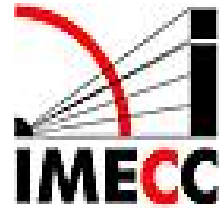




Universidade Estadual de Campinas
Instituto de Matemática, Estatística e
Computação Científica - IMECC
Departamento de Matemática Aplicada



Reticulados algébricos: Abordagem matricial e simulações

Agnaldo José Ferrari

Tese de doutorado

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

Campinas, 2012

¹Este trabalho contou com apoio financeiro parcial do CNPq - processo n° 143269/2008 – 9

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO
CIENTÍFICA

Agnaldo José Ferrari

Reticulados algébricos: Abordagem matricial e simulações

Tese de Doutorado apresentada ao Instituto de
Matemática, Estatística e Computação Científica
da UNICAMP para obtenção do título de doutor
em Matemática Aplicada.

Orientadora: Profa. Dra. Sueli Irene Rodrigues Costa

Este exemplar corresponde à redação final da tese defendida pelo aluno Agnaldo José Ferrari,
e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.



Assinatura do Orientador

Campinas, 2012

FICHA CATALOGRÁFICA ELABORADA POR
ANA REGINA MACHADO - CRB8/5467
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

F412r Ferrari, Agnaldo José, 1969-
Reticulados algébricos : abordagem matricial e simulações /
Agnaldo José Ferrari. – Campinas, SP : [s.n.], 2012.

Orientador: 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. Empacotamento de esferas. 5. Geometria
discreta. I. Costa, Sueli Irene Rodrigues, 1949-. II. Universidade
Estadual de Campinas. Instituto de Matemática, Estatística e
Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em inglês: Algebraic lattices : matrix approach and simulations

Palavras-chave em inglês:

Minimum distance

Lattice theory

Algebraic number theory

Sphere packings

Discrete geometry

Área de concentração: Matemática Aplicada

Titulação: Doutor em Matemática Aplicada

Banca examinadora:

Sueli Irene Rodrigues Costa [Orientador]

Reginaldo Palazzo Júnior

José Plínio de Oliveira Santos

Antonio Aparecido de Andrade

José Carmelo Interlando

Data de defesa: 15-06-2012

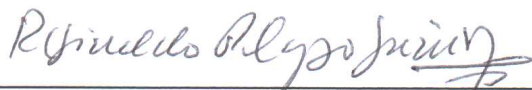
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 15 de junho de 2012 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.



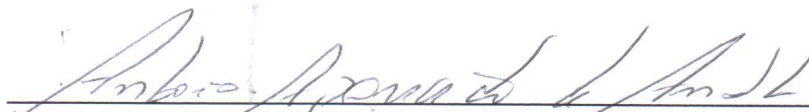
Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA



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



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



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



Prof(a). Dr(a). JOSÉ CARMELO INTERLANDO

“Há um tempo em que é preciso abandonar as roupas usadas, que já tem a forma do nosso corpo, e esquecer os nossos caminhos, que nos levam sempre aos mesmos lugares. É o tempo da travessia: e, se não ousarmos fazê-la, teremos ficado, para sempre, à margem de nós mesmos.”

Fernando Pessoa

À minha esposa Renata
e meu filho Gael,
dedico.

AGRADECIMENTOS

Ao concluir este trabalho agradeço:

À minha orientadora Prof^a. Dr^a. Sueli Irene Rodrigues Costa, pelo conhecimento, experiência, amizade e confiança durante todo este processo. Uma pessoa com um coração enorme e que sempre nos incentiva a melhorar.

Aos membros da banca examinadora, pelas valiosas sugestões.

Ao Prof. Dr. Antonio Aparecido de Andrade, por ter me dado a oportunidade de fazer a primeira iniciação científica no curso de graduação do IBILCE-UNESP e por ter me orientado no curso de Mestrado. Não tenho como retribuir tudo o que fez por mim.

À Prof^a. Dr^a. Grasielle Cristiane Jorge, minha colega desde a graduação, pelos companheirismo nestes 10 anos, e por ter contribuído diretamente em alguns resultados deste trabalho.

Ao Prof. Dr. José Plínio de Oliveira Santos, pelas palavras de incentivo em todos os momentos. Um dos profissionais mais sérios e dedicados que conheci.

Ao Prof. Dr. João Eloir Strapasson, por ter contribuído diretamente neste trabalho.

Ao Prof. Dr. Cristiano Torezzan, pelo apoio desde o início do curso de Doutorado.

Ao Prof. Dr. Felix Silva Costa, meu colega do curso de Doutorado em Matemática Aplicada, pela amizade e companheirismo.

Aos demais colegas do laboratório pelo agradável convívio: Allan, Campello, Cecília, Franz, João Paulo e Nolmar.

Aos amigos Durval, Luis, Casagrande, José Antonio e Danilo, pela acolhida no curso de verão para o doutorado.

Aos amigos Cleber e Jerry, pela acolhida no final do curso de doutorado.

À minha esposa Renata, por ter acreditado num projeto grandioso e ter me dado toda a tranquilidade para poder realizá-lo. Sem o seu carinho e incentivo eu não teria conseguido.

À minha mãe Evanira e ao meu irmão Vilmosnei pelo apoio durante esta caminhada.

Aos meus primos Vamberto e Miriam, que estão sempre torcendo pelo meu sucesso e pelo apoio dado antes mesmo do início deste projeto.

Aos amigos da minha terra natal, que estão sempre comigo: TC, Roberta, Ana Luisa, Mauro, Jesus Claudio, Paulo Franco, Maria Helena, Edmundo e Andréia.

Aos meus tios Orizanir e Ozias, pelo incentivo e apoio dados em momentos difíceis.

Ao meu pai Ambrósio Ferrari (in memoriam), um simples lavrador que trabalhou a vida toda para melhorar a condição de vida da família e que infelizmente não pode vivenciar a conclusão deste projeto. Pai, onde quer que esteja, espero que acompanhe este momento, eu te amo.

Ao CNPQ, pelo apoio financeiro.

RESUMO

Neste trabalho abordamos a construção de reticulados usando propriedades da Teoria Algébrica dos Números. Enfocamos a construção de alguns reticulados com características especiais, conhecidos na literatura, via reticulados ideais, através de uma abordagem matricial e algorítmica. Além disso, construímos uma família de reticulados D_n rotacionados, para n uma potência de 2, apresentando boas estimativas de distância produto e diversidade, parâmetros que minimizam probabilidade de erro em canais Rayleigh com desvanecimento, e apresentando boa densidade de empacotamento, em relação aos reticulados $\mathbb{Z}^n$, parâmetro que minimiza a probabilidade de erro em canais gaussianos. Apresentamos também a construção de uma família de reticulados unimodulares em dimensão potência de 2 que, considerando o “trade-off” entre distância produto mínima relativa e rotulamento de bit, oferece melhor desempenho para o canal Rayleigh com desvanecimento do que as famílias de $\mathbb{Z}^n$ rotacionados conhecidas na literatura.

ABSTRACT

In this work we approach lattice constructions using properties of algebraic number theory. One focus is on the construction of some well known lattices via ideal lattices, through a matrix and algorithmic approach. Furthermore, one constructs a family of rotated D_n lattices, for n a power of 2, presenting good estimates for product distance and diversity, parameters which minimize error probability transmission for the Rayleigh fading channels and presenting good packing density, when compared to $\mathbb{Z}^n$ lattices, parameter which minimize error probability transmission for Gaussian channels. We present a new construction of a family of n -dimensional unimodular lattices when n is a power of 2 that, considering the “trade-off” between minimum product distance and bit labeling, offers better performance for the Rayleigh fading channel than the families of rotated $\mathbb{Z}^n$ lattices known on literature.

SUMÁRIO

Lista de Tabelas	xix
Lista de Figuras	xxi
Lista de símbolos	xxiii
Introdução	1
1 Preliminares	5
1.1 Teoria da Informação e Codificação	5
1.1.1 Canal gaussiano	8
1.1.2 Canal Rayleigh com desvanecimento	11
1.2 Conexão entre Reticulados e Teoria da Informação	14

1.3	Motivação e objetivos do trabalho	17
1.4	Conceitos básicos	18
1.4.1	Módulos	18
1.4.2	Teoria Algébrica dos Números	19
1.4.3	Corpos ciclotômicos	23
2	Reticulados	31
2.1	Conceitos básicos	31
2.2	Empacotamento esférico	36
2.3	Alguns reticulados especiais e suas propriedades	40
3	Reticulados algébricos	53
3.1	Conceitos básicos	54
3.2	Reticulado ideal	56
3.3	Reticulados via a perturbação do homomorfismo canônico	58
3.3.1	Diversidade	61
3.3.2	Distância produto mínima	62
3.3.3	Densidade de centro	67
3.4	Resultados conhecidos na literatura	70
4	Construção algébrica de reticulados densos - Abordagem matricial	79
4.1	Matriz mudança de base - Algoritmo de busca	80

4.2	Reticulados rotacionados - condições de existência	83
4.2.1	Reticulado A_2	84
4.2.2	Reticulado D_4	86
4.2.3	Reticulado E_6	88
4.2.4	Reticulado E_8	90
4.2.5	Reticulado K_{12}	91
4.3	Distância produto mínima dos reticulados densos - Comparação	98
5	Construção de reticulados D_n sobre corpos totalmente reais	101
5.1	Via Reticulados ideais	102
5.1.1	Reticulados D_n rotacionados, $n = 2^{r-2}$, $r \geq 4$	102
5.2	Via $\mathbb{Z}$ -módulos	115
5.2.1	Reticulados D_n rotacionados, $n = 2^{r-2}$, $r \geq 4$	115
5.2.2	Reticulados D_n rotacionados, $n = \frac{p-1}{2}$, p primo	120
6	Construção de reticulados unimodulares sobre corpos totalmente reais	125
6.1	Reticulados $\mathbb{Z}^4$ e $\mathbb{Z}^8$ rotacionados	140
6.1.1	Distância produto mínima	143
6.1.2	Distância produto mínima - Comparação com outras construções . . .	143
6.2	Reticulados $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ rotacionados	144
6.2.1	Distância produto mínima	151

6.2.2	Distância produto mínima - Comparação com outras construções . .	151
6.3	Reticulados $\mathbb{Z}^8 \oplus \frac{1}{\sqrt{2}}\mathcal{E}_8^r$ rotacionados	154
6.3.1	Densidade de centro	155
6.3.2	Distância produto mínima	156
	Perspectivas futuras	159
	Referências bibliográficas	161
	Índice Remissivo	167

LISTA DE TABELAS

3.1	Discriminante mínimo - dimensão 2 a 8	71
3.2	Polinômio minimal de θ , onde $\mathbb{K} = \mathbb{Q}(\theta)$ - dimensão 2 a 8.	73
3.3	Distância produto mínima de reticulados $\mathbb{Z}^n$ - dimensão 2 a 30.	78
4.1	Parâmetros do reticulado ideal rotacionado de A_2	84
4.2	Parâmetros do reticulado ideal rotacionado de D_4	87
4.3	Parâmetros do reticulado ideal rotacionado de E_6	89
4.4	Parâmetros do reticulado ideal rotacionado de E_8	90
4.5	Parâmetros do reticulado ideal rotacionado de K_{12}	92
4.6	Distância produto mínima de A_2 , D_4 , E_6 , E_8 e K_{12} - Comparação.	98
5.1	Parâmetros do reticulado ideal rotacionado de D_n	103
5.2	Parâmetros do reticulado ideal rotacionado de D_n - dimensões 4, 8 e 16. . . .	103

5.3	Distâncias produto mínimas de $\mathbb{Z}^n$ e D_n - Comparação	113
5.4	Distância produto e densidade de centro $\mathbb{Z}^n$ e D_n via $\mathbb{Z}$ -módulos - Comparação.	119
5.5	Distância produto e densidade de centro de $\mathbb{Z}^n$ e D_n - Comparação.	124
6.1	Parâmetros do reticulado unimodular rotacionado - dimensões 4, 8 e 16.	127
6.2	Parâmetros do reticulado unimodular rotacionado - caso geral.	127
6.3	Elemento α do reticulado ideal unimodular - dimensões 4, 8 e 16.	127
6.4	Distância produto mínima de $\mathbb{Z}^4$ e $\mathbb{Z}^8$ via $\mathbb{Q}(\zeta_{2^r, 3, 5})$ - Comparação.	144
6.5	Distância produto mínima de $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ na dimensão 16 - Comparação.	152
6.6	Distância produto mínima de $\mathbb{Z}^n$ e $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, $n \geq 32$ - Comparação.	153

LISTA DE FIGURAS

1.1	Modelo do sistema de comunicação	7
1.2	Propagação de sinal por múltiplos percursos	12
2.1	Reticulado $\mathbb{Z}^2$ com uma região fundamental.	32
2.2	Regiões de Voronoi associadas ao reticulado Λ	40
2.3	Reticulado A_2	42
2.4	Reticulado hexagonal com região de Voronoi associada à origem.	43
2.5	Empacotamento do reticulado fcc.	44
2.6	Empacotamento do reticulado bcc.	45
5.1	Distâncias produto mínimas de $\mathbb{Z}^n$ e D_n - Gráfico	114
6.1	Distância produto mínima $\mathbb{Z}^n$ e $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ - gráfico.	153

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
$\mathbb{L}, \mathbb{M}, \mathbb{K}$	corpos de números
$\mathbb{L}/\mathbb{K}$	extensão de corpos
$[\mathbb{L} : \mathbb{K}]$	grau de $\mathbb{L}/\mathbb{K}$
$Gal(\mathbb{L}/\mathbb{K})$	grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$Aut(\mathbb{L})$	conjunto dos automorfismos do corpo $\mathbb{L}$
$\mathbb{L}^H$	corpo fixo pelo conjunto H
$A[X]$	anel dos polinômios sobre A em X
$\mathbb{K}(R_f)$	corpo de raízes do polinômio f
$Tr_{\mathbb{L}/\mathbb{K}}$	traço em relação à extensão $\mathbb{L}/\mathbb{K}$
$\mathcal{N}_{\mathbb{L}/\mathbb{K}}$	norma em relação à extensão $\mathbb{L}/\mathbb{K}$
$\mathcal{O}_{\mathbb{K}}$	anel dos inteiros algébricos do corpo $\mathbb{K}$
$\mathcal{A}$	ideal
$d_{\mathbb{K}}$	discriminante do corpo $\mathbb{K}$

$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$	codiferente em relação à extensão $\mathbb{K}/\mathbb{Q}$
$\mathcal{N}(\mathcal{A})$	norma do ideal $\mathcal{A}$
ζ_n	$e^{2\pi i/n} = \cos \frac{2\pi}{n} + \operatorname{sen} \frac{2\pi}{n}$: raiz primitiva n-ésima da unidade
$\varphi(n)$	função de Euler para o inteiro n
$\mathbb{Q}(\zeta_n)$	n-ésimo corpo ciclotômico
$\mu(n)$	função de Möbius para o inteiro n
vol	volume
$\det(A)$	determinante de A
Δ	densidade de empacotamento
δ	densidade de centro
τ	kissing number
η	norma mínima
ρ	raio de empacotamento
d_{min}	distância mínima entre dois pontos
div	diversidade
d_p^l	distância l-produto
$d_{p,min}$	distância produto mínima
$d_{p,rel}$	distância produto mínima relativa
bcc	reticulado body-centered cubic
fcc	reticulado face-centered cubic
mcc	reticulado mean-centered cubic
r_1	número de mergulhos canônicos reais
r_2	metade do número de mergulhos canônicos complexos
$\bar{x}$	conjugado complexo do elemento x
$AWGN$	additive white gaussian noise (ruído aditivo gaussiano branco)
CSI	channel state information (estado de informação do canal)
SNR	relação sinal-ruído

E_b	energia média por bit
N_0	variância gaussiana
E_b/N_0	razão sinal-ruído
ML	máxima verossimilhança
P_e	probabilidade de erro
erf	função erro
$erfc$	função erro complementar
$b_\alpha(e_i, e_j)$	forma traço
t_α	$\min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x \bar{x}), x \in \mathcal{A}, x \neq 0\}$

INTRODUÇÃO

O presente trabalho tem como marco inicial os estudos realizados durante o curso de Mestrado em Matemática no IBILCE-UNESP sob a orientação do Prof. Dr. Antonio Aparecido de Andrade. Os estudos baseiam-se na obtenção de reticulados via Teoria Algébrica dos Números. Dado $\mathbb{K}$ um corpo de números, a imagem de um ideal $\mathcal{A}$, contido no anel dos inteiros algébricos do corpo $\mathbb{K}$, pelo homomorfismo canônico $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ ou pela perturbação do homomorfismo canônico $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ é um reticulado no $\mathbb{R}^n$, chamado de reticulado algébrico. Tais reticulados constituem a classe dos reticulados ideais, que são reticulados dotados com uma forma traço. Uma importante aplicação dos reticulados está relacionada à Teoria da Informação, mais especificamente à Teoria dos Códigos Corretores de Erros, que tem como um marco o trabalho de Shannon [16]. Constelações de sinais com estrutura de reticulados são consideradas boas para transmissão de sinais, pois a estrutura linear e simétrica dos reticulados simplifica a tarefa de decodificação.

Com o ingresso no Programa de Doutorado em Matemática Aplicada no IMECC-UNICAMP, foi possível assimilar novas técnicas para resolução de problemas, como por exemplo o uso de novos recursos computacionais e a familiarização com os algoritmos. Aliado a isso, ressalto a importância de algumas disciplinas da grade curricular do programa, como por exemplo a disciplina MT402 - Matrizes, que foi de suma importância para o de-

seenvolvimento deste trabalho.

O objetivo deste trabalho é a construção de reticulados algébricos que propiciem constelações de sinais que sejam eficientes para transmissão em canal gaussiano e canal Rayleigh com desvanecimento, que são os canais mais frequentes em sistemas de comunicação digital.

Mais especificamente, este trabalho está organizado como segue:

O Capítulo 1 é dividido em duas partes:

- (i) Introduzimos, de forma concisa, princípios básicos relacionados à Teoria da Informação e Codificação, com o intuito de situar o leitor no contexto do tema aqui desenvolvido. Apresentamos os canais mais comumente usados nos sistemas de comunicação, o canal gaussiano e uma estimativa para a probabilidade de erro neste canal com um limitante superior (Limitante de Bhattacharyya), e o canal Rayleigh com desvanecimento, também com uma estimativa para a probabilidade de erro. Ainda nesta parte, explicamos em detalhes a motivação e objetivos do trabalho, a aplicação dos reticulados algébricos à Teoria da Informação.
- (ii) Fazemos uma breve revisão de conceitos básicos que serão utilizados no desenvolvimento do trabalho, a saber: Módulos e Submódulos, Tópicos de Teoria Algébrica dos Números e Teoria de Galois, e conceitos relacionados a corpos ciclotômicos, pois a maioria dos resultados conhecidos na literatura é baseada nos reticulados obtidos sobre estes corpos de números, assim como a nossa contribuição neste trabalho.

No Capítulo 2 introduzimos os conceitos relativos a reticulados enfocando seus principais parâmetros: matriz geradora, matriz de Gram, região fundamental, região de Voronoi, determinante, volume; além disso são apresentadas as definições de sub-reticulado, reticulado dual, reticulado isodual e reticulados equivalentes. Abordamos também conceitos relativos a empacotamento esférico de reticulados: densidade de empacotamento, raio de empacotamento, norma mínima, densidade de centro, raio de cobertura, densidade de cobertura e número de vizinhos, “kissing number”. Por fim, apresentamos alguns reticulados especiais, conhecidos na literatura.

No Capítulo 3 introduzimos os conceitos relativos a reticulados algébricos e reticulados ideais. Mostramos que o reticulado obtido via perturbação do homomorfismo canônico é um reticulado ideal e estabelecemos seus principais parâmetros: diversidade, distância produto e densidade de centro. Por fim, apresentamos as principais contribuições conhecidas na literatura referente aos reticulados algébricos e suas aplicações à Teoria da Informação.

No Capítulo 4 construímos algebricamente versões rotacionadas dos reticulados A_2 , D_4 , E_6 , E_8 e K_{12} via subcorpos maximais reais de corpos ciclotômicos. A prova da versão rotacionada do reticulado K_{12} é feita através de uma abordagem matricial e com o uso de um algoritmo que busca pela matriz mudança de base. Além disso, calculamos a distância produto mínima destes reticulados e comparamos com os reticulados $\mathbb{Z}^n$ nas respectivas dimensões. Em [28] são construídos os mesmos reticulados mas com uma diferente abordagem.

No Capítulo 5 tendo em vista construir reticulados que possam ser utilizados simultaneamente nos canais gaussiano e Rayleigh com desvanecimento, reproduzimos algumas famílias de reticulados D_n rotacionados de duas maneiras distintas, via reticulados ideais e via $\mathbb{Z}$ -módulos. Estas construções fazem parte do artigo conjunto “Rotated D_n -lattices” [33], submetido em Dezembro de 2011. Além disso, comparamos as distâncias produto mínimas com outras constelações.

No Capítulo 6, usando o subcorpo maximal real do corpo ciclotômico $\mathbb{Q}(\zeta_{2^{r-3.5}})$, reproduzimos os reticulados $\mathbb{Z}^4$ e $\mathbb{Z}^8$ para $r = 1$ e $r = 2$, respectivamente. Para $r \geq 3$, reproduzimos uma nova família de reticulados unimodulares que são versões rotacionadas do reticulado $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, onde $\mathcal{E}_8^r$ representa a soma direta das $2^{r-2} - 1$ cópias do reticulado E_8 . Nos três casos, calculamos a distância produto mínima e comparamos o desempenho. Levando em conta o “trade-off” entre distância produto mínima e forma da constelação, a família $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ apresenta melhor desempenho para o canal Rayleigh com desvanecimento em comparação com as constelações $\mathbb{Z}^n$ conhecidas na literatura. Fizemos também, uma perturbação do reticulado $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ de modo que o reticulado perturbado possui melhor densidade de empacotamento, e construímos um algoritmo para verificar o efeito da perturbação sobre a

distância produto mínima do novo reticulado.

Na parte final enumeramos as perspectivas futuras de continuidade deste trabalho.

CAPÍTULO 1

PRELIMINARES

Neste capítulo introduzimos de forma concisa os principais conceitos relativos à Teoria da Informação e Codificação, apresentando os canais mais comumente usados para transmissão de sinais, o canal gaussiano e o canal Rayleigh com desvanecimento. Aliado a isso, fazemos também a conexão entre Reticulados e Teoria de Informação e expomos a motivação e objetivos do nosso trabalho. As referências utilizadas foram [13], [29], [30], [36], [38], [42], [57], [58] e [61]. Introduzimos também alguns conceitos básicos necessários ao desenvolvimento do tema.

1.1 Teoria da Informação e Codificação

Um sistema de comunicação pode ser considerado como um conjunto de equipamentos e meios físicos com a finalidade de transportar uma informação de uma fonte até um des-

tinatório usando um canal de comunicação. A seguir apresentamos a modelagem para este sistema.

- **Fonte**

Pode ser uma pessoa ou uma máquina que gera uma onda sonora contínua ou uma sequência de símbolos discretos. No caso de fonte contínua, faz-se a conversão para símbolos discretos. Assim, pode-se considerar que os dados gerados pela fonte são símbolos de um alfabeto $\mathcal{A}$.

- **Codificador de Fonte**

Associa as saídas da fonte às sequências $(\mathbf{u}_j) = (u_1, \dots, u_k)$ 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.

- **Codificador de Canal**

Transforma a sequência de informação $(\mathbf{u}_j)$ em outra sequência $(\mathbf{v}_j) = (v_1, \dots, v_n)$ chamada de palavra código de canal. Este estágio tem por objetivo inserir redundância na sequência $(\mathbf{u}_j)$ com o objetivo de 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. Para a transmissão, o modulador então associa a cada palavra código um símbolo analógico, que é então enviado pelo canal.

- **Canal**

É o meio físico por onde a informação é transmitida/armazenada e está sujeito a vários tipos de ruídos, imperfeições e interferências que geram distorções, de forma que o sinal recebido nem sempre coincide com o sinal enviado. São exemplos de canais:

(i) **Canais de transmissão:** Linhas telefônicas, meios de propagação de sinais entre

antenas de rádio, antenas de microondas, estações terrestres e satélites, fibras óticas, cabos coaxiais, etc.

(ii) **Canais de armazenagem:** Fitas cassetes, CD's, memórias de computador, etc.

Na próxima seção, daremos detalhes sobre alguns tipos de canais.

- **Demodulador**

O demodulador recebe o sinal (que pode estar ou não com ruído) e faz a melhor estimativa para o sinal enviado, fornecendo uma sequência de símbolos de $\mathcal{A}$.

- **Decodificador de canal**

Devido ao ruído, é possível que a sequência de símbolos na saída do demodulador não seja uma palavra código. Então o decodificador de canal associará uma palavra código, que é a melhor estimativa para o possível símbolo enviado.

- **Decodificador de fonte**

Associa a palavra código obtida do decodificar de canal à suposta sequência original de símbolos enviada. Quando a fonte é contínua, neste momento o sinal discreto é convertido em sinal contínuo. Em um sistema eficiente, a estimativa será uma reprodução do sinal gerado pela fonte.

Uma esquematização deste processo é apresentado na Figura 1.1.

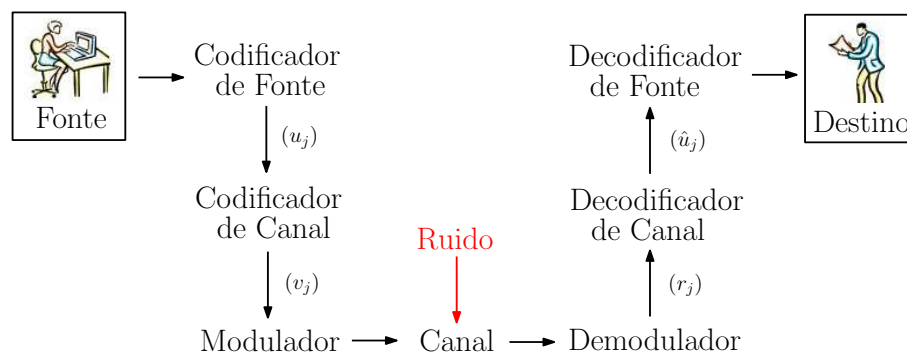


Figura 1.1: Modelo do sistema de comunicação

1.1.1 Canal gaussiano

O canal gaussiano é um canal de comunicação do tipo AWGN (*Additive White Gaussian Noise*) onde predominam atenuações e atrasos de propagação do sinal, e o termo AWGN é usado para caracterizar os canais onde o ruído que interfere na comunicação é um ruído branco adicionado ao sinal. A escolha de uma constelação de sinais para a transmissão através deste tipo de canal constitui um dos principais problemas na concepção dos sistemas de comunicação.

O desempenho de uma constelação de sinais é medido pela probabilidade de erro na transmissão dos sinais $P(e)$. Na modulação de sinais, o objetivo é encontrar meios para determinar ou estimar a probabilidade de erro associada. Quando consideramos transmissões codificadas, palavras código são vetores reais n -dimensionais $\mathbf{x} = (x_1, \dots, x_n)$ tomados de alguma constelação de sinal $\mathcal{S} \subseteq \mathbb{R}^n$. Uma m -upla de bits de entrada é associada a um ponto de sinal $\mathbf{x} = (x_1, \dots, x_n)$, e o sinal recebido será

$$\mathbf{r} = \mathbf{x} + \mathbf{n}, \quad (1.1.1)$$

onde $\mathbf{n} = (n_1, \dots, n_n)$ é uma amostra de um processo aleatório gaussiano com variância N_0 (unilateral) e média nula. Cada ponto é rotulado por m dígitos binários.

A *eficiência espectral* mede o número de bits por duas dimensões,

$$\eta = \frac{2m}{n},$$

e a *relação sinal ruído* por bit é dada por

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

onde E_b é a energia média por bit e N_0 é a variância gaussiana (potência do ruído).

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 medida

$$m(\mathbf{x}|\mathbf{r}) = \sum_{i=1}^n ||r_i - x_i||^2 \quad (1.1.2)$$

A minimização de (1.1.2) pode ser uma operação muito complexa quando se tem um conjunto de sinais arbitrários com um grande número de pontos.

Probabilidade de erro

Denotamos por $P_e(\mathcal{S})$ a probabilidade de erro quando enviamos um ponto da constelação de sinais $\mathcal{S}$ e por $P(\mathbf{x}|\hat{\mathbf{x}})$ a probabilidade de erro par-a-par, ou seja, a probabilidade de quando $\mathbf{x}$ é transmitido, o ponto recebido está mais próximo de $\hat{\mathbf{x}}$ do que de $\mathbf{x}$ de acordo com a métrica definida em (1.1.2). Para uma constelação de sinais arbitrária $\mathcal{S}$, temos

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

Se a constelação de sinais $\mathcal{S}$ for geometricamente uniforme, então a probabilidade de erro quando enviamos qualquer ponto da constelação é a mesma, $P_e(\mathcal{S}) = P_e(\mathcal{S}|\mathbf{x})$, para qualquer ponto transmitido $\mathbf{x} \in \mathcal{S}$. Assumiremos que $\mathcal{S}$ é uma constelação finita.

Aplicando o limitante da união, temos um limitante superior para a probabilidade de erro do ponto

$$P_e(\mathcal{S}) \leq \sum_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x}|\hat{\mathbf{x}}). \quad (1.1.3)$$

A primeira desigualdade leva em consideração os efeitos de bordo da constelação finita $\mathcal{S}$. Vamos agora introduzir duas funções muito utilizadas em Teoria da Comunicação. A primeira delas é a *função erro*, definida por

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

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

$$erfc : \mathbb{R}_+ \longrightarrow [0, 1]$$

$$x \mapsto \frac{2}{\sqrt{\pi}} \int_0^\infty e^{-t^2} dt.$$

Após alguns cálculos, é demonstrado em [58] que

$$P(\mathbf{x}|\hat{\mathbf{x}}) = \frac{1}{2} \operatorname{erfc} \left(\frac{\|\mathbf{x} - \hat{\mathbf{x}}\|}{2\sqrt{N_0}} \right). \quad (1.1.4)$$

O cálculo aproximado da probabilidade de erro pode ser feito por limitantes inferiores e superiores como, por exemplo, o limitante de Bhattacharyya (limitante superior) [58], que será estabelecido a seguir.

Consideremos uma constelação $\mathcal{S} = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M\}$ de M sinais equiprováveis que esteja representada no $\mathbb{R}^n$. Para obtermos um limitante superior para a probabilidade de erro observamos que um erro ocorre quando, usando a decodificação com a regra (ML) na Equação 1.1.2, o ponto recebido $\mathbf{r}_j$ está mais próximo de $\hat{\mathbf{x}}_j$ do que de $\mathbf{x}_j$, isto é, $m(\hat{\mathbf{x}}_j|\mathbf{r}) \leq m(\mathbf{x}_j|\mathbf{r})$. Efetuando alguns cálculos e combinando as Equações (1.1.3) e (1.1.4) podemos escrever

$$P_e(\mathcal{S}) \leq \frac{1}{M} \sum_{j=1}^M \sum_{\hat{\mathbf{x}}_j \neq \mathbf{x}_j} \frac{1}{2} \operatorname{erfc} \left(\frac{\|\mathbf{x}_j - \hat{\mathbf{x}}_j\|}{2\sqrt{N_0}} \right). \quad (1.1.5)$$

e conseqüentemente,

$$P_e(\mathcal{S}) \leq \frac{1}{M} \sum_{j=1}^M \sum_{\hat{\mathbf{x}}_j \neq \mathbf{x}_j} \exp \left(-\frac{\|\mathbf{x}_j - \hat{\mathbf{x}}_j\|^2}{4N_0} \right), \quad (1.1.6)$$

que é conhecido como *limitante de Bhattacharyya*.

Podemos também estabelecer um limitante superior um pouco pior, mas que depende do conhecimento de um simples parâmetro da constelação de sinais. Definimos

$$d_{\min} = \min\{\|\mathbf{x}_j - \hat{\mathbf{x}}_j\|; \mathbf{x}_j \neq \hat{\mathbf{x}}_j, \mathbf{x}_j, \hat{\mathbf{x}}_j \in \mathcal{S}\},$$

assim,

$$\operatorname{erfc} \left(\frac{\|\mathbf{x}_j - \hat{\mathbf{x}}_j\|}{2\sqrt{N_0}} \right) \leq \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right)$$

e conseqüentemente da Equação (1.1.5) obtemos

$$P_e(\mathcal{S}) \leq \frac{1}{M} \sum_{j=1}^M \sum_{\hat{\mathbf{x}}_j \neq \mathbf{x}_j} \frac{1}{2} \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right) = \frac{M-1}{2} \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right). \quad (1.1.7)$$

Usando um raciocínio análogo, podemos estabelecer um limitante inferior para a probabilidade de erro dado por

$$P_e(\mathcal{S}) \geq \frac{1}{M} \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right). \quad (1.1.8)$$

Das Equações (1.1.7) e (1.1.8) temos que

$$\frac{1}{M} \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right) \leq P_e(\mathcal{S}) \leq \frac{M-1}{2} \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right). \quad (1.1.9)$$

Percebe-se que para uma quantidade de pontos M fixa, a probabilidade de erro depende de $d_{\min}$. Assim, dizemos que $d_{\min}$ é o parâmetro mais importante que determina a qualidade da constelação de sinais, especialmente para ruídos pequenos. Uma constelação com o maior valor para $d_{\min}$ possui a menor probabilidade de erro. Mas, quando a probabilidade de erro não é muito pequena, maximizar $d_{\min}$ talvez não seja suficiente para minimizar $P_e(\mathcal{S})$. Em [58] é mostrado que um outro parâmetro torna-se relevante na determinação de $P_e(\mathcal{S})$. Temos que

$$P_e(\mathcal{S}) \lesssim \frac{\nu}{2} \operatorname{erfc} \left(\frac{d_{\min}}{2\sqrt{N_0}} \right), \quad (1.1.10)$$

onde ν denota o número de sinais a uma distância $d_{\min}$ de um sinal fixo $\mathbf{x} \in \mathcal{S}$, e $\lesssim$ significa uma aproximação do limitante superior e $P_e(\mathcal{S})$ fica cada vez mais próximo do limitante a medida que N_0 aproxima-se de zero.

Agora, temos que (1.1.10) pode ser reescrita como

$$P_e(\mathcal{S}) \lesssim \frac{\nu}{2} \operatorname{erfc} \left(\sqrt{\frac{nS}{2}} \Delta^{1/n} \right), \quad (1.1.11)$$

onde S é relação sinal ruído normalizada e Δ é a densidade de empacotamento da constelação de sinais ([42], pp.71 – 72). Quanto maior o valor de Δ menor é a probabilidade de erro para a constelação de sinais.

1.1.2 Canal Rayleigh com desvanecimento

O canal Rayleigh com desvanecimento é um canal de comunicação terrestre que possui como principal característica a propagação por múltiplos percursos, que são formados pela

reflexão e/ou difração do sinal transmitido em estruturas próximas ao receptor, tais como edifícios e árvores (Figura 1.2). A soma vetorial dos vários sinais dos múltiplos percursos pode resultar em uma interferência construtiva ou destrutiva do sinal recebido, assim dizemos que o ruído é multiplicativo. A intensidade do sinal pode variar ao longo do tempo, e 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.

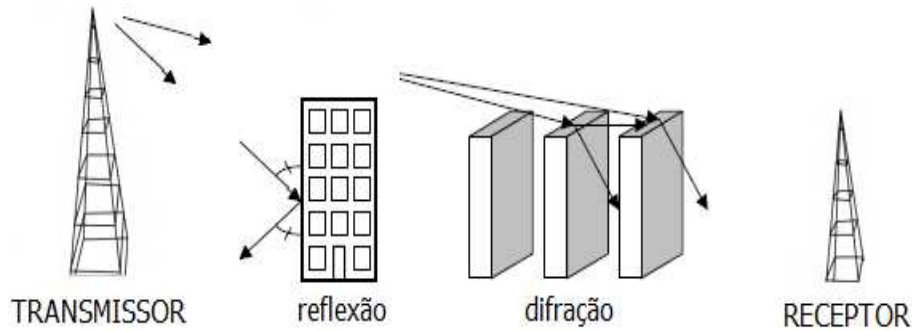


Figura 1.2: Propagação de sinal por múltiplos percursos

Quando um sinal $\mathbf{x} = (x_1, \dots, x_n)$ tomado de alguma constelação de sinal $\mathcal{S} \subseteq \mathbb{R}^n$ é transmitido através de um canal com desvanecimento, o sinal recebido é

$$\mathbf{r} = \alpha * \mathbf{x} + \mathbf{n}, \quad (1.1.12)$$

onde $\mathbf{n} = (n_1, \dots, n_n)$ é o ruído gaussiano e $\alpha = (\alpha_1, \dots, \alpha_n)$ são os coeficientes de desvanecimento com segundo momento unitário e $*$ representa o produto componente a componente.

Assumindo CSI (Channel State Information) perfeito, a detecção por *Máxima Verossi-*

milhança (ML) requer a minimização da seguinte medida

$$m(\mathbf{x}|\mathbf{r}, \alpha) = \sum_{i=1}^n ||r_i - \alpha_i x_i||^2 \quad (1.1.13)$$

Probabilidade de erro

Vimos que, denotando por $P_e(\mathcal{S})$ a probabilidade de erro quando enviamos um ponto da constelação de sinais $\mathcal{S}$ e por $P(\mathbf{x}|\hat{\mathbf{x}})$ a probabilidade de erro par a par, ou seja, a probabilidade de quando $\mathbf{x}$ é transmitido, o ponto recebido está mais próximo de $\hat{\mathbf{x}}$ do que de $\mathbf{x}$ de acordo com a métrica definida em (1.1.13), para uma constelação de sinais arbitrária $\mathcal{S}$, temos

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

Aplicando o limitante da união, temos um limitante superior para a probabilidade de erro do ponto

$$P_e(\mathcal{S}) \leq \sum_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x}|\hat{\mathbf{x}}). \quad (1.1.14)$$

Em [38] é visto que a probabilidade de erro para uma relação sinal-ruído grande satisfaz

$$P(\mathbf{x}|\hat{\mathbf{x}}) \leq \frac{1}{2} \prod_{x_i \neq \hat{x}_i} \frac{8N_0}{(x_i - \hat{x}_i)^2} = \frac{1}{2} \frac{(8N_0)^l}{d_p^l(\mathbf{x}, \hat{\mathbf{x}})^2}, \quad (1.1.15)$$

onde

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

é a *distância l-produto* de $\mathbf{x}$ a $\hat{\mathbf{x}}$ quando estes dois pontos diferem em l componentes. Agora, a Equação (1.1.14) reescrita satisfaz

$$P_e(\mathcal{S}) \leq \sum_{l=L}^n \frac{1}{2} \frac{(8N_0)^l}{d_p^l(\mathbf{x}, \hat{\mathbf{x}})^2}, \quad (1.1.16)$$

onde L é o número mínimo de componentes distintas entre quaisquer dois pontos da constelação, e é chamado de *diversidade*. Em outras palavras, L é a distância mínima de Hamming entre quaisquer dois pontos da constelação. A fim de minimizarmos a probabilidade

de erro no canal Rayleigh com desvanecimento, devemos minimizar o lado direito da desigualdade (1.1.16). Nota-se que quanto maior for o valor de L menos termos existirão no somatório, assim maximizar L diminui o limitante para a probabilidade de erro. Em seguida, percebe-se que $d_p^L(\mathbf{x}, \hat{\mathbf{x}})^2$ aparece no denominador em cada termo do somatório, assim maximizar $d_{p,min} = \min\{d_p^L(\mathbf{x}, \hat{\mathbf{x}})\}$ também diminui o limitante para a probabilidade de erro. Assim, para obtermos uma baixa probabilidade de erro assintoticamente, em ordem de relevância temos que

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

A diversidade é limitada pela dimensão n da constelação, e a diversidade máxima é $L = n$.

1.2 Conexão entre Reticulados e Teoria da Informação

Nas duas seções anteriores apresentamos dois canais comumente usados em comunicação digital, e dada uma constelação de sinais $\mathcal{S}$ apresentamos limitantes para a probabilidade de erro nesses canais.

Constelações de sinais tendo estrutura de reticulados são consideradas boas para transmissão de sinais com alta eficiência espectral (número de bits por duas dimensões), e satisfazem algumas condições pré-estabelecidas:

1. A constelação de sinais $\mathcal{S}$ é *geometricamente uniforme*, pois um reticulado possui esta característica.
2. Uma m -upla de bits de entrada é associada a um ponto de sinal $\mathbf{x} = (x_1, \dots, x_n)$ no espaço euclidiano n -dimensional $\mathbb{R}^n$. Cada ponto é rotulado por m dígitos binários.

Quando usamos códigos reticulados, a constelação de sinais $\mathcal{S}$ finita (de cardinalidade 2^m) é obtida das primeiras camadas de pontos do reticulado.

Para a transmissão em um canal gaussiano, vimos por (1.1.11) que a probabilidade de erro satisfaz

$$P_e(\mathcal{S}) \lesssim \frac{\nu}{2} \operatorname{erfc} \left(\sqrt{\frac{nS}{2}} \Delta^{1/n} \right),$$

onde ν denota o número de vizinhos a um sinal fixo $\mathbf{x} \in \mathcal{S}$ e Δ denota a densidade de empacotamento da constelação. Se a constelação tem a estrutura de reticulado então ν denota o número de vizinhos “kissing number” de um ponto fixo do reticulado, e Δ denota a densidade de empacotamento do reticulado associado à constelação. Portanto, 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 com bom desempenho podem ser obtidas de reticulados com alta densidade de empacotamento, e a estrutura linear e simétrica dos reticulados usualmente simplifica a tarefa de decodificação.

Para a transmissão em um canal Rayleigh com desvanecimento, o problema é construir constelações de sinais com energia média mínima para uma desejada taxa de erro, dada a eficiência espectral. Vimos por (1.1.16) que a probabilidade de erro satisfaz

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

onde $d_p^l(\mathbf{x}, \hat{\mathbf{x}})$ é a *distância l-produto* de $\mathbf{x}$ a $\hat{\mathbf{x}}$ quando estes dois pontos diferem em l componentes e L é o número mínimo de componentes distintas entre quaisquer dois pontos da constelação, chamado *diversidade*. Para minimizarmos a probabilidade de erro, em ordem de relevância, temos que

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

Uma interessante abordagem foi feita usando resultados da Teoria Algébrica dos Números [45]. Através de corpos de números totalmente reais, algumas boas constelações de reticulados associadas a canais Rayleigh com desvanecimento são encontradas. Isto se deve ao fato de que reticulados obtidos via corpos de números totalmente reais possuem diversidade máxima $L = n$, o que será visto nos próximos capítulos. Constelações de sinais com bom desempenho para o canal gaussiano podem ser ruins quando usadas para o canal Rayleigh com desvanecimento, por exemplo se tiverem baixa diversidade. Por outro lado, constelações com bom desempenho para o Canal Rayleigh podem ser ruins para o canal gaussiano, por exemplo se tiverem baixa densidade de empacotamento. Assim, um meio para obter constelações eficientes para ambos os canais é buscar reticulados densos com diversidade máxima e distância produto grande.

Na construção de constelações de sinais, dois aspectos fundamentais devem ser levados em conta: o *rotulamento do bit* e a *forma da constelação*. Estas questões são críticas para a complexidade das implementações práticas e são estreitamente relacionada uma com a outra.

- **Rotulamento de bit**

Consiste em aplicar os bits da entrada a pontos na constelação de sinais. Para evitar uma grande tabela de procura, para a eficácia do rotulamento do bit, precisamos de um algoritmo simples que aplica bits a sinais. Quando consideramos uma constelação obtida de um reticulado com a forma

$$\mathcal{S} = \{\mathbf{x} = \mathbf{u}M; \mathbf{u} = (u_1, \dots, u_n) \in A\} \subset \Lambda$$

onde M é uma matriz geradora do reticulado Λ e $A \subset \mathbb{Z}^n$ é um conjunto finito, o mais simples algoritmo para rotulamento que podemos usar é obtido executando o rotulamento de bit sobre as componentes inteiras u_i do vetor $\mathbf{u}$. Se nos restringirmos ao algoritmo simples de rotulamento acima, observamos que isto induz a uma forma de constelação similar ao paralelotope fundamental (reticulado $\mathbb{Z}^n$).

- **Forma da constelação**

Constelações limitadas por uma esfera tem o melhor “ganho de forma” em termos

de energia média. Mas 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 possa induzir muita perda de energia.

Constelações de reticulados $\mathbb{Z}^n$ são boas candidatas: elas são ligeiramente piores em termos de ganho de forma, pois os reticulados $\mathbb{Z}^n$ não são os mais densos em suas dimensões, mas são usualmente mais fáceis de rotular e decodificar. Assim, oferecem bom equilíbrio entre boa forma e facilidade de rotulamento. Neste sentido, existem muitas contribuições acerca da construção de constelação de sinais com a forma cúbica (Reticulados $\mathbb{Z}^n$) ([4], [5], [24], [26], [30], [37] e [54]), que serão detalhadas neste trabalho.

1.3 Motivação e objetivos do trabalho

A motivação do trabalho está fundamentada no que foi exposto na Seção 1.2, ou seja, a construção de reticulados representando constelações de sinais que sejam eficientes para o canal gaussiano, onde boas constelações são aquelas com alta densidade de empacotamento, e para o canal Rayleigh com desvanecimento, onde boas constelações são aquelas com diversidade máxima e distância produto grande. Nosso objetivo será também a construção de constelações de sinais que sejam eficientes para ambos os canais, um interesse prático é que tais constelações podem ser usadas na transmissão de dados entre um móvel e uma base ou entre um móvel e um satélite, através do mesmo sistema de modulação/demodulação, entre outras possíveis aplicações.

Nas construções usamos resultados relacionados à Teoria Algébrica dos Números. Mais especificamente, os objetivos do trabalho estão listados nos itens abaixo.

- Construção dos reticulados A_2 , D_4 , E_6 , E_8 e K_{12} , que são os reticulados mais densos em suas respectivas dimensões, via corpos totalmente reais, logo com diversidade máxima.

Ressaltamos que a construção do reticulado K_{12} é feita através de uma abordagem matricial e algorítmica.

- Construção de uma família de reticulados D_n sobre corpos totalmente reais, via $\mathbb{Z}$ -módulos e via reticulados ideais representando constelações de sinais eficientes para ambos os canais.
- Construção de uma família de reticulados unimodulares sobre corpos totalmente reais apresentando desempenho superior, para o canal Rayleigh com desvanecimento, às construções conhecidas na literatura. Além disso, realizamos uma perturbação desta família de reticulados unimodulares e através de simulações fizemos uma análise do efeito produzido sobre a densidade de empacotamento e distância produto.

1.4 Conceitos básicos

O objetivo desta seção é apresentar alguns conceitos relativos à Módulos, Teoria Algébrica dos Números e Corpos Ciclotômicos, que serão necessários para as técnicas abordadas neste trabalho.

1.4.1 Módulos

Definição 1.4.1. *Seja A um anel comutativo com unidade. Um A -módulo é um grupo abeliano M , juntamente com uma aplicação $\varphi : A \times M \longrightarrow M$, denotada por $(a, m) \longrightarrow am$, tal que, quaisquer que sejam os elementos $a, b \in A$ e $m, n \in M$, tem-se:*

1. $(a + b)m = am + bm$,
2. $a(m + n) = am + an$,
3. $(ab)m = a(bm)$,

4. $1m = m$.

Definição 1.4.2. Dizemos que um A -módulo M é um A -módulo livre quando existe uma família $(x_i)_{i \in I}$ de elementos de M , satisfazendo as seguintes condições:

1. A família $(x_i)_{i \in I}$ é linearmente independente.
2. Todo elemento $x \in M$ é uma combinação linear da família $(x_i)_{i \in I}$.
3. Qualquer família satisfazendo as condições acima é chamada uma base do A -módulo livre, onde o número de elementos da base é o posto de M . Se I é um conjunto finito, dizemos que o A -módulo M é finitamente gerado, ou do tipo finito.

Definição 1.4.3. Sejam A um anel, M um A -módulo e $N \subset M$, $N \neq \emptyset$. Dizemos que N é um submódulo do A -módulo M , se:

1. N é um subgrupo de M .
2. $(\forall a \in A) (\forall n \in N) \Rightarrow an \in N$.

Teorema 1.4.1. [57] Se A é um anel principal, M um A -módulo livre de posto n , e M' um A -submódulo de M , então

1. M' é livre de posto q , $0 \leq q \leq n$.
2. Se $M' \neq \{0\}$, então existe uma base $\{e_1, \dots, e_n\}$ de M e elementos não nulos $a_1, \dots, a_q \in A$ tais que $\{a_1 e_1, \dots, a_q e_q\}$ é uma base de M' , e que a_i divide a_{i+1} , para $1 \leq i \leq q-1$.

1.4.2 Teoria Algébrica dos Números

Definição 1.4.4. Sejam $\mathbb{K}$ e $\mathbb{L}$ subcorpos dos números complexos $\mathbb{C}$. Dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, ou que $\mathbb{L}/\mathbb{K}$ é uma extensão de corpos, sempre que $\mathbb{K}$ for um subcorpo de $\mathbb{L}$.

Definição 1.4.5. O grau da extensão $\mathbb{L}/\mathbb{K}$, denotado por $[\mathbb{L} : \mathbb{K}]$, é definido como sendo a dimensão de $\mathbb{L}$ visto como $\mathbb{K}$ -espaço vetorial. Dizemos que $\mathbb{L}/\mathbb{K}$ é uma extensão finita quando $[\mathbb{L} : \mathbb{K}] < \infty$.

Definição 1.4.6. Sejam $\mathbb{L}/\mathbb{K}$ uma extensão de corpos, e $\alpha \in \mathbb{L}$. Se existe um polinômio mônico irredutível $f(X) \in \mathbb{K}[X] \setminus \{0\}$ tal que $f(\alpha) = 0$, dizemos que α é um número algébrico sobre $\mathbb{K}$. Tal polinômio é chamado de polinômio minimal de α sobre $\mathbb{K}$.

Definição 1.4.7. Dizemos que a extensão $\mathbb{L}$ de $\mathbb{K}$ é uma extensão algébrica se todo elemento $\alpha \in \mathbb{L}$ for raiz