melhor configuração de M pontos sobre S^{n-1} de modo a otimizar (maximizar ou minimizar) certos

parâmetros de interesse, que podem ser: distância mínima entre pontos, raio de cobertura, *kissing number*, coeficiente de quantização, erro de integração, dentre outros.

A escolha do parâmetro a ser otimizado vai depender de sua aplicação. Em telecomunicações, códigos esféricos tem sido amplamente estudados em conexão com a transmissão de sinais sobre um canal Gaussiano [5, 6, 30, 32, 52].

Um sistema típico de comunicações é ilustrado na Figura 2. De maneira resumida, pode-se descrever o processo da seguinte forma: Mensagens produzidas por uma *fonte de informação* são convertidas para a forma digital e então enviadas a um *destino* através de um *canal*. Esse processo de codificação de fonte envolve *quantização* ou conversão analógica-digital e possui relações com reticulados e códigos esféricos. O canal de transmissão é *ruidoso*, de forma que a mensagem recebida pode ser ligeiramente diferente da transmitida. A teoria da codificação busca maneiras de se realizar esta comunicação de forma eficiente, barata e o mais fiel possível.

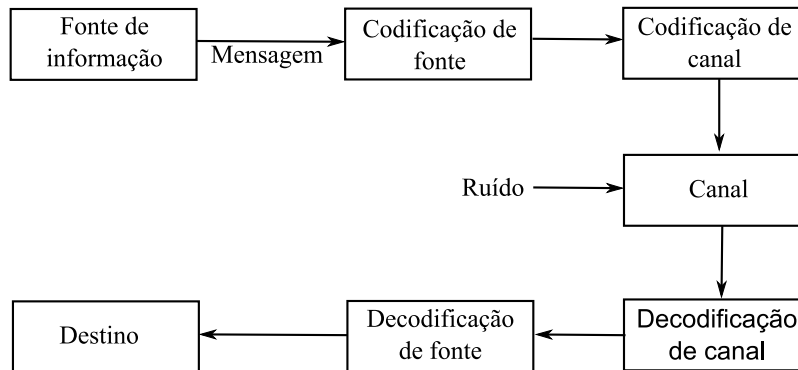


Figura 2: Diagrama de bloco de um sistema de comunicações.

Em um sistema de comunicação como ilustrado na Figura 2, a codificação de canal depende da escolha de um conjunto especial de sinais denominado *código*, cujos elementos são projetados para serem facilmente distinguíveis entre si, mesmo sob interferência de ruído. Somente sinais do código são utilizados na transmissão.

O codificador de canal recebe a saída (*output*) do codificador de fonte e a substitui por um sinal do código, que é então transmitido através do canal. O decodificador de canal reverte esse processo, assumindo que o sinal que fora transmitido é o ponto do

código que está mais próximo do recebido. Finalmente o decodificador de fonte recupera a mensagem original.

Existem dois principais modelos idealizados de canais. Um deles é o *canal binário simétrico*, onde somente sequências de 0's e 1's são transmitidas e recebidas. Para esse canal, existe uma vasta gama de códigos bastante conhecidos, como os códigos de Hamming, BCH, Red-Solomon, Golay, Goppa dentre outros. Não é sobre essa classe de códigos que versará esta tese.

Um segundo modelo de canal é o chamado *canal Gaussiano* ou *canal AWGN*, um canal aditivo onde o ruído é Gaussiano branco.

Um canal Gaussiano permite a transmissão de sinais contínuos, onde todas as frequências acima de um certo W ciclos por segundos (denominada *largura de banda* do canal) são atenuadas completamente e frequências abaixo de W passam sem atenuações. No curso do sinal, o canal adiciona a mensagem um *ruído branco* com distribuição Gaussiana que independe do sinal enviado.

Neste canal, um sinal transmitido $f(t)$ pode ser representado por um ponto $f = (f_1, f_2, \dots, f_n)$ num espaço Euclidiano n -dimensional. O canal adiciona um vetor $e = (e_1, e_2, \dots, e_n)$, cujas componentes são variáveis aleatórias, independentes, com distribuição Gaussiana de média 0 e variância σ^2 (denominada potência média do ruído). O sinal recebido é representado por $y = f + e$.

Um código para o canal Gaussiano é um conjunto de pontos no \mathbb{R}^n . Se existem M pontos no código, cada um representando um sinal com largura de banda W e duração de T segundos, a taxa do código é definida por

$$R = \frac{1}{T} \log_2 M \text{ bits/sec.}$$

Uma vez que o decodificador de canal assumirá que o sinal transmitido é o ponto do código que estiver mais próximo do vetor recebido $y = f + e$, se o ruído for “pequeno”, o sinal será recuperado completamente. Porém, se o ruído for “grande”, o vetor recebido pode estar próximo de algum outro ponto do código e será decodificado incorretamente.

Uma maneira de reduzir os efeitos do ruído consiste em escolher pontos do código bastante afastados. Porém, isso requer um aumento na energia dos sinais (aumento

da norma dos vetores do código). Equacionar esta relação de custo-benefício é um importante problema na codificação de um canal Gaussiano.

Existe um resultado surpreendente, demonstrado por Shannon em seu famoso trabalho [47], que estabelece a possibilidade de se realizar uma comunicação essencialmente livre de erros neste canal, sempre que a taxa de transmissão não ultrapasse um valor crítico denominado *capacidade do canal*. Resultados similares são conhecidos para outros canais, incluindo o canal binário simétrico.

Precisamente, o teorema de Shannon afirma que, num canal Gaussiano limitado em faixa, para qualquer taxa R abaixo da capacidade do canal,

$$C = W \log_2 \left(1 + \frac{P}{\sigma^2} \right),$$

fazendo T e, portanto, $n = 2WT$ suficientemente grandes, é possível encontrar um código com taxa R e potência média menor que P para o qual a probabilidade de erro na decodificação é arbitrariamente pequena. Reciprocamente, tal código não existe para taxas $R > C$.

Pode-se entender esse resultado da seguinte forma: Como os sinais f têm potência média menor do que P , eles pertencem ao interior de uma esfera de raio \sqrt{nP} [8]. Fazendo n suficientemente grande, pode-se assumir que o ruído $e \in \mathbb{R}^n$ é tal que $\|e\|^2 \leq n(\sigma^2 + \epsilon)$, onde ϵ é arbitrariamente pequeno. Em outras palavras, com alta probabilidade o vetor recebido $y = f + e$ pertence a uma pequena esfera de raio menor ou igual a $\sqrt{n(\sigma^2 + \epsilon)}$ centrada em f . Se os pontos do código estiverem suficientemente afastados, o vetor recebido será decodificado corretamente com probabilidade próxima de 1.

Um relevante problema na transmissão de sinais através de um canal Gaussiano consiste em procurar pelos melhores códigos nos quais os sinais possuem a mesma energia (código com energia constante). É exatamente este problema que possui estreitas relações com o estudo de códigos esféricos. Como observado em [8], para pequenos valores de σ , a procura do melhor código de energia constante para o canal Gaussiano está estreitamente relacionada com o problema de empacotar chapéus n -dimensionais na superfície de uma esfera. A menos de escala, pode-se considerar o problema na esfera unitária S^{n-1} .

No contexto da aplicação, esta será nossa principal motivação. Não obstante, no decorrer do trabalho será dada ênfase aos aspectos matemáticos do problema, que por si, já são instigantes o suficiente.

A principal questão que será abordada é o problema do empacotamento de chapéus em esferas Euclidianas, ou simplesmente o problema do **empacotamento de esferas**:

- Como alocar M pontos (x_1, x_2, \dots, x_M) sobre S^{n-1} de modo a maximizar a distância mínima entre eles?

Precisamente, deseja-se escolher M pontos sobre S^{n-1} de forma a

$$\text{maximizar} \left(\min_{i \neq j} \|x_i - x_j\| \right).$$

Como $x_k \in S^{n-1} \ \forall k$, tem-se $\|x_i - x_j\| = 2 - 2\langle x_i, x_j \rangle$ e uma formulação alternativa para o problema do empacotamento é:

$$\text{minimizar} \left(\max_{i \neq j} \langle x_i, x_j \rangle \right).$$

Algumas vezes será interessante considerar um problema dual:

- Dada uma distância mínima d , qual é o maior número de pontos M que podem ser alocados em S^{n-1} com distância maior ou igual a d ?

Outras aplicações derivam problemas matemáticos interessantes, que possuem relações com o problema do empacotamento esférico, como, por exemplo:

- **Cobertura esférica:** Como escolher M pontos (x_1, x_2, \dots, x_M) em S^{n-1} de modo a minimizar a distância máxima de um ponto qualquer de S^{n-1} até o ponto x_i mais próximo?

$$\text{minimizar} \max_{y \in S^{n-1}} \max_{i=1 \dots M} \|x_i - y\|$$

A diferença entre os problemas de empacotamento e cobertura pode ser ilustrada nos seguintes termos: Imagine que uma estação de rádio deseja transmitir a final da copa do mundo de futebol para torcedores fanáticos que vivem na lua. Para tanto a

empresa decide instalar na superfície lunar M torres de transmissão idênticas de modo a cobrir a maior área possível. Do ponto de vista da administração da empresa eles estão pensando em empacotamento esférico. É desejável evitar redundâncias, o que significa evitar intersecções entre as áreas cobertas pelas torres, alocando-as o mais afastado possível. Porém, do ponto de vista dos torcedores, eles desejam se deslocar pouco até chegar a um ponto onde possam ouvir o rádio. Eles desejam uma cobertura.

À primeira instância, empacotamento e cobertura parecem ter soluções idênticas. Bons empacotamentos com 30 pontos deveriam significar boas coberturas com 30 pontos. No entanto, exceto em casos muito especiais, isso não é verdade. A discussão dessas diferenças embora instigante, foge do escopo desta tese e pode ser encontrada em [29].

Outra maneira estudar o empacotamento em esferas Euclidianas está relacionada ao seguinte problema:

- **Kissing number**¹: Qual é o maior número $\tau(n, p, r)$ de esferas n -dimensionais de raio p que podem tocar simultaneamente uma esfera n -dimensional de raio r ?

A formulação clássica do problema do máximo *kissing number* $\tau(n, p, r)$ é para $p = r$ e, neste caso, adota-se simplesmente a notação $\tau(n)$, uma vez que, tendo as esferas raios iguais, τ passa a depender unicamente da dimensão. O caso geral considerado aqui possui estreitas relações com o problema do empacotamento esférico.

Com efeito, considere duas esferas n -dimensionais, com centros em y_1 e y_2 e raio p que tangenciam simultaneamente uma esfera centrada em x , com raio r . O plano que passa pelo centro das três esferas determina um perfil como o ilustrado na Figura 3. Por semelhança de triângulos tem-se

$$\frac{d}{2p} = \frac{r}{r + p},$$

ou seja $d = \frac{2pr}{r + p}$. Tomando uma homotetia com fator $1/r$, a esfera central torna-se unitária e os pontos de tangência permanecem inalterados. De modo que, determinar o

¹ A denominação *kissing number* é devida ao jogo de bilhar. Em inglês, quando duas bolas de bilhar se tocam é utilizado o termo *kiss*. Nesta tese manteremos o termo em inglês por ser uma notação clássica.

maior número de esferas de raio p podem tocar simultaneamente uma esfera de raio r é equivalente a determinar o melhor código esférico com distância mínima maior ou igual à $\frac{2p}{r+p}$. Em particular, se $p = r$ tem-se $d = 1$ e o problema clássico de determinar $\tau(n)$ é equivalente a encontrar melhor código esférico com distância mínima $d \geq 1$.

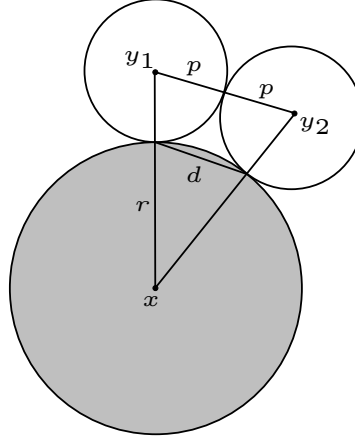


Figura 3: Conexão entre kissing number e códigos esféricos

Kissing numbers conhecidos

Para $n = 2$, o problema do máximo $\tau(n)$ (Figura 4), bem como o problema do melhor código esférico com M pontos pode ser facilmente resolvido. Ambas as soluções são obtidas inscrevendo-se polígonos regulares em S^1 . Em particular, se as esferas tiverem raios unitários (problema clássico) o ângulo interno α deve ser igual a $\frac{\pi}{3}$. Assim,

$$\tau(2) = \left\lfloor \frac{2\pi}{\pi/3} \right\rfloor = 6$$

No espaço tri-dimensional o problema é bem mais interessante e mais complexo. Em \mathbb{R}^3 esse problema é conhecido como *problema da 13ª esfera*, ou *problema de Gregory-Newton*. Tal denominação tem origem em 1694 durante uma famosa conversa entre David Gregory e Isac Newton sobre a seguinte pergunta:

- Uma esfera pode tocar 13 esferas de mesmo raio?

Newton pensava que não: “o número máximo é 12”. Gregory acreditava que a resposta era sim.

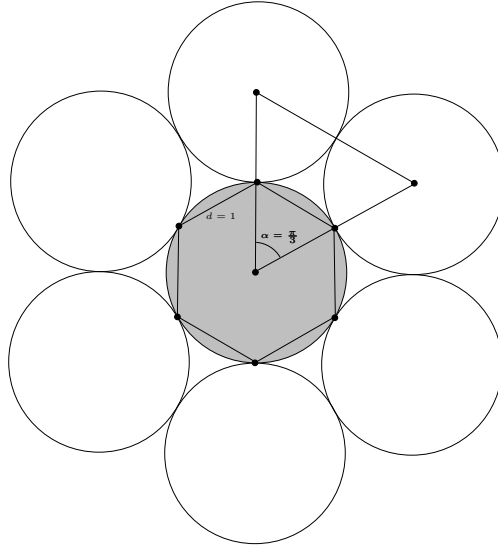


Figura 4: Kissing number em \mathbb{R}^2 com círculos de mesmo raio ($p = r = 1$).

Ambos sabiam que, se 12 esferas de raios iguais a 1 fossem colocadas nos vértices de um icosaedro regular, de forma a tangenciar uma esfera unitária no interior deste poliedro, elas não tocariam suas vizinhas, conforme pode ser visto na Figura 6. Sendo assim, elas poderiam ser ligeiramente deslocadas e ainda continuariam tangenciando a esfera central. De fato, o melhor código esférico com doze pontos em \mathbb{R}^3 , $\mathcal{C}(12, 3)$ tem distância mínima $d = \sqrt{2 - 2/\sqrt{5}} \approx 1.05146$ e é obtido inscrevendo-se um icosaedro em S^2 . Esta distância, ligeiramente maior do que 1, implica que os centros das esferas externas distam pelo menos 2.10292, deixando um pequeno espaço (0.1022) para movimentá-las.

Esse fato, além de implicar que $\tau(3) \geq 12$, dava margem a expectativa de que um arranjo diferente do icosaedral poderia possibilitar um espaço extra para a 13ª esfera. Gregory ainda tinha a seu favor outro argumento.

Seja $ch(3, \frac{\pi}{6})$ um chapéu esférico na superfície de S^2 com raio angular $\frac{\pi}{6}$. A distância mínima entre o centro de dois chapéus $ch(3, \frac{\pi}{6})$ disjuntos é pelo menos 1. Assim, $\tau(3)$ é limitado superiormente pelo maior número de chapéus $ch(3, \frac{\pi}{6})$ que podem ser

empacotados sem intersecção sobre S^2 . Esse número pode ser estimado dividindo-se a área da superfície de S^2 pela área de um chapéu.

$$\tau(3) \leq \frac{\text{área}(S^2)}{\text{área}(ch(3, \frac{\pi}{6}))} = 14.9282\dots,$$

de modo que $12 \leq \tau(3) \leq 14$.

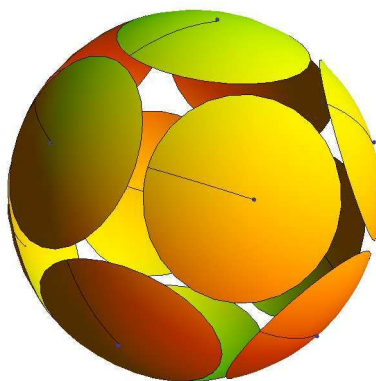


Figura 5: Doze chapéus esféricos sobre S^2 com centros nos vértices de um icosaedro regular.

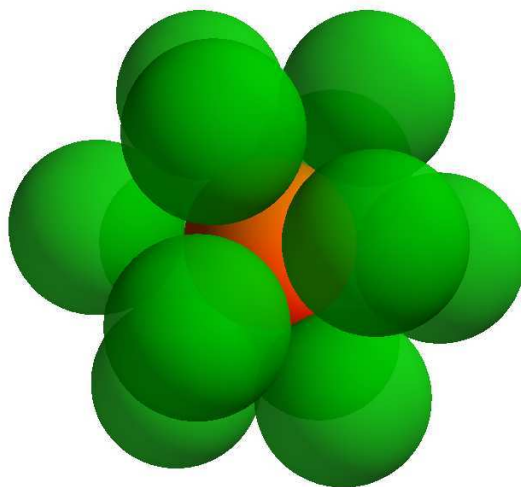


Figura 6: Doze esferas unitárias com centro nos vértices de um icosaedro tangenciando S^2 .

O problema da 13ª esfera só foi resolvido em 1953, com o trabalho de Shütte e van der Waerden [46]. Newton estava certo, $\tau(3) = 12$. Uma referência sobre essa prova pode ser encontrada em [64].

Sabia-se durante algum tempo que a solução em \mathbb{R}^4 estava entre 24 e 25. Não é difícil produzir uma solução com 24 hiperesferas tangenciando uma central, basta considerar os 24 vetores de norma mínima do reticulado D_4 . Contudo, como no caso do icosaedro em \mathbb{R}^3 , sobra espaço livre entre as esferas, o que daria margem à possibilidade para uma 25ª. Em 2003, Oleg Musin [40] surpreendeu a comunidade matemática anunciando a prova de que $\tau(4) = 24$. Após quase cinco anos de revisão e depois de três versões, a prova foi finalmente publicada no conceituado periódico *Annals of Mathematics* em 2008, [41].

Em dimensões 8 e 24, se sabe que $\tau(8) = 240$ e $\tau(24) = 196.560$. Em ambas soluções, os centros das esferas são os vetores de norma mínima de dois reticulados² excepcionalmente densos e simétricos conhecidos como E_8 e Leech. Exceto nesses casos, não se conhece a prova para kissing numbers em dimensões maiores do que 4. O que se conhece são limitantes inferiores e superiores [9, 35, 43]. Uma boa referência para o assunto pode ser encontrada em [44].

A Tabela 1 apresenta uma lista, baseada em [39], com limitantes para kissing numbers em várias dimensões.

Como já foi dito, o objetivo desta tese é o estudo de métodos para o problema do empacotamento esférico. Se um método para determinar o melhor código esférico n -dimensional para qualquer distância mínima for conhecido, o problema do máximo kissing number $\tau(n, r, p)$ estará resolvido. Isso dá uma ideia da dificuldade desse problema.

Nesta tese apresentamos duas contribuições. No Capítulo 2, desenvolvemos um método para procura do melhor código esférico obtido como órbita de um vetor unitário inicial sob ação de um grupo comutativo de matrizes ortogonais. A segunda contribuição é apresentada no Capítulo 3, onde propomos uma nova família de códigos esféricos, na qual os pontos são alocados em camadas de toros planares.

² Uma descrição mais específica sobre reticulados é dada na Seção 1.1

Dimensão	Melhor $\tau(n)$ conhecido	Limitante superior
1	2	2
2	6	6
3	12	12
4	24	24
5	40	44
6	72	78
7	126	134
8	240	240
9	306	364
10	500	554
11	582	870
12	840	1.357
13	1.130	2.069
14	1.582	3.183
15	2.564	4.866
16	4.320	7.355
17	5.346	11.072
18	7.398	16.572
19	10.688	24.812
20	17.400	36.764
21	27.720	54.584
22	49.896	82.340
23	93.150	124.416
24	196.560	196.560

Tabela 1: Melhores kissing numbers conhecidos e respectivos limitantes superiores para várias dimensões. Em destaque kissing numbers ótimos.

O trabalho está organizado da seguinte forma: No Capítulo 1 são apresentados conceitos e resultados importantes sobre reticulados e uma revisão das principais técnicas conhecidas para construção de códigos esféricos. No Capítulo 2 estudamos o problema de encontrar um código de grupo comutativo ótimo. Na Seção 2.3, propomos um método para obter o melhor código de grupo comutativo n -dimensional de ordem M , que se baseia na associação entre tais códigos em dimensão $2k$ e reticulados k -dimensionais. Utilizando fatorações matriciais conhecidas, como as formas normais de Hermite e Smith, demonstramos que é possível reduzir o número de casos a serem analisados através da identificação de códigos isométricos que podem ser descartados. No Capítulo 3 introduzimos uma nova família de códigos esféricos, cujos pontos são alocados em camadas de toros mergulhadas na superfície da esfera unitária. Além de limitantes, inferior e superior, para o número máximo de pontos, um método para construção destes códigos é apresentado explicitamente, alguns exemplos são construídos e

uma análise comparativa com os melhores códigos conhecidos é apresentada. Os resultados mostram que tais códigos têm desempenho comparável aos melhores códigos esféricos estruturados conhecidos, com destaque para uma potencial vantagem no processo de codificação/decodificação, decorrente da homogeneidade, estrutura de grupo e associação a reticulados na metade da dimensão

RETICULADOS E CÓDIGOS ESFÉRICOS

Neste capítulo apresentamos um resumo sobre reticulados e códigos esféricos. Além de tornar clara a notação que será utilizada no decorrer desta tese, o objetivo é também inserir, de forma sintética, definições e resultados necessários ao desenvolvimento dos Capítulos 2 e 3. Além disso, procuramos apresentar uma revisão sobre as principais técnicas conhecidas para obtenção de códigos esféricos.

1.1 Reticulados

O estudo de reticulados tem apresentado conexões com muitas áreas da matemática. Além de sua conhecida relação com problemas empacotamentos e coberturas esféricas, novas aplicações têm surgido, dentre as quais o uso de reticulados no desenvolvimento dos chamados criptossistemas pós-quânticos [4] merecem um destaque especial pelo impacto em inovação que podem impulsionar.

Nesta tese, reticulados ocupam um lugar central nos principais resultados que foram obtidos nos Capítulos 2 e 3.

Um reticulado Λ é o conjunto de todas as combinações lineares a coeficientes inteiros de um conjunto $\beta = \{u_1, u_2, \dots, u_m\}$ de m vetores linearmente independentes do espaço vetorial \mathbb{R}^n ($m \leq n$), i. e.,

$$\Lambda = \left\{ x = \sum_{i=1}^m a_i u_i : a_i \in \mathbb{Z} \ \forall \ i \right\}.$$

O conjunto β é denominado uma *base* de Λ e a matriz A , cujas linhas são os vetores da base β , é chamada uma *matriz geradora* de Λ . Um reticulado pode admitir diferentes matrizes geradoras, ou diferentes bases. Assim, a notação Λ_β ou Λ_A será utilizada quando for necessária uma referência específica a alguma base β ou matriz geradora A .

A *distância mínima* d_Λ de um reticulado Λ é a menor distância euclidiana entre dois pontos quaisquer de Λ ,

$$d_\Lambda = \min_{x \neq y \in \Lambda} \|x - y\|$$

A matriz $G = AA^T$ é denominada *matriz de Gram* do reticulado e tem grande importância na caracterização métrica de Λ_A . Como é usual, o determinante da matriz G é denominado *discriminante* ou *determinante* de Λ e denotado por $\det(\Lambda)$. Geometricamente $\det(\Lambda)$ é o quadrado do volume k -dimensional do paralelotopo fundamental:

$$\mathcal{P}_\beta = \left\{ y \in \mathbb{R}^n : y = \sum_{i=1}^m t_i u_i, 0 \leq t_i < 1, t_i \in \mathbb{R} \right\}.$$

Por esta razão, o número $V = \sqrt{\det(\Lambda)}$ é chamado volume do reticulado Λ .

Como Λ admite várias bases, o paralelotopo fundamental não é único, no entanto seu volume é invariante à escolha de uma particular base do reticulado. Isto decorre do fato que, se A e B são as matrizes associadas a duas bases β e γ de Λ , então existe uma matriz unimodular H (entradas inteiras e $\det(H) = \pm 1$), tal que $B = HA$. Assim,

$$\det(BB^T) = \det(HAA^TH^T) = \det(H) \det(AA^T) \det(H^T) = \det(AA^T)$$

Um paralelotopo fundamental \mathcal{P} contém exatamente um ponto do reticulado, além disso, o conjunto $(\Lambda + \mathcal{P})$ da união de todas as translações de \mathcal{P} por um ponto do reticulado Λ é uma pavimentação do espaço \mathbb{R}^m [10].

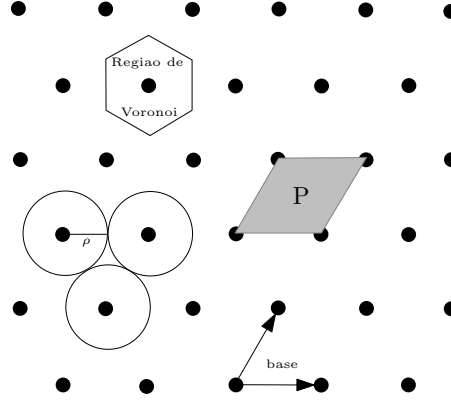


Figura 1.1: Reticulado A_2 .

A região de Voronoi de um ponto $v \in \Lambda$ é o conjunto de todos os pontos do \mathbb{R}^m que estão mais próximos do ponto v do que de qualquer outro ponto do reticulado Λ .

$$R_\Lambda(v) = \{x \in \mathbb{R}^m : \|v - x\| \leq \|u - x\|, \forall u \in \Lambda\}.$$

Se um subconjunto Λ' de um reticulado Λ é também um reticulado, dizemos que Λ' é um subreticulado de Λ .

Um *subreticulado* $\Lambda' \subset \Lambda$ é dito *ortogonal* (ou *retangular*) se, e somente se, existe uma base de vetores ortogonais β' para Λ' . Subreticulados ortogonais desempenham papel fundamental nesta tese, uma vez que possuem estreita relação com códigos esféricos gerados por grupos comutativos [49].

À qualquer base ordenada $\beta = \{u_1, u_2, \dots, u_m\}$ de um reticulado Λ , é possível associar um conjunto $GS_\beta = \{b_1, b_2, \dots, b_m\}$ de vetores ortogonais, aplicando recursivamente o processo de ortogonalização de *Gram-Schmidt*:

$$\begin{aligned} b_1 &= u_1 \\ b_i &= u_i - \sum_{j=1}^{i-1} \frac{\langle u_i, b_j \rangle}{\langle b_j, b_j \rangle} u_j, \quad i = 2, \dots, m \end{aligned}$$

Os vetores b_i podem não pertencer ao reticulado Λ_β . No entanto, se $\langle u_i, u_j \rangle$ for um número racional para todo i e j , é possível encontrar um múltiplo de b_i que pertence a Λ_β , o que permite escrever:

Proposição 1.1 [3] *Se uma matriz de Gram de um reticulado Λ possui somente elementos racionais (se Λ é racional), então Λ possui um subreticulado ortogonal Λ' .*

A título de exemplo, considere a matriz de Gram do reticulado hexagonal A_2 , gerado pelos vetores $(0, 1)$ e $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ no plano,

$$G = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix},$$

Como os elementos de G são todos racionais, A_2 possui um subreticulado ortogonal. De fato, A_2 contém o subreticulado Λ' gerado pelos vetores $(1, 0)$ e $(0, \sqrt{3})$.

Além disso, A_2 pode ser visto como a união de dois conjuntos disjuntos de pontos, como ilustrado na Figura 1.2. O primeiro conjunto é exatamente o subreticulado Λ' , enquanto o segundo é formado pelas translações dos pontos de Λ' pelo vetor $v = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.

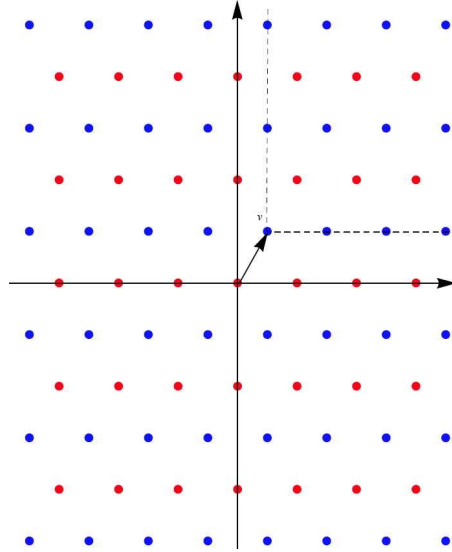


Figura 1.2: Reticulado hexagonal A_2 decomposto em duas classes retangulares.

Uma maneira útil de representar reticulados que possuem subreticulados ortogonais é através do *diagrama de treliça* do reticulado, como descrito na próxima seção.

1.1.1 Diagrama de treliça de reticulados

Diagramas de treliça foram introduzidos por Forney [20] em 1967, onde o algoritmo de Viterbi, inicialmente apresentado em [63], foi utilizado para decodificação de códigos convolucionais. A estrutura de treliça associada a reticulados é abordada em [21, 22, 55] e também em [3], onde a complexidade destes diagramas é estudada para a decodificação eficiente de códigos baseados em reticulados.

Esta subseção faz um resumo dos conceitos básicos sobre diagramas de treliça de reticulados, baseado em [3]. O conteúdo apresentado aqui também compõe o trabalho [18].

Sejam $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$ uma sequência de espaços vetoriais com $\dim(V_i) = i$, e W_i o complemento ortogonal de V_{i-1} em V_i para $1 \leq i \leq n$. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado n -dimensional, P_{V_i} e P_{W_i} os operadores projeção de \mathbb{R}^n sobre os espaços vetoriais V_i e W_i , respectivamente, $\Lambda_{V_i} = \Lambda \cap V_i$ e $\Lambda_{W_i} = \Lambda \cap W_i$.

Para a construção de um diagrama de treliça de um reticulado Λ , definimos os grupos quocientes:

$$\Sigma_i(\Lambda) = \frac{P_{V_i}(\Lambda)}{\Lambda_{V_i}} : \text{espaço de estado no nível } i, 0 \leq i \leq n.$$

$$G_i(\Lambda) = \frac{P_{W_i}(\Lambda)}{\Lambda_{W_i}} : \text{grupo de rotulamento na seção } i, 1 \leq i \leq n.$$

Definição 1.1 *O diagrama de treliça T de um reticulado Λ é um grafo, cujos nós em cada nível i , $0 \leq i \leq n$, são elementos de $\Sigma_i(\Lambda)$ e as arestas entre os níveis $i-1$ e i são rotuladas por elementos de $G_i(\Lambda)$.*

No diagrama de treliça T de um reticulado Λ , cada $x \in \Lambda$ percorre um único caminho representado por uma sequência de nós $\sigma(x) = (\sigma_0(x), \dots, \sigma_n(x))$, onde $\sigma_i(x) = \Lambda_{V_i} + P_{V_i}(x)$, que estão conectados por uma sequência de arestas $g(x) = (g_1(x), \dots, g_n(x))$, onde $g_i(x) = \Lambda_{W_i} + P_{W_i}(x)$.

