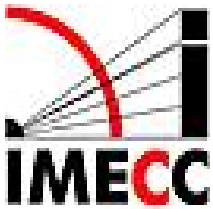
Universidade Estadual de Campinas
Instituto de Matemática, Estatística e
Computação Científica - IMECC
Departamento de Matemática



Reticulados e Códigos

Carina Alves

Tese de doutorado

Orientadora: **Prof^a. Dr^a. Sueli Irene Rodrigues Costa**

Novembro - 2008

Campinas - SP

[1]Este trabalho contou com apoio financeiro da Fapesp - processo n^o 04/12370 – 8

RETICULADOS E CÓDIGOS

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Carina Alves e aprovada pela comissão julgadora.

Campinas, 03 de Novembro de 2008.

Profa. Dra. Sueli Irene Rodrigues Costa

Orientadora

Banca Examinadora

1. Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)
2. Prof. Dr. Marcelo Firer (IMECC-UNICAMP)
3. Prof. Dr. José Plínio de Oliveira Santos (IMECC-UNICAMP)
4. Prof. Dr. Antonio Aparecido de Andrade (UNESP)
5. Prof. Dr. Marcelo Muniz Silva Alves (UFPR)

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do título de DOUTORA em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Bibliotecária: Maria Júlia Milani Rodrigues - CRB8a 2116

Alves, Carina

AL87r Reticulados e Códigos / Carina Alves – Campinas, [S.P.:s.n.], 2008.

Orientadora: Sueli Irene Rodrigues Costa

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

1. Distância mínima. 2. Teoria dos reticulados. 3. Teoria dos números algébricos. 4. Empacotamentos de esferas. 5. Geometria Discreta. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Lattices and codes

Palavras-chave em inglês (keywords): 1. Minimum distance. 2. Lattice theory. 3. Algebraic number theory. 4. Sphere packings. 5. Discrete geometry.

Área de concentração: Álgebra, Geometria/Topologia

Titulação: Doutora em Matemática

Banca examinadora:

Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)
Prof. Dr. Marcelo Firer (IMECC-UNICAMP)
Prof. Dr. José Plínio de Oliveira Santos (IMECC-UNICAMP)
Prof. Dr. Antonio Aparecido de Andrade (UNESP)
Prof. Dr. Marcelo Muniz Silva Alves (UFPR)

Data da defesa: 03/11/2008

Programa de Pós-Graduação: Doutorado em Matemática

Tese de Doutorado defendida em 03 de novembro de 2008 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). MARCELO FIRER

Prof(a). Dr(a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS

Prof(a). Dr(a). ANTONIO APARECIDO DE ANDRADE

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

"Meu Deus...
Não me deixes embriagar com o êxito,
quando o consigo,
nem a desesperar, se fracasso.
Sobretudo, faz-me sempre recordar que o fracasso
é a prova que antecede o êxito."

Mahatma Gandhi

Aos meus pais, Vanir e Atamir,

à minha irmã Luciana

e a todos aqueles que sempre tiveram por mim apreço e amor,

por tudo que esta conquista representa para eles,

assim como para mim.

dedico.

Agradecimentos

Ao concluir este trabalho, agradeço:

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

De maneira especial gostaria de agradecer a Profª. Drª. Sueli Irene Rodrigues Costa, pelo privilégio que tive em ser sua orientanda, pela competente e segura orientação durante o desenvolvimento do trabalho, pelo constante incentivo, paciência e amizade e por estes anos de convivência que muito me ensinou.

Aos membros da banca, pela disponibilidade e atenção despendida ao trabalho e por suas contribuições.

Aos professores da Universidade Estadual Paulista do Campus de São José do Rio Preto, pela amizade e excelente formação durante a graduação e o mestrado. Em particular, ao Prof. Dr. Antonio Aparecido de Andrade pela valiosa orientação durante a graduação e o mestrado, pelas parcerias durante o doutorado e pelas oportunidades, por ele, a mim oferecidas e às Profª. Drª. Aparecida Francisco da Silva, Erminia de L. C. Fanti e Maria Gorete Carreira Andrade, muita gratidão pelo incentivo, conselhos e amizade.

Aos professores da Unicamp pelos conhecimentos valiosos repassados durante todo o curso de doutorado.

Aos professores, Prof. Dr. Marcelo M. S. Alves, Prof. Dr José Plínio de Oliveira Santos, Prof. Marcelo Firer e Prof. Dr. Carlile Lavor, pelo estímulo, atenção e amizade.

Ao Prof. Dr. Emanuele Viterbo da Universidade da Calábria (UNICAL) - Itália, por ter me proporcionado a oportunidade de fazer um estágio em seu grupo de pesquisa, e também à todos os colegas do grupo de pesquisa da UNICAL.

*Aos meus pais Vanir Caldeira Alves e Atamir José Alves que me ensinam, me incentivam e possibilitam a sonhar e crer que tudo é possível. Que a todo momento, através de um abraço forte e um sorriso sincero, me fazem ver a vida com outros olhos, pelo apoio incondicional e pelo incentivo que sempre me deram em tudo que busquei realizar.

*A minha irmã Luciana Alves, por me apoiar principalmente nos momentos difíceis e por compartilhar os momentos de alegria.

*Aos meus avós que plantaram a semente no meu coração de perseverança e solidariedade, humildade e confiança, de amor e paz.

*Ao Thiago, pelo carinho, apoio e compreensão durante todo o tempo. Agradeço também à sua família, por todo apoio que me deram.

*Aos meus colegas e amigos de grupo de pesquisa do grupo de "Teoria de Informação e Códigos", Antônio, Allan, Andréia, Cristiano, João, Nolmar, Rogério e Tatiana, pela interação, discussões, sugestões e pelo agradável convívio.

*A todos os colegas e amigos de doutorado, companheiros de luta, Ana Cristina, Cristiane (em especial, estudando juntas desde a graduação), Luci Any, Mariana, Rosane, Fábio e Fabiano, por compartilhar as alegrias, tristezas e dificuldades durante nossa caminhada que ora completamos e que me proporcionaram a aquisição de um bem valoroso e grande: o binômio coleguismo-amizade.

*Aos amigos Agnaldo, Danilo, Grasiele, Katia, Tatiane e Paulo, pela valiosa amizade desde os tempos de graduação.

*A minha amiga Ana Patricia, que conheci na Itália e que muito me ajudou. Através dela pude perceber que nos lugares mais improváveis é possível encontrar pessoas que parecem ser anjos enviados por Deus.

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

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

*A Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) pelo fundamental apoio na iniciação científica, mestrado, doutorado (Processo 04/12370-8) e projetos temáticos (Processos 02/07473-7 e 07/07473-7) no qual este trabalho se inclui.

Este trabalho não é apenas minha conquista, é a conquista de todas aquelas pessoas, que durante os últimos dois anos, apoiaram, ajudaram, sem medir esforços, e acima de tudo, acreditaram que era possível. À todas estas pessoas eu agradeço.

Resumo

Neste trabalho abordamos questões associadas à minimização da probabilidade de erro para a transmissão de sinais em canais gaussianos e em canais com desvanecimento do tipo Rayleigh. Usando a teoria de reticulado ideal, construímos rotações do reticulado n-dimensional dos inteiros via corpos ciclotômicos. Reticulados construídos deste modo permitem estimativas da distância produto mínima, parâmetro que controla a probabilidade de erro no envio de informações em canais com desvanecimento do tipo Rayleigh. Apresentamos uma nova construção de tais reticulados no caso em que n é uma potência de 2 e no caso em que $n = 3$. Estudamos os códigos esféricos que são associados a reticulados com o intuito de obter a maior distância euclidiana mínima, parâmetro que controla a probabilidade de erro em canais gaussianos. Códigos esféricos gerados por grupos comutativos de matrizes ortogonais em dimensão par, $2m$, podem ser determinados, via mergulhos de toros planares, pelo quociente de dois reticulados em $\mathbb{R}^m$, onde o sub-reticulado possui uma base cujos vetores são mutuamente ortogonais. Pesquisamos a existência de sub-reticulados nestas condições, nos reticulados com maior densidade de empacotamento em dimensões 2, 3, 4 e 8. Pudemos assim construir famílias de códigos de grupo comutativo que se aproximam do limitante para a distância mínima nas dimensões 4, 6, 8 e 16.

Abstract

We approach here some problems related to minimizing the error probability in signals transmission over Gaussian and Rayleigh channels. Algebraic ideal lattice theory is used to construct rotations of the n-dimensional integer lattice via cyclotomic fields. This construction allows to evaluate the minimum product distance of the lattice, parameter which controls the signal transmission probability through Rayleigh fading channels. We present here such constructions in the cases $n = 3$ and n a power of 2. Spherical codes generated by commutative group codes of orthogonal matrices in even dimensions, $2m$, can be determined by a quotient of n-dimensional lattices, where the sublattice has an orthogonal basis. We characterize families of such sublattices in the lattices with best packing densities in dimensions 2, 3, 4, 6 e 8 and construct the associated spherical codes which approach the commutative group code upper bound for the minimum distance.

CONTEÚDO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Q}$	conjunto dos números racionais
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
$\partial(f(X))$	grau do polinômio f(X)
L, M, K	corpos de números
L/K	extensão de corpos
$[L:K]$	grau de L/K
$\prod$	produtório
$\sum$	somatório
$\det A$	determinante de A
(a_{ij})	matriz
$d(\alpha_1, \ldots, \alpha_n)$	discriminante de uma n-upla
$\mathcal{O}_K$	anel dos inteiros de K
$\#X$	cardinalidade do conjunto X
$\mathfrak{a}, \mathfrak{b}, \mathcal{I} \ldots$	ideais
$\varphi(n)$	função de Euler para o inteiro n
$A[X]$	anel dos polinômios sobre A em X
r_1	número de mergulhos canônicos reais
r_2	número de mergulhos canônicos complexos
ζ_n	$e^{2\pi i/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, raiz primitiva n-ésima da unidade

$\overline{x}$	conjugado complexo do elemento x
d_K	discriminante absoluto do corpo K
$Tr_{L/K}$	traço em relação à extensão L/K
$\mathcal{N}_{L/K}$	norma em relação à extensão L/K
$irr(\alpha, K)$	polinômio irredutível de α sobre K
$< \alpha_1, \ldots, \alpha_n >$	ideal gerado por $\alpha_1, \ldots, \alpha_n$
$Gal(L/K)$	grupo de Galois de L/K
fcc	reticulado face-centered cubic
mcc	reticulado mean-centered cubic
$\min(X)$	mínimo do conjunto X
ρ	raio de empacotamento
$\delta(\Lambda)$	densidade de centro do reticulado Λ
$\overline{\sigma}$	conjugação complexa ($\overline{\sigma}(x) = \overline{x}$)
vol	volume
d_{min}	distância mínima entre dois pontos
$d_{p,min}$	distância produto mínima
Δ	densidade de empacotamento esférico
η	eficiência espectral
E	energia da constelação
E_b	energia média por bit
N_0	variância gaussiana
L	diversidade
$erf(x)$	função erro
$erfc(x)$	função erro complementar
$AWGN$	additive white gaussian noise (ruído aditivo gaussiano branco)
CSI	channel state information (estado de informação do canal)
E_s	energia média da constelação
P_e	probabilidade de erro
E_b/N_0	razão sinal-ruído
τ	kissing number
QAM	quadrature amplitude modulation
PSK	phase shifting keying

INTRODUÇÃO

Nos últimos anos tem-se observado uma enorme expansão na área de telecomunicações. A esta expansão está associada a necessidade cada vez maior de desenvolver sistemas de comunicação que possibilitem fornecer serviços de excelente qualidade, a altas taxas de transmissão e de capacidade de armazenamento.

Uma análise de um sistema de comunicação foi brilhantemente formulada por Shannon [37], em 1948, a qual inclui o Teorema da Codificação de Canais. Em linhas gerais, este resultado diz que para transmissão de dados abaixo de uma taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

Uma maneira de se projetar um conjunto de sinais que se aproxime dos padrões prometidos na teoria de Shannon é representar cada sinal como um ponto em um espaço n-dimensional. O processo de projetar um conjunto de palavras-código pode ser reduzido a um problema geométrico de alocação de pontos em uma região de um espaço.

Os códigos construídos a partir de reticulados constituem numa das técnicas de alocação de pontos. Eles constituem uma ferramenta importante na codificação de canal [14].

A confirmação da existência de empacotamentos densos de esferas em espaços de alta dimensão desencadeou vínculos entre o estudo de empacotamentos e a teoria de codificação. Em [32] J. Leech e N.J.A. Sloane estabeleceram as primeiras relações entre empacotamento de esferas e os códigos corretores de erro; e desenvolveram a "construção código" de muitos reticulados conhecidos. A busca de empacotamentos densos como métodos de modulação

codificada teve sucesso com o trabalho de Forney et al. [26] em 1984, no qual sistemas de modulação codificada em bloco foram construídos usando-se reticulados densos nas dimensões 4, 8, 16 e 24- com ganhos de codificação em torno de 1.5, 3.0, 4.5, 6.0 dB, respectivamente.

A teoria dos números algébricos tem sido bastante útil no desenvolvimento de códigos corretores de erros e reticulados. Corpos finitos foram a ferramenta chave para o desenvolvimento dos códigos binários, estruturas que despertaram gradativamente o interesse dos pesquisadores em teoria das comunicações.

Constelações de sinais tendo estrutura de reticulados são consideradas boas para transmissão de sinais, pois a estrutura linear e altamente simétrica dos reticulados usualmente simplifica a tarefa de decodificação.

O problema de encontrar boas constelações de sinais para a transmissão em um canal com desvanecimento Rayleigh, que modela algumas formas de comunicação sem fio, é construir constelações de sinais com energia média mínima para uma desejada taxa de erro, dada a eficiência espectral (número de bits por duas dimensões). Uma interessante abordagem tem sido recentemente proposta, na qual faz-se uso de alguns resultados de teoria dos números algébricos. Usando corpos de números totalmente reais, algumas boas constelações de reticulados apropriadas para canais com desvanecimento Rayleigh são encontradas. Nestas constelações é possível obter diversidade máxima (as componentes entre dois pontos do reticulado são todas distintas). Quanto maior a diversidade e a distância produto mínima, menor será a probabilidade de erro nestes canais.

Constelações de sinais sobre reticulados com estas propriedades e que sejam rotações do reticulado $\mathbb{Z}^n$ são especiais para este tipo de transmissão por terem também "ganho de forma"(relacionado à energia média).

Com esta motivação, abordamos neste trabalho a construção, como reticulado ideal, de reticulados $\mathbb{Z}^n$-rotacionados, usando corpos ciclotômicos. Apresentamos uma nova construção de tais reticulados, no caso em que n é uma potência de 2, através do subcorpo maximal real do n-ésimo corpo ciclotômico e também no caso em que $n = 3$.

O problema de encontrar boas constelações de sinais para um canal de transmissão gaussiano (com distribuição normal de probabilidade de erro) pode ser relacionado ao estudo de empacotamento esférico de reticulados. Constelações esféricas geradas por grupos comutativos com boa performance podem ser obtidas de reticulados com alta densidade de

empacotamento.

Um dos principais fatores para que a transmissão de um sinal ocorra com baixa probabilidade de erro é que a distância euclidiana mínima entre os pontos seja grande. Por isso a análise de desempenho de uma constelação de sinais passa, em boa parte dos casos, pelo cálculo de sua distância mínima.

Um código esférico n-dimensional é um subconjunto discreto de uma esfera neste espaço. Observamos que os elementos de conjuntos quaisquer de sinais $\{p_1, \cdots, p_n\}$ não nulos em $\mathbb{R}^n$ podem ser codificados e decodificados como pares $(u_i, ||p_i||)$, $u_i = \frac{p_i}{||p_i||}$, $i = 1, \cdots, n$ onde $\mathcal{C} = \{u_1, \cdots, u_n\}$ é um código esférico.

Para códigos esféricos, características como boa distância mínima, regiões de decisão isométricas e perfil de distâncias homogêneo da constelação de sinais são determinantes para uma baixa probabilidade de erro na transmissão de sinais através de um canal gaussiano.

Em [39], Slepian estabeleceu de maneira geral os conceitos sobre códigos esféricos para o canal gaussiano. Neste trabalho, Slepian apresentou a construção dos códigos gerados por grupos de matrizes ortogonais que geram pontos sobre a superfície de uma hiperesfera, de modo uniforme.

De maneira geral, dada uma dimensão n e um número de pontos M, queremos saber qual o código esférico $[M, n]$ com a maior distância mínima. Tal código é chamado ótimo.

Na busca por códigos de grupo ótimos, os principais esforços são a construção de limitantes para o número de pontos $M = (n, d)$ de tais códigos, a construção de códigos que tenham distâncias mínimas próximas da distância limite, a determinação do melhor vetor inicial da esfera unitária do $\mathbb{R}^n$ que, para um determinado grupo gerador, maximiza a distância mínima entre dois pontos quaisquer do código.

Para grupos que geram um grande número de pontos, a busca pelo vetor inicial ótimo usando técnicas de programação por busca exaustiva, torna-se um problema computacional de custo muito alto.

Uma importante contribuição neste sentido ocorreu em 1976, quando Biglieri e Elia [11] propuseram um algoritmo para resolver o problema do vetor inicial para códigos de grupo cíclico. Nele, os autores convertem o problema original num problema de programação linear. Porém, uma dificuldade desse método reside no fato de que, fixada a dimensão n e um número de pontos M, podem existir um número grande de grupos cíclicos de matrizes

com M elementos $n \times n$. Isso implica que o custo computacional da procura por códigos de grupo cíclico ótimos pode tornar-se exaustivamente alto.

Dados M e n, ainda em [11], Biglieri e Elia mostram que o número de casos que devemos verificar para encontrar o código de grupo cíclico ótimo é $\left(\begin{array}{c} M/2 \\ n/2 \end{array} \right)$. Neste sentido, pesquisadores vem tentando cada vez mais reduzir o número de casos, mas ainda assim $\left(\begin{array}{c} M/2 \\ n/2 \end{array} \right)$ é aproximadamente um limitante inferior para o número total de casos a serem testados, para grupos comutativos em geral.

Em trabalho recente [42], os autores apresentaram um método de procura de códigos de grupo comutativo que, assim como em [11], também traduz o problema do vetor inicial em um problema de programação linear. Neste trabalho, os autores apresentam um algoritmo computacional para a busca de códigos de grupo comutativo ótimos em $\mathbb{R}^4$ e $\mathbb{R}^6$. Descartando códigos isométricos eles reduzem o número de casos a serem analisados na procura do código ótimo, porém à medida que o número de pontos aumenta, o número de operações envolvidas inviabiliza o cálculo. Assim, ainda não se sabe qual é o código ótimo para um número muito grande de pontos ou em dimensões mais altas.

Isto motivou-nos a utilizar ferramentas que gerassem um procedimento possível para em casos especiais gerar códigos de grupos comutativos em que a distância mínima se aproxime do limitante superior.

Códigos esféricos em dimensão par gerados por grupos comutativos de matrizes ortogonais podem ser determinados pelo quociente de dois reticulados na metade da dimensão, quando o sub-reticulado é "retangular" (isto é, quando os vetores que o geram são mutuamente ortogonais), [17]. Deste modo, pesquisamos a existência de sub-reticulados, a partir de reticulados que possuam boa densidade de empacotamento, mais especificamente neste trabalho, A_2, D_3, D_4, e E_8 que são os que tem maior densidade de empacotamento em suas respectivas dimensões.

Com este método, construímos códigos esféricos em $\mathbb{R}^4$, $\mathbb{R}^6$, $\mathbb{R}^8$, $\mathbb{R}^{16}$ gerados por grupos comutativos, sem a necessidade de analisar casos e comparamos a distância mínima obtida com o limitante específico para códigos de grupo comutativos estabelecido em [18] e, quando possível, comparamos com a distância mínima do código ótimo obtido em [42].

Através de famílias específicas de sub-reticulados, sobre certas condições, obtemos códigos

esféricos de grupo comutativo muito bons e em alguns casos obtemos o código ótimo.

Em síntese, motivados pela minimização da probabilidade de erro para transmissão tanto em canais com desvanecimento como em gaussianos, dividimos nosso trabalho em duas vertentes:

1. No caso do canal com desvanecimento do tipo Rayleigh, abordamos a teoria de reticulados ideais com o objetivo de construir reticulados $\mathbb{Z}^n$-rotacionados que possuam diversidade máxima e maior distância produto mínima.

2. No caso do canal gaussiano, abordamos a teoria necessária para construir códigos esféricos gerados por grupos comutativos com distância euclidiana mínima que se mostraram muito próximas das ótimas, as quais são conhecidas para dimensões baixas e número não muito grande de pontos e se aproximam do limitante superior para um grande número de pontos. Esta construção parte da pesquisa da existência de subreticulados "retangulares", nos reticulados com maior densidade de empacotamento em dimensões 2, 3, 4 e 8.

Mais especificamente, organizamos nosso trabalho conforme delineamos na sequência.

No Capítulo 1, apresentamos alguns tópicos referentes à teoria da informação e codificação e abordamos aspectos do problema de se lidar com a probabilidade e erro em canais gaussianos e em canais com desvanecimento do tipo Rayleigh, com o objetivo de situar o objeto da pesquisa no contexto dessa teoria. Discorremos também sobre conceitos e resultados básicos de teoria dos números algébricos, corpos ciclotômicos e decomposição de ideais primos, essenciais ao nosso trabalho de pesquisa, com o objetivo de tornar este trabalho mais auto-contido e fixar notações. Incluímos as referências necessárias para demonstrações e aprofundamento destes tópicos.

No Capítulo 2, apresentamos o conceito de reticulados e alguns dos problemas que envolvem reticulados como por exemplo, densidade de empacotamento, número de "vizinhos"e norma mínima. Apresentamos então a construção de reticulados via o mergulho canônico de um corpo de números algébricos e em seguida, detalhamos de uma forma especial os reticulados algébricos munidos com uma forma traço. Abordamos ainda a diversidade e a distância produto mínima de um tal reticulado, que é denominado reticulado ideal.

O conteúdo destes capítulos proporciona ferramentas necessárias para os resultados que são apresentados no Capítulo 3, relacionados ao problema de minimizar a probabilidade de erro em canais com desvanecimento do tipo Rayleigh. Motivados por este problema, procuramos por reticulados $\mathbb{Z}^n$-rotacionados com diversidade máxima e maior distância produto mínima. Apresentamos a construção de tais reticulados no caso em que n é uma potência de 2 e no caso em que $n = 2$ e $r = 3$, através do subcorpo maximal real do n-ésimo corpo ciclotômico, respectivamente. Estas construções são temas dos artigos em conjunto [1] e [2], respectivamente. Na parte final deste capítulo abordamos os isomorfismos existentes entre o reticulado ideal sobre $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ e os reticulados já conhecidos, incluindo uma análise comparativa da distância produto mínima.

No Capítulo 4, damos início à segunda vertente de nosso trabalho, com o estudo de códigos esféricos gerados por grupos comutativos e o problema de alocar pontos sobre a superfície de uma hiperesfera com a maior distância euclidiana mínima. Com o intuito de estabelecer uma conexão entre códigos esféricos e reticulados, apresentamos conceitos e resultados sobre códigos de grupo comutativo, forma normal de Smith, toros planares e limitantes para códigos de grupo comutativo.

No Capítulo 5, apresentamos a construção de códigos esféricos a partir do quociente de reticulados. Pesquisamos a existência de sub-reticulados retangulares em reticulados que possuem boa densidade de empacotamento, mais especificamente neste trabalho, A_2, D_3, D_4, e E_8 que são os que tem maior densidade de empacotamento em dimensões 2, 3, 4 e 8, respectivamente. Através de famílias específicas de sub-reticulados e sob certas condições, obtemos códigos esféricos associados a grupos comutativos muito bons (sub-ótimos). Os valores obtidos são compatíveis com algumas das distâncias mínimas ótimas conhecidas (dimensões 4 e 6, e número pequeno de pontos) aproximando-se do limitante superior [18] nestas dimensões e quando o número de pontos cresce.

CAPÍTULO 1

Preliminares

Neste capítulo, expomos de modo conciso, alguns tópicos sobre Teoria da Informação e Codificação relacionados ao trabalho. Apresentamos uma coletânea de resultados básicos de teoria dos números algébricos, corpos ciclotômicos e decomposição de ideais primos.

O objetivo é fornecer a base teórica para o desenvolvimento do trabalho. Admitindo pré-requisitos mais gerais, omitimos as demonstrações e optamos por apenas citar as fontes onde se encontram as mesmas. Desta maneira tentamos tornar este trabalho enxuto, conciso, de fácil entendimento, e o mais auto-suficiente possível.

Textos que contém de forma complementar os tópicos aqui apresentados são, por exemplo: [3], [40], [35], [22] e [30]. Para um estudo detalhado destes tópicos, há as referências [14], [36], [33] e [44].

1.1 Teoria da Informação e Codificação

Podemos considerar um *sistema de comunicação* como sendo um conjunto de equipamentos e meios físicos, que tem por objetivo o transporte da informação de uma fonte a um destinatário via um canal de comunicação. De um modo geral, podemos trabalhar com dois tipos de sistemas de comunicação:

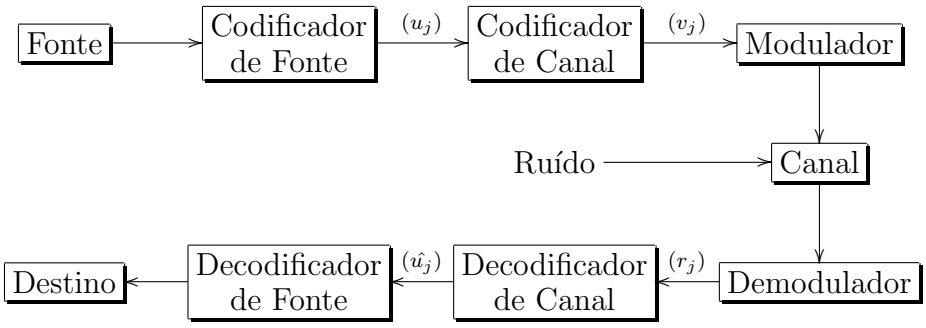


Figura 1.1: **Modelo do sistema**

- **Sistema analógico** onde a informação (ex. voz) é transmitida por meio de sinais elétricos, magnéticos ou eletromagnéticos que variam continuamente em amplitude e/ou frequência e/ou fase e tempo.
- **Sistema digital** onde a informação é transmitida em uma sequência de mensagens discretas por meio de sinais elétricos, magnéticos, eletromagnéticos ou luminosos (fibras óticas) que variam em amplitude e/ou fase e/ou frequência em intervalos fixos de tempo.

1.1.1 Modelo do sistema de transmissão e terminologia

Um sistema de comunicação digital pode ser esquematizado na Figura (1.1),
sendo:

- **Fonte** (de informação): pode ser uma pessoa ou uma máquina que gera uma onda sonora contínua ou uma sequência de símbolos discretos.
- **Codificador de fonte:** associa as saídas da fonte às sequências $(u_j) = (u_1, \cdots, u_k)$ de dígitos (geralmente binários) chamadas de sequências de informação ou palavras código fonte. Tendo em vista a eliminação de redundâncias, nesta etapa deve-se utilizar o menor número possível de dígitos por unidade de tempo para representar a saída da fonte. Além disso, a saída da fonte deve ser reconstruída a partir da sequência de informação associada sem ambiguidades.
- **Codificador de canal:** transforma a palavra código fonte (u_j) em uma outra sequência $(v_j) = (v_1, \cdots, v_n)$ chamada de palavra código de canal. Este estágio tem por objetivo

inserir redundância na sequência (u_j) com vistas a minimizar a interferência de ruídos no canal.

- **Modulador:** gera formas de ondas que são apropriadas para a transmissão através do canal. O modulador digital transforma símbolos discretos da saída do codificador de canal em um sinal contínuo com duração de T segundos, de tal forma que a amplitude e/ou frequência e/ou fase seja(m) alterada(s) de acordo com a necessidade. Algumas destas técnicas são conhecidas como:

  - PAM (pulse amplitude modulation) ou ASK (amplitude shift-keying): alteração de amplitude.

  - FSK (frequency shift-keying): alteração de frequência.

  - PSK (phase shift-keying): alteração de fase.

  - QAM (quadrature amplitude modulation): alteração de amplitude e fase.

- **Canal:** é o meio físico por onde a informação é transmitida/armazenada.

- **Demodulador, decodificador de canal e decodificador de fonte:** fazem o inverso do modulador, codificador de canal e codificador de fonte, respectivamente.

1.1.2 Constelações de sinais

Os principais objetivos a serem alcançados quando da proposta de novos sistemas de comunicação é que estes sistemas apresentem um melhor desempenho sob o critério da probabilidade de erro.

Por outro lado, a informação a ser transmitida através de um sistema de comunicação estará sempre sujeita a um conjunto de interferências que no processo de modelagem serão alocadas ao canal de transmissão. Essa coletânea de interferências é denominada *ruído.* Devido à natureza do ruído, sua modelagem é probabilística. Dessa forma, a caracterização estatística do mesmo se realiza através do estabelecimento da função densidade de probabilidade. Essa modelagem é relevante, pois através dela é que o receptor poderá ser projetado de maneira ótima.

Uma vez realizada essa modelagem, o passo seguinte está relacionado com o processamento do sinal, propriamente dito, a ser utilizado na transmissão da informação de tal forma que a ação do ruído possa ser melhor controlada. Existem várias formas de realizar esse processamento. Uma delas é através do uso de um esquema de modulação apropriado. Uma outra, é através do uso de um esquema de codificação específico. Ainda uma outra, através da combinação dos dois procedimentos anteriores, etc.

Palavras-código e sinais podem ser representados por meio de esquemas compostos por pontos e vértices de grafos em espaços de curvatura constante. Ao conjunto de tais pontos chamamos indistintamente de *constelações de sinais*.

Exemplo 1.1.1. *A Figura (1.2) ilustra uma constelação do tipo 4-PAM com* $d_{min} = 2$ *em* $\mathbb{R}$, *onde* d_{min} *é a distância euclidiana mínima entre os sinais.*

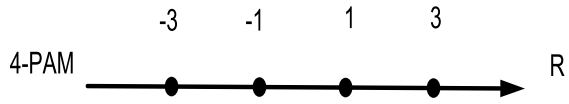


Figura 1.2: **Representação geométrica do esquema de modulação 4-PAM.**

Exemplo 1.1.2. *A Figura (1.3) ilustra uma constelação do tipo 2-PSK em* $\mathbb{R}^2$.

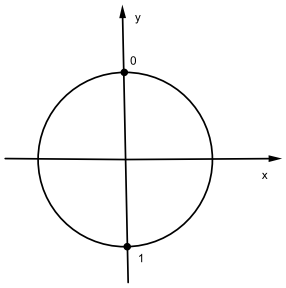


Figura 1.3: **Representação geométrica do esquema de modulação 2-PSK**

A modulação PSK está intimamente ligada às rotações do espaço euclidiano. Suponhamos que uma informação possa ser representada binariamente, por exemplo, ligar e desligar a luz de um quarto, ou, abrir e fechar uma porta. Ligar é "0" e desligar é "1". Vamos associar cada uma destas operações a uma fase de um sinal contínuo. Ao "zero" associamos a fase

zero e ao "um" associamos a fase π. Tais fases, por conseguinte, estão associadas a dois sinais contínuos

$$x_i(t) = \cos[\pi t + (i-1)\pi],\ t \in (0,2),\ i = 1,\ 2.$$

Mas, $x_1(t) = \cos[\pi t]$ *e* $x_2(t) = -\cos[\pi t]$. *Escritas como combinação das funções*

$$\{-\sin[\pi t],\ \cos[\pi t]\},$$

temos que $x_1(t) = 0.(-\sin[\pi t]) + 1.(\cos[\pi t])$ *e* $x_2(t) = 0.(-\sin[\pi t]) - 1.(\cos[\pi t])$. *Assim, representamos "zero" pelo ponto* $(0,1)$ *e "um" pelo ponto* $(0,-1)$, *conforme a Figura (1.3).*

Esta construção se generaliza para o conjunto de M sinais

$$x_i(t) = \cos[\pi t + 2(i-1)\pi/M],\ t \in (0,2),\ i = 1,\ 2\cdots,M.$$

conhecido por $M-PSK$, *cuja representação geométrica é um polígono regular de M vértices. De fato,*

$$x_i(t) = \cos(\pi t).\cos(2(i-1)\pi/M) - \sin(\pi t).\sin(2(i-1)\pi/M)$$

e, portanto, ao sinal i associamos o vetor $(\cos(2(i-1)\pi/M), \sin(2(i-1)\pi/M))$.

O que se busca então, é determinar características geométricas e algébricas de tal forma que se consiga determinar o desempenho do sistema de comunicação sob a menor probabilidade de erro, maior taxa e menor potência de transmissão, etc. Em geral, no processo de modulação projetamos as constelações de sinais com uma estrutura geométrica euclidiana de tal forma que possamos minimizar, na demodulação, a ação do ruído.

Sinais contínuos podem ser representados de forma discreta, ou seja, por um conjunto de pontos em esferas euclidianas ([9], p.62). Isto simplifica muito a análise dos esquemas de modulação digital.

Um tipo fundamental de representação discreta é baseada em conjuntos de sinais chamados *ortonormais*.

Como o espaço vetorial gerado por uma constelação de sinais $\mathcal{S}$ é um espaço vetorial com produto interno de dimensão finita [19], podemos construir um conjunto de funções ortonormais $\{\phi_i(t)\}_{i=1}^{N}$ através do processo de ortonormalização de Gram-Schmidt, de tal maneira que

$$s_j(t) = \sum_{i=1}^{N} s_{ij}\phi_i(t).$$

Assim, para cada sinal continuo $s_i(t) \in \mathcal{S}$ associamos um vetor $\{(s_{1i}, \cdots, s_{Ni}) \in \mathbb{R}^N;\ i = 1, \cdots, M\}$.

O modelo vetorial simplifica muito a análise dos sistemas. Portanto, determinar um conjunto de sinais consiste basicamente em escolher um conjunto de vetores no espaço vetorial euclidiano, levando-se em conta critérios de projeto, como probabilidade de erro e taxa de transmissão.

1.1.3 Canal gaussiano e canal com desvanecimento do tipo Rayleigh

Os sistemas de comunicação móvel, em particular os sistemas de telefonia celular, têm se destacado nessa nova era. Novas tecnologias surgem a cada instante e com elas, a possibilidade de implementação de novos serviços. A principal razão para tanto esforço tecnológico se deve a uma busca por sistemas que possibilitem fornecer serviços de excelente qualidade, a altas taxas de transmissão, em meio a um ambiente de comunicação altamente hostil que é o canal de comunicação móvel.

Os canais de comunicação móvel são agrupados em dois tipos: canal via satélite e canal terrestre.

- **Canal gaussiano**

O canal de comunicação via satélite é um canal do tipo AWGN (*Additive White Gaussian Noise*) onde predominam fortes atenuações e muitas vezes grandes atrasos de propagação do sinal.

O termo AWGN é utilizado em modulamentos matemáticos para caracterizar aqueles canais onde o tipo de ruído responsável por degradar a comunicação é um ruído branco adicionado ao sinal. Este ruído recebe este nome por alusão ao fato da cor branca ser formada da soma de todas as outras cores. A teoria acerca do desenvolvimento de receptores ótimos para a utilização em canais AWGN já se tornou clássica.

A escolha de um conjunto de sinais para a transmissão através de um canal gaussiano constitui um dos principais problemas na concepção de sistemas de comunicação.

A constelação de sinais é denominada de código (M, N) para o canal gaussiano, onde M denota o número de sinais e N a dimensão do espaço euclidiano gerado.

A razão para um código esférico ser também chamado de constelação de sinais é que todo conjunto de sinais contínuos pode ser representado por um conjunto de pontos na esfera euclidiana. Esta maneira geométrica de ver os sinais possibilitou um avanço importante no manuseio desses conjuntos.

Um tipo especial de código esférico é o gerado por um grupo finito de matrizes ortogonais. Como as matrizes ortogonais determinam isometrias do espaço euclidiano, estes códigos possuem regiões de decisão isométricas e uma distribuição de pontos homogênea, o que facilita na hora das análises de desempenho e decodificação.

- **Canal com desvanecimento do tipo Rayleigh**

O canal de comunicação terrestre tem como característica principal a propagação por múltiplos percursos. Estes múltiplos percursos são formados pela reflexão e/ou difração do sinal transmitido em estruturas próximas ao receptor, tais como edifícios, árvores, etc. A soma vetorial dos vários sinais dos múltiplos percursos pode resultar em uma interferência construtiva ou destrutiva do sinal recebido. Com o movimento, as estruturas em torno do receptor vão se modificando e, por consequência, as interferências passam constantemente da situação construtiva para a destrutiva, fazendo com que a intensidade do sinal recebido varie ao longo do tempo. Esse fenômeno de alteração na intensidade do sinal recebido é denominado *desvanecimento por múltiplos percursos*.

Quando o desvanecimento é caracterizado por um número grande de raios refletidos, e as componentes do sinal possuem obstáculos, ele é modelado por uma distribuição de probabilidades de Rayleigh. Para melhorar o desempenho sobre canais com desvanecimento, é realizado um processo de otimização que consiste em rotacionar a constelação, preservando a distância euclidiana entre seus pontos.

O objetivo é propor métodos de codificação e diversidade que possibilitem a redução da taxa de erro de transmissão nos sistemas de comunicação móvel via terrestre. Decorre daí a necessidade de se estudar códigos que sejam "bons corretores de erros" e que possibilitem resgatar o sinal original mesmo depois de distorções (ruídos).

É neste contexto que constelações de sinais de reticulados rotacionados têm sido propostas para transmissão sobre o canal com desvanecimento do tipo Rayleigh. Reticulados construídos via o mergulho canônico de um corpo de números algébricos são providos de

uma ferramenta eficiente para construção de tais códigos reticulados. A razão é que os dois principais parâmetros para a construção destes códigos, a diversidade e a distância produto mínima do reticulado, estão diretamente relacionadas com as propriedades do corpo de números em questão.

1.1.4 Probabilidade de erro

O desempenho de uma constelação é medido pela probabilidade de erro na transmissão dos sinais $P(e)$. Uma das principais preocupações no estudo de modulação de sinais é encontrar meios para determinar ou estimar a probabilidade de erro associada a sinais.

Quando consideramos transmissões codificadas, palavras-código são vetores reais n-dimensionais $\mathbf{x} = (x_1, \ldots, x_n)$, tomados de alguma constelação de sinal $\mathcal{S} \subseteq \mathbb{R}^n$.

Quando usamos códigos reticulados, $\mathbf{x}$ pertence a uma constelação de sinais n-dimensional $\mathcal{S}$ (de cardinalidade 2^m) obtida de um conjunto de pontos do reticulado $\Lambda = \{\mathbf{x} = \mathbf{u}M_\Lambda\}$, onde $\mathbf{u}$ é um vetor com coordenadas inteiras e M_Λ é a matriz geradora do reticulado, como veremos nos próximos capítulos.

Sejam $\mathbf{r} = (r_1, \cdots, r_n)$ o vetor recebido e $\alpha = (\alpha_1, \cdots, \alpha_n)$ coeficientes de desvanecimento. Assumindo CSI (*Channel State Information*) perfeito, isto é, o receptor tem perfeito conhecimento de todos os coeficientes do canal, a detecção por *Máxima Verossimilhança* (ML) requer a minimização da seguinte métrica

$$m(\mathbf{x}|\mathbf{r}) = \sum_{i=1}^{n} ||r_i - x_i||^2, \tag{1.1}$$

para o canal gaussiano, e

$$m(\mathbf{x}|\mathbf{r}, \alpha) = \sum_{i=1}^{n} ||r_i - \alpha_i x_i||^2. \tag{1.2}$$

para o canal Rayleigh com desvanecimento.

- Se o sinal $\mathbf{x} \equiv \mathbf{x}(t)$ é transmitido através de um canal gaussiano, o sinal recebido no intervalo de tempo $0 \leq t \leq T$ é dado por

  $$\mathbf{r}(t) = \mathbf{x}(t) + n(t),$$

  onde $n = (n_1, \cdots, n_n)$ é uma amostra de um processo aleatório gaussiano com variância N_0 e média nula.

- Se o sinal $\mathbf{x} \equiv \mathbf{x}(t)$ é transmitido através de um canal com desvanecimento do tipo Rayleigh, o sinal recebido no intervalo de tempo $0 \leq t \leq T$ é dado por

$$\mathbf{r}(t) = \alpha * \mathbf{x}(t) + n(t),$$

onde $n = (n_1, \cdots, n_n)$ é o ruído gaussiano e $\alpha = (\alpha_1, \cdots, \alpha_n)$ são coeficientes de desvanecimento com segundo momento unitário e $*$ representa o produto interno.

Consideramos a transmissão de dados sobre um canal com desvanecimento com uma única antena e com desvanecimento plano, ou seja, a alteração de amplitude das várias componentes do sinal transmitido ocorre de maneira uniforme em toda faixa de frequências do sinal.

Observamos que o sucesso na decodificação do sinal depende também da distância entre os sinais, que, por sua vez, depende da quantidade de energia que se disponibiliza para o envio do sinal.

Denotamos por $P_e(\mathcal{S})$ a probabilidade de erro quando enviamos um ponto da constelação de sinais $\mathcal{S}$, e por $P(\mathbf{x} \to \hat{\mathbf{x}})$ a probabilidade de erro par a par, a probabilidade que, quando $\mathbf{x}$ é transmitido, o ponto recebido está mais próximo de $\hat{\mathbf{x}}$ do que de $\mathbf{x}$ de acordo com as métricas definidas em (1.1) e (1.2).

Para uma constelação de sinais arbitrária $\mathcal{S}$, temos

$$P_e(\mathcal{S}) = \frac{1}{|\mathcal{S}|} \sum_{\mathbf{x} \in \mathcal{S}} P_e(\mathcal{S} \mid \mathbf{x} \text{ transmitido}).$$

Isto pode ser bastante simplificado no caso de códigos reticulados. Como um reticulado infinito é *geometricamente uniforme*, a probabilidade de erro quando enviamos um ponto do reticulado é a mesma, $P_e(\Lambda) = P_e(\Lambda \mid \mathbf{x})$, para qualquer ponto transmitido $\mathbf{x} \in \mathbf{\Lambda}$. Assumiremos então que $\mathcal{S}$ é uma constelação finita obtida de Λ.

Agora aplicamos o limitante da união, o qual nos dá um limite superior para a probabilidade de erro do ponto:

$$P_e(\mathcal{S}) \leq P_e(\Lambda) = \bigcup_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \sum_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x} \to \hat{\mathbf{x}}) \tag{1.3}$$

A primeira desigualdade leva em conta os efeitos de bordo da constelação finita $\mathcal{S}$ comparada ao reticulado infinito Λ.

- **Limitante superior para a probabilidade de erro no canal gaussiano**

Shannon (1948) em sua teoria matemática da comunicação mostra que, dado um canal com largura de faixa w seria possível, através de alguma técnica, alcançar um limite máximo de erro arbitrariamente pequeno.

Segundo Shannon

$$C = w \log_2 (1 + SNR),$$

onde C é a *capacidade do canal* em bits/segundo e a *razão sinal-ruído* (SNR) por bit é dada por

$$SNR = \frac{E_b}{N_0},$$

onde $E_b = \dfrac{E_s}{\log_2 M}$ é a *energia média por bit*, E_s é a energia média da constelação e N_0 é a *variância gaussiana*.

A teoria de Shannon pode ser considerada como uma teoria da "existência," ou seja, afirma ser possível alcançar a taxa C, mas não estabelece a maneira ou técnica de fazê-lo.

Hoje, elaboradas técnicas de codificação e/ou modulação estão permitindo cada vez mais a aproximação do limite estabelecido por Shannon a probabilidades de erro cada vez menores.

Para canais afetados por ruído do tipo AWGN, o cálculo aproximado da probabilidade de erro pode ser feito por estimadores como, por exemplo, o limitante de Bhattacharyya ([8], pp. 190-192), que estabelecemos a seguir.

Consideremos uma constelação $\{x_j\}_{j=1}^{M}$ de M sinais equiprováveis que esteja representada no $\mathbb{R}^n$.

Para obtermos um limite superior para a probabilidade de erro observamos que um erro ocorre quando, usando a decodificação com a regra ML (1.1), o ponto recebido r_j está mais próximo de $\hat{x_j}$ do que de x_j, isto é, $m(\hat{x_j} \mid r) \leq m(x_j \mid r)$.

A *densidade gaussiana* associada a x_j em $\mathbb{R}^n$ para canais AWGN é dada por

$$\begin{aligned} g_{x_j} \quad : \quad & \mathbb{R}^n \to \mathbb{R}_+ \\ & y \mapsto \frac{1}{\sqrt{(2\pi N_0)^n}} exp\left(-\frac{||y - x_j||^2}{2N_0}\right) \end{aligned}$$

sendo $||.||$ a norma euclidiana em $\mathbb{R}^n$, N_0 a variância gaussiana.

Com isso, a probabilidade de acerto na transmissão do sinal x_j é igual ao volume (n-dimensional) acima da região de Voronoi V_j de x_j e abaixo do gráfico de g_{x_j}, que é dada por

$$P_a(x_j) = \frac{1}{\sqrt{(2\pi N_0)^n}} \int_{V_j} exp\left(-\frac{||y-x_j||^2}{2N_0}\right) dV_{\mathbb{R}^n}$$

sendo $dV_{\mathbb{R}^n}$ elemento de volume cartesiano em $\mathbb{R}^n$.

Como

$$P_e(x_j) = 1 - P_a(x_j)$$

e os sinais são equiprováveis, a probabilidade de erro P_e associada à constelação de sinais é dada por

$$P_e(\mathcal{S}) = \frac{1}{M} \sum_{j=1}^{M} \frac{1}{\sqrt{(2\pi N_0)^n}} \int_{\mathbb{R}^n - V_j} exp\left(-\frac{||y-x_j||^2}{2N_0}\right) dV_{\mathbb{R}^n}. \tag{1.4}$$

Vamos estabelecer um limitante superior para (1.4), antes porém, é útil introduzir a notação usual para duas funções muito utilizadas em Teoria da Informação e Codificação. Uma delas é a *função erro*, definida por

$$\begin{aligned} erf &: \mathbb{R}_+ \to [0,1] \\ &\quad y \mapsto \frac{2}{\sqrt{\pi}} \int_0^y e^{-t^2} dt. \end{aligned}$$

A outra é a *função erro complementar*, definida por $erfc(x) = 1 - erf(x)$, ou seja,

$$\begin{aligned} erfc &: \mathbb{R}_+ \to [0,1] \\ &\quad y \mapsto \frac{2}{\sqrt{\pi}} \int_y^\infty e^{-t^2} dt. \end{aligned}$$

Após alguns cálculos, é demonstrado em [3] que:

$$P_e(\mathcal{S}) = \frac{1}{M} \sum_{j=1}^{M} P_e(x_j) \leq \frac{1}{M} \sum_{j=1}^{M} \sum_{i=1}^{v_j} \frac{1}{2} erfc\left(\frac{||x_j - x_{j_i}||}{2\sqrt{2N_0}}\right)$$

onde x_{j_i}, $i = 1, \cdots, v_j$ são os sinais que determinam a região de Voronoi de x_j e v_j é a quantidade de sinais vizinhos a x_j que influenciam (determinam um lado) em V_j.

Como

$$\frac{1}{M}\sum_{j=1}^{M}\sum_{i=1}^{v_j}\frac{1}{2}erfc\left(\frac{||x_j - x_{j_i}||}{2\sqrt{2N_0}}\right) \leq \frac{1}{M}\sum_{j=1}^{M}\sum\frac{1}{2}erfc\left(\frac{||x_j - \hat{x}_j||}{2\sqrt{2N_0}}\right)$$

e

$$erfc(x) \leq exp(-x^2),$$

temos que

$$\begin{aligned}\frac{1}{M}\sum_{j=1}^{M}\sum_{i=1}^{v_j}\frac{1}{2}erfc\left(\frac{||x_j - \hat{x}_j||}{2\sqrt{2N_0}}\right) &\leq \frac{1}{M}\sum_{j=1}^{M}\sum_{i=1}^{v_j}\frac{1}{2}exp\left(-\frac{||x_j - \hat{x}_j||^2}{8N_0}\right)\\ &< \frac{1}{M}\sum_{j=1}^{M}\sum exp\left(-\frac{||x_j - \hat{x}_j||^2}{8N_0}\right)\end{aligned}$$

Portanto, para um canal $AWGN$, a expressão (1.3) torna-se

$$P_e(\mathcal{S}) < \frac{1}{M}\sum_{j=1}^{M}\sum exp\left(-\frac{||x_j - \hat{x}_j||^2}{8N_0}\right)$$

que é conhecido como o *limitante de Bhattacharyya*.

Deste modo, uma das condições para que a probabilidade de erro seja baixa, é aumentar a distância entre as palavras da constelação. Assim, um dos primeiros objetivos na construção de uma constelação de sinais $\mathcal{S}$ é maximizar $d_{min}(\mathcal{S}) = min\{||x_j - \hat{x}_j||; x_j, \hat{x}_j \in \mathcal{S}\}$, para um número fixo de pontos e energia média fixada.

- **Limitante superior para a probabilidade de erro no canal Rayleigh**

Para obtermos um limite superior para a probabilidade de erro $P(\mathbf{x} \to \hat{\mathbf{x}})$, observamos que um erro ocorre quando, usando a decodificação com a regra ML (1.2), o ponto recebido $\mathbf{r}$ está mais próximo de $\hat{\mathbf{x}}$ do que de $\mathbf{x}$, isto é, $m(\hat{\mathbf{x}}|r, \alpha) \leq m(\mathbf{x}|r, \alpha)$.

A probabilidade de erro condicional é dada por

$$\begin{aligned}P(\mathbf{x} \to \hat{\mathbf{x}} \mid \alpha) &= P(\sum_{i=1}^{n}||r_i - \alpha_i\hat{x}_i||^2 \leq \sum_{i=1}^{n}||r_i - \alpha_i x_i||^2 \mid \mathbf{x}\,\text{transmitido})\\ &= P(\sum_{i=1}^{n}||\alpha_i(x_i - \hat{x}_i) + n_i||^2 \leq \sum_{i=1}^{n}||n_i||^2)\\ &= P(\sum_{i=1}^{n}\alpha_i^2(x_i - \hat{x}_i)^2 + 2\sum_{i=1}^{n}\alpha_i(x_i - \hat{x}_i)n_i \leq 0).\end{aligned}$$

Seja $\chi = \sum_{i=1}^{n} \alpha_i(x_i - \hat{x}_i)n_i$ uma combinação linear de variáveis aleatórias gaussianas n_i, isto é, χ é gaussiana com média nula e variância

$$\sigma_\chi^2 = N_0 \sum_{i=1}^{n} \alpha_i^2(x_i - \hat{x}_i)^2.$$

Seja $A = \frac{1}{2}\sum_{i=1}^{n} \alpha_i^2(x_i - \hat{x}_i)^2$ uma constante. Podemos escrever a probabilidade de erro condicional em termos de χ e A :

$$P(\mathbf{x} \to \hat{\mathbf{x}} \mid \alpha) = P(-\chi \geq A) = Q(A/\sigma_\chi)$$

onde $Q(x) = (2\pi)^{-1}\int_x^\infty exp(-t^2/2)dt$ é a função gaussiana enfraquecida. Como $Q(x)$ pode ser limitado superiormente por uma exponencial $Q(x) \leq \frac{1}{2}exp(-x^2/2)$, a probabilidade de erro condicional é

$$P(\mathbf{x} \to \hat{\mathbf{x}} \mid \alpha) \leq \frac{1}{2}exp\left(-\frac{A^2}{2\sigma_\chi^2}\right) = \frac{1}{2}exp\left(-\frac{1}{8N_0}\sum_{i=1}^{n}\alpha_i^2(x_i - \hat{x}_i)^2\right).$$

A probabilidade de erro $P(\mathbf{x} \to \hat{\mathbf{x}})$ é calculada pela média $P(\mathbf{x} \to \hat{\mathbf{x}} \mid \alpha)$ sobre o coeficiente com desvanecimento α :

$$P(\mathbf{x} \to \hat{\mathbf{x}}) = \int P(\mathbf{x} \to \hat{\mathbf{x}} \mid \alpha)p(\alpha)d\alpha \leq \frac{1}{2}\int exp\left(-\frac{1}{8N_0}\sum_{i=1}^{n}\alpha_i^2(x_i - \hat{x}_i)^2\right)p(\alpha)d\alpha.$$

A probabilidade diferencial é $p(\alpha)d\alpha = p(\alpha_1)\cdots p(\alpha_n)d\alpha_1\cdots d\alpha_n$, onde $p(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$ é a *distribuição de Rayleigh normalizada*. Substituindo na última desigualdade, obtemos

$$\begin{aligned} P(\mathbf{x} \to \hat{\mathbf{x}}) &\leq \frac{1}{2}\prod_{i=1}^{n}\int_0^\infty exp\left(-\frac{1}{8N_0}\sum_{i=1}^{n}\alpha_i^2(x_i - \hat{x}_i)^2\right)p(\alpha_i)d\alpha_i \\ &= \frac{1}{2}\prod_{i=1}^{n}\int_0^\infty 2\alpha_i exp(-C_i\alpha_i^2)d\alpha_i \end{aligned}$$

onde $C_i = 1 + (x_i - \hat{x}_i)^2/(8N_0)$. Calculando a integral, obtemos

$$P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \frac{1}{2}\prod_{i=1}^{n}\frac{1}{1 + \frac{(x_i - \hat{x}_i)^2}{8N_0}}. \tag{1.5}$$

Para razão sinal-ruído grande

$$P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \frac{1}{2} \prod_{x_i \neq \hat{x}_i} \frac{1}{\frac{(x_i - \hat{x}_i)^2}{8N_0}} = \frac{1}{2} \frac{(8N_0)^\ell}{d_p^{(\ell)}(\mathbf{x}, \hat{\mathbf{x}})^2} \tag{1.6}$$

onde

$$d_p^{(\ell)}(\mathbf{x}, \hat{\mathbf{x}}) = \prod_{x_i \neq \hat{x}_i} ||x_i - \hat{x}_i|| \tag{1.7}$$

é a distância *distância ℓ-produto* de $\mathbf{x}$ a $\hat{\mathbf{x}}$ quando estes dois pontos diferem em ℓ componentes. Rearranjando a equação (1.3), obtemos

$$P_e(\mathcal{S}) \leq \sum_{\ell=L}^{n} \frac{1}{2} \frac{(8N_0)^\ell}{d_p^{(\ell)}(\mathbf{x}, \hat{\mathbf{x}})^2} \tag{1.8}$$

onde L é o número mínimo de componentes distintas entre quaisquer dois pontos da constelação, e é chamado *diversidade de modulação* ou *ordem de diversidade* da constelação de sinal, mas diremos simplesmente *diversidade*.

Observe que os termos dominantes na soma (1.8) são encontrados para $L = \min(\ell)$. Entre os termos em (1.8) satisfazendo $L = min(\ell)$, o termo dominante é encontrado para $d_{p,\min} = \min d_p^{(L)}$. Assim para obtermos uma baixa probabilidade de erro assintoticamente, em ordem de relevância temos que:

1- **Maximizar a diversidade** $L = \mathbf{min}(\ell)$**.**
2- **Maximizar** $d_{p,\min} = \mathbf{min}(d_p^{(L)}(\mathbf{x}, \hat{\mathbf{x}}))$.

Observação 1.1.1. *A diversidade é obviamente limitada pela dimensão n da constelação, e a diversidade máxima é $L = n$. Consequentemente, alta diversidade é obtida em alta dimensão.*

Neste trabalho o problema de transmissão de informação em canais de comunicações móveis é enfrentado com a utilização de técnicas que minimizem a probabilidade de erro. O objetivo principal é analisar técnicas para os dois canais citados, a fim de minimizar a probabilidade de erro. Nos Capítulos 2 e 3 estudamos reticulados que são associados a códigos para transmissão em canais com desvanecimento do tipo Rayleigh. Nos Capítulos 4 e 5 estudamos códigos esféricos de grupo associados a canais AWGN.

1.2 Teoria dos números algébricos

Esta seção apresenta, de forma concisa, conceitos e resultados básicos em teoria dos números algébricos, necessários para as técnicas aqui abordadas, tal como a definição de inteiro algébrico, diferente, norma e traço relativos e polinômio característico.

Sejam K e L subcorpos dos números complexos $\mathbb{C}$. Dizemos que L é uma extensão de K ou que L/K é uma *extensão de corpos*, sempre que K for um subcorpo de L.

A dimensão do K-espaço L é denotada por $[L : K]$ e é chamada de *grau* de L/K. Dizemos que L/K é uma *extensão finita* quando $[L : K] < \infty$.

Seja L/K uma extensão de corpos, e $\alpha \in L$. Se existe um polinômio mônico irredutível $f(X) \in K[X]\backslash\{0\}$ tal que $f(\alpha) = 0$, dizemos que α é um *número algébrico* sobre K. Tal polinômio é chamado de *polinômio minimal* de α sobre K.

Dizemos que a extensão L de K é *extensão algébrica* se todo elemento $\alpha \in L$ for raiz de algum polinômio não-nulo f em $K[X]$.

O conjunto dos números algébricos de K sobre $\mathbb{Q}$ é um anel, chamado o *anel dos inteiros algébricos* de K, e denotado por $\mathcal{O}_K$.

Seja K uma extensão finita de $\mathbb{Q}$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K, temos que $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$, cuja base é chamada de *base integral*.

Um *corpo de números* é uma extensão finita de $\mathbb{Q}$. Se a dimensão de K como $\mathbb{Q}$-espaço vetorial é n, dizemos que K é um corpo de números de grau n.

Todo corpo de números K é da forma $K = \mathbb{Q}(\theta)$ para algum número algébrico $\theta \in K$. Assim K é um $\mathbb{Q}$-espaço vetorial gerado por potências de θ. Se K tem grau n então $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base de K e o grau do polinômio minimal de θ sobre $\mathbb{Q}$ é n, isto é, $\partial(f(X)) = n$.

Se o polinômio minimal de θ sobre $\mathbb{Q}$ tem todas as suas raízes em K, dizemos que K é uma *extensão de Galois* de $\mathbb{Q}$. O conjunto dos automorfismos do corpo $Gal(K/\mathbb{Q}) = \{\sigma : K \to K | \sigma(x) = x, \forall\, x \in \mathbb{Q}\}$ é um grupo, chamado o *grupo de Galois* de K sobre $\mathbb{Q}$.

Definição 1.2.1. *Sejam K e L duas extensões de um corpo E. Um homomorfismo de corpos $\varphi : K \to L$ é dito ser um E-***homomorfismo** *se para todo $a \in E$ tem-se que $\varphi(a) = a$ (isto é, $\varphi|_E$ é a identidade de E).*

Observação 1.2.1. *Todo homomorfismo $\varphi : K \to L$ de subcorpos de $\mathbb{C}$ é um $\mathbb{Q}$-homomorfismo e se φ é injetivo podemos chamá-lo de* **mergulho**.

O próximo teorema diz respeito a um homomorfismo entre tais corpos.

Teorema 1.2.1. *[36] Sejam K, L, subcorpos de $\mathbb{C}$ onde L é uma extensão de K e $[L : K] = n < \infty$. Então, existe $\theta \in L$ tal que $L = K(\theta)$ e existem exatamente n K-homomorfismos de L em $\mathbb{C}$, $\sigma_i : L \to \mathbb{C}$, $i = 1, \ldots, n$, tal que $\sigma_i(\theta) = \theta_i$, onde θ_i são as raízes distintas em $\mathbb{C}$ do polinômio minimal de θ sobre K.*

Tomando $\theta = \theta_1$, notamos que $\sigma_1(\theta) = \theta_1 = \theta$ e assim σ_1 é a aplicação identidade, $\sigma_1(\ell) = \ell$, para todo $\ell \in L$. Quando aplicamos o mergulho σ_i a um elemento arbitrário $x \in L$, $x = \sum_{k=1}^{n} a_k\theta^k, a_k \in K$, usando as propriedades de K-homomorfismo temos

$$\sigma_i(x) = \sigma_i\left(\sum_{k=1}^{n} a_k\theta^k\right) = \sum_{k=1}^{n} \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^{n} a_k\theta_i^k \in \mathbb{C}$$

e temos que a imagem de x sobre σ_i é univocamente identificada por θ_i.

Os elementos $\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)$ são chamados os *K-conjugados* de x e

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

são chamados respectivamente a **norma** e o **traço** de x da extensão L/K.

Sejam $K \subset L$ corpos, $[L : K] = n$, $x, y \in L$ e $a \in K$. Valem as seguintes propriedades:

1. $Tr_{L/K}(x + y) = Tr_{L/K}(x) + Tr_{L/K}(y)$;
2. $Tr_{L/K}(ax) = aTr_{L/K}(x)$;
3. $Tr_{L/K}(a) = na$;
4. $N_{L/K}(xy) = N_{L/K}(x).N_{L/K}(y)$;
5. $N_{L/K}(a) = a^n$.

No caso $K \subseteq L \subseteq M$, dado $x \in M$, temos:

- $Tr_{M/K}(x) = Tr_{L/K}(Tr_{M/L}(x))$;
- $N_{M/K}(x) = N_{L/K}(N_{M/L}(x))$.

Em particular, se $x \in L$, então

- $Tr_{M/K}(x) = [M : L]Tr_{L/K}(x)$;
- $N_{M/K}(x) = N_{L/K}(x)^{[M:L]}$.

Lema 1.2.1. *[24] Para qualquer $x \in K$, temos $N(x)$ e $Tr(x) \in \mathbb{Q}$. Se $x \in \mathcal{O}_K$, temos $N(x)$ e $Tr(x) \in \mathbb{Z}$.*

Definição 1.2.2. *Seja $\{\omega_1, \ldots, \omega_n\}$ uma base integral de $\mathcal{O}_K$. O* **discriminante** *de K é definido como $d_K = det[\sigma_j(\omega_i)]^2$.*

Observação 1.2.2. *O discriminante independe da escolha da base.*

Sejam m e n os graus das extensões K e L, respectivamente, sobre $\mathbb{Q}$ e seja $d = mdc(d_K, d_L)$, onde d_K e d_L são o discriminante de K e L, respectivamente.

Teorema 1.2.2. *[33] Se $[KL : \mathbb{Q}] = mn$, então $\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.*

Corolário 1.2.1. *[33] Se $[KL : \mathbb{Q}] = mn$ e $d = 1$ então $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.*

1.2.1 Corpos ciclotômicos

Uma classe importante dos corpos de números é a classe dos corpos ciclotômicos. Nosso objetivo nesta seção é determinar o anel dos inteiros algébricos, base integral e discriminante dos corpos ciclotômicos.

Um elemento $\zeta \in \mathbb{C}$ é chamado uma raiz *n-ésima da unidade* se $\zeta^n = 1$, n inteiro, $n \geq 1$, e é dito *raiz primitiva n-ésima da unidade* se $\zeta^n = 1$ mas $\zeta^d \neq 1$ para qualquer $1 \leq d < n$.

As raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$.

O número complexo ζ^m é uma raiz primitiva n-ésima da unidade se, e somente se, $mdc(m, n) = 1$, isto é, o número de raízes primitivas n-ésimas da unidade é dado por

$$\varphi(n) = \#\{0 < m < n : mdc(m, n) = 1, m \in \mathbb{Z}\},$$

onde φ é a **função de Euler**.

Definição 1.2.3. *Dizemos que L é o n-ésimo* **corpo ciclotômico** *se L é resultante da adjunção de $\mathbb{Q}$ e uma raiz primitiva n-ésima da unidade, $L = \mathbb{Q}(\zeta_n)$.*

Sendo $L = \mathbb{Q}(\zeta_n)$ onde, ζ_n é uma raiz primitiva n-ésima da unidade, temos que $[L : \mathbb{Q}] = \varphi(n)$.

Teorema 1.2.3. *[33] O anel dos inteiros de $L = \mathbb{Q}(\zeta_n)$ é $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}\}$ é uma base integral de $\mathcal{O}_L$.*

Teorema 1.2.4. *[22] Seja $\zeta_n \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade. Então $L = \mathbb{Q}(\zeta_n)$ é uma extensão galoisiana de $\mathbb{Q}$, cujo grupo de Galois $Aut(L/\mathbb{Q})$ é canonicamente isomorfo a $(\mathbb{Z}_n)^*$, e portanto abeliano de ordem $\varphi(n)$.*

Assim, temos o isomorfismo $Aut(L/\mathbb{Q}) \simeq (\mathbb{Z}_n)^*$. Obviamente $(\mathbb{Z}_n)^*$ é abeliano, mas nem sempre é cíclico. Prova-se que $(\mathbb{Z}_n)^*$ é cíclico se, e somente se, $n = 2$, 4, p^r ou $2p^r$, para p primo ímpar e $r \geq 1$ [35].

O grupo de Galois $Aut(L/\mathbb{Q})$ consiste dos $\varphi(n)$ automorfismos σ_j onde $mdc(j, n) = 1$, $j = 1, \cdots, \varphi(n)$, sendo σ_j univocamente determinado por $\sigma_j(\zeta_n) = \zeta_n^j$; em particular, σ_1 é a identidade de L.

Dado um corpo L, o subcorpo de L fixado ponto a ponto pela conjugação complexa é chamado *o subcorpo maximal real* de L.

Proposição 1.2.1. *[31] Seja $L = \mathbb{Q}(\zeta_n)$, com ζ_n uma raiz primitiva n-ésima da unidade, temos que*

i) $K = \mathbb{Q}(\alpha)$, $\alpha = \zeta_n + \zeta_n^{-1}$, é o subcorpo maximal real de L;

ii) o anel dos inteiros algébricos de K é $\mathbb{Z}[\alpha]$;

iii) $1, \alpha, \cdots, \alpha^{\frac{\varphi(n)}{2}-1}$ formam uma base integral de K.

Um resultado envolvendo corpos ciclotômicos e o conceito de corpos de números abelianos, devido a Kronecker e Weber, é o seguinte:

Teorema 1.2.5. *[31] Seja K uma extensão finita e abeliana dos racionais (isto é, galoisiana com grupo de Galois abeliano). Então K está contido em algum corpo ciclotômico.*

O principal invariante dos corpos de números algébricos é caracterizado nos corpos ciclotômicos pelo seguinte teorema:

Teorema 1.2.6. *[44] O discriminante de $L = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

$$d_L = d_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Como consequência segue que

- se $n = p$, então $d_L = (-1)^{\frac{(p-1)}{2}} p^{p-2}$;
- se $n = p^r$ então $d_L = (-1)^{\frac{(p-1)p^{r-1}}{2}} p^{p^{r-1}\cdot(r(p-1)-1)}$, r inteiro positivo.

Teorema 1.2.7. *[31] O discriminante de $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ sobre $\mathbb{Q}$ é dado por:*
i) $d_K = p^{\frac{p-3}{2}}$, *se* $n = p \geq 5$;
ii) $d_K = 2^{(r-1)2^{r-2}-1}$, *se* $n = 2^r$;
iii) $d_K = p^{\frac{(r+1)(p-1)p^{r-1}-p^r-1}{2}}$, *se* $n = p^r$, $p \neq 2$, $r > 1$.

Proposição 1.2.2. *[25] Se $L = \mathbb{Q}(\zeta_{p^r})$ então*

$$Tr_{L/\mathbb{Q}}(\zeta_{p^r}^k) = \begin{cases} 0 \quad se \quad mdc(k, p^r) < p^{r-1}; \\ -p^{r-1} \quad se \quad mdc(k, p^r) = p^{r-1}; \\ p^{r-1}(p-1) \quad se \quad mdc(k, p^r) > p^{r-1}. \end{cases}$$

Corolário 1.2.2. *[25] Se $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ então*

$$Tr_{K/\mathbb{Q}}(\zeta_{p^r}^k + \zeta_{p^r}^{-k}) = \begin{cases} 0 \quad se \quad mdc(k, p^r) < p^{r-1}; \\ -p^{r-1} \quad se \quad mdc(k, p^r) = p^{r-1}; \\ p^{r-1}(p-1) \quad se \quad mdc(k, p^r) > p^{r-1}. \end{cases}$$

Demonstração: Pela transitividade do traço temos

$$Tr_{L/\mathbb{Q}}(\zeta_{p^r}^k) + Tr_{L/\mathbb{Q}}(\zeta_{p^r}^{-k}) = Tr_{L/\mathbb{Q}}(\zeta_{p^r}^k + \zeta_{p^r}^{-k}) = Tr_{K/\mathbb{Q}}(Tr_{L/K}(\zeta_{p^r}^k + \zeta_{p^r}^{-k})) = 2Tr_{K/\mathbb{Q}}(\zeta_{p^r}^k + \zeta_{p^r}^{-k}).$$

Como $Tr_{L/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{L/\mathbb{Q}}(\zeta_{p^r}^{-k})$, segue que $Tr_{K/\mathbb{Q}}(\zeta_{p^r}^k + \zeta_{p^r}^{-k}) = Tr_{L/\mathbb{Q}}(\zeta_{p^r}^k)$ e, pela Proposição (1.2.2), o resultado segue. ∎

1.2.2 Decomposição de ideais primos

Nesta seção veremos que todo ideal no anel dos inteiros de um corpo de números pode ser fatorado unicamente como produto de ideais primos.

Definição 1.2.4. *Um* **ideal** $\mathcal{I}$ *de um anel comutativo* R *é um subgrupo aditivo de* R *o qual é estável sob a multiplicação por* R*, isto é,* $a\mathcal{I} \subset \mathcal{I}$ *para todo* $a \in R$*. Um ideal* $\mathcal{I}$ *é* **principal** *se ele é da forma* $\mathcal{I} = (x) = xR = \{xy, y \in R\}$, $x \in \mathcal{I}$.

Definição 1.2.5. *Dizemos que um ideal* $\mathcal{I}$ *é* **primo** *se ele satisfaz a seguinte propriedade: se* $xy \in \mathcal{I}$ *então* $x \in \mathcal{I}$ *ou* $y \in \mathcal{I}$.

A noção de ideal pode ser estendida como a seguir.

Definição 1.2.6. *Um* **ideal fracionário** $\mathcal{I}$ *é um* $\mathcal{O}_K$*-submódulo de* K *tal que existe* $d \in \mathcal{O}_K \setminus \{0\}$ *com* $\mathcal{I} \subseteq d^{-1}\mathcal{O}_K$.

Teorema 1.2.8. *[40] Todo ideal* $\mathcal{I} \neq 0$ *de* $\mathcal{O}_K$ *tem uma* $\mathbb{Z}$*-base livre,* $\{v_1, \cdots, v_n\}$ *onde* n *é o grau de* K.

Definição 1.2.7. *Seja* $\mathcal{I}$ *um ideal de* $\mathcal{O}_K$*. Sua norma é definida por* $N(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$.

Observação 1.2.3. *Segue diretamente que se* $\mathcal{I} = a\mathcal{O}_K$ *é principal, então* $N(\mathcal{I}) = |N_{K/\mathbb{Q}}(a)|$.

Sabemos que para todo $n \in \mathbb{Z}$, existe uma única fatoração em números primos. Esta noção de fatoração é substituída de modo análogo para ideais.

Teorema 1.2.9. *[36] Todo ideal* $\mathcal{I}$ *de* $\mathcal{O}_K$ *pode ser escrito de forma única como um produto de potências de ideais primos:*

$$\mathcal{I} = \prod_{i=1}^{m} \mathcal{B}_i^{e_i}.$$

Exemplo 1.2.1. *Se* p *é um número primo e* $\mathcal{O}_K$ *é o anel dos inteiros algébricos de* $K = \mathbb{Q}(\zeta_p)$*, então o ideal* $p\mathcal{O}_K$ *é da forma* $p\mathcal{O}_K = (1-\zeta_p)^{p-1}\mathcal{O}_K$*. De fato: Se* $1 \leq k, j \leq p-1$*, então existe um inteiro* t*, onde* $1 \leq t \leq p-1$ *tal que* $j \equiv kt (\mathrm{mod}\, p)$*. Assim,*

$$1 - \zeta_p^j = 1 - (\zeta_p^k)^t = (1-\zeta_p^k)(1 + \zeta_p^k + \cdots + (\zeta_p^k)^{t-1}),$$

e portanto, $(1-\zeta_p^k)|(1-\zeta_p^j)$. *Analogamente* $(1-\zeta_p^j)|(1-\zeta_p^k)$. *Assim,* $1-\zeta_p^j$ *e* $1-\zeta_p^k$ *são associados em* $\mathcal{O}_K$. *Como o polinômio minimal de* $\mathbb{Q}(\zeta_p)$, $X^{p-1}+\cdots+X+1$, *é igual ao* p*-ésimo polinômio ciclotômico:* $\phi_p(X)=\prod_{k=1}^{p-1}(X-\zeta^k)$ *segue que, avaliando o polinômio em* $X=1$, *obtemos que* $p=\prod_{k=1}^{p-1}(1-\zeta^k)$. *Logo, existe um elemento invertível* β *em* $\mathcal{O}_K$ *tal que* $p=(1-\zeta_p)^{p-1}\beta$. *Assim,* $p\mathcal{O}_K=(1-\zeta_p)^{p-1}\mathcal{O}_K$.

Definição 1.2.8. *O conjunto* $\mathcal{D}_{K/\mathbb{Q}}^{-1}=\{x\in K \mid \forall\,\alpha\in\mathcal{O}_K, Tr_{K/\mathbb{Q}}(x\alpha)\in\mathbb{Z}\}$ *é um ideal fracionário de* $\mathcal{O}_K$ *chamado o* **codiferente**. *O seu ideal inverso* $\mathcal{D}_{K/\mathbb{Q}}$ *é um ideal inteiro de* $\mathcal{D}_K$ *chamado o* **diferente**.

CAPÍTULO 2

Reticulados

Os reticulados têm se mostrado bastante úteis em aplicações na teoria das comunicações. Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular.

Devido ao fato de os códigos geometricamente uniformes serem caracterizados pela existência de isometrias (simetrias) internas, estes possuem várias propriedades interessantes e, neste caso, há mais ferramentas para o estudo da geometria do código. Isso dá mais uma boa razão para estudar o problema de empacotamento via reticulados, pois todo reticulado é geometricamente uniforme.

Neste capítulo apresentamos as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e mergulho canônico. Através do mergulho canônico obtemos um método de gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel dos inteiros de um corpo de números. O grande desafio é encontrar o anel dos inteiros de qualquer corpo de números, uma vez que são conhecidos apenas o anel dos inteiros dos corpos quadráticos e dos corpos ciclotômicos. Deste modo, no presente capítulo apresentamos um estudo sobre reticulados no $\mathbb{R}^n$. Lembramos que os reticulados de maior interesse são aqueles com maior densidade de empacotamento.

2.1 Reticulados

Nesta seção apresentamos o conceito de reticulados enfocando suas principais propriedades. Para maiores detalhes ver [14].

Definição 2.1.1. *Seja* $\mathbf{v}_1, \ldots, \mathbf{v}_m$ *um conjunto de vetores linearmente independentes em* $\mathbb{R}^n$ *(tal que* $m \leq n$*). O conjunto de pontos*

$$\Lambda = \{\mathbf{x} = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i,\ \lambda_i \in \mathbb{Z}\}$$

é chamado um **reticulado** *de posto* m*, e* $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ *é chamado uma base do reticulado.*

Definição 2.1.2. *O paralelepípedo formado pelos pontos*

$$\theta_1 \mathbf{v}_1 + \cdots + \theta_m \mathbf{v}_m,\ 0 \leq \theta_i < 1$$

é chamado um **paralelepípedo fundamental** *ou* **região fundamental** *do reticulado.*

Exemplo 2.1.1. $\Lambda = \mathbb{Z}^2$ *é um reticulado gerado pelos vetores* $e_1 = (1, 0)$ *e* $e_2 = (0, 1)$ *com região fundamental descrita na figura abaixo.*

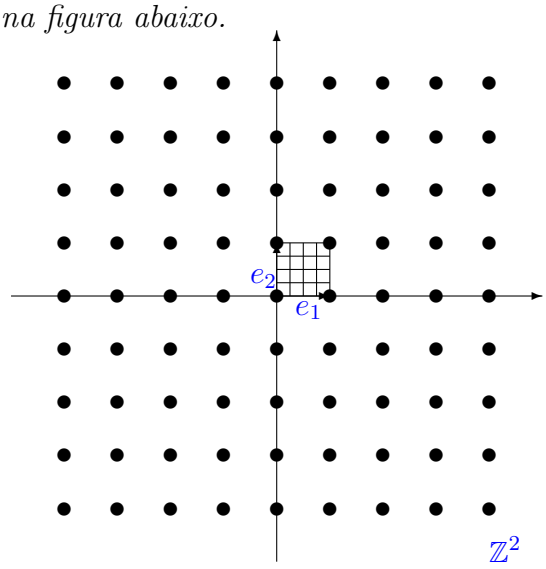


Figura 2.1: **Reticulado** $\Lambda = \mathbb{Z}^2$

Definição 2.1.3. *Seja* $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ *uma base de* Λ. *Se* $v_i = (v_{i1}, \ldots, v_{in})$, *para* $i = 1, \cdots, m$, *a matriz*

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

é chamada uma **matriz geradora** *para o reticulado. A matriz* $G = MM^t$ *é chamada uma* **matriz de Gram** *para o reticulado, onde* t *denota a transposição.*

Como M contém os vetores da base do reticulado $\{\mathbf{v}_i\}_{i=1}^m$, a (i, j)-ésima entrada da matriz G é o produto interno $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \mathbf{v}_i \cdot \mathbf{v}_j^t$.

Os pontos do reticulado são formados por

$$\Lambda = \{\mathbf{x} = \lambda M | \lambda \in \mathbb{Z}^m\}.$$

Definição 2.1.4. *O* **determinante do reticulado** Λ *é definido como sendo o determinante da matriz* G

$$det(\Lambda) = det(G).$$

Um reticulado é dito ter *posto máximo* se $m = n$, e neste caso M é uma matriz quadrada. Assim,

$$det(\Lambda) = (det(M))^2.$$

Definição 2.1.5. *Para reticulados de posto máximo, a raiz quadrada do determinante do reticulado é o volume do paralelepípedo fundamental, também chamado* **volume do reticulado**, *e denotado por* $vol(\Lambda)$.

O volume do reticulado independe da base escolhida pois as bases de um mesmo reticulado diferem pelo produto de uma matriz invertível com entradas inteiras. Dessa forma, faz sentido definir o volume de Λ como sendo o volume de uma região fundamental.

Definição 2.1.6. *Seja* B *uma matriz* $n \times n$ *com entradas inteiras. Um* **sub-reticulado** *de* Λ *é dado por*

$$\Lambda' = \{\mathbf{x} = \lambda BM | \lambda \in \mathbb{Z}^n\}.$$

Num reticulado Λ de dimensão n em $\mathbb{R}^n$, temos naturalmente uma estrutura de anel induzida por $\mathbb{Z}^n$ e portanto, um grupo aditivo abeliano a ele associado. Assim, um sub-reticulado Λ' é então um subgrupo de Λ, e podemos considerar o grupo quociente Λ/Λ'.

O índice do sub-reticulado Λ' é a cardinalidade do grupo quociente Λ/Λ' e

$$|\Lambda/\Lambda'| = \frac{vol(\Lambda')}{vol(\Lambda)} = \frac{\sqrt{\det(\Lambda')}}{\sqrt{\det(\Lambda)}} = |det(B)|.$$

É sempre possível encontrar um sub-reticulado de um dado reticulado considerando sua *versão escalonada* por um fator inteiro.

Dado um reticulado Λ, um *reticulado escolonado* Λ' pode ser obtido multiplicando os vetores do reticulado por uma constante, isto é, $\Lambda' = c\Lambda$ onde $c \in \mathbb{R}$. Assim, Λ' é um sub-reticulado de Λ quando $c \in \mathbb{Z}$.

Mais geralmente, temos a seguinte definição.

Definição 2.1.7. *Se um reticulado pode ser obtido de outro por uma rotação, reflexão ou mudança de escalar, dizemos que eles são* **equivalentes**.

Consequentemente, duas matrizes geradoras M e M' definem reticulados equivalentes se, e somente se, eles são descritos por $M' = cUMB$, onde c é uma constante não nula, U é uma matriz com entradas inteiras e determinante ± 1 e B é uma matriz real ortogonal. As correspondentes matrizes de Gram são relacionadas por $G' = c^2UGU^t$. Se U tem determinante ± 1 e $c = 1$ então M e M' são reticulados congruentes.

Assim, temos que ter em mente que o mesmo reticulado pode ser representado em algumas diferentes maneiras. Como uma consequência, dado uma matriz de Gram (ou geradora), não é fácil determinar qual é o reticulado correspondente. Invariantes tais como a dimensão e o determinante poderão ajudar, mas um dos cuidados que temos que ter é que tendo o mesmo determinante não é suficiente para garantir que dois reticulados são equivalentes. Essas considerações serão importantes mais tarde, quando construiremos constelações de reticulados algébricos onde a orientação do reticulado no espaço euclidiano se torna importante.

Definição 2.1.8. a) *Um* **empacotamento esférico**, *ou simplesmente um empacotamento no* $\mathbb{R}^n$, *é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de*

quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.

b) *Um* **empacotamento reticulado** *é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* Λ *de* $\mathbb{R}^n$.

Estamos interessados no empacotamento associado a um reticulado Λ em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n;\ |x| \leq k\}$ com o reticulado Λ é um conjunto finito, de onde segue que o número $d_{min} = min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\}$ está bem definido e $(d_{min})^2$ é chamado de **norma mínima**. Observamos que $\rho = d_{min}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento, este raio é então chamado de **raio de empacotamento**.

Dado um empacotamento no $\mathbb{R}^n$, associado a um reticulado Λ com base $\{v_1, \cdots, v_n\}$, definimos a sua **densidade de empacotamento** de esferas de raio r como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a **densidade de empacotamento** de Λ é igual a

$$\Delta(\Lambda) = \frac{\text{Volume da parte da região fundamental coberta pelas esferas}}{\text{Volume da região fundamental}} = \frac{\mathcal{V}ol(\mathcal{B}(\rho))}{\mathcal{V}ol(\Lambda)} = \\ = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\sqrt{\det(MM^t)}},$$

$$\text{onde } \mathcal{V}ol(\mathcal{B}(1)) = \begin{cases} \dfrac{\pi^{n/2}}{(\frac{n}{2})!}, \text{ se n é par} \\ \\ \dfrac{2^n\pi^{(n-1)/2}((n-1)/2)!}{n!}, \text{ se n é ímpar} \end{cases}$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Exemplo 2.1.2. *Se* $\Lambda = \mathbb{Z}^2$ *com base* $(1,0)$ *e* $(0,2)$, *temos que* $\rho = 1/2$, $\mathcal{V}ol(\mathcal{B}(1)) = \pi.1 = \pi$, *o volume do reticulado é* $\mathcal{V}ol(\Lambda) = 1.2 = 2$, *a densidade de empacotamento é*

$$\Delta(\Lambda) = \mathcal{V}ol(\mathcal{B}(1)).\frac{\rho^2}{\mathcal{V}ol(\Lambda)} = \pi\frac{1}{4}.\frac{1}{2} = \frac{\pi}{8}$$

e a densidade de centro é $\delta(\Lambda) = 1/8$.

A seguir reunimos alguns dos conceitos importantes em reticulados.

- Se o raio das esferas em um empacotamento em $\mathbb{R}^n$ associado a um reticulado Λ é aumentado além do raio de empacotamento, então as esferas no empacotamento sobrepõem-se. Se o novo raio é suficientemente grande, todo ponto do espaço gerado por Λ estará dentro no mínimo de uma esfera. O menor raio que resulta em uma cobertura do espaço gerado por Λ é o **raio de cobertura** do empacotamento.

- Sejam Λ um reticulado, β uma base de Λ e V o espaço vetorial gerado por esta base. Definimos a **região de Voronoi** de $v \in \Lambda$ ($V(v)$) como sendo a região que contém todos os pontos de V que estão mais próximos de v do que qualquer outro ponto u do reticulado, isto é, $V(v) = \{x \in V; ||x - v|| \leq ||x - u||, \forall\, u \in \Lambda\}$.

- O **"número de vizinhos"** ou **"kissing number"** é o número máximo de vezes que uma esfera no espaço n-dimensional pode tocar uma esfera central (todas as esferas são de mesmo tamanho e não podem interceptar outra esfera). Denotaremos o "número de vizinhos" pela letra grega τ.

- Se Λ é um reticulado em $\mathbb{R}^n$, então o **reticulado dual** de Λ é

$$\Lambda^* = \{X \in \mathbb{R}^n : X \cdot U \in \mathbb{Z} \,\text{para todo}\, U \in \Lambda\},$$

  O asterisco será usado para indicar o dual.

- Um reticulado é chamado de **reticulado isodual** se ele é isométrico ou geometricamente congruente ao seu dual, isto é, se ele difere do seu dual somente por (possivelmente) uma rotação e reflexão.

- A conceito de um **quantizador** n-dimensional é dado a seguir. Sejam dados M pontos $P_1, \cdots, P_M$ em $\mathbb{R}^n$. A entrada x é um ponto arbitrário de $\mathbb{R}^n$; a saída é o ponto P_i mais próximo de x. Se o ponto mais próximo P_i não é único, então a saída é escolhida aleatoriamente dentre os pontos P_i mais próximos de x.

  A ação de um quantizador também pode ser descrita dizendo que o espaço $\mathbb{R}^n$ é particionado nas células de Voronoi $V(P_1), V(P_2) \cdots$ ao redor de P_i; se a entrada x pertence

a $V(P_i)$, a saída é P_i. Se todas as células de Voronoi $V(P_i)$ são congruentes (como no caso quando os P_i formam um reticulado) a um politopo Π, e colocarmos a origem de coordenadas no centróide de Π, definimos a quantização do erro de Π, que é o **segundo momento normalizado** por

$$G(\Pi) = \frac{\frac{1}{n-1}\int_{\Pi} x \cdot x dx}{V(\Pi)^{1+\frac{2}{n-1}}}, \tag{2.1}$$

onde $V(\Pi)$ é o volume n-dimensional de Π. Se os pontos P_i formam um reticulado Λ, com células de Voronoi congruentes a um politopo Π, escrevemos $G(\Lambda) = G(\Pi)$. *O problema de quantizadores em reticulados é encontrar um reticulado n-dimensional Λ para o qual $G(\Lambda)$ é um mínimo.*

Não é difícil mostrar que a solução do problema de quantizador um-dimensional é colocar pontos P_i uniformemente ao londo da reta real e assim formar o reticulado inteiro $\mathbb{Z}$. As células de Voronoi são intervalos de comprimento 1, e tomamos Π sendo o intervalo $[-1/2, 1/2]$. De (2.1) temos

$$G_1 = \frac{\int_{-1/2}^{1/2} x^2 dx}{\int_{-1/2}^{1/2} dx} = \frac{1}{12} = 0.083333...$$

Para o problema bidimensional, foi mostrado em [43] que os pontos deveriam formar um reticulado hexagonal; correspondentemente

$$G_2 = G(\text{hexágono regular}) = \frac{5}{36\sqrt{3}} = 0.0801875...$$

Enquanto o problema geral está sem solução em dimensões maiores, a solução para o problema de quantizador em reticulados é conhecida em três dimensões [4]: o melhor quantizador é o reticulado *body centered cubic* (bcc), e

$$G(bcc) = G(\text{octaedro truncado}) = \frac{19}{192 \cdot 2^{1/3}} = 0.078543...$$

Foi mostrado em [4] que o reticulado bcc é o único reticulado no qual $G(\Pi)$ é sempre um mínimo local. Para fins de comparação,

$$G(fcc) = G(\text{dodecaedro rômbico}) = 2^{-11/3} = 0.078745...$$

Em dimensões maiores os melhores reticulados quantizadores não são conhecidos.

Os melhores quantizadores n-dimensionais conhecidos até agora são sempre os reticulados duais dos reticulados de melhores densidades de empacotamento. Entretanto, não se espera que isto sempre acontecerá.

Dimensão	Melhores quantizadores conhecidos	Reticulados com maior densidade de empacotamento conhecidos
2	A_2^*	A_2
3	A_3^*	A_3
4	D_4^*	D_4
5	D_5^*	D_5
6	E_6^*	E_6
7	E_7^*	E_7
8	E_8^*	E_8
24	Λ_{24}^*	Λ_{24}

Tabela 2.1: **Melhores quantizadores conhecidos e reticulados com maior densidade de empacotamento**

2.1.1 Os reticulados raízes

As definições e algumas propriedades básicas de alguns reticulados conhecidos são dadas aqui. Os reticulados A_n, D_n, E_n e $\mathbb{Z}^n$ são chamados de **reticulados raízes** por causa de uma associação com o sistema de raízes de certas álgebras de Lie. Um modo de definir estes

reticulados é

$$\begin{aligned}
\mathbb{Z}^n &= \{(x_1, \ldots, x_n) : \ x_i \in \mathbb{Z}\} \\
A_n &= \{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} : \ x_1 + \cdots + x_{n+1} = 0\} \\
D_n &= \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \text{ é par}\} \\
E_8 &= \{(x_1, \ldots, x_8) : \text{todos } x_i \in \mathbb{Z} \text{ ou todos } x_i \in \mathbb{Z} + 1/2, \textstyle\sum x_i \text{ é par}\} \\
E_6 &= \{(x_1, \ldots, x_8) \in E_8 : x_1 + x_8 = x_2 + \cdots + x_7 = 0\} \\
E_7 &= \{(x_1, \ldots, x_8) \in E_8 : x_1 + \cdots + x_8 = 0\}
\end{aligned}$$

O reticulado A_n é chamado de reticulado *hexagonal* para $n = 2$. Para $n = 3$ é chamado de reticulado *face-centered cubic* (fcc) e tem a maior densidade de empacotamento entre todos os reticulados 3-dimensionais. O reticulado D_n é chamado de reticulado *checkerboard*. Quando $n = 3$ este reticulado equivale ao reticulado fcc. O reticulado E_8 é chamado de reticulado *Gosset*.

2.1.2 O reticulado mcc

Em [15] foi mostrado que entre todos os reticulados isoduais 3-dimensionais, o reticulado *mean-centered cubic* ou (mcc) tem, para uma distância mínima fixada, (raio de empacotamento) o menor raio de cobertura e em [16] que este reticulado é um ótimo quantizador. Sua base geradora é $\left\{\left(\sqrt{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}, 0\right), \left(\sqrt{\frac{1}{2}}, 0, \sqrt[4]{\frac{1}{2}}\right), \left(0, \sqrt[4]{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}\right)\right\}$. O reticulado mcc tem matriz de Gram

$$\frac{1}{2}\begin{pmatrix} 1+\sqrt{2} & -1 & -1 \\ -1 & 1+\sqrt{2} & 1-\sqrt{2} \\ -1 & 1-\sqrt{2} & 1+\sqrt{2} \end{pmatrix} \tag{2.2}$$

com determinante 1.

As propriedades de alguns dos reticulados mencionados acima e seus duais estão na Tabela (2.2).

Reticulado	Volume da região fundamental	Distância Mínima	Norma Mínima	Raio de cobertura	Densidade de centro	Kissing number	Segundo momento normalizado
$\mathbb{Z}^n$	1	1	1	$\frac{\sqrt{n}}{2}$	2^{-n}	$2n$	$\frac{1}{12}$
A_n	$\sqrt{n+1}$	$\sqrt{2}$	2	$\sqrt{\frac{\left\lfloor \frac{n+1}{2} \right\rfloor \left(n+1-\left\lfloor \frac{n+1}{2} \right\rfloor\right)}{n+1}}$	$\frac{2^{-n/2}}{(n+1)^{1/2}}$	$n(n+1)$	$\frac{1}{n+1}^{1/n} \left\lfloor \frac{1}{12} + \frac{1}{6(n+1)} \right\rfloor$
A_n^*	$\frac{1}{\sqrt{n+1}}$	$\sqrt{\frac{n}{n+1}}$	$\frac{n}{n+1}$	$\sqrt{\frac{n(n+2)}{12(n+1)}}$	$\frac{n^{n/2}}{2^n (n+1)^{(n-1)/2}}$	2, se $n=1$ $2n+2$, se $n \geq 2$	$*$
D_n	2	$\sqrt{2}$	2	1, se $n=3$ $\sqrt{n}$, se $n \geq 4$	$2^{-(n+2)/2}$	$2n(n-1)$	$\frac{1}{2^{2/n}} \left(\frac{1}{12} + \frac{1}{2n(n+1)}\right)$
D_n^*	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$, se $n=3$ 1, se $n \geq 4$	$\frac{3}{4}$, se $n=3$ 1, se $n \geq 4$	$\frac{\sqrt{5}}{2}$, se $n=3$ $2^{1-n}\sqrt{n/2}$, se n é par $\frac{\sqrt{2n-1}}{2}$, se $n \geq 5$ e n é ímpar	1	8, se $n=3$ 24, se $n=4$ $2n$, se $n \geq 5$	$*$
E_8	1	$\sqrt{2}$	2	1	$\frac{1}{16}$	240	$\frac{929}{12960}$
mcc	1	$(\frac{1}{2} + \sqrt{\frac{1}{2}})^{\frac{1}{4}}$	$\sqrt{\frac{1}{2} + \sqrt{\frac{1}{2}}}$	$3^{0.5}2^{-1.25}$	$0.1657\cdots$	8	$\frac{17+4\sqrt{2}}{288} = 0.0786696\cdots$

$*$ O segundo momento normalizado é descrito por uma relação de recorrência, e omitimos aqui.

Tabela 2.2: $*$ **Propriedades de alguns reticulados.**

2.2 Reticulados via corpos de números

A definição de mergulho canônico estabelece uma correspondência um a um entre os elementos do corpo de números algébrico de grau n e os vetores do espaço euclidiano n-dimensional. Nesta seção apresentamos a geração de reticulados via ideais do anel de inteiros de um corpos de números através do mergulho canônico.

Sejam K um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_j : K \to \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de K sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(K) \subseteq \mathbb{R}$ diz-se que σ_j é **real**, caso contrário, σ_j é dito **imaginário**. Quando todos os monomorfismos são reais diz-se que K é um **corpo totalmente real** e quando os monomorfismos são todos imaginários diz-se que K é um **corpo totalmente complexo**. Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, temos que $\alpha \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(K) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(K) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$. Então $n - r_1$ é um número par, assim podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in K$, temos que o homomorfismo $\sigma_K : K \to \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ definido por

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2},$$

é um homomorfismo injetivo de anéis, chamado de **mergulho canônico** de K em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$.

O par (r_1, r_2) é chamado a **assinatura** de K. Se $r_2 = 0$ dizemos que o corpo de números é *totalmente real* e se $r_1 = 0$ dizemos que o corpo de números é *totalmente complexo*.

Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com $\mathbb{R}^n$, e este homomorfismo pode também ser visto como

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

onde as notações $\Re(x)$ e $\Im(x)$ representam as partes real e imaginária do número complexo x, respectivamente.

Observação 2.2.1. *Podemos definir um mergulho similar se considerarmos ao invés da extensão $K/\mathbb{Q}$ a extensão relativa L/K.*

Exemplo 2.2.1. *Considere o corpo ciclotômico* $K = \mathbb{Q}(\zeta_5)$, *onde* $\zeta_5 = e^{\frac{2\pi i}{5}}$ *e* $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* K *em* $\mathbb{C}$. *Como* K *é um corpo totalmente complexo, temos que* $r_1 = 0$ *e* $r_2 = 2$. *Os 4 monomorfismos são dados por* $\sigma_1(\zeta_5) = \zeta_5$, $\sigma_2(\zeta_5) = \zeta_5^2$, $\sigma_3(\zeta_5) = \zeta_5^3$, $\sigma_4(\zeta_5) = \zeta_5^4$. *Se* $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 \in K$, *com* $a, b, c, d, e \in \mathbb{Q}$, *temos que* $\sigma_K(x) = (\Re\sigma_1(x), \Im\sigma_1(x), \Re\sigma_2(x), \Im\sigma_2(x))$.

Uma das aplicações deste mergulho é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria dos números algébricos, através de propriedades herdadas de K. Isto pode ser visto de maneira formal no resultado que segue.

Teorema 2.2.1. *[36] Sejam* $\{w_1, \cdots, w_n\}$ *uma base integral de* K *e* $\sigma : K \to \mathbb{C}$ *o mergulho canônico. Os* n *vetores* $\mathbf{v_i} = \sigma(w_i) \in \mathbb{R}^n$, $i = 1, \cdots, n$ *são linearmente independentes e definem um reticulado em* $\mathbb{R}^n$, *denominado* **reticulado algébrico** *de posto máximo,* $\Lambda = \sigma(\mathcal{O}_K)$.

Proposição 2.2.1. *[36] Seja* K *um corpo de números de grau* n *e* M *um* $\mathbb{Z}$*-submódulo livre de* K *de posto* n. *Se* $(x_i)_{1\leq i\leq n}$ *é uma* $\mathbb{Z}$*-base de* M, *então* $\sigma(M)$ *é um reticulado em* $\mathbb{R}^n$.

Concluímos assim, que o ingrediente chave para a construção de reticulados algébricos tem sido a existência de uma $\mathbb{Z}$-base livre em K. Como $\mathcal{O}_K$ e seus ideais são $\mathbb{Z}$-módulos livres de posto n, podemos mergulhá-los em $\mathbb{R}^n$ para obter um reticulado algébrico.

A matriz geradora M de um reticulado algébrico é dada por

$$M = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_{r_1}(w_1) & \Re\sigma_{r_1+1}(w_1) & \cdots & \Im\sigma_{r_1+r_2}(w_1) \\ \vdots & & & \vdots & & \\ \sigma_1(w_n) & \cdots & \sigma_{r_1}(w_n) & \Re\sigma_{r_1+1}(w_n) & \cdots & \Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}, \tag{2.3}$$

onde $\{w_1, \cdots, w_n\}$ é aqui uma base de $\mathcal{O}_K$.

Um reticulado algébrico Λ' construído a partir de um ideal $\mathcal{I} \subset \mathcal{O}_K$ fornece um sub-reticulado ([14], [7]) do reticulado algébrico Λ construído a partir de $\mathcal{O}_K$. Se $\mathcal{I} = \mathfrak{a}\mathcal{O}_K$, então a matriz geradora M é dada por

$$M = \begin{pmatrix} \sigma_1(\mathfrak{a}w_1) & \cdots & \sigma_{r_1}(\mathfrak{a}w_1) & \Re\sigma_{r_1+1}(\mathfrak{a}w_1) & \cdots & \Im\sigma_{r_1+r_2}(\mathfrak{a}w_1) \\ \vdots & & & \vdots & & \\ \sigma_1(\mathfrak{a}w_n) & \cdots & \sigma_{r_1}(\mathfrak{a}w_n) & \Re\sigma_{r_1+1}(\mathfrak{a}w_n) & \cdots & \Im\sigma_{r_1+r_2}(\mathfrak{a}w_n) \end{pmatrix} \tag{2.4}$$

onde $\{w_1, \cdots, w_n\}$ é uma base de $\mathcal{O}_K$. Equivalentemente, a matriz (2.4) é a matriz (2.3) multiplicada pela matriz diagonal

$$\begin{pmatrix} \sigma_1(\mathfrak{a}) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\mathfrak{a}) \end{pmatrix}.$$

Dada a matriz geradora acima, é fácil calcular o determinante do reticulado. Por definição, temos

$$\begin{aligned} det(\Lambda) &= |det(M)|^2 \\ &= |det[\sigma_j(\mathfrak{a}w_i)]|^2 \\ &= |\mathcal{N}(\mathfrak{a})|^2 |det[\sigma_j(w_i)]|^2 \\ &= |\mathcal{N}(\mathfrak{a})|^2 d_K. \end{aligned}$$

A Tabela (2.3) informa sobre com qual corpo de números é possível construir algebricamente os reticulados com maior densidade de empacotamento (D_4, E_6, E_8, Λ_{24}) e maior densidade de empacotamento conhecida (K_{12}, Λ_{16}) em suas respectivas dimensões.

Λ	$\mathbb{Q}(\theta)$	Ideais
D_4	$\theta = \zeta_8$	$(2, \theta + 1)$
E_6	$\theta = \zeta_9$	$(3, (\theta + 1)^2)$
E_8	$\theta = \zeta_{20}$	$(5, \theta - 2)$
K_{12}	$\theta = \zeta_{21}$	$(7, \theta + 3)$
Λ_{16}	$\theta = \zeta_{40}$	$(2, \theta^4 + \theta^3 + \theta^2 + \theta + 1)$ e $(5, \theta^2 + 2)$
Λ_{24}	$\theta = \zeta_{39}$	$(3, \theta^3 + \theta^2 - 1)$, $(3, \theta^3 + \theta^2 + \theta + 1)$ e $(13, \theta - 3)$

Tabela 2.3: **Reticulados construídos a partir dos corpos ciclotômicos.**

Viterbo propôs o problema de encontrar uma construção algébrica para o reticulado *mean centered cubic* (mcc). Baseado em sua matriz geradora (2.2), Viterbo propôs extensões de corpos do tipo

$$6 = \varphi(m) \begin{cases} K = \mathbb{Q}(\zeta_m + \zeta_m^{-1}, \sqrt{2}) \\ |3 = n = \varphi(m)/2 \\ \mathbb{Q}(\sqrt{2}) \\ |2 \\ \mathbb{Q} \end{cases} \tag{2.5}$$

onde os possíveis valores de m são 7, 3^2, 14 e 18.

De modo análogo as construções existentes tomamos todos os possíveis ideais principais na extensão relativa $\mathcal{O}_{K/\mathbb{Q}(\sqrt{2})}$ e a partir daí, fazendo o uso da Proposição (2.2.1), aplicamos o mergulho canônico para então obtermos a matriz geradora do reticulado obtido. Para trabalhar com extensões relativas usamos o programa algébrico *Kash* [21]. Calculando a densidade de centro de todos os reticulados obtidos via este processo, para todos os possíveis valores de m, vimos que todas diferem da densidade de centro do reticulado mcc, lembrando que esta é uma condição necessária, mas não suficiente para que tais reticulados sejam uma construção algébrica do reticulado mcc. Assim concluímos que via a extensão de corpos (2.5) não é possível obter uma construção algébrica do reticulado mcc, o que não descarta a possibilidade de existir construções algébricas para o reticulado mcc considerando outras extensões de corpos.

2.3 Reticulado ideal

Esta seção é dedicada aos reticulados ideais, isto é, reticulados algébricos dotados com uma forma traço.

Seja K um corpo de números, isto é, uma extensão finita de $\mathbb{Q}$, de grau $n = [K : \mathbb{Q}]$.

Definição 2.3.1. *Um corpo de números K é chamado um* **corpo** CM *se existe um corpo de números totalmente real $\mathbb{F}$ tal que K é uma extensão quadrática totalmente imaginária de $\mathbb{F}$.*

Definição 2.3.2. *Seja L uma extensão de K. O* **fecho de Galois** *de L/K é um corpo $M \supset L$ que é uma extensão de Galois de K e é minimal neste sentido, isto é, nenhum subcorpo próprio de M contendo L é o corpo de decomposição de algum polinômio $p \in L[X]$.*

Observação 2.3.1. *Denotamos por K^{Gal} o fecho de Galois de K sobre $\mathbb{Q}$. Note que se K é um corpo CM, então a conjugação complexa comuta com todos os elementos de $Gal(K^{Gal}/\mathbb{Q})$.*

Definição 2.3.3. *1. Uma* **involução** $\mathbb{Q}$*- linear* $^{-}: K \longrightarrow K$ *é uma aplicação aditiva e multiplicativa tal que* $\bar{\bar{x}} = x$*, para* $\forall\, x \in K$*.*

2. O conjunto $\mathbb{F} = \{x \in K \,|\, \bar{x} = x\}$ *é um corpo, chamado* **corpo fixo da involução**.

Proposição 2.3.1. *[5] Com as notações da Definição (2.3.3) temos que* $[K : \mathbb{F}] \leq 2$.

Demonstração: Seja K um corpo de números de grau n e seja G o grupo de Galois de K, ou seja, o grupo dos automorfismos de K em $\mathbb{C}$.

$$\begin{array}{ccc} K & \longrightarrow & \{id\} \\ | & & | \\ \mathbb{F} & \longrightarrow & H = \{id, {}^{-}\},\ \text{pois } {}^{-} = id \\ \vdots & & \vdots \\ & \longrightarrow & G \end{array}$$

Pelo Teorema da Correspondência de Galois, segue que $[K : \mathbb{F}] = (H : \{id\}) = o(H)$. Temos que $H = \{id, {}^{-}\}$, logo $o(H) = 1$, se ${}^{-} = id$, ou $o(H) = 2$, se ${}^{-} \neq id$. Portanto, $o(H) \leq 2$ e consequentemente, $[K : \mathbb{F}] \leq 2$. ∎

Definição 2.3.4. *Um* **reticulado inteiro** *é um par (L, b), onde L é um $\mathbb{Z}$- módulo livre de posto n e $b : L \times L \to \mathbb{Z}$ é uma forma $\mathbb{Z}$- bilinear simétrica.*

Definição 2.3.5. *Seja $\{v_1, v_2, \cdots, v_n\}$ uma base de L. A matriz que representa a forma bilinear b é dada por $(b(v_i, v_j))_{i,j=1}^{n}$. O* **determinante** *de b é o determinante da matriz de b em alguma base de L.*

Definição 2.3.6. *Seja $\mathcal{I}$ um ideal de $\mathcal{O}_K$, e seja $\alpha \in \mathbb{F}$ tal que $\alpha\mathcal{I}\bar{\mathcal{I}} \subset \mathcal{D}_{K/\mathbb{Q}}^{-1}$. Um* **reticulado ideal** *é um reticulado inteiro $(\mathcal{I}, b_\alpha)$, onde*

$$b_\alpha : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z},\ b_\alpha(x, y) = Tr_{K/\mathbb{Q}}(\alpha x \bar{y}),\ \forall\, x, y \in \mathcal{I}.$$

Note que a condição $\alpha\mathcal{I}\bar{\mathcal{I}} \subset \mathcal{D}_{K/\mathbb{Q}}^{-1}$ garante que o reticulado seja inteiro e a escolha $\alpha \in \mathbb{F}$ garante que a forma traço seja simétrica:

$$b_\alpha(x,y) = Tr_{K/\mathbb{Q}}(\alpha x\bar{y}) = \overline{Tr_{K/\mathbb{Q}}(\bar{\alpha}\bar{x}y)} = b_\alpha(y,x),$$

onde a última igualdade vale pois $Tr_{K/\mathbb{Q}}(z) \in \mathbb{Q}$, para todo $z \in K$ e $\bar{}$ é $\mathbb{Q}$-linear.

O determinante de um reticulado dado é o quadrado do volume da região fundamental [20]. No caso de reticulados ideais, ele está relacionado a d_K, o discriminante do corpo de números K. Denotamos por $det(\Lambda)$ ou $det(b)$ se $\Lambda = (L, b)$.

Proposição 2.3.2. *[5] Seja $(\mathcal{I}, b_\alpha)$ um ideal reticulado, então $|det(b)| = |d_K|\mathcal{N}(\mathcal{I})^2\mathcal{N}(\alpha)$.*

Demonstração: Como $\mathcal{I}$ é um $\mathbb{Z}$-módulo livre de posto n sobre $\mathcal{O}_K$ existe uma base $\{u_1, \ldots, u_n\}$ de $\mathcal{O}_K$ e inteiros positivos $q_1, \ldots, q_n$ tais que $\{u_1q_1, \ldots, u_nq_n\}$ é uma base para $\mathcal{I}$ [36]. Expressando-se a matriz geradora de $(\mathcal{I}, b)$ nesta base, mostra-se, de forma direta, que

$$|det(b)| = |d_K|N(\mathcal{I})^2N(\alpha).$$

◪

2.4 Reticulados via a perturbação do mergulho canônico

Nesta seção apresentamos uma pertubação do mergulho canônico e a geração de reticulados a partir dela.

Definição 2.4.1. *Seja α um elemento totalmente real e totalmente positivo de K, isto é, $\sigma_i(\alpha)$ é real e totalmente positivo para todo i.*

O homomorfismo $\sigma_\alpha(x) : K \to \mathbb{R}^n$ definido por

$$\begin{aligned}\sigma_\alpha(x) \;=\; & (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \ldots, \\ & \sqrt{2\alpha_{r_2}}\Re(\sigma_{r_2}(x)), \sqrt{2\alpha_{r_2}}\Im(\sigma_{r_2}(x))),\end{aligned}$$

onde $\alpha_i = \sigma_i(\alpha) > 0$, para $i = 1, \cdots, n$ é chamado uma **perturbação do mergulho canônico** *ou* **mergulho canônico torcido**.

Corolário 2.4.1. *[34] Seja G um $\mathbb{Z}$-módulo livre de posto n de $\mathcal{O}_K$ com $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$. Então a imagem de $\sigma_\alpha(G)$ de G em $\mathbb{R}^n$ é um reticulado com geradores $\{\sigma_\alpha(w_1), \ldots, \sigma_\alpha(w_n)\}$.*

Note que o principal fator que define o mergulho canônico e a perturbação do mergulho de K em $\mathbb{R}^n$ é uma $\mathbb{Z}$-base de n elementos. Como todo ideal $\mathcal{I}$ de $\mathcal{O}_K$ possui uma $\mathbb{Z}$-base de n elementos, podemos construir reticulados a partir de $\mathcal{I} \subset \mathcal{O}_K$ (ou $\mathcal{I} = \mathcal{O}_K$).

Lembre que um reticulado Λ pode ser definido por meio de sua matriz geradora M, isto é,

$$\Lambda = \{\mathrm{x} = \lambda M | \lambda \in \mathbb{Z}^n\},$$

e que sua correspondente matriz de Gram é definida por $G = MM^t$, onde t denota a matriz transposta. Desse modo temos a seguinte definição:

Definição 2.4.2. *Seja $\{w_1, \cdots, w_n\}$ uma $\mathbb{Z}$-base de $\mathcal{I}$. O reticulado $\sigma_\alpha(\mathcal{I})$ tem matriz geradora M dada por*

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_1) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_2) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(w_2) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_n) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_n) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}.$$

onde $\alpha_j = \sigma_j(\alpha),\ \forall j$.

Proposição 2.4.1. *[34] Seja K um corpo de números totalmente real ou CM. Então o reticulado $\sigma_\alpha(\mathcal{I})$ é um reticulado ideal.*

Demonstração: Para mostrar que $\sigma_\alpha(\mathcal{I})$ é um reticulado ideal mostramos que a forma bilinear associada é uma forma traço.

Sabemos a que matriz de Gram $G = MM^t = (g_{ij})_{i,j=1}^n$, com

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{r_1} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j) + \\ &\quad \sum_{k=1}^{r_2} 2\alpha_{r_1+k}[\Re(\sigma_{r_1+k}(w_i))\Re(\sigma_{r_1+k}(w_j)) + \Im(\sigma_{r_1+k}(w_i))\Im(\sigma_{r_1+k}(w_j))] \\ &= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_1} 2\alpha_{r_1+k}\Re(\sigma_{r_1+k}(w_i)(\sigma_{r_1+k})(\overline{w_j})) \\ &= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_1} \alpha_{r_1+k}\sigma_{r_1+k}(w_i\overline{w_j}) + \sum_{k=1}^{r_1} \alpha_{r_1+k}\overline{\sigma_{r_1+k}(w_i\overline{w_j})} \end{aligned}$$

$$= \quad Tr(\alpha w_i \overline{w_j}).$$

A segunda igualdade vale pois a conjugação complexa comuta com todos os σ_i, $i = 1, \cdots, n$, (ver Observação (2.3.1)). Provamos assim que as entradas da matriz G são da forma traço. Agora, como $\{w_1, \cdots, w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$, para $\forall\, x, y \in \mathcal{I}$ temos

$$\begin{aligned} b_\alpha(x,y) &= b_\alpha\left(\sum_{i=1}^{n} a_i w_i,\, \sum_{j=1}^{n} b_j w_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j b_\alpha(w_i,\, w_j) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j Tr_{K/\mathbb{Q}}(\alpha w_i \overline{w_j}) = Tr_{K/\mathbb{Q}}\left(\alpha \sum_{i=1}^{n} a_i w_i \sum_{j=1}^{n} b_j \overline{w_j}\right) \\ &= Tr_{K/\mathbb{Q}}(\alpha x \overline{y}), \end{aligned} \tag{2.6}$$

onde $a_i,\, b_j \in \mathbb{Z}$. Portanto a forma bilinear é uma forma traço, assim, concluímos que $\sigma_\alpha(\mathcal{I})$ é um reticulado ideal. ◪

Note a hipótese sobre α, comparada à Definição (2.3.6). Aqui α não é mais tomado satisfazendo $\alpha\mathcal{I}\overline{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$. Então o reticulado não é necessariamente inteiro. Esta condição foi substituída exigindo α totalmente real e totalmente positivo, assim $\sigma_j(\alpha) = \alpha_j$ é totalmente real e totalmente positivo e desse modo $\sqrt{\alpha_j}$ está bem definido para todo j.

A concepção de ideais reticulados tem duas vantagens. Uma delas é poder ver um reticulado em $\mathbb{R}^n$ dado por uma matriz geradora, e a outra é que os pontos do reticulado são imagens de inteiros algébricos através do mergulho canônico aplicado em $\mathcal{O}_K$. Deste modo, este processo enfatiza a correspondência entre os pontos $\mathbf{x} \in \Lambda \subseteq \mathbb{R}^n$ e os inteiros algébricos.

Usando a matriz geradora dada na Definição (2.4.2), um ponto do reticulado pode ser expresso como

$$\begin{aligned} \mathbf{x} &= (x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+r_2}) \\ &= (\sum_{i=1}^{n} \lambda_i \sqrt{\alpha_1}\sigma_1(w_i), \ldots, \sum_{i=1}^{n} \lambda_i \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_i)), \ldots, \sum_{i=1}^{n} \lambda_i \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_i))), \\ &\quad \lambda_i \in \mathbb{Z}, \quad i = 1, \ldots, n. \\ &= (\sqrt{\alpha_1}\sigma_1(\sum_{i=1}^{n} \lambda_i w_i), \ldots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(\sum_{i=1}^{n} \lambda_i w_i), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(\sum_{i=1}^{n} \lambda_i w_i)). \end{aligned}$$

Portanto,

$$\mathbf{x} = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)) = \sigma_\alpha(x)$$

para algum inteiro algébrico $x = \sum_{i=1}^{n} \lambda_i w_i \in \mathcal{I}$.

Esta correspondência entre um vetor $\mathbf{x} \in \mathbb{R}^n$ e um inteiro algébrico x de $\mathcal{O}_K$ facilita o cálculo de alguns elementos de reticulados que em geral são difíceis de se calcular.

2.4.1 Diversidade

Motivados pela minimização da probabilidade de erro em canais com desvanecimento do tipo Rayleigh, procuramos por reticulados com diversidade máxima e maior distância produto mínima.

Lembramos que dados dois vetores x e y no $\mathbb{R}^n$, a diversidade entre eles (ou distância mínima de Hamming) é o número de componentes em que eles diferem.

Dado um subconjunto $S \subseteq \mathbb{R}^n$, a **diversidade** ou a distância mínima de Hamming de S é

$$\min_{\mathbf{x},\mathbf{y} \in \mathbf{S}} \#\{i \mid x_i \neq y_i, \;\; i = 1, \ldots, n\}.$$

Todo reticulado Λ é um subconjunto do $\mathbb{R}^n$, então podemos estender essa definição a reticulados. Como reticulados tem estrutura de grupo, isto é, a soma de quaisquer dois pontos de Λ está em Λ, a distância de Hamming entre dois vetores pode ser reformulada como o número de componentes não nulas de qualquer vetor em Λ.

Definição 2.4.3. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$. A* **diversidade** *de Λ é definida como*

$$div(\Lambda) = \min_{0 \neq \mathbf{x} \in \mathbf{\Lambda}} \#\{i \mid x_i \neq 0, \;\; i = 1, \ldots, n\}.$$

Teorema 2.4.1. *[34] Os reticulados ideais $\Lambda = (\mathcal{I}, b_\alpha)$ exibem uma diversidade $div(\Lambda) = r_1 + r_2$, onde (r_1, r_2) é a assinatura de K.*

Demonstração: Seja $\mathbf{x} \neq 0$ um ponto arbitrário de Λ,

$$\mathbf{x} = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x)) = \sigma_\alpha(x),$$

com $x \in \mathcal{I} \subseteq \mathcal{O}_K$. Como $\mathbf{x} \neq 0$, segue que $x \neq 0$ e os primeiros r_1 coeficientes de $\mathbf{x}$ são não nulos. O número mínimo de coeficientes não nulos dos $2r_2$ que restaram é r_2, pois as partes real e imaginária de um homomorfismo complexo não podem se anular simultaneamente. Assim, a $div(\Lambda) \geq r_1 + r_2$. Agora, se $x = 1$, então $\sigma_j(1) = 1$, para $\forall\, j = 1, \cdots, r_1 + r_2$, e portanto $\sigma_\alpha(1)$ fornece $r_1 + r_2$ coeficientes não nulos, o que conclui a demonstração. ∎

2.4.2 Distância produto mínima

Estudamos o problema de calcular a distância produto mínima de reticulados ideais. Seja Λ um reticulado em $\mathbb{R}^n$. Se Λ tem diversidade $l \leq n$, definimos sua distância l-produto mínima por

$$d^l_{p,min}(\Lambda) = \min_{\mathbf{x}\neq\mathbf{y}\,\in\,\mathbf{\Lambda}} \prod |x_i - y_i|,$$

ou equivalentemente, podemos considerar a distância de $\mathbf{x} = (x_1, \cdots, x_n)$ à origem, por

$$d^l_{p,min}(\Lambda) = \min_{0\neq\mathbf{x}\,\in\,\mathbf{\Lambda}} \prod |x_i|,$$

onde ambos os produtos são tomados sobre as l componentes não nulas dos vetores.

Pelo Teorema (2.4.1) os reticulados ideais construídos sobre um corpo de números totalmente real (isto é, de assinatura $(n, 0)$) tem diversidade máxima. Em seguida, focaremos neste caso, e então assumimos que a diversidade é sempre maximal.

Definição 2.4.4. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n e $\mathbf{x} = (x_1, \cdots, x_n) \in \Lambda$. A* **distância produto mínima** *de Λ é*

$$d_{p,min}(\Lambda) = \min_{0\neq\mathbf{x}\,\in\,\mathbf{\Lambda}} \prod_{i=1}^{n} |x_i|.$$

Seja K um corpo de números totalmente real de grau n com discriminante d_K. A distância produto mínima de um reticulado ideal está relacionada com propriedades algébricas do corpo de números.

Teorema 2.4.2. *[34] Seja $\mathcal{I}$ um ideal de $\mathcal{O}_K$. A distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{I}, b_\alpha)$ de determinante $det(\Lambda)$ é*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(\Lambda)}{d_K}} min(\mathcal{I})$$

onde $min(\mathcal{I}) = \min_{0\neq\, x\,\in\,\mathcal{I}} \frac{|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{I})}$.

Demonstração: Seja $\mathbf{x} = \sigma_\alpha(x)$ um ponto do reticulado em $\mathbb{R}^n$, com $x \in \mathcal{I} \subseteq \mathcal{O}_K$ seu correspondente inteiro algébrico. Temos:

$$d_{p,min}(\Lambda) = \min_{0\neq\mathbf{x}\in\Lambda} \prod_{j=1}^{n} |x_j| = \min_{x\in\mathcal{I}} \prod_{j=1}^{n} |\sqrt{\sigma_j(\alpha)}\sigma_j(x)| = \sqrt{\mathcal{N}(\alpha)} \min_{x\neq 0\in\mathcal{I}} |N(x)|$$

Como, pela Proposição (2.3.2), $det(\Lambda) = \mathcal{N}(\alpha)\mathcal{N}(\mathcal{I})^2 d_K$ segue que $\sqrt{\mathcal{N}(\alpha)} = \dfrac{\sqrt{det(\Lambda)}}{\sqrt{d_K}\mathcal{N}(\mathcal{I})}$. Logo concluímos que

$$\begin{aligned} d_{p,min}(\Lambda) &= \sqrt{\mathcal{N}(\alpha)} \min_{x\neq 0\in\mathcal{I}} |\mathcal{N}(x)| = \frac{\sqrt{det(\Lambda)}}{\sqrt{d_K}\mathcal{N}(\mathcal{I})} \min_{x\neq 0\in\mathcal{I}} |\mathcal{N}(x)| \\ &= \sqrt{\frac{det(\Lambda)}{d_K}} \min_{x\neq 0\in\mathcal{I}} \frac{|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{I})} = \sqrt{\frac{det(\Lambda)}{d_K}} \min(\mathcal{I}). \end{aligned}$$

■

Corolário 2.4.2. *[34] Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_K$ então a distância produto mínima de Λ é*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_K}}.$$

Demonstração: De acordo com o Teorema (2.4.2), precisamos provar que $\min\limits_{0\neq x\in\mathcal{I}} \mathcal{N}(x) = \mathcal{N}(\mathcal{I})$. Como $\mathcal{I}$ é um ideal principal, segue que $\mathcal{I} = (\mathfrak{a})$, para $a \in \mathcal{I}$, e $\mathcal{N}(\mathcal{I}) = |\mathcal{N}(\mathfrak{a})|$. Se $x \in \mathcal{I}$, $x \neq 0$, então $x = \mathfrak{a}z$ para algum $z \in \mathcal{O}_K$. Assim,

$$|\mathcal{N}(x)| = |\mathcal{N}(\mathfrak{a})||\mathcal{N}(z)| \geq |\mathcal{N}(\mathfrak{a})| = \mathcal{N}(\mathcal{I})$$

e a igualdade é verdadeira se, e somente se, $\mathcal{N}(z) = \pm 1$, isto é, se, e somente se, z é uma unidade. Portanto, o mínimo é atingido para $x = \mathfrak{a}z$, onde z é uma unidade.

Agora, como $min(\mathcal{I}) = \min\limits_{0\neq x\in\mathcal{I}} \dfrac{|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{I})} = \dfrac{\mathcal{N}(\mathcal{I})}{\mathcal{N}(\mathcal{I})} = 1$ segue que $d_{p,min}(\Lambda) = \sqrt{\dfrac{det(\Lambda)}{d_K}}$. ■

Note que no caso em que $\mathcal{I} \subset \mathcal{O}_K$ é principal, a $d_{p,min}$ depende somente de d_K, o discriminante de K. No caso de ideais não principais a $d_{p,min}$ depende também de $min(\mathcal{I})$, que é difícil de avaliar. Como $min(\mathcal{I})$ aumenta quando o ideal não é principal, a questão é se o discriminante aumenta proporcionalmente.

Um modo de argumentar que $min(\mathcal{I})$ aumenta tanto quanto o discriminante é que existem limitantes conhecidos sobre $min(\mathcal{I})$ que dependem do discriminante, por exemplo, o limitante de Minkowski:

$$min(\mathcal{I}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{d_K},$$

onde K é um corpo de números de grau n e assinatura (r_1, r_2).

Apesar de ser possível determinar $d_{p,min}$ no caso de ideais não principais, esta ainda é uma questão em aberto. Em [34] é possível ver alguns exemplos em que ideais não principais apresentam valores piores para a $d_{p,min}$.

CAPÍTULO 3

Construção Algébrica de Reticulados

Neste capítulo apresentamos alguns métodos para construir reticulados que sejam eficientes para o canal com desvanecimento.

Na construção de constelações de sinais, dois aspectos fundamentais devem ser considerados: *rotulamento de bit* e a *forma da constelação*.

Estas questões são críticas para detectar a complexidade das implementações práticas e são estreitamente relacionadas uma com a outra. O rotulamento de bit consiste em aplicar os bits da entrada a pontos na constelação de sinais. Se queremos evitar o uso de uma grande tabela de procura, para performance do rotulamento de bit, precisamos de um algoritmo simples que aplica bits a sinais. Quando consideramos uma constelação obtida de um reticulado com a forma

$$\mathcal{C} = \{\mathbf{x} = \mathbf{u}M : \mathbf{u} = (u_1, \ldots, u_n) \in S_0^n\} \subset \Lambda,$$

o mais simples algoritmo de rotulamento que podemos usar é obtido executando o rotulamento de bit sobre as componentes inteiras u_i do vetor $\mathbf{u}$. Estes são usualmente restritos a chamada constelação 2^η/2-PAM, $S_0 = \{\pm 1, \pm 3, \ldots, \pm(2^\eta/2 - 1)\}$, onde η é o número de bits por duas dimensões. O rotulamento de Gray de cada 2^η/2-PAM componente unidimensional é uma eficiente estratégia para reduzir a probabilidade de erro [46]. Se nos restringirmos ao algoritmo simples de rotulamento acima, observamos que isto induz a uma forma da

constelação similar ao paralelepípedo fundamental do reticulado base.

Por outro lado, sabemos que tais constelações limitadas por uma esfera têm o melhor "ganho de forma" (em termos de energia média). Infelizmente, rotular uma constelação de forma esférica não é sempre uma tarefa fácil, sem usar uma tabela de busca. Assim, uma boa alternativa é escolher um reticulado no qual a forma do paralelepípedo fundamental não induza muita perda de energia.

Constelações de reticulados com forma cúbica são boas candidatas: elas são ligeiramente piores em termos do ganho de forma, pois estes reticulados não são os mais densos em suas dimensões mas são usualmente mais fáceis de rotular e decodificar.

Desta forma, códigos reticulados isomorfos a $\mathbb{Z}^n$ oferecem um bom equilíbrio entre boa forma e facilidade de rotulamento.

Portanto, nosso objetivo agora é a construção de tais $\mathbb{Z}^n$ reticulados com diversidade máxima e ótima distância produto mínima.

Em termos de reticulado ideal, isto significa que dado n, procuramos um corpo de números K de grau n e um ideal $\mathcal{I} \subseteq \mathcal{O}_K$ tal que $\Lambda = (\mathcal{I}, b_\alpha)$ seja equivalente a $\mathbb{Z}^n$, $n \geq 2$. Isto é, este reticulado admite uma matriz ortogonal como geradora e, em relação a esta base, a matriz de Gram é a identidade. Do ponto de vista geométrico, um reticulado $\Lambda' = (\mathcal{I}, b_\alpha)$ sobre $\mathcal{I} \subseteq \mathcal{O}_K$ é um sub-reticulado de $\Lambda = (\mathcal{O}_K, b_\alpha)$. A idéia é que dado um reticulado Λ, procurar-se um sub-reticulado que seja $\mathbb{Z}^n$ escalonado.

O determinante do reticulado será um critério útil para nos ajudar a encontrar o $\mathbb{Z}^n$-reticulado. Uma versão escalonada de $\mathbb{Z}^n$ é da forma $(\sqrt{c}\mathbb{Z})^n$ para algum inteiro c, tal que seu determinante é $det(G) = det(M)^2 = c^n$, pois o determinante de $\mathbb{Z}^n$ é 1. Usando a Proposição (2.3.2), deduzimos a seguinte condição necessária (mas não suficiente):

$$N(\mathcal{I})^2 N(\alpha)|d_K| = c^n \tag{3.1}$$

onde c é um inteiro. Podemos supor c o menor inteiro tal que $N(\alpha) \in \mathbb{Z}$. Se assumirmos que $\mathcal{I} = \mathcal{O}_K$, essa expressão é simplificada para

$$N(\alpha)|d_K| = c^n. \tag{3.2}$$

Esta condição necessária será útil para a escolha de um α para a construção de códigos $\mathbb{Z}^n$-reticulados. Uma vez que α é encontrado, um modo de verificar que de fato encontramos

um reticulado $\mathbb{Z}^n$-rotacionado é calcular a matriz de Gram MM^t, e certificar-se que obtemos a matriz identidade.

Deste modo, apresentamos 6 métodos para construir reticulados ideais $\mathbb{Z}^n$, e faremos a construção detalhada dos métodos 3 e 4, os quais encontram-se nos artigos em conjunto [1] e [2], respectivamente. Os outros métodos podem ser encontrados em [34].

1. **Construção quadrática**: usando o anel de inteiros do corpo quadrático construímos $\mathbb{Z}^2$-reticulados rotacionados.

2. **Construção ciclotômica via** $\mathbb{Q}(\zeta_p)$: usando o anel de inteiros do subcorpo maximal real de $\mathbb{Q}(\zeta_p)$, construímos $\mathbb{Z}^n$-reticulados rotacionados em dimensão $n = \frac{p-1}{2}$, $p \geq 5$ um número primo.

3. **Construção ciclotômica via** $\mathbb{Q}(\zeta_{2^r})$: usando o anel dos inteiros do subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r})$, construímos $\mathbb{Z}^n$-reticulados rotacionados em dimensão $n = 2^{r-2}$, $r \geq 1$.

4. **Construção ciclotômica via** $\mathbb{Q}(\zeta_{3^2})$: usando o anel dos inteiros do subcorpo maximal real de $\mathbb{Q}(\zeta_{3^2})$, construímos o $\mathbb{Z}^n$-reticulado rotacionado em dimensão 3.

5. **Construção cíclica**: usando o inverso do codiferente de um corpo cíclico de grau primo ímpar construímos $\mathbb{Z}^n$ reticulados rotacionados de dimensão prima ímpar.

6. **Construção mista**: combina as construções ciclotômica via $\mathbb{Q}(\zeta_p)$ e cíclica, resultando em reticulados de outras dimensões.

3.1 Construção ciclotômica via $\mathbb{Q}(\zeta_{2^r})$

Nesta seção faremos a construção de reticulados ideais $\mathbb{Z}^n$-rotacionados via o anel de inteiros do subcorpo maximal real do corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$. Os resultados obtidos aqui foram publicados em artigo conjunto [1].

Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{2^r})$ um corpo ciclotômico e $K = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ o subcorpo real maximal de $\mathbb{Q}(\zeta_{2^r})$, onde r é um inteiro positivo e ζ_{2^r} é uma raiz primitiva 2^r-ésima da unidade. Temos que o grau de $\mathbb{Q}(\zeta_{2^r})$ sobre $\mathbb{Q}$ é 2^{r-1} e o grau de $\mathbb{Q}(\zeta_{2^r})$ sobre K é 2, cujo polinômio minimal de ζ_{2^r} sobre K é dado por $x^2 - (\zeta_{2^r} + \zeta_{2^r}^{-1})x + 1$.

$$2^{r-1}\begin{cases}\mathbb{Q}(\zeta_{2^r})\\ |2\\ \mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})\\ |2^{r-2}=n\\ \mathbb{Q}\end{cases}$$

Seja $\Lambda = (\mathcal{O}_K, b_\alpha)$ um reticulado ideal. Como vimos em (3.1), uma condição necessária (mas não suficiente) para Λ ser isomorfo a $(\sqrt{c}\mathbb{Z})^n$, uma versão escalonada de $\mathbb{Z}^n$, é que

$$N(\alpha)d_K = c^n.$$

Assim temos que $N(\alpha)2^{(r-1)2^{r-2}} = c^{2^{r-2}} \overset{c=2^{r-1}}{\Rightarrow} N(\alpha) = 2$.

O elemento $\alpha = (1-\zeta_{2^r})(1-\zeta_{2^r}^{-1})$ é um elemento de $\mathcal{O}_K$ no qual a norma é 2. De fato, temos que

$$2\mathbb{Z}[\zeta] = (1-\zeta_{2^r})^{\phi(2^r)}\mathbb{Z}[\zeta]$$

em $\mathbb{Q}(\zeta_{2^r})$ tal que $N_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}(1-\zeta_{2^r}) = 2$. Usando a transitividade da norma, obtemos

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}(1-\zeta_{2^r}) &= N_{K/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_{2^r})/K}(1-\zeta_{2^r}))\\ &= N_{K/\mathbb{Q}}((1-\zeta_{2^r})(1-\zeta_{2^r}^{-1})) \end{aligned}$$

Consequentemente, $\alpha = (1-\zeta_{2^r})(1-\zeta_{2^r}^{-1})$ é um elemento de $K = \mathbb{Z}[\zeta_{2^r}+\zeta_{2^r}^{-1}]$ cuja norma é 2.

Como já foi mencionado, isto não garante a existência de uma versão escalonada de $\mathbb{Z}^n$. Para mostrar sua existência temos que construir explicitamente.

Proposição 3.1.1. *Considere $e_0 = 1$ e $e_i = \zeta_{2^r}^i + \zeta_{2^r}^{-i}$, para $i = 1, 2, \cdots, n-1$.*

1. *Se $i = 0, 1, \cdots, n-1$ então* $b_\alpha(e_i, e_i) = \begin{cases} 2n & \text{se } i = 0\\ 4n & \text{se } i \neq 0. \end{cases}$

2. *Se $i \neq 0$ então* $b_\alpha(e_i, e_0) = \begin{cases} -2n & \text{se } i = 1\\ 0 & \text{se } i \neq 1. \end{cases}$

3. Se $i \neq 0$, $j \neq 0$ e $i \neq j$ então $b_\alpha(e_i, e_j) = \begin{cases} -2n & se \quad \mid i-j \mid = 1 \\ 0 & \textit{caso contrário.} \end{cases}$

Demonstração: Pelo Corolário (1.2.2) temos que $Tr_{K/\mathbb{Q}}(\alpha e_0) = Tr(\alpha) = 2^{r-1}$, pois $mdc(1, 2^r) < 2^{r-1}$, e portanto $b_\alpha(e_0, e_0) = Tr_{K/\mathbb{Q}}(\alpha) = 2n$. Agora, como $mdc(i, 2^r) < 2^{r-1}$, para todo $i = 1, 2, \cdots, n$, segue que

$$\begin{aligned} b_\alpha(e_i, e_0) &= Tr_{K/\mathbb{Q}}(\alpha e_i) = Tr_{K/\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^i + \zeta^{-i})) \\ &= 2Tr_{K/\mathbb{Q}}(\zeta + \zeta^{-1}) - Tr_{K/\mathbb{Q}}(\zeta^{i+1} + \zeta^{-(i+1)}) - Tr_{K/\mathbb{Q}}(\zeta^{i-1} + \zeta^{-(i-1)}) \\ &= Tr_{K/\mathbb{Q}}(\zeta^{i-1} + \zeta^{-(i-1)}) \\ &= \begin{cases} -2n & \text{se} \quad i = 1 \\ 0 & \text{caso contrário.} \end{cases} \end{aligned}$$

Também, como $mdc(2i, 2^r), mdc(2i \pm 1, 2^r) < 2^{r-1}$, para todo $i = 1, 2, \cdots, n-1$, segue que

$$\begin{aligned} b_\alpha(e_i, e_i) &= Tr_{K/\mathbb{Q}}(\alpha e_i^2) = Tr_{K/\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^{2i} + \zeta^{-2i} + 2)) \\ &= 2Tr_{K/\mathbb{Q}}(\zeta^{2i} + \zeta^{-2i}) + Tr_{K/\mathbb{Q}}(4) - Tr_{K/\mathbb{Q}}(\zeta^{2i+1} + \zeta^{-(2i+1)}) \\ &\quad -Tr_{K/\mathbb{Q}}(\zeta^{2i-1} + \zeta^{-(2i-1)}) - 2Tr_{K/\mathbb{Q}}(\zeta + \zeta^{-1}) \\ &= 4n. \end{aligned}$$

Finalmente para $i \neq 0$, $j \neq 0$ and $i \neq j$, pois $mdc(i \pm j, 2^r), mdc(i + j \pm 1, 2^r) < 2^{r-1}$ segue que

$$\begin{aligned} b_\alpha(e_i, e_j) &= Tr_{K/\mathbb{Q}}(\alpha e_i e_j) = Tr_{K/\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^i + \zeta^{-i})(\zeta^j + \zeta^{-j})) \\ &= 2Tr_{K/\mathbb{Q}}(\zeta^{i+j} + \zeta^{-(i+j)}) + 2Tr_{K/\mathbb{Q}}(\zeta^{i-j} + \zeta^{-(i-j)}) \\ &\quad -Tr_{K/\mathbb{Q}}(\zeta^{i+j+1} + \zeta^{-(i+j+1)}) - Tr_{K/\mathbb{Q}}(\zeta^{i-j+1} + \zeta^{-(i-j+1)}) \\ &\quad -Tr_{K/\mathbb{Q}}(\zeta^{-i+j+1} + \zeta^{-(-i+j+1)}) - Tr_{K/\mathbb{Q}}(\zeta^{i+j-1} + \zeta^{-(i+j-1)}) \\ &= \begin{cases} -2n & \text{se} \quad \mid i-j \mid = 1 \\ 0 & \text{caso contrário,} \end{cases} \end{aligned}$$

o que conclui a demonstração. ∎

Corolário 3.1.1. *Se $Q(x, y) = \frac{1}{2^{r-1}} Tr_{K/\mathbb{Q}}(\alpha xy)$ então a matriz de Q na base $\{e_0, e_1, \cdots, e_{n-1}\}$,*

onde $e_0 = 1$, $e_i = \zeta_{2^r}^i + \zeta_{2^r}^{-i}$, $i = 1, \cdots, n-1$, *é dada por*

$$G = \begin{pmatrix} 1 & -1 & 0 & \cdots & & & \\ -1 & 2 & -1 & 0 & \cdots & & \\ 0 & -1 & 2 & \cdots & & & \\ & & & & \vdots & & \\ & & & & 2 & -1 & 0 \\ & & & \vdots & -1 & 2 & -1 \\ & & & \vdots & 0 & -1 & 2 \end{pmatrix}.$$

A matriz G do Corolário (3.1.1) é a matriz de Gram do reticulado $\mathbb{Z}^n$ relativa à base $\{w_0, w_1, \cdots, w_{n-1}\}$ definida por: $w_0 = E_0$, $w_i = -E_{i-1} + E_i$, $i = 1, 2, \cdots, n-1$ onde $\{E_j\}_{j=0}^{n-1}$ é a base canônica de $\mathbb{R}^n$, que é a base do reticulado $\mathbb{Z}^n$.

Isto implica que

$$\begin{aligned} \varphi : \quad & \Lambda \to \mathbb{Z}^n \\ & e_i \longmapsto w_i \end{aligned}$$

é um isomorfismo isométrico sobre o reticulado $\mathbb{Z}^n$.

Observando que

$$\begin{aligned} \varphi^{-1} : \quad & \mathbb{Z}^n \longrightarrow \Lambda \\ & E_i \longmapsto f_i = \sum_{j=0}^{i} e_j \end{aligned}$$

temos o seguinte resultado:

Proposição 3.1.2. *Seja* $\{f_0, f_1, \cdots, f_{n-1}\}$, *onde* $f_i = \sum_{j=0}^{i} e_j$, *para todo* $i = 0, 1, \cdots, n-1$, *uma outra base de* $\mathcal{O}_K$. *Então*

$$\frac{1}{2^{r-1}} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij},$$

isto é, o reticulado $(\mathcal{O}_K, \frac{1}{2^{r-1}} b_\alpha)$ *é isomorfo a* $\mathbb{Z}^n$, *onde* δ_{ij} *é o delta de Kronecker.*

Seja $Gal(K,\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_n\}$ o grupo de Galois de K sobre $\mathbb{Q}$. Então o reticulado gerado pelo anel dos inteiros algébricos tem a $n \times n$ matriz geradora dada por

$$M = \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \cdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}.$$

O elemento rotacionado pode ser representado pela matriz diagonal

$$A = diag(\sqrt{\sigma_k(\alpha)})_{k=1}^{n}$$

A matriz mudança de base de $\{e_j\}$ para $\{f_j\}$ é dada por

$$T = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix}.$$

Finalmente, a matriz geradora do $\mathbb{Z}^n$-reticulado é dada por

$$R = \frac{1}{\sqrt{2^{r-1}}} TMA.$$

Exemplo 3.1.1. *Seja $\mathbb{Q}(\zeta)$ um corpo ciclotômico e $K = \mathbb{Q}(\zeta + \zeta^{-1})$ seu subcorpo maximal real, onde $\zeta = \zeta_{2^3}$. Considerando a base $\{e_0 = 1, e_1 = \zeta + \zeta^{-1}\}$ de $\mathcal{O}_K$ e $b_\alpha(x,y) = \frac{1}{4} Tr_{K/\mathbb{Q}}(\alpha xy)$, onde $\alpha = 2 - (\zeta + \zeta^{-1})$, temos que a matriz de b_α é dada por*

$$G = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

Por outro lado, temos que

$$R = \tfrac{1}{2} TMA = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix} \begin{pmatrix} \sqrt{2-\sqrt{2}} & 0 \\ 0 & \sqrt{2+\sqrt{2}} \end{pmatrix} =$$

$$\begin{pmatrix} (-1-\sqrt{2})(\sqrt{2-\sqrt{2}}) & (-1+\sqrt{2})\sqrt{2+\sqrt{2}} \\ -\sqrt{2-\sqrt{2}} & -\sqrt{2+\sqrt{2}} \end{pmatrix} = \begin{pmatrix} -0.92388 & -0.382683 \\ 0.382683 & -0.92388 \end{pmatrix}.$$

E portanto $R.R^t = I_n$.

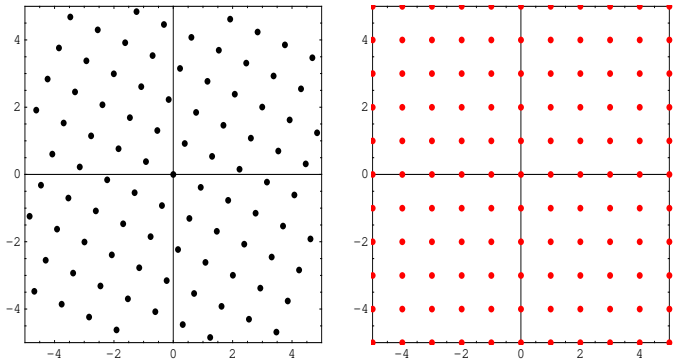


Figura 3.1: **Representação geométrica do reticulado ideal Λ e do reticulado $\mathbb{Z}^n$.**

- Reticulado ideal $\Lambda = (\mathcal{O}_K, b_\alpha)$

- Reticulado $\mathbb{Z}^n$

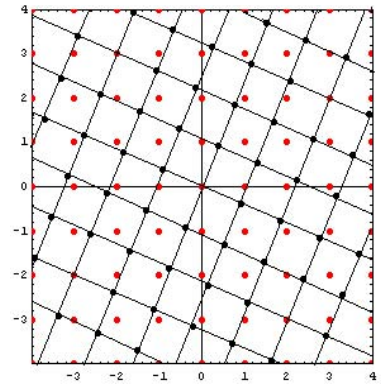


Figura 3.2: **O reticulado ideal Λ é um $\mathbb{Z}^n$ rotacionado.**

3.2 Construção ciclotômica via $\mathbb{Q}(\zeta_{3^2})$

Nesta seção faremos uma construção explícita da construção do $\mathbb{Z}^3$-reticulado rotacionado sobre o anel dos inteiros do subcorpo real maximal $K = \mathbb{Q}(\zeta_{3^2} + \zeta_{3^2}^{-1})$ de $\mathbb{L} = \mathbb{Q}(\zeta_{3^2})$. Os resultados obtidos aqui foram publicados em artigo conjunto [2].

Temos que $[K : \mathbb{Q}] = 3$, $\{e_0 = 1, e_1 = \zeta_{3^2} + \zeta_{3^2}^{-1}, e_2 = \zeta_{3^2}^2 + \zeta_{3^2}^{-2}\}$ é uma base integral de K e, pelo Teorema (1.2.7), temos que $d_K = 3^4$.

$$(3-1)3^{2-1} = 6 \begin{cases} \mathbb{Q}(\zeta_{3^2}) \\ |2 \\ \mathbb{Q}(\zeta_{3^2} + \zeta_{3^2}^{-1}) \\ |3 = n \\ \mathbb{Q} \end{cases}$$

Seja $\Lambda = (\mathcal{O}_K, b_\alpha)$ um reticulado ideal. Análogo à construção anterior, precisamos encontrar um elemento α tal que

$$N(\alpha)d_K = c^n.$$

Assim, temos que $N(\alpha)3^4 = c^3 \overset{c=3^2}{\Longrightarrow} N(\alpha) = 3^2$. Pelo uso da transitividade da norma, temos que $\alpha = ((1-\zeta_{3^2})(1-\zeta_{3^2}^{-1}))^2$ é um elemento de $\mathcal{O}_K$ cuja norma é 3^2 e consequentemente $\alpha = \frac{1}{3^2}((1-\zeta_{3^2})(1-\zeta_{3^2}^{-1}))^2$ é um elemento de $\mathcal{O}_K$ tal que $N(\alpha)d_K = 1 = det(\mathbb{Z}^n)$.

Proposição 3.2.1. *Se $Q(x,y) = \frac{1}{3^2}Tr_{K/\mathbb{Q}}(\alpha xy)$ então a matriz de Q na base $\{e_0, e_1, e_2\}$ onde $e_0 = 1$, $e_i = \zeta_{3^2} + \zeta_{3^2}^{-1}$, $i = 1, 2$, é dada por*

$$G = \begin{pmatrix} 2 & -3 & 2 \\ -3 & 6 & -5 \\ 2 & -5 & 5 \end{pmatrix}.$$

Observe que a matriz G é a matriz de Gram do $\mathbb{Z}^3$-reticulado rotacionado com base $\{w_0, w_1, w_2\}$ com $w_0 = -E_0 - E_1$, $w_1 = 2E_0 + E_1 + E_2$, $w_2 = -2E_0 - E_2$ onde $\{E_0, E_1, E_2\}$ é a base canônica de $\mathbb{Z}^3$. Isto implica que $\varphi(e_i) = w_i$, para $i = 0, 1, 2$, é um isomorfismo isométrico sobre o $\mathbb{Z}^3$-reticulado. A base que corresponde a base canônica de $\mathbb{Z}^3$ através deste

isomorfismo é dada por $f_i = \varphi^{-1}(E_i)$, para $i = 0, 1, 2$, isto é, $f_0 = -e_0 - e_1 - e_2$, $f_1 = e_1 + e_2$ e $f_2 = 2e_0 + 2e_1 + e_2$.

Portanto temos como um resultado direto:

Proposição 3.2.2. *Se $\{f_0, f_1, f_2\}$, onde $f_0 = -e_0 - e_1 - e_2$, $f_1 = e_1 + e_2$ e $f_2 = 2e_0 + 2e_1 + e_2$, é uma outra base de $\mathcal{O}_K$, então*

$$\frac{1}{3^2} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij},$$

i.e., o reticulado $(\mathcal{O}_K, \frac{1}{3^2} b_\alpha)$ é isomorfo a $\mathbb{Z}^3$.

Equivalentemente, poderíamos ter tomado $\alpha = \frac{1}{3^2}((1 - \zeta_{3^2})(1 - \zeta_{3^2}^{-1}))^2$ e teríamos o isomorfismo entre $(\mathcal{O}_K, b_\alpha)$ e $\mathbb{Z}^3$.

Observação 3.2.1. *Exigindo as condições acima no caso em que $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ e $\mathbb{L} = \mathbb{Q}(\zeta_{p^r})$, p um primo ímpar e r um inteiro positivo, chegamos que $c = p^r$ e $N_{K/\mathbb{Q}}(\alpha) = p^{\frac{1}{2}(p^{r-1}+1)}$, onde $\alpha = \dfrac{1}{p^r}((1 - \zeta_{p^r})(1 - \zeta_{p^r}^{-1}))^{\frac{1}{2}(p^{r-1}+1)}$. Porém, ao contrário da construção via $\mathbb{Q}(\zeta_{2^r})$, não é possível obter o isomorfismo entre $(\mathcal{O}_K, b_\alpha)$ e $\mathbb{Z}^n$, para todo p e r.*

O teorema a seguir estabelece uma condição necessária e suficiente para que um reticulado obtido algebricamente seja um reticulado $\mathbb{Z}^n$-rotacionado.

Teorema 3.2.1. *[10] Seja Λ um reticulado que admite uma base ortogonal ordenada $\beta = \{b_1, \ldots, b_n\}$, isto é, $||b_i|| \leq ||b_{i+1}||$ para $1 \leq i \leq n-1$, e $\alpha = \{e_1, \ldots, e_n\}$ uma base de Minkowski de Λ. Então $e_i = \pm b_i$, $\forall i = 1, \ldots, n$ a menos de uma possível reordenação entre os vetores de mesma norma em β.*

Corolário 3.2.1. *[10] Um reticulado é um $\mathbb{Z}^n$-rotacionado se, e somente se, sua base reduzida de Minkowski tem por matriz de Gram a identidade.*

Todo reticulado Λ pode ser descrito por diferentes bases, porém, algumas são melhores do que outras. Aquelas cujos elementos são os menores (para a correspondente norma associada a forma quadrática) são chamadas *reduzidas*.

Os algoritmos que encontramos (por exemplo, o contido no programa *Mathematica*) para a *redução de Minkowski* são aplicados à matriz geradora que tenha coordenadas inteiras, o que não ocorre em grande parte dos reticulados obtidos algebricamente. O algoritmo

computacional [41] que utilizamos foi desenvovido por J. Strapasson durante a nossa pesquisa e aplica-se diretamente à matriz de Gram, informando também qual a transformação linear correspodente à mudança de base envolvida.

A *redução de base LLL* (*Lenstra-Lenstra-Lovász*) vem sendo muito utilizada pois, embora não seja tão eficiente quanto a de Minkowski, tem complexidade computacional bem menor.

Os conceitos envolvendo redução de Minkowski e redução de base LLL podem ser encontradas em [13].

Exemplo 3.2.1. *Seja* $\alpha = \frac{1}{27}(1-\zeta_{3^3})(1-\zeta_{3^3}^{-1})^5$. *De modo análogo as duas contruções anteriores, obtemos a seguinte matriz de Gram*

$$G = \begin{pmatrix} 248 & -170 & 87 & -34 & 22 & -44 & 85 & -124 & 140 \\ -170 & 175 & -144 & 95 & -70 & 77 & -88 & 85 & -80 \\ 87 & -144 & 183 & -180 & 150 & -114 & 77 & -44 & 30 \\ -34 & 95 & -180 & 238 & -224 & 150 & -70 & 22 & -7 \\ 22 & -70 & 150 & -224 & 238 & -180 & 95 & -33 & 4 \\ -44 & 77 & -114 & 150 & -180 & 183 & -143 & 77 & -15 \\ 85 & -88 & 77 & -70 & 95 & -143 & 165 & -125 & 40 \\ -124 & 85 & -44 & 22 & -33 & 77 & -125 & 128 & -70 \\ 140 & -80 & 30 & -7 & 4 & -15 & 40 & -70 & 84 \end{pmatrix}.$$

Fazendo a redução da base pelo método de redução de Minkowski [41], e fazendo algumas operações com matrizes de determinante ± 1, *obtemos a seguinte matriz reduzida:*

$$G = \left(\begin{array}{c|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & -1 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 2 & 0 & -1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 2 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 & 0 & 2 & -1 & -1 \\ 0 & 0 & -1 & 0 & 1 & 0 & -1 & 2 & 0 \\ 0 & 1 & -1 & -1 & 0 & 0 & -1 & 0 & 2 \end{array}\right).$$

Permutando linhas e colunas na segunda submatriz, isto é, reordenando os vetores da base, temos:

$$G = \left(\begin{array}{c|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 2 \end{array}\right).$$

Embora $\det(\Lambda) = 1$, *pelo Corolário (3.2.1) concluímos que* $\Lambda \not\simeq \mathbb{Z}^9$.

A primeira parte do somando é $\mathbb{Z}$ *e a segunda, por [14], é a matriz de Gram do reticulado* E_8, *na base de Minkowiski.*

Assim, $\Lambda = (\mathcal{O}_K, b_\alpha) \simeq \mathbb{Z} \oplus E_8$.

Exemplo 3.2.2. *Seja* $\alpha = \dfrac{1}{25}(1 - \zeta_{5^2})(1 - \zeta_{5^2}^{-1})^3$. *De modo análogo ao exemplo anterior obtemos a seguinte matriz de Gram*

$$G = \begin{pmatrix} 21 & -14 & 8 & -6 & 6 & -5 & 2 & 2 & -5 & 6 \\ -14 & 19 & -16 & 8 & -3 & 2 & -1 & -1 & 2 & -2 \\ 8 & -16 & 19 & -13 & 4 & 1 & -1 & -1 & 2 & -2 \\ -6 & 8 & -13 & 15 & -9 & 1 & 1 & 2 & -5 & 6 \\ 6 & -3 & 4 & -9 & 12 & -9 & 4 & -3 & 6 & -8 \\ -5 & 2 & 1 & 1 & -9 & 15 & -13 & 8 & -6 & 6 \\ 2 & -1 & -1 & 1 & 4 & -13 & 19 & -16 & 8 & -3 \\ 2 & -1 & -1 & 2 & -3 & 8 & -16 & 19 & -13 & 4 \\ -5 & 2 & 2 & -5 & 6 & -6 & 8 & -13 & 15 & -9 \\ 6 & -2 & -2 & 6 & -8 & 6 & -3 & 4 & -9 & 12 \end{pmatrix}.$$

Novamente, fazendo a redução da base pelo método de Minkowski, e fazendo algumas operações com matrizes de determinante ± 1*, obtemos a seguinte matriz reduzida:*

$$G = \left(\begin{array}{cc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & 0 & -1 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & -1 & -1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 & -1 & 0 & 1 & 2 \end{array}\right).$$

Permutando linhas e colunas na segunda submatriz, isto é, reordenando os vetores da base, temos:

$$G = \left(\begin{array}{cc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{array}\right).$$

Embora $\det(\Lambda) = 1$, *pelo Corolário (3.2.1) concluímos que* $\Lambda \not\simeq \mathbb{Z}^{10}$.

A primeira parte do somando é um $\mathbb{Z}^2$ *e a segunda, por [14], é a matriz de Gram do reticulado* E_8.

Assim, $(\mathcal{O}_K, b_\alpha) \simeq \mathbb{Z}^2 \oplus E_8$.

Como os reticulados construídos possuem diversidade máxima, segue que o desempenho do reticulado é avaliado pela distância produto mínima.

A Tabela (3.1) compara alguns valores da $\sqrt[n]{d_{p,min}}$ para as construções que resultam em reticulados $\mathbb{Z}^n$ rotacionados, citadas anteriormente.

Nas construções, ciclotômica via $\mathbb{Q}(\zeta_p)$, cíclica e mista, para uma dada dimensão não é possível fazer estas três construções, ou seja, para cada dimensão existe uma (ou duas) apropriada. Além disso, quando é possível realizar duas construções não é possível comparar qual construção é melhor pois o valor da distância produto mínima do reticulado é o mesmo. Este fato não acontece com a construção ciclotômica via $\mathbb{Q}(\zeta_{2^r})$ e via $\mathbb{Q}(\zeta_{3^2})$.

Observando a Tabela (3.1) concluímos que as duas novas construções possuem $d_{p,min}$ menor do que as construções já existentes [7], mas a construção ciclotômica via $\mathbb{Q}(\zeta_{2^r})$ facilita o cálculo da $d_{p,min}$ em dimensões altas 2^{r-2} o que não é uma tarefa fácil de calcular para as outras construções, principalmente em determinadas dimensões 2^{r-2} onde é necessário combinar a construção ciclotômica via $Q(\zeta_p)$ e cíclica.

n	Ciclot. $\mathbb{Q}(\zeta_p)$	Cíclica	Mista	Ciclot. $\mathbb{Q}(\zeta_{2^r})$	Ciclot. $\mathbb{Q}(\zeta_{3^2})$
2	0.66874030	-	-	0.594604	-
3	0.52275795	0.52275795	-	-	0.48075
4	-	-	0.39763	0.385553	-
5	0.38321537	0.38321537	-	-	-
6	0.34344479	-	0.34958931	-	-
7	-	0.23618809	-	-	-
8	0.28952001	-	-	0.261068	-
9	0.27018738	-	-	-	-
10	-	-	0.25627156	-	-
11	0.24045444	0.24045444	-	-	-
12	-	-	0.22967537	-	-
13	-	0.16002224	-	-	-
14	0.20942547	-	-	-	-
15	0.20138689	-	0.20032888	-	-
16	-	-	0.19361370	0.180648	-
17	-	0.11292301	-	-	-
18	0.18174408	-	0.18174408	-	-
19	-	0.08308268	-	-	-
20	0.17136718	-	-	-	-
21	0.16678534	-	-	-	-
22	-	-	0.16080	-	-
23	0.15859921	0.15859921	-	-	-
24	-	-	0.15134889	-	-
25	-	-	0.10574672	-	-
26	0.14825905	-	-	-	-
27	-	-	0.14124260	-	-
28	-	-	0.14005125	-	-
29	0.13967089	0.13967089	-	-	-
30	0.13711677	-	0.13711677	-	-

Tabela 3.1: **Distância produto mínima.**

CAPÍTULO 4

Códigos de Grupo Comutativo e Reticulados

Neste Capítulo estudamos os códigos esféricos que são associados a reticulados. Iniciamos com uma motivação ao estudo de códigos esféricos para lidar com o problema de alocar pontos sobre a superfície de uma esfera no espaço $\mathbb{R}^{2m}$ com a maior distância euclidiana mínima. Introduzimos códigos de grupo comutativo, toros planares, representação de grupos, limitantes para códigos de grupo comutativos e aplicações da forma normal de Smith na caracterização do grupo. As principais referências utilizadas foram [18], [17] e [13].

4.1 Códigos esféricos

Constelações de sinais com mesma norma constituem-se nos códigos esféricos, introduzidos a seguir.

Um código esférico é um subconjunto finito da esfera unitária euclidiana S^n, contida em $\mathbb{R}^{n+1}$. A *distância mínima* de um código esférico n-dimensional $\mathcal{C} \subset S^n$ é definida como

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

onde $||x - y||$ é a distância euclidiana em $\mathbb{R}^{n+1}$ entre os pontos do código x e y. A distância mínima de um código esférico está diretamente relacionada à "qualidade" do código em muitas aplicações de codificação do canal.

Um dos principais fatores para que a transmissão de um sinal ocorra com baixa probabilidade de erro é que a distância euclidiana mínima entre os pontos seja grande. Por isso a análise de desempenho de uma constelação de sinais passa, em boa parte dos casos, pelo cálculo de sua distância mínima.

A *separação angular* entre dois pontos (que são vetores em $\mathbb{R}^n$) x, $y \in S^{n-1}$ é $\arccos \angle_{x,y}$. A *separação angular mínima* do código esférico $\mathcal{C}$ (Fig. 4.1) é definida como

$$\theta = 2 \operatorname{arcsen}\left(\frac{d}{2}\right). \tag{4.1}$$

O conjunto dos pontos sobre S^{n-1} cuja separação angular de um ponto fixo $x \in S^{n-1}$ é menor do que ϕ é chamado de *chapéu esférico* centrado em x com ângulo ϕ e é denotado por

$$\mathcal{C}_x(n, \phi) = \{y \in S^{n-1} : x.y > \cos\phi\}.$$

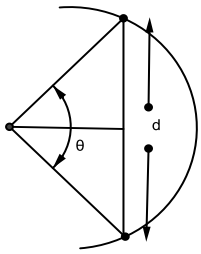


Figura 4.1: **Separação angular mínima** θ.

Em [39], Slepian estabeleceu de maneira geral os conceitos sobre códigos de grupo e códigos esféricos para o canal gaussiano. Neste trabalho, Slepian apresentou a construção

dos códigos de grupo para a alocação de pontos sobre a superfície de uma hiperesfera e os problemas da escolha do grupo e do vetor inicial. Desde então, vários pesquisadores vêm buscando aplicar esta teoria, de modo a conseguir alcançar o objetivo de alocação dos pontos sobre uma hiperesfera com a maior distância euclidiana mínima através da obtenção do grupo que é admitido no processo.

De maneira geral, dada a dimensão n e um número de pontos M queremos saber qual o código esférico $[M, n]$ com a maior distância mínima. Este código é chamado **ótimo**. Achar um código ótimo é um problema muito difícil. Na esfera euclidiana $S^2 \subset \mathbb{R}^3$, este problema é conhecido como o problema de Tammes. Configurações ótimas de pontos na esfera $S^2 \subset \mathbb{R}^3$ são conhecidas apenas para $M \leq 12$ e $M = 24$, segundo [23]. Todas as outras são as "melhores conhecidas", sem um prova formal de que são ótimas.

Dentre os esforços para resolver este problema estão:

- A construção de limitantes para o número de pontos $M = M(n, d)$ de um código esférico que envolva a dimensão n e a distância mínima d.
- A construção de códigos que tenham distâncias mínimas melhores que as conhecidas para uma determinada dimensão e quantidade de pontos.
- A determinação do vetor inicial, da esfera unitária do $\mathbb{R}^n$ que, para um determinado grupo gerador, maximiza a distância mínima entre dois pontos quaisquer do código.

Para códigos de grupo comutativo e grande número de pontos a busca pelo vetor inicial ótimo usando programação linear, torna-se um problema computacional de alta complexidade, e isto motivou-nos a utilizar ferramentas que viabilizassem um procedimento da procura de códigos muito bons em casos especiais.

Os códigos de grupo comutativo em dimensão par, $2m$, podem ser vistos sobre toros de curvatura gaussiana nula, os toros planares ([18], [17]). Tal caracterização permitiu a construção de limitantes para a cardinalidade de um código de grupo comutativo em termos de sua distância mínima, de seu vetor inicial e da máxima densidade de empacotamento de esferas em $\mathbb{R}^m$, onde m é a dimensão do toro [18].

A partir de agora, todas as constelações estudadas serão esféricas, ou seja, todos os pontos terão energia igual e constante. Na comparação de constelações de sinais, vamos supor que

todos os pontos têm energia igual a um, ou seja, as constelações estão sobre a esfera unitária.

4.2 Códigos de grupo comutativo

Nesta seção definimos códigos de grupo com foco nos códigos de grupo comutativo, pois códigos esféricos gerados por grupos comutativos de matrizes ortogonais podem ser determinados pelo quociente de dois reticulados, quando o sub-reticulado é "retangular" ([17], [18]). Além disso, apresentamos aplicações da forma normal de Smith na caracterização do grupo gerador.

Como as matrizes ortogonais determinam isometrias do espaço euclidiano, estes códigos são geometricamente uniformes, como definido no Capítulo 2. Assim, possuem as regiões de decisão isométricas e uma distribuição de pontos homogênea, o que facilita na hora das análises de desempenho e decodificação.

Vamos analisar uma classe de códigos de grupo para o canal gaussiano, gerada a partir de grupos comutativos de matrizes ortogonais. Tais códigos, podem ser descritos de maneira muito parecida com a dos códigos algébricos lineares. Nosso estudo pressupõe o modelo vetorial do canal gaussiano branco (AWGN), conforme descrito no Capítulo 1.

Definição 4.2.1. *Seja $x_0 \in \mathbb{R}^n$ e G um grupo de matrizes $n \times n$. Chamamos de* **órbita** *de x_0 por G ao conjunto*

$$G(x_0) = \{g(x_0);\, g \in G\}.$$

Definição 4.2.2. *Um* **código de grupo** $\mathcal{C}$ *é a órbita de um vetor v na esfera unitária S^{n-1} por um subgrupo $G = \{O_i\}_{i=1}^{M}$ do grupo das matrizes ortogonais $n \times n$, $\mathbf{O}(n)$, tal que o código $\mathcal{C} = \{O_i v\}_{i=1}^{M}$ é substancial em $\mathbb{R}^n$ (não está contido em um hiperespaço, isto é, subespaço vetorial de codimensão 1).*

Quando o subgrupo de $\mathbf{O}(n)$ for comutativo, teremos um **código de grupo comutativo**.

Uma consequência imediata desta definição é que um código de grupo é geometricamente uniforme, isto é, existe sempre uma isometria que leva uma palavra em uma outra da constelação. Portanto, todas as regiões de decisão são isométricas, o conjunto das distâncias de

uma palavra a todas as outras e o número de seus vizinhos é invariante em toda a constelação. Assim, a probabilidade de erro de todas as palavras é a mesma.

Uma forma canônica para o grupo G pode ser obtida do seguinte teorema:

Teorema 4.2.1. *[27] Um grupo comutativo $G = \{O_i\}_{i=1}^{M}$ de $n \times n$ matrizes ortogonais reais pode ser levado por uma transformação ortogonal Q em matrizes de blocos diagonais da forma*

$$\tilde{O}_i = \left[R\left(\frac{2\pi k_{i1}}{M}\right), \cdots, R\left(\frac{2\pi k_{im}}{M}\right), \mu_{2m+1}(i), \cdots \mu_n(i) \right]_{n\times n} = Q^t O_i Q, \tag{4.2}$$

onde k_{ij} são inteiros, os blocos $R(a)$ são rotações em dimensão 2,

$$R(a) = \begin{pmatrix} \cos(a) & -\operatorname{sen}(a) \\ \operatorname{sen}(a) & \cos(a) \end{pmatrix},$$

e $\mu_l(i) = \pm 1$, $l = 2m+1, \cdots, n$.

Estamos interessados em estabelecer uma conexão entre códigos de grupo e reticulados. Para caracterizar um código de grupo comutativo como o quociente de reticulados é necessário determinar o conjunto de geradores e a classificação do grupo correspondente. Estes serão importantes para determinarmos as configurações dos pontos no código esférico. Os grupos cíclicos tem uma estrutura algébrica mais simples, pois possuem uma única matriz geradora.

No que segue, mostraremos como resolver este problema.

Definição 4.2.3. *Um conjunto gerador de um grupo G é um subconjunto S de G tal que todos os elementos de G se escrevem como produto de elementos de S e dos seus inversos.*

Como todo reticulado é um $\mathbb{Z}$-módulo livre, o teorema dos divisores elementares será útil no que se segue para determinar a estrutura do grupo G.

Teorema 4.2.2. *(Teorema dos Divisores Elementares, [13]). Seja L um $\mathbb{Z}$-submódulo de um módulo livre L' e de mesmo posto. Então existem inteiros positivos $d_1, \cdots, d_n$ (chamados de divisores elementares de L em L') satisfazendo as seguintes condições:*

1. *Para todo i tal que $1 \leq i < n$ temos d_i divide d_{i+1}, isto é, $d_i | d_{i+1}$.*

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_n é o expoente de L'/L.

3. Existe uma $\mathbb{Z}$-base $(w_1, \cdots, w_n)$ de L' tal que $(d_1w_1, \cdots, d_nw_n)$ é uma $\mathbb{Z}$-base de L.

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

Podemos determinar a estrutura do grupo G de modo matricial e para isto usamos a seguinte definição:

Definição 4.2.4. *Dizemos que uma matriz B de ordem $n \times n$ está na* **forma normal de Smith** *se B é uma matriz diagonal com coeficientes inteiros não negativos tal que $b_{i,i}|b_{i+1,i+1}$ para todo $i < n$.*

O teorema a seguir explica o uso desta definição.

Teorema 4.2.3. *[13] Se A é uma matriz $n \times n$, com coeficientes em um domínio de ideais principais R e determinante não nulo, então existe uma única matriz D na forma normal de Smith tal que $D = PAQ$, com P e Q matrizes unimodulares em R.*

Neste trabalho consideraremos $R = \mathbb{Z}$.

Como ilustração encontramos D para matrizes 2×2. Considere

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}, \quad \det A \neq 0.$$

Seja $d = mdc(a, b)$, então pela identidade de Bezout, $\exists\, x,\, y \in \mathbb{Z}$ tal que $d = ax + by$. Temos que

$$d|a \Longrightarrow \exists\, \alpha \in \mathbb{Z} \mid a = \alpha d$$

$$d|b \Longrightarrow \exists\, \beta \in \mathbb{Z} \mid b = \beta d$$

Logo, $d = \alpha dx + \beta dy \Longrightarrow 1 = \alpha x + \beta y$. Então, a matriz $\begin{bmatrix} x & y \\ -\beta & \alpha \end{bmatrix}$ tem determinante igual a 1. Isto garante que ela é invertível.

Além disso,

$$\begin{bmatrix} x & y \\ -\beta & \alpha \end{bmatrix} . \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} d & cx+dy \\ -a\beta+b\alpha & -c\beta+\alpha d \end{bmatrix} .$$

Como d divide $-a\beta + b\alpha$, uma operação por linha reduz esta matriz a uma da forma

$$\begin{bmatrix} d & u \\ 0 & v \end{bmatrix} .$$

Um argumento similar, aplicado à primeira linha ao invés da primeira coluna, permite-nos multiplicar a direita por uma matriz invertível e obter uma matriz da forma

$$\begin{bmatrix} d_1 & 0 \\ \star & \star \end{bmatrix},$$

onde $d_1 = mdc(d, u)$.

Continuando este processo, alternando entre a primeira linha e primeira coluna, produziremos uma sequência de elementos d, $d_1, \cdots$ tal que $d_1|d$, $d_2|d_1, \cdots, d_{i+1}|d_i, \cdots$.

Considerando (a) o ideal gerado por a, onde $a \in \mathbb{Z}$, temos que

$$(d) \subseteq (d_1) \subseteq (d_2) \subseteq \cdots$$

Como qualquer sequência crescente de ideais principais é estacionária [36], devemos ter em um número finito de passos, a redução a uma matriz da forma

$$\begin{bmatrix} f & 0 \\ g & h \end{bmatrix} \quad ou \quad \begin{bmatrix} f & g \\ 0 & h \end{bmatrix}$$

onde f divide g.

Com mais uma operação de linha ou coluna, chegaremos em uma matriz da forma

$$\begin{bmatrix} f & 0 \\ 0 & k \end{bmatrix} .$$

Para obter a forma normal de Smith, seja $e = mdc(f, k)$. Pela identidade de Bezout, $\exists\, x, y \in \mathbb{Z}$ tal que $e = fx + ky$. Temos

$$e|f \Longrightarrow \exists\, \alpha \in \mathbb{Z} \mid f = \alpha e$$

$$e|k \Longrightarrow \exists\, \beta \in \mathbb{Z} \mid k = \beta e$$

Fazendo as seguintes operações de linha e coluna,

$$\begin{bmatrix} f & 0 \\ 0 & k \end{bmatrix} \longrightarrow \begin{bmatrix} f & 0 \\ fx & k \end{bmatrix} \longrightarrow \begin{bmatrix} f & 0 \\ fx+ky & k \end{bmatrix} = \begin{bmatrix} f & 0 \\ e & k \end{bmatrix} = \begin{bmatrix} \alpha e & 0 \\ e & k \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 0 & -k\alpha \\ e & k \end{bmatrix} = \begin{bmatrix} 0 & -k\alpha \\ e & \beta e \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & -k\alpha \\ e & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} e & 0 \\ 0 & -k\alpha \end{bmatrix},$$

obtemos uma matriz diagonal na forma normal de Smith pois $e|(-k\alpha)$. ◪

No caso geral, se $d_i = b_{i,i}$ indicar o i-ésimo elemento da diagonal na forma normal de Smith, o Teorema (4.2.3) pode ser escrito

$$A = P^{-1}.\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & d_n \end{pmatrix}.Q^{-1}$$

com $d_i|d_{i+1}$ para $1 \leq i < n$.

A forma normal de Smith pode ser reinterpretada no contexto de reticulados, que é o que utilizaremos no próximo capítulo.

Considere α e β duas bases de $\mathbb{R}^m$, Λ_α um sub-reticulado de Λ_β, Λ_α e Λ_β gerados por α e β, respectivamente, e $A = (a_{ij})$, $a_{ij} \in \mathbb{Z}$ a matriz da base α escrita em relação à base β por colunas. Assim, de acordo com a Definição (2.1.6), escrevendo na forma coluna temos que

$$\Lambda_\alpha = \{\mathbf{x^t} = M_\beta^t A \lambda^t | \lambda^t \in \mathbb{Z}^m\},$$

onde M_β é a matriz geradora de Λ_β.

Estamos interessados em determinar o número de pontos M e o grupo obtido pelo quociente $\dfrac{\Lambda_\beta}{\Lambda_\alpha}$. Do Capítulo 2,

$$\left|\frac{\Lambda_\beta}{\Lambda_\alpha}\right| = \frac{vol(\Lambda_\alpha)}{vol(\Lambda_\beta)} = |det(A)|.$$

Logo, o número de pontos M é dado pelo módulo do determinante da matriz A. Determinamos o grupo e o conjunto de geradores do quociente $\frac{\Lambda_\beta}{\Lambda_\alpha}$ através do seguinte teorema:

Teorema 4.2.4. *Sejam $\alpha = \{v_1, \cdots, v_m\}$ e $\beta = \{w_1, \cdots, w_m\}$ duas bases de $\mathbb{R}^m$, Λ_α e Λ_β os reticulados gerados por α e β, respectivamente, e $\Lambda_\alpha \subset \Lambda_\beta$. Se $A = (a_{ij})$, $a_{i,j} \in \mathbb{Z}$ é a matriz da base α escrita em relação à base β, então a classificação e o conjunto de geradores do grupo $\Lambda_\beta/\Lambda_\alpha$ são obtidos da forma normal de Smith de A.*

Demonstração: Como todo reticulado é um $\mathbb{Z}$-módulo livre, as condições do Teorema (4.2.2) são válidas para reticulados. Para garantir a existência de inteiros positivos $d_1, \cdots, d_m$ que satisfaçam tais condições, basta aplicarmos o Teorema (4.2.3) na matriz A. Deste modo, $D = PAQ$ está na forma normal de Smith, isto é, D é uma matriz diagonal com coeficientes inteiros não nulos tal que $d_i | d_{i+1}$.

Seja $\varphi : \mathbb{Z}^m \longrightarrow \Lambda_\beta/\Lambda_\alpha$ o homomorfismo sobrejetivo que envia $(z_1, \cdots, z_m)$ a $\sum_{i=1}^{m} z_i w_i + \Lambda_\alpha$, então $\Lambda_\beta/\Lambda_\alpha \simeq \mathbb{Z}^m/ker\varphi$ (isomorfismo de grupos).

Seja $\tilde{\beta} = \{\tilde{w}_1, \cdots, \tilde{w}_m\}$ uma base de Λ_β dada pela Proposição (4.2.2) item 3, tal que $\{d_1\tilde{w}_1, \cdots, d_m\tilde{w}_m\}$ é base de Λ_α. Considere o homomorfismo sobrejetivo $\gamma : \mathbb{Z}^n \longrightarrow \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$ dado por $\gamma(z_1, \cdots, z_m) = (\tilde{z}_1 + d_1\mathbb{Z}, \cdots, \tilde{z}_m + d_m\mathbb{Z})$, onde $\sum_{i=1}^{m} z_i w_i = \sum_{i=1}^{m} \tilde{z}_i \tilde{w}_i$. Temos que, $ker\varphi$ é também o núcleo do homomorfismo sobrejetivo γ e então, $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$ é também isomorfo a $\mathbb{Z}^m/Ker\varphi$. Portanto, $\Lambda_\beta/\Lambda_\alpha \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$.

Sendo Q unimodular, quando operada à direita da matriz A, ela define uma mudança de base no reticulado Λ_α. Deste modo, $AQ = P^{-1}D$ é também geradora de Λ_α. Como $\Lambda_\beta/\Lambda_\alpha \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$, as colunas de P^{-1} determinam um conjunto de vetores $\{\tilde{p}_i\}$, $i = 1, \cdots, m$ que representam as coordenadas dos geradores de $\Lambda_\beta/\Lambda_\alpha$ de ordem d_i, na base β. Isto pode ser detalhado da seguinte forma:

Como A é a matriz da base α escrita em relação à base β por colunas, isto é,

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix} = \begin{bmatrix} w_1 & w_2 & \cdots & w_m \end{bmatrix} . A$$

Segue então que

$$\begin{aligned}
\begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix}.Q &= \begin{bmatrix} w_1 & w_2 & \cdots & w_m \end{bmatrix}.AQ \\
\begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix}Q &= \begin{bmatrix} w_1 & w_2 & \cdots & w_m \end{bmatrix}.P^{-1}D \\
\begin{bmatrix} \tilde{v}_1 & \tilde{v}_2 & \cdots & \tilde{v}_m \end{bmatrix} &= \begin{bmatrix} w_1 & w_2 & \cdots & w_m \end{bmatrix}.\begin{bmatrix} \tilde{p}_{11} & \tilde{p}_{12} & \cdots & \tilde{p}_{1m} \\ \tilde{p}_{21} & \tilde{p}_{22} & \cdots & \tilde{p}_{2m} \\ \vdots & & \vdots & \\ \tilde{p}_{m1} & \tilde{p}_{m2} & \cdots & \tilde{p}_{mm} \end{bmatrix}.D \\
&= [\ \tilde{p}_{11}w_1 + \cdots + \tilde{p}_{m1}w_m \quad \cdots \quad \tilde{p}_{1m}w_1 + \cdots + \tilde{p}_{mm}w_m\ ].D \\
&= \begin{bmatrix} h_1 & \cdots & h_m \end{bmatrix}.D
\end{aligned}$$

Assim, $d_i h_i = \tilde{v}_i \in \Lambda_\alpha$ e então, $\overline{d_i h_i} = \overline{0}$, ou seja, h_i é elemento de ordem d_i e os geradores do grupo $\dfrac{\Lambda_\beta}{\Lambda_\alpha}$ são os $\overline{h_i'}s$, $i = 1, \cdots, m$ tais que $d_i \neq 1$. ◪

Outro resultado que permite calcular a ordem de um elemento no grupo gerado pelo quociente de reticulados é dado a seguir.

Proposição 4.2.1. *[17] Sejam α e β duas bases de $\mathbb{R}^m$, Λ_α e Λ_β os reticulados gerados por α e β, respectivamente, e suponha que $\Lambda_\alpha \subset \Lambda_\beta$. Seja A a matriz da base α escrita em relação à base β por colunas, v um vetor de Λ_β, e A_i a matriz obtida de A substituindo v^t pela i-ésima coluna de A. Então a ordem de $\overline{v} = v + \Lambda_\alpha$ em $\Lambda_\beta/\Lambda_\alpha$ é dada por $|A|/mdc\{|A_1|, \cdots, |A_m|\}$, onde $|A| = |\det A|$.*

4.3 Toros planares

Nesta seção introduzimos os toros planares e descrevemos como estes "intermediam" a construção de códigos esféricos. As referências para esta seção são: [17] e [18].

O *toro planar* $T_{(\delta_1,\cdots,\delta_m)}$ pode ser identificado como o seguinte subconjunto da esfera S^{2m-1} :

$$T_\delta = T_{(\delta_1,\cdots,\delta_m)} = \{(x_1, x_2, \cdots, x_{2m}) \in \mathbb{R}^{2m};\ \delta_i^2 = x_{2i-1}^2 + x_{2i}^2 \ e\ \sum_{i=1}^{m} \delta_i^2 = R^2\}.$$

A cada $\delta = (\delta_1, \cdots, \delta_m) \in S^{m-1}$, $\delta_i \geq 0$, $i = 1, \cdots, m$, associamos um toro ou sua

degeneração de maneira que $\bigcup_{\delta\in S^{m-1},\,\delta_i\geq 0} T_\delta = S^{2m-1}$, ou seja, a esfera em $\mathbb{R}^{2m}$ é "folheada" por toros.

Seja

$$\begin{aligned}\psi \;:\; & \mathbb{R}^m \longrightarrow \mathbb{R}^{2m} \\ & y \longmapsto \psi(y) = \left(\delta_1\cos(\frac{y_1}{\delta_1}), \delta_1\,\mathrm{sen}(\frac{y_1}{\delta_1}), \cdots, \delta_m\cos(\frac{y_m}{\delta_m}), \delta_m\,\mathrm{sen}(\frac{y_m}{\delta_m})\right), \qquad (4.3)\end{aligned}$$

onde $y = (y_1, \cdots, y_m)$ são coordenadas em relação a uma base ortogonal.

A aplicação ψ é claramente diferenciável, tem imagem igual ao toro T_δ e

$$\frac{\partial\psi}{\partial y_i} = d\psi_y(e_i) = -sin\left(\frac{y_i}{\delta_i}\right)e_{2i-1} + cos\left(\frac{y_i}{\delta_i}\right)e_{2i}$$

satisfaz $< d\psi_y(e_i), d\psi_y(e_j) >= \left\langle \frac{\partial\psi}{\partial y_i}, \frac{\partial\psi}{\partial y_j}\right\rangle =< e_i, e_j >= \begin{cases} 1, \, se\, i = j \\ 0, \, se\, i \neq j \end{cases}$. Portanto ψ é uma isometria local entre $\mathbb{R}^m$ e a imagem $T_\delta = \psi(\mathbb{R}^m) \subset \mathbb{R}^{2m}$. Como a curvatura gaussiana em $\mathbb{R}^m$ é nula, segue que os toros T_δ tem curvatura gaussiana nula, neste sentido, ele pode ser localmente "planificado" em $\mathbb{R}^m$. Assim em uma região local onde ψ é injetiva, ângulos, comprimentos, áreas e qualquer volume k- dimensional $k \leq m$, serão então preservados e o volume m-dimensional de T_δ é o volume da hipercaixa: $(2\pi)^m \prod_{i=1}^{m} \delta_i$.

Geometricamente, o toro planar T_δ pode ser caracterizado como o quociente de $\mathbb{R}^m$ pelo grupo de translações gerados por m vetores mutuamente ortogonais. Conjuntos de sinais que são imagens no toro planar n-dimensional gerados, por exemplo, por algum reticulado m-dimensional definirão códigos esféricos $2m$-dimensionais.

A parametrização ψ induz uma relação de equivalência em $\mathbb{R}^m$ cujas classes formam um conjunto chamado toro planar abstrato.

Um conjunto de representantes para essa relação é o paralelepípedo $\prod_{i=1}^{m}[0, 2\pi\delta_i)$. Este conjunto de representantes pode ser visto como um espaço quociente onde os lados paralelos do paralelepípedo são identificados.

O espaço quociente é definido do seguinte modo: seja Λ o reticulado gerado pelos vetores $v_i = 2\pi\delta_i e_i$, onde $\{e_i\}$ é a base canônica do $\mathbb{R}^m$, $\alpha = \{v_1, \cdots, v_m\}$. Dizemos que $x = (x_1, \cdots, x_m)$ e $y = (y_1, \cdots, y_m)$ são equivalentes se $x_i = y_i \mod 2\pi\delta_i$, ou seja, $x - y \in \Lambda$. Neste caso, escrevemos $x = y \mod \Lambda$ e denotamos o espaço quociente por $\frac{\mathbb{R}^m}{\Lambda}$.

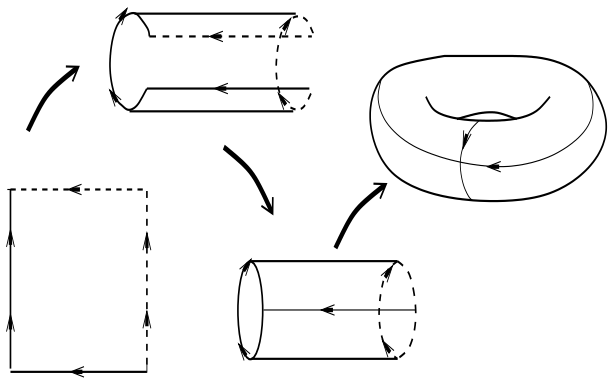


Figura 4.2: **A construção do toro planar**

Dada uma base ortogonal qualquer $\alpha = \{v_1, \cdots, v_m\}$, um toro planar $T_\alpha = T_\delta$, $\delta = (\delta_1, \cdots, \delta_m)$, $\delta_i = \dfrac{||v_i||}{2\pi}$ pode ser também definido pela aplicação

$$\begin{aligned} \mu_\delta \quad : \quad & \mathbb{R}^m \longrightarrow \mathbb{R}^m \\ & x \longmapsto \mu_\delta(x) = x \mod \Lambda = x - \sum_{i=1}^{m} \lfloor x_i \rfloor \, v_i \end{aligned} \tag{4.4}$$

onde $x = \sum_{i=1}^{m} x_i v_i$ e $\lfloor x_i \rfloor$ denota a parte inteira de x_i, isto é, o maior inteiro que é menor do que ou igual a x_i. Se $e_i = \dfrac{v_i}{||v_i||}$ a relação de equivalência de μ_δ e ψ é a mesma.

Como a imagem de ψ é T_δ e ψ está bem definida no quociente $\dfrac{\mathbb{R}^m}{\Lambda}$, ou seja, $\psi(x) = \psi(y)$ se, e somente se, $x = y \mod \Lambda$, o quociente $\dfrac{\mathbb{R}^m}{\Lambda}$ é identificado com o domínio da aplicação ψ e, por conseguinte, $\dfrac{\mathbb{R}^m}{\Lambda}$ com T_δ.

O toro também pode ser visto como um produto de círculos de raio $\delta_i = \dfrac{||v_i||}{2\pi}$ e um ponto sobre ele pode ser obtido a partir de qualquer outro através de um produto direto de rotações.

Como a área do toro é proporcional ao produto dos raios dos círculos, dentre todos os toros contidos em S^{2m-1} o de área máxima é dado por $\delta = (\delta_1, \delta_1, \cdots, \delta_1)$, ou seja, $T_\delta = S^1_{\delta_1} \times \cdots \times S^1_{\delta_1}$ (produto de m círculos de igual raio) [38].

4.3.1 Expressões para as distâncias na imagem por ψ.

Ao considerarmos a construção de códigos esféricos em $\mathbb{R}^{2m}$ partindo de sinais em $\mathbb{R}^m$ e usando a aplicação ψ, um ponto crucial é saber como a distância $d(p,q)$ em $\mathbb{R}^m$ será deformada para a distância $d(\psi(p),\psi(q))$ em $\mathbb{R}^{2m}$. Assim, considerando um toro T_δ na esfera unitária contida em $\mathbb{R}^{2m}$ e a aplicação (4.3) com $\delta_i = \dfrac{||v_i||}{2\pi}$ temos

$$\psi(y) = \left(\frac{||v_1||}{2\pi}\cos\left(\frac{2\pi y_1}{||v_1||}\right), \frac{||v_1||}{2\pi}\operatorname{sen}\left(\frac{2\pi y_1}{||v_1||}\right), \cdots, \frac{||v_m||}{2\pi}\cos\left(\frac{2\pi y_m}{||v_m||}\right), \frac{||v_m||}{2\pi}\operatorname{sen}\left(\frac{2\pi y_m}{||v_m||}\right)\right) \tag{4.5}$$

onde $\displaystyle\sum_{i=1}^{m}\left(\frac{v_i}{2\pi}\right)^2 = 1$, e $x = (x_1,\cdots,x_m)$ e $y = (y_1,\cdots,y_m)$ são palavras de um código. Assim definimos a distância euclidiana ao quadrado entre $\psi(x)$ e $\psi(y)$ na esfera de $\mathbb{R}^{2m}$ por

$$\begin{aligned} d^2(\psi(x),\psi(y)) &= ||\psi(x)-\psi(y)||^2 = 4\sum_{i=1}^{m}\left(\frac{||v_i||}{||v_1||+\cdots||v_m||}\right)^2 \operatorname{sen}^2\left(\frac{\pi(x_i-y_i)}{||v_i||}\right) = \\ &= 4\sum_{i=1}^{m}\delta_i^2\operatorname{sen}^2\left(\frac{x_i-y_i}{2\delta_i}\right). \end{aligned} \tag{4.6}$$

Um caso particular que utilizaremos no caso de grupos comutativos é $y = \mathbf{0} = (0,\cdots,0)$, pois sendo estes geometricamente uniformes, o perfil de distâncias a um ponto é igual para todos os pontos e podemos escolher $\psi(\mathbf{0})$ para estes cálculos.

$$\begin{aligned} d^2(\psi(x),\psi(\mathbf{0})) &= ||\psi(x)-\psi(\mathbf{0})||^2 = 4\sum_{i=1}^{m}\left(\frac{||v_i||}{||v_1||+\cdots||v_m||}\right)^2 \operatorname{sen}^2\left(\frac{\pi x_i}{||v_i||}\right) \\ &= 4\sum_{i=1}^{m}\delta_i^2\operatorname{sen}^2\left(\frac{x_i}{2\delta_i}\right) \overset{(4.1)}{=} 4\sum_{i=1}^{m}\delta_i^2\operatorname{sen}^2\left(\frac{\theta_i}{2}\right). \end{aligned} \tag{4.7}$$

4.3.2 Deformação das distâncias por ψ.

O desenvolvimento a seguir visa deduzir como as distâncias de pontos em $\mathbb{R}^m$ são afetadas pelo mergulho ψ do toro.

Dado $y \in \mathbb{R}^m$, tal que $||y|| = r$, ou seja, $d(y,\mathbf{0}) = r$, que estimativa temos para $d(\psi(y),\psi(\mathbf{0}))$?

A proposição a seguir estabelece limitantes para a deformação de distâncias feitas pela transformação ψ que descreve o toro planar. Este resultado será muito importante na dedução de que poderemos reduzir a um conjunto pequeno de pontos a busca pela distância mínima de um código de grupo. A demonstração que apresentamos é inspirada em desenvolvimentos feitos em [18] e [38].

Proposição 4.3.1. *Seja ψ definida em (4.3), $y \in \mathbb{R}^m$, tal que $||y|| = r \leq 2\pi\delta_{min}$ onde $\delta_{min} = \min\{\delta_i;\ i = 1, \cdots, m\}$ então*

$$4\delta_{min}^2 \operatorname{sen}^2\left(\frac{r}{2\delta_{min}}\right) \leq d^2(\psi(y), \psi(\mathbf{0})) \leq 4(\delta_1^2 + \cdots + \delta_m^2)\operatorname{sen}^2\left(\frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}}\right) \leq r^2.$$

Demonstração: Seja $D(y) = d^2(\psi(y), \psi(\mathbf{0})) = ||\psi(y) - \psi(\mathbf{0})||^2 = 4\sum_{i=1}^{m} \delta_i^2 \operatorname{sen}^2(\frac{y_i}{2\delta_i})$ e $S_r = \{y \in \mathbb{R}^m; d^2(y, \mathbf{0}) = r^2\}$, onde $d^2(y, \mathbf{0}) = \sum_{i=1}^{m} y_i^2$. 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 de máximo e mínimo absolutos devem satisfazer o sistema de equações

$$\begin{cases} \nabla D(y) = 2\lambda y \\ y_1^2 + \cdots + y_m^2 = r^2 \end{cases}$$

Como $\dfrac{\partial D}{\partial y_i}(y) = 4\delta_i \operatorname{sen}\left(\dfrac{y_i}{2\delta_i}\right)\cos\left(\dfrac{y_i}{2\delta_i}\right) = 2\delta_i \operatorname{sen}\left(\dfrac{y_i}{\delta_i}\right)$, o sistema fica

$$\lambda y_i = \delta_i \operatorname{sen}\left(\frac{y_i}{\delta_i}\right) \ \ e \ \ \sum_{i=1}^{m} y_i^2 = r^2.$$

Assim, se I é o conjunto de índices i tais que $y_i \neq 0$, segue que os quocientes

$$\frac{\operatorname{sen}\left(\dfrac{y_i}{\delta_i}\right)}{\dfrac{y_i}{\delta_i}}, \quad -\pi \leq \frac{y_i}{\delta_i} \leq \pi,\ i \in I$$

são todos iguais. Seja $h(x) = \dfrac{\operatorname{sen} x}{x}$. Então, $h'(x) = \dfrac{x\cos x - \operatorname{sen} x}{x^2}$.

Afirmação: $p(x) = x\cos x - \operatorname{sen} x$ é decrescente em $[0, \pi]$.

De fato, $p'(x) = -x \operatorname{sen} x \leq 0$, $\forall\, x \in [0, \pi]$.

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 em $(0, \pi]$, portanto injetora em $(0, \pi]$, então $\dfrac{y_i}{\delta_i} = \dfrac{y_l}{\delta_l}$ 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 $y_1^2 + \cdots + y_m^2 = r^2$.

1-) Se $y_i \neq 0$ e $y_j = 0$, $\forall j \neq i$, e $i, j = 1, \cdots, m$ então $y_i^2 = r^2$ implica $y_i = \pm r$. Logo, $y = (0, \cdots, 0, \pm r, 0, \cdots, 0)$.

2-) Se $y_i, y_j \neq 0$ e $y_k = 0$, $\forall\, k \neq i, j$ e $i, j, k = 1, \cdots, m$ então $y_i^2 + y_j^2 = r^2$. Como para

$\forall\, i,\ j = 1, \cdots, m$ temos $\dfrac{y_i}{\delta_i} = \dfrac{y_j}{\delta_j}$, segue que $y_i = \dfrac{y_j \delta_i}{\delta_j}$. Logo, $\dfrac{y_j^2 \delta_i^2}{\delta_j^2} + y_j^2 = r^2 \Rightarrow$ $y_j^2 \left(\dfrac{\delta_i^2}{\delta_j^2} + 1 \right) = r^2 \overset{\delta_j^2}{\Rightarrow} y_j^2(\delta_i^2 + \delta_j^2) = r^2 \delta_j^2 \Rightarrow y_j^2 = \dfrac{r^2 \delta_j^2}{\delta_i^2 + \delta_j^2} \Rightarrow y_j = \pm \dfrac{r\delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}$. Assim, $y_i = \dfrac{\pm \dfrac{r\delta_j}{\sqrt{\delta_i^2 + \delta_j^2}} \delta_i}{\delta_j} = \pm \dfrac{r\delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}$. Logo, $y = \left(0, \cdots, 0, \pm \dfrac{r\delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \cdots, 0, \pm \dfrac{r\delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \cdots, 0 \right)$.

m-) Seguindo desta forma, para $y_i \neq 0$, $\forall\, i = 1, \cdots, m$ temos que

$$y = \left(\pm \frac{r\delta_1}{\sqrt{\delta_1^2 + \cdots + \delta_m^2}}, \pm \frac{r\delta_2}{\sqrt{\delta_1^2 + \cdots + \delta_m^2}}, \cdots, \pm \frac{r\delta_m}{\sqrt{\delta_1^2 + \cdots + \delta_m^2}} \right).$$

Concluímos então que os pontos críticos serão da forma:

$$\begin{aligned}
&C_m^1 \quad \text{pontos} \quad y = (0, \cdots, 0, \quad r, 0, \cdots, 0) \\
&C_m^2 \quad \text{pontos} \quad y = \left(0, \cdots, 0, \pm \frac{r\delta_i}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \cdots, 0, \pm \frac{r\delta_j}{\sqrt{\delta_i^2 + \delta_j^2}}, 0, \cdots, 0 \right) \\
&\vdots \\
&C_m^m \quad \text{pontos} \quad y = \frac{r(\pm\delta_1, \pm\delta_2, \cdots, \pm\delta_m)}{\sqrt{\delta_1^2 + \cdots + \delta_m^2}}
\end{aligned}$$

Agora, vamos analisar o máximo e o mínimo da função D restrita a $y_1^2 + \cdots + y_m^2 = r^2$.

Sem perda de generalidade, assumimos δ_i de forma ordenada: $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_m$.

• Para os pontos críticos da forma (1) temos

$$D(y) = d^2(\psi(y), \psi(\mathbf{0})) = 4\delta_i^2 \operatorname{sen}^2\left(\frac{r}{2\delta_i}\right) = r^2 \left(\frac{\operatorname{sen}\left(\frac{r}{2\delta_i}\right)}{\frac{r}{2\delta_i}}\right)^2 .$$

Seja $f(x) = r^2 \left(\dfrac{\operatorname{sen}\left(\frac{r}{2x}\right)}{\frac{r}{2x}}\right)^2$ e $g(z) = \left(\dfrac{\operatorname{sen} z}{z}\right)^2$. Observamos que $f(x) = r^2 g\left(\dfrac{r}{2x}\right)$. Assim,

$$f'(x) = r^2 g'\left(\frac{r}{2x}\right)\left(\frac{-2r}{4x^2}\right) = -\frac{r^3}{2x^2} g'\left(\frac{r}{2x}\right). \tag{4.8}$$

Seja $h(z) = \dfrac{\operatorname{sen} z}{z}$. 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 $\dfrac{r}{2x} \in (0, \pi]$ então $g'\left(\dfrac{r}{2x}\right) < 0$. Logo, de (4.8), temos que $f'(x) > 0$ se $\dfrac{r}{2x} \in (0, \pi]$, ou seja, $f(x)$ é crescente se $\dfrac{r}{2x} \in (0, \pi]$.

Como $\delta_i \geq \delta_m$, $\forall i = 1, \cdots, m$, segue que

$$f(\delta_i) = 4\delta_i^2 \operatorname{sen}^2\left(\frac{r}{2\delta_i}\right) \geq 4\delta_m^2 \operatorname{sen}^2\left(\frac{r}{2\delta_m}\right) = f(\delta_m),\ \frac{r}{2\delta_i} \in (0, \pi].$$

• Para os pontos críticos da forma (2), temos

$$\begin{aligned} D(y) &= d^2(\psi(y), \psi(\mathbf{0})) = 4\left(\delta_i^2 \operatorname{sen}^2\left(\frac{\frac{r\delta_i}{\sqrt{\delta_i^2+\delta_j^2}}}{2\delta_i}\right) + \delta_j^2 \operatorname{sen}^2\left(\frac{\frac{r\delta_j}{\sqrt{\delta_i^2+\delta_j^2}}}{2\delta_j}\right)\right) \\ &= 4(\delta_i^2+\delta_j^2)\operatorname{sen}^2\left(\frac{r}{2\sqrt{\delta_i^2+\delta_j^2}}\right) = r^2\left(\frac{\operatorname{sen}\left(\frac{r}{2\sqrt{\delta_i^2+\delta_j^2}}\right)}{\frac{r}{2\sqrt{\delta_i^2+\delta_j^2}}}\right)^2 . \end{aligned}$$

Como $f(x)$ é crescente e $\sqrt{\delta_i^2+\delta_j^2} \geq \sqrt{\delta_{i+1}^2+\delta_{j+1}^2} \geq \cdots \geq \sqrt{\delta_{m-1}^2+\delta_m^2} \geq \delta_m$ segue que $f(\sqrt{\delta_i^2+\delta_j^2}) \geq f(\delta_m)$, $\forall\, i, j = 1, \cdots, m$. Portanto,

$$4(\delta_i^2+\delta_j^2)\operatorname{sen}^2\left(\frac{r}{2\sqrt{\delta_i^2+\delta_j^2}}\right) \geq 4\delta_m^2 \operatorname{sen}^2\left(\frac{r}{2\delta_m}\right),\quad \frac{r}{2\sqrt{\delta_i^2+\delta_j^2}} \in (0, \pi].$$

Continuando deste modo, para os pontos críticos da forma (m) temos,

$$D(y) = d^2(\psi(y), \psi(\mathbf{0})) = r^2 \left(\frac{\operatorname{sen}\left(\frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}} \right)}{\frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}}} \right)^2 .$$

Mais uma vez, usando o fato de que $f(x)$ é crescente e

$$\sqrt{\delta_1^2 + \cdots + \delta_m^2} \geq \sqrt{\delta_1^2 + \cdots + \hat{\delta}_i^2 + \cdots + \delta_m^2} \geq \sqrt{\delta_1^2 + \cdots + \hat{\delta}_i^2 + \cdots + \hat{\delta}_j^2 + \cdots + \delta_m^2} \geq \cdots$$

$$\cdots \geq \sqrt{\delta_i^2} \geq \delta_m,$$

onde $\hat{\delta}_l$ denota a ausência de δ_l na soma acima, segue que

$$4(\delta_1^2 + \cdots + \delta_m^2) \operatorname{sen}^2 \left(\frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}} \right) \geq 4\delta_m^2 \operatorname{sen}^2 \left(\frac{r}{2\delta_m} \right), \quad \frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}} \in (0, \pi].$$

Como em cada um dos casos temos as seguintes restrições:

$$\begin{aligned} & r \leq 2\pi\delta_i, \quad i = 1, \cdots, m \\ & r \leq 2\pi\sqrt{\delta_i^2 + \delta_j^2}, \quad i, j = 1, \cdots, m \\ & \vdots \\ & r \leq 2\pi\sqrt{\delta_1^2 + \cdots + \delta_m^2}, \end{aligned}$$

e $2\pi\sqrt{\delta_1^2 + \cdots + \delta_m^2} \geq \cdots \geq 2\pi\sqrt{\delta_i^2 + \delta_j^2} \geq 2\pi\delta_i \geq 2\pi\delta_m$, tomando $r \leq 2\pi\delta_m$, temos que

$$4\delta_m^2 \operatorname{sen}^2 \left(\frac{r}{2\delta_m} \right) \leq d^2(\psi(y), \psi(\mathbf{0})) \leq 4(\delta_1^2 + \cdots + \delta_m^2) \operatorname{sen}^2 \left(\frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}} \right),$$

$\forall\, y$ tal que $||y|| = r$.

Portanto o valor mínimo será obtido para,

$$y = (0, \cdots, 0, \pm r, 0, \cdots, 0)$$

na posição onde $\delta_i = \delta_{min}$ (valor mínimo de δ) e o valor máximo será para

$$y = \frac{r}{\sqrt{\delta_1^2 + \cdots + \delta_m^2}} (\pm\delta_1, \cdots, \pm\delta_m)$$

(sobre a diagonal da "caixa" que define o toro).

Ainda, como $\operatorname{sen} x < x$, $\forall x > 0$, segue que

$$2\sqrt{\delta_1^2 + \cdots + \delta_m^2}\,\operatorname{sen}\left(\frac{r}{2\sqrt{\delta_1^2 + \cdots + \delta_m^2}}\right) < r$$

o que conclui a demonstração. ◪

De acordo com a Proposição (4.3.1) a pior deformação ocorre na direção do vetor de norma mínima do sub-reticulado.

Observação 4.3.1. *Quando a esfera de $\mathbb{R}^{2n}$ é unitária isto é, $(\sum_{i=1}^{m} \delta_i^2 = 1)$, vale a seguinte desigualdade*

$$4\delta_{min}^2 \operatorname{sen}^2\left(\frac{r}{2\delta_{min}}\right) \leq d^2(\psi(y), \psi(\mathbf{0})) \leq 4\operatorname{sen}^2\left(\frac{r}{2}\right) \leq r^2.$$

4.3.3 Códigos de grupo comutativo e toros planares

Os códigos de grupo comutativo em dimensão par, $2m$, podem ser vistos sobre os toros planares descritos na seção anterior. Tal caracterização permitiu a construção de limitantes para a cardinalidade de um código de grupo comutativo em termos de sua distância mínima, de seu vetor inicial e da máxima densidade de empacotamento de esferas em $\mathbb{R}^m$, onde m é a dimensão do toro [18]. Embora códigos de grupo comutativo não sejam geralmente os melhores dentre os códigos de grupo no que diz respeito a distância mínima, eles oferecem menor complexidade no processo de codificação/decodificação como é apresentado em [45].

Como, pelo Teorema (4.2.1), qualquer grupo comutativo pode ser considerado como gerado por um grupo de matrizes dadas por (4.2), podemos derivar a seguinte proposição:

Proposição 4.3.2. *(Lugar geométrico dos códigos de grupo comutativo, [18]) Todo código de grupo comutativo é equivalente a um código de grupo comutativo χ cujo vetor inicial é $u = (u_1, \cdots, u_n)$ e seus pontos tem a forma*

$$(R(a_{i1})(u_1, u_2), \cdots, R(a_{im})(u_{2m-1}, u_{2m}), \mu_{2m+1}(i)u_{2m+1}, \cdots, \mu_n(i)u_n), \tag{4.9}$$

onde $a_{ij} = \dfrac{2\pi k_{ij}}{M}$ e $R(a_{ij})$ é a rotação no plano de ângulo a_{ij}. Mais do que isto, se $n = 2m$, χ está contido no toro planar T_δ, onde $\delta = (\delta_1, \cdots, \delta_m)$ satisfaz $\delta_i^2 = u_{2i-1}^2 + u_{2i}^2$.

Demonstração: A demonstração é direta considerando matrizes divididas em blocos 2×2. Cada um destes blocos na diagonal atua preservando o círculo contido no plano dado pelos pares de coordenadas subsequentes. Começando com o vetor inicial $u = (u_1, \cdots, u_n)$, onde $\delta_j^2 = u_{2j-1}^2 + u_{2j}^2$, com $1 \leq j \leq \left\lfloor \frac{n}{2} \right\rfloor$, um j-bloco na diagonal de qualquer matriz do grupo G é uma matriz ortogonal 2×2 que leva o par (u_{2j-1}, u_{2j}) em outro par no mesmo círculo de raio δ_j. ∎

Se no Teorema (4.2.1) tivermos $2m = l$, então o código comutativo $G(u)$ é gerado por matrizes de rotação 2×2 nos pares (u_{2i-1}, u_{2i}), $i = 1, \cdots, m$, isto é,

$$(R(a_{i1})(u_1, u_2), \cdots, R(a_{im})(u_{2m-1}, u_{2m})),$$

onde $u = (u_1, \cdots, u_{2m})$, $G(u) \subset T_\delta \subset \mathbb{R}^{2m}$, $\delta = (\delta_1, \cdots, \delta_m)$, $\delta_i^2 = u_{2i-1}^2 + u_{2i}^2$.

Neste caso, dizemos que o grupo comutativo G é *livre de blocos de reflexão.* Por blocos de reflexão nos referimos a blocos 2-dimensionais

$$\pm \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

que aparecem na forma canônica quando $2m < n$.

Para códigos de grupo comutativo livres de blocos de reflexão, é sempre possível considerar o vetor inicial como $u = (\delta_1, 0, \cdots, \delta_m, 0)$. De fato, podemos considerar $(u_{2k-1}, u_{2k}) \neq (0, 0)$, $k = 1, \cdots, m$, pois se $(u_{2k-1}, u_{2k}) = (0, 0)$ o código de grupo gerado não é substancial pois, uma vez que, estará contido num espaço de dimensão $2n - 2$. Seja $\delta_k = \sqrt{u_{2k-1}^2 + u_{2k}^2}$, temos então $(u_{2k-1}, u_{2k}) = \delta_k(\cos\theta_k, \operatorname{sen}\theta_k)$, onde $(\cos\theta_k, \operatorname{sen}\theta_k) = \frac{1}{\delta_k}(u_{2k-1}, u_{2k})$. A isometria $\mathbb{R}^{2m} \longrightarrow \mathbb{R}^m$ dada por $(R(-\theta_1), \cdots, R(-\theta_m))$ leva o vetor inicial $u = (u_1, \cdots, u_{2m})$ em $(\delta_1, 0, \cdots, \delta_n, 0)$.

Assim o vetor inicial determina o toro planar T_δ no qual o código estará contido. Além disto, como veremos a seguir, códigos de grupo comutativo em dimensão par, $n = 2m$, cujas matrizes do grupo gerador são livres de reflexão, estão diretamente relacionados a reticulados.

O vetor inicial $u = (\delta_1, 0, \delta_2, 0, \cdots, \delta_m, 0)$ é a imagem através do toro da função ψ (4.5) de $\mathbf{0} \in \mathbb{R}^m$. Podemos associar à rotação dada pelo j-bloco 2×2 de O_i a um deslocamento na direção e_j em $\mathbb{R}^{\frac{n}{2}=m}$, gerando um reticulado. Mais especificamente; existe uma corres-

pondência, através da função ψ, entre $O_i u$, onde

$$O_i = \left[R\left(\frac{2\pi k_{i1}}{M}\right), \cdots, R\left(\frac{2\pi k_{i\frac{n}{2}}}{M}\right) \right]_{n\times n},$$

e o ponto

$$\left(\frac{2\pi k_{i1}\delta_1}{M}, \cdots, \frac{2\pi k_{i\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right)$$

no reticulado $\prod_{i=1}^{m}\left(\frac{2\pi\delta_i}{M}\right)\mathbb{Z} \subset \mathbb{R}^m$, restrito à hipercaixa $B = \prod_{i=1}^{m}[0, 2\pi\delta_i)$. De fato,

$$\psi\left(\frac{2\pi k_{i1}\delta_1}{M}, \cdots, \frac{2\pi k_{i\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right) = O_i u$$

e

$$\begin{aligned}
\psi(x_1, \cdots, x_{\frac{n}{2}}) = O_i(u) &\Leftrightarrow \psi(x_1, \cdots, x_{\frac{n}{2}}) = \psi\left(\frac{2\pi k_{i1}\delta_1}{M}, \cdots, \frac{2\pi k_{i\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right) \\
&\Leftrightarrow (x_1, \cdots, x_{\frac{n}{2}}) \equiv \left(\frac{2\pi k_{i1}\delta_1}{M}, \cdots, \frac{2\pi k_{i\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right) \mod 2\pi\delta \\
&\Leftrightarrow (x_1, \cdots, x_{\frac{n}{2}}) = \left(\frac{2\pi k_{i1}\delta_1}{M}, \cdots, \frac{2\pi k_{i\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right) + 2\pi(\delta_1 t_1, \cdots, \delta_{\frac{n}{2}} t_{\frac{n}{2}}),
\end{aligned}$$

$t_i \in \mathbb{Z}$, $i = 1, \cdots, \frac{n}{2}$. Assim, $\psi^{-1}(O_i(u)) = (x_1, \cdots, x_{\frac{n}{2}}) = \left(\frac{2\pi k_{i1}\delta_1}{M}, \cdots, \frac{2\pi k_{i\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right) + 2\pi(\delta_1 t_1, \cdots, \delta_{\frac{n}{2}} t_{\frac{n}{2}})$.

Isto nos leva à seguinte proposição:

Proposição 4.3.3. *[18] Seja $G(u) = \{O(u), O \in G\}$, $u \in S^{n-1}$ um código de grupo comutativo de ordem M em dimensão par, onde $u = (\delta_1, 0, \cdots, \delta_{\frac{n}{2}}, 0)$. Se os elementos de G são blocos livres de reflexão então a imagem inversa $\psi^{-1}(G(u))$ é o reticulado Λ gerado pelo conjunto*

$$\left\{ v_\ell ; v_\ell = \left(\frac{2\pi k_{\ell 1}\delta_1}{M}, \cdots, \frac{2\pi k_{\ell\frac{n}{2}}\delta_{\frac{n}{2}}}{M}\right) \right\}$$

que contém o reticulado $\prod_{i=1}^{m}\left(\frac{2\pi\delta_i}{M}\right)\mathbb{Z}$ como um sub-reticulado "retangular".

O quociente dos reticulados $\dfrac{\Lambda}{\prod_{i=1}^{m}(2\pi\delta_i\mathbb{Z})}$ induz um grafo sobre o toro planar cujos vértices são precisamente $G(u)$. Este quociente de reticulados pode ser visto como o código de bloco

linear sobre $\mathbb{Z}_M$ gerado pelo conjunto $\{k_\ell; k_\ell = (k_{\ell 1}, \cdots, k_{\ell \frac{n}{2}})\}$ deformado pela aplicação

$$\phi(x_1, \cdots, x_{\frac{n}{2}}) = 2\pi(\delta_1 x_1, \cdots, \delta_{\frac{n}{2}} x_{\frac{n}{2}}).$$

Uma referência para códigos de bloco lineares sobre $\mathbb{Z}_M$ é [11].

Como temos representantes de todas as classes do quociente na "caixa" que define o toro planar, o código de grupo dado na Proposição (4.3.3), é a imagem do reticulado acima na "caixa" B que define o toro planar T_δ.

Do ponto de vista de códigos, o importante é ter distâncias mínimas maiores possíveis. Para um número fixo M o código esférico será a imagem de M pontos do sub-reticulado que estão dentro da "caixa" que define o toro. É de se esperar que um maior espaçamento entre os pontos no $\mathbb{R}^m$ ocorra para toros com maior volume m-dimensional. Como comentamos, uma esfera em $\mathbb{R}^{2m}$ é folheada por toros, dentre estes o de área máxima é o que é definido por uma "caixa quadrada": T_δ com $\delta = \left(\frac{1}{\sqrt{m}}, \cdots, \frac{1}{\sqrt{m}}\right)$ para uma esfera de raio 1. De fato, dado que ψ, tal como em (4.3), é uma isometria local entre o paralelepípedo $\prod_{i=1}^{m}[0, 2\pi\delta_i)$ e T_δ, segue que a área desses objetos é a mesma. Ou seja, $A(\delta) = (2\pi)^m \prod_{i=1}^{m} \delta_i$.

Para maximizar $A(\delta)$ restrita a $G(\delta) = |\delta|^2 - 1 = 0$, usaremos o método dos multiplicadores de Lagrange. Notamos que

$$\nabla A = (2\pi)^m \sum_{i=1}^{m} (\delta_1 \cdots \widehat{\delta_i} \cdots \delta_m) e_i,$$

onde $\widehat{\delta_j}$ denota a ausência de δ_j no produto $\delta_1 \cdots \delta_m$ e

$$\nabla G = 2(\delta_1, \cdots, \delta_m).$$

Assim, o problema se resume a encontrar as soluções do sistema

$$\begin{cases} (2\pi)^m(\delta_1 \cdots \widehat{\delta_i} \cdots \delta_m) = \lambda 2\delta_j \quad 1 \leq j \leq m \\ |\delta|^2 = 1 \end{cases}.$$

Multiplicando a primeira equação por δ_j, obtemos que todos os pesos devem ser iguais. Usando este fato na segunda equação, segue que

$$m\delta_1^2 = \sum_{i=1}^{m} \delta_1^2 = \sum_{i=1}^{m} \delta_i^2 = 1.$$

Logo, $\delta_i = \dfrac{1}{\sqrt{m}}$. Portanto a maior área que um toro plano T_δ pode ter é $A(\frac{1}{\sqrt{m}}, \cdots, \frac{1}{\sqrt{m}}) = (\frac{2\pi}{\sqrt{m}})^m$.

4.4 Limitantes para códigos de grupo comutativo

No que segue introduzimos o limitante dado em [18] para códigos de grupo comutativo.

Consideremos um código em T_δ com M pontos e distância mínima d. Isto equivale a um empacotamento de M chapéus esféricos sobre T_δ de maneira que seus centros distem entre si no mínimo d. Como a área $\frac{n}{2}$-dimensional ocupada por estes chapéus é no máximo a área do próprio toro T_δ, o número de chapéus também é limitado. Vamos dar uma estimativa para a área destes chapéus e depois apresentar um limitante para M, supondo que a distância mínima d é fixa.

Um chapéu esférico sobre o toro T_δ centrado em x_0 e de raio $\rho = \dfrac{d}{2}$ é definido por

$$B^{T_\delta}(x_0, \rho) = \{x \in T_\delta; \langle x_0 - x,\, x_0 - x\rangle^{1/2} \leq \rho\}.$$

Para cada parâmetro $\delta = (\delta_1, \cdots, \delta_m)$, o volume $\frac{n}{2}$-dimensional $V(\delta)$ do toro T_δ é o produto das medidas dos lados da "caixa" que o gera: $\displaystyle\prod_{i=1}^{\frac{n}{2}}(2\pi\delta_i)$. Como todo código de grupo comutativo de dimensão par com vetor de raio δ mora em T_δ, $V(\delta)$ certamente traz restrições sobre a distância mínima deste código. Observamos que o volume de $B^{T_\delta}(x_0, \rho)$ é o mesmo que o de $S_\rho = \psi^{-1}(B^{T_\delta}(x_0, \rho)$, pois ψ é uma isometria local e procuramos uma estimativa para este último.

Como os toros planares são homogêneos [12], o volume de S_ρ independe do ponto central x_0 escolhido, depende apenas de ρ e da proporção da "caixa" (dada pelos δ_i) que define o toro planar. Assim, o problema se restringe a obter uma estimativa do volume do conjunto

$$S_\rho = \{y \in \mathbb{R}^m;\, D(y) \leq \rho^2\},\ \textit{onde}\ D(y) = ||\psi(y) - \psi(\mathbf{0})||^2 = 4\sum_{i=1}^{m} \delta_i^2 \operatorname{sen}^2\left(\frac{y_i}{2\delta_i}\right).$$

Observamos que o bordo do conjunto S_ρ, ou seja, $\{y \in \mathbb{R}^m;\, D(y) = \rho^2\}$ é um compacto, portanto a função $G(y_1, \cdots, y_m) = \displaystyle\sum_{i=1}^{m} y_i^2$ restrita a ele assume máximo e mínimo. Usando o método dos multiplicadores de Lagrange, em [18] é obtido o resultado a seguir, o qual adaptamos para obter o resultado dual na Proposição (4.3.1).

Proposição 4.4.1. *[18] O máximo e o mínimo de* $G(y_1, \cdots, y_m) = \sum_{i=1} y_i^2$ *restrita ao bordo de* S_ρ*, ou seja, ao conjunto* $\{y \in \mathbb{R}^m;\, D(y) = \rho^2\}$*, onde* $D(y) = 4\sum_{i=1}^{m} \delta_i^2 \operatorname{sen}^2\left(\frac{y_i}{2\delta_i}\right)$*, são* $4\mu^2 \operatorname{arcsen}^2(\frac{\rho}{2\mu})$ *e* $4\operatorname{arcsen}^2(\frac{\rho}{2})$*, respectivamente, onde* μ *é o menor dos raios* δ_i*.*

Corolário 4.4.1. *[38] O volume (m-dimensional) do conjunto* S_ρ *é no máximo* $V_m(2\mu \operatorname{arcsen}(\frac{\rho}{2\mu}))^m$ *e no mínimo* $V_m(2\operatorname{arcsen}(\frac{\rho}{2}))^m$*, onde* V_m *é o volume da esfera* $S^{m-1} \subset \mathbb{R}^m$ *de raio 1 e* μ *é o menor dos raios* δ_i*.*

Ainda, devido à homogeneidade do toro temos a seguinte proposição, que será usada para estabelecer um limitante superior para códigos de grupo comutativo em dimensão par:

Proposição 4.4.2. *[18] Seja* T_δ *o toro planar em* $\mathbb{R}^{2m}$*,* $x \in T_\delta$ *e* ψ *sua parametrização. Então* $B(\psi^{-1}(x), 2\operatorname{arcsen}(\frac{\rho}{2})) \subset \psi^{-1}(B^{T_\delta}(x,\rho)) \subset B(\psi^{-1}(x), 2\mu \operatorname{arcsen}(\frac{\rho}{2\mu}))$*, onde* $B(y,r)$ *denota a bola em* $\mathbb{R}^m$ *centrada na origem em* y *e raio* r*,* μ *é o menor raio* δ_i*.*

Todo código $\{x_l\}_{l=1}^M$ com distância mínima d em T_δ é um empacotamento de M chapéus $B^{T_\delta}(x_l, d/2)$, implicando na união disjunta de conjuntos $\cup_{l=1}^M \psi^{-1}(B^{T_\delta}(x_l, d/2))$ em $\prod_{i=1}^{m}[0, 2\pi\delta_i)$, pois ψ é uma bijeção. Portanto a união $\cup_{l=1}^M B(\psi^{-1}(x_l, 2\operatorname{arcsen}(d/4)))$ é disjunta. Consequentemente, reduzimos o problema de empacotamento em T_δ para um problema de empacotamento de M bolas no paralelepípedo $\prod_{i=1}^{m}[0, 2\pi\delta_i)$. Como no paralelepípedo $\psi^{-1}(\{x_l\}_{l=1}^M)$ é um subconjunto de um subgrupo discreto de $\mathbb{R}^m$, ou seja, está contido em um reticulado de $\mathbb{R}^m$, este empacotamento deve satisfazer Δ_m, a densidade máxima de empacotamento de um reticulado em $\mathbb{R}^m$. Mais ainda, nos limitantes aparece o quociente $\Lambda_m = \dfrac{\Delta_m}{V_m}$, onde V_m é o volume da esfera de raio 1 em $\mathbb{R}^m$. Este quociente é conhecido como a máxima densidade de centro de um reticulado em $\mathbb{R}^m$.

Consideramos um código de grupo comutativo livre de reflexões, $G(u)$, de ordem M em $\mathbb{R}^{2m}$ e um empacotamento por chapéu esférico de raio ρ centrado na palavra código. A imagem inversa da união dos M chapéus tem um volume $m = \frac{n}{2}$-dimensional menor do que o volume total da "caixa" em $\mathbb{R}^m$, então

$$M \operatorname{volume}(\psi^{-1}(B^{T_\delta}(u,\rho))) \leq \prod_{i=1}^{m}(2\pi\delta_i).$$

Além disso, usando a Proposição (4.4.2), para $x = u$ (vetor inicial) e $\psi^{-1}(x) = 0 \in \mathbb{R}^m$ podemos afirmar que

$$M\text{volume}\left(B(0, 2\,\text{arcsen}\,\frac{\rho}{2})\right) \leq \prod_{i=1}^{m}(2\pi\delta_i)\Delta_{G(u)} \leq \prod_{i=1}^{m}(2\pi\delta_i)\Delta_m,$$

onde $\Delta_{G(u)}$ é a densidade do reticulado associado ao código (Proposição 4.3.3) e Δ_m é a melhor densidade do reticulado em dimensão m. Portanto, temos

$$MV_m\left(2\,\text{arcsen}\,\frac{\rho}{2}\right)^m \leq \prod_{i=1}^{m}(2\pi\delta_i)\Delta_m, \tag{4.10}$$

onde V_m é o volume da esfera unitária em $\mathbb{R}^m$.

Denotando $\Lambda_m = \dfrac{\Delta_m}{V_m}$ a melhor densidade de centro para reticulados em $\mathbb{R}^m$, enunciaremos um limitante de código de grupo comutativo envolvendo algumas propriedades de reticulados.

Proposição 4.4.3. *[18] Todo código de grupo comutativo $G(u)$ de ordem M em $\mathbb{R}^{2m}$ livre de blocos 2×2 de reflexão com distância mínima d e vetor inicial $(u_1, \cdots, u_{2m})$ satisfaz*

$$M \leq \frac{\pi^m \prod_{i=1}^{m}(u_{2i-1}^2 + u_{2i}^2)^{1/2}\Lambda_m}{(\text{arcsen}\,\frac{d}{4})^m} \leq \Lambda_m\left(\frac{\pi}{(\text{arcsen}\,\frac{d}{4}).m^{1/2}}\right)^m,$$

onde Λ_m é a densidade de centro máxima de um reticulado em $\mathbb{R}^m$.

Demonstração: Basta observar que o raio de empacotamento é definido por $\rho = \dfrac{d}{2}$. Substituindo ρ em (4.10) e isolando M segue a primeira desigualdade. A segunda desigualdade segue do fato de que, como mostramos na Seção (4.3), o toro de área máxima em uma esfera unitária tem todos os raios iguais a $\dfrac{1}{\sqrt{m}}$. Assim,

$$\pi^m \prod_{i=1}^{m}(u_{2i-1}^2 + u_{2i}^2)^{1/2} \leq \left(\frac{\pi}{m^{1/2}}\right)^m.$$

■

Podemos enunciar a proposição acima como limitação para a distância mínima, da seguinte forma:

Proposição 4.4.4. *(Limitante do toro) [18] Todo código de grupo comutativo $G(u)$ de ordem M em $\mathbb{R}^{2m}$ livre de blocos 2×2 com distância mínima d e vetor inicial $(u_1,\cdots,u_{2m})$ satisfaz*

$$d \leq 4\,\mathrm{sen}\left(\pi\left(\frac{\sqrt{\prod_{i=1}^{m}(u_{2i-1}^2+u_{2i}^2)}\Lambda_m}{M}\right)^{\frac{1}{m}}\right) \leq 4\,\mathrm{sen}\left(\pi\left(\frac{m^{-1/2}.\Lambda_m^{1/m}}{M^{1/m}}\right)\right),$$

onde Λ_m é a densidade de centro máxima de um reticulado em $\mathbb{R}^m$.

Para M grande, d será pequeno e pela Proposição (4.4.2), a imagem inversa do chapéu esférico estará arbitrariamente mais próxima do empacotamento reticulado em $\mathbb{R}^m$ e portanto estarão próximos do limitante estabelecido aqui. Esta propriedade segue do fato que o raio máximo e o raio mínimo na Proposição (4.4.2) tende a 1, $\lim_{\rho\to 0}\dfrac{2\,\mathrm{arcsen}\left(\frac{\rho}{2}\right)}{2\mu\,\mathrm{arcsen}\left(\frac{\rho}{2\mu}\right)}=1$.

Isto significa que a imagem inversa de um chapéu esférico de raio ρ no toro plano em $\mathbb{R}^{2m}$ será aproximado, para ρ pequeno, a uma bola em $\mathbb{R}^m$.

Para fins comparativos, este resultado será de grande importância no próximo capítulo, no qual construímos códigos esféricos com o objetivo de obter distâncias mínimas mais próximas do limitante da Proposição (4.4.4).

4.4.1 Procedimentos para gerar códigos de grupo comutativo com boa distância mínima.

De acordo com o exposto até aqui, para o cálculo da distância mínima de códigos esféricos construídos através do quociente de reticulados, faremos as seguintes considerações:

1. Seja Λ_α um sub-reticulado de Λ_β, Λ_α e Λ_β com bases $\alpha=\{v_1,\cdots,v_m\}$ ortogonal e $\beta=\{w_1,\cdots,w_m\}$, respectivamente. Se $A=(a_{ij})_{i,j=1}^m$, $a_{ij}\in\mathbb{Z}$ é a matriz da base α escrita em relação à base β por colunas, isto é,

$$\left[\begin{array}{cccc} v_1 & v_2 & \cdots & v_m \end{array}\right] = \left[\begin{array}{cccc} w_1 & w_2 & \cdots & w_m \end{array}\right] . \left[\begin{array}{cccc} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{mm} \end{array}\right] \tag{4.11}$$

então para cada $\delta_i = \dfrac{||v_i||}{2\pi}$, o código esférico associado tem por vetor inicial $u = (\delta_1, 0, \delta_2, 0 \cdots, \delta_m, 0)$ com grupo comutativo $G = \{O_i\}_{i=1}^{M}$ e $M = |\det A|$ pontos.

2. De (4.11) segue que

$$\left[\begin{array}{cccc} w_1 & w_2 & \cdots & w_m \end{array}\right] = \left[\begin{array}{cccc} v_1 & v_2 & \cdots & v_m \end{array}\right] . \left[\begin{array}{cccc} \tilde{a}_{11} & \tilde{a}_{21} & \cdots & \tilde{a}_{m1} \\ \tilde{a}_{12} & \tilde{a}_{22} & \cdots & \tilde{a}_{m2} \\ \vdots & \vdots & & \vdots \\ \tilde{a}_{1m} & \tilde{a}_{2m} & \cdots & \tilde{a}_{mm} \end{array}\right],$$

onde $(\tilde{a}_{ij})_{i,j=1}^{m} = A^{-1} = \dfrac{1}{\det A}.(\mathrm{Cof}(A))^t$.

Logo,

$$\left[\begin{array}{cccc} w_1 & w_2 & \cdots & w_m \end{array}\right] = \left[\begin{array}{cccc} v_1 & v_2 & \cdots & v_m \end{array}\right] . \frac{1}{\det A} \left[\begin{array}{cccc} k_{11} & k_{21} & \cdots & k_{m1} \\ k_{12} & k_{22} & \cdots & k_{m2} \\ \vdots & \vdots & \cdots & \vdots \\ k_{1m} & k_{2m} & \cdots & k_{mm} \end{array}\right] \tag{4.12}$$

Portanto,

$$w_i = \frac{1}{\det A} k_{i1} v_1 + \frac{1}{\det A} k_{i2} v_2 + \cdots + \frac{1}{\det A} k_{im} v_m.$$

Tomando $v_i = 2\pi\delta_i e_i$, $i = 1, \cdots, m$ temos que,

$$\begin{aligned} w_i &= \frac{1}{\det A} k_{i1} 2\pi\delta_1 e_1 + \frac{1}{\det A} k_{i2} 2\pi\delta_2 e_2 + \cdots + \frac{1}{\det A} k_{im} 2\pi\delta_m e_m \\ &= \left(\frac{1}{\det A} k_{i1} 2\pi\delta_1, \frac{1}{\det A} k_{i2}\pi\delta_2, \cdots, \frac{1}{\det A} k_{im}\pi\delta_m \right). \end{aligned}$$

Aplicando a função ψ definida em (4.3), temos que

$$\begin{aligned}\psi(w_i) &= \left(\frac{||v_1||}{2\pi}\cos\left(\frac{2\pi k_{i1}}{\det A}\right), \frac{||v_1||}{2\pi}\,\mathrm{sen}\left(\frac{2\pi k_{i1}}{\det A}\right), \cdots, \frac{||v_m||}{2\pi}\cos\left(\frac{2\pi k_{im}}{\det A}\right), \frac{||v_m||}{2\pi}\,\mathrm{sen}\left(\frac{2\pi k_{im}}{\det A}\right)\right) \\ &= \begin{bmatrix} R\left(\frac{2\pi k_{i1}}{\det A}\right) & & \\ & \ddots & \\ & & R\left(\frac{2\pi k_{im}}{\det A}\right) \end{bmatrix} \cdot \begin{bmatrix} \frac{||v_1||}{2\pi} \\ 0 \\ \vdots \\ \frac{||v_m||}{2\pi} \\ 0 \end{bmatrix}.\end{aligned}$$

Ou seja, o código esférico gerado pelo quociente $\frac{\Lambda_\beta}{\Lambda_\alpha}$, tem por um vetor inicial o vetor da direita e por matrizes ortogonais geradoras O_i dadas acima à esquerda.

3. A forma normal de Smith fornece um conjunto mínimo de geradores no toro e estes determinarão matrizes de rotação geradoras em $\mathbb{R}^{2m}$. As matrizes de rotação geradoras determinarão a disposição de cada palavra-código $\tilde{O}_i u$, $i = 1, \cdots, m$ em $S^{2m-1} \subset \mathbb{R}^{2m}$.

   No Teorema (4.2.4) mostramos que $\overline{h}_i = \overline{\tilde{p}_{1i}w_1 + \cdots + \tilde{p}_{mi}w_m}$ é de ordem d_i, e portanto, um gerador do grupo quociente. Vamos ver agora como determinar as matrizes de rotação a partir dos geradores do grupo.

   Temos,

$$[\ h_1 \quad \cdots \quad h_m\ ] = [\ w_1 \quad \cdots w_m\ ]. \begin{bmatrix} \tilde{p}_{11} & \cdots & \tilde{p}_{1m} \\ \tilde{p}_{21} & \cdots & \tilde{p}_{2m} \\ \vdots & \vdots & \\ \tilde{p}_{m1} & \cdots & \tilde{p}_{mm} \end{bmatrix}.$$

   De (4.12) segue que,

$$[\ h_1 \quad \cdots \quad h_m\ ] = [\ v_1 \quad \cdots v_m\ ]. \frac{1}{\det A} \begin{bmatrix} k_{11} & \cdots & k_{m1} \\ k_{12} & \cdots & k_{m1} \\ \vdots & \vdots & \vdots \\ k_{1m} & \cdots & k_{mm} \end{bmatrix} \cdot \begin{bmatrix} \tilde{p}_{11} & \cdots & \tilde{p}_{1m} \\ \tilde{p}_{21} & \cdots & \tilde{p}_{2m} \\ \vdots & \vdots & \\ \tilde{p}_{m1} & \cdots & \tilde{p}_{mm} \end{bmatrix}.$$

   Portanto,

$$h_i = \frac{1}{\det A}(k_{11}\tilde{p}_{1i} + \cdots + k_{m1}\tilde{p}_{mi})v_1 + \cdots + \frac{1}{\det A}(k_{1m}\tilde{p}_{1i} + \cdots + k_{mm}\tilde{p}_{mi})v_m.$$

Assim, o grupo comutativo $G = \{O_i\}_{i=1}^{M}$ é levado em matrizes de blocos diagonais da forma

$$\tilde{O}_i = \left[R\left(\frac{2\pi(k_{11}\tilde{p}_{1i} + \cdots + k_{m1}\tilde{p}_{mi})}{\det A}\right), \cdots, R\left(\frac{2\pi(k_{1m}\tilde{p}_{1i} + \cdots + k_{mm}\tilde{p}_{mi})}{\det A}\right)\right]_{2m\times 2m}$$

e neste caso, o código de grupo $G(u)$ será gerado por rotações 2×2 nos pares $(\delta_i = \frac{||v_i||}{2\pi}, 0)$, $i = 1, \cdots, m$.

4. De (4.7), a distância euclidiana mínima ao quadrado de $\psi(w_j)$ à $\psi(\mathbf{0})$, $w_j = (w_{j1}, w_{j2}, \cdots, w_{jm}) \in \Lambda_\beta$, $j = 1, \cdots, m$, onde w_j é um dos vetores que geram Λ_β é

$$d^2(\psi(w_j), \psi(\mathbf{0})) = 4\sum_{i=1}^{m} \delta_i^2 \operatorname{sen}^2\left(\frac{\frac{2\pi k_{ji}\delta_i}{M}}{2\delta_i}\right) = 4\sum_{i=1}^{m} \delta_i^2 \operatorname{sen}^2\left(\frac{\pi k_{ji}}{|\det A|}\right) =$$
$$= 4\sum_{i=1}^{m} \delta_i^2 \operatorname{sen}^2(\pi \tilde{a}_{ji}).$$

5. Estamos interessados em encontrar a maior distância euclidiana mínima no código esférico. Mostraremos no Capítulo 5, em cada uma das construções de sub-reticulados lá desenvolvidas, que a menor distância é atingida, sob certas restrições, pela imagem de um dos vetores de norma mínima da base que gera o reticulado e para isto fazemos o uso da Proposição (4.3.1). É este fato que viabiliza o cálculo da distância mínima do código esférico, de forma quase imediata, mesmo para códigos com um enorme número de pontos.

Observação 4.4.1. *Um dos fatores importantes a considerar na construção de sub-reticulados é a deformação. Onde existe maior deformação a distância mínima é pior. A deformação é maior na direção de colagem do toro, e esta coincide com os vetores do sub-reticulado. Como a distância mínima é atingida pela imagem de um dos vetores de norma mínima da base que gera o reticulado, o ideal é que os vetores do sub-reticulado se afastem o máximo possível dos vetores de norma mínima do reticulado original.*

CAPÍTULO 5

Construção de Códigos Esféricos Através do Quociente de Reticulados

Nosso objetivo neste capítulo é a construção de códigos esféricos através do quociente de reticulados, de forma a obter as melhores distâncias mínimas. Assim, pesquisamos a existência de sub-reticulados Λ_α $\mathbb{Z}^m$- rotacionados ou "retangulares" (os vetores da base α são mutuamente ortogonais) a partir de reticulados Λ_β que possuam boa densidade de empacotamento, mais especificamente neste trabalho, A_2, D_3, D_4 *e* E_8 que são os que tem maior densidade de empacotamento em suas respectivas dimensões.

Num reticulado Λ_β de dimensão m em $\mathbb{R}^m$, temos naturalmente uma estrutura de anel induzida por $\mathbb{Z}^n$ e portanto, um grupo aditivo abeliano a ele associado. Dado um sub-reticulado $\Lambda_\alpha \subset \Lambda_\beta$, o quociente $\dfrac{\Lambda_\beta}{\Lambda_\alpha}$ terá portanto, estrutura de grupo e poderá ser identificado com um grafo num toro planar m-dimensional, ou seja, as classes laterais de Λ_α em Λ_β podem ser vistas como vértices de um grafo sobre o toro planar gerado por Λ_α e induzem um código esférico em $\mathbb{R}^{2m}$. A estrutura de grupo do quociente de reticulados $\dfrac{\Lambda_\beta}{\Lambda_\alpha}$ determinará o grupo gerador do código e a sua representação nas matrizes ortogonais $2m \times 2m$.

Para obtermos as melhores distâncias mínimas procuramos por condições que tornem os vetores da base α com normas aproximadamente iguais, isto é, com a base de forma a deixar a "caixa" que define o toro mais próxima de um "cubo", o qual determina o toro de maior

"área" na esfera do $\mathbb{R}^{2m}$.

Destacamos também as proposições (5.1.1), (5.3.1), (5.4.1), (5.5.1), que mostram-se particularmente importantes quando os valores são grandes para o número de pontos M. Nestes casos, por exemplo, a busca por exaustão é inviável computacionalmente e baseados nestes resultados, temos que basta calcular as distâncias para um número pequeno de pontos (as imagens dos vetores de norma mínima) para determinarmos a distância mínima do código independente de quão grande seja M.

5.1 Sub-reticulados "retangulares" do reticulado hexagonal A_2

Considere o reticulado $\Lambda_\beta = A_2$, com $\beta = \{(1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\}$, uma base de A_2. Nosso interesse é encontrar um sub-reticulado Λ_α de Λ_β, tal que $\alpha = \{v_1, v_2\}$ seja uma base ortogonal de Λ_β, isto é, $< v_1, v_2 >= 0$.

Se

$$v_1 = aw_1 + bw_2$$

$$v_2 = cw_1 + dw_2,$$

onde a, b, c, $d \in \mathbb{Z}$ e $w_1 = (1,0)$, $w_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$, então podemos escrever $< v_1, v_2 >$ da seguinte forma:

$$\begin{aligned} < v_1, v_2 > &= \begin{bmatrix} a & b \end{bmatrix} . \begin{bmatrix} < w_1, w_1 > & < w_1, w_1 > \\ < w_2, w_1 > & < w_2, w_2 > \end{bmatrix} . \begin{bmatrix} c \\ d \end{bmatrix} \\ &= \begin{bmatrix} a & b \end{bmatrix} . \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix} . \begin{bmatrix} c \\ d \end{bmatrix} \end{aligned}$$

Observamos que a matriz acima dada pelo produto interno entre os vetores da base β é a matriz de Gram do reticulado A_2.

Sem perda de generalidade, podemos considerar $w_1 = (\sqrt{2}, 0)$ e $w_2 = \sqrt{2}.(\frac{1}{2}, \frac{\sqrt{3}}{2})$, de modo a tornar a matriz de Gram com coeficientes inteiros.

Logo,

$$
\begin{aligned}
< v_1, v_2 > &= \left[\begin{array}{cc} a & b \end{array}\right] . \left[\begin{array}{cc} 2 & 1 \\ 1 & 2 \end{array}\right] . \left[\begin{array}{c} c \\ d \end{array}\right] \\
&= \left[\begin{array}{cc} a & b \end{array}\right] . \left[\begin{array}{cc} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{-\sqrt{2}} & \frac{1}{\sqrt{2}} \end{array}\right] . \left[\begin{array}{cc} 1 & 0 \\ 0 & 3 \end{array}\right] . \left[\begin{array}{cc} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{array}\right] . \left[\begin{array}{c} c \\ d \end{array}\right] \\
&= \left[\begin{array}{cc} a & b \end{array}\right] \frac{1}{\sqrt{2}} \left[\begin{array}{cc} 1 & 1 \\ -1 & 1 \end{array}\right] . \left[\begin{array}{cc} 1 & 0 \\ 0 & 3 \end{array}\right] . \frac{1}{\sqrt{2}} \left[\begin{array}{cc} 1 & -1 \\ 1 & 1 \end{array}\right] . \left[\begin{array}{c} c \\ d \end{array}\right] \\
&= \left[\begin{array}{cc} \tilde{a} & \tilde{b} \end{array}\right] . \left[\begin{array}{cc} 1 & 0 \\ 0 & 3 \end{array}\right] . \left[\begin{array}{c} \tilde{c} \\ \tilde{d} \end{array}\right],
\end{aligned}
$$

onde $\left[\begin{array}{cc} \tilde{a} & \tilde{b} \end{array}\right] = \frac{1}{\sqrt{2}} \left[\begin{array}{cc} a-b & a+b \end{array}\right]$ e $\left[\begin{array}{cc} \tilde{a} & \tilde{b} \end{array}\right] = \frac{1}{\sqrt{2}} \left[\begin{array}{cc} c-d & c+d \end{array}\right]$.

Assim, $< v_1, v_2 >= 0 \Longleftrightarrow < (\tilde{a}, \tilde{b}), (\tilde{c}, 3\tilde{d}) >= 0 \Longrightarrow (\tilde{c}, 3\tilde{d}) = \lambda(-\tilde{b}, \tilde{a}) \Longrightarrow \left\{\begin{array}{l} \tilde{c} = -\lambda\tilde{b} \\ \tilde{d} = \frac{\lambda}{3}\tilde{a} \end{array}\right.$

$$
\begin{aligned}
\left[\begin{array}{c} c \\ d \end{array}\right] &= \frac{1}{\sqrt{2}} \left[\begin{array}{cc} 1 & 1 \\ -1 & 1 \end{array}\right] . \left[\begin{array}{c} \tilde{c} \\ \tilde{d} \end{array}\right] \\
&= \frac{1}{\sqrt{2}} \left[\begin{array}{cc} 1 & 1 \\ -1 & 1 \end{array}\right] . \left[\begin{array}{c} -\lambda\tilde{b} \\ \frac{\lambda}{3}\tilde{a} \end{array}\right] \\
&= \frac{\lambda}{\sqrt{2}} \left[\begin{array}{cc} 1 & 1 \\ -1 & 1 \end{array}\right] . \frac{1}{\sqrt{2}} \left[\begin{array}{c} -(a+b) \\ \frac{a-b}{3} \end{array}\right] \\
&= \frac{\lambda}{2} \left[\begin{array}{c} -a-b+\frac{a}{3}-\frac{b}{3} \\ a+b+\frac{a}{3}-\frac{b}{3} \end{array}\right] \\
&= \frac{\lambda}{2} \left[\begin{array}{c} \frac{-2}{3}a-\frac{4}{3}b \\ \frac{4}{3}a+\frac{2}{3}b \end{array}\right] \\
&= \frac{\lambda}{3} \left[\begin{array}{c} -(a+2b) \\ 2a+b \end{array}\right].
\end{aligned}
$$

- $\lambda = 3k$, $k \in \mathbb{Z}$ ou
- $3|(-(a+2b))$ e $3|(2a+b)$

Mas como, v_2 é solução, múltiplos dele com coordenadas inteiras na base $\{w_i\}$ também são soluções, obtemos o teorema a seguir:

Teorema 5.1.1. *Os sub-reticulados de A_2 que admitem uma base $\alpha = \{v_1, v_2\}$ ortogonal são da forma $\Lambda_\alpha =< v_1, v_2 >$, com*

$$v_1 = l_1 v_1^* \text{ e } v_2 = l_2 v_2^*, \quad l_1,\, l_2 \in \mathbb{Z}^*,$$

onde v_1^* e v_2^* podem ser das formas

i) $v_1^* = aw_1 + bw_2$, *com* $mdc(a,b) = 1$ *e*

$$\begin{cases} v_2^* = -(a+2b)w_1 + (2a+b)w_2, \\ ou \\ v_2^* = -\dfrac{(a+2b)}{3}w_1 + \dfrac{(2a+b)}{3}w_2, \text{ caso } 3|(-(a+2b)) \text{ e } 3|(2a+b). \end{cases}$$

ii) $v_1^* = w_1$ *e* $v_2^* = -w_1 + 2w_2$

iii) $v_1^* = w_2$ *e* $v_2^* = -2w_1 + w_2$

Chamaremos de *geradores primitivos* os vetores v_1^* e v_2^* do teorema acima.

Sobre o número de pontos do quociente de reticulados e do código esférico associado temos:

Para geradores do tipo i)

$$\#\left(\frac{\Lambda_\beta}{\Lambda_\alpha}\right) = l_1 l_2 \left| det \begin{bmatrix} a & -(a+2b) \\ b & 2a+b \end{bmatrix} \right| = l_1 l_2 (2a^2 + ab + ab + 2b^2)$$
$$= l_1 l_2 (2a^2 + 2ab + 2b^2) = 2 l_1 l_2 (||v_1^*||^2).$$

ou

$$\#\left(\frac{\Lambda_\beta}{\Lambda_\alpha}\right) = l_1 l_2 \left| det \begin{bmatrix} a & \frac{-(a+2b)}{3} \\ b & \frac{2a+b}{3} \end{bmatrix} \right| = \frac{l_1 l_2}{3}(2a^2 + ab + ab + 2b^2)$$
$$= \frac{l_1 l_2}{3}(2a^2 + 2ab + 2b^2) = \frac{2 l_1 l_2}{3}(||v_1^*||^2).$$

Para geradores do tipo ii)

$$\#\left(\frac{\Lambda_\beta}{\Lambda_\alpha}\right) = l_1 l_2 \left| det \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} \right| = 2 l_1 l_2.$$

Para geradores do tipo iii)

$$\#\left(\frac{\Lambda_\beta}{\Lambda_\alpha}\right) = l_1 l_2 \left| det \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \right| \;\; = \;\; 2l_1 l_2.$$

Observação 5.1.1. *Observamos, portanto que este número é sempre par, e que para qualquer número par $2k$, $k \in \mathbb{Z}$ existe um sub-reticulado "retangular" de A_2 de cada um dos tipos definidos acima tal que $\#\left(\frac{\Lambda_\beta}{\Lambda_\alpha}\right) = 2k$.*

Analisaremos os reticulados provindos de geradores primitivos do tipo **i)**, e mais adiante nos restringiremos aos do tipo **i)** onde, $v_2^* = -(a+2b)w_1 + (2a+b)w_2$.

Teorema 5.1.2. *Nas condições do Teorema (5.1.1), assumimos sub-reticulados do tipo (i) e $mdc(l_1, l_2) = 1$. O grupo associado ao quociente de reticulados $\frac{A_2}{< v_1, v_2 >}$ será cíclico se, e somente se, na forma normal de Smith de $A = (a_{ij})$ correspondente ao sub-reticulado "retangular" existe a_{kl} tal que $3 \not| a_{kl}$.*

Demonstração: Afirmação: A forma normal de Smith de uma matriz 2×2, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ é do tipo

$$D = \begin{bmatrix} 1 & 0 \\ 0 & det(A) \end{bmatrix} \tag{5.1}$$

se, e somente se, $mdc(a_{11}, a_{12}, a_{21}, a_{22}) = 1$.

De fato, suponhamos que $mdc(a_{11}, a_{12}, a_{21}, a_{22}) = k > 1$, então $A = k.\tilde{A}$. A forma normal de Smith de $\tilde{A}$ é

$$P\tilde{A}Q = \tilde{D}$$
$$kP\tilde{A}Q = k\tilde{D}$$
$$Pk\tilde{A}Q = k\tilde{D}$$
$$PAQ = k\tilde{D}$$

e portanto a forma normal de Smith de A não é do tipo (5.1).

Reciprocamente, se a forma normal de Smith de uma matriz não tem o número 1 na posição d_{11}, temos que $D = d_{11}\tilde{D}$. Analisando a forma normal de Smith de A, temos $PAQ =$

D. Logo,

$$PAQ = d_{11}\tilde{D}$$
$$A = d_{11}P^{-1}\tilde{D}Q^{-1}$$

e portanto $mdc(a_{11}, a_{12}, a_{21}, a_{22}) \neq 1$.

Agora, procuramos inicialmente pela forma normal de Smith da matriz A do tipo **i)**,

$$A = \tilde{A}_1 \begin{bmatrix} l_1 a & -l_2(a+2b) \\ l_1 b & l_2(2a+b) \end{bmatrix} \quad ou \quad A = \tilde{A}_2 \begin{bmatrix} l_1 a & \frac{-l_2(a+2b)}{3} \\ l_1 b & \frac{l_2(2a+b)}{3} \end{bmatrix}$$

com $mdc(a,b) = 1$ *e* $mdc(l_1, l_2) = 1$.

Analisamos, primeiramente, o caso $A = \tilde{A}_1$.

Suponhamos p primo, $(p \neq 1)$ e p dividindo todos os elementos da matriz.

Temos que,

- $p|l_1$

  De fato, $p|l_1 a$ e $p|l_1 b$, como $mdc(a,b) = 1 \Longrightarrow p|l_1$.

- $p \not| l_2$

  De fato, $mdc(l_1, l_2) = 1$.

  Logo, $p|(a+2b)$ e $p|(2a+b) \Longrightarrow \begin{cases} a+2b = pk_1,\ k_1 \in \mathbb{Z} \\ 2a+b = pk_2,\ k_2 \in \mathbb{Z} \end{cases} \Longrightarrow \begin{cases} 2a+4b = 2pk_1 \\ -2a-b = -pk_2 \end{cases} \Longrightarrow$

  $3b = p(2k_1 - k_2) \Longrightarrow b = \dfrac{p(2k_1 - k_2)}{3}$.

De $a + 2b = pk_1$ temos

$$3pk_1 = 3a + 2(3b) = 3a + 2p(2k_1 - k_2) \Longrightarrow 3a = p(2k_2 - k_1).$$

Se $p \neq 3$ então $p|a$ e $p|b$, contradição pois $mdc(a,b) = 1$. Logo, $p = 3$.

Agora, analisamos o caso $A = \tilde{A}_2$.

Novamente, suponhamos p primo, $(p \neq 1)$ e p dividindo todos os elementos da matriz.

Temos que,

- $p|l_1$

  De fato, $p|l_1 a$ e $p|l_1 b$, como $mdc(a,b) = 1 \Longrightarrow p|l_1$.

- $p \not| l_2$

  De fato, $mdc(l_1, l_2) = 1$.

  Logo, $p|\frac{(a+2b)}{3}$ e $p|\frac{(2a+b)}{3} \Longrightarrow \begin{cases} a+2b = p3k_1,\ k_1 \in \mathbb{Z} \\ 2a+b = p3k_2,\ k_2 \in \mathbb{Z} \end{cases} \Longrightarrow \begin{cases} 2a+4b = 6pk_1 \\ -2a-b = -3pk_2 \end{cases} \Longrightarrow$
  $3b = 3p(2k_1 - k_2) \Longrightarrow b = p(2k_1 - k_2)$.

Substituindo,

$$a + 2p(2k_1 - k_2) = 3pk_1 \Longrightarrow a = p(k_1 - 2pk_2).$$

O que é absurdo, pois $mdc(a, b) = 1$. Logo, $\exists\, i,\ j$ tal que $p \not| a_{ij}$, $i, j = 1, 2$, e portanto, $mcd(a_{11}, a_{12}, a_{13}, a_{14}) = 1$, o que implica que o grupo correspondente é cíclico. ◪

Neste trabalho, consideramos os sub-reticulados do tipo (i) do Teorema (5.1.1), com

$$v_1^* = aw_1 + bw_2 \text{ e } v_2^* = -(a+2b)w_1 + (2a+b)w_2.$$

Estes sub-reticulados apresentam melhor desempenho quando mergulhados nos toros planares de esferas no $\mathbb{R}^4$ quando satisfazem:

1. $||v_1^*|| \approx ||v_2^*||$, **ou seja, a "caixa" que define o toro está mais próxima de ser "quadrada".**

   $||v_1^*||^2 = a^2 + ab + b^2$

   $||v_2^*||^2 = \frac{3}{4}(2a+b)^2 + \left(-a - 2b + \frac{1}{2}(2a+b)\right)^2 = 3a^2 + 3b^2 + 3ab.$

   Portanto, $||v_2^*||^2 = 3||v_1^*||^2$. Logo, os bons tamanhos ocorrerão quando tomarmos $v_1 = l_1 v_1^*$ e $v_2 = l_2 v_2^*$ com $\dfrac{|l_1|}{|l_2|} \approx \sqrt{3} \approx 1,73205$. Ou seja, o sub-reticulado estará mais próximo de ser "quadrado" se satisfizer esta condição.

2. **Maior ângulo mínimo entre os vetores de A_2 e os vetores v_1 e v_2.**

   Considerando que a "caixa" seja "quadrada", temos que devido à simetria no eixo x basta considerar $a > b > 0$ e assim o ângulo entre v_1 e w_1 é menor do que 30^o. A situação ótima ocorre quando $\theta = 15^o$ (maior ângulo mínimo - ângulos iguais entre v_1 e w_1 e entre v_2 e w_2).

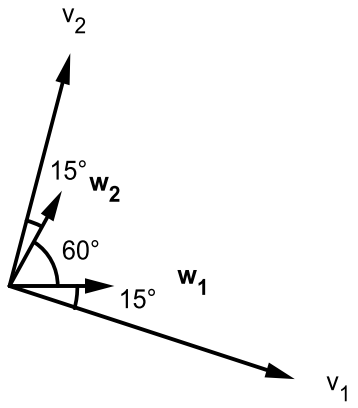


Figura 5.1: **Ângulo**

Vamos estabelecer a condição algébrica para que este ângulo seja 15^o, ou seja, $\frac{\pi}{12}$.

Sabemos que $\cos(\frac{\pi}{12}) = \frac{1+\sqrt{3}}{2\sqrt{2}}$ e que $\cos\theta = \cos\angle_{v_1,w_1} = \dfrac{2a+b}{\sqrt{2}\sqrt{2a^2+2ab+2b^2}} = \dfrac{2a+b}{2\sqrt{a^2+b^2+ab}}$.

O ângulo mínimo é maior possível $\iff \cos\theta = \cos(\frac{\pi}{12})$.

Logo, $\dfrac{2a+b}{\sqrt{2}\sqrt{2a^2+2ab+2b^2}} = \dfrac{1+\sqrt{3}}{2\sqrt{2}} \iff \dfrac{(2a+b)^2}{4(a^2+ab+b^2)} = \left(\dfrac{1+\sqrt{3}}{2\sqrt{2}}\right)^2 \iff (2a+b)^2 = 4(a^2+b^2+ab)\left(\dfrac{1+\sqrt{3}}{2\sqrt{2}}\right)^2$.

Supondo $b \neq 0$, seja $k = \dfrac{a}{b}$. Dividindo a última igualdade por b^2 dos dois lados, temos:

$(2k+1)^2 = 4(k^2+1+k).\left(\dfrac{1+\sqrt{3}}{2\sqrt{2}}\right)^2 \implies k = -2-\sqrt{3}$ ou $k = 1+\sqrt{3}$.

Como estamos considerando $a > b > 0$, a solução válida é $k = 1+\sqrt{3} \approx 2,73205$.

Portanto, o ângulo mínimo é o maior possível para $\dfrac{a}{b} = 1+\sqrt{3}$.

No que segue, analisamos o código esférico gerado pela aplicação ψ definida no retângulo gerado pela base v_1, v_2 como é descrita no Capítulo 4.

Mostraremos uma condição suficiente para que a distância mínima nos códigos esféricos gerados por grupos comutativos construídos em $\mathbb{R}^4$ seja atingida pela imagem de um dos

vetores de norma mínima, obtidos a partir da base que gera o reticulado A_2. Antes, porém, fazemos as seguintes observações:

1. $\operatorname{sen} x \geq x - \dfrac{x^3}{3!}$, $\forall\, x \geq 0$.
2. O reticulado $\Lambda_\beta = A_2$ possui 6 vetores de norma mínima, 1, obtidos a partir da base que o gera: w_1, w_2, $w_3 = -w_1 + w_2$ e seus simétricos.

Denotaremos o conjunto destes vetores por w_{min}. Notamos que se $\tilde{w} \in \Lambda$, $\tilde{w} \in w_{min}$, então

$$||\tilde{w}|| \geq \sqrt{3} \text{ (segunda maior norma neste reticulado).} \tag{5.2}$$

Proposição 5.1.1. *Se* $v_{min} = \min\{||v_1||, ||v_2||\} \geq \dfrac{\sqrt[4]{3}\pi}{\sqrt{2(\sqrt{3}-1)}} \approx 3,417$ *então a distância mínima no código esférico em* $\mathbb{R}^4$*, definida por* ψ *(4.5), é atingida por algum* $\psi(w)$*, onde* $||w|| = 1$, $w \in \Lambda_\beta$*, tem norma mínima.*

Demonstração: Suponhamos inicialmente que $v_{min} = 2\pi\delta_{min} > 1$. Da Proposição (4.3.1), temos que $d(\psi(w), \psi(0)) < d(w, 0) = 1$ para $w \in w_{min}$.

Seja agora $\tilde{w} \in \Lambda_\beta$ tal que $||\tilde{w}|| > 1 \Rightarrow ||\tilde{w}|| \geq \sqrt{3}$ (5.2). Pela Proposição (4.3.1),

$$\begin{aligned} d(\psi(\tilde{w}), \psi(0)) &\geq 2\delta_{min} \operatorname{sin}\left(\frac{r}{2\delta_{min}}\right) = 2\frac{v_{min}}{2\pi} \operatorname{sin}\left(\frac{\sqrt{3}}{\frac{2v_{min}}{2\pi}}\right) = \frac{v_{min}}{\pi} \operatorname{sin}\left(\frac{\sqrt{3}\pi}{v_{min}}\right) \\ &\geq \frac{v_{min}}{\pi}\left(\frac{\sqrt{3}\pi}{v_{min}} - \left(\frac{\sqrt{3}\pi}{v_{min}}\right)^3 \frac{1}{3!}\right) = \sqrt{3} - \frac{\sqrt{3}\pi^2}{2v_{min}^2}. \end{aligned}$$

Queremos saber quando $\sqrt{3} - \dfrac{\sqrt{3}\pi^2}{2v_{min}^2} \geq 1$. Seja $x = v_{min}$. Temos então $2(\sqrt{3}-1)x^2 - \sqrt{3}\pi^2 \geq 0$; $x > 0$, e então a inequação é satisfeita para $x > \dfrac{\sqrt[4]{3}\pi}{\sqrt{2(\sqrt{3}-1)}} \approx 3,417$, donde concluímos a proposição. ∎

Observação 5.1.2. *Quando* $v_{min} < 3,417$*, temos que para caixas aproximadamente quadradas, isto é,* $||v_1|| \approx ||v_2||$*, onde* v_1 *e* v_2 *são ortogonais entre si,*

$$M = \frac{|Vol(\Lambda_\alpha)|}{|Vol(\Lambda_\beta)|} \approx \frac{||v_i||^2}{\frac{\sqrt{3}}{2}} < \frac{2(3,417)^2}{\sqrt{3}} = 13,4822 < 14.$$

Ou seja, neste caso a Proposição (5.3.1) só não será válida para um número de pontos menor do que 14. Como procuramos por códigos esféricos que sejam mais próximos do limitante da Proposição (4.4.4), temos que de acordo com as considerações finais do Capítulo 4, isto acontecerá para valores grandes de M.

Exemplo 5.1.1. *Considere* $a = 273$, $b = 100$. *Logo,* $c = -(a + 2b) = -473$ *e* $d = 2a + b = 646$. *Observe que* $mdc(a, b) = 1 = mdc(c, d)$. *Portanto estes são geradores primitivos do reticulado* Λ_α. *Assim temos,*

$$\begin{aligned} v_1^* &= \ 273w_1 + 100w_2 \\ v_2^* &= -473w_1 + 646w_2, \end{aligned}$$

e para cada $\delta_i = \dfrac{||v_i||}{2\pi}$, $i = 1, 2$, *o código esférico tem por vetor inicial* $u = (\delta_1, 0, \delta_2, 0)$ *e* $M = |det(A)| = \left| det \begin{pmatrix} 273 & -473 \\ 100 & 646 \end{pmatrix} \right| = 223658$ *pontos.*

Calculando a forma normal de Smith, chegamos na matriz diagonal $\begin{bmatrix} 1 & 0 \\ 0 & 223658 \end{bmatrix}$ *e na matriz* $P^{-1} = \begin{bmatrix} 273 & 101 \\ 100 & 37 \end{bmatrix}$. *Logo, pelo Teorema (4.2.4),* $G \simeq \mathbb{Z}_{223658}$ *e o elemento* $\overline{101w_1 + 37w_2}$ *é um elemento de ordem 223658.*

Agora, para este sub-reticulado de A_2 *ter um melhor desempenho, procuramos:*

1. $k = \dfrac{a}{b} \approx 2,73205.$

2. $v_1 = l_1 v_1^*,\ v_2 = l_2 v_2^*$ *com* $\dfrac{|l_1|}{|l_2|} = \sqrt{3} \approx 1,73205.$

Vemos que a primeira condição é satisfeita, pois $\frac{273}{100} \approx 2,73205$. *Agora, para a segunda condição tomando, por exemplo,* $l_1 = 7$ *e* $l_2 = 4$, *temos que* $\dfrac{7}{4} = 1,75 \approx \sqrt{3}$.

Assim, para que o desempenho do sub-reticulado seja bom, vamos considerar

$$\begin{aligned} v_1 &= 7v_1^* \\ v_2 &= 4v_2^*. \end{aligned}$$

Agora, $a = 1911$, $b = 700$, $c = -1892$ *e* $d = 2584$.

Assim, $M = |det(A)| = \left| det \begin{pmatrix} 1911 & -1892 \\ 700 & 2584 \end{pmatrix} \right| = 6262424$. *Pelo Teorema (4.2.4),* $G \cong \mathbb{Z}_{6262424}$ *e o elemento* $\overline{81w_1 + 299w_2}$ *é um elemento de ordem 6262424. Portanto* $\overline{81w_1 + 299w_2}$ *gera o grupo G.*

Escrevendo os vetores de norma mínima em relação à base de Λ_α*, temos que*

$$\begin{cases} w_1 = \dfrac{646.v_1 - 175.v_2}{1565606} \\ \\ w_2 = \dfrac{1892.v_1 + 1911.v_2}{6262424} \\ \\ w_3 = \dfrac{-692.v_1 + 2611.v_2}{6262424} \end{cases}$$

Logo, por (4.7),

$$\begin{aligned} d_{min} = \min_{\neq 0}\{d(\psi(w_i), \psi(\mathbf{0})) &= \frac{2}{\sqrt{||v_1||^2 + ||v_2||^2}} \sqrt{\sum_{j=1}^{2} ||v_j||^2 \sin^2\left(\pi \frac{w_{ij}}{||v_i||}\right)},\ i = 1, \cdots, 3\} \\ &= \min_{\neq 0}\{0.00190773, 0.00190773, 0.00190773\} = 0.00190773. \end{aligned}$$

Calculando o limitante da Proposição (4.4.4), obtemos que a $d_{min} \leq 0.00190778$*, uma diferença de apenas* 0.00000005*. Logo, este código está próximo do limitante, para* 6262424 *pontos.*

Observamos que se tivéssemos calculado a distância mínima sem a exigência do ângulo e da norma obteríamos $d_{min} = 0.00939436$ *e o limitante* ≤ 0.010095 *para* 223658 *pontos, uma diferença de* 0.000700655.

Dados M e n, em [11], Biglieri e Elia mostram que o número de casos que devemos verificar para encontrar o código ótimo para grupos cíclicos é da ordem de $\begin{pmatrix} M/2 \\ n/2 \end{pmatrix}$. Para grupos abelianos gerais este número é ainda muito maior. Processos de busca, a partir de isometrias como de [42] reduzem bastante este número, no entanto, um limitante inferior para o número total de casos a serem analisados para os comutativos gerais é ainda da ordem dada acima.

A medida que o número de pontos aumenta, o número de operações envolvidas inviabiliza o cálculo, assim, para um número muito grande de pontos ou em dimensões mais altas, ainda não se sabe qual é o código ótimo.

O método que propomos neste trabalho, permite calcular diretamente um vetor inicial, distância mínima, geradores e grupo para códigos que são ótimos ou estão muito próximos destes sem a necessidade de analisar casos.

No exemplo acima, para 6262424 pontos, devem ser analisados aproximadamente 4.902.242.728.866 casos em uma busca exaustiva.

Exemplo 5.1.2. *Considere* $a = 3$, $b = -1$. *Logo,* $c = -(a + 2b) = -1$ *e* $d = 2a + b = 5$. *Observe que* $mdc(a, b) = 1 = mdc(c, d)$. *Portanto estes são geradores primitivos do reticulado* Λ_α. *Assim temos*

$$v_1^* = 3w_1 - 1w_2$$
$$v_2^* = -1w_1 + 5w_2.$$

O número de pontos é $M = |det(A)| = \left| det \begin{pmatrix} 3 & -1 \\ -1 & 5 \end{pmatrix} \right| = 14$. *Usando a forma normal de Smith, chegamos na matriz diagonal* $\begin{bmatrix} 1 & 0 \\ 0 & 14 \end{bmatrix}$ *e na matriz* $P^{-1} = \begin{bmatrix} -1 & 0 \\ 5 & 1 \end{bmatrix}$. *Logo, pelo Teorema (4.2.4)* $G \simeq \mathbb{Z}_{14}$ *e o elemento* $\overline{w_2}$ *é um elemento de ordem 14. Portanto,* $\overline{w_2}$ *gera o grupo* $G \simeq \frac{\Lambda_\beta}{\Lambda_\alpha}$.

Temos que $A^{-1} = \begin{pmatrix} \frac{5}{14} & \frac{1}{14} \\ \frac{1}{14} & \frac{3}{14} \end{pmatrix}$ *e portanto* $w_2 = \frac{1}{14}v_1 + \frac{3}{14}v_2$, *que é associado à matriz geradora do grupo comutativo de matrizes ortogonais* 4×4, $\tilde{O}_2 = [R_1, R_2] = \left[R\left(2\pi\frac{1}{14}\right), R\left(2\pi\frac{3}{14}\right) \right]$.

Para cada $\delta_i = \frac{||v_i||}{2\pi}$, $i = 1, 2$ *o código esférico associado tem por vetor inicial* $u = (\delta_1, 0, \delta_2, 0)$. *O código de grupo* $G(u)$ *será gerado por rotações* 2×2, R_i, *nos pares* $(\delta_i, 0)$, $i = 1, 2$.

Observamos que $||v_1^*|| \approx 2,64575$ *e* $||v_2^*|| \approx 4,58258$, *logo,* $||v_{min}|| \approx 2,64575 < 3,417$. *Não podemos portanto utilizar a Proposição (5.1.1) para garantir que a distância mínima será obtida pela imagem de algum vetor de norma mínima através da função* ψ *(4.3). Deste*

modo, calculamos a distância mínima comparando todas as distâncias dos 14 pontos da imagem.

Fazendo o quociente de $\frac{\Lambda_\beta}{\Lambda_\alpha}$ *temos o grafo no toro planar* T_α*, Figura (5.2).*

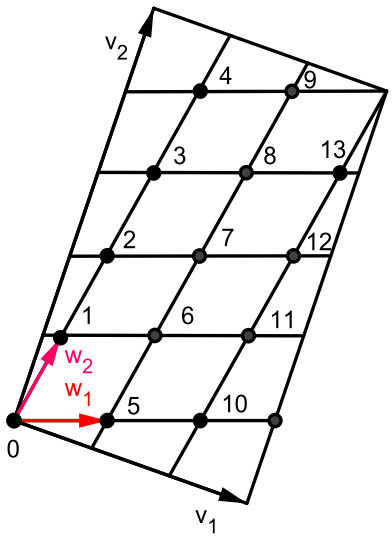


Figura 5.2: **Grafo no toro planar**

Agora, para sabermos os pontos do código esférico, basta calcularmos a imagem dos vértices do grafo no toro planar. Aplicando a função μ_α *definida em (4.4) no gerador* $\overline{w_2}$ *encontramos que o grafo no toro planar* T_α *tem 14 vértices, a saber*

$p_0 = (0,0)$	$p_4 = (2, 2\sqrt{3})$	$p_8 = (\frac{5}{2}, \frac{3\sqrt{3}}{2})$	$p_{12} = (3, \sqrt{3})$
$p_1 = (\frac{1}{2}, \frac{\sqrt{3}}{2}) = w_2$	$p_5 = (1,0) = w_1$	$p_9 = (3, 2\sqrt{3})$	$p_{13} = (\frac{7}{2}, \frac{3\sqrt{3}}{2})$
$p_2 = (1, \sqrt{3})$	$p_6 = (\frac{3}{2}, \frac{\sqrt{3}}{2})$	$p_{10} = (2,0)$	
$p_3 = (\frac{3}{2}, \frac{3\sqrt{3}}{2})$	$p_7 = (2, \sqrt{3})$	$p_{11} = (\frac{5}{2}, \frac{\sqrt{3}}{2})$	

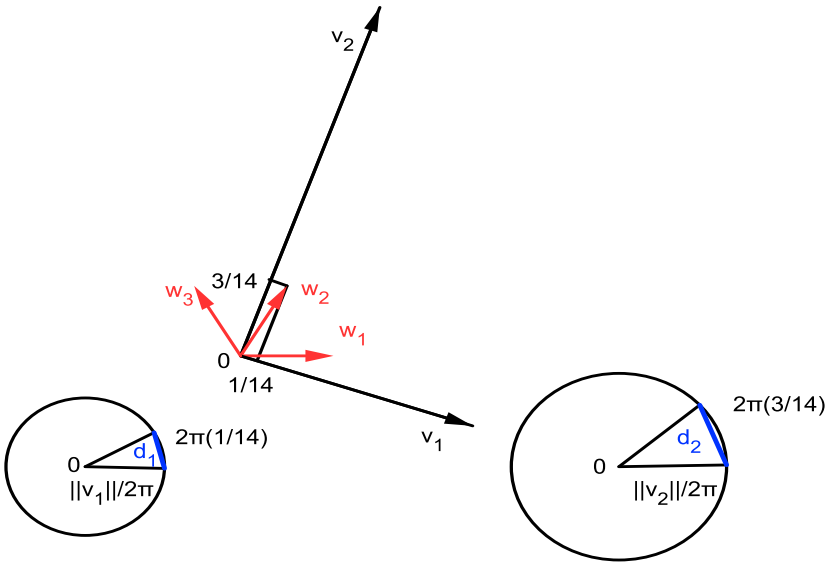
Observamos que w_1 *também gera* G.

Por (4.7),

$$d_{min} = \min\{d(\psi(p_0), \psi(p_i)),\ 1 \leq i \leq 13\} = 0,979945 = d(\psi(p_0), \psi(p_1)) = d(\psi(p_0), \psi(p_{10})).$$

Observação 5.1.3. *Por (4.7), calculamos aqui a distância mínima na esfera unitária, já normalizando os vetores, isto é,* $\sum_{i=1}^{2}\left(\frac{||v_i||}{2\pi}\right)^2 = 1$.

Geometricamente podemos visualizar, por exemplo, a distância mínima na imagem; entre as imagens do vetor $w_2 = \frac{1v_1 + 3v_2}{14}$ *e do vetor* $(0,0)$*, como a raiz quadrada da soma dos quadrados das cordas em dois círculos, Figura(5.3).*



$$\mathbf{d^2(\psi(w_2),\psi(0))=d_1^2+d_2^2}$$

Figura 5.3: **Visualização da distância mínima**

Calculando o limitante da Proposição (4.4.4), obtemos que a $d_{min} \leq 1,25443$*, uma diferença de* $0,274481$*. Logo, este código esta longe do limitante para* 14 *pontos.*

Uma das razões disto é o fato de que as condições (1) e (2) não são satisfeitas:

$$||v_1^*|| = 2,64575 \not\approx ||v_2^*|| = 4,58258 \quad e \quad \left|\frac{a}{b}\right| = \left|\frac{3}{-1}\right| = 3 \not\approx 2,73205.$$

Alguns valores de l_1 e l_2 que satisfazem a condição (1) e alguns valores de a e b que satisfazem a condição (2) são listados na Tabela (5.1).

l_1	l_2
26	15
45	26
52	30
57	33
59	34
64	37
71	41
78	45
90	52

a	b
11	4
19	7
30	11
41	15
52	19
60	22
71	26
82	30
90	33

Tabela 5.1: **Alguns valores de l_1, l_2 e a, b.**

A Tabela (5.2) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^4$ e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4). A tabela apresenta também, de acordo com [11], o número total de casos que deveriam ser aproximadamente analisados.

M	d_{min}	δ_1	δ_2	Limitante	Grupo	Casos [11]
141180	0.012706	0.707368	0.706845	0.0127061	$\mathbb{Z}_{141180}$	2.491.438.755
423540	0.00733585	0.707368	0.706845	0.00733588	$\mathbb{Z}_{423540}$	22.423.160.565
1053780	0.00465076	0.707368	0.706845	0.00465077	$\mathbb{Z}_{1053780}$	138.806.272.605
1270620	0.00423537	0.706845	0.707368	0.00423537	$\mathbb{Z}_3 \oplus \mathbb{Z}_{423540}$	201.809.080.395

Tabela 5.2: **Comparação entre a distância mínima de códigos de grupo comutativo em $\mathbb{R}^4$ e o limitante da Proposição (4.4.4).**

Observamos que a distância mínima esta muito próxima do limitante.

5.2 Construção dos reticulados D_n e E_8

Existem várias relações entre códigos e reticulados. Nesta seção, apresentamos apenas umas delas, chamada "*construção A*", dada em [14] e [19]. Essa construção será importante para construirmos famílias de sub-reticulados dos reticulados D_n e E_8.

A aplicação

$$\begin{aligned} \phi : \mathbb{Z}^n &\longrightarrow \mathbb{Z}_2^n \\ (a_1, \cdots, a_n) &\longmapsto (\overline{a_1}, \cdots, \overline{a_n}) \end{aligned}$$

é sobrejetora e satisfaz a condição

$$\phi(u+v) = \phi(u) + \phi(v), \ \forall\, u,\, v \in \mathbb{Z}^n,$$

isto é, é um homomorfismo de grupos.

Isto faz com que a cada código binário linear C seja associado um reticulado, o reticulado $\Lambda(C) = a\phi^{-1}(C)$, onde $a > 0$ é uma constante escolhida de modo conveniente.

Se C_n é o código

$$C_n = \{(x_1, x_2, \cdots, x_n) \in \mathbb{Z}_2^n;\ \sum_{i=1}^{n} x_i = 0\}, \tag{5.3}$$

de parâmetros $[n, n-1, 2]$, então o reticulado D_n é igual a $\Lambda(C_n) = \phi^{-1}(C_n)$. (aqui, tomaremos o escalar $a = 1$), [19].

Como exemplo, se considerarmos a seguinte versão do código de Hamming H_3 com parâmetros $[7, 4, 3]$: o código definido como o núcleo da transformação linear dada pela matriz,

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

Estendemos agora H_3 a um código $\tilde{H}_3$ de comprimento 8, por

$$(x_1, x_2, \cdots, x_7, (x_1 + \cdots + x_7)), \tag{5.4}$$

onde $(x_1, x_2, \cdots, x_7)$ está em H_3.

Como pode ser visto em [19], a *construção A* a partir de $\tilde{H}_3$ gera E_8, isto é, $E_8 = \Lambda(\tilde{H}_3) = \frac{1}{\sqrt{2}}\phi^{-1}(\tilde{H}_3)$.

Um resultado importante que nos fornece uma família de sub-reticulados de $\Lambda(C)$ é dado pela seguinte proposição que será utilizada nas próximas seções.

Proposição 5.2.1. *([19],[14]) O reticulado $2a\mathbb{Z}^n$ sempre está contido em $\Lambda(C)$.*
Demonstração: Seja $x \in 2a\mathbb{Z}^n$. Assim existem $x_1, \cdots, x_n \in \mathbb{Z}$ tais que $x = 2a(x_1, \cdots, x_n) = a(2x_1, \cdots, 2x_n)$. Devemos provar que $x \in a\phi^{-1}C$, ou seja, $x = ay$, onde $y \in \phi^{-1}(C)$, e por conseguinte, $c = \phi(y)$, para algum $c \in C$. De fato, $\phi(2x_1, \cdots, 2x_n) = (0, \cdots, 0)$, logo, $x \in \Lambda(C) = a\phi^{-1}(C)$. ∎

Podemos agora obter códigos esféricos a partir de sub-reticulados gerados por $2a\mathbb{Z}^n$, $a > 0$.

5.3 Sub-reticulados "retangulares" de D_3

5.3.1 Sub-reticulados "retangulares" de D_3 gerados por $2\mathbb{Z}^n$

Para $n = 3$, temos que $\alpha = \{(2,0,0),(0,2,0),(0,0,2)\}$ é uma base de $2\mathbb{Z}^3 = \Lambda_\alpha$. Agora consideremos $\beta = \{(1,-1,0),(-1,-1,0),(0,1,-1)\}$ a base de $D_3 = \Lambda_\beta$ obtido pela *construção A* do código C_3 (5.3). Pela Proposição (5.2.1), Λ_α é um sub-reticulado de Λ_β. Observamos que os vetores de α são mutuamente ortogonais e portanto conjunto de sinais 3-dimensionais no toro planar gerados por D_3 definirão códigos esféricos 6-dimensionais.

Sejam

$$\begin{aligned} v_1 &= (2,0,0) \qquad & w_1 &= (1,-1,0) \\ v_2 &= (0,2,0) \qquad & w_2 &= (-1,-1,0) \\ v_3 &= (0,0,2) \qquad & w_3 &= (0,1,-1) \end{aligned}$$

Observamos que como $||v_1|| = ||v_2|| = ||v_3||$ o paralelepípedo que define o toro através de ψ (4.3) forma um cubo.

O reticulado $\Lambda_\beta = D_3$ possui 12 vetores de norma mínima, $\sqrt{2}$, obtidos a partir da base que o gera: w_1, w_2, w_3, $w_4 = -w_2 - w_3$, $w_5 = w_1 + w_3$, $w_6 = -w_1 - w_2 - w_3$ e seus

simétricos, onde $||w_{min}|| = \sqrt{2}$. Denotaremos o conjunto destes vetores por w_{min}. Notamos que se $\tilde{w} \in \Lambda$, $\tilde{w} \in w_{min}$, então

$$||\tilde{w}|| \geq 2 \text{ (segunda maior norma neste reticulado).} \tag{5.5}$$

Mostraremos agora que a distância mínima no código esférico em $\mathbb{R}^6$ é obtida pela imagem de um destes vetores de norma mínima, dentro de certas condições.

Proposição 5.3.1. *Se* $v_{min} = \min\{||v_1||, ||v_2||, ||v_3||\} \geq \dfrac{2\pi}{\sqrt{3(2-\sqrt{2})}} \approx 4,73969$ *então a distância mínima no código esférico em* $\mathbb{R}^6$*, definida por* ψ *(4.5), é atingida por algum* $\psi(w)$*, onde* $||w|| = \sqrt{2}$*,* $w \in \Lambda_\beta$*, tem norma mínima.*

Demonstração: Suponhamos inicialmente que $v_{min} = 2\pi\delta_{min} > \sqrt{2}$. Da Proposição (4.3.1), temos que $d(\psi(w), \psi(0)) < d(w, 0) = \sqrt{2}$ para $w \in w_{min}$.

Seja agora $\tilde{w} \in \Lambda_\beta$ tal que $||\tilde{w}|| > \sqrt{2} \Rightarrow ||\tilde{w}|| \geq 2$ (5.5). Pela Proposição (4.3.1),

$$\begin{aligned} d(\psi(\tilde{w}), \psi(0)) &\geq 2\delta_{min} \sin\left(\frac{r}{2\delta_{min}}\right) = 2\frac{v_{min}}{2\pi} \sin\left(\frac{2}{\frac{2v_{min}}{2\pi}}\right) = \frac{v_{min}}{\pi} \sin\left(\frac{2\pi}{v_{min}}\right) \\ &\geq \frac{v_{min}}{\pi}\left(\frac{2\pi}{v_{min}} - \left(\frac{2\pi}{v_{min}}\right)^3 \frac{1}{3!}\right) = 2 - \frac{4\pi^2}{3v_{min}^2}. \end{aligned}$$

Queremos saber quando $2 - \frac{4\pi^2}{3v_{min}^2} \geq \sqrt{2}$. Seja $x = v_{min}$. Temos então $3(2-\sqrt{2})x^2 - 4\pi^2 \geq 0$; $x > 0$, e então a inequação é satisfeita para $x > \dfrac{2\pi}{\sqrt{3(2-\sqrt{2})}} \approx 4,73969$, donde concluímos a proposição. ∎

Observação 5.3.1. *Quando* $v_{min} < 4,73969$*, temos que, para caixas aproximadamente cúbicas, isto é,* $||v_1|| \approx ||v_2|| \approx ||v_3||$*,*

$$M = \frac{|Vol(\Lambda_\alpha)|}{|Vol(\Lambda_\beta)|} \approx \frac{||v_i||^3}{2} < \frac{(4,73969)^3}{2} = 53,2378 < 54.$$

Ou seja, neste caso a Proposição (5.3.1) só não será válida para um número de pontos menor que 54. Como procuramos por códigos esféricos que sejam mais próximos do limitante da Proposição (4.4.4), temos que de acordo com as considerações finais do Capítulo 4, isto acontecerá para valores grandes de M.

Ilustramos o caso $l = 1$, embora este exemplo não seja substancial pois 4 pontos estão sempre contidos num espaço afim tridimensional.

O sistema

$$v_1 = k_1w_1 + k_2w_2 + k_3w_3$$
$$v_2 = k_4w_1 + k_5w_2 + k_6w_3$$
$$v_3 = k_7w_1 + k_8w_2 + k_9w_3$$

onde $k_i \in \mathbb{Z}$, $i = 1, \cdots, 9$ tem como solução $k_1 = 1$, $k_2 = -1$, $k_3 = 0$, $k_4 = -1$, $k_5 = -1$, $k_6 = 0$, $k_7 = -1$, $k_8 = -1$, $k_9 = -2$.

Desta forma

$$v_1 = 1.w_1 - 1.w_2 + 0.w_3$$
$$v_2 = -1.w_1 - 1.w_2 + 0.w_3$$
$$v_3 = -1.w_1 - 1.w_2 - 2.w_3$$

e

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

Como $|detA| = 4$, obtemos um código esférico com 4 pontos no $\mathbb{R}^6$.

Tomando $\tilde{v}_1 = lv_1$, $\tilde{v}_2 = lv_2$ e $\tilde{v}_3 = lv_3$, com $l \in \mathbb{Z}^*$ é possível gerar uma família de reticulados quocientes com $|4l^3|$ pontos.

Calculando a forma normal de Smith da matriz A obtemos

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

e, pelo Teorema (4.2.4), $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ e $< \overline{-w_2}, \overline{-w_3} >$ são os geradores do grupo.

Como $M = 4 < 54$, não podemos garantir, pela Proposição (5.1.1), que a distância mínima será obtida pela imagem de algum vetor de norma mínima, através da função ψ (4.3), deste modo calculamos a distância mínima comparando as distâncias entre as imagens dos 4 pontos e do vetor inicial.

Agora, para sabermos os pontos do código esférico, basta calcularmos a imagem dos vértices do grafo no toro planar.

Aplicando a função μ_α definida em (4.4) nos geradores do grupo G encontramos os 4 pontos a saber:

$$(0,0,0),\ (1,1,0),\ (0,1,1)\ (1,0,1).$$

Os pontos do código esférico associado são:

$$\psi(0,0,0) = \ (\tfrac{1}{\pi},0,\tfrac{1}{\pi},0,\tfrac{1}{\pi},0)$$

$$\psi(1,1,0) = \ (-\tfrac{1}{\pi},0,-\tfrac{1}{\pi},0,\tfrac{1}{\pi},0)$$

$$\psi(0,1,1) = \ (\tfrac{1}{\pi},0,-\tfrac{1}{\pi},0,-\tfrac{1}{\pi},0)$$

$$\psi(1,0,1) = \ (-\tfrac{1}{\pi},0,\tfrac{1}{\pi},0,-\tfrac{1}{\pi},0)$$

De (4.7), a distância mínima destes 4 pontos na esfera unitária é $d_{min} = 1,63299$ e o vetor inicial é $\{(0.57735, 0, 0.57735, 0, 0.57735, 0)\}$.

Como a distância entre todos os 4 pontos é a mesma, $1,63299$, temos que estes pontos são os vértices de um tetraedro. Portanto, este código é um tetraedro, o melhor código contido na esfera unitária em $\mathbb{R}^6$ para 4 pontos [23], embora não substancial.

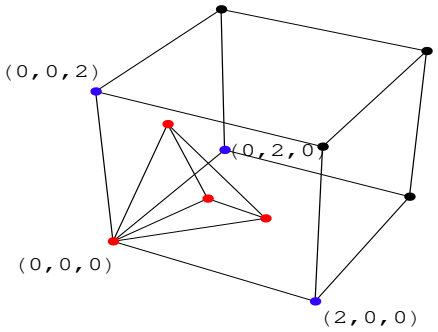


Figura 5.4: **Pré-imagem dos pontos do "código tetraedro" no** $\mathbb{R}^6$

A Tabela (5.3) apresenta alguns códigos esféricos gerados por grupos comutativos da família (5.3.1) em $\mathbb{R}^6$ com $4l^3$ pontos e sua respectiva distância mínima comparada com o

limitante da Proposição (4.4.4). A tabela apresenta também, de acordo com [11], o número aproximado de casos que devem ser analisados, numa busca exaustiva.

M	d_{min}	δ_1	δ_2	δ_3	Limitante	Grupo	Casos [11]	Método Exaustivo [42]	Tempo
4	1.63299	0.57735	0.57735	0.57735	2.39287	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	0	1.63299	0.03 s
32	1.1547	0.57735	0.57735	0.57735	1.26069	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$	560	1.1547	1.735 s
108	0.816497	0.57735	0.57735	0.57735	0.848537	$\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$	24.804	0.816497	39.31 s
256	0.624919	0.57735	0.57735	0.57735	0.638531	$\mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$	341.376	0.624919	393.91 s
500	0.504623	0.57735	0.57735	0.57735	0.511615	$\mathbb{Z}_5 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$	2.573.000	0.504623	2392.77 s
864	0.42265	0.57735	0.57735	0.57735	0.426703	$\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$	13.343.760	0.42265	17594.2 s
1372	0.363375	0.57735	0.57735	0.57735	0.36593	$\mathbb{Z}_7 \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_{14}$	53.569.740	0.363375	46581.7 s
2048	0.318581	0.57735	0.57735	0.57735	0.320294	$\mathbb{Z}_8 \oplus \mathbb{Z}_{16} \oplus \mathbb{Z}_{16}$	178.433.024	*	

* Não obtido computacionalmente pelo método proposto em [42].

Tabela 5.3: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.3.1) em $\mathbb{R}^6$ e o limitante da Proposição (4.4.4).**

Os cálculos do método proposto em [42] foram feitos em um computador com a seguinte configuração: Intel(R) Core(TM)2, CPU 6600, 2.40 GHz, 4 Giga de Ram, e programas: Mathematica 6.0, Windows XP.

Para M= 4, 32, 108, 256, 500, 864 e 1372, como pode ser observado na tabela, obtemos o código ótimo. Os outros valores de M apresentados na tabela estão muito próximos do limitante (4.4.4), donde concluímos que com esta família obtemos códigos esféricos gerados por grupos comutativos muito bons, pois como previsto em (4.4.4), para códigos com grande número de pontos gerados a partir dos reticulados com densidade de centro máxima, aproximamos do limitante.

Quando o número de pontos é muito grande, o número aproximado de casos a serem testados também é muito grande e assim, o método proposto em [42], mesmo com uma redução no número de casos, não permite obter computacionalmente o código ótimo.

5.3.2 Sub-reticulados "retangulares" de D_3 gerados por $\{(m, m+1, m(m+1)), (-m(m+1), -m, m+1), ((m+1), -m(m+1), m)\}$

Uma base de vetores ortogonais de mesma norma e coordenadas inteiras em $\mathbb{R}^3$ dada em [17] é $\gamma = \{s_1, s_2, s_3\}$ onde $s_1 = (m, m+1, m(m+1))$, $s_2 = (-m(m+1), -m, m+1)$ e $s_3 =$

$((m+1), -m(m+1), m)$, $m \in \mathbb{Z}$.

Considerando $\tilde{\alpha} = \{\tilde{v}_1 = 2s_1, \tilde{v}_2 = 2s_2, \tilde{v}_3 = 2s_3\}$, temos que $\Lambda_{\tilde{\alpha}} \subset \Lambda_\alpha = 2\mathbb{Z}^3 \subset \Lambda_\beta$. Observamos que os vetores de $\tilde{\alpha}$ são mutuamente ortogonais, portanto conjunto de sinais 3-dimensionais no toro planar gerados por D_3 definirão códigos esféricos 6-dimensionais.

Observamos que como $||\tilde{v}_1|| = ||\tilde{v}_2|| = ||\tilde{v}_3||$ o paralelepípedo que define o toro forma um cubo. De modo análogo ao caso anterior, podemos gerar uma família de sub-reticulados tomando $\tilde{\tilde{v}}_i = l\tilde{v}_i$, $l \in \mathbb{Z}^*$, $i = 1, \cdots 3$.

Deste modo o sistema,

$$\begin{aligned}
\tilde{v}_1 &= k_1 v_1 + k_2 v_2 + k_3 v_3 \\
\tilde{v}_2 &= k_4 v_1 + k_5 v_2 + k_6 v_3 \\
\tilde{v}_3 &= k_7 v_1 + k_8 v_2 + k_9 v_3
\end{aligned}$$

onde $k_i \in \mathbb{Z}$, $i = 1, \cdots, 9$ tem como solução $k_1 = m$, $k_2 = m+1$, $k_3 = m(m+1)$, $k_4 = -m(m+1)$, $k_5 = -m$, $k_6 = m+1$, $k_7 = (m+1)$, $k_8 = -m(m+1)$, $k_9 = m$.

Desta forma

$$\begin{aligned}
\tilde{v}_1 &= mv_1 + (m+1)v_2 + m(m+1)v_3 \\
&= m(w_1 - w_2) + (m+1)(-w_1 - w_2) + m(m+1)(-w_1 - w_2 - 2w_3) \\
&= (-1 - m - m^2)w_1 - (1 + 3m + m^2)w_2 - 2m(1+m)w_3
\end{aligned}$$

$$\begin{aligned}
\tilde{v}_2 &= -m(m+1)v_1 - mv_2 + (m+1)v_3 \\
&= -m(m+1)(w_1 - w_2) - m(-w_1 - w_2) + (m+1)(-w_1 - w_2 - 2w_3) \\
&= (-1 - m - m^2)w_1 + (-1 + m + m^2)w_2 - 2(1+m)w_3
\end{aligned}$$

$$\begin{aligned}
\tilde{v}_3 &= (m+1)v_1 - m(m+1)v_2 + mv_3 \\
&= (m+1)(w_1 - w_2) - m(m+1)(-w_1 - w_2) + m(-w_1 - w_2 - 2w_3) \\
&= (1 + m + m^2)w_1 + (-1 - m + m^2)w_2 - 2mw_3
\end{aligned}$$

Logo, a matriz da base $\tilde{\alpha}$ escrita em relação à base β é dada por:

$$A = \begin{bmatrix}
-1 - m - m^2 & -1 - m - m^2 & 1 + m + m^2 \\
-1 - 3m - m^2 & -1 + m + m^2 & -1 - m + m^2 \\
-2m(1+m) & -2(1+m) & -2m
\end{bmatrix}$$

e obtemos então um código esférico com $|det(A)| = |4(1 + m + m^2)^3|$ pontos. Variando o valor de m e l podemos construir uma família de sub-reticulados com $|4l^3(1 + m + m^2)^3|$ pontos. Tomando $m = 0$ temos um caso particular da família anterior.

A Tabela (5.4) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^6$ com $|4(1+m+m^2)^3|$ pontos e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4). A tabela apresenta também, de acordo com [11], o número aproximado de casos que deveriam ser analisados.

M	d_{min}	δ_1	δ_2	δ_3	Limitante	Grupo	Casos [11]
6912	0.188099	0.57735	0.57735	0.57735	0.213657	$\mathbb{Z}_4 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{72}$	6873736320
8788	0.189724	0.57735	0.57735	0.57735	0.197235	$\mathbb{Z}_{26} \oplus \mathbb{Z}_{338}$	14129680344
10976	0.165574	0.57735	0.57735	0.57735	0.183157	$\mathbb{Z}_2 \oplus \mathbb{Z}_{28} \oplus \mathbb{Z}_{196}$	27533005136
13500	0.150599	0.57735	0.57735	0.57735	0.170955	$\mathbb{Z}_5 \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{90}$	51235033500
37044	0.120105	0.57735	0.57735	0.57735	0.122129	$\mathbb{Z}_{42} \oplus \mathbb{Z}_{882}$	1058868536040
70304	0.095065	0.57735	0.57735	0.57735	0.0986477	$\mathbb{Z}_2 \oplus \mathbb{Z}_{52} \oplus \mathbb{Z}_{676}$	7238720418800
119164	0.0820375	0.57735	0.57735	0.57735	0.0827392	$\mathbb{Z}_{62} \oplus \mathbb{Z}_{1922}$	35251054560060
237276	0.0634018	0.57735	0.57735	0.57735	0.0657688	$\mathbb{Z}_3 \oplus \mathbb{Z}_{78} \oplus \mathbb{Z}_{1014}$	278297444097036
296352	0.0601007	0.57735	0.57735	0.57735	0.0610714	$\mathbb{Z}_2 \oplus \mathbb{Z}_{84} \oplus \mathbb{Z}_{1764}$	542217533785200
318028	0.05936	0.57735	0.57735	0.57735	0.0596513	$\mathbb{Z}_{86} \oplus \mathbb{Z}_{3698}$	670110839909364

Tabela 5.4: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.3.2) em $\mathbb{R}^6$ e o limitante da Proposição (4.4.4).**

Como pode ser observado na tabela, o número aproximado de casos a serem testados é muito grande. Não sendo computacional viável assim, encontrar o código ótimo para um número muito grande de pontos. Em nosso trabalho não é necessário analisar casos, deste modo, a determinação de códigos cujas as distâncias se aproximam do limitante (4.4.4) para um grande número de pontos é viável pois o cálculo só é feito para pontos na esfera que correspondem as imagens dos vetores de norma mínima, obtidos a partir dos geradores do reticulado. Novamente, para um grande número de pontos podemos observar a aproximação ao limitante.

5.3.3 Sub-reticulados "retangulares" de D_3 obtidos a partir da construção de uma base ortogonal

Consideramos a base de $\Lambda_\beta = D_3 = \{(1,-1,0),(-1,-1,0),(0,1,-1)\}$, obtido pela *construção A* do código C_3 (5.3). Seja $w_1 = (1,-1,0)$, $w_2 = (-1,-1,0)$ *e* $w_3 = (0,1,-1)$.

Observamos que esta base não é ortogonal. Somente os vetores w_1 e w_2 o são. O procedimento novamente é procurar um sub-reticulado de D_3 que possua uma base ortogonal.

Como os dois primeiros vetores da base são ortogonais, procuramos inicialmente por um vetor $\tilde{w}$ em Λ_β tal que w_1, w_2, *e* $\tilde{w}$ sejam ortogonais.

Seja $\tilde{w} = (a,b,c)$. O sistema

$$\begin{cases} w_1.\tilde{w} = 0 \\ w_2.\tilde{w} = 0 \end{cases}$$

tem como solução $a = b = 0$.

Logo, $\tilde{w} = (0,0,c)$, $\forall\, c \in \mathbb{R}$ é um vetor ortogonal a w_1 e w_2. Agora, resta saber se o reticulado gerado por $\alpha = \{w_1, w_2, \tilde{w}\}$ é um sub-reticulado de Λ_β.

De fato, ele é um sub-reticulado de Λ_β pois $(0,0,c) = k_1w_1 + k_2w_2 + k_3w_3$ resulta em

$$(0,0,c) = -\frac{c}{2}w_1 - \frac{c}{2}w_2 - cw_3,$$

e para que os múltiplos dos vetores da base sejam inteiros c deve ser múltiplo de 2, ou seja, $c = 2k$, $k \in \mathbb{Z}$.

Com isso, podemos encontrar várias famílias de códigos esféricos associados, bastando variar o valor de k.

Observe que como $||v_1|| = ||v_2|| = \dfrac{1}{\sqrt{2}|k|}||v_3||$ os bons tamanhos ocorrerão quando tomarmos $\tilde{v}_1 = l_1v_1$, $\tilde{v}_2 = l_2v_2$ e $\tilde{v}_3 = l_3v_3$, l_i, $i = 1\cdots,3 \in \mathbb{Z}^*$ com $|l_1| = |l_2| = \sqrt{2}|k||l_3|$.

Alguns valores de l_1, l_2 e l_3 que se aproximam desta condição são apresentados na Tabela (5.5). A Tabela (5.6) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^6$ obtidos a partir dos valores de l_i, $i = 1\cdots,3$ da tabela acima e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4). A tabela apresenta também, de acordo com [11], o número aproximado de casos que devem ser analisados numa busca exaustiva.

$k=1$			$k=2$			$k=3$			$k=4$		
l_1	l_2	l_3	l_1	l_2	l_3	l_1	l_2	l_3	l_1	l_2	l_3
17	17	12	17	17	6	17	17	4	17	17	3
24	17	17	31	31	11	34	34	8	34	34	6
27	27	19	34	34	12	38	38	9	45	45	8
31	31	22	37	37	13	47	47	11	51	51	9
34	34	24	45	45	16	51	51	12	57	57	10

Tabela 5.5: **Valores de l_1, l_2 e l_3.**

M	d_{min}	δ_1	δ_2	δ_3	Limitante	Casos [11]
2312	0.250992	0.68831	0.68831	0.229039	0.307633	256799620
3468	0.244872	0.666795	0.666795	0.33282	0.268805	867449684
6936	0.212298	0.577684	0.577684	0.576683	0.21341	6945607516
19584	0.150632	0.577016	0.577016	0.578017	0.151027	156433548480
21142	0.13481	0.666397	0.666397	0.33441	0.147224	196822030405
27702	0.134268	0.578276	0.578276	0.575493	0.134546	442790268525
27744	0.123026	0.666795	0.666795	0.33282	0.134478	444807460240
35594	0.113134	0.667127	0.667127	0.331486	0.123764	939325126090
42284	0.116678	0.576651	0.576651	0.578747	0.116861	1574799714180
55488	0.106604	0.577684	0.577684	0.576683	0.106743	3558844518944

Tabela 5.6: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.3.3) em $\mathbb{R}^6$ e o limitante da Proposição (4.4.4).**

Valem aqui as mesmas observações quanto a aproximação feitas nas Tabelas (5.3) e (5.4).

5.4 Sub-reticulados "retangulares" de D_4

5.4.1 Sub-reticulados "retangulares" de D_4 gerados por $2\mathbb{Z}^4$

Para $n = 4$, temos que $\alpha = \{(2,0,0,0),(0,2,0,0),(0,0,2,0),(0,0,0,2)\}$ é uma base de $2\mathbb{Z}^4 = \Lambda_\alpha$. Agora consideramos $\beta = \{(-1,-1,0,0),(1,-1,0,0),(0,1,-1,0),(0,0,1,-1)\}$ a base de $D_4 = \Lambda_\beta$ obtido pela *construção A* do código C_4 (5.3). Pela Proposição (5.2.1), temos que Λ_α é um sub-reticulado de Λ_β.

Sejam

$$v_1 = (2,0,0,0), \quad v_2 = (0,2,0,0), \quad v_3 = (0,0,2,0), \quad v_4 = (0,0,0,2)$$
$$w_1 = (-1,-1,0,0), \quad w_2 = (1,-1,0,0), \quad w_3 = (0,1,-1,0), \quad w_4 = (0,0,1,-1).$$

Escrevendo v_i na base β :

$$\begin{aligned} v_1 &= -w_1 + w_2 \\ v_2 &= -w_1 - w_2 \\ v_3 &= -w_1 - w_2 - 2w_3 \\ v_4 &= -w_1 - w_2 - 2w_3 - 2w_4 \end{aligned}$$

temos que a matriz de α em relação à base β é dada por:

$$A = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & -2 \end{bmatrix}$$

e obtemos um código esférico com $|\det A| = 8$ pontos no $\mathbb{R}^8$.

Como $||v_1|| = ||v_2|| = ||v_3|| = ||v_4||$ a "caixa" que define o toro forma um "cubo". Tomando $\tilde{v}_1 = lv_1$, $\tilde{v}_2 = lv_2$, $\tilde{v}_3 = lv_3$ e $\tilde{v}_4 = lv_4$, com $l \in \mathbb{Z}^*$ é possível gerar uma família de sub-reticulados com $8l^4$ pontos.

O reticulado $\Lambda_\beta = D_4$ possui 24 vetores de norma mínima, $\sqrt{2}$, obtidos a partir da base que o gera: w_1, w_2, w_3, w_4, $w_5 = -w_1 - w_2 - 2w_3 - w_4$, $w_6 = -w_1 - w_3$, $w_7 = w_2 + w_3$, $w_8 = -w_1 - w_2 - w_3$, $w_9 = -w_1 - w_2 - w_3 - w_4$, $w_{10} = w_3 + w_4$, $w_{11} = -w_1 - w_3 - w_4$, $w_{12} = w_2 + w_3 + w_4$ e seus simétricos. Denotaremos o conjunto destes vetores por w_{min}. Notamos que se $\tilde{w} \in \Lambda$, $\tilde{w} \in w_{min}$, então

$$||\tilde{w}|| \geq 2 \text{ (segunda maior norma neste reticulado).} \tag{5.6}$$

Mostraremos agora que a distância mínima no código esférico em $\mathbb{R}^8$ é obtida pela imagem de um destes vetores de norma mínima, dentro de certas condições.

Proposição 5.4.1. *Se* $v_{min} = \min\{||v_1||, ||v_2||, ||v_3||, ||v_4||\} \geq \dfrac{2\pi}{\sqrt{3(2-\sqrt{2})}} \approx 4,73969$ *então a distância mínima no código esférico em* $\mathbb{R}^8$*, definida por* ψ *(4.5), é atingida por algum* $\psi(w)$*, onde* $||w|| = \sqrt{2}$*,* $w \in \Lambda_\beta$*, tem norma mínima.*

Demonstração: Suponhamos inicialmente que $v_{min} = 2\pi\delta_{min} > \sqrt{2}$. Da Proposição (4.3.1), temos que $d(\psi(w), \psi(0)) < d(w, 0) = \sqrt{2}$ para $w \in w_{min}$.

Seja agora $\tilde{w} \in \Lambda_\beta$ tal que $||\tilde{w}|| > \sqrt{3} \Rightarrow ||\tilde{w}|| \geq 2$ (5.6). Pela Proposição (4.3.1),

$$\begin{aligned} d(\psi(\tilde{w}), \psi(0)) &\geq 2\delta_{min} \sin\left(\frac{r}{2\delta_{min}}\right) = 2\frac{v_{min}}{2\pi} \sin\left(\frac{2}{\frac{2v_{min}}{2\pi}}\right) = \frac{v_{min}}{\pi} \sin\left(\frac{2\pi}{v_{min}}\right) \\ &\geq \frac{v_{min}}{\pi}\left(\frac{2\pi}{v_{min}} - \left(\frac{2\pi}{v_{min}}\right)^3 \frac{1}{3!}\right) = 2 - \frac{4\pi^2}{3v_{min}^2}. \end{aligned}$$

Queremos saber quando $2 - \frac{4\pi^2}{3v_{min}^2} \geq \sqrt{2}$. Seja $x = v_{min}$. Temos então $3(2-\sqrt{2})x^2 - 4\pi^2 \geq 0$, $x > 0$, e então a inequação é satisfeita para $x > \dfrac{2\pi}{\sqrt{3(2-\sqrt{2})}} \approx 4,73969$, donde concluímos a proposição. ∎

Observação 5.4.1. *Quando $v_{min} < 4,73969$, temos que para caixas aproximadamente quadradas, isto é, $||v_1|| \approx ||v_2|| \approx ||v_3|| \approx ||v_4||$,*

$M = \dfrac{Vol(\Lambda_\alpha)}{Vol(\Lambda_\beta)} = \dfrac{||v_i||^4}{2} < \dfrac{(4,73969)^4}{2} = 252,331 < 253.$

Ou seja, neste caso a Proposição (5.3.1) só não será válida para um número de pontos menor que 253. Como procuramos por códigos esféricos que sejam mais próximos do limitante da Proposição (4.4.4), temos que de acordo com as considerações finais do Capítulo 4, isto acontecerá para valores grandes de M.

A Tabela (5.7) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^8$ com $8l^4$ pontos e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4). A tabela apresenta também uma estimativa para um limitante inferior [11] do número total de casos a serem analisados numa busca exaustiva.

5.4.2 Sub-reticulados "retangulares" de D_4 gerados pelos quatérnios

Podemos fazer o uso das estruturas algébricas dos quatérnios para obter sub-reticulados de D_4.

M	d_{min}	δ_1	δ_2	δ_3	δ_4	Limitante	grupo	Casos [11]
648	0.707107	0.5	0.5	0.5	0.5	0.736258	$\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$	450710001
2048	0.541196	0.5	0.5	0.5	0.5	0.553578	$\mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$	45545029376
5000	0.437016	0.5	0.5	0.5	0.5	0.443375	$\mathbb{Z}_5 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$	1623700780625
10368	0.366025	0.5	0.5	0.5	0.5	0.369712	$\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$	30057022811376

Tabela 5.7: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.4.1) em $\mathbb{R}^8$ e o limitante da Proposição (4.4.4).**

A partir de qualquer vetor $v_1 = (a, b, c, d)$, identificamos $v_1 \equiv a+bi+cj+dk$ (quatérnios) e tomando $v_2 = iv_1$, $v_3 = jv_1$ e $v_4 = kv_1$, obtemos uma base ortogonal $\delta = \{v_1, v_2, v_3, v_4\}$.

Para provar que δ é uma base ortogonal, resumidamente discutimos duas propriedades básicas da norma dos quatérnios.

Se v é um vetor unitário de $\mathbb{R}^4$, a multiplicação à direita (e à esquerda) por v é uma isometria R_v. De fato, o conjugado $\overline{w}$ de um quatérnio $w = a + bi + cj + dk$ é definido como $\overline{w} = a - bi - cj - dk$. A norma quaterniônica de w é $|w| = \sqrt{w\overline{w}}$, que é igual a norma euclidiana $||w||$ de w.

Além disso, a norma quaterniônica satisfaz $|wv| = |w|.|v|$. Portanto, se v é um vetor unitário dos quatérnios, então R_v é uma isometria, pois

$$||R_v(w)|| = |R_v(w)| = |wv| = |w||v| = |w| = ||w||.$$

Agora seja $u_1 = a + bi + cj + dk$ e consideramos o vetor unitário $v = \dfrac{u_1}{|u_1|}$. Como $\{1, i, j, k\}$ é uma base ortogonal, $\delta' = \{R_v(1), R_v(i), R_v(j), R_v(k)\} = \{v, iv, jv, kv\}$ é uma base ortogonal (os ângulos também são preservados por isometria). Finalmente, $\delta = |u_1|\delta' = \{u_1, iu_1, ju_1, ku_1\}$ é uma base ortogonal.

Deste modo, consideramos a base $\beta = \{(1, -1, 0, 0), (-1, -1, 0, 0), (0, 1, -1, 0), (0, 0, 1, -1)\}$ de D_4 obtido pela *construção A* do código C_4 (5.3) e a base $\gamma = \{(a, b, c, d), (-b, a, d, -c), (-c, -d, a, b), (-d, c, -b, a)\}$ obtida como exposto acima, onde $s_1 = (a, b, c, d)$, $s_2 = (-b, a, d, -c)$, $s_3 = (-c, -d, a, b)$, $s_4 = (-d, c, -b, a)$.

Seja $\tilde{\alpha} = \{\tilde{v}_1 = 2s_1, \tilde{v}_2 = 2s_2, \tilde{v}_3 = 2s_3, \tilde{v}_4 = 2s_4\}$, temos que $\Lambda_{\tilde{\alpha}} \subset \Lambda_\alpha = 2\mathbb{Z}^4 \subset \Lambda_\beta$. Observamos que os vetores de $\tilde{\alpha}$ são ortogonais entre si, portanto conjunto de sinais 4-dimensionais no toro planar gerados por D_4 definirão códigos esféricos 8-dimensionais e como $||\tilde{v}_1|| = ||\tilde{v}_2|| = ||\tilde{v}_3|| = ||\tilde{v}_4||$ a "caixa" que define o toro forma um "cubo".

Escrevendo $\tilde{v_i}$ na base β :

$$\begin{aligned}
\tilde{v_1} &= av_1 + bv_2 + cv_3 + dv_4 \\
&= a(-w_1 + w_2) + b(-w_1 - w_2) + c(-w_1 - w_2 - 2w_3) + d(-w_1 - w_2 - 2w_3 - 2w_4) \\
&= (-a - b - c - d)w_1 + (+a - b - c - d)w_2 + (-2c - 2d)w_3 - 2dw_4
\end{aligned}$$

$$\begin{aligned}
\tilde{v_2} &= -bv_1 + av_2 + dv_3 - cv_4 \\
&= -b(-w_1 + w_2) + a(-w_1 - w_2) + d(-w_1 - w_2 - 2w_3) - c(-w_1 - w_2 - 2w_3 - 2w_4) \\
&= (-a + b + c - d)w_1 + (-a - b + c - d)w_2 + (+2c - 2d)w_3 + 2cw_4
\end{aligned}$$

$$\begin{aligned}
\tilde{v_3} &= -cv_1 - dv_2 + av_3 + bv_4 \\
&= -c(-w_1 + w_2) - d(-w_1 - w_2) + a(-w_1 - w_2 - 2w_3) + b(-w_1 - w_2 - 2w_3 - 2w_4) \\
&= (-a - b + c + d)w_1 + (-a - b - c + d)w_2 + (-2a - 2b)w_3 - 2bw_4
\end{aligned}$$

$$\begin{aligned}
\tilde{v_4} &= -dv_1 + cv_2 - bv_3 + av_4 \\
&= -d(-w_1 + w_2) + c(-w_1 - w_2) - b(-w_1 - w_2 - 2w_3) + a(-w_1 - w_2 - 2w_3 - 2w_4) \\
&= (-a + b - c + d)w_1 + (-a + b - c - d)w_2 + (-2a + 2b)w_3 - 2aw_4
\end{aligned}$$

Logo, a matriz de $\tilde{\alpha}$ escrita em relação à base β é dada por:

$$A = \begin{bmatrix}
-a-b-c-d & -a+b+c-d & -a-b+c+d & -a+b-c+d \\
+a-b-c-d & -a-b+c-d & -a-b-c+d & -a+b-c-d \\
-2c-2d & +2c-2d & -2a-2b & -2a+2b \\
-2d & 2c & -2b & -2a
\end{bmatrix}$$

e obtemos um código esférico com $|\det A| = 8(a^2 + b^2 + c^2 + d^2)^2$ pontos. Para $a = l$, $b = c = d = 0$, temos um caso particular da família anterior. Tomando $\tilde{\tilde{v}}_1 = l\tilde{v}_1$, $\tilde{\tilde{v}}_2 = l\tilde{v}_2$, $\tilde{\tilde{v}}_3 = l\tilde{v}_3$, $\tilde{\tilde{v}}_4 = l\tilde{v}_4$, com $l \in \mathbb{Z}^*$ é possível gerar uma família de sub-reticulados com $8l^4(a^2 + b^2 + c^2 + d^2)^2$ pontos. Como todo número inteiro positivo n pode ser escrito como soma de 4 quadrados perfeitos então é possível construir códigos com $8l^4n^2$ pontos.

Variando os valores de a, b, c, e d, podemos construir uma família de sub-reticulados cujos pontos são múltiplos de 8.

A Tabela (5.8) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^8$ com $8(a^2+b^2+c^2+d^2)^2$ pontos e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4). A tabela apresenta também, de acordo com [11], o número aproximado de casos que devem ser analisados numa busca exaustiva.

M	d_{min}	δ_1	δ_2	δ_3	δ_4	Limitante	Grupo	Casos [11]
392	0.791524	0.5	0.5	0.5	0.5	0.833474	$\mathbb{Z}_2 \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_{14}$	59626385
800	0.664066	0.5	0.5	0.5	0.5	0.698876	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{20}$	1050739900
1152	0.619657	0.5	0.5	0.5	0.5	0.638531	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$	4538847600
1352	0.59686	0.5	0.5	0.5	0.5	0.613684	$\mathbb{Z}_2 \oplus \mathbb{Z}_{26} \oplus \mathbb{Z}_{26}$	8624108025
1800	0.551501	0.5	0.5	0.5	0.5	0.57161	$\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{30}$	27155621025
2048	0.541196	0.5	0.5	0.5	0.5	0.553578	$\mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$	45545029376
2592	0.510672	0.5	0.5	0.5	0.5	0.522105	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_{36}$	117002820060
2888	0.498712	0.5	0.5	0.5	0.5	0.508256	$\mathbb{Z}_2 \oplus \mathbb{Z}_{38} \oplus \mathbb{Z}_{38}$	180406227001
3200	0.480187	0.5	0.5	0.5	0.5	0.495454	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{20}$	272043839600
6272	0.413686	0.5	0.5	0.5	0.5	0.419043	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{28} \oplus \mathbb{Z}_{28}$	4022182244080

Tabela 5.8: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.4.2) em $\mathbb{R}^8$ e o limitante da Proposição (4.4.4).**

Convém observar novamente que em todos os casos bastou calcular a distância mínima entre todas as imagens dos vetores de norma mínima e do vetor inicial, o que é de crucial importância quando a dimensão e o número de pontos aumenta.

5.5 Sub-reticulados "retangulares" de E_8

5.5.1 Sub-reticulados "retangulares" de E_8 gerados por $2\left(\frac{1}{\sqrt{2}}\right)\mathbb{Z}^8$.

Para $n=8$, temos que $\alpha = \{(\frac{2}{\sqrt{2}},0,0,0,0,0,0,0), (0,\frac{2}{\sqrt{2}},0,0,0,0,0,0), (0,0,\frac{2}{\sqrt{2}},0,0,0,$

$0,0), (0,0,0,\frac{2}{\sqrt{2}},0,0,0,0), (0,0,0,0,\frac{2}{\sqrt{2}},0,0,0), (0,0,0,0,0,\frac{2}{\sqrt{2}},0,0), (0,0,0,0,0,0,\frac{2}{\sqrt{2}},0), (0,$

$0,0,0,0,0,0,\frac{2}{\sqrt{2}})\}$ é uma base de $2\left(\frac{1}{\sqrt{2}}\right)\mathbb{Z}^8 = \Lambda_\alpha$.

Agora consideramos $\beta = \frac{1}{\sqrt{2}}\{(2,0,0,0,0,0,0,0), (-1,1,0,0,0,0,0,0), (0,-1,1,0,0,0,0,0),$

$(0,0,-1,1,0,0,0,0), (0,0,0,-1,1,0,0,0), (0,0,0,0,-1,1,0,0), (0,0,0,0,0,-1,1,0), (\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})\}$ a base de $E_8 = \Lambda_\beta$ obtido pela *construção A* do código de Hamming $\tilde{H}_3$ (5.4).

Pela Proposição (5.2.1), Λ_α é um sub-reticulado de Λ_β.

Escrevendo a base de Λ_α em relação a base de Λ_β temos

$$\begin{aligned}
v_1 &= w_1 + 0w_2 + 0w_3 + 0w_4 + 0w_5 + 0w_6 + 0w_7 + 0w_8 \\
v_2 &= w_1 + 2w_2 + 0w_3 + 0w_4 + 0w_5 + 0w_6 + 0w_7 + 0w_8 \\
v_3 &= w_1 + 2w_2 + 2w_3 + 0w_4 + 0w_5 + 0w_6 + 0w_7 + 0w_8 \\
v_4 &= w_1 + 2w_2 + 2w_3 + 2w_4 + 0w_5 + 0w_6 + 0w_7 + 0w_8 \\
v_5 &= w_1 + 2w_2 + 2w_3 + 2w_4 + 2w_5 + 0w_6 + 0w_7 + 0w_8 \\
v_6 &= 1w_1 + 2w_2 + 2w_3 + 2w_4 + 2w_5 + 2w_6 + 0w_7 + 0w_8 \\
v_7 &= 1w_1 + 2w_2 + 2w_3 + 2w_4 + 2w_5 + 2w_6 + 2w_7 + 0w_8 \\
v_8 &= -7w_1 - 12w_2 - 10w_3 - 8w_4 - 6w_5 - 4w_6 - 2w_7 + 4w_8
\end{aligned}$$

e

$$A = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & -7 \\
0 & 2 & 2 & 2 & 2 & 2 & 2 & -12 \\
0 & 0 & 2 & 2 & 2 & 2 & 2 & -10 \\
0 & 0 & 0 & 2 & 2 & 2 & 2 & -8 \\
0 & 0 & 0 & 0 & 2 & 2 & 2 & -6 \\
0 & 0 & 0 & 0 & 0 & 2 & 2 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 4
\end{bmatrix}.$$

Como $|\det A| = 256$, obtemos um código esférico com 256 pontos. Observamos que como $||v_1|| = \cdots = ||v_8||$ a "caixa" que define o toro forma um "cubo". Tomando $\tilde{v}_i = lv_i,\ l \in \mathbb{Z}^*,\ i = 1, \cdots 8$ é possível gerar uma família de sub-reticulados com $256l^8$ pontos.

O reticulado $\Lambda_\beta = E_8$ possui 240 vetores de norma mínima, obtidos a partir da base que o gera, e esta norma é igual a 1:

- $C_8^2 = 28$ permutações do vetor $\frac{1}{\sqrt{2}}(1,-1,0,0,0,0,0,0)$.
- $C_8^2 = 28$ permutações do vetor $\frac{1}{\sqrt{2}}(1,1,0,0,0,0,0,0)$.
- $C_8^1 = 1$ permutações do vetor $\frac{1}{\sqrt{2}}(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$.

- $C_8^2 = 28$ permutações do vetor $\frac{1}{\sqrt{2}}(-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$.
- $C_8^4/2 = 35$ permutações do vetor $\frac{1}{\sqrt{2}}(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$.

e seus simétricos.

Denotaremos o conjunto destes vetores por w_{min}. Notamos que se $\tilde{w} \in \Lambda$, $\tilde{w} \in w_{min}$, então

$$||\tilde{w}|| \geq \sqrt{2} \text{ (segunda maior norma neste reticulado).} \tag{5.7}$$

Mostraremos agora que a distância mínima no código esférico em $\mathbb{R}^{16}$ definida por ψ (4.5) é obtida pela imagem de um dos vetores de norma mínima, dentro de certas condições.

Proposição 5.5.1. *Se* $v_{min} = \min\{||v_1||, \cdots, ||v_8||\} \geq \dfrac{\sqrt[4]{2}\pi}{\sqrt{3}} \approx 2.15698$ *então a distância mínima no código esférico em* $\mathbb{R}^{16}$, *definida por* ψ *(4.5), é atingida por algum* $\psi(w)$, *onde* $||w|| = 1$, $w \in \Lambda_\beta$, *tem norma mínima.*

Demonstração: Suponhamos inicialmente que $v_{min} = 2\pi\delta_{min} > 1$. Da Proposição (4.3.1), temos que $d(\psi(w), \psi(0)) < d(w, 0) = 1$ para $w \in w_{min}$.

Seja agora $\tilde{w} \in \Lambda_\beta$ tal que $||\tilde{w}|| > 1 \Rightarrow ||\tilde{w}|| \geq \sqrt{2}$ (5.7). Pela Proposição (4.3.1),

$$\begin{aligned} d(\psi(\tilde{w}), \psi(0)) &\geq 2\delta_{min} \sin\left(\frac{r}{2\delta_{min}}\right) = 2\frac{w_{min}}{2\pi} \sin\left(\frac{\sqrt{2}}{\frac{2w_{min}}{2\pi}}\right) = \frac{w_{min}}{\pi} \sin\left(\frac{\sqrt{2}\pi}{w_{min}}\right) \\ &\geq \frac{w_{min}}{\pi}\left(\frac{\sqrt{2}\pi}{w_{min}} - \left(\frac{\sqrt{2}\pi}{w_{min}}\right)^3 \frac{1}{3!}\right) = \sqrt{2} - \frac{\sqrt{2}\pi^2}{3w_{min}^2}. \end{aligned}$$

Queremos saber quando $\sqrt{2} - \frac{\sqrt{2}\pi^2}{3w_{min}^2} \geq 1$. Seja $x = v_{min}$. Temos então $3x^2 - \sqrt{2}\pi^2 \geq 0$; $x > 0$, e então a inequação é satisfeita para $x \geq \dfrac{\sqrt[4]{2}\pi}{\sqrt{3}} \approx 2,15698$, donde concluímos a proposição. ∎

Observação 5.5.1. *Quando* $v_{min} < 2,15698$, *temos que para caixas aproximadamente "quadradas", isto é,* $||v_i|| \approx ||v_j||$, $i, j = 1, \cdots, 8$

$$M = \frac{|Vol(\Lambda_\alpha)|}{|Vol(\Lambda_\beta)|} \approx \frac{||v_i||^8}{\frac{1}{16}} < 16(2,15698)^8 = 7497,02 < 7498.$$

Ou seja, neste caso a Proposição (5.3.1) só não será válida para um número de pontos menor que 7498. Como procuramos por códigos esféricos que sejam mais próximos do limitante da Proposição (4.4.4), temos que de acordo com as considerações finais do Capítulo 4, isto acontecerá para valores grandes de M.

A Tabela (5.9) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^{16}$ com $256l^8$ pontos e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4).

l	M	d_{min}	Limitante	Grupo
2	65536	0.707107	0.780361	$\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$
3	16777216	0.382683	0.392069	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$

Tabela 5.9: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.5.1) em $\mathbb{R}^{16}$ e o limitante da Proposição (4.4.4).**

Como já comentamos, um limitante inferior para o número total de casos que deveriam ser analisados para 65536 pontos em $\mathbb{R}^{16}$ é da ordem de $\binom{M/2}{n/2} =$ 32938804052325523969860020727808 e para 16777216 pontos o número de casos é 608131121276655053225075868114231674616718159773696. Como pode ser observado, o número aproximado de casos a serem testados é exageradamente grande.

5.5.2 Sub-reticulados "retangulares" de E_8 gerados pelos octônios

Os octônios ou números de Cayley formam uma álgebra de dimensão 8 com base $\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$. Um octônio é um número da forma

$$\alpha = a + be_1 + ce_2 + de_3 + ee_4 + fe_5 + ge_6 + he_7$$

onde a, b, c, d, e, f, g, h são números reais e $1, e_1, e_2, e_3, e_4, e_5, e_6, e_7$, são unidades simbólicas satisfazendo a tabela:

$*$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_4	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	$-e_4$	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	$-e_3$	$-e_3$	$-e_2$	e_1	-1

O conjunto dos octônios é denotado por K,

$$K = \{\alpha = a + be_1 + ce_2 + de_3 + ee_4 + fe_5 + ge_6 + he_7 | \, a, b, c, d, e, f, g, h \in \mathbb{R}\}.$$

Cada octônio $\alpha = a + be_1 + ce_2 + de_3 + ee_4 + fe_5 + ge_6 + he_7$ pode ser identificado com $(a, b, c, d, e, f, g, h) \in \mathbb{R}^8$ e uma base ortogonal é dada por $\{(a, b, c, d, e, -f, -g, -h)$, $(-b, a, d, -c, -f, -e, h, -g), (-c, -d, a, b, -g, -h, -e, f), (-d, c, -b, a, -h, g, -f, -e)$, $(-e, f, g, h, a, b, c, d), (f, e, h, -g, -b, a, -d, c), (g, -h, e, f, -c, d, a, -b), (h, g, -f, e, -d, -c,$ $b, a)\}$ [28].

Consideramos a base de $E_8 = \Lambda_\beta$ obtido pela *construção A* do código de Hamming $\tilde{H}_3$ (5.4):

$$\begin{aligned} \beta \;=\; & \{(2,0,0,0,0,0,0,0),\ (-1,1,0,0,0,0,0,0),\ (0,-1,1,0,0,0,0,0), \\ & (0,0,-1,1,0,0,0,0),\ (0,0,0,-1,1,0,0,0),\ (0,0,0,0,-1,1,0,0), \\ & (0,0,0,0,0,-1,1,0),\ (\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\ \tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2})\} \end{aligned}$$

e a base

$$\begin{aligned} \gamma \;=\; & \{(a,b,c,d,e,-f,-g,-h), (-b,a,d,-c,-f,-e,h,-g), (-c,-d,a,b,-g,-h,-e,f), \\ & (-d,c,-b,a,-h,g,-f,-e), (-e,f,g,h,a,b,c,d), (f,e,h,-g,-b,a,-d,c) \\ & (g,-h,e,f,-c,d,a,-b), (h,g,-f,e,-d,-c,b,a)\} \end{aligned}$$

obtida acima, onde

$$\begin{aligned} s_1 &= (a,b,c,d,e,-f,-g,-h), & s_2 &= (-b,a,d,-c,-f,-e,h,-g)\\ s_3 &= (-c,-d,a,b,-g,-h,-e,f), & s_4 &= (-d,c,-b,a,-h,g,-f,-e)\\ s_5 &= (-e,f,g,h,a,b,c,d), & s_6 &= (f,e,h,-g,-b,a,-d,c)\\ s_7 &= (g,-h,e,f,-c,d,a,-b), & s_8 &= (h,g,-f,e,-d,-c,b,a). \end{aligned}$$

Seja

$$\begin{aligned} \tilde{\alpha} \;=\; & \{\tilde{v}_1 = \frac{2}{\sqrt{2}}s_1,\ \tilde{v}_2 = \frac{2}{\sqrt{2}}s_2,\ \tilde{v}_3 = \frac{2}{\sqrt{2}}s_3,\ \tilde{v}_4 = \frac{2}{\sqrt{2}}s_4,\ \tilde{v}_5 = \frac{2}{\sqrt{2}}s_5,\\ & \tilde{v}_6 = \frac{2}{\sqrt{2}}s_6,\ \tilde{v}_7 = \frac{2}{\sqrt{2}}s_7,\ \tilde{v}_8 = \frac{2}{\sqrt{2}}s_8\}, \end{aligned}$$

temos que $\Lambda_{\tilde{\alpha}} \subset \Lambda_\alpha = 2\left(\frac{1}{\sqrt{2}}\right)\mathbb{Z}^8 \subset \Lambda_\beta$.

Escrevendo a base de $\Lambda_{\tilde{\alpha}}$ em relação a base de Λ_β temos que

$$\begin{aligned} \tilde{v_1} &= (a+b+c+d+e-f-g+7h)w_1 + (2b+2c+2d+2e-2f-2g+12h)w_2\\ &+ (2c+2d+2e-2f-2g+10h)w_3 + (2d+2e-2f-2g+8h)w_4 + (2e-2f-2g+\\ &+ 6h)w_5 + (-2f-2g+4h)w_6 + (-2g+2h)w_7 - 4hw_8 \end{aligned}$$

$$\begin{aligned} \tilde{v_2} &= (a-b-c+d-e-f+7g+h)w_1 + (2a-2c+2d-2e-2f+12g+2h)w_2\\ &+ (-2c+2d-2e-2f+10g+2h)w_3 + (-2c-2e-2f+8g+2h)w_4 + (-2e-2f+\\ &+ 6g2h)w_5 + (-2e+4g+2h)w_6 + (2g+2h)w_7 - 4gw_8 \end{aligned}$$

$$\begin{aligned} \tilde{v_3} &= (a+b-c-d-e-7f-g-h)w_1 + (2a+2b-2d-2e-12f-2g-2h)w_2\\ &+ (2a+2b-2e-10f-2g-2h)w_3 + (2b-2e-8f-2g-2h)w_4 + (-2e-6f-2g\\ &- 2h)w_5 + (-2e-4f-2h)w_6 + (-2e-2f)w_7 + 4fw_8 \end{aligned}$$

$$\begin{aligned} \tilde{v_4} &= (a-b+c-d+7e-f+g-h)w_1 + (2a-2b+2c+12e-2f+2g-2h)w_2\\ &+ (2a-2b+10e-2f+2g-2h)w_3 + (2a+8e-2f+2g-2h)w_4 + (6e-2f+2g\\ &- 2h)w_5 + (4e-2f+2g)w_6 + (2e-2f)w_7 - 4ew_8 \end{aligned}$$

$$\begin{aligned} \tilde{v_5} &= (a+b+c-7d-e+f+g+h)w_1 + (2a+2b+2c-12d+2f+2g+2h)w_2\\ &+ (2a+2b+2c-10d+2g+2h)w_3 + (2a+2b+2c-8d+2h)w_4 + (2a+2b+2c-\end{aligned}$$

$$
\begin{aligned}
&- \quad 6d)w_5 + (2b + 2c - 4d)w_6 + (2c - 2d)w_7 + 4dw_8
\end{aligned}
$$

$$
\begin{aligned}
\tilde{v_6} = &(a - b - 7c - d + e + f - g + h)w_1 + (2a - 2b - 12c - 2d + 2e - 2g + 2h)w_2 \\
&+ \quad (2a - 2b - 10c - 2d - 2g + 2h)w_3 + (2a - 2b - 8c - 2d - 2g)w_4 + (2a - 2b - 6c - \\
&- \quad 2d)w_5 + (2a - 4c - 2d)w_6 + (-2c - 2d)w_7 + 4cw_8
\end{aligned}
$$

$$
\begin{aligned}
\tilde{v_7} = &(a + 7b - c + d + e + f + g - h)w_1 + (2a + 12b - 2c + 2d + 2e + 2f - 2h)w_2 \\
&+ \quad (2a + 10b - 2c + 2d + 2e + 2f)w_3 + (2a + 8b - 2c + 2d + 2f)w_4 + (2a + 6b - 2c + \\
&+ \quad 2d)w_5 + (2a + 4b + 2d)w_6 + (2a + 2b)w_7 - 4bw_8
\end{aligned}
$$

$$
\begin{aligned}
\tilde{v_8} = &(-7a + b - c - d + e - f + g + h)w_1 + (-12a + 2b - 2c - 2d + 2e - 2f + 2g) \\
&\quad w_2 + (-10a + 2b - 2c - 2d + 2e - 2f)w_3 + (-8a + 2b - 2c - 2d + 2e)w_4 + (-6a + \\
&+ \quad 2b - 2c - 2d)w_5 + (-4a + 2b - 2c)w_6 + (-2a + 2b)w_7 + 4aw_8
\end{aligned}
$$

Calculando o determinante da matriz de $\tilde{\alpha}$ escrita em relação à base β obtemos um código esférico com $256(a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2)^4$ pontos. Para $a = l$, $b = c = \cdots = h = 0$, $l \in \mathbb{Z}^*$ temos um caso particular da família anterior.

Tomando $\tilde{\tilde{v}}_i = l\tilde{v}_i$, $i = 1, \cdots, 8$, $l \in \mathbb{Z}^*$ é possível gerar uma família de sub-reticulados com $256l^8(a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2)^4$ pontos.

A Tabela (5.10) apresenta alguns códigos esféricos gerados por grupos comutativos em $\mathbb{R}^{16}$ com $256(a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2)^4$ pontos e sua respectiva distância mínima comparada com o limitante da Proposição (4.4.4). A tabela apresenta também, de acordo com [11], um limitante inferior para o número total de casos que deveriam ser analisados.

M	d_{min}	Limitante	Casos
268435456	0.275242	0.277457	261191145086068936653171791724577476325337671666593779679232 0
4294967296	0.195563	0.196271	1121807645550044857430034032128075496671657214078394729825258948683366 4
68719476736	0.138492	0.138812	4818127208935104418174310552778887251195562604401668455827736631474000948415 69 28

Tabela 5.10: **Comparação entre a distância mínima de códigos de grupo comutativo de família (5.5.2) em $\mathbb{R}^{16}$ e o limitante da Proposição (4.4.4).**

Observamos que nesta tabela a distância mínima converge mais rápido para o limitante (4.4.4) do que nos códigos de grupo comutativos obtidos a partir de (5.5.1). Isto acontece devido a que neste caso mais geral possibilitamos mais rotações e portanto mais possibilidades de um maior ângulo entre os vetores do sub-reticulado e os vetores de norma mínima de E_8, com a consequente menor deformação das distâncias medidas em $\mathbb{R}^{16}$.

CAPÍTULO 6

Conclusões Finais e Perspectivas Futuras

Neste trabalho pesquisamos a construção de códigos esféricos gerados por grupos comutativos de matrizes ortogonais. Como as matrizes ortogonais determinam isometrias do espaço euclidiano, segue que estes códigos são geometricamente uniformes. Códigos esféricos gerados deste modo podem ser determinados pelo quociente de dois reticulados, $\frac{\Lambda}{\Lambda'}$ ([18],[17]), quando os vetores que geram Λ' são ortogonais entre si. De maneira geral, dada uma dimensão n e um número de pontos M, queremos saber qual o código esférico $[M, n]$ com a maior distância euclidiana mínima. Este código é chamado *ótimo* e, uma busca exaustiva para encontrá-los envolve um número de casos com limitante inferior da ordem $\begin{pmatrix} M/2 \\ n/2 \end{pmatrix}$. Para um grande número de pontos, a busca por exaustão é inviável computacionalmente, o que motivou-nos a desenvolver um modo de encontrar códigos esféricos muito bons sem a necessidade de analisar casos, bastando calcular somente as distâncias para um número pequeno de pontos (as imagens dos vetores de norma mínima de reticulados conhecidos) para determinarmos a distância mínima do código independente de quão grande seja M. Construímos famílias de sub-reticulados "retangulares" a partir de reticulados com maior densidade de empacotamento, onde a distância mínima se aproxima cada vez mais do limitante dado em [18], para um grande número de pontos. Considerando reticulados Λ com

maior densidade de empacotamento nas dimensões 2, 3, 4 e 8, fizemos o uso de algumas técnicas para a construção de sub-reticulados Λ' de Λ como, por exemplo, a "Construção A" ([14], [19]), os quatérnios e o números de Cayley [28].

Apresentamos também neste trabalho, o conteúdo de dois artigos em conjunto, [1] e [2]. Baseados na construção de reticulados $\mathbb{Z}^n$-rotacionados onde $n = (p-1)/2$ e $p \geq 5$ um número primo apresentada por Bayer-Fluckiger et al. [7], estendemos esta construção para o caso em que $n = 2^{r-1}$, $r \geq 1$ e $n = 3$, fazendo o uso da teoria de reticulado ideal. Em termos de reticulado ideal, dado n, procuramos um corpo de números K de grau n e um ideal $\mathcal{I} \subseteq \mathcal{O}_K$ tal que $\Lambda = (\mathcal{I}, b_\alpha)$ seja equivalente a $\mathbb{Z}^n$, $n \geq 2$, isto é, $\Lambda = (\mathcal{I}, b_\alpha)$ admite uma matriz ortogonal como geradora e, em relação a esta base, a matriz de Gram é a identidade. Do ponto de vista geométrico, um reticulado $\Lambda' = (\mathcal{I}, b_\alpha)$ sobre $\mathcal{I} \subseteq \mathcal{O}_K$ é um sub-reticulado de $\Lambda = (\mathcal{O}_K, b_\alpha)$. A idéia é que dado um reticulado Λ, procura-se um sub-reticulado que seja $\mathbb{Z}^n-$ rotacionado. Quando $n = p^r$, é possível verificar no trabalho de Bayer-Fluckiger [6], que neste caso não temos o isomorfismo entre Λ e $\mathbb{Z}^n$.

Como perspectivas futuras algumas possíveis extensões dos resultados aqui obtidos são:

- pesquisar outras técnicas na obtenção de sub-reticulados nas dimensões 2, 3, 4 e 8.
- encontrar sub-reticulados de outros reticulados com maior densidade de empacotamento conhecidas, por exemplo, D_5, E_6, E_7, K_{12}, Λ_{16} e Λ_{24}.
- pesquisar novas construções algébricas para estes reticulados, pois acreditamos que o uso das construções algébricas destes reticulados possam ser uma boa ferramenta para encontrar sub-reticulados.
- usar a teoria de reticulados ideais para produzirmos sub-reticulados dos reticulados de maior densidade de empacotamento, estabelecendo assim, uma conexão entre reticulado ideal na construção de códigos esféricos gerados por grupos comutativos de matrizes ortogonais.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANDRADE, A.A., ALVES, C. & BERTOLDI, T.C. "Rotated Lattices via the Cyclotomic Field $Q(\zeta_{2^r})$". *International Journal of Applied Mathematics*, v. 19, n. 3, pp. 321-331, August 2006.

[2] ANDRADE, A.A., ALVES, C. & BERTOLDI, T.C. "New constructions of rotated lattices". *International Journal of Applied Mathematics*, v. 20, n. 8, pp. 1079 -1087, 2007.

[3] AUGUSTINI, E. "Constelações de Sinais em Espaços Hiperbólicos". *tese de doutorado*, IMECC- UNICAMP, 2002.

[4] BARNES, E.S. "The optimal lattice quantizer in three dimensions". *Algebraic Discrete Methods* , v. 4, n. 1, pp. 30-41, March 1983.

[5] BAYER-FLUCKIGER, E. "Lattices and Number Fields". *Contemp. Math.*, v. 241, pp. 69-84, 1999.

[6] BAYER-FLUCKIGER, E. "Ideal Lattices". *Cambridge Univ. Press*, pp. 168-184, 2002.

[7] BAYER-FLUCKIGER, E., OGGIER, F. & VITERBO, E. "New Algebraic Constructions of Rotated $\mathbb{Z}^n$-Lattice Constellations for the Rayleigh Fading Channel". *IEEE Transactions on Information Theory*, v. 50, n. 4, pp. 702-714, April 2004.

[8] BENEDETTO, S. & BIGLIERI, E. "Principles of Digital Transmission With Wireless Applications". *Kluwer Academic / Plenum Publishers*, New York, 1999.

[9] BENEDETTO S., BIGLIERI E. & CASTELLANI V. "Digital Transmission Theory". *Prentice-Hall*, 1987.

[10] BERTOLDI, T. C. "Abordagem Algébrica e Geométrica de Reticulados". *Tese de Doutorado*, IMECC-UNICAMP, 2007.

[11] BIGLIERI, E. & ELIA, M. "On the Existence of Groups Codes for the Gaussian Channel". *IEEE Transactions on Information Theory*, v. 18, pp. 399-402, October, 1976.

[12] CARMO, M.P. do "Differential Geometry of Curves and Surfaces". *Prentice-Hall*, 1976.

[13] COHEN, H.C. "A Course in Computational Algebraic Number Theory". *Springer-Verlag*, New York, September 1993.

[14] CONWAY, J.H. & SLOANE, N.J.A. "Sphere Packings, Lattices and Groups". *Springer-Verlag*, New York, 1999.

[15] CONWAY, J.H. & SLOANE, N.J.A. "On lattices equivalent to their duals". *J. Number Theory*, v. 48, pp. 373-382, 1994.

[16] CONWAY, J.H. & SLOANE, N.J.A. "The optimal isodual lattice quantizer in three dimensions". *Advances in Mathematics of Communications*, v. 1, n. 2, pp. 257-260, 2007.

[17] COSTA, S.I.R., AUGUSTINI, E. & PALAZZO, R. "Graphs, Tessellations and Perfect Codes on Flat Tori". *IEEE Transactions on Information Theory*, v. 50, n. 10, pp. 2363-2377, October 2004.

[18] COSTA, S.I.R. & SIQUEIRA, R.M. "Flat Tori, Lattices and Bounds for Commutative Group Codes". *Designs, Codes and Cryptography*, v.49, n.1-3, pp. 307-321, 2008.

[19] COSTA, S.I.R., SIQUEIRA, R.M., LAVOR, C.C. & ALVES, M.M.S. "Uma Introdução à Teoria de Códigos". *Sociedade Brasileira de Matemática Aplicada e Computacional*, São Carlos-SP, 2006.

[20] CRAIG, M."Extreme Forms and Cyclotomy". *Math.* 25, pp. 44-56, 1978.

[21] DABERKOW, M., FIEKER, C., KLÜNERS, J., POHST, M., ROEGNER, K. & WILDANGER, K. "KANT V4". *J. Symbolic Comp.* v. 24, pp. 267-283, 1997. Disponível em: $\langle http://www.math.tu-berlin.de/\sim kant/download.html\rangle$. Último acesso em: 25/06/2008.

[22] ENDLER, O. "Teoria dos Números Algébricos". *IMPA*, Rio de Janeiro, 1986.

[23] ERICSON, T. & ZINOVIEV, V. "Codes on Euclidean Spheres". *North-Holland*, Elsevier Science, 2001.

[24] ESMONDE, J. & MURTY, M. "Problems in Algebraic Number Theory". *Springer-Verlag*, New York, 1999.

[25] FLORES, A.L. "Reticulados em Corpos Abelianos". *Tese de Doutorado*, FEEC - UNICAMP, Campinas, 2000.

[26] FORNEY, G.D., GALLAGER, G.R., LANG, G., LONGSTAFF, F.M. & QURESHI, S.U. "Efficient Modulation for Band-Limited Channels". *IEEE Transactions on Information Theory*, v. 2, pp. 632-647, 1984.

[27] GANTMACHER, F.R. "The theory of matrices". *Publisher: American Mathematical Society*, v. 1, Chelsea, 1959.

[28] GENTILI, E.H. "Dos complexos aos números de Cayley: Uma abordagem geométrica". *Dissertação de Mestrado*, IMECC-UNICAMP, 2002.

[29] HAMKINS, J. "Gaussian Source Coding with Spherical Codes". *IEEE Transactions on Information Theory*, v. 48, n. 11, pp. 2980-2988, November 2002.

[30] HERSTEIN, I.N. "Tópicos de Álgebra". *Editora Polígono S.A.*, 1970.

[31] JESUS, C.H.S de. "Discriminante dos subcorpos de corpos ciclotômicos de condutores potência de um primo ímpar". *Tese de Doutorado*, UFPB, 2007.

[32] LEECH, J. & SLOANE, N.J.A. "Sphere Packing and Error- Correcting Code". *Canad. J. Math*, v. 23, pp. 718-745, 1971.

[33] MARCUS, D.A. "Numbers Fields". *Springer-Verlag*, New York, 1977.

[34] OGGIER, F. "Algebraic Methods for Channel Coding". *Tese de doutorado*, École Polytechnique fédérale de Laisanne, 2005.

[35] RIBENBOIM, P. "Algebraic Numbers". *Wiley - Interscience*, 1972.

[36] SAMUEL, P. "Algebraic Theory of Numbers". *Hermana*, Paris, 1967.

[37] SHANNON, C. "Mathematical Theory of Communication". *Bell Systems Technical Journal*, v. 27, pt. I: pp. 379-423; pt. II: pp. 623-656, 1948.

[38] SIQUEIRA, R.M. "Códigos Esféricos com Simetrias Cíclicas". *Tese de Doutorado*, IMECC-UNICAMP, 2006.

[39] SLEPIAN, D. "Group Codes for the Gaussian Channel". *Bell Syst. Tech. Journal*, v. 47, pp. 575-602, September 1968.

[40] STEWART, I. & TALL, D. "Algebric Number Theory". *Chapman & Hall*, New York, 1987.

[41] STRAPASSON, J.E., "Geometria Discreta e Códigos". *Tese de Doutorado*, IMECC-UNICAMP, 2007.

[42] TOREZZAN, C., COSTA, S.I.R. & STRAPASSON, J.E. "Códigos de grupo comutativo para o canal gaussiano: Aproximando-se do limitante". *XXVI Simpósio Brasileiro de Telecomunicações - SBrT*, Rio de Janeiro, 02-05 de setembro de 2008.

[43] TÓTH G.F. "Sur la représentation d' une population infinie par une nombre fini d' elements". *Acta Math. Acad. Scient. Hung*, v. 10, pp. 229-304, 1959.

[44] WASHINGTON, L.C. "Introduction to Ciclotomic Fields". *Springer-Verlag*, New York, 1982.

[45] VAISHAMPAYAN, V.A. & COSTA, S.I.R. "Curves on a Sphere, Shift-Map Dynamics, and Error Control for Continuous Alphabet Sources". *IEEE Transactions on Information Theory*, v. 49, n. 7, pp. 1658-1672, July 2003.

[46] VITERBO, E. & OGGIER, F. "Algebraic Number Theory and Code Design for Rayleigh Fading Channels", *Foundations and Trends in Communications and Information Theory*, v. 1, n.3, 2004.

ÍNDICE REMISSIVO