Na treliça do reticulado Λ_B tem-se que $\sigma(\Lambda)$ e $g(\Lambda)$ são isomorfos [19], e a cardinalidade de ambos, denotada por $N(\Lambda_B)$, é igual ao número de caminhos distintos na treliça.

Exemplo 1.1 *Sejam $b_1 = (2, 0)$ e $b_2 = (1, 2)$ os vetores que geram um reticulado $\Lambda \subset \mathbb{R}^2$. Tomando a sequência de espaços vetoriais $\{0\} = V_0 \subset V_1 \subset V_2 = \mathbb{R}^2$, com*

$V_1 = \text{ger}((2, 0))$, onde $\text{ger}(S)$ denota o espaço vetorial gerado por S . Temos $W_1 = V_1$ e $W_2 = \text{ger}((0, 1)) = \text{ger}((0, 4))$, logo

$$\sum_0(\Lambda) = \sum_2(\Lambda) = 0, \quad \sum_1(\Lambda) = (1, 0)\mathbb{Z}/(2, 0)\mathbb{Z},$$

$G_1(\Lambda) = (1, 0)\mathbb{Z}/(2, 0)\mathbb{Z}$, $G_2(\Lambda) = (0, 2)\mathbb{Z}/(0, 4)\mathbb{Z}$, onde $v\mathbb{Z}$ representa o grupo aditivo gerado por v (o conjunto de todos os múltiplos inteiros de v). E conseqüentemente,

$$\sigma(\Lambda) = \{(0, (2, 0)\mathbb{Z}, 0), (0, (1, 0) + (2, 0)\mathbb{Z}, 0)\},$$

$$g(\Lambda) = \{((2, 0)\mathbb{Z}, (0, 4)\mathbb{Z}), ((1, 0) + (2, 0)\mathbb{Z}, (0, 2) + (0, 4)\mathbb{Z})\}.$$

Os caminhos na treliça correspondem às classes laterais do subreticulado ortogonal gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (0, 4)$. Estas classes são ilustradas pelos conjuntos de pontos pretos e brancos no reticulado Λ da Figura 1.3.

Dizemos que Λ tem uma treliça finita se existe um diagrama de treliça para Λ com um número finito de nós (ou arestas). Um reticulado n -dimensional Λ possui treliça finita se, e somente se, ele possui um subreticulado ortogonal n -dimensional Λ' [3].

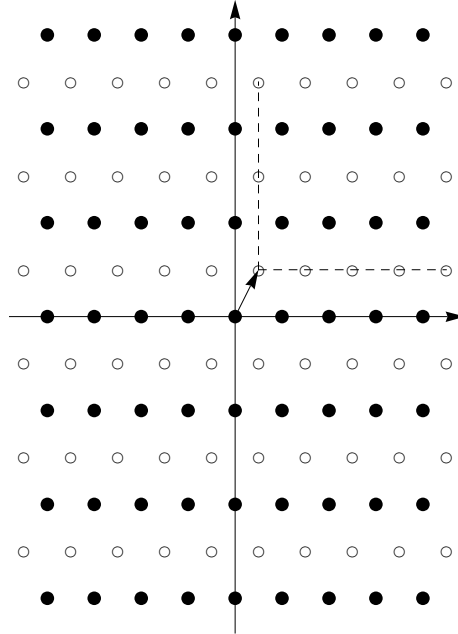


Figura 1.3: Reticulado gerado por b_1 e b_2 , decomposto em duas classes laterais.

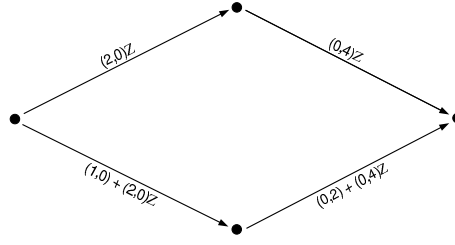


Figura 1.4: Uma treliça do reticulado gerado por b_1 e b_2 .

Exemplo 1.2 Como já mencionamos, o reticulado A_2 pode ser decomposto em duas classes retangulares (Figura 1.2). Vamos construir o diagrama de treliça de A_2 para entender como isso pode ser representado num grafo.

Sejam $b_1 = (1, 0)$, $b_2 = (1/2, \sqrt{3}/2)$ os vetores da base de A_2 .

No sistema de coordenadas-treliça $W_1 = \text{span}(1, 0)$ e $W_2 = \text{span}(0, 1)$, o reticulado A_2 tem a treliça representada na Figura 1.5.

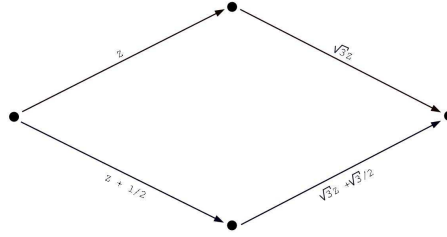


Figura 1.5: Um diagrama treliça de A_2 .

Os grupos de rotulamento são $G_1 = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ e $G_2 = \frac{\sqrt{3}}{2}\mathbb{Z}/\sqrt{3}\mathbb{Z}$.

Note que os dois caminhos da treliça correspondem às classes laterais do subreticulado ortogonal

$$\mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \text{ em } A_2,$$

que aparecem em destaque na Figura 1.2.

O sistema de subespaços $\{W_i\}_{i=1}^n$, correspondendo à cadeia V_0, \dots, V_n , é chamado de *sistema de coordenadas-treliça* Λ para T . Assim, um reticulado Λ possui treliça finita se, e somente se, $\dim(\Lambda_{W_i}) = 1$, para todo i . Neste caso, o subreticulado ortogonal correspondente Λ' é $\Lambda_{W_1} \oplus \dots \oplus \Lambda_{W_n}$.

Exemplo 1.3 *Seja $b_1 = (-8, 0, -56)$, $b_2 = (-8, 0, -256)$ e $b_3 = (-4, -25, -425)$ os vetores que geram um reticulado $\Lambda \subset \mathbb{R}^3$. No sistema de coordenadas-treliça*

$$W_1 = \text{span}(\hat{b}_1) = \text{span}(b_1),$$

$$W_2 = \text{span}(\hat{b}_2) = \text{span}(28, 0, -4),$$

$$W_3 = \text{span}(\hat{b}_3) = \text{span}((0, -25, 0)).$$

Λ tem a treliça da Figura 1.6.

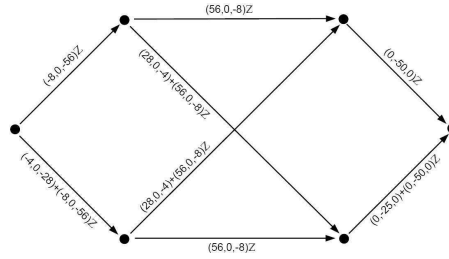


Figura 1.6: Um diagrama treliça de Λ

Os grupos de rotulamento são dados por:

$$G_1 = (-4, 0, -28)\mathbb{Z}/(-8, 0, -56)\mathbb{Z},$$

$$G_2 = (28, 0, -4)\mathbb{Z}/(56, 0, -8)\mathbb{Z}e$$

$$G_3 = (0, -25, 0)\mathbb{Z}/(0, -50, 0)\mathbb{Z}.$$

Note que os quatro caminhos da treliça correspondem às classes laterais do subreticulado ortogonal

$$(-8, 0, -56)\mathbb{Z} \oplus (56, 0, -8)\mathbb{Z} \oplus (0, -50, 0)\mathbb{Z} \text{ em } \Lambda.$$

No entanto, podemos perguntar: esta é a treliça mínima para Λ ?

A rigor, é possível encontrar a treliça mínima de um reticulado racional através da inspeção de diferentes bases, porém, métodos de busca exaustiva aplicados a problemas de reticulados podem tornar-se impraticáveis devido ao alto custo computacional.

Ainda não se conhece um método geral para resolver este problema. Em [18] apresentamos uma alternativa para abordar este problema em casos específicos. No caso do reticulado anterior, por exemplo, existe um diagrama de treliça com apenas dois caminhos.

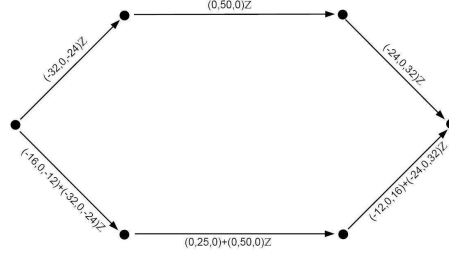


Figura 1.7: Uma treliça mínima para Λ

Além da treliça mínima, a obtenção de diversos outros parâmetros de um reticulado, como vetor de norma mínima, densidade, raio de cobertura, resultam em problemas computacionalmente muito difíceis, os denominados problemas NP [38]. No entanto, existem alguns reticulados especiais, para os quais estes valores são conhecidos [3]. A próxima seção, apresenta os principais deles.

1.1.2 Alguns reticulados notáveis

Os reticulados \mathbb{Z}^n , A_n , D_n e E_8 são denominados *reticulados-raízes* devido sua associação à certos sistemas em Álgebras de Lie. Esta associação não é necessária para definir esses reticulados, que serão amplamente utilizados nesta tese numa abordagem bastante geométrica.

Uma maneira de defini-los é:

$$\begin{aligned}
 \mathbb{Z}^n &\hat{=}\{(x_1, x_2, \dots, x_n) : x_i \in \mathbb{Z}\}; \\
 A_n &\hat{=}\{(x_1, x_2, \dots, x_n) \in \mathbb{Z}^{n+1} : x_1 + x_2 + \dots + x_n = 0\}; \\
 D_n &\hat{=}\{(x_1, x_2, \dots, x_n) \in \mathbb{Z}^n : x_1 + x_2 + \dots + x_n \text{ é par}\}; \\
 E_8 &\hat{=}\{(x_1, x_2, \dots, x_8) : x_i \in \mathbb{Z} \text{ ou } x_i + 1/2 \in \mathbb{Z} \text{ e } \sum x_i \text{ é par}\}
 \end{aligned}
 \tag{1.1}$$

Muitas propriedades de um reticulado são invariantes à alteração de escala ou orientação. Neste sentido, diz-se que dois reticulados Λ_A e Λ_B são *equivalentes* quando um pode ser obtido através de uma isometria, composta com uma dilatação ou contração do outro. Ou seja, se existem matrizes geradoras A e B de Λ_A e Λ_B , tais que $A = \alpha UB$, onde $\alpha \in \mathbb{R}$ e U é uma matriz ortogonal.

Por exemplo, o reticulado bi-dimensional A_2 pode ser gerado pela matriz

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

no entanto, conforme definido em (1.1), A_2 é a intersecção do reticulado \mathbb{Z}^3 com o plano $x + y + z = 0$. Neste caso, uma matriz geradora é:

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

Com efeito, A pode ser obtida de A' por meio de uma rotação (a mesma que leva o vetor $(1, 1, 1)$, ortogonal ao plano de soma zero, no vetor $(0, 0, \sqrt{3})$) seguida de uma dilatação de $\frac{1}{\sqrt{2}}$.

$$\frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{\sqrt{2}}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} & \frac{\sqrt{2}}{\sqrt{3}} \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \\ \frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -1 & -1 \end{pmatrix} \right)^t = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \end{pmatrix}$$

Neste caso, considera-se que os reticulados Λ_A e $\Lambda_{A'}$ são equivalentes.

1.1.3 Reticulados e empacotamentos esféricos

Um empacotamento esférico ou simplesmente empacotamento, é um conjunto enumerável de bolas abertas, de mesmo raio, mutuamente disjuntas.

Denomina-se empacotamento reticulado quando o centro das bolas são os pontos de um reticulado. A todo reticulado Λ tem-se um empacotamento esférico associado, que é dado por bolas cujo raio é metade da distância mínima entre pontos de Λ .

O *raio de empacotamento* é o raio das bolas abertas do empacotamento. Geralmente é assumido como o maior raio possível, tal que existam esferas tangentes, mas não exista nenhuma intersecção entre elas.

A *densidade* Δ de um empacotamento é fração do espaço total ocupado pelas bolas do empacotamento.

A densidade de um empacotamento reticulado pode ser calculada a partir de sua matriz geradora A ,

$$\Delta = \frac{V_{nr}}{\sqrt{\det(AA^T)}},$$

onde, V_{nr} é o volume de bola n -dimensional de raio r , igual ao raio do empacotamento.

O volume V_{nr} pode ser calculado baseando-se no volume da esfera unitária n -dimensional V_n , definido por

$$V_n = \int_{x \in \mathbb{R}^n: \|x\| \leq 1} dx = \frac{\pi^{n/2}}{\Gamma(\frac{n+2}{2})}, \quad (1.2)$$

onde Γ denota a função Gamma, definida por $\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt$.

V_n também pode ser reescrito como

$$V_n = \frac{2\pi^{n/2}}{n\Gamma(\frac{n}{2})} = \begin{cases} \frac{\pi^{n/2}}{(n/2)!} & \text{se } n \text{ é par} \\ \frac{2^n \pi^{(n-1)/2} ((n-1)/2)!}{n!} & \text{se } n \text{ é ímpar} \end{cases} \quad (1.3)$$

Utilizando (1.2), tem-se que $V_{nr} = r^n V_n$. O volume ¹ $(n-1)$ -dimensional, ou “área de superfície” de S^{n-1} é dada por

$$A(S^{n-1}) = \int_{x \in \mathbb{R}^n: \|x\|=1} dx = nV_n$$

A Figura 1.8 apresenta um gráfico do volume e da área da esfera euclidiana unitária para algumas dimensões. Pode-se notar que o volume cresce até a dimensão $n = 5$ e decresce para $n > 5$.

¹ Uma observação que contraria a intuição: A esfera unitária S^{n-1} pode ser inscrita num hipercubo de aresta 2, de modo a tangenciar cada face deste poliedro. Podemos concluir imediatamente de (1.3) que, tanto o volume, quanto a área superficial de S^{n-1} tendem a zero quando n cresce. No entanto o volume do cubo que contém a esfera cresce indefinidamente com n ($\text{VCubo} = 2^n$).

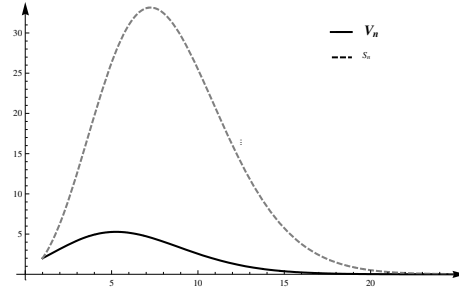


Figura 1.8: Área (S_n) e volume (V_n) da esfera unitária em várias dimensões.

Na comparação entre densidades de reticulados na mesma dimensão, o volume V_n da esfera unitária aparece como fator comum. Ao dividir a densidade de empacotamento Δ por V_n , tem-se uma medida δ denominada *densidade de centro* do reticulado:

$$\delta = \frac{\Delta}{V_n}.$$

Embora a densidade de empacotamento dos principais reticulados, como os definidos em (1.1), seja conhecida, o cálculo da densidade de empacotamento de um reticulado qualquer é um problema bastante difícil. Isso porque envolve, invariavelmente, o conhecimento do vetor de norma mínima do reticulado, o que, no caso geral, é um problema NP completo [38].

Se o raio das esferas num empacotamento em \mathbb{R}^m for aumentado continuamente, em algum instante esferas irão se sobrepor. Se o novo raio for suficientemente grande, qualquer ponto do \mathbb{R}^m ficará dentro de pelo menos uma dessas novas esferas. Isto é denominado uma *cobertura esférica* do espaço \mathbb{R}^m . O menor raio que resulta numa cobertura esférica é denominado *raio de cobertura*. Assim como no caso do raio de empacotamento, um importante problema em geometria é encontrar o menor raio de cobertura dentre todas as coberturas de \mathbb{R}^m .

Embora reticulados resultem em alguns dos melhores empacotamentos conhecidos, em algumas dimensões a maior densidade de empacotamento não provém de um reticulado. A Tabela 1.1 apresenta uma lista dos melhores empacotamentos esféricos conhecidos até a dimensão 24, de acordo com [10]. O tipo “NR” significa que o referido empacotamento não é reticulado.

Dimensão	Nome do empacotamento	Densidade de empacotamento	Densidade de centro	Tipo
0	Λ_0	1	1	R
1	A_1	1	0.5	R
2	A_2	0.9069	0.28868	R
3	D_3	0.74048	0.17678	A
4	D_4	0.61685	0.125	R
5	D_5	0.46526	0.08839	A
6	E_6	0.37295	0.07217	A
7	E_7	0.2953	0.0625	A
8	E_8	0.25367	0.0625	R
9	Λ_9	0.14577	0.04419	A
10	P_{10c}	0.09962	0.03906	NR
11	P_{11a}	0.06624	0.03516	NR
12	K_{12}	0.04945	0.03704	R
13	P_{13a}	0.03201	0.03516	NR
14	Λ_{14}	0.02162	0.08278	A
15	Λ_{15}	0.01686	0.04419	A
16	Λ_{16}	0.01471	0.0625	A
17	Λ_{17}	0.00811	0.0625	A
18	Λ_{18}	0.005928	0.07217	A
19	Λ_{19}	0.004121	0.08839	A
20	Λ_{20}	0.003226	0.125	A
21	Λ_{21}	0.002466	0.17678	A
22	Λ_{22}	0.002128	0.28868	R
23	Λ_{23}	0.001905	0.5	R
24	Λ_{24}	0.00193	1	R

Tabela 1.1: Melhores empacotamentos esféricos conhecidos até a dimensão 24. Tipo “R” significa reticulado, “NR” não reticulado e “A” significa que existem ambos os tipos.

1.2 Construção de códigos esféricos

Seja $M(n, d)$ o maior número de pontos que podem ser alocados sobre a superfície de S^{n-1} tal que a distância euclidiana entre dois pontos distintos quaisquer seja maior ou igual a d . Algumas vezes, o número $M(n, d)$ pode ser referido como a cardinalidade do *melhor código esférico* n -dimensional com distância mínima d .

De forma análoga denotaremos por $d(M, n)$ a maior distância mínima possível entre M pontos sobre S^{n-1} .

Determinar $M(n, d)$ ou $d(M, n)$ são problemas que, embora antigos e amplamente estudados, ainda encontram-se em aberto. Como já foi dito, para $n = 2$, esse problema

tem como solução trivial o polígono de M lados inscrito em S^2 . Contudo soluções ótimas para $M(n, d)$ com $n > 2$ são conhecidas apenas para um número muito pequeno de casos. Mesmo em R^3 só se tem a prova de otimalidade para $M \leq 12$ e $M = 24$ [16]. Não obstante, para algumas dimensões e cardinalidades existem listas dos melhores códigos conhecidos, sem a prova de que sejam definitivamente ótimos. Atualmente, uma das principais referências sobre o assunto é a página web mantida pelo Dr. Neil J. A. Sloane, pesquisador do AT&T Labs Research, [53].

Sem a possibilidade de solução direta para o problema do máximo $M(n, d)$, o estudo de limitantes inferiores e superiores tem merecido destaque e muitos limitantes tem se tornado conhecidos.

Todavia, ainda existe um intervalo significativo entre os limitantes inferiores e superiores para $M(n, d)$, sobretudo quando $d \rightarrow 0$ ou quando n cresce.

Naturalmente qualquer código conhecido \mathcal{C} , com os parâmetros M, n, d é um limitante inferior para $M(n, d)$.

No decorrer desta seção, apresentamos limitantes superiores e alguns dos principais métodos para construção de códigos esféricos.

1.2.1 Limitantes superiores

Sejam $x, y \in \mathcal{C}(M, n, d)$, dois pontos distintos de um código esférico com distância mínima d , o ângulo entre estes pontos é dado por $\cos^{-1}(\langle x, y \rangle)$. Como d é a distância mínima no código, então o ângulo de separação mínima, ou simplesmente ângulo mínimo entre seus pontos é

$$\theta = 2 \arcsin(d/2).$$

O conjunto dos pontos da esfera S^{n-1} cuja separação angular de um ponto $X \in S^{n-1}$ é ϕ é chamado chapéu esférico centrado em X e de ângulo ϕ . Este chapéu será denotado por

$$C_X(n, \phi) = \{y \in S^{n-1}; \langle x, y \rangle > \cos(\phi)\}.$$

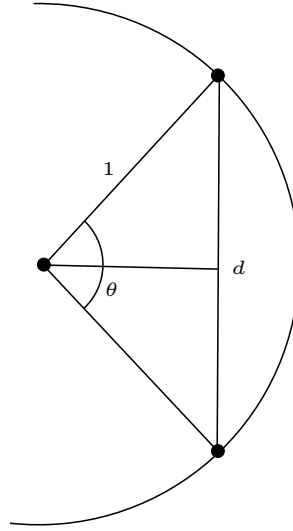


Figura 1.9: Relação entre distância mínima d e ângulo mínimo θ em um códigos esférico.

Se o ponto central do chapéu não for importante denotaremos simplesmente por $C(n, \phi)$. É possível demonstrar [16] que a área do chapéu esférico é

$$A(C(n, \phi)) = k_{n-1} \int_0^\phi (\sin \alpha)^{n-2} d\alpha, \text{ onde}$$

$$k_n = \begin{cases} \frac{(2\pi)^{n/2}}{(n-2)!!} & n = 2, 4, \dots \\ \frac{2 \cdot (2\pi)^{(n-1)/2}}{(n-2)!!} & n = 3, 5, \dots \end{cases} \quad (1.4)$$

$$n!! = \begin{cases} n(n-2)(n-4) \dots 1 & n \text{ ímpar} \\ n(n-2)(n-4) \dots 2 & n \text{ par} \end{cases}.$$

O Limitante da União

Assim como o argumento utilizado na discussão sobre o problema da 13ª esfera, os cálculos feitos acima permitem a obtenção de um limitante para o número de pontos de um código esférico. Um código com M pontos e distância mínima d implica em M chapéus esféricos disjuntos com ângulo $\theta/2$, onde θ satisfaz $d = 2 \sin \theta/2$, sobre a esfera. Logo, a área ocupada por esses chapéus é limitada superiormente pela área total da esfera. Segue portanto a proposição abaixo.

Proposição 1.2 *Limitante da União*

Seja um código esférico n -dimensional com M pontos e distância mínima $d = 2 \sin \theta/2$. Então, em termos do coeficiente k_n definido em 1.4, a seguinte desigualdade deve ser satisfeita:

$$M \leq \frac{A(C(n, \pi))}{A(C(n, \theta/2))} = \frac{k_n}{k_{n-1} \int_0^{\theta/2} \sin^{n-2} \alpha d\alpha}.$$

O Limitante de Tóth, Coxeter e Böröckzy

Um dos primeiros limitantes sobre códigos esféricos em \mathbb{R}^3 é devido a L. Fejes Tóth, 1943.

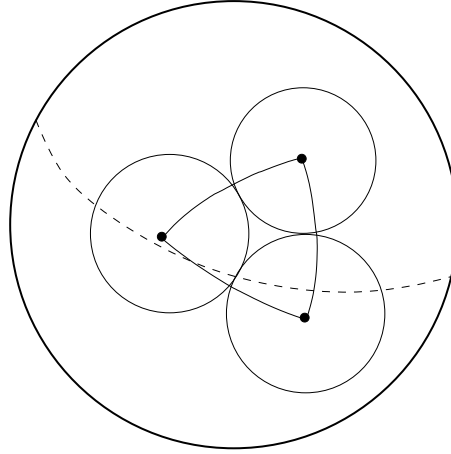


Figura 1.10: Três pontos na esfera S^2 com seus respectivos chapéus esféricos. O limitante de Tóth envolve estimativas para a área não ocupada pelos chapéus, interna ao triângulo formado pelos pontos.

Proposição 1.3 *Limitante de Tóth, [58, 17]*

Todo código esférico $\mathcal{C}(M, 3)$ tem ângulo mínimo θ satisfazendo

$$\theta \leq \cos^{-1} \left(\frac{\cot^2 \frac{M\pi}{6(M-2)}}{2} \right).$$

Este limitante é alcançado por códigos $\mathcal{C}(4, 3, \sqrt{8/3})$, $\mathcal{C}(6, 3, \sqrt{2})$ e $\mathcal{C}(12, 3, \sqrt{2 - 2/\sqrt{5}})$, o tetraedro regular, o octaedro e o icosaedro inscritos em S^2 . Sua construção utiliza estimativas sobre a área de triângulos esféricos.

Mais tarde, em 1963, Coxeter, disse ser “intuitivamente óbvio” que n esferas $(n-2)$ -dimensionais são empacotadas da melhor maneira possível quando cada uma toca todas, de maneira que seus centros são os n vértices do simplex regular. Ele se baseava nas ideias que Tóth utilizou para estabelecer o limitante para $n = 3$. Essa conjectura só foi resolvida 25 anos depois, em 1978, por Böröckzy [7]. Coxeter havia obtido como consequência da sua conjectura um limitante para códigos esféricos que, após a prova de Böröckzy, passou a ser chamado limitante de Böröckzy - Coxeter.

Proposição 1.4 *Limitante de Böröckzy - Coxeter*

Todo código esférico $C(n, M)$ tem ângulo mínimo θ e número de pontos M satisfazendo

$$M \leq \frac{2F_{n-1}(\alpha)}{F_n(\alpha)},$$

onde $\sec 2\alpha = \sec \theta + n - 2$ e $F_n(\alpha)$ é a função de Schläfli definida por

$$F_n(\alpha) = \frac{2^n U}{n \cdot n! V_n}$$

onde U é a área de um simplexo esférico regular de ângulo 2α contido em S^{n-1} e V_n é o volume da esfera S^{n-1} .

Infelizmente, o cálculo da área desses simplexos é muito complicado para $n > 3$ o que, na prática, torna o limitante Böröckzy - Coxeter difícil de manipular.

Os limitantes de Rankin

Em 1954, Rankin propôs alguns limitantes para códigos esféricos euclidianos que, além de fácil manipulação, possibilitaram demonstrar que duas classes de códigos esféricos, chamadas simplex e biortogonal, são ótimas. Nos limitaremos aqui a enunciar tais limitantes, uma referência mais completa sobre o assunto pode ser encontrada em [16] ou no próprio artigo do autor [45].

Proposição 1.5 *Limitante de Rankin I*

Todo código esférico $\mathcal{C}(M, n, d)$ satisfaz $d^2 \leq \frac{2M}{M-1}$.

Proposição 1.6 *Limitante de Rankin II*

Todo código esférico $\mathcal{C}(M, n, d)$, com $\sqrt{2} < d \leq 2$ satisfaz $M \leq n + 1$.

Proposição 1.7 *Limitante de Rankin III*

Todo código esférico $\mathcal{C}(M, n, d)$ com $d \geq \sqrt{2}$ satisfaz $M \leq 2n$.

Outros limitantes superiores para códigos esféricos

Kabatiansky e Levenshtein [31] utilizando programação linear mostraram que, para $0 < \theta < \frac{\pi}{2}$ e n suficientemente grande,

$$\frac{1}{n} \log_2 M(n, 2 \sin \frac{\theta}{2}) \leq \frac{1 + \sin \theta}{2 \sin \theta} \log_2 \left(\frac{1 + \sin \theta}{2 \sin \theta} \right) - \frac{1 - \sin \theta}{2 \sin \theta} \log_2 \left(\frac{1 - \sin \theta}{2 \sin \theta} \right) \quad (1.5)$$

O método de programação linear também possibilitou outras estimativas para $M(n, 2 \sin \theta/2)$. Delsart [14] mostrou que

$$M(n, 2 \sin \theta/2) \leq \frac{n(1 - \cos \theta)(2 + (n + 1) \cos \theta)}{1 - n \cos^2 \theta}. \quad (1.6)$$

Astola [2] obteve

$$M(n, 2 \sin \theta/2) \leq \frac{1}{2} n \log_e (n \cos \theta). \quad (1.7)$$

Existem ainda limitantes baseados na densidade Δ de empacotamentos em \mathbb{R}^n [10],

$$\Delta \leq (\sin \theta/2)^n M(n + 1, 2 \sin \theta/2), \text{ para } 0 \leq \theta \leq \pi.$$

e, também limitantes específicos para classes de códigos esféricos particulares, como, por exemplo, o limitante (2.2) [49] para códigos de grupo comutativo que será apresentado no Capítulo 2.

No entanto, não se conhece um limitante que tenha performance superior a todos outros. A comparação entre tais estimativas constituiu-se num interessante problema de pesquisa, cujas variáveis envolvem basicamente M e n .

A seguir, passamos ao outro lado da inequação, com o estudo de limitantes inferiores para $M(n, d)$.

1.2.2 Limitantes inferiores

Qualquer código esférico $\mathcal{C}(M, n, d)$ conhecido torna-se um limitante inferior para $M(n, d)$ ou para $d(M, n)$. A seguir descrevemos alguns dos principais métodos utilizados para a construção de códigos esféricos. Nos Capítulos 2 e 3 apresentamos nossa contribuição ao problema.

1.2.3 Códigos esféricos obtidos via empacotamentos

Uma maneira de se construir códigos esféricos consiste em considerar pontos em certas camadas de reticulados n -dimensionais e projetá-los na esfera unitária S^{n-1} (normalizar os vetores da camada). Formalmente, seja Λ um reticulado em \mathbb{R}^n com raio de empacotamento ρ . Denotaremos por P a origem do sistema de coordenadas, que pode ser escolhida convenientemente sobre um ponto de Λ ou em algum ponto do \mathbb{R}^n de forma a ficar equidistante de um certo número de pontos do reticulado. Suponha que existam M pontos em Λ cujos centros distam r de P e a menor distância entre dois quaisquer destes M pontos seja \hat{d} . Quando reescalados, os pontos desta camada formam um código esférico $\mathcal{C}(M, n)$ com distância mínima

$$d = \hat{d}/r. \quad (1.8)$$

Exemplo 1.4 Na Figura 1.11 temos as cinco primeiras camadas do reticulado hexagonal A_2 , com o ponto P na origem (ou sobre um ponto de A_2 , o que é equivalente). Cada uma dessas camadas definem um código esférico $\mathcal{C}(M, 2)$. Destas 5 camadas, somente os códigos com $M = 6$ pontos resultam num arranjo ótimo.

Exemplo 1.5 Consideremos os pontos do reticulado D_4 , com a origem P em um de seus pontos e distância mínima $\rho = 1/\sqrt{2}$. A primeira camada contém 24 pontos (kissing number) a distância de $\sqrt{2}$ de P . Após reescalar cada coordenada por $1/\sqrt{2}$, obtém-se um código esférico $\mathcal{C}(24, 4, 1)$.

O número de pontos de um reticulado que distam um certo valor r da origem é dado pela série theta de Λ . Apesar da série theta dos principais reticulados ser conhecida

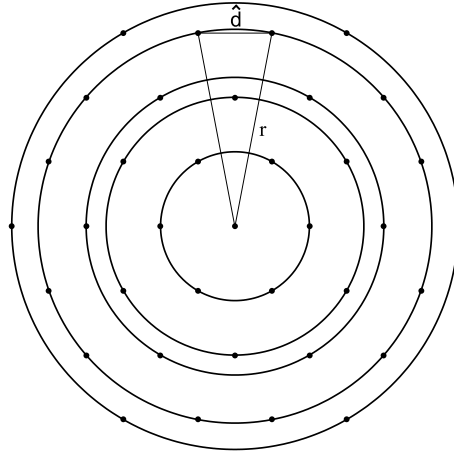


Figura 1.11: As cinco primeiras camadas do reticulado A_2 .

[10], não se sabe qual camada de um reticulado resultará em um bom código esférico. Além disso, em geral não se conhece uma fórmula explícita para a distância mínima entre os pontos numa dada camada. Claramente a distância mínima \hat{d} em cada camada é maior ou igual a distância mínima no reticulado todo, no entanto a distância mínima no código esférico (1.8) depende também de r , ou seja do quanto estes pontos estão afastados da origem.

Exemplo 1.6 O reticulado D_3 tem distância mínima $d = \sqrt{2}$. Na primeira camada de D_3 existem 12 pontos cuja distância mínima entre eles é $\hat{d} = \sqrt{2}$. Estes pontos formam um código esférico $\mathcal{C}(12, 3, 1)$, o qual não é ótimo para $M = 12$ e $n = 3$. Como já foi dito, o melhor código $\mathcal{C}(12, 3)$ tem distância mínima $d = \sqrt{2 - 2/\sqrt{5}} \approx 1.05146$ e é obtido inscrevendo-se um icosaedro regular em S^2 . As Figuras 1.12 e 1.13 ilustram a diferença destes arranjos de pontos em termos dos chapéus esféricos.

Uma pergunta natural é: Existe um ponto P em \mathbb{R}^3 tal que existam 12 vetores do reticulado D_3 equidistante de P que, após projetados numa esfera unitária centrada em P , determinam um icosaedro regular. Em outras palavras, o código ótimo $\mathcal{C}\left(12, 3, \sqrt{2 - 2/\sqrt{5}}\right)$ pode ser obtido reescalando 12 vetores do reticulado D_3 ?

Exemplo 1.7 Na segunda camada de D_3 existem 6 pontos a distância 2, logo pode-se construir um código esférico $\mathcal{C}(6, 3, \sqrt{2})$ que, neste caso, é um código ótimo (o código bi-ortogonal). Procedendo de maneira análoga para as cinco primeiras camadas de D_3 ,

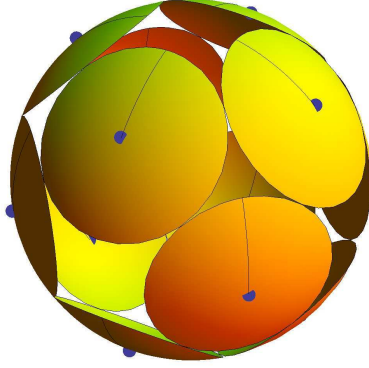


Figura 1.12: Doze chapéus esféricos sobre S^2 com centros nos vetores de norma mínima do reticulado D_3 .

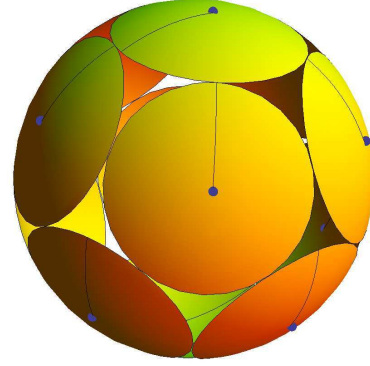
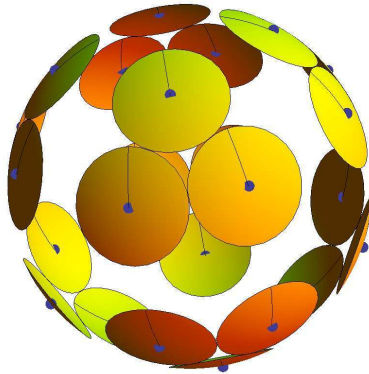
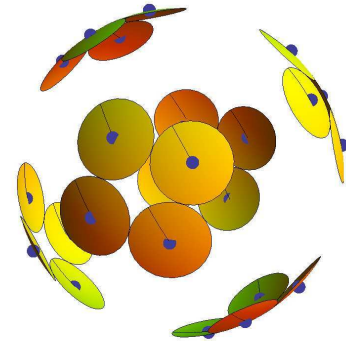


Figura 1.13: Doze chapéus esféricos sobre S^2 com centros nos vértices de um icosaedro regular inscrito em S^2 .

podemos obter códigos esféricos com 12, 6, 24, 12, 24 pontos respectivamente. É relevante observar que os dois códigos com 24 pontos que aparecem na lista não são equivalentes. O primeiro, formado pelos vetores de D_3 com norma igual a $\sqrt{6}$, resultam no código esférico $\mathcal{C}(24, 3, 1/\sqrt{3})$, enquanto o segundo, formado pelos 24 vetores de D_3 com norma igual a $\sqrt{10}$, resultam no código esférico $\mathcal{C}(24, 3, 1/\sqrt{5})$. A Figura 1.14 ilustra essa diferença. Pode-se notar pelas Figuras que ambos códigos não são ótimos.



$\mathcal{C}(24, 3, 1/\sqrt{3})$ obtido normalizando os vetores da 3ª camada do reticulado D_3 .



$\mathcal{C}(24, 3, 1/\sqrt{5})$ obtido normalizando os vetores da 5ª camada do reticulado D_3 .

Figura 1.14: Códigos esféricos $\mathcal{C}(24, 3)$ obtidos do reticulado D_3 .

Apesar de existirem muitos trabalhos interessantes sobre a obtenção de códigos esféricos via camadas de reticulados, mais notavelmente [51], esta técnica ainda apresenta

deficiências para a abordagem do problema geral de encontrar o melhor código $\mathcal{C}(M, n)$. Na prática, o cálculo da distância mínima entre os pontos das camadas é difícil, a escolha adequada da localização da origem P pode alterar a função theta do reticulado, e o número de pontos nas camadas pode tornar-se desconhecido. Além disso, esta construção só permite a solução para algumas cardinalidades M .

1.2.4 Códigos esféricos obtidos de códigos binários

É possível obter-se um código esférico de um código binário de comprimento n , bastando substituir cada 0 por 1 e cada 1 por -1 e depois normalizar o vetor resultante, dividindo-o por $\frac{1}{\sqrt{n}}$. Se a distância mínima no código binário (distância de Hamming) é igual a d_H , então a correspondente distância euclidiana mínima será

$$d = 2\sqrt{d_H/n}.$$

Por exemplo, o código binário formado pelas palavras (01111101) e (11110000) resulta no código esférico formado pelos pontos $\frac{1}{\sqrt{8}}(1, -1, -1, -1, -1, -1, 1, -1)$ e $\frac{1}{\sqrt{8}}(-1, -1, -1, -1, 1, 1, 1, 1)$. Neste caso, a distância de Hamming $d_H = 4$ corresponde a distância euclidiana $d = \sqrt{2}$.

Como o número máximo de pontos num código binário de comprimento n é limitado por 2^n , esta técnica impede a construção de códigos esféricos com cardinalidade $M \geq 2^n$.

No entanto, a relação entre códigos esféricos e binários pode ser explorada através de diferentes óticas. Por exemplo, considerando apenas códigos lineares, a cota de Singleton implica que, num código linear binário de comprimento n e cardinalidade M , a distância de Hamming satisfaz

$$d_H \leq 1 + n - \log_2 M,$$

usando $d = 2\sqrt{d_H/n}$, obtêm-se um limitante para o número de pontos M de um código esférico construído via códigos binários lineares

$$M \leq 2^{k(1-d^2/4)+1}.$$

1.2.5 Códigos obtidos via métodos de otimização

O problema de encontrar códigos esféricos com maior distância mínima possível via métodos de otimização é um exemplo de problema *multimodal* [42] (existem muitos pontos de otimalidade local e também muitos pontos de otimalidade global). Esta característica dificulta sua abordagem via métodos de minimização local e o uso de técnicas de otimização global implicam num aumento considerável de esforço computacional. Não obstante, alguns dos melhores códigos esféricos conhecidos [53], foram obtidos via métodos de otimização, sobretudo para pequenos valores de M ($M \leq 130$) em dimensões baixas ($n \leq 5$).

A formulação mais simples do problema consiste em

$$\begin{aligned} & \max \min_{x_i \neq x_j} ||x_i - x_j|| \\ \text{Suj. a } & ||x_k|| = 1 \quad k = 1, 2, \dots, M. \end{aligned}$$

Uma formulação alternativa consiste escrevê-lo em termos do produto interno euclidiano

$$\begin{aligned} & \min \max_{i \neq j} \langle x_i, x_j \rangle \\ \text{Suj. a } & ||x_k|| = 1 \quad k = 1, 2, \dots, M. \end{aligned}$$

Inspirado em [34], podemos aplicar o artifício clássico para transformar problemas de minimax em problemas de minimização adicionando-lhe restrições de desigualdades,

$$\begin{aligned} & \min \quad z \\ \text{Suj. a } & \quad z \geq \langle x_i, x_j \rangle \quad \forall i \neq j \\ & ||x_k|| = 1, \quad k = 1, 2, \dots, M. \end{aligned} \tag{1.9}$$

Adicionando variáveis de folga ao primeiro conjunto de restrições e modificando o segundo conjunto a fim de eliminar não suavidades na primeira derivada, tem-se o seguinte problema de programação não linear

$$\begin{aligned}
 \min \quad & z \\
 \text{Suj. a: } \quad & z - \langle x_i, x_j \rangle - w_{i,j} = 0 \quad \forall i \neq j \\
 & \langle x_k, x_k \rangle = 1, \quad k = 1, 2, \dots, M \\
 & w \geq 0.
 \end{aligned} \tag{1.10}$$

Como o número de restrições em (1.10) está diretamente associado ao número de pontos no código, o custo computacional para resolver o problema cresce muito rapidamente e, pode tornar-se impeditivo se a quantidade de pontos for moderadamente grande.

Existe uma vasta gama de métodos de otimização para resolver (1.10), inclusive abordagens baseadas em heurísticas, tais como *simulated annealing*, *busca tabu* e outros métodos de otimização discreta que tem obtido significativo sucesso na obtenção de bons códigos esféricos [42]. Vários dos melhores códigos esféricos conhecidos [53] foram obtidos em [33] utilizando funções de custo que modelam um sistema de repulsão de energia, por exemplo

$$C(X) = \sum_{1 \leq i < j \leq M} \left(\frac{\lambda}{\|x_i - x_j\|^2} \right)^m,$$

onde λ é um fator de escala e m um inteiro positivo escolhidos convenientemente para acelerar a convergência dos métodos.

A rigor, códigos obtidos via métodos de otimização podem ter distâncias mínimas potencialmente maiores que os obtidos por outras técnicas. Porém, em geral, tais códigos não possuem nenhuma estrutura (simetria, homogeneidade) associada o que, para aplicações como a transmissão de sinais sobre um canal gaussiano, constitui-se numa importante desvantagem. Para fins de codificação e decodificação, é desejável que os pontos do código sejam facilmente gerados, além de possuírem características que reduzam a complexidade nestes processos.

1.3 Códigos esféricos com distâncias assintoticamente pequenas

As técnicas apresentadas até aqui permitem construir códigos esféricos apenas para alguns valores de M ou, dito de outra forma, não permitem a construção de códigos esféricos para distâncias assintoticamente pequenas, $d \rightarrow 0$.

Nesta seção, apresentamos os três principais métodos para construção de códigos esféricos para qualquer distância mínima d . No terceiro capítulo trazemos nossa contribuição para este problema.

1.3.1 Códigos esféricos *apple-peeling*

Em [15], El Gamal et. al. descrevem o uso da heurística *Simulated Annealing* para a construção de códigos esféricos e apresentam alguns códigos obtidos. Como critério de comparação de seus resultados, os autores descrevem, no apêndice daquele artigo, um método para alocação de pontos na superfície da esfera unitária e derivam um limitante inferior para $M(n, d)$. Curiosamente o resultado do anexo se mostraria mais relevante do que propriamente o conteúdo do artigo.

A maneira de alocar os pontos em [15] lembra a técnica utilizada para se descascar uma maçã², por isso, o denominaram de *apple-peeling code*.

A construção de um código apple-peeling $\mathcal{C}_A(M, n, d)$ é feita de maneira recursiva a partir de um código esférico $\mathcal{C}^*(M, n - 1, d)$ na dimensão anterior.

Seja $\mathcal{C}^*(M, n - 1, d)$ um código esférico $(n - 1)$ -dimensional com ângulo mínimo $\theta = 2 \arcsin(d/2)$. O código *apple-peeling* $\mathcal{C}_A(M, n, d)$ com respeito a $\mathcal{C}^*(M, n - 1, d)$ é o conjunto de pontos

$$\{(x_1(i, j) \cos \eta(i), \dots, x_{n-1}(i, j) \cos \eta(i), \sin(\eta(i)))\}$$

² No Brasil é mais comum descascar laranjas com essa técnica.

onde

$$\begin{aligned} i &\in \{l \in \mathbb{Z} : -\pi/2 \leq \eta(l) \leq \pi/2\} \\ j &\in \{1, \dots, M\} \\ \eta(j) &\equiv (i + 1/2)\theta \\ x(i, j) &= (x_1(i, j), \dots, x_{n-1}(i, j)) \text{ é o } j\text{-ésimo ponto de } \mathcal{C}^*(M, n-1, d). \end{aligned}$$

Em [15] é demonstrado que $\mathcal{C}_A(M, n, d)$ tem, de fato, distância mínima igual a d .

Somando sobre todos os possíveis valores de i , pode-se estabelecer o seguinte limite inferior para o número de pontos em um código esférico $\mathcal{C}(M, n, 2 \sin \theta/2)$.

Teorema 1.1 [15] *Para $0 \leq \theta \leq \pi$ e $n \geq 3$, existe um código esférico $\mathcal{C}(M, n, 2 \sin(\theta/2))$ que satisfaz*

$$M \geq 2 \sum_{i=0}^{\lceil \frac{\pi}{2\theta} - \frac{1}{2} \rceil} M \left(n-1, \arccos^* \left(\frac{\cos \theta - \sin^2((i + 1/2)\theta)}{\cos^2((i + 1/2)\theta)} \right) \right),$$

onde

$$\arccos^*(x) = \begin{cases} \arccos(x), & \text{se } -1 \leq x < 1 \\ 2\pi, & \text{se } x < -1 \end{cases}.$$

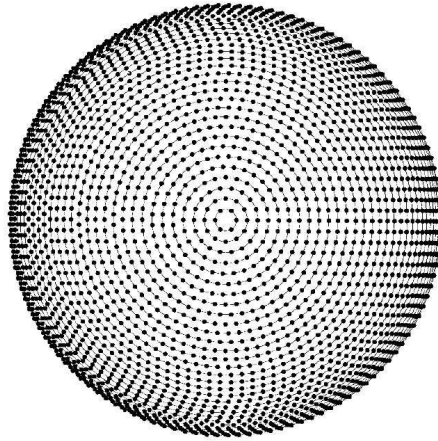


Figura 1.15: Exemplo de um código esférico $\mathcal{C}_A(4764, 3, 0.05)$.

Se $d \rightarrow 0$, o número de pontos em qualquer código esférico pode naturalmente aumentar. Para distâncias assintoticamente pequenas pode-se colocar um número arbitrariamente grande de pontos sobre S^{n-1} . Por exemplo, fazendo $d \rightarrow 0$ é possível construir códigos esféricos $\mathcal{C}(M, n, d)$, com $M \rightarrow \infty$, alocando os pontos apenas sobre um círculo máximo de S^{n-1} . No entanto, fazendo isso, estamos utilizando uma região muito pequena da superfície da esfera unitária.

Uma medida da eficiência da técnica utilizada para construir uma código $\mathcal{C}(M, n, d)$ consiste em analisar a *densidade do código*

$$\Delta_{\mathcal{C}}(M, n, d) = \frac{M \cdot A(C(n, \arcsin d/2))}{A(S^{n-1})}.$$

ou seja, a proporção da “área da superfície” de S^{n-1} que é ocupada pelos chapéus esféricos centrados nos pontos do código, com separação angular

$$\phi = \frac{\theta}{2} = \arcsin d/2.$$

Quando $d \rightarrow 0$, é intuitivo esperar que

$$\Delta_{\mathcal{C}}(M, n, d) \rightarrow \Delta(n-1),$$

onde $\Delta(n-1)$ é a densidade do melhor empacotamento esférico $(n-1)$ -dimensional³. Por exemplo, o melhor empacotamento de moedas de um centavo sobre a superfície da terra deve se parecer muito com o empacotamento do reticulado hexagonal A_2 no plano.

Baseados nesta idéia, Hamkins e Zeger [25, 26] apresentam duas famílias de códigos que são assintoticamente densas na esfera, i.e., $\Delta_{\mathcal{C}}(M, n, d) \rightarrow \Delta(n-1)$, quando $d \rightarrow 0$.

1.3.2 Códigos *wrapped*

Em [25], Hamkins e Zeger definem uma aplicação de $\mathbb{R}^{n-1} \mapsto \mathbb{R}^n$ que projeta “(embrulha)” um subconjunto finito de pontos de um empacotamento esférico $(n -$

³ Uma prova formal deste fato é dada em [25].

1)–dimensional na superfície de S^{n-1} . O resultado é a construção de um código esférico denominado *wrapped*. Apresentamos a seguir um resumo sobre a construção deste código.

Seja Λ um empacotamento esférico em \mathbb{R}^{n-1} com distância mínima d e densidade Δ_Λ . Define-se como a *latitude* de um ponto $x = (x_1, \dots, x_n)$ por $l_x = \arcsin(x_n)$, i. e., o ângulo entre o “equador” e x . Seja $0 = \alpha_0 < \alpha_1 < \dots < \alpha_N = 1$ uma sequência de latitudes de fronteira. O i –ésimo anel A_i é definido como o conjunto de pontos $x = (x_1, \dots, x_n) \in S^{n-1}$ que satisfazem $\alpha_i \leq \arcsin x_n < \alpha_{i+1}$, isto é, o conjunto de pontos entre duas latitudes consecutivas. Os números α_j devem ser escolhidos convenientemente para proporcionar a maior quantidade de pontos possível no código. O i –ésimo *anel* é definido como o conjunto de pontos $x = (x_1, \dots, x_n) \in S^{n-1}$ que satisfazem $\xi_i \leq x_n < \xi_{i+1}$, isto é, o conjunto de pontos entre duas latitudes consecutivas.

Para cada i , define-se uma aplicação $f_i : A_i \mapsto \mathbb{R}^{n-1}$ como segue.

Para cada $x = (x_1, \dots, x_n) \in A_i$, seja

$$\mathcal{C}_W(M, n, d) = \bigcup_i f_i^{-1}(\Lambda \setminus \{0\}) \setminus B.x_L = \arg \min_z \{ \|x - z\| : z = (z_1, \dots, z_{n-1}, \sin \alpha_i) \in S^{n-1} \}, \quad (1.11)$$

i.e., o ponto de S^{n-1} que mora na fronteira entre os anéis A_{i-1} e A_i e está mais próximo de x , conforme ilustrado na Figura 1.16.

Seja $x' = (x_1, \dots, x_{n-1})$ o ponto obtido de x suprimindo-lhe a última coordenada. A função f_i é definida por

$$f_i(x) = \frac{x'}{\|x'\|} (\|(x_L)'\| - \|x_L - x\|)_+,$$

onde $(x)_+ = \max(0, x)$.

Seja

$$B_i = \{x \in A_i : \|x - x_L\| < d\}.$$

O código esférico denominado *wrapped* com respeito ao empacotamento Λ é definido como

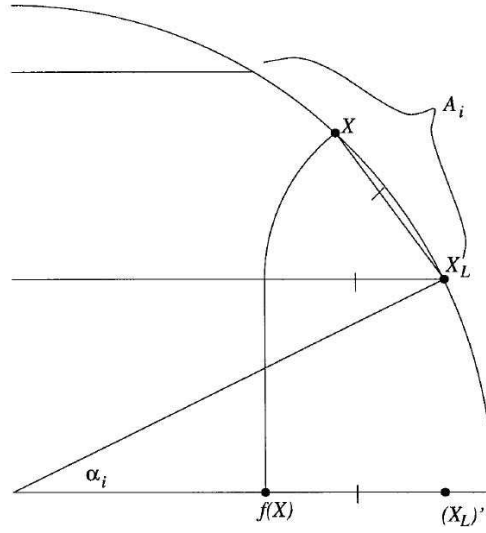


Figura 1.16: Interpretação geométrica de f_i [25].

$$\mathcal{C}_W(M, n, d) = \bigcup_i f_i^{-1}(\Lambda \setminus \{0\}) \setminus B. \quad (1.12)$$

A Figura 1.17 mostra parte de um $\mathcal{C}_W(4802, 3, 0.05)$.

Em [25] é demonstrado que, se o empacotamento Λ tem distância mínima d , então o código $\mathcal{C}_W(M, n)$ também terá distância mínima d . Além disso, $\Delta_{\mathcal{C}_W} \rightarrow \Delta(n-1)$, quando $d \rightarrow 0$, ou seja, o código esférico $\mathcal{C}_W(M, n)$ é assintoticamente denso na esfera.

É importante observarmos que, para a construção de um $\mathcal{C}_W(M, n)$, faz-se necessário uma cuidadosa definição das latitudes α_i que definirão os anéis A_i . Além disso, a obtenção de cada ponto do código exige a solução do problema de minimização (1.11). Ou seja, apesar de terem performance excelente quando $d \rightarrow 0$, a construção de um $\mathcal{C}_W(M, n, d)$ para uma fixada distância mínima d , pode envolver um considerável esforço matemático e computacional.

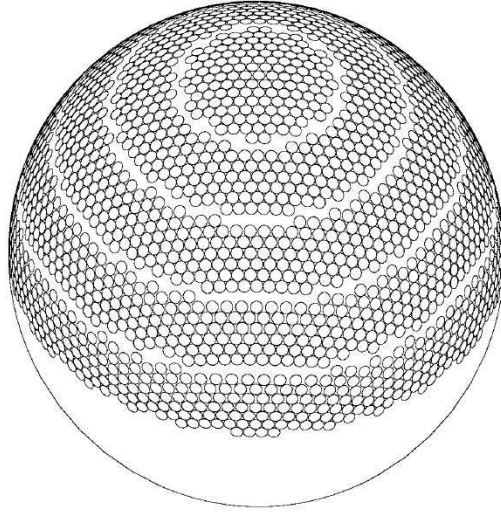


Figura 1.17: Código esférico $\mathcal{C}_W(M, 3, 0.05)$ [25].

1.3.3 Códigos esféricos laminados

A segunda família de códigos esféricos construída por Hamkins e Zeger [26], utiliza uma ideia análoga a construção de reticulados laminados [10], daí sua denominação *códigos esféricos laminados*⁴.

Novamente os pontos são alocados em anéis na superfície de S^{n-1} , porém, o preenchimento de cada anel é feito utilizando um código esférico da dimensão anterior $\mathcal{C}(M, n-1, d)$, enquanto os códigos wrapped utilizam um subconjunto de empacotamento esférico em \mathbb{R}^{n-1} .

A construção de um código esférico laminado, conforme apresentada em [26], utiliza uma série de aplicações e detalhes que omitiremos aqui.

Geometricamente os códigos laminados se parecem bastante com os códigos apple-peeling, com uma sutil e importante distinção. No código apple-peeling, os pontos também são alocados em camadas (ou anéis) sobre S^{n-1} . No entanto, não existe a preocupação em “encaixar”, em entrelaçar, duas camadas consecutivas. Na construção dos códigos laminados, duas camadas consecutivas dentro do mesmo anel, são construídas de modo que fiquem perfeitamente encaixadas, ou entrelaçadas. Esta diferença é fundamental para a obtenção de códigos esféricos densos, sobretudo quando $d \rightarrow 0$. A

⁴ Traduzido do termo original em inglês *laminated spherical codes*.

diferença entre a densidade dos códigos apple-peeling e os laminados é semelhante a diferença entre a densidade dos reticulados \mathbb{Z}^n e os laminados Λ_n . Como é conhecido, \mathbb{Z}^n tem densidade bem inferior a Λ_n quando n cresce.

A Figura 1.18 apresenta uma comparação entre os códigos esféricos apple-peeling, wrapped e laminados em \mathbb{R}^3 para a distância mínima $d = 0.05$. O código apple-peeling possui 4764 pontos, o wrapped 4802 e laminado 5244 pontos.

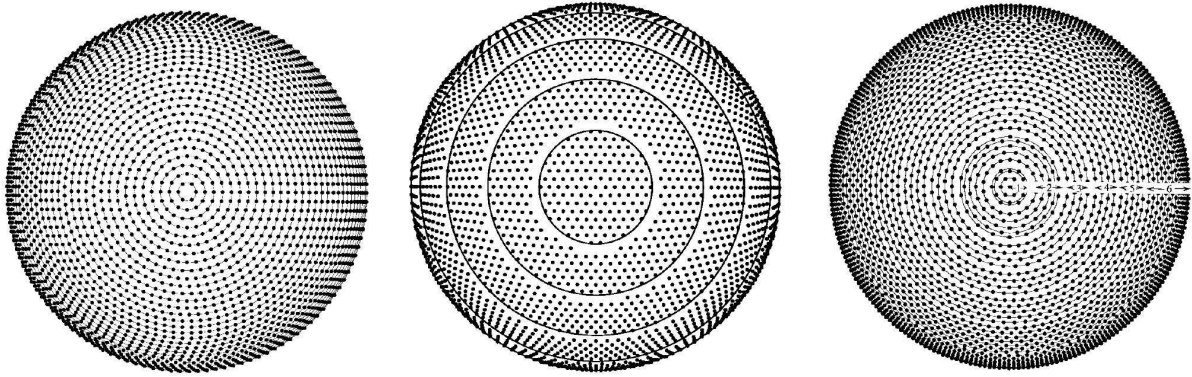


Figura 1.18: Comparação entre códigos esféricos apple-peeling, wrapped e laminados. Da esquerda para a direita, tem-se, $\mathcal{C}_A(4764, 3, 0.05)$, $\mathcal{C}_W(4802, 3, 0.05)$ e $\mathcal{C}_L(5244, 3, 0.05)$.

É demonstrado em [26] que os códigos esféricos laminados, assim como os wrapped, são assintoticamente densos em S^{n-1} . No entanto, a construção de um $\mathcal{C}_L(M, n, d)$ depende, além do conhecimento de um $\mathcal{C}(M, n-1, d)$, da definição criteriosa dos anéis em S^{n-1} e de uma série de aplicações para intercalar as camadas, o que, na prática, pode demandar um alto esforço computacional.

Os códigos esféricos em camadas de toros, que estamos introduzindo no Capítulo 3 têm, para certas distâncias mínimas, desempenho melhor que os três códigos citados nesta seção, com a vantagem de serem mais facilmente gerados. Em cada uma das camadas desses códigos os pontos são gerados como órbita de um grupo comutativo de matrizes ortogonais, que estão associados a reticulados na dimensão metade.

Embora os códigos que propomos não sejam assintoticamente densos na esfera unitária, como os laminados e wrapped, sua densidade pode se aproximar da densidade de um produto cartesiano de reticulados densos (Conjectura 3.1). Além disso, a forte estrutura associada a estes códigos permite importantes vantagens na sua construção,

assim como na codificação/decodificação dos mesmos. Outra potencial vantagem é que um código esférico em camadas de toros pode ser mais facilmente construído para uma dada distância d e, como mostrado na Tabela 3.6, tais códigos podem ter performance superior aos melhores códigos estruturados que são conhecidos, sobretudo para valores de d que não são arbitrariamente pequenos.

Códigos provenientes de reticulados, ou mais especificamente, códigos de grupo, merecem atenção especial. No capítulo 2 apresentamos uma técnica para a obtenção de uma classe de códigos esféricos com forte estrutura algébrica e geométrica, os denominados códigos de grupo comutativo. Nestes códigos os pontos são gerados como órbita de um vetor inicial x_0 sob a ação de um grupo comutativo de matrizes ortogonais.

CÓDIGOS DE GRUPO COMUTATIVO

Neste Capítulo estudamos códigos esféricos gerados como órbita de um vetor unitário sob a ação de um grupo comutativo de matrizes ortogonais, os denominados códigos de grupo comutativo. Nossa primeira contribuição neste Capítulo consiste em estabelecer a solução do problema do vetor inicial para códigos de grupo comutativo como um problema de programação linear, estendendo as idéias que Biglieri e Elia utilizaram para resolver este problema para códigos de grupo cíclico [5].

Na Seção 2.3 concentram-se os principais resultados deste Capítulo, que culminam com o desenvolvimento de um método para a procura do melhor código de grupo comutativo, fixados a dimensão e o número de pontos. O método que desenvolvemos aqui baseia-se na associação entre tais códigos na dimensão $2k$ e reticulados k -dimensionais conforme estudada em [12, 49, 62]. Utilizamos fatorações matriciais conhecidas, como as formas normais de Hermite e Smith, para reduzir o número de casos a serem analisados através da identificação de códigos isométricos que podem ser descartados. Os resultados desta Seção foram incorporados no artigo [57], submetido para publicação em fev-2008.

Para finalizar, na Seção 2.6 mostramos que a decodificação de um código de grupo comutativo $2k$ -dimensional pode ser feita utilizando diagramas de treliça de reticulados k -dimensionais e apresentamos algoritmo para esta decodificação. A complexidade de decodificação de um código de grupo comutativo $2k$ -dimensional é equivalente a

complexidade de decodificação num reticulado k -dimensional que possui um diagrama de treliça finito. Alguns resultados deste estudo constam no trabalho [18].

2.1 Códigos de grupo comutativo

Um código de grupo comutativo é um código esférico obtido pela ação de um grupo comutativo de matrizes ortogonais sobre um vetor inicial unitário.

De forma mais precisa, seja \mathcal{O}_n o grupo multiplicativo de matrizes ortogonais de ordem $n \times n$ e $G(M, n)$ um subgrupo comutativo de ordem M em \mathcal{O}_n .

Um *código de grupo comutativo* $\mathcal{C}_G(M, n)$ é um conjunto de M vetores unitários, não contidos em um hiperplano, que são órbita de um vetor x_0 da esfera unitária $S^{n-1} \subset \mathbb{R}^n$ por um dado $G(M, n)$, isto é,

$$\mathcal{C}_G(M, n) = \{G_1x_0, G_2x_0, \dots, G_Mx_0\}.$$

Códigos de grupo comutativos fazem parte de uma classe mais ampla denominada *códigos geometricamente uniformes*. Essa classe, introduzida por Forney em [23], caracteriza-se pela existência de uma isometria do espaço que leva uma palavra do código à outra, o que, no caso dos $\mathcal{C}_G(M, n)$, é uma imediata consequência da definição.

Para aplicações na transmissão de sinais através de um canal Gaussiano, códigos geometricamente uniformes possuem importantes vantagens. Como observou Forney em [20], “as propriedades do código são as mesmas em cada ponto”, as regiões de decisão, o perfil de distâncias, o número de vizinho é igual para qualquer palavra do código, em particular para o vetor inicial.

Como é usual, a *distância mínima* em $\mathcal{C}_G(M, n)$ é definida por

$$d = \min_{\substack{x, y \in \mathcal{C}_G \\ x \neq y}} \|x - y\|,$$

Quando necessário, a notação $\mathcal{C}_G(M, n, d)$ será usada para se referir à um $\mathcal{C}_G(M, n)$ com distância mínima igual a d .

Para um dado $G(M, n)$, a distância mínima no código $\mathcal{C}_G(M, n)$ pode variar consideravelmente em função da escolha do vetor inicial x_0 . Um dos problemas clássicos em códigos de grupo consiste em, fixado um grupo de matrizes $G(M, n)$, encontrar o vetor inicial x_0 que maximiza a distância mínima em $\mathcal{C}_G(M, n)$. Esse problema, denominado *problema do vetor inicial* (PVI), ainda não está resolvido para o caso geral (códigos de grupo quaisquer), mas foi estudado em alguns importantes casos. Na Seção 2.2 mostramos que, para códigos de grupos comutativos, o PVI é equivalente a um problema de programação linear.

Não obstante, o interesse principal desse Capítulo é o que se pode considerar uma generalização do problema do vetor inicial:

- Dentre todos os códigos de grupo comutativos $\mathcal{C}_G(M, n, d)$ qual é aquele que possui a maior distância mínima d ?

Tal código é denominado *ótimo* para os parâmetros M e n . Precisamente, dizemos que um $\mathcal{C}_G(M, n, d)$ é *ótimo* se d é maior ou igual que a distância mínima de qualquer outro $\mathcal{C}_G(M, n)$. No estudo deste problema, estão envolvidas todas as possíveis representações matriciais de um grupo abeliano de ordem M em \mathcal{O}_n , além da solução do problema do vetor inicial para cada uma delas.

Um resultado conhecido sobre a representação irredutível de um grupo finito de matrizes ortogonais $G(M, n)$ é estabelecido no seguinte Teorema:

Teorema 2.1 ((Teorema 12.1, [24])) *Todo elemento G_i em um grupo comutativo de matrizes ortogonais pode ser escrito, através de uma mesma matriz ortogonal Q , na seguinte forma pseudo diagonal:*

$$Q^T G_i Q = \text{diag}[R_1(i), \dots, R_k(i), \mu(i)_{2k+1}, \dots, \mu(i)_n]_{n \times n}, \quad (2.1)$$

$$\text{onde } R_j(i) = \begin{pmatrix} \cos(\frac{2\pi b_{ij}}{M}) & -\sin(\frac{2\pi b_{ij}}{M}) \\ \sin(\frac{2\pi b_{ij}}{M}) & \cos(\frac{2\pi b_{ij}}{M}) \end{pmatrix},$$

$$b_{ij} \in \mathbb{Z} \text{ and } \mu(i)_l = \pm 1, l = 2k + 1, \dots, n$$

Esta maneira de escrever cada matriz em $G(M, n)$ na forma diagonal por blocos de rotação no plano será muito útil no decorrer deste Capítulo.

Outro resultado importante para a abordagem que será dada é a associação entre códigos de grupo de comutativos e reticulados, como estudado em [49].

A Proposição a seguir estabelece uma relação entre um código de grupo comutativo $\mathcal{C}_G(M, 2k)$ e um reticulado k -dimensional.

Proposição 2.1 ([49], p. 5) *Seja $\mathcal{C}_G(M, 2k)$ um código de grupo comutativo de ordem M , em dimensão par, com vetor inicial $u = (\delta_1, 0, \dots, \delta_k, 0)$. Se $2k = n$ em (2.1), isto é, os elementos de $G(M, n)$ são livres de blocos 2×2 de reflexão, então a imagem inversa $\psi^{-1}(\mathcal{C}_G(M, n))$ é um reticulado Λ gerado por k vetores da forma*

$$v_i = \left(\frac{2\pi b_{i1}\delta_1}{M}, \frac{2\pi b_{i2}\delta_2}{M}, \dots, \frac{2\pi b_{ik}\delta_k}{M} \right), 1 \leq i \leq k,$$

que contém um subreticulado Λ' gerado por k vetores da forma

$$w_i = 2\pi\delta_i e_i, 1 \leq i \leq k,$$

onde e_i são os vetores canônicos do \mathbb{R}^n e

$$\psi(y) = \left(\delta_1 \cos\left(\frac{y_1}{\delta_1}\right), \delta_1 \sin\left(\frac{y_1}{\delta_1}\right), \dots, \delta_k \cos\left(\frac{y_k}{\delta_k}\right), \delta_k \sin\left(\frac{y_k}{\delta_k}\right) \right)$$

é a parametrização canônica de um toro planar¹.

O seguinte limitante também será utilizado para propósitos comparativos.

Proposição 2.2 ([49], p. 5) *Todo código de grupo comutativo em \mathbb{R}^{2k} de ordem M , livre de blocos 2×2 de reflexão, com distância mínima d e vetor inicial $(u_1, u_2, \dots, u_{2k})$ satisfaz*

$$M \leq \frac{\pi^k \sqrt{\prod_{i=1}^k (u_{2i-1}^2 + u_{2i}^2)} \Lambda_k}{(\arcsin \frac{d}{4})^k} \leq \frac{\pi^k \Lambda_k}{(\arcsin \frac{d}{4})^k k^{k/2}}, \quad (2.2)$$

onde Λ_k é a máxima densidade de centro de um empacotamento reticulado em \mathbb{R}^k .

¹ Toros planares são apresentados na Seção 3.1, por enquanto não necessitaremos nada além da aplicação ψ .

2.2 Problema do vetor inicial em códigos de grupo comutativo

Dado um grupo $G(M, n)$ deseja-se encontrar $x \in S^{n-1}$ que resolve:

$$\max_{x \in S^{n-1}} \left(\min_{G_i \neq I_n} \|G_i x - x\|^2 \right)$$

A abordagem desenvolvida aqui é baseada no estudo do problema do vetor inicial para códigos de grupo cíclico feita em [5] e também inspirada em [49].

Na sequência, mostramos que o problema do vetor inicial em $\mathcal{C}_G(M, n)$ é equivalente a um problema de programação linear (PL). Este PL, quando restrito ao caso cíclico, é equivalente ao apresentado em [5].

De acordo com (2.1), pode-se escrever

$$f_i(x) = \|G_i x - x\|^2 = 4 \sum_{j=1}^q (x_{2j-1}^2 + x_{2j}^2) \sin^2 \frac{\pi b_{i,j}}{M} + 4 \sum_{j=2q+1}^n (1 - \mu(i)_j)^2 x_j^2.$$

Considerando

$$y_j = \begin{cases} (x_{2j-1}^2 + x_{2j}^2) & , \text{ if } j = 1, \dots, q \\ x_{j+q}^2 & , \text{ if } j = q+1, \dots, n-q \end{cases},$$

tem-se

$$f_i(y) = 4 \sum_{j=1}^q y_j \left(\sin^2 \frac{\pi b_{i,j}}{M} \right) + 4 \sum_{j=q+1}^{n-q} y_j (1 - \mu(i)_{j+q})^2,$$

e, então

$$\max_{x \in S^{n-1}} (\min \|G_i x - x\|^2) = \max_{y \in S^{(n-q-1)}} (\min f_i(y)).$$

Este problema de *max min*, que é linear em y , pode ser convertido no seguinte problema de programação linear:

$$\max z$$

Sujeito a

$$\left\{ \begin{array}{l} z \leq f_i(y) \\ \sum_{k=1}^{n-q} y_i = 1 \\ y_i \geq 0 \\ z \geq 0 \end{array} \right. \quad (2.3)$$

Escrevendo (2.3) na forma padrão de um problema de programação linear, temos:

$$\min c^t w$$

Sujeito a

$$\left\{ \begin{array}{l} Aw \leq b \\ w \geq 0 \end{array} \right.$$

onde:

$$\begin{aligned} c^t &= (1, 0, \dots, 0) \in R^{n-q+1} \\ b^t &= (1, -1, 0, \dots, 0) \in R^{\lfloor \frac{M}{2} \rfloor + 2} \\ A &= \begin{pmatrix} 0 & 1 & \dots & 1 \\ 0 & -1 & \dots & -1 \\ 1 & -m_{1,1} & \dots & -m_{n-q,1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & -m_{1, \lfloor \frac{M}{2} \rfloor} & \dots & -m_{n-q, \lfloor \frac{M}{2} \rfloor} \end{pmatrix} \\ m_{i,j} &= (j - \text{ésimo}) \text{ coeficiente da função } f_i. \end{aligned}$$

Portanto, o problema do vetor inicial para códigos de grupo comutativo é equivalente a um problema de programação linear com $n - q + 1$ variáveis e $\lfloor \frac{M}{2} \rfloor + 2$ restrições.

2.3 Códigos de grupo comutativo ótimos

A procura pelo melhor código de grupo comutativo $\mathcal{C}_{\mathcal{G}}(M, n)$, para um dado número de pontos M e dimensão n , pode ser dividida em duas etapas. A primeira consiste em, fixados M e n , determinar o conjunto de todos os grupos $G(M, n)$ em \mathcal{O}_n . Em seguida, o problema do vetor inicial pode ser resolvido para cada caso utilizando o PL deduzido na Seção anterior. O código ótimo será aquele que tiver a maior distância mínima dentre todos os analisados.

Na prática, essa abordagem exaustiva do problema torna-se inviável. O número total de grupos finitos $G(M, n)$ em \mathcal{O}_n pode ser arbitrariamente grande, sua cardinalidade está relacionada com a *função de Euler* de M , ou seja, com o número de divisores de M . O número total de grupos $G(M, n)$ é da ordem de $\binom{M/2}{n/2}$ [5].

O problema complica-se dessa maneira porque mesmo grupos isomorfos necessitam ser analisados, dado que a distância mínima em $\mathcal{C}_{\mathcal{G}}$ pode variar, dependendo de qual representação matricial em \mathcal{O}_n é escolhida para cada grupo. Dois diferentes grupos finitos $G_1(M, n)$ e $G_2(M, n)$ relacionados ao mesmo grupo abstrato \mathcal{G} podem gerar códigos $\mathcal{C}_{\mathcal{G}}(M, n)$ *não isométricos*.

Por exemplo, sabemos que, a menos de isomorfismo, os grupos abstratos de ordem $M = 128$ são apenas

$$\mathcal{G} = \{\mathbb{Z}_{128}; \mathbb{Z}_2 \oplus \mathbb{Z}_{64}; \mathbb{Z}_4 \oplus \mathbb{Z}_{32}; \mathbb{Z}_8 \oplus \mathbb{Z}_{16}\}.$$

No entanto, para $n = \{4, 6, 8\}$, tem-se, respectivamente, $\{2016, 41664, 635376\}$ grupos $G(128, n)$ em \mathcal{O}_n .

Alguns grupos isomorfos geram códigos $\mathcal{C}_G(M, n)$ não isométricos. Por exemplo, considere dois grupos cíclicos $G(128, 4)$, gerados pelas matrizes $G_{(1,5,128)}$ e $G_{(1,10,128)}$, onde

$$G_{(a,b,M)} = \begin{pmatrix} \cos\left(\frac{a * 2\pi}{M}\right) & \sin\left(\frac{a * 2\pi}{M}\right) & 0 & 0 \\ -\sin\left(\frac{a * 2\pi}{M}\right) & \cos\left(\frac{a * 2\pi}{M}\right) & 0 & 0 \\ 0 & 0 & \cos\left(\frac{b * 2\pi}{M}\right) & \sin\left(\frac{b * 2\pi}{M}\right) \\ 0 & 0 & -\sin\left(\frac{b * 2\pi}{M}\right) & \cos\left(\frac{b * 2\pi}{M}\right) \end{pmatrix}. \quad (2.4)$$

Após resolver o problema do vetor inicial para ambos os grupos, obtém-se dois códigos: $\mathcal{C}_G(128, 4, 0.24)$ e $\mathcal{C}_G(128, 4, 0.38)$, que possuem distâncias mínimas diferentes, apesar de que $G_{(1,5,128)}$ e $G_{(1,10,128)}$ são duas representações para o mesmo grupo abstrato \mathbb{Z}_{128} .

Por outro lado, os grupos $G(128, 4)$, gerados por $G_{(1,5,128)}$ e $G_{(27,7,128)}$, produzem exatamente o mesmo código $\mathcal{C}_G(128, 4, 0.24)$.

Como será mostrado mais adiante, o melhor código de grupo comutativo $\mathcal{C}_G(128, 4)$ tem distância mínima igual a 0.4061.

Os resultados apresentados a seguir permitem identificar esses códigos isométricos e, então, resolver o PVI apenas para um conjunto relevante de grupos, os quais a menos de isometria na esfera, geram códigos idênticos.

No exemplo dado acima, ($M = 128$) após o descarte de códigos isométricos é necessário considerar apenas $\{71, 2539, 55789\}$ $G(128, n)$ grupos para $n = \{4, 6, 8\}$, respectivamente.

O primeiro Teorema que apresentamos (Teorema 2.4) é uma extensão de um clássico resultado de Hermite, daí sua denominação *Forma Normal de Hermite Estendida*. Especificamente, o que acrescentamos foi a possibilidade de considerar as colunas da matriz resultante de uma Forma Normal de Hermite ordenadas por máximo divisor comum (mdc).

Antes de prosseguirmos, vamos estabelecer de forma mais precisa a relação entre códigos de grupo comutativo e reticulados.

Seja Λ_T um reticulado em \mathbb{R}^k , gerado por uma matriz T , cujas linhas são formadas pelos vetores $\{t_1, t_2, \dots, t_k\}$. Seja Λ'_R um subreticulado ortogonal de Λ_T , gerado pelos vetores $\{r_1, r_2, \dots, r_k\}$, com $\langle r_i, r_j \rangle = 0 \forall i \neq j$. Como $\Lambda'_R \subset \Lambda_T$, existe uma matriz W , com coeficientes inteiros tal que

$$WT = R.$$

W é a matriz que expressa os vetores de R como combinação linear dos vetores de T .

Como vimos no Capítulo 1, o número de pontos M no quociente $\frac{\Lambda_T}{\Lambda_R}$ (que será o número de pontos no código de grupo comutativo) é determinado por

$$M = \left| \frac{\Lambda_T}{\Lambda_R} \right| = \frac{\det(R)}{\det(T)} = \det(W).$$

Qualquer ponto $x \in \Lambda_T$ pode ser escrito na base R , da seguinte forma

$$x = \frac{1}{M} \sum_{i=1}^k a_{ij} r_i,$$

Para tanto, basta verificar que, como $WT = R$ temos $T = W^{-1}R$. Denotando por A a transposta da matriz dos cofatores de W , temos que a base T de Λ pode ser escrita na forma $T = \frac{1}{M}BR$.

O conjunto X de todos os pontos de Λ_T escritos na base R , com coeficientes $0 \leq a_{ij} \leq M$, tem exatamente M pontos, que pertencem ao paralelepípedo retangular definidos pelos vetores r_i . Identificando os lados opostos deste paralelepípedo temos um toro planar de raios $\|r_i\|$, que mora numa esfera do \mathbb{R}^{2k} de raio $\rho = \sum_{i=1}^k \|r_i\|^2$.

A imagem de X pela aplicação

$$\psi(y) = \left(\|r_1\| \cos\left(\frac{y_1}{\|r_1\|}\right), \|r_1\| \sin\left(\frac{y_1}{\|r_1\|}\right), \dots, \|r_k\| \cos\left(\frac{y_k}{\|r_k\|}\right), \|r_k\| \sin\left(\frac{y_k}{\|r_k\|}\right) \right)$$

define um código de grupo comutativo em \mathbb{R}^{2k} com vetor inicial $x_0 = (\|r_1\|, \|r_2\|, \dots, \|r_k\|)$ sobre uma esfera de raio ρ .

Como estamos interessados em construir códigos de grupo comutativo em esferas unitárias, precisamos fazer um ajuste de escala na construção apresentada anteriormente.

Seja, $x_0 = (\delta_1, 0, \dots, \delta_k, 0) \in S^{k-1}$, vamos denotar por Λ'_V o subreticulado obtido de Λ_R pela dilatação de cada vetor r_i de um fator $\frac{2\pi\delta_i}{\|r_i\|}$, i.e.,

$$\Lambda'_V = \text{span} \{v_1, v_2, \dots, v_k\}, \text{ com } v_i = \frac{2\pi\delta_i}{\|r_i\|} r_i.$$

Afetando os pontos de Λ_T por esta dilatação, o conjunto X , reescrito na nova base v_i conterá os vetores

$$x_j = (x_{j1}, x_{j2}, \dots, x_{jk}), \text{ onde } x_{ji} = \frac{2\pi\delta_i b_{ji}}{M}, \text{ com } 1 \leq b_{ji} \leq M \forall i, j.$$

A imagem de

$$\psi_{x_0}(x_j) = \left(\delta_1 \cos\left(\frac{x_{j1}}{\delta_1}\right), \delta_1 \sin\left(\frac{x_{j1}}{\delta_1}\right), \dots, \delta_k \cos\left(\frac{x_{jk}}{\delta_k}\right), \delta_k \sin\left(\frac{x_{jk}}{\delta_k}\right) \right)$$

pertence a S^{2k-1} para todo $1 \leq j \leq M$. O código de grupo comutativo $\mathcal{C}_G(M, 2k)$ será dado pela união das $\psi_{x_0}(x_j)$ para todos os pontos $x_j \in X$.

Como usual, a caracterização de um código de grupo comutativo é feita através do conjunto de geradores do grupo $G(M, n)$ e seu vetor inicial. A seguir mostramos como obter o conjunto dos geradores e, também, a classificação do grupo de $G(M, n)$, a partir da matriz W .

Definição 2.1 *Um conjunto gerador de um grupo G é um subconjunto S de G tal que todos os elementos de G são escritos como produto de elementos de S e dos seus inversos.*

O Teorema dos divisores elementares pode ser utilizado para determinar a estrutura do grupo G .

Teorema 2.2 *(Teorema dos Divisores Elementares, [8]). Seja L um \mathbb{Z} -submódulo de um módulo livre L' e de mesmo posto. Então existem inteiros positivos d_1, \dots, d_n (chamados de divisores elementares de L em L') satisfazendo a seguinte condição:*

1. Para todo i tal que $1 \leq i < n$ temos $d_{i+1} | d_i$.

2. Como \mathbb{Z} -módulos, temos o isomorfismo

$$L'/L \simeq \bigoplus_{1 \leq i \leq n} \frac{\mathbb{Z}}{d_i \mathbb{Z}},$$

e em particular $[L' : L] = d_1 \cdots d_n$ e d_1 é o expoente de L'/L .

3. Aí existe uma \mathbb{Z} -base (v_1, \dots, v_n) de L' tal que $(d_1 v_1, \dots, d_n v_n)$ é uma \mathbb{Z} -base de L .

Além disso, os d_i são unicamente determinados por L e L' .

Definição 2.2 *Seja $M_k(\mathbb{Z})$ o conjunto das matrizes $k \times k$ com elementos inteiros. Denota-se por $GL_k(\mathbb{Z}) \subset M_k(\mathbb{Z})$ o subconjunto daquelas que são inversíveis em $M_k(\mathbb{Z})$, isto é, aquelas com determinante igual a ± 1 . Tais matrizes são denominadas unimodulares.*

O Teorema a seguir permite determinar a estrutura do grupo $G = \frac{\Lambda_T}{\Lambda_R}$ de modo matricial.

Teorema 2.3 (Forma Normal de Smith, ([8], p.76)) *Seja A uma matriz $k \times k$, com coeficientes inteiros e determinante não nulo. Então existe uma única $D = (d_{i,j})$, matriz diagonal com $d_{i+1,i+1} | d_{i,i}$, tal que $D = V A U$ com U e V elementos de $GL_k(\mathbb{Z})$.*

A matriz D é dita Forma Normal de Smith de A .

Como todo reticulado é um \mathbb{Z} -módulo livre, as condições do Teorema 2.2 são válidas para reticulados. Para garantir a existência de inteiros positivos d_1, \dots, d_m que satisfaçam tais condições, basta aplicarmos o Teorema 2.3 na matriz W .

Deste modo, pelo Teorema 2.3, existe $D = PWQ$ na forma normal de Smith, isto é, D é uma matriz diagonal com coeficientes inteiros não nulos tal que $d_{i+1} | d_i$.

Como $WT = R$, temos $P^{-1}DQ^{-1}T = R$ ou $DQ^{-1}T = PR$. Uma vez que as matrizes P e Q^{-1} são unimodulares, quando operadas a esquerda de T e R definem mudanças de bases nos reticulados correspondentes. Assim, a matriz $\tilde{T} = Q^{-1}T$ gera o mesmo

reticulado Λ_T e $\tilde{R} = PR$ gera Λ_R . Cada linha \tilde{t}_i da matriz \tilde{T} contém um elemento gerador, de ordem d_i , do grupo $G(M, n) = \Lambda_T / \Lambda_R$. Como a dilatação feita não altera a estrutura do grupo quociente, a classificação do grupo provém de D e o conjunto dos geradores de $G(M, n)$ estão dados em \tilde{T} .

Esta associação entre códigos de grupo comutativo e reticulados permite uma abordagem diferente para o problema da procura por códigos de grupo comutativo ótimos. Ao invés de analisar todos os grupos $G(M, n)$ em \mathcal{O}_n é suficiente analisar os reticulados em \mathbb{R}^k que possuem subreticulados ortogonais e que determinam quociente com cardinalidade M . A primeira vista, os dois problemas tem o mesmo nível de dificuldade, no entanto, os Teoremas 2.4 e 2.5 mostram que é possível caracterizar precisamente estes reticulados e reduzir o número de casos a serem analisados.

Teorema 2.4 (Forma Normal de Hermite Estendida) *Seja B uma matriz $k \times k$ com coeficientes em \mathbb{Z} . Então existe uma única matriz triangular superior $T = UBV$, com $U \in GL_k(\mathbb{Z})$ e V uma matriz de permutação. Além disso, T satisfaz as seguintes condições:*

- a) $0 < T(i, i) \leq T(i+1, i+1), \quad \forall \quad 1 \leq i \leq k-1;$
- b) $0 \leq T([1 : i-1], i) < T(i, i), \quad \forall \quad 2 \leq i \leq k;$
- c) $T(i, i) \leq \text{mdc}(T([i : j], j)), \quad \forall \quad 1 \leq i < j \leq k;$

onde $T([p : q], r)$ são os elementos das linhas p até q da r -ésima coluna de T .

Demonstração:

A prova será feita por indução em k .

Para $k = 1$ é trivial. Suponha que seja válida para $n < k$.

Seja V_1 uma matriz que permuta as colunas de B de tal forma que o mdc das colunas de BV_1 fiquem em ordem crescente.

Seja $d_1 = \text{mdc}((BV_1)_{i,1})$ o mdc da primeira coluna de BV_1 e \tilde{U}_1 uma matriz unimodular, tal que

$$\tilde{U}_1 B V_1 = \left[\begin{array}{c|c} d_1 & \\ \hline a_2 d_1 & \\ \vdots & \\ a_k d_1 & \end{array} \middle| \bar{B}_{k,k-1} \right], \quad (2.5)$$

isto é, o produto de sua primeira linha pela primeira coluna de $B V_1$ é igual a d_1 .

Considerando

$$\hat{U}_1 = \left[\begin{array}{c|c} 1 & 0 \ \dots \ 0 \\ \hline -a_2 & \\ \vdots & Id_{k-1} \\ -a_k & \end{array} \right], \quad (2.6)$$

a matriz que faz a eliminação Gaussian na primeira coluna de $B V_1$, temos

$$\underbrace{\hat{U}_1 \tilde{U}_1}_{=U_1} B V_1 = \left[\begin{array}{c|c} d_1 & \\ \hline 0 & \\ \vdots & \\ 0 & \end{array} \middle| \tilde{B}_{k,k-1} \right]. \quad (2.7)$$

Seja B_1 a submatriz de $U_1 B V_1$ obtida da eliminação de sua 1ª linha e 1ª coluna. Assim, B_1 é uma matriz $(k-1) \times (k-1)$, por hipótese de indução existem matrizes \tilde{U} unimodular e \tilde{V} permutação tal que $\tilde{T} = \tilde{U} \tilde{B}_1 \tilde{V}$.

Assim,

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & \tilde{U} \end{bmatrix} U_1 B V_1 \begin{bmatrix} 1 & 0 \\ 0 & \tilde{V} \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & \tilde{U} \end{bmatrix} \begin{bmatrix} d_1 & * \\ 0 & B_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \tilde{V} \end{bmatrix} \\ &= \begin{bmatrix} d_1 & * \\ 0 & \tilde{U} B_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \tilde{V} \end{bmatrix} \\ &= \begin{bmatrix} d_1 & * \tilde{V} \\ 0 & \tilde{U} B_1 \tilde{V} \end{bmatrix} \\ &= \begin{bmatrix} d_1 & * \tilde{V} \\ 0 & \tilde{T} \end{bmatrix} = T. \end{aligned} \quad (2.8)$$

Caso $T(i, j) < 0$ ou $T(i, j) > T(j, j)$ para algum j , fazemos a operação elementar $\ell_i = \ell_i - \left\lfloor \frac{T_{i,j}}{T_{j,j}} \right\rfloor \ell_j$, o que equivale a uma multiplicação a esquerda por uma matriz unimodular U_j .

Como U e V são inversíveis, T é única, e a prova está concluída. ■

O Teorema a seguir apresenta uma caracterização de isometria entre códigos de grupo comutativo $2k$ -dimensionais através da matriz geradora de reticulados k -dimensionais associados aos códigos.

Teorema 2.5 *Todo código de grupo comutativo $\mathcal{C}_G(M, 2k)$, cujo grupo $G(M, 2k)$ é livre de blocos 2×2 de reflexão, é isométrico a um código obtido como quociente de reticulados $\frac{\Lambda_T}{\Lambda_{MI_k}}$ onde a matriz T , geradora do reticulado Λ_T satisfaz as seguintes condições:*

1. T é triangular superior de acordo com o Teorema 2.4;
2. $\det(T) = M^{k-1}$;
3. Existe uma matriz W , com elementos em \mathbb{Z} que satisfaz $WT = MI_k$, onde I_k é a matriz identidade $k \times k$;
4. Os elementos da diagonal de T satisfazem $T(i, i) = \frac{M}{a_i}$ onde $(a_i)^i \cdot (a_{i+1} \cdots a_k) \leq M$;

Demonstração:

Seja B uma matriz geradora do reticulado associado ao código \mathcal{C}_G , de acordo com a Proposição 2.1. Pelo Teorema 2.4, existe uma matriz triangular superior T , tal que, $T = UBV$. A matriz U é unimodular, logo define uma mudança de base no reticulado gerado por B enquanto V é uma isometria por permutação de coordenadas. Ambas operações não afetam a métrica do reticulado, portanto as matrizes B e $T = UBV$ definem reticulados que são associados à códigos isométricos.

Pela Proposição 2.1, a matriz B gera um reticulado que contém um subreticulado gerado por MI_k . Como os reticulados Λ_B e Λ_T são isométricos, temos:

- i. A cardinalidade do quociente $\frac{\Lambda_T}{\Lambda_M I_k}$ deve ser igual a M , que é o número de pontos no código. Além disso, de $\det(M I_k) = M^k$ conclui-se que $\det(T) = M^{k-1}$.
- ii. Como o sistema $xT = M e_i$ tem solução em Z^k para todo $1 \leq i \leq k$, W é a matriz cujas linhas são formadas por estas soluções.

Como consequência de ii. os elementos da diagonal de T devem dividir o número M .

Em particular, $T(i, i) = \frac{M}{a_i}$, $a_i \in \mathbb{Z}$, $\forall 1 \leq i \leq k$.

Além disso, pelo Teorema 2.4,

$$T(i, i) \leq T(i+1, i+1) \text{ então } \frac{M}{a_i} \leq \frac{M}{a_{i+1}} \text{ e } a_{i+1} \leq a_i.$$

Como

$$\det(T) = \frac{M}{a_1} \frac{M}{a_2} \dots \frac{M}{a_k} = M^{k-1},$$

tem-se

$$(a_1 a_2 \dots a_k) = M \Rightarrow (a_i)^i \cdot (a_{i+1} \dots a_k) \leq M.$$

■

Vale ressaltar que nem todas as matrizes triangulares superiores T satisfazem as propriedades do Teorema 2.5. Por exemplo, para $M = 12$, a matriz

$$T = \begin{bmatrix} 2 & 3 & 0 \\ 0 & 6 & 6 \\ 0 & 0 & 12 \end{bmatrix},$$

satisfaz as hipóteses do Teorema 2.4 e $\det(T) = 12^2$ mas, para obter $WT = 12 I_3$, é necessário que:

$$W = \begin{bmatrix} 6 & -3 & 3/2 \\ 0 & 2 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

porém, neste caso W não tem elementos inteiros.

No próximo Teorema, mostramos como obter a classificação do grupo e seu conjunto de geradores.

Teorema 2.6 *Seja T uma matriz que satisfaz as condições do Teorema 2.5 e $W = MT^{-1}$. Então, a classificação e o conjunto de geradores do grupo $G(M, n)$ associado ao código de grupo comutativo $\mathcal{C}_G(M, n)$ obtido como o quociente dos reticulados $\frac{\Lambda_T}{\Lambda_{MI}}$ provém da Forma Normal de Smith de W .*

Demonstração:

Seja $D = VWU$, a Forma Normal de Smith de W . Tem-se $WT = MI_k \Rightarrow V^{-1}DU^{-1}T = MI_k \Rightarrow DU^{-1}T = VM I_k$. Como as matrizes U^{-1} e V são unimodulares, quando operadas à esquerda das matrizes geradoras T e MI_k definem uma mudança de base nesses reticulados. A classificação e os geradores do grupo seguem do Teorema 2.2. Neste caso \mathcal{G} é isomorfo a grupo $\mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_k}$ e as linhas de $U^{-1}T$ formam um conjunto de geradores. ■

Os Teoremas 2.4, 2.5 e 2.6 permitem a implementação de um algoritmo computacional que, dados M e n , procura pelo melhor código $\mathcal{C}_G(M, n)$ através da seleção de casos relevantes² a serem testados.

O exemplo a seguir ilustra o procedimento para $M = 128$ e $n = 4$.

Exemplo 2.1 *Seja $A = \begin{pmatrix} \frac{128}{a_1} & w \\ 0 & \frac{128}{a_2} \end{pmatrix}$ uma matriz geradora de um reticulado associado a um código qualquer $\mathcal{C}_G(128, 4)$.*

Pelo Teorema 2.5, a_i divide 128, além disso $(a_2)^2 \leq 128$, logo $a_2 \in \{1, 2, 4, 8\}$. Assim, as possíveis diagonais de A são $\{(1, 128), (2, 64), (4, 32), (8, 16)\}$.

Para cada diagonal fixada, o conjunto de valores w deve ser determinado utilizando

$$\frac{M}{a_1} \leq \text{mdc}(w, \frac{M}{a_2});$$

² Estamos utilizando o termo “casos relevantes”, ao invés de “casos não isométricos”, devido ao fato que, dentre os códigos de grupo comutativo associados aos reticulados que satisfazem os Teoremas 2.4, 2.5 podem haver (poucos) códigos isométricos, em particular aqueles que são equivalente por redução de Adams [13]. Uma implementação cuidadosa do método pode considerar também estas reduções.

Assim,

$$A = \begin{pmatrix} 1 & w \\ 0 & 128 \end{pmatrix} \Rightarrow w \in \{0, 1, 2, 3, \dots, 64\};$$

$$A = \begin{pmatrix} 2 & w \\ 0 & 64 \end{pmatrix} \Rightarrow w \in \{0, 2, 4, 6, \dots, 32\};$$

$$A = \begin{pmatrix} 4 & w \\ 0 & 32 \end{pmatrix} \Rightarrow w \in \{0, 4, 8, 16\};$$

$$A = \begin{pmatrix} 8 & w \\ 0 & 16 \end{pmatrix} \Rightarrow w \in \{0, 8\}.$$

Finalmente, para cada um desses 88 casos, o problema do vetor inicial deve ser resolvido. Somente a matriz que determina a maior distância mínima e o respectivo vetor inicial necessitam ser guardados.

$$\text{Neste exemplo } A = \begin{pmatrix} 1 & 11 \\ 0 & 128 \end{pmatrix} \text{ e } x_0 = (0.65098, 0, 0.759095, 0)^t.$$

A classificação do grupo e o conjunto de geradores são obtidos usando a Forma Normal de Smith de $W = MA^{-1}$.

Neste caso, o melhor código $\mathcal{C}_{\mathcal{G}}(128, 4)$ é um código de grupo cíclico, cuja matriz geradora é

$$G_{(1,11,128)} = \begin{pmatrix} \cos\left(\frac{1 * 2\pi}{128}\right) & \sin\left(\frac{1 * 2\pi}{128}\right) & 0 & 0 \\ -\sin\left(\frac{1 * 2\pi}{128}\right) & \cos\left(\frac{1 * 2\pi}{128}\right) & 0 & 0 \\ 0 & 0 & \cos\left(\frac{11 * 2\pi}{128}\right) & \sin\left(\frac{11 * 2\pi}{128}\right) \\ 0 & 0 & -\sin\left(\frac{11 * 2\pi}{128}\right) & \cos\left(\frac{11 * 2\pi}{128}\right) \end{pmatrix}.$$

Este código tem a distância mínima $d = 0,406179$.

O Algoritmo 1, apresentado a seguir, resume as principais etapas do método para busca do melhor código de grupo comutativo de ordem M em \mathbb{R}^n .

Entrada: M e $n = 2k$

Saída: Conjunto de geradores do melhor código de grupo comutativo de ordem M em \mathbb{R}^n e o respectivo vetor inicial.

início

$dist \leftarrow 0$;

$x_0 \leftarrow \text{zeros}(k, 1)$;

$T \leftarrow \text{zeros}(k, k)$;

$div \leftarrow \{d_1, d_2, \dots, d_w\}$: o conjunto dos divisores de M ;

$A \leftarrow [a_1|, a_2|, \dots, a_j|]$: cujas colunas contém todas as possíveis diagonais da matriz T de acordo com o Teorema 2.5;

para $i = 1, 2, \dots, j$ **faça**

 Construa todas matrizes $T_{i,w}$, na forma o Teorema 2.5;

 Para cada matriz $T_{i,w}$ resolva o problema do vetor inicial, obtendo $dist_{iw}$

 e $x_{0_{iw}}$;

se $dist_{iw} > dist$ **então**

$dist \leftarrow dist_{iw}$

$x_0 \leftarrow x_{0_{iw}}$

$T \leftarrow T_{iw}$

fim

fim

 Classifique o grupo associado a matriz $W = MT^{-1}$, de acordo com o Teorema 2.6, obtendo a matriz G geradora do código.

 Imprima: G , x_0 e $dist$;

fim

Algoritmo 1: Resumo do método para procura do melhor código de grupo comutativo dados a dimensão e o número de pontos.

Utilizando uma implementação do Algoritmo 1, foi possível determinar os melhores códigos de grupo comutativo para diversos valores de M em várias dimensões. Na próxima Seção apresentamos alguns dos resultados computacionais obtidos.

2.4 Resultados computacionais

Comentários sobre a implementação.

Os resultados apresentados nesta Seção foram obtidos implementando e compilando o Algoritmo 2 no software *Mathematica 6.0* e rodados numa máquina Intel Core 2 duo, 2.40GHz, 4GB RAM, sem processamento paralelo.

A escolha deste software, em detrimento de outra linguagem de melhor desempenho computacional, como C^{++} ou *Fortran*, foi em parte motivada por nosso particular interesse em comparar o número de casos necessários a serem analisados para se encontrar o melhor código de grupo comutativo em relação ao número total casos, inicialmente sem a preocupação com o tempo de processamento. Em segundo lugar (e também relevante) a opção foi motivada pela existência de bons pacotes para as decomposições de Smith e Hermite e de funções listáveis, nativas do *Mathematica* que são apropriadas para trabalho com reticulados.

Naturalmente, a obtenção de códigos de grupo comutativo em dimensões altas, com um número grande de pontos, demanda um esforço computacional que pode exigir a implementação do método em linguagens de melhor performance. Se este for o interesse, uma opção alternativa pode ser a implementação apenas do *loop* interno do Algoritmo 1 (evitando a programação das decomposições de Smith e Hermite), uma vez que a classificação e a obtenção do conjunto de geradores do melhor código de grupo pode ser feita em separado.

Outra solução que pode resultar numa significativa melhora no desempenho computacional é uma implementação eficiente do método para resolver o PL associado ao problema do vetor inicial. Este PL deve ser resolvido para cada grupo e, na prática, é a etapa mais cara do *loop* interno do Algoritmo 1. Em nossa implementação, os testes com o método *simplex revisado* tiveram melhor performance do que os testes com alguns *métodos de pontos interiores*. Uma explicação para isso é que procuramos códigos ótimos em dimensões menores do que 20 e métodos de pontos interiores sobressaem ao *simplex* para problemas grandes.

Número de casos analisados

Os gráficos apresentados nas Figuras 2.1 e 2.2 ilustram a relação entre o número total de casos (estimado por $\binom{M/2}{n/2}$) e o número de casos distintos que foram efetivamente testados para obtenção do melhor $\mathcal{C}_G(M, n)$.

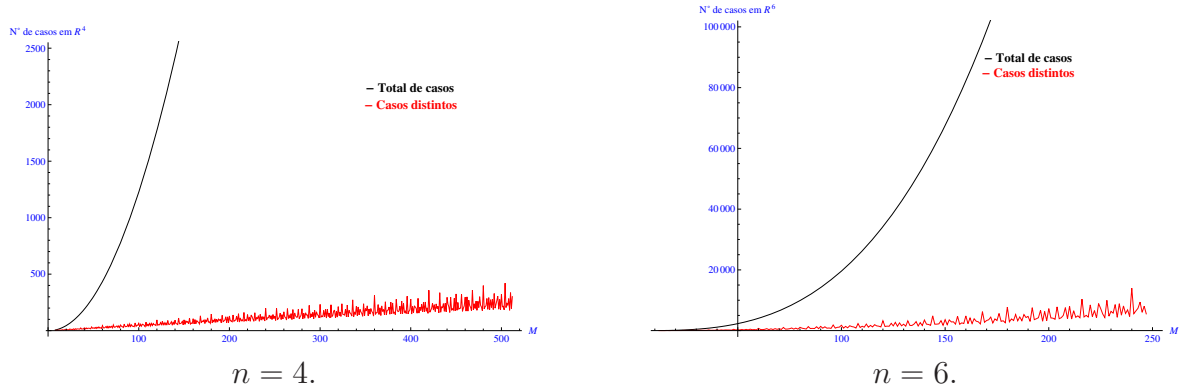


Figura 2.1: Comparação entre o número total de casos e o número de casos analisados (casos distintos) para obter o melhor $\mathcal{C}_G(M, n)$.

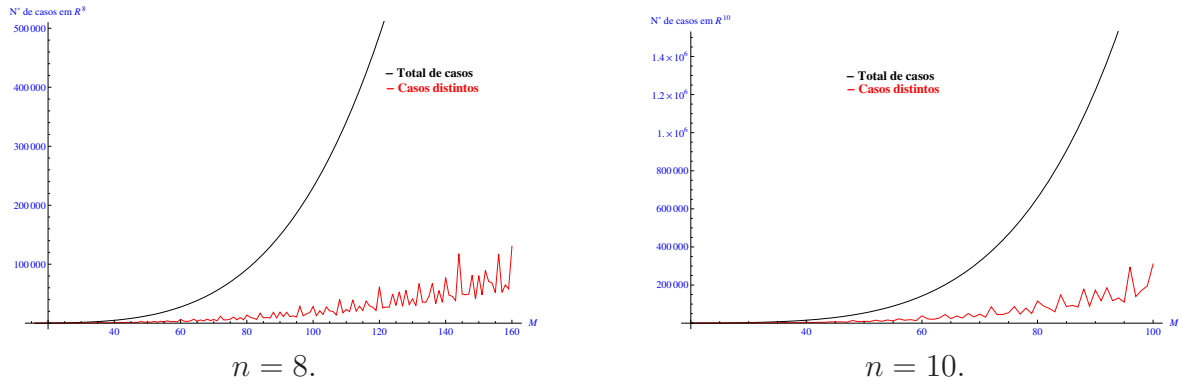


Figura 2.2: Comparação entre o número total de casos e o número de casos analisados (casos distintos) para obter o melhor $\mathcal{C}_G(M, n)$.

A Tabela 2.1 mostra uma comparação entre o número de casos e o tempo gasto na procura do melhor código $\mathcal{C}_G(M, 4)$ antes e depois da seleção dos casos relevantes.

Exemplos de códigos de grupo comutativo ótimos

As Tabelas 2.2 e 2.3 apresentam alguns códigos de grupo comutativo ótimos em \mathbb{R}^4 e \mathbb{R}^6 .

M	Total de casos (busca exaustiva)	Tempo estimado (em segundos)	Casos testados usando o algoritmo	Tempo (em segundos)
32	120	0.177s	21	0.031s
64	496	1.631s	38	0.125s
128	2016	14.197s	71	0.500s
256	8128	116.720s	136	1.953s
512	32640	900.741s	265	7.313s
1024	130816	7451.5s	522	29.734s
2048	523776	62158.8s	1035	122.828s
4096	2096128	523157s	2060	514.14s
8192	8386560	$4.594 \times 10^6 s$	4109	2250.88s
16384	33550336	$4.10526 \times 10^7 s$	8206	10041s
32768	134209536	$3.77984 \times 10^8 s$	16399	46185.7s

Tabela 2.1: Comparação entre o número de casos e o tempo gasto na procura do melhor código $\mathcal{C}_G(M, 4)$.

Quando o grupo é cíclico, $G(M, n)$ é gerado pela matriz $G_{a,b,M}$, conforme apresentada (2.4), com (a, b) dados na coluna Gerador (a, b) . Quando o grupo é não cíclico, existem dois geradores, caracterizados pelos pares (a, b) . O vetor inicial ótimo $(\delta_1, 0, \delta_2, 0)$ foi encontrado resolvendo o PL correspondente. A última coluna apresenta o limitante superior específico para distância mínima em códigos de grupo comutativos (Proposição 2.2). Como a Tabela sugere, o limitante pode ser assintoticamente atingido pelos melhores códigos de grupo comutativo, tomando M arbitrariamente grande. A Figura 2.3 ilustra esse fato para $n = 4$ e $n = 6$.

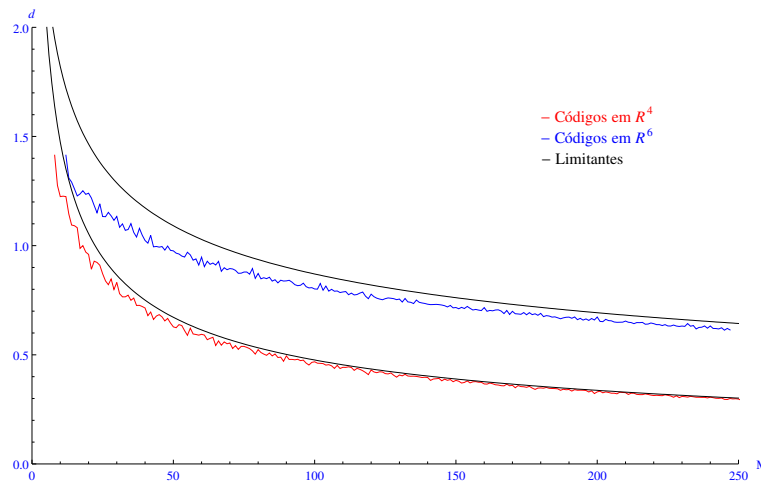


Figura 2.3: Comparação entre a distância mínima dos melhores códigos de grupo comutativo em \mathbb{R}^4 e \mathbb{R}^6 e os respectivos limitantes.

M	d_{min}	δ_1	δ_2	Grupo	Gerador (a, b)	Limitante
10	1.224	0.707	0.707	\mathbb{Z}_{10}	(1 3)	1.474
20	0.959	0.678	0.734	\mathbb{Z}_{20}	(3 4)	1.054
30	0.831	0.707	0.707	\mathbb{Z}_{30}	(3,5)	0.864
40	0.714	0.607	0.794	\mathbb{Z}_{40}	(4 5)	0.750
50	0.628	0.707	0.706	\mathbb{Z}_{50}	(7 2)	0.672
100	0.468	0.757	0.653	$\mathbb{Z}_5 \oplus \mathbb{Z}_{20}$	(0 20), (5 10)	0.476
200	0.330	0.750	0.660	\mathbb{Z}_{200}	(93 1)	0.337
300	0.273	0.656	0.754	$\mathbb{Z}_5 \oplus \mathbb{Z}_{60}$	(60 120), (10 15)	0.275
400	0.237	0.686	0.727	\mathbb{Z}_{400}	(189 1)	0.238
500	0.211	0.674	0.738	\mathbb{Z}_{500}	(13 20)	0.213
600	0.193	0.676	0.736	\mathbb{Z}_{600}	(191 198)	0.194
700	0.180	0.718	0.695	\mathbb{Z}_{700}	(14 25)	0.180
800	0.168	0.670	0.742	\mathbb{Z}_{800}	(16 25)	0.168
900	0.158	0.704	0.709	\mathbb{Z}_{900}	(197 2)	0.159
1000	0.149	0.716	0.697	\mathbb{Z}_{1000}	(33 4)	0.150

Tabela 2.2: Códigos de grupo comutativo ótimos em R^4 com M pontos.

Desempenho dos melhores códigos de grupo comutativo encontrados

Na transmissão de sinais em um canal Gaussiano, a taxa de informação por largura de banda, definida como

$$\frac{R}{W} = \frac{2 \log_2 M}{n}$$

é utilizada para comparar a eficiência de códigos esféricos. Na Figura 2.4 apresentamos uma comparação entre alguns dos melhores códigos $\mathcal{C}_G(M, n)$ que encontramos, com outros códigos de grupo comutativo conhecidos, como o simplex, bi-ortogonal e também alguns códigos analisados em [5].

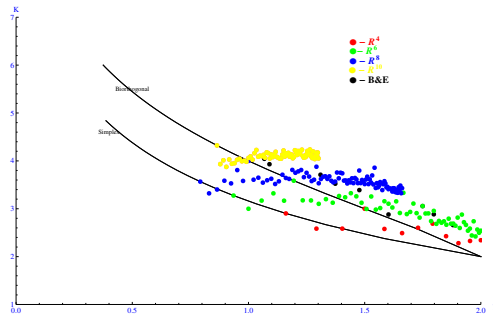


Figura 2.4: Comparação de performance entre alguns códigos de grupo comutativo $\mathcal{C}_G(M, n)$ para o canal Gaussiano. B&E referem-se a códigos apresentados por Biglieri e Elia em [5].

M	d_{min}	δ_1	δ_2	δ_3	Grupo	Gerador (a,b,c)	Limitante
10	1.414	0.632	0.632	0.447	\mathbb{Z}_{10}	(3,1,5)	1.820
20	1.240	0.554	0.620	0.554	\mathbb{Z}_{20}	(2,5,6)	1.465
30	1.133	0.534	0.654	0.534	\mathbb{Z}_{30}	(3,5, 9)	1.287
40	1.044	0.603	0.522	0.603	$\mathbb{Z}_2 \oplus \mathbb{Z}_{20}$	(20,0,20), (32,10,4)	1.173
50	0.976	0.604	0.506	0.615	\mathbb{Z}_{50}	(7,6, 34)	1.091
100	0.804	0.515	0.684	0.515	$\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$	(50, 10, 0), (30, 0, 10)	0.870
200	0.673	0.555	0.619	0.555	\mathbb{Z}_{200}	(28, 25, 4)	0.692
300	0.585	0.585	0.498	0.639	$\mathbb{Z}_5 \oplus \mathbb{Z}_{60}$	(0, 0, 60), (25, 30, 30)	0.605
400	0.540	0.562	0.605	0.562	$\mathbb{Z}_{20} \oplus \mathbb{Z}_{20}$	(300, 40, 0), (60, 0, 20)	0.550
500	0.504	0.577	0.577	0.577	$\mathbb{Z}_5 \oplus \mathbb{Z}_{10}, \otimes \mathbb{Z}_{10}$	(100, 0, 0), (50, 50, 0), (50, 0, 50)	0.511
600	0.472	0.549	0.630	0.549	$\mathbb{Z}_2 \oplus \mathbb{Z}_{300}$	(300, 0, 300), (384, 50, 12)	0.481
700	0.445	0.531	0.612	0.585	\mathbb{Z}_{700}	(457, 664, 298)	0.457
800	0.427	0.617	0.486	0.617	$\mathbb{Z}_{20} \oplus \mathbb{Z}_{40}$	(80,0,40),(20,80,60)	0.437
900	0.413	0.592	0.591	0.547	$\mathbb{Z}_3 \oplus \mathbb{Z}_{300}$	(0,300,0),(759,36,3)	0.420
1000	0.397	0.560	0.632	0.535	\mathbb{Z}_{1000}	(319,694,45)	0.406

Tabela 2.3: Códigos de grupo comutativo ótimos em R^6 com M pontos.

Neste gráfico, cada código é representado por um ponto no sistema de coordenadas $(\frac{R}{W}, K)$, onde $K = (1 - \rho) \log_2 M$ e ρ é o maior produto escalar entre dois pontos de $\mathcal{C}_G(M, n)$.

Como podemos observar na Figura 2.4, alguns dos melhores $\mathcal{C}_G(M, n)$ tem performance superior aos códigos bi-ortogonal, simplex e também alguns códigos apresentados em [5], i.e., exibem maior distância mínima para a mesma taxa de informação por largura de banda R/W .

2.5 Códigos de grupo comutativo em dimensão ímpar

Códigos de grupo comutativos em dimensão ímpar $n = 2k + 1$ são gerados por um grupo $G(M, 2k + 1)$ cujas matrizes $G_i \in G(M, 2k + 1)$ tem a seguinte forma pseudo diagonal [49]

$$G_i = [R_1(i), \dots, R_k(i), \pm 1], \forall \ 1 \leq i \leq M.$$

Isto implica que um código $\mathcal{C}_G(M, 2k + 1)$ tem um número par de pontos M e é formado pela união de duas cópias escalonadas de um $\mathcal{C}_G(\frac{M}{2}, 2k)$ contidas em hiperplanos paralelos. Sendo assim, o melhor código de grupo comutativo de ordem $M = 2p$ em R^{2k+1} pode ser determinado encontrando o melhor $\mathcal{C}_G(\frac{M}{2}, 2k)$, na dimensão anterior, com vetor inicial $x_0 = (\delta_1, 0, \dots, \delta_k, 0)$. Em seguida, o melhor vetor inicial

$y_\theta = (\cos \theta x_0, \sin \theta)$, para $\mathcal{C}_G(M, 2k+1)$ pode ser encontrado, resolvendo um problema de otimização a um parâmetro [49].

2.6 Decodificação em códigos de grupo comutativo

Uma importante questão em decodificação de canal é como encontrar um ponto do código mais próximo de um ponto arbitrário em \mathbb{R}^n . Este processo é denominado *decodificação*.

Códigos estruturados podem oferecer muitas vantagens no processo de decodificação, especialmente quando se pode utilizar informações cruciais sobre sua estrutura. Neste sentido, os denominados códigos geometricamente uniformes [23] e mais especificamente códigos de grupo [50] merecem atenção especial devido a simetrias provenientes de suas estruturas algébricas.

Nesta Seção, mostramos que a decodificação de um código de grupo comutativo $2k$ -dimensional, pode ser feita através da decodificação de um reticulado em \mathbb{R}^k .

O método é baseado em máxima verossimilhança, ou decodificação por mínima distância. Mais precisamente, seja $x \in \mathbb{R}^{2k}$ um ponto qualquer, $\mathcal{C}_G(M, 2k)$ um código de grupo comutativo com vetor inicial $x_0 = (\delta_1, 0, \dots, \delta_k, 0)$ e B uma matriz geradora do reticulado k -dimensional Λ associado a $\mathcal{C}_G(M, 2k)$, busca-se

$$y = \arg \min_{y_i \in \mathcal{C}_G} \|x - y_i\|.$$

A Proposição a seguir mostra que o primeiro passo para decodificar x é normalizá-lo.

Proposição 2.3 *Para qualquer $x \in \mathbb{R}^n$ e qualquer código esférico \mathcal{C} , tem-se que*

$$\arg \min_{y \in \mathcal{C}} \left\| \frac{x}{\|x\|} - y \right\| = \arg \min_{y \in \mathcal{C}} \|x - y\|.$$

Demonstração:

Se $y \in \mathcal{C}$ é tal que,

$$\left\| \frac{x}{\|x\|} - y \right\| \leq \left\| \frac{x}{\|x\|} - z \right\|, \quad \forall z \in \mathcal{C},$$

tem-se que

$$2 - 2 \left\langle \frac{x}{\|x\|}, y \right\rangle \leq 2 - 2 \left\langle \frac{x}{\|x\|}, z \right\rangle \Rightarrow \langle x, y \rangle \geq \langle x, z \rangle.$$

Assim,

$$\|x - y\| = \|x\|^2 + 1 - 2 \langle x, y \rangle \leq \|x\|^2 + 1 - 2 \langle x, z \rangle = \|x - z\|.$$

Portanto,

$$\arg \min_{y \in \mathcal{C}} \left\| \frac{x}{\|x\|} - y \right\| = \arg \min_{y \in \mathcal{C}} \|x - y\|.$$

■

Para qualquer vetor unitário $x = (x_1, x_2, \dots, x_{2k-1}, x_{2k})$, podemos escrever

$$\begin{aligned} x &= \left(\sqrt{x_1^2 + x_2^2} \left(\frac{x_1}{\sqrt{x_1^2 + x_2^2}}, \frac{x_2}{\sqrt{x_1^2 + x_2^2}} \right), \dots \right), \\ x &= \left(\gamma_1 \left(\cos \frac{\theta_1}{\gamma_1}, \sin \frac{\theta_1}{\gamma_1} \right), \dots, \gamma_k \left(\cos \frac{\theta_k}{\gamma_k}, \sin \frac{\theta_k}{\gamma_k} \right) \right), \end{aligned} \quad (2.9)$$

onde,

$$\begin{aligned} \gamma_i &= \sqrt{x_{2i-1}^2 + x_{2i}^2}, \quad 1 \leq i \leq k, \\ \theta_i &= \arccos \left(\frac{x_{2i-1}}{\gamma_i} \right) \gamma_i, \quad 1 \leq i \leq k. \end{aligned}$$

Isto significa que x pertence ao toro planar de raios γ_i , $1 \leq i \leq k$.

De acordo com a *Proposição 2.1*, seja T_{x_0} o toro planar que contém o código $\mathcal{C}_G(M, 2k)$ e w o vetor em T_{x_0} mais próximo de x .

De acordo com [56],

$$w = \left(\delta_1 \left(\cos \frac{\theta_1}{\gamma_1}, \sin \frac{\theta_1}{\gamma_1} \right), \dots, \delta_k \left(\cos \frac{\theta_k}{\gamma_k}, \sin \frac{\theta_k}{\gamma_k} \right) \right),$$

e a distância mínima entre T_{x_0} e x é dada por $d_* = \|x - w\|$.

Portanto, o segundo passo para decodificação é projetar x em T_{x_0} obtendo w .

Como $w \in T_{x_0}$ podemos utilizar a imagem inversa $z = \psi_{x_0}^{-1}(w) \in \mathbb{R}^k$ (“planificar o toro”) e obter $z \in \mathbb{R}^k$, ou seja,

$$z = \left(\frac{\delta_1 \theta_1}{\gamma_1}, \frac{\delta_2 \theta_2}{\gamma_2}, \dots, \frac{\delta_k \theta_k}{\gamma_k} \right).$$

Finalmente a decodificação pode ser realizada procurando o ponto do reticulado Λ mais próximo de z utilizando um diagrama de treliça de Λ .

A seguir apresentamos um resumo do método.

Algoritmo para decodificação em $C_G(M, 2k)$:

Dado um código de grupo comutativo $C_G(M, 2k)$, com vetor inicial $x_0 = (\delta_1, 0, \delta_2, 0, \dots, \delta_k, 0)$, uma treliça T do reticulado Λ associado ao código e um ponto $x \in \mathbb{R}^{2k}$:

1º Passo: Faça

$$\frac{x}{\|x\|} = (x_1, x_2, \dots, x_{2k-1}, x_{2k});$$

2º Passo: Obtenha o ponto $z \in \mathbb{R}^k$,

$$z = \left(\frac{\delta_1 \theta_1}{\gamma_1}, \frac{\delta_2 \theta_2}{\gamma_2}, \dots, \frac{\delta_k \theta_k}{\gamma_k} \right),$$

e decodifique z no reticulado Λ através da treliça T , obtendo o ponto $u = (u_1, u_2, \dots, u_k)$.

3º Passo: O resultado da decodificação de x em $C_G(M, 2k)$ é a imagem de u por ψ_{x_0} , ou seja,

$$y = \left(\delta_1 \cos\left(\frac{u_1}{\delta_1}\right), \delta_1 \sin\left(\frac{u_1}{\delta_1}\right), \dots, \delta_k \cos\left(\frac{u_k}{\delta_k}\right), \delta_k \sin\left(\frac{u_k}{\delta_k}\right) \right).$$

A etapa mais cara do processo de decodificação apresentado acima é o **2º Passo**, que consiste numa decodificação em reticulado na metade da dimensão do código. Como é comentado em [18], este custo está diretamente relacionado à complexidade da treliça do reticulado associado ao código. Por exemplo, o número de operações C requeridas pelo Algoritmo de Viterbi para decodificar $\Lambda_T \subset \mathbb{R}^k$ satisfaz [3]

$$C \leq k(7N(\Lambda_T) - N(\Lambda_T)^{1/k} + 4k).$$

Na decodificação que estamos propondo, não se faz necessário gerar os pontos do código esférico $C_G(M, 2k)$, o que pode significar uma importante vantagem do ponto de vista de utilização de memória na decodificação. O número de candidatos que precisam ser efetivamente computados e armazenados na memória é menor ou igual ao número de caminhos na treliça utilizada.

Na Figura 2.5 apresentamos uma ilustração do método de decodificação aqui proposto. Os rótulos das linhas pontilhadas indicam a sequência de passos do método. O conteúdo apresentado nesta seção compõe o trabalho [18].

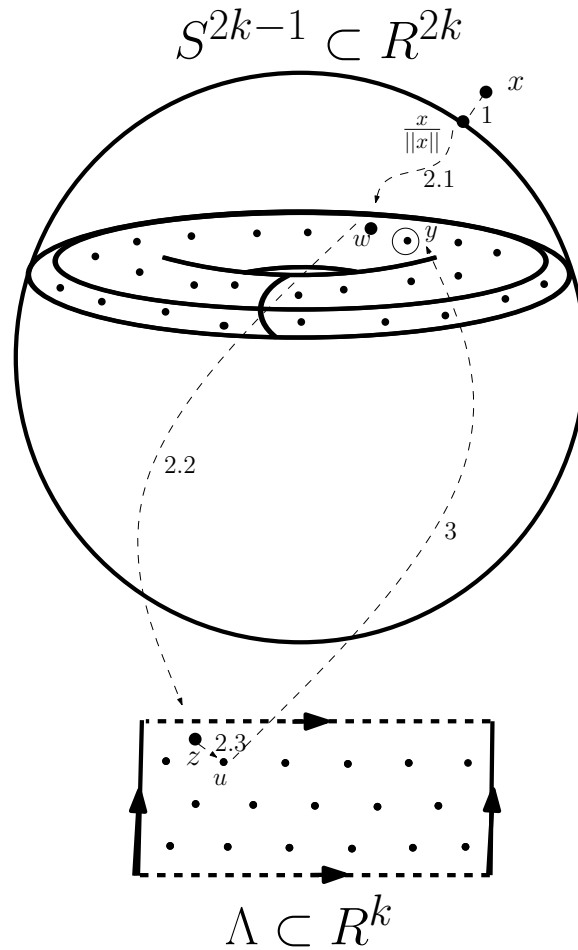


Figura 2.5: Ilustração do método de decodificação.

CÓDIGOS ESFÉRICOS EM CAMADAS DE TOROS

A conexão entre toros planares e códigos esféricos foi estudada em [48], com atenção particular a códigos de grupo comutativo, e também em [62, 11]. Em [49] foi demonstrado que códigos de grupo comutativo em dimensões pares moram em toros planares e podem ser vistos como certos reticulados na metade da dimensão. Este fato já foi utilizado no Capítulo 2 para a dedução do método de procura de códigos de grupo comutativo.

Nosso interesse aqui vai além dessa classe de códigos. Vamos apresentar uma nova família de códigos esféricos, cujos pontos são alocados em camadas de toros, mergulhadas na superfície da esfera unitária.

O capítulo é iniciado com a apresentação formal dos toros planares e na Seção 3.1.1 deduzimos expressões para distâncias entre toros na esfera e também para deformações provocadas pelo mergulho da caixa retangular que define o toro na superfície da esfera unitária.

Na Seção 3.2 introduzimos os códigos esféricos em camadas de toros. A nova técnica consiste em folhear a esfera unitária por toros planares que formarão as camadas do código. Para cada camada determina-se um conjunto de pontos de modo a formar um código esférico com uma dada distância mínima d .

Na seção 3.3 apresentamos limitantes, inferior e superior, para o número de pontos no código e, na Seção 3.4, discutimos como utilizar os conceitos estudados no Capítulo 2 para construir códigos esféricos homogêneos em cada camada, os códigos quase comutativos.

Ao longo de todo o capítulo alguns exemplos são construídos e os resultados mostram que tais códigos têm desempenho comparável aos melhores códigos esféricos estruturados conhecidos (apple-pelling, wrapped, laminados), com destaque para uma potencial vantagem no processo de codificação/decodificação, decorrente da homogeneidade, estrutura de grupo e associação a reticulados na metade da dimensão. Além disso os pontos do código podem ser facilmente gerados como os pontos de um código de grupo comutativo em cada camada.

3.1 Toros planares

Um *toro planar* é uma subvariedade k -dimensional do \mathbb{R}^{2k} , com curvatura gaussiana nula, definido como um produto cartesiano de k círculos em \mathbb{R}^2 , de raios δ_i , com $\sum_{i=1}^k \delta_i^2 = 1$, i.e.,

$$T_\delta = S_1^1 \times S_2^1 \times \cdots \times S_k^1.$$

Mais precisamente, seja $\delta = (\delta_1, \dots, \delta_k)$ um vetor unitário em \mathbb{R}^k , tal que $\delta_i \geq 0 \ \forall \ 1 \leq i \leq k$. O toro planar T_δ associado é um subconjunto de pontos da esfera unitária S^{2k-1} dado por

$$T_\delta = \{(x_1, x_2, \dots, x_{2k}) \in \mathbb{R}^{2k}; \delta_i^2 = x_{2i-1}^2 + x_{2i}^2, \ 1 \leq i \leq k\}. \quad (3.1)$$

Cada ponto de S^{2k-1} pertence a algum toro planar ou a uma de suas degenerações (conf. (2.9). Além disso,

$$\bigcup_{\delta \in S^{k-1} : \delta_i \geq 0} T_\delta = S^{2k-1}.$$

Dizemos, assim, que S^{2k-1} pode ser folheada por toros planares.

Seja $y = (y_1, y_2, \dots, y_k) \in \mathbb{R}^k$, a aplicação $\psi_\delta : \mathbb{R}^k \longrightarrow \mathbb{R}^{2k}$ definida por

$$y \longmapsto \psi_\delta(y) = \left(\delta_1 \cos \left(\frac{y_1}{\delta_1} \right), \delta_1 \sin \left(\frac{y_1}{\delta_1} \right), \dots, \delta_k \cos \left(\frac{y_k}{\delta_k} \right), \delta_k \sin \left(\frac{y_k}{\delta_k} \right) \right) \quad (3.2)$$

é denominada *parametrização canônica* do toro T_δ .

A aplicação ψ_δ é claramente diferenciável,

$$\frac{\partial \psi_\delta}{\partial y_i} = -\sin \left(\frac{y_i}{\delta_i} \right) e_{2i-1} + \cos \left(\frac{y_i}{\delta_i} \right) e_{2i},$$

além disso,

$$\left\langle \frac{\partial \psi_\delta}{\partial y_i}, \frac{\partial \psi_\delta}{\partial y_j} \right\rangle = \langle e_i, e_j \rangle,$$

onde $\{e_i\}$ é a base canônica do \mathbb{R}^k . Ou seja, ψ_δ é uma isometria local entre \mathbb{R}^k e o toro T_δ . Isto implica que, em uma região onde ψ_δ é injetiva, ângulos, distâncias, áreas e volumes k -dimensionais são preservados por ψ_δ .

Assim como o cilindro circular reto em \mathbb{R}^3 pode ser “aberto” num retângulo bidimensional, o toro planar também pode ser “planificado”, gerando um conjunto de pontos que corresponde a uma caixa (ou hipercaixa) cujos lados são ortogonais. Daremos uma explicação mais formal para o que isto significa.

Dizemos que x e y em \mathbb{R}^k são equivalentes por uma aplicação ψ , se $\psi(x) = \psi(y)$. Nestes termos, ψ_δ induz uma relação de equivalência em \mathbb{R}^k .

Um conjunto de representantes das classes de equivalência dessa relação é o paraleloto fundamental \mathcal{P}_δ do reticulado Λ gerado pelos vetores $u_i = 2\pi\delta_i e_i$, $1 \leq i \leq k$, i.e.,

$$\mathcal{P}_\delta = \{x \in \mathbb{R}^k : 0 \leq x_i < 2\pi\delta_i\}.$$

O toro planar T_δ pode ser visto como o paralelepípedo (que é o fecho de \mathcal{P}_δ onde lados paralelos da caixa são identificados. Claramente, $x = (x_1, \dots, x_k)$ e $y = (y_1, \dots, y_k)$ são equivalentes se $x_i = y_i \pmod{2\pi\delta_i}$, ou seja, $x - y \in \Lambda$. Neste caso, denotamos $x = y \pmod{\Lambda}$ e o espaço quociente por $\frac{\mathbb{R}^k}{\Lambda}$.

Como a imagem de ψ_δ é T_δ e ψ_δ está bem definida no quociente $\frac{\mathbb{R}^k}{\Lambda}$, ou seja, $\psi_\delta(x) = \psi_\delta(y)$ se, e somente se, $x = y \pmod{\Lambda}$, temos que T_δ é também imagem de ψ_δ restrita a \mathcal{P}_δ .

Outra propriedade satisfeita por toros planares é a homogeneidade. Para qualquer par de pontos p e q em T_δ existe uma isometria de \mathbb{R}^{2k} que preserva T_δ e leva p em q . Esta isometria é um produto de matrizes de rotações bidimensionais que não afetam os raios que definem T_δ .

Como observado em [48], construir uma isometria entre dois pontos de um toro planar T_δ é equivalente a construir uma translação entre a pré-imagem destes pontos na caixa localmente isométrica a T_δ .

3.1.1 Distâncias em toros planares

Um código esférico em \mathbb{R}^{2k} pode ser construído considerando a imagem, por ψ_δ , de um conjunto discreto de pontos $Y \in \mathcal{P}_\delta$. Claramente $\psi_\delta(Y) \in S^{2k-1}$ e a distância mínima no código dependerá, além de Y , da particular escolha do vetor $\delta \in \mathbb{R}^k$ que define o toro e também da distorção provocada por ψ_δ .

Se dois pontos b e c forem escolhidos sobre S^{k-1} , de modo que os toros T_b e T_c estejam afastados a uma distância d , um código esférico gerado como imagem das aplicações ψ_b e ψ_c terá distância mínima d , desde que $\|\psi_b(x) - \psi_b(y)\| \geq d$ e $\|\psi_c(z) - \psi_c(w)\| \geq d$, para todo x, y e z, w pertencente a cada uma das caixas que definem o domínio de ψ_b e ψ_c , respectivamente.

A Proposição a seguir estabelece que a distância mínima entre dois toros T_b e T_c é igual a distância mínima entre os pontos b e c em S^{k-1} .

Proposição 3.1 *Sejam $b = (b_1, b_2, \dots, b_k)$ e $c = (c_1, c_2, \dots, c_k)$ vetores unitários em \mathbb{R}^k com coordenadas não negativas, a distância mínima entre dois toros T_c e T_b , definidos de acordo com (3.1) é dada por*

$$d(T_c, T_b) = \|c - b\| = \left(\sum_{i=1}^k (c_i - b_i)^2 \right)^{1/2}. \quad (3.3)$$

Demonstração:

Sem perda de generalidade, e para simplificar a notação, vamos supor que $b_i \neq 0$ e $c_i \neq 0, \forall 1 \leq i \leq k$. Caso contrário, poderíamos simplesmente incluir estas condições em cada um dos somatórios que aparecem a seguir, evitando as indefinições em $\frac{x_i}{b_i}$ e $\frac{y_i}{c_i}$.

Seja $D = d^2(T_b, T_c)$, para todo $x \in \mathcal{P}_b$ e todo $y \in \mathcal{P}_c$, de (3.2) temos

$$\begin{aligned}
 D &= \sum_{i=1}^k \left(b_i \cos \left(\frac{x_i}{b_i} \right) - c_i \cos \left(\frac{y_i}{c_i} \right) \right)^2 - \left(b_i \sin \left(\frac{x_i}{b_i} \right) - c_i \sin \left(\frac{y_i}{c_i} \right) \right)^2 \\
 &= \sum_{i=1}^k b_i^2 + c_i^2 - 2b_i c_i \left(\cos \left(\frac{x_i}{b_i} \right) \cos \left(\frac{y_i}{c_i} \right) + \sin \left(\frac{x_i}{b_i} \right) \sin \left(\frac{y_i}{c_i} \right) \right) \\
 &= \sum_{i=1}^k b_i^2 + c_i^2 - 2b_i c_i \left(\cos \left(\frac{x_i}{b_i} - \frac{y_i}{c_i} \right) \right) \\
 &= \sum_{i=1}^k (b_i - c_i)^2 + 4 \sum_{i=1}^k b_i c_i \sin^2 \left(\frac{1}{2} \left(\frac{x_i}{b_i} - \frac{y_i}{c_i} \right) \right).
 \end{aligned}$$

De onde

$$D \geq \sum_{i=1}^k (b_i - c_i)^2 = \|b - c\|^2,$$

com a igualdade valendo se, e somente se,

$$\frac{x_i}{b_i} = \frac{y_i}{c_i}.$$

■

Se considerarmos $b = c$ na Proposição 3.1, obtemos uma expressão para a distância entre dois pontos no mesmo toro T_b , como estabelecido a seguir.

Proposição 3.2 *Sejam $b = (b_1, b_2, \dots, b_k) \in S^{k-1}$ com $b_i \geq 0, i = 1, \dots, k$, u e $v \in \mathcal{P}_b$, a distância entre os pontos $\psi_b(u)$ e $\psi_b(v) \in T_b$ é dada por*

$$\|\psi_b(u) - \psi_b(v)\| = 2 \sqrt{\sum_{i=1}^k b_i^2 \sin^2 \left(\frac{u_i - v_i}{2b_i} \right)} \quad (3.4)$$

A Proposição a seguir estabelece um limitante inferior e superior para (3.4) e será bastante útil na construção dos códigos em camadas de toros.

Proposição 3.3 *Seja $b = (b_1, b_2, \dots, b_k) \in S^{k-1}$, com $b_i \geq 0, i = 1, \dots, k$ e $b_* = \min_{1 \leq i \leq k} b_i$. Para qualquer $y \in \mathcal{P}_b$, a distância $\|\psi_b(y) - \psi_b(0)\|$ satisfaz*

$$\frac{2\|y\|}{\pi} \leq 2b_* \sin\left(\frac{\|y\|}{2b_*}\right) \leq \|\psi_b(y) - \psi_b(0)\| \leq 2 \sin\left(\frac{\|y\|}{2}\right) \leq \|y\|. \quad (3.5)$$

A demonstração (Apêndice 1) [1] utiliza o método dos multiplicadores de Lagrange e baseia-se no fato de que deformação mínima na imagem de ψ ocorre na direção do vetor $u_{min} = (b_1, b_2, \dots, b_k)$ e a deformação máxima na direção de $u_{max} = b_* e_*$.

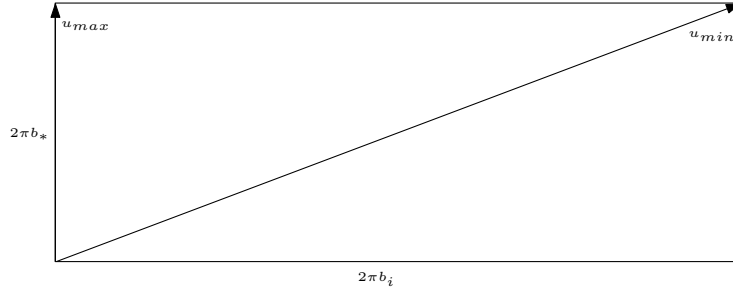


Figura 3.1: Direções de deformação máxima e mínima em um toro planar.

3.2 Códigos esféricos em camadas de toros

Nosso objetivo é construir um código esférico em \mathbb{R}^{2k} , com distância mínima maior ou igual a um valor estabelecido d . Tal código será denotado por $\mathcal{C}_T(2k, d)$.

A ideia intuitiva que está por traz da construção dos $\mathcal{C}_T(2k, d)$ é a seguinte. Dada uma distância mínima d , vamos “fatiar” a esfera unitária S^{2k-1} por toros planares, de forma que a distância mínima entre quaisquer dois desses toros seja maior ou igual a d . Em seguida, para cada um dos toros T_δ obtidos, iremos selecionar um conjunto de pontos da caixa \mathcal{P}_δ correspondente ao toro de forma que, quando mergulhados no \mathbb{R}^{2k} por (3.2) tenham distância mínima maior ou igual a d . O $\mathcal{C}_T(2k, d)$ será formado pela união de todas estas camadas.

A pré-imagem dos pontos de cada camada de um $\mathcal{C}_T(2k, d)$ está contida em uma caixa retangular na metade da dimensão do código. Além disso, o ideal é escolher os pontos na caixa de modo que, ao aplicarmos ψ o $\mathcal{C}_T(2k, d)$ resultante também será homogêneo em cada camada (como pontos de um reticulado).

3.2.1 A construção dos códigos esféricos em camadas de toros.

Dados $k \geq 2$ e $d \in (0, \sqrt{2}]$, seja $\mathcal{C}(k, d)$ um código esférico k -dimensional qualquer, com distância mínima maior ou igual a d . O código esférico $\mathcal{C}_T(2k, d)$ é construído em duas etapas, como segue:

- (i) Seleccionamos os pontos em $\mathcal{C}(k, d)$ que possuem somente coordenadas não negativas. Vamos denotar este subcódigo por

$$\mathcal{C}(k, d)_+ = \{c \in \mathcal{C}(k, d) : c_i \geq 0, \quad 1 \leq i \leq k\}.$$

Cada ponto $c \in \mathcal{C}(k, d)_+$ define um toro planar T_c na esfera unitária S^{2k-1} .

- (ii) Para cada toro T_c definido por $\mathcal{C}(k, d)_+$, determinamos um conjunto finito de pontos

$$Y_{T_c} \subset \mathcal{P}_c$$

tal que

$$\|\psi_c(y) - \psi_c(x)\| \geq d \quad \forall x, y \in Y_{T_c}.$$

O código esférico resultante é dado por

$$\mathcal{C}_T(2k, d) = \bigcup_{c \in \mathcal{C}(k, d)_+} \psi(Y_{T_c}).$$

A estrutura de um $\mathcal{C}_T(2k, d)$ está diretamente relacionada ao subcódigo $\mathcal{C}(k, d)_+$ e ao conjunto de pontos Y_{T_c} escolhidos. Em (i) é desejável que $\mathcal{C}(k, d)_+$ tenha boa densidade em S^{k-1} e, se possível, alguma propriedade algébrica ou geométrica. Para este propósito, podemos considerar um $\mathcal{C}_T(k, d)$ ou qualquer código esférico k -dimensional

conhecido, como os descritos no Capítulo 1. Inclusive um código esférico não estruturado pode ser usado, uma vez que a cardinalidade dos toros é pequena em relação ao número de pontos no código. Para a etapa (ii), uma boa opção consiste em considerar pontos de algum reticulado k -dimensional conhecido, ou ainda, pontos gerados por grupos comutativos, ou cíclicos, como apresentados na Seção 3.4.

3.3 Limitantes para $\mathcal{C}_T(2k, d)$

Nesta seção apresentamos limitantes, inferior e superior, para o número máximo de pontos em um código esférico em camadas de toros. O termo limitante inferior, tem aqui o significado de que existe um código $\mathcal{C}_T(2k, d)$ que tem pelo menos esse número de pontos. Naturalmente, é sempre possível retirar pontos de qualquer uma das camadas e produzir um $\mathcal{C}_T(2k, d)$ com uma cardinalidade menor.

3.3.1 Um limitante inferior para o número máximo de pontos

Para um dado $d \in (0, \sqrt{2}]$, podemos construir um $\mathcal{C}_T(2k, d)$, escolhendo Y_{T_c} como um subconjunto de um reticulado retangular contido em cada uma das caixas \mathcal{P}_c , associadas às camadas de toros do código.

Com efeito, seja $c_i = (c_{i1}, c_{i2}, \dots, c_{ik}) \in \mathcal{C}(k, d)_+$ um toro selecionado para a construção de um $\mathcal{C}_T(2k, d)$ e u um ponto de um reticulado retangular k -dimensional obtido pela dilatação do reticulado \mathbb{Z}^k em cada uma das direções canônicas,

$$u = \sum_{j=1}^k m_j a_{ij} e_j,$$

onde a_{ij} representa o fator de dilatação da j -ésima coordenada e m_j é um inteiro.

Cada lado da caixa \mathcal{P}_{c_i} , associada ao toro c_i , tem comprimento igual a $2\pi c_{ij}$, logo podemos determinar o número máximo de pontos deste reticulado que cabem na caixa, encontrando, para cada $1 \leq j \leq k$, o menor $a_{ij} \in \mathbb{R}$ que satisfaz

$$d(\psi_c(a_{ij}e_i), \psi_c(0)) \geq d.$$

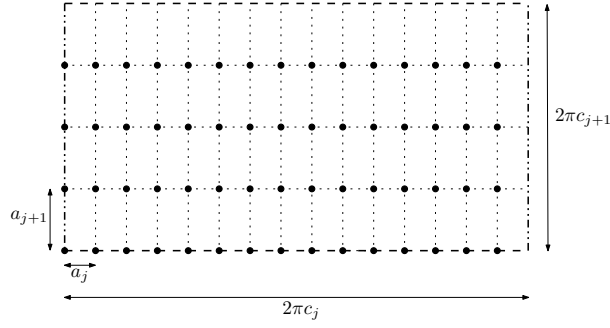


Figura 3.2: Ilustração de uma grade colocada num toro planificado

Como

$$d(\psi_c(a_{ij}e_i), \psi_c(0)) = 2c_{ij} \operatorname{sen} \left(\frac{a_{ij}}{2c_{ij}} \right) \leq d,$$

devemos ter

$$a_{ij} \geq 2c_{ij} \operatorname{arcsen} \left(\frac{d}{2c_{ij}} \right)$$

Com base nisso, podemos estabelecer a seguinte Proposição.

Proposição 3.4 *Para um dado $\mathcal{C}(k, d)_+$ com $|\mathcal{C}(k, d)_+|$ pontos, é possível a construção de um $\mathcal{C}_T(2k, d)$ com $M(2k, d)$ pontos, onde*

$$M(2k, d) = \sum_{i=1}^{|\mathcal{C}(k, d)_+|} \prod_{j=1}^k W_{ij}$$

e

$$W_{ij} = \begin{cases} \left\lfloor \frac{\pi}{\operatorname{arcsen} \frac{d}{2c_{ij}}} \right\rfloor, & \text{se } \left| \frac{d}{2c_{ij}} \right| \leq 1 \\ 1, & \text{se } \left| \frac{d}{2c_{ij}} \right| > 1 \end{cases}$$

3.3.2 Um limitante superior

Suponha novamente que tenhamos $|\mathcal{C}(k, d)_+|$ toros definidos pelo subcódigo $\mathcal{C}(k, d)_+$. Seja $c_i = (c_{i1}, c_{i2}, \dots, c_{ik})$ o i -ésimo elemento de $\mathcal{C}(k, d)_+$. Sem perda de generalidade

vamos assumir que $c_{ij} \geq c_{ij+1} \forall i, j$. Podemos utilizar (2.2) para obter o seguinte limitante superior para o número de pontos $M_{T_{c_i}}$ em cada um dos toros $T_{c_i} \in \mathcal{C}(k, d)_+$.

$$M_{T_{c_i}} \leq \left\lfloor \frac{\pi^k}{(\arcsen \frac{d}{4})^k} \prod_{j=1}^k c_{ij} \Lambda_k \right\rfloor = M_{T_{c_i}}^*$$

onde Λ_k é a máxima densidade de centro de um empacotamento em \mathbb{R}^k .

No entanto, uma consideração adicional se faz necessária.

Se algum c_{ij} for muito pequeno, podemos obter

$$\left\lfloor \frac{\pi^k}{(\arcsen \frac{d}{4})^k} \prod_{j=1}^k (c_{ij}) \Lambda_k \right\rfloor \approx 0.$$

Neste caso devemos remover a última coordenada de c_i e distribuir os pontos numa das faces da caixa correspondente ao toro T_{c_i} .

Seja

$$M_{T_{c_i}}^p = \left\lfloor \frac{\pi^p}{(\arcsen \frac{d}{4})^p} \prod_{j=1}^p (c_{ij}) \Lambda_p \right\rfloor, \quad 1 \leq p \leq k$$

o número máximo de pontos que cabem na p -face da caixa ($p = 1$ corresponde a colocar os pontos num círculo de raio igual a c_{i1} e $p = k$ corresponde a colocar os pontos na caixa retangular k -dimensional definida pelas coordenadas de c_i).

Assim, o número máximo de pontos que podem ser alocados em cada toro é dado por

$$M_{T_{c_i}}^* = \max_{1 \leq p \leq k} M_{T_{c_i}}^p.$$

Desta forma, podemos estabelecer um limitante superior para o número total de pontos em um $\mathcal{C}_T(2k, d)$, usando $M_{T_{c_i}}^*$ como definido acima.

Proposição 3.5 *Dado um $\mathcal{C}(k, d)_+$ com $|\mathcal{C}(k, d)_+|$ pontos, o número total de pontos em um $\mathcal{C}_T(2k, d)$ satisfaz*

$$M(2k, d) \leq \sum_{i=1}^{|\mathcal{C}(k, d)_+|} M_{T_{c_i}}^*$$

A Tabela 3.1 mostra uma comparação entre os limitantes aqui desenvolvidos e alguns códigos esféricos $\mathcal{C}_T(2k, d)$ construídos na Seção 3.4. É possível notar que o limitante superior pode ser assintoticamente atingido quando d decresce.

d	$\mathcal{C}_T(4, d)$	Limitante inferior	Limitante superior
0.5	172	120	194
0.4	308	208	360
0.3	798	612	826
0.2	2718	2148	2854
0.1	22,406	18,884	22,478
0.01	2.279×10^7	1.967×10^7	2.279×10^7

Tabela 3.1: Comparação entre limitantes e alguns códigos $\mathcal{C}_T(4, d)$.

3.3.3 Códigos esféricos em camadas de toros nas dimensões ímpares

A folheação da esfera unitária por toros planares foi feita para dimensões pares. Contudo, podemos construir um código $\mathcal{C}_T(2k+1, d)$ em duas etapas.

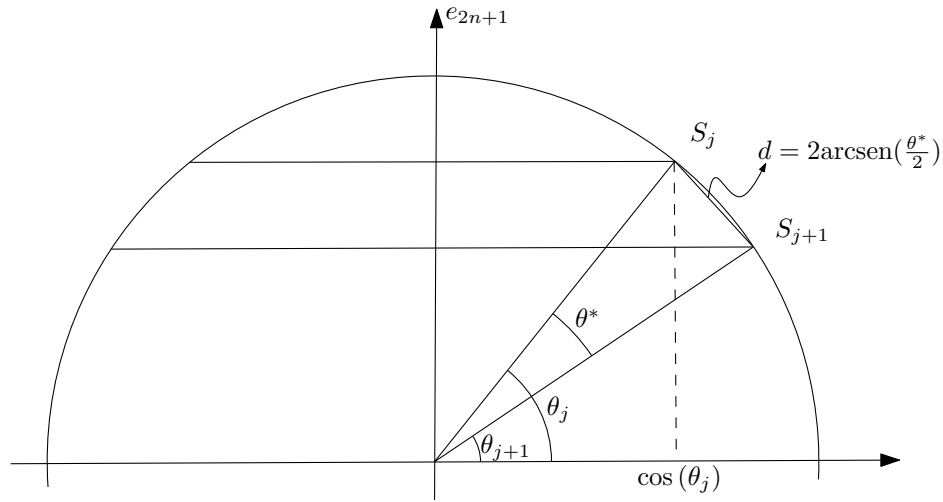
Inicialmente “cortamos” a esfera unitária $S^{2k} \subset \mathbb{R}^{2k+1}$ por hiperplanos perpendiculares ao vetor canônico e_{2k+1} , de forma que a distância mínima entre dois hiperplanos quaisquer seja pelo menos d . Cada um desses cortes determina uma esfera em \mathbb{R}^{2k} que pode ser normalizada e, sobre a esfera unitária resultante, pode-se construir um \mathcal{C}_T escalonado.

Seja θ^* o ângulo entre dois hiperplanos consecutivos. Se $\theta^* \geq 2 \arcsen\left(\frac{d}{2}\right)$, a distância entre os hiperplanos será pelo menos d e o raio de cada esfera S_j será dado por $r_j = \cos(\theta_j)$, com $\theta_j = \frac{\pi}{2} - j\theta^*$, conforme ilustrado na Figura 3.3.

A Tabela 3.2 apresenta uma comparação entre alguns $\mathcal{C}_T(5, d)$ e códigos apple-peeling apresentados em [15].

3.3.4 Densidade de um $\mathcal{C}_T(2k, d)$

Geometricamente, a diferença entre um código esférico em camadas de toros e um código apple-peeling consiste no fato que, no $\mathcal{C}_T(2k, d)$ a esfera de dimensão $2k$ é folheada

Figura 3.3: Primeira etapa da construção de um $\mathcal{C}_T(2k+1, d)$.

d	$\mathcal{C}_T(5, d)$	$\mathcal{C}_A(5, d)$
0.8	48	48
0.7	98	64
0.6	196	160
0.5	374	336
0.4	872	872
0.3	3,232	2,960
0.2	17,140	15,424
0.1	296,426	256,760
0.05	4,824,018	4,164,152

Tabela 3.2: Comparação entre códigos esféricos em \mathbb{R}^5 .

por toros planares e cada camada do código é construída através de um empacotamento esférico k -dimensional. Nos apple-peeling, as esferas são folheadas recursivamente por hiperplanos, até obter-se um círculo, onde, finalmente, é inscrito um polígono regular.

Esta diferença se reflete em termos da densidade do código resultante. É esperado que a densidade de um $\mathcal{C}_T(2k, d)$ se comporte como a densidade de um cartesiano de empacotamentos esféricos.

Em cada toro T_c é possível atingir, assintoticamente, a densidade do melhor empacotamento em \mathbb{R}^k , fazendo $d \rightarrow 0$ [49]. No entanto a densidade do $\mathcal{C}_T(2k, d)$, depende da escolha dos toros T_c , ou seja, depende do subcódigo $\mathcal{C}(k, d)_+$.

Considerando a melhor escolha para cada um dos casos, podemos estabelecer a seguinte Conjectura sobre a densidade dos códigos esféricos em camadas de toros.

Conjectura 3.1 *A densidade $\Delta_{\mathcal{C}_T}$ de um código esférico em camadas de toros $\mathcal{C}_T(2k, d)$, construído na Seção 3.2.1, satisfaz*

$$\Delta_{\mathcal{C}_T} \leq \Delta_{\Lambda_k \times \Lambda_{k-1}},$$

onde $\Delta_{\Lambda_k \times \Lambda_{k-1}}$ representa a densidade do empacotamento esférico, obtido como um cartesiano dos melhores empacotamentos esféricos k -dimensional e $(k-1)$ -dimensional.

Em termos assintóticos, quando $d \rightarrow 0$, a densidade de um $\mathcal{C}_T(2k, d)$ é melhor do que a densidade de um código apple-pelling. No entanto, conforme apresentamos no Capítulo 1, existem duas famílias de códigos (wrapped e laminados) que são assintoticamente densos na esfera, isto é, atingem a densidade do melhor empacotamento esférico da dimensão anterior. Os códigos esféricos em camadas de toros não são assintoticamente densos na esfera, mas possuem outras importantes vantagens, sobretudo para distâncias não muito pequenas ($d > 0.01$).

3.4 Códigos esféricos quase comutativos

Códigos esféricos gerados por grupos comutativos, conforme estudado no Capítulo 2, possuem uma forte estrutura algébrica que lhes confere excelentes propriedades de homogeneidade e simetria. No entanto, quando o número de pontos aumenta, a densidade destes códigos torna-se ruim, devido ao fato de morarem num único toro planar (ou em dois, nas dimensões ímpares).

Nesta seção mostramos como utilizar a boa estrutura desses códigos, para construir um código esférico $\mathcal{C}_T(2k, d)$, em camadas de toros que contém, em cada uma, um código de grupo comutativo. Daí a denominação de *códigos esféricos quase comutativos*. No mesmo sentido, utilizaremos o termo *código esférico quase cíclico* quando cada uma das camadas contiver um código de grupo cíclico.

A ideia básica para a construção dos códigos esféricos quase comutativos, consiste em determinar um código de grupo comutativo para cada um dos toros definidos na etapa (i) da construção de um $\mathcal{C}_T(2k, d)$.

Para construir um código de grupo comutativo no toro T_{c_i} precisamos definir um grupo comutativo de matrizes ortogonais $G(M, k)$, de ordem M e um vetor inicial x_0 .

Na Seção 2.2, estudamos o problema do vetor inicial para códigos de grupo comutativos, onde era procurado o melhor vetor inicial x_0 para um dado grupo $G(M, k)$. Aqui, temos um problema dual.

O vetor inicial do código de grupo comutativo $\mathcal{C}_{\mathcal{G}_{c_i}}$, que será construído no toro T_{c_i} , é conhecido

$$x_{0i} = (c_{i1}, \dots, c_{ik}).$$

Além disso, também sabemos que a distância mínima do código é um valor dado d . Estas duas informações eram exatamente o que se procurava no problema do vetor inicial.

O que nos interessa agora é a solução do seguinte problema:

- Para um dado vetor inicial $x_0 \in S^{k-1}$ e $d \in (0, 2]$, qual é o grupo comutativo $G(M, k)$ de matrizes ortogonais que determina um código de grupo comutativo $\mathcal{C}_{\mathcal{G}}(M, d)$ com a maior cardinalidade M ?

Formalmente, dado um vetor unitário x_0 e $d \in (0, 2]$, desejamos

$$\begin{aligned} &\text{maximizar} && M \\ &\text{Suj. a} && \|G_i x_0 - x_0\| \geq d \quad i = 1, 2, \dots, M. \end{aligned} \tag{3.6}$$

De acordo com (2.1), os elementos $G_i \in G(M, k)$ podem ser escritos na forma pseudo-diagonal

$$G_i = \text{diag}[R_1(i), \dots, R_w(i), \mu(i)_{2w+1}, \dots, \mu(i)_k]_{k \times k},$$

onde

$$R_j(i) = \begin{pmatrix} \cos(\frac{2\pi b_{ij}}{M}) & -\sin(\frac{2\pi b_{ij}}{M}) \\ \sin(\frac{2\pi b_{ij}}{M}) & \cos(\frac{2\pi b_{ij}}{M}) \end{pmatrix} \text{ e } b_{ij} \in Z \text{ and } \mu(i)_l = \pm 1, l = 2w+1, \dots, k.$$

Desta forma, as variáveis do problema (3.6) são todos os elementos b_{ij} que definem as rotações $R_j(i)$. Ou, o que é equivalente, são todas as representações de um grupo abstrato de ordem M em \mathcal{O}_k .

Na seção 3.4.1 abordamos (3.6) de maneira subótima, construindo grupos comutativos que são quocientes do melhor reticulado bidimensional. Desta forma possivelmente estaremos colocando uma quantidade menor de pontos M_i nos toros T_{c_i} , em troca do conhecimento dos parâmetros do empacotamento esférico associado à pré-imagem de cada toro.

Uma abordagem mais otimizada de (3.6) é apresentada na Seção 3.4.2, onde propomos um algoritmo para a procura do melhor código de grupo cíclico em cada camada. Como veremos, para distâncias mínimas assintoticamente pequenas, ambas soluções resultam em códigos com densidades muito próximas.

Não obstante, a resolução de (3.6) para códigos de grupo comutativo com distâncias não tão pequenas, pode ainda ser melhor explorada para maximizar a quantidade de pontos do código.

3.4.1 Códigos quase comutativos construídos a partir do reticulado A_2

Nesta seção apresentamos a construção de um código esférico quase comutativo em \mathbb{R}^4 que contém, em cada camada, pontos do reticulado A_2 ligeiramente deformado. Como consequência, obteremos um código homogêneo em cada camada, cuja pré-imagem pode ser vista como um grupo finito aditivo em \mathbb{R}^2 , dado pelo quociente de dois reticulados.

A primeira etapa desta construção consiste em escolher um bom código esférico em \mathbb{R}^2 , que irá definir os toros em S^3 que serão utilizados no código.

Como o melhor código esférico em \mathbb{R}^2 com distância mínima d é único, a menos de rotação, e é simétrico (o código é o conjunto de pontos de um polígono regular inscrito em S^1), a única escolha que resta é determinar uma boa rotação para os pontos no quadrante positivo. Nossa escolha consiste em alocar os pontos sobre S^1 , de forma que

fiquem simétricos em relação a reta bissetriz do primeiro quadrante, conforme ilustrado na Figura 3.4. Assim,

$$SC(2, d)_+ = \left\{ (\cos(\alpha_{\pm j}), \sin(\alpha_{\pm j})), 0 \leq \alpha_{\pm j} \leq \frac{\pi}{2}, 1 \leq j \leq k \right\}, \quad (3.7)$$

com

$$\alpha_{\pm j} = \frac{\pi}{4} \pm (2j - 1) \arcsen\left(\frac{d}{2}\right), \quad 1 \leq j \leq \left\lfloor \frac{\pi - 2 \arcsen(d/2)}{8 \arcsen(d/2)} \right\rfloor. \quad (3.8)$$

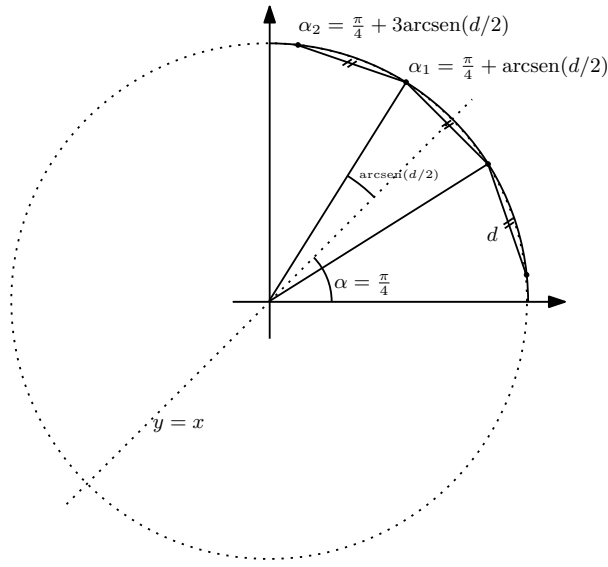


Figura 3.4: $SC(2, d)_+$ simétrico em relação a reta $y = x$

A segunda etapa da construção consistem em “preencher” cada toro definido em $SC(2, d)_+$.

Dado $c_i = (c_{i1}, c_{i2}) \in \mathcal{C}(k, d)_+$ e $d \in (0, \sqrt{2}]$, vamos construir um código de grupo comutativo, com vetor inicial c_i sobre o toro planar T_{c_i} , que tenha distância mínima maior ou igual a d , quocientando o reticulado A_2 por algum subreticulado ortogonal.

Sem perda da generalidade, vamos considerar $c_{i2} > c_{i1}$, caso contrário podemos considerar o toro simétrico.

Seja

$$\mathcal{P}_{c_i} = \{x \in \mathbb{R}^2 : 0 \leq x_1 \leq 2\pi c_{i1} \text{ e } 0 \leq x_2 \leq 2\pi c_{i2}\}.$$

a caixa que representa a planificação do toro T_{c_i} .

Geometricamente, o que precisamos fazer é deformar o reticulado A_2 de forma que a imagem de seus pontos pela aplicação ψ_{c_i} (3.2) satisfaça

$$||\psi_{c_i}(z) - \psi_{c_i}(w)|| \geq d, \quad \forall \quad z, w \in \mathcal{P}_{c_i}. \quad (3.9)$$

Além disso, para que os pontos no toro T_{c_i} formem um grupo comutativo, devemos ajustar um subreticulado ortogonal $\Lambda^i \subset A_2$ de forma que seus pontos coincidam com os vértices de \mathcal{P}_{c_i} .

Seja

$$A_2^i = \beta_i \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix},$$

a matriz geradora do reticulado A_2 , multiplicada por um fator de dilatação $\beta_i > 0$, que será determinado para satisfazer (3.9).

Claramente, o reticulado gerado por A_2^i terá distância mínima β_i , uma vez que a distância mínima em A_2 é igual a 1.

Como $c_{i1} \leq c_{i2}$, segue de (3.3) que β_i deve satisfazer

$$\beta_i \geq 2c_{i1} \arcsen\left(\frac{d}{2c_{i1}}\right)$$

Naturalmente, para que β_i esteja bem definido devemos garantir que $c_{i1} \geq \frac{d}{2}$. Na verdade vamos impor uma condição mais forte do que esta.

Em alguns toros (muito “magrinhos”) onde $c_{i1} \approx 0$, mesmo que $c_{i1} \geq \frac{d}{2}$, pode ocorrer que a deformação β_i seja tão grande em relação à distância mínima d , que vale a pena descartar c_{i1} , considerando que T_{c_i} é degenerado num círculo.

Vamos impor esta condição precisamente. Dizemos que um toro definido por $c_i = (c_{i1}, c_{i2})$, com $c_{i1} \leq c_{i2}$ é *d-degenerado* se $c_{i1} \leq \frac{d}{\sqrt{3}}$ ¹. Neste caso, os pontos da camada serão os vértices de um polígono regular de lado d , inscrito na circunferência de raio igual c_{i2} .

¹ O valor $c_{i1} \leq \frac{d}{\sqrt{3}}$ é obtido impondo que $\frac{2\pi c_{i1} - \beta_i}{\beta_i} \geq 2$, ou seja, é possível colocar ao menos dois pontos na direção e_1 da caixa.

Assim, o número de pontos num toro degenerado T_{c_i} é dado por

$$M_i = \left\lfloor \frac{\pi}{\arcsen\left(\frac{d}{2c_{i2}}\right)} \right\rfloor.$$

Nos toros degenerados, os pontos serão da forma

$$x = (c_{i1}, 0, c_{i2} \cos(\Delta_i u), c_{i2} \sin(\Delta_i u)),$$

onde

$$\Delta_i = 2 \arcsen\left(\frac{d}{2c_{i2}}\right) \text{ e } u = 1, 2, \dots, M_i.$$

Para os toros não degenerados ($c_{i1} > \frac{d}{\sqrt{3}}$), vamos considerar a menor deformação possível, ou seja,

$$\beta_i = 2c_{i1} \arcsen\left(\frac{d}{2c_{i1}}\right). \quad (3.10)$$

Note que

$$\beta_i = 2c_{i1} \arcsen\left(\frac{d}{2c_{i1}}\right) = \left(\frac{\arcsen\left(\frac{d}{2c_{i1}}\right)}{\frac{d}{(2c_{i1})}}\right) d,$$

como

$$\lim_{x \rightarrow 0} \frac{\arcsen(x)}{x} = 1,$$

concluimos que a deformação provocada por ψ_{c_i} torna-se arbitrariamente pequena quando $d \rightarrow 0$.

Seja Λ^i um subreticulado ortogonal de A_2^i gerado pelos vetores $v_{i1} = \beta_i(1, 0)$ e $v_{i2} = \beta_i(0, \sqrt{3})$.

Para cada toro não degenerado T_{c_i} , definimos o conjunto de vértices

$$V_i = \{\gamma_{i1}v_{i1}, \gamma_{i2}v_{i2}\},$$

onde

$$\gamma_{i1} = \left\lfloor \frac{2\pi c_{i1} - \beta_i}{\beta_i} \right\rfloor \text{ e } \gamma_{i2} = \left\lfloor \frac{2\pi c_{i2} - \beta_i}{\beta_i \sqrt{3}} \right\rfloor$$

determinam o número máximo de múltiplos de v_{ij} que cabem na caixa \mathcal{P}_{c_i} .

Os vértices em V_i definem uma caixa retangular $\mathcal{Q}(\Lambda^i) \subset \mathcal{P}_{c_i}$,

$$\mathcal{Q}(\Lambda^i) = \{x = (x_1, x_2) \in \mathbb{R}^2 : 0 \leq x_1 \leq \gamma_{i1}v_{i1} \text{ e } 0 \leq x_2 \leq \gamma_{i2}v_{i2}\}.$$

O conjunto de pontos do toro não degenerado T_{c_i} , que formam esta camada do código, é dado por

$$Y_{T_{c_i}} = A_2^i \cap \mathcal{Q}(\Lambda^i).$$

O número de pontos do código neste toro é dado por

$$M_i = 2(\gamma_{i1} + 1)(\gamma_{i2} + 1).$$

A Figura 3.5 ilustra este procedimento.

Um ajuste final deve ser feito, dilatando os vetores da caixa $\mathcal{Q}(\Lambda^i)$ em cada uma das direções, de modo que seus vértices coincidam com os vértices do toro T_{c_i} .

Podemos utilizar o Teorema 2.6 para obter a classificação do grupo comutativo em cada camada, bem como seu conjunto de geradores do grupo, considerando a Forma Normal de Smith da matriz

$$W = \begin{pmatrix} \beta_i & 0 \\ \beta_i \frac{1}{2} & \beta_i \frac{\sqrt{3}}{2} \end{pmatrix}^{-1} \begin{pmatrix} \beta_i \gamma_{i1} & 0 \\ 0 & \beta_i \gamma_{i2} \sqrt{3} \end{pmatrix}.$$

A Tabela 3.3 apresenta a cardinalidade e a densidade de vários códigos de grupo comutativo em \mathbb{R}^4 . Pode-se notar que a densidade se aproxima da densidade do reticulado $\Lambda = A_2 \times \mathbb{Z}$ que é de 0.604599788078, confirmando, neste caso, a conjectura 3.1.

d	M	Densidade
0, 5	168	0, 557042
0, 1	22028	0, 584311
0, 01	$2, 2726 \times 10^7$	0, 602834
0, 001	$2, 2786 \times 10^{10}$	0, 604442
0, 0001	$2, 2792 \times 10^{14}$	0, 604585

Tabela 3.3: Códigos esféricos quase comutativo em \mathbb{R}^4 para várias distâncias mínimas.

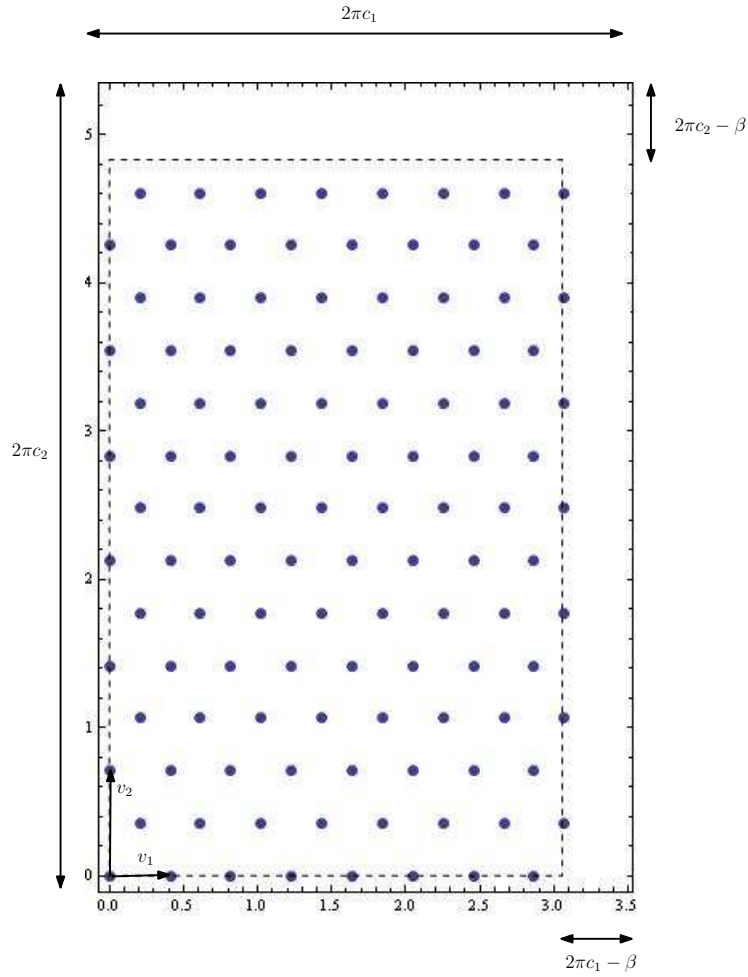


Figura 3.5: Uma camada de um código esférico quase comutativo.

A técnica descrita aqui, para a construção de um $\mathcal{C}_T(4, d)$, pode ser utilizada para produzir códigos esféricos quase comutativos em qualquer dimensão. Em particular, em dimensões onde o reticulado D_n ainda tem boa densidade, a construção torna-se ainda mais prática, pois podemos utilizar o subreticulado ortogonal $2\mathbb{Z}^n \subset D_n$.

3.4.2 Códigos esféricos quase cíclicos

Podemos construir um código esférico em camadas de toros, colocando em cada uma das camadas um código de grupo cíclico. A título de exemplificar como isso pode ser feito, vamos apresentar a construção de um código esférico quase cíclico em \mathbb{R}^4 . As ideias utilizadas neste podem ser naturalmente estendidas para dimensões maiores.

A primeira etapa da construção é idêntica à desenvolvida na seção anterior. A diferença estará na maneira de preencher cada camada.

Sabemos que a planificação de cada toro T_{c_i} é um retângulo cujos lados medem $2\pi c_{i1}$ e $2\pi c_{i2}$.

Na etapa (ii), vamos preencher cada toro T_{c_i} procurando um código de grupo cíclico com distância d com vetor inicial $x_{0_i} = (\cos(\alpha_j), 0, \sin(\alpha_j), 0)$ (definido em 3.8) que tenha o maior número de pontos possível.

Um código de grupo cíclico de ordem M em \mathbb{R}^4 é a órbita de um vetor inicial x_{0_i} , sobre a ação de um grupo cíclico de matrizes ortogonais gerado por uma matriz

$$G_i = \begin{pmatrix} \cos(\frac{2\pi g_{i1}}{M}) & \sin(\frac{2\pi g_{i1}}{M}) & 0 & 0 \\ -\sin(\frac{2\pi g_{i1}}{M}) & \cos(\frac{2\pi g_{i1}}{M}) & 0 & 0 \\ 0 & 0 & \cos(\frac{2\pi g_{i2}}{M}) & \sin(\frac{2\pi g_{i2}}{M}) \\ 0 & 0 & -\sin(\frac{2\pi g_{i2}}{M}) & \cos(\frac{2\pi g_{i2}}{M}) \end{pmatrix},$$

onde $\text{mdc}(g_{i1}, g_{i2}) = 1$. A pré-imagem de um código de grupo cíclico por $\psi_{x_{0_i}}$ é um subreticulado em \mathbb{R}^2 .

A procura pelo melhor código de grupo cíclico pode ser feita utilizando uma variação do método para procura do melhor código de grupo comutativo apresentando no Capítulo 2. Aqui temos a distância mínima d do código, mas não sabemos quantos pontos cabem em cada toro, ou seja, qual a cardinalidade M do grupo.

Uma alternativa é utilizar (2.2), para obter um limitante superior para esta quantidade e procurar, dentre os casos relevantes (Teorema 2.5), se existe algum código de grupo cíclico com M pontos e distância mínima d . Se existe, paramos a procura e alocamos os pontos no toro, através da órbita do grupo. Caso contrário, fazemos $M \leftarrow M - 1$ e repetimos o processo, até encontrar um código.

Um algoritmo para procura do melhor código de grupo em cada toro é apresentando a seguir.

Entrada: $d, x_{0_i} = (\cos(\alpha_i), 0, \sin(\alpha_i), 0)$
Saída: Geradores: $\{g_{i_1}, g_{i_2}\}$

$$M = \left\lfloor \frac{\pi^2 \cos(\alpha_i) \sin(\alpha_i)}{2\sqrt{3} \arcsen\left(\frac{d}{4}\right)^2} \right\rfloor;$$

$continue = 1;$
while $continue$ **do**
 para $g_{i_1} = 1$ **to** $\lfloor \frac{M}{2} \rfloor$ **faça**
 para $g_{i_2} = 1$ **to** $\lfloor \frac{M}{2} \rfloor$ **faça**
 se $\gcd(g_{i_1}, g_{i_2}) = 1$ **então**
 $\bar{d} = \min_{1 \leq j \leq \lfloor \frac{M}{2} \rfloor} \|(G_i)^j x_0 - x_0\|;$
 se $\bar{d} \geq d$ **então**
 Imprima $\{g_{i_1}, g_{i_2}\};$
 $continue = 0;$
 Pare;
 fim
 fim
 fim
 fim
 $M = M - 1;$
end

Algoritmo 2: Algoritmo para procura do melhor código de grupo cíclico com distância d e vetor inicial x_{0_i} .

3.4.3 Exemplo de um $\mathcal{C}_T(4, 0.3)$ quase cíclico

Apresentamos a seguir a construção de um código esférico quase cíclico em \mathbb{R}^4 com distância mínima $d = 0.3$.

- De (3.8) temos $\alpha_1 = 0.935966$, $\alpha_2 = 1.2371$ e $\alpha_3 = 1.53824$, que definem o subconjunto de nosso $SC(k, d)_+$ acima da linha $y = x$, de acordo com (3.7).
- Para cada T_{α_j} , devemos encontrar o melhor código de grupo cíclico utilizando o algoritmo 2. A Tabela 3.4 apresenta esses resultados.

Toro	α	δ_1	δ_2	dmin	M	(g_{i_1}, g_{i_2})
$T_{\alpha_{+1}}$	0.935966	0.593041	0.805173	0.30225	233	{1,98}
$T_{\alpha_{+2}}$	1.237103	0.327535	0.944839	0.301406	146	{22,1}
$T_{\alpha_{+3}}$	1.538240	0.032551	0.99947	0.312869	20	{0,1}

Tabela 3.4: Parâmetros de um $\mathcal{C}_T(4, 0.3)$ quase cíclico para os toros acima da reta $y = x$.

- Finalmente, para cada toro $T_{\alpha+i}$ consideramos a camada simétrica definida por $T_{\alpha-i}$, fazendo apenas uma permutação de coordenadas (Tabela 3.5).

Toro	α	δ_1	δ_2	dmin	M	Gerador
$T_{\alpha-1}$	0.634829	0.805173	0.593041	0.30225	233	{98,1}
$T_{\alpha-2}$	0.333694	0.944839	0.327535	0.301406	146	{1,22}
$T_{\alpha-3}$	0.032559	0.99947	0.032551	0.312869	20	{1,0}

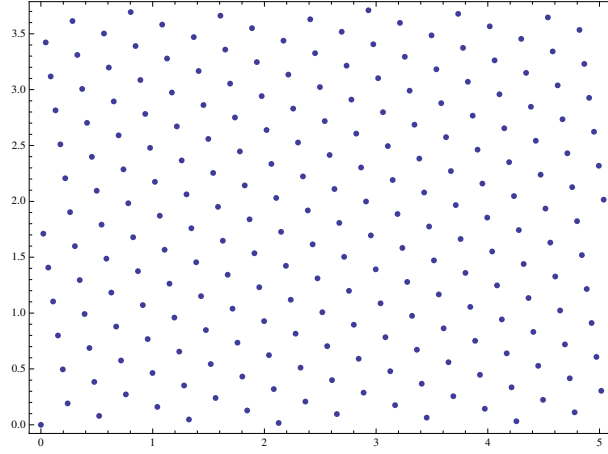
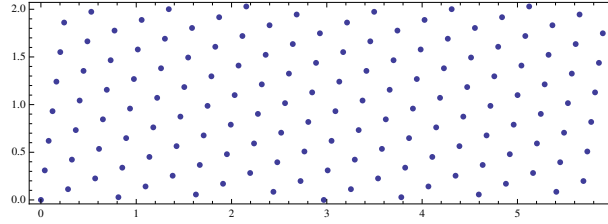
Tabela 3.5: Parâmetros de um $\mathcal{C}_T(4, 0.3)$ quase cíclico para os toros abaixo da reta $y = x$

O código resultante $\mathcal{C}_T(4, 0.3)$ tem 6 camadas, duas a duas simétricas, com 20, 146, 233, 233, 146, 20 pontos respectivamente. O número total de pontos no código é 798.

Observação: Os pontos em um código quase cíclico podem ser gerados facilmente. Neste exemplo, para gerar os 798 pontos do código, são necessárias apenas as informações que constam na segunda e nas duas últimas colunas da Tabela 3.4, ou seja, apenas 12 parâmetros são necessários para calcular as coordenadas dos 798 pontos do código em \mathbb{R}^4 .

Nas Figuras 3.6 e 3.7 apresentamos a pré-imagem de duas camadas do código $\mathcal{C}_T(4, 0.3)$. Pode-se notar que a distribuição de pontos em cada uma das caixas “tende” à distribuição de pontos do reticulado A_2 , indicando que a solução encontrada pelo algoritmo 2 corresponde a um empacotamento com boa densidade no plano.

Na Tabela 3.6, apresentamos uma comparação entre alguns códigos quase cíclicos para \mathbb{R}^4 e outros códigos esféricos conhecidos.

Figura 3.6: Pré-imagem do toro $T_{\alpha_{-1}}$.Figura 3.7: Pré-imagem do toro $T_{\alpha_{-2}}$.

d	$\mathcal{C}_T(4, d)$	apple-peeling	wrapped	laminados
0.5	172	136	*	*
0.4	308	268	*	*
0.3	798	676	*	*
0.2	2.718	2.348	*	*
0.1	22.406	19.364	17.198	16.976
0.01	$2,27 \times 10^7$	$1,97 \times 10^7$	$2,31 \times 10^7$	$2,31 \times 10^7$

Tabela 3.6: Códigos esféricos em \mathbb{R}^4 para várias distâncias mínimas. * significa valores não conhecidos

3.5 Decodificação de códigos esféricos em camadas de toros

Seja $\mathcal{C}_T(2k, d)$ um código esférico no qual as camadas de toros são definidas pelos vetores $c_i \in \mathcal{C}(k, d)_+$, $1 \leq i \leq \mu = |\mathcal{C}(k, d)_+|$. Dado $x \in S^{2k-1}$, um vetor unitário qualquer², queremos encontrar $y \in \mathcal{C}_T(2k, d)$ tal que

$$\|x - y\| \leq \|x - z\| \quad \forall z \in \mathcal{C}_T(2k, d).$$

Podemos escrever

$$\begin{aligned} x &= \left(\gamma_1 \left(\frac{x_1}{\gamma_1}, \frac{x_2}{\gamma_1} \right), \gamma_2 \left(\frac{x_3}{\gamma_2}, \frac{x_4}{\gamma_2} \right), \dots, \gamma_k \left(\frac{x_{2k-1}}{\gamma_k}, \frac{x_{2k}}{\gamma_k} \right) \right) \\ x &= \left(\gamma_1 \left(\cos \frac{\theta_1}{\gamma_1}, \sin \frac{\theta_1}{\gamma_1} \right), \dots, \gamma_k \left(\cos \frac{\theta_k}{\gamma_k}, \sin \frac{\theta_k}{\gamma_k} \right) \right). \end{aligned} \quad (3.11)$$

Onde,

$$\begin{aligned} \gamma_i &= \sqrt{x_{2i-1}^2 + x_{2i}^2}, \quad 1 \leq i \leq k \\ \theta_i &= \arccos \left(\frac{x_{2i-1}}{\gamma_i} \right) \gamma_i, \quad 1 \leq i \leq k. \end{aligned}$$

Isto significa que x pertence a um toro planar cujos raios são as coordenadas do vetor $c_x = (\gamma_1, \gamma_2, \dots, \gamma_k)$. Em geral x_c não pertence ao conjunto $\mathcal{C}(k, d)_+$.

Seja

$$\bar{x}_i = \left(c_{i1} \left(\cos \frac{\theta_1}{\gamma_1}, \sin \frac{\theta_1}{\gamma_1} \right), \dots, c_{ik} \left(\cos \frac{\theta_k}{\gamma_k}, \sin \frac{\theta_k}{\gamma_k} \right) \right)$$

a projeção ortogonal de x no toro T_{c_i} , i.e.,

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

Vamos denotar por

$$\Delta_i = \|x - \bar{x}_i\|$$

² De acordo com a Proposição 2.3, é suficiente considerarmos o vetor x unitário, caso contrário ($se \|x\| > 1$) podemos simplesmente normalizá-lo.

a menor distância entre o ponto x e o toro T_{c_i} .

Seja ξ o índice que corresponde ao toro mais próximo de x , i. e. $\Delta_\xi \leq \Delta_i, \forall 1 \leq i \leq \mu$.

Com alta probabilidade, o vetor $y \in \mathcal{C}_T(2k, d)$ mais próximo de x pertence ao toro T_{c_ξ} e pode ser encontrado decodificando o vetor

$$z_\xi = \psi_{c_\xi}^{-1}(\bar{x}_\xi) = \left(\frac{\theta_1 c_{\xi_1}}{\gamma_1}, \frac{\theta_2 \delta_2}{\gamma_2}, \dots, \frac{\theta_k c_{\xi_k}}{\gamma_k} \right)$$

na caixa k -dimensional \mathcal{P}_{c_ξ} correspondente à planificação do toro T_{c_ξ} , utilizando um algoritmo similar ao Algoritmo 1 desenvolvido para decodificação em códigos de grupo comutativo (se o conjunto de pontos na caixa \mathcal{P}_{c_ξ} são os pontos de um reticulado, o algoritmo é idêntico).

Seja $w_\xi \in \mathbb{R}^k$ o ponto que decodifica z_ξ na caixa \mathcal{P}_{c_ξ} e $y_\xi = \psi_{c_\xi}(w_\xi)$ sua imagem em S^{2k-1} . Vamos denotar por $d_\xi = \|y_\xi - x\|$ a distância entre o ponto x e o candidato a decodificação $y_\xi \in \mathcal{C}_T(2k, d)$.

Se $d_\xi < \frac{d}{2}$ a decodificação está terminada, e assumiremos que y_i é o vetor do código mais perto de x . Caso contrário, pode existir um ponto y_i em algum outro toro T_{c_i} que esteja mais próximo de x do que y_ξ . Vamos determinar precisamente, quais os toros do código necessitam ser testados.

Seja $\mathcal{N} = (\xi_1, \xi_2, \dots, \xi_j)$, $j \leq \mu$, o conjunto de índices correspondente aos toros T_{c_i} que satisfazem

$$\Delta_i < d_\xi,$$

Vamos considerar que \mathcal{N} está ordenado, de forma que $\Delta_{\xi_i} \leq \Delta_{\xi_{i+1}} \quad \forall i = 1, 2, \dots, j$.

Devemos então decodificar

$$z_{\xi_i} = \psi_{c_{\xi_i}}^{-1}(\bar{x}_{\xi_i}), \quad \forall \xi_i \in \mathcal{N}$$

obtendo, assim, um conjunto candidatos $Y = \{y_\xi, y_{\xi_1}, y_{\xi_2}, \dots, y_{\xi_j}\}$, $Y \subset \mathcal{C}_T(2k, d)$, com cada $y_{\xi_j} \in T_{c_{\xi_j}}$.

O resultado da decodificação de x será o ponto $y^* \in Y$ que satisfaz

$$\|y^* - x\| \leq \|y - x\| \quad \forall y \in Y.$$

A cardinalidade dos toros é pequena em relação ao número de pontos no código, além disso, a condição $\Delta_i < d_\xi$ será satisfeita por um número ainda menor de toros, de modo que o conjunto Y deve conter poucos candidatos.

Como no caso dos códigos de grupo comutativo, para a decodificação num $C_T(2k, d)$ não é necessário listar os pontos do código esférico, apenas os candidatos do conjunto Y precisam ser calculados explicitamente. Além disso, a cada decodificação em $T_{c_{\xi_j}}$ obtém um valor d_{ξ_j} que, se for menor do que d_ξ pode ser utilizado para restringir ainda mais o conjunto Y .

A Figura 3.8 ilustra o procedimento de decodificação num $C_T(2k, d)$. Cada circunferência representa um toro T_c do código. No caso ilustrado, apenas os toros T_{c_ξ} (o mais próximo de x) e o toro T_{c_w} devem ser analisados.

A complexidade da decodificação num código esférico em camadas de toros $2k$ -dimensional é dominada pela complexidade de duas decodificações em dimensão k , uma para encontrar os toros, outra para construir o conjunto Y .

A decodificação em códigos esféricos em camadas de toros é um estudo ainda em andamento e pode ser aprimorada, principalmente em relação ao cálculo preciso do número de operações envolvidas.

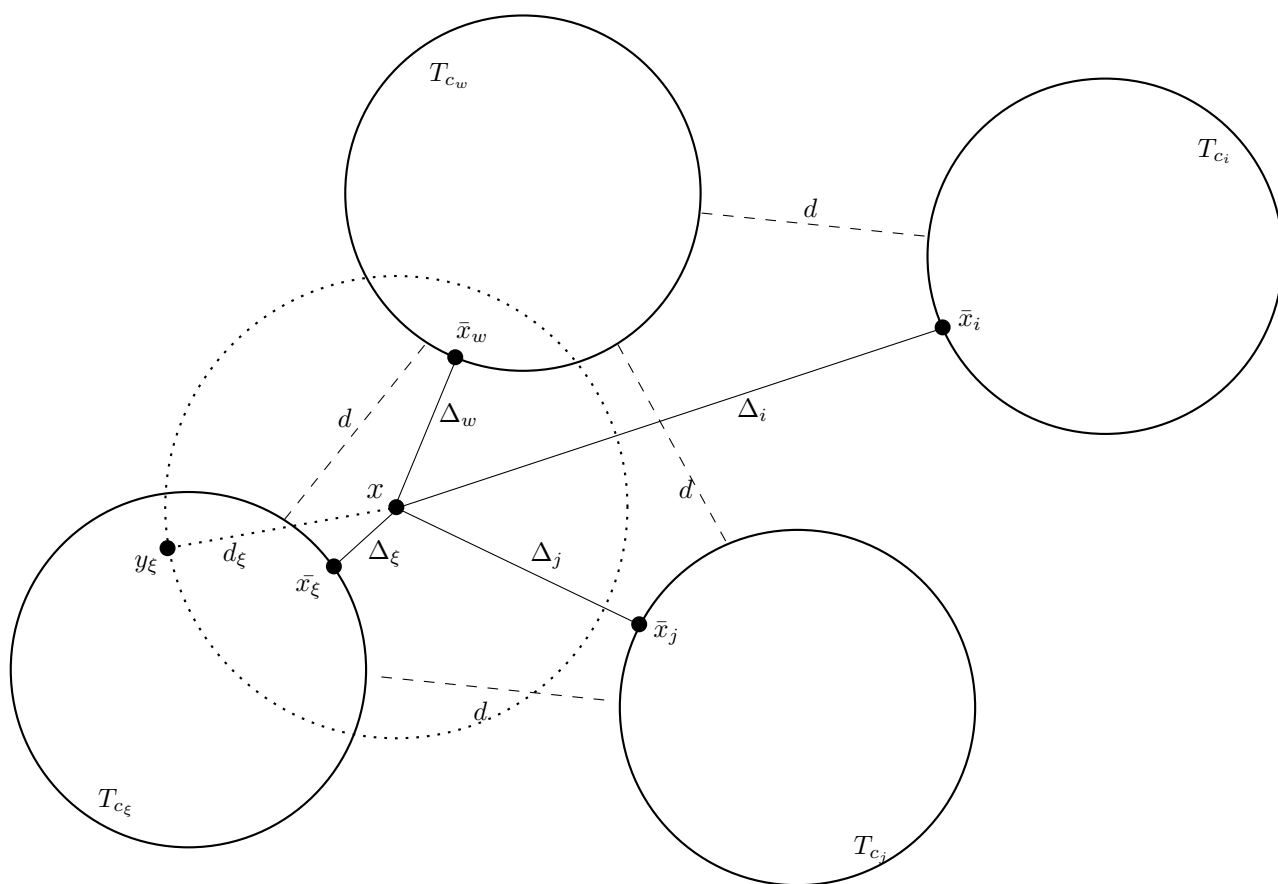


Figura 3.8: Ilustração do processo de decodificação num $\mathcal{C}_T(2k, d)$.

Considerações finais e perspectivas futuras

O assunto central deste trabalho é o estudo do problema do empacotamento em esferas euclidianas para a construção de códigos esféricos. No Capítulo 2 desenvolvemos um método que permite encontrar um código esférico de grupo comutativo com máxima distância mínima, dados a dimensão e o número de pontos do código. Uma nova família de códigos esféricos foi introduzida no Capítulo 3, os códigos \mathcal{C}_T . Estes códigos podem ser construídos em qualquer dimensão, a partir de uma distância mínima dada, distribuindo os pontos em camadas de toros que folheiam a esfera unitária. Devido a sua associação com reticulados, os \mathcal{C}_T possuem uma forte estrutura algébrica e geométrica. Em cada camada, os pontos do código podem ser gerados por um grupo de matrizes ortogonais.

Existem várias conexões entre as contribuições dadas neste trabalho e estudos que ainda podem ser desenvolvidos. Por exemplo, a decodificação de códigos esféricos $2k$ –dimensionais através de diagrama de treliça de reticulados k –dimensionais pode ser melhor explorada. Como devem ser construídas as camadas de toros de modo a minimizar a complexidade de decodificação do código? Baseado em [62], códigos de grupos cíclicos podem ser decodificados através do cálculo da distância de um conjunto discreto de pontos à uma reta. Em que circunstâncias este processo é vantajoso em relação ao uso de treliças?

Outra possibilidade é a construção de códigos esféricos em camadas de toros para aplicações específicas como, por exemplo, quantização esférica. Alguns dos melhores resultados conhecidos para este problema [28] utilizam os códigos n –dimensionais *wrapped* que são decodificados em reticulados no \mathbb{R}^{n-1} . Que tipo de vantagens podem ser obtidas se a decodificação for feita em reticulados na metade da dimensão do código?

Como distribuir os pontos em cada camada dos toros de modo a facilitar o cálculo das regiões de Voronoi do código?

Uma conexão que parece bastante promissora é a relação entre os códigos esféricos em camadas de toros e alguns trabalhos de G. Ungerboeck [59, 60, 61] sobre "Trellis code modulation". Neste sentido, um problema importante é a construção de um particionamento da constelação de sinais de modo a obter-se uma maior distância livre entre sequencias que podem ser transmitidas. A construção em camadas de toros fornece uma alternativa natural para este particionamento, que poderia ser utilizado para obtenção de um ganho em bits (bitgain) na transmissão de sinais sobre um canal Gaussiano.

As ideias utilizadas para a construção dos códigos esféricos em camadas de toros podem ser estendidas para a construção de curvas contínuas na esfera unitária. Para este problema, que tem conexão com codificação conjunta fonte-canal [62], procura-se colocar a maior curva possível sobre S^{n-1} de modo que a distância entre duas voltas quaisquer da curva seja pelo menos um valor d . Podemos construir toros em S^{n-1} afastados a uma distância d e, sobre cada toro, "enrolar" uma curva contínua. Qual a melhor maneira de construir a curva em cada toro? Uma alternativa pode ser utilizar o método desenvolvido no Capítulo 2 para procura do melhor código de grupo comutativo, restringindo-o para o caso cíclico e adaptá-lo para calcular a distância entre retas numa caixa retangular.

Alguns aprofundamentos pontuais podem ser feitos para melhorar aspectos específicos de construções que foram apresentadas neste trabalho, por exemplo:

- Na procura por códigos de grupos comutativos ótimos:
 - É possível a solução de todos os problemas do vetor inicial de uma única vez?
 - O conjunto de casos a serem analisados, classificados nos teoremas 2.4 e 2.5, pode ainda ser refinado? Seja inicialmente, seja iterativamente, após a obtenção de um código com boa distância?
- Na construção de códigos esféricos quase comutativos:

- Como otimizar o número de pontos em cada toro? Ou seja, para um dado vetor inicial $x_0 \in S^{k-1}$ e $d \in (0, 2]$, qual é o grupo comutativo $G(M, k)$ de matrizes ortogonais que determina um código de grupo comutativo $\mathcal{C}_G(M, d)$ com a maior cardinalidade M ?
- A construção e a decodificação destes códigos está fortemente relacionada com subreticulados retangulares. Neste sentido a obtenção de subreticulados ortogonais que resultem em treliças de baixa complexidade é um problema importante, sobretudo para a construção de códigos em dimensões maiores.

A associação entre códigos de grupo comutativo $2k$ -dimensionais e reticulados em \mathbb{R}^k permite uma conexão natural com o estudo de alguns criptossistemas pósquânticos baseados em reticulados [4]. Um importante problema nesta área é o cálculo do vetor de norma mínima de certos reticulados Q -ários, que podem ser vistos como os pontos do quociente de reticulados, restrito a uma caixa ortogonal, ou seja, a pré-imagem de um código de grupo comutativo. Por interesse prático, tais problemas são considerados em dimensões altas ($n \geq 500$), o que implica em chaves públicas grandes e uma preocupação constante em diminuí-las. A conexão com códigos de grupo comutativo, ou cíclicos, pode ser utilizada para reduzir o tamanho dessas chaves? Algoritmos para decodificação em códigos de grupo comutativo podem ser adaptados para ataques à criptossistemas baseados em reticulados?

Neste sentido, há ainda outras conexões que podem ser investigadas, como a utilização de códigos esféricos para a construção de criptossistemas pósquânticos. Até o momento, os criptossistemas baseados em códigos conhecidos na literatura [4] utilizam códigos binários. É possível a utilização de códigos esféricos? Que tipos de códigos? Como construir uma chave pública?

Referências Bibliográficas

- [1] Alves, C. *Tese de doutorado: Reticulados e Códigos*. PhD thesis, Universidade Estadual de Campinas - Unicamp., 2008.
- [2] Astola, J. T. The tietäväinen bound for spherical codes. *Disc. Appl. Math* 7 (1984).
- [3] Banihashemi, A., & Blake, I. On the trellis complexity of root lattices and their duals. *IEEE Trans. Inform. Theory* 45, 6 (Sept. 1999), 2168–2172.
- [4] Bernstein, D. J., Buchmann, J., & Dahmen, E. *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 2008.
- [5] Biglieri, E., & Elia, M. Cyclic-group codes for the gaussian channel (corresp.). *IEEE Transaction on Information Theory* 22, 5 (Sep 1976), 624–629.
- [6] Blake, I. F. The leech lattice as a code for the gaussian channel. *Information and Control* 19, 1 (1971), 66–74.
- [7] Böröczky, K. Packing of spheres in spaces of constant curvature". *Acta Math. Acad. Scient. Hung.* 32 n. 3-4 (1978), 243–261.
- [8] Cohen, H. *A course in computational algebraic number theory*. Springer-Verlag New York, Inc., New York, NY, USA, 1996.
- [9] Cohn, H., & Elkies, N. New upper bounds on sphere packings i. *Annals of Mathematics*. 157 (2003), 689.
- [10] Conway, J. H., & Sloane, N. J. A. *Sphere packings, lattices and groups*, third ed., vol. 290. Springer-Verlag, New York, 1999.

- [11] Costa, S., Strapasson, J. E., Siqueira, R., & Muniz, M. Circulant graphs, lattices and spherical codes. *International Journal of Applied Mathematics* 20 (2007), 581–594.
- [12] Costa, S. I. R., Muniz, M., Agustini, E., & Palazzo, R. Graphs, tessellations, and perfect codes on flat tori. *IEEE Trans. Inform. Theory* 50, 10 (2004), 2363–2377.
- [13] Costa, S. I. R., Strapasson, J. E., Siqueira, R. M., & Muniz, M. Circulant graphs, lattices and spherical codes. *International Journal of Applied Mathematics* 20 (2007), 581–594.
- [14] Delsarte, P. Spherical codes and designs. *Geom. Dedic* 6 (1977).
- [15] El Gamal, A. A., Hemachandra, L. A., I., S., & Wei, V. K. Using simulated annealing to design good codes. *IEEE Trans. Inform. Theory* IT-33 no 1 (1987), 116–123.
- [16] Ericson, T., & Zinoviev, V. *Codes on Euclidean Spheres*. North-Holland Mathematical Library, 2001.
- [17] Fejes Tóth, L. Über die dichteste kugellagerung. *Math. Zeitschrift* 48 (1943), 676–684.
- [18] Ferrari, A. J., Torezzan, C., Jorge, G. C., & Costa, S. I. R. Um algoritmo de treliça para decodificação em códigos de grupo comutativo. In *XXVII Simpósio Brasileiro de Telecomunicações, SBrT 2009* (2009).
- [19] Forney, G. D., & Trott, M. D. The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders. *IEEE Trans. Inform. Theory* IT-39 (1993), 1491–1513.
- [20] Forney, Jr., G. D. Final report on a coding system design for advanced solar missions. Tech. rep., Contract NAS2–3637, NASA Ames Research, 1976.
- [21] Forney, Jr., G. D. Coset codes. I. Introduction and geometrical classification. *IEEE Trans. Inform. Theory* 34, 5, part 2 (1988), 1123–1151. Coding techniques and coding theory.

- [22] Forney, Jr., G. D. Coset codes. II. Binary lattices and related codes. *IEEE Trans. Inform. Theory* 34, 5, part 2 (1988), 1152–1187. Coding techniques and coding theory.
- [23] Forney, Jr., G. D. Geometrically uniform codes. *IEEE Trans. Inform. Theory* 37, 5 (1991), 1241–1260.
- [24] Gantmacher, F. R. *The theory of matrices. Vol. 1. Transl. from the Russian by K. A. Hirsch. Reprint of the 1959 translation.* Providence, RI: AMS Chelsea Publishing, 1998.
- [25] Hamkins, J., & Zeger, K. Asymptotically dense spherical codes. i. wrapped spherical codes. *IEEE Trans. Inform. Theory* 43, 6 (Nov. 1997), 1774–1785.
- [26] Hamkins, J., & Zeger, K. Asymptotically dense spherical codes .ii. laminated spherical codes. *IEEE Trans. Inform. Theory* 43, 6 (Nov. 1997), 1786–1798.
- [27] Hamkins, J., & Zeger, K. Optimal rate allocation for shape-gain gaussian quantizers. In *Proc. IEEE International Symposium on Information Theory* (24–29 June 2001), p. 182.
- [28] Hamkins, J., & Zeger, K. Gaussian source coding with spherical codes. *IEEE Trans. Inform. Theory* 48, 11 (Nov. 2002), 2980–2989.
- [29] Hardin, R. H., & Sloane, N. J. A. Codes (spherical) and designs (experimental). *Different Aspects of Coding Theory, ed. A. R. Calderbank, AMS Series Proceedings Symposia Applied Math* 50 (1995), 179–206.
- [30] Ingemarsson, I. Commutative group codes for the gaussian channel. *IEEE Transaction on Information Theory* 19, 2 (Mar 1973), 215–219.
- [31] Kabatiansky, G. A., & Levenshtein, V. I. Bounds for packing on a sphere and in space. *PPI* 1 (1978).
- [32] Karlof, J. Decoding spherical codes for the gaussian channel. *IEEE Trans. Inform. Theory* 39, 1 (1993), 60–65.

-
- [33] Kottwitz, D. A. The densest packing of equal circles on a sphere. *Acta Crystallographica Section A* 47, 3 (May 1991), 158–165.
- [34] Krejić, N., Martínez, J. M., Mello, M., & Pilotta, E. A. Validation of an augmented lagrangian algorithm with a gauss-newton hessian approximation using a set of hard-spheres problems. *Comput. Optim. Appl.* 16, 3 (2000), 247–263.
- [35] Levenshtein, V. I. Boundaries for packings in n-dimensional euclidean space. *Dokl. Akad. Nauk* 6 (1979), 1299–1303.
- [36] McLaren, A. D. Optimal numerical integration on a sphere. *Math. Comp.* 17 (1963), 361–383.
- [37] Melnyk, T. W., Knop, O., & Smith, W. R. Extremal arrangements of points and unit charges on a sphere: equilibrium configurations revisited. *Can. J. Chem.* 55 (1977), 1745–1761.
- [38] Micciancio, D., & Goldwasser, S. *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.
- [39] Mittelman, H. D., & Vallentin, F. High accuracy semidefinite programming bounds for kissing numbers. *arxiv: 0902.1105 1* (2009), 1–7.
- [40] Musin, O. R. The problem of the twenty-five spheres. *UMN* 58 (2003), 153–154.
- [41] Musin, O. R. The kissing number in four dimensions. *Annals of Mathematics* 1 (2008), 1.
- [42] Nurmela, K. J. Constructing spherical codes by global optimization methods. Tech. rep., Digital Systems Laboratory, 1995.
- [43] Odlyzko, A. M., & Sloane, N. J. A. New bounds on the number of unit spheres that can touch a unit sphere in n dimensions. *J. Comb. Theory, Ser. A* 26, 2 (1979), 210–214.

- [44] Pfender, F., Ziegler, G. M., Unter, G., & Ziegler, M. Kissing numbers, sphere packings, and some unexpected proofs. *Notices Amer. Math. Soc* 51 (2004), 873–883.
- [45] Rankin, R. A. The closest packing of spherical caps in n dimensions. *Proc. Glasgow Math. Assoc.* 2 (1954), 139–144.
- [46] Schütte, K., & van der Waerden, B. Das problem der dreizehn kugeln. *Math. Ann.* 125 (1953), 325–334.
- [47] Shannon, C. E. A mathematical theory of communication. *Bell system technical journal* 27 (1948).
- [48] Siqueira, R. M. *Tese de doutorado: Codigos esfericos com simetrias ciclicas*. PhD thesis, Universidade Estadual de Campinas., 2006.
- [49] Siqueira, R. M., & Costa, S. I. Flat tori, lattices and bounds for commutative group codes. *Des. Codes Cryptography* 49, 1-3 (2008), 307–321.
- [50] Slepian, D. Group codes for the gaussian channel. *The Bell System Technical Journal* 47 (1968), 575–602.
- [51] Sloane, N. Tables of sphere packings and spherical codes. *IEEE Trans. Inform. Theory* 27, 3 (May 1981), 327–338.
- [52] Sloane, N. J. A. A note on the leech lattice as a code for the gaussian channel. *Information and Control* 46, 3 (1980), 270–272.
- [53] Sloane, N. J. A. Spherical codes: Nice arrangements of points on a sphere in various dimensions. web page. World Wide Web electronic publication, May Consultada em maio de 2009. <http://www.research.att.com/njas/packings/>.
- [54] Tarnay, T., & Gáspár, Z. Spherical circle-packing in nature, practice and theory. *Topologie Structurale* 9 (1984), 39–58.
- [55] Tarokh, V., Vardy, A., & Zeger, K. Universal bound on the performance of lattice codes. *IEEE Trans. Inform. Theory* 45, 2 (1999), 670–681.

- [56] Torezzan, C., Costa, S. I. R., & Vaishampayan, V. A. Spherical codes on torus layers. *International Symposium on Information Theory*. . (2009), .
- [57] Torezzan, C., Strapasson, J. E., Costa, S. I. R., & Siqueira, R. M. Optimum commutative group codes. (*Submetido para: SIAM J. Discrete Math.*) . (2008), .
- [58] Tóth, F. Über eine abschätzung des kürzesten abstandes zweier punkte eines auf einer kugelfläche liegenden punktsystems. *Jahresbericht Deut. Math. Verein* 53 (1943), 66–68.
- [59] Ungerboeck, G. Channel coding with multilevel/phase signals. *IEEE Transactions on Information Theory* 28, 1 (Jan 1982), 55–67.
- [60] Ungerboeck, G. Trellis-coded modulation with redundant signal sets part i: Introduction. *IEEE Communications Magazine*. 25, 2 (Feb 1987), 5–11.
- [61] Ungerboeck, G. Trellis-coded modulation with redundant signal sets part ii: State of the art. *IEEE Communications Magazine*. 25, 2 (Feb 1987), 12–21.
- [62] Vaishampayan, V. A., & Costa, S. I. R. Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. *IEEE Trans. Inform. Theory* 49, 7 (2003), 1658–1672.
- [63] Viterbi, A. Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. *Information Theory, IEEE Transactions on* 13, 2 (1967), 260–269.
- [64] Zong, C. *Sphere Packings*. Universitext, 1999.

ANEXO1

Demonstração da proposição 3.2, [1].

Seja $D(y) = d^2(\psi(y), \psi(0)) = \|\psi(y) - \psi(0)\|^2 = 4 \sum_{i=1}^m \delta_i^2 \sin^2(\frac{y_i}{2\delta_i})$ e $S_r = \{y \in \mathbb{R}^m; d^2(y) = r^2\}$. Como S_r é um conjunto compacto a função D restrita a ele assume máximo e mínimo.

Usando o método dos multiplicadores de Lagrange vê-se que estes pontos y devem satisfazer o sistema de equações

$$\begin{cases} \nabla D(y) = 2\lambda y \\ y_1^2 + \dots + y_m^2 = r^2 \end{cases}$$

Como $\frac{\partial D}{\partial y_i}(y) = 4\delta_i \sin\left(\frac{y_i}{2\delta_i}\right) \cos\left(\frac{y_i}{2\delta_i}\right) = 2\delta_i \sin\left(\frac{y_i}{\delta_i}\right)$, o sistema fica

$$\lambda y_i = \delta_i \sin\left(\frac{y_i}{\delta_i}\right) \text{ e } 4 \sum_{i=1}^m \delta_i^2 \sin^2\left(\frac{y_i}{2\delta_i}\right) = r^2.$$

Assim, se I é o conjunto de índices i tais que $y_i \neq 0$, segue que os quocientes

$$\frac{\sin\left(\frac{y_i}{\delta_i}\right)}{\frac{y_i}{\delta_i}}, \quad -\pi \leq \frac{y_i}{\delta_i} \leq \pi, \quad i \in I$$

são todos iguais. Seja $h(x) = \frac{\sin x}{x}$. Então, $h'(x) = \frac{x \cos x - \sin x}{x^2}$.

Afirmção: $p(x) = x \cos x - \sin x$ é decrescente em $[0, \pi]$.

De fato, $p'(x) = -x \sin x \leq 0, \forall x \in [0, \pi]$.

Assim, se $x > 0$ então $p(x) < p(0) = 0$. Portanto, $h'(x) < 0, \forall x \in (0, \pi]$. Logo, $h(x)$ é decrescente em $(0, \pi]$. Assim, como $h(x)$ é função par e decrescente $(0, \pi]$, portanto injetora em $(0, \pi]$, então $\frac{y_i}{\delta_i} = \frac{y_l}{\delta_l}$ para todo i e l em I .

Sendo I o conjunto dos índices i tais que $y_i \neq 0$, temos os seguintes casos a considerar, restritos a $y_1^2 + \dots + y_m^2 = r^2$.

1-) Se $y_i \neq 0$ e $y_j = 0, \forall j \neq i$, e $i, j = 1, \dots, m$ então $y_i^2 = r^2$ implica $y_i = \pm r$. Logo, $y = (0, \dots, 0, \pm r, 0, \dots, 0)$.

2-) Se $y_i, y_j \neq 0$ e $y_k = 0, \forall k \neq i, j$ e $i, j, k = 1, \dots, m$ então $y_i^2 + y_j^2 = r^2$. Como para

$\forall i, j = 1, \dots, m$ temos $\frac{y_i}{\delta_i} = \frac{y_j}{\delta_j}$, segue que $y_i = \frac{y_j \delta_i}{\delta_j}$. Logo, $\frac{y_j^2 \delta_i^2}{\delta_j^2} + y_j^2 = r^2 \Rightarrow y_j^2 \left(\frac{\delta_i^2}{\delta_j^2} + 1 \right) = r^2 \Rightarrow y_j^2 (\delta_i^2 + \delta_j^2) = r^2 \delta_j^2 \Rightarrow y_j^2 = \frac{r^2 \delta_j^2}{\delta_i^2 + \delta_j^2} \Rightarrow y_j = \pm \frac{r \delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}$. Assim,

$$y_i = \frac{\pm \frac{r \delta_j}{\sqrt{\delta_i^2 + \delta_j^2}} \delta_i}{\delta_j} = \pm \frac{r \delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}. \text{ Logo, } y = \left(0, \dots, 0, \pm \frac{r \delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \dots, 0, \pm \frac{r \delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \dots, 0 \right).$$

m-) Seguindo desta forma, para $y_i \neq 0, \forall i = 1, \dots, m$ temos que

$$y = \left(\pm \frac{r \delta_1}{\sqrt{\delta_1^2 + \dots + \delta_m^2}}, \pm \frac{r \delta_2}{\sqrt{\delta_1^2 + \dots + \delta_m^2}}, \dots, \pm \frac{r \delta_m}{\sqrt{\delta_1^2 + \dots + \delta_m^2}} \right).$$

Concluimos então que os pontos críticos serão da forma:

$$\begin{aligned}
C_m^1 \text{ pontos } y &= (0, \dots, 0, \quad, r, 0, \dots, 0) \\
C_m^2 \text{ pontos } y &= \left(0, \dots, 0, \pm \frac{r\delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \dots, 0, \pm \frac{r\delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \dots, 0 \right) \\
&\vdots \\
C_m^m \text{ pontos } y &= \frac{r(\pm\delta_1, \pm\delta_2, \dots, \pm\delta_m)}{\sqrt{\delta_1^2 + \dots + \delta_m^2}}
\end{aligned}$$

Agora, vamos analisar o máximo e o mínimo da função D restrita a $y_1^2 + \dots + y_m^2 = r^2$.

Sem perda de generalidade, assumimos δ_i de forma ordenada: $\delta_1 \geq \delta_2 \geq \dots \geq \delta_m$.

- Para os pontos críticos da forma (1) temos

$$D(y) = d^2(\psi(y), \psi(0)) = 4\delta_i^2 \sin^2 \left(\frac{r}{2\delta_i} \right) = r^2 \left(\frac{\sin \left(\frac{r}{2\delta_i} \right)}{\frac{r}{2\delta_i}} \right)^2.$$

$$\text{Seja } f(x) = r^2 \left(\frac{\sin \left(\frac{r}{2x} \right)}{\frac{r}{2x}} \right)^2 \text{ e } g(z) = \left(\frac{\sin z}{z} \right)^2. \text{ Observamos que } f(x) = r^2 g \left(\frac{r}{2x} \right).$$

Assim,

$$f'(x) = r^2 g' \left(\frac{r}{2x} \right) \left(\frac{-2r}{4x^2} \right) = -\frac{r^3}{2x^2} g' \left(\frac{r}{2x} \right). \quad (\text{A.1})$$

Seja $h(z) = \frac{\sin z}{z}$. Como $h(z)$ é decrescente e positiva em $(0, \pi]$ segue que $(h(z))^2 = g(z)$ é decrescente em $(0, \pi]$, ou seja, $g'(z) < 0$ em $(0, \pi]$.

Se $\frac{r}{2x} \in (0, \pi]$ então $g' \left(\frac{r}{2x} \right) < 0$. Logo, de (A.1), temos que $f'(x) > 0$ se $\frac{r}{2x} \in (0, \pi]$, ou seja, $f(x)$ é crescente se $\frac{r}{2x} \in (0, \pi]$.

Como $\delta_i \geq \delta_m, \forall i = 1, \dots, m$, segue que

$$f(\delta_i) = 4\delta_i^2 \sin^2 \left(\frac{r}{2\delta_i} \right) \geq 4\delta_m^2 \sin^2 \left(\frac{r}{2\delta_m} \right) = f(\delta_m), \quad \frac{r}{2x} \in (0, \pi].$$

- Para os pontos críticos da forma (2), temos

$$\begin{aligned}
 D(y) &= d^2(\psi(y), \psi(0)) = 4 \left(\delta_i^2 \sin^2 \left(\frac{\frac{r\delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}}{2\delta_i} \right) + \delta_j^2 \sin^2 \left(\frac{\frac{r\delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}}{2\delta_j} \right) \right) \\
 &= 4(\delta_i^2 + \delta_j^2) \sin^2 \left(\frac{r}{2\sqrt{\delta_i^2 + \delta_j^2}} \right) = r^2 \left(\frac{\sin \left(\frac{r}{2\sqrt{\delta_i^2 + \delta_j^2}} \right)}{\frac{r}{2\sqrt{\delta_i^2 + \delta_j^2}}} \right)^2.
 \end{aligned}$$

Como $f(x)$ é crescente e $\sqrt{\delta_i^2 + \delta_j^2} \geq \sqrt{\delta_{i+1}^2 + \delta_{j+1}^2} \geq \dots \geq \sqrt{\delta_{m-1}^2 + \delta_m^2} \geq \delta_m$ segue que $f(\sqrt{\delta_i^2 + \delta_j^2}) \geq f(\delta_m)$, $\forall i, j = 1, \dots, m$. Portanto,

$$4(\delta_i^2 + \delta_j^2) \sin^2 \left(\frac{r}{2\sqrt{\delta_i^2 + \delta_j^2}} \right) \geq 4\delta_m^2 \sin^2 \left(\frac{r}{2\delta_m} \right), \quad \frac{r}{2\sqrt{\delta_i^2 + \delta_j^2}} \in (0, \pi].$$

Continuando deste modo, para os pontos críticos da forma (m) temos,

$$D(y) = d^2(\psi(y), \psi(0)) = r^2 \left(\frac{\sin \left(\frac{r}{2\sqrt{\delta_1^2 + \dots + \delta_m^2}} \right)}{\frac{r}{2\sqrt{\delta_1^2 + \dots + \delta_m^2}}} \right)^2.$$

Mais uma vez, usando o fato de que $f(x)$ é crescente e

$$\begin{aligned}
 \sqrt{\delta_1^2 + \dots + \delta_m^2} &\geq \sqrt{\delta_1^2 + \dots + \hat{\delta}_i^2 + \dots + \delta_m^2} \geq \sqrt{\delta_1^2 + \dots + \hat{\delta}_i^2 + \dots + \hat{\delta}_j^2 + \dots + \delta_m^2} \geq \dots \\
 &\dots \geq \sqrt{\delta_i^2} \geq \delta_m,
 \end{aligned}$$

onde $\hat{\delta}_l$ denota a ausência de δ_l na soma acima, segue que

$$4(\delta_1^2 + \dots + \delta_m^2) \sin^2 \left(\frac{r}{2\sqrt{\delta_1^2 + \dots + \delta_m^2}} \right) \geq 4\delta_m^2 \sin^2 \left(\frac{r}{2\delta_m} \right), \quad \frac{r}{2\sqrt{\delta_1^2 + \dots + \delta_m^2}} \in (0, \pi].$$

Como em cada um dos casos temos as seguintes restrições:

$$\begin{aligned} r &\leq 2\pi\delta_i, \quad i = 1, \dots, m \\ r &\leq 2\pi\sqrt{\delta_i^2 + \delta_j^2}, \quad i, j = 1, \dots, m \\ &\vdots \\ r &\leq 2\pi\sqrt{\delta_1^2 + \dots + \delta_m^2}, \end{aligned}$$

e $2\pi\sqrt{\delta_1^2 + \dots + \delta_m^2} \geq \dots \geq 2\pi\sqrt{\delta_i^2 + \delta_j^2} \geq 2\pi\delta_i \geq 2\pi\delta_m$, tomando $r \leq 2\pi\delta_m$, temos que

$$4\delta_m^2 \sin^2 \left(\frac{r}{2\delta_m} \right) \leq d^2(\psi(y), \psi(0)) \leq 4(\delta_1^2 + \dots + \delta_m^2) \sin^2 \left(\frac{r}{2\sqrt{\delta_1^2 + \dots + \delta_m^2}} \right),$$

$\forall y$ tal que $\|y\| = r$.

Portanto o valor mínimo será obtido para,

$$y = (0, \dots, 0, \pm r, 0, \dots, 0)$$

na posição onde $\delta_i = \delta_{min}$ (valor mínimo de δ) e o valor máximo será para $\tilde{\delta} = \sqrt{\delta_1^2 + \dots + \delta_m^2}$, ou seja,

$$y = \frac{r}{\sqrt{\delta_1^2 + \dots + \delta_m^2}} (\pm\delta_1, \dots, \pm\delta_m)$$

(sobre a diagonal da “caixa” que define o toro).

Ainda, como $\sin x < x$, $\forall x > 0$, segue que

$$2\sqrt{\delta_1^2 + \dots + \delta_m^2} \sin \left(\frac{r}{2\sqrt{\delta_1^2 + \dots + \delta_m^2}} \right) < r$$

o que conclui a demonstração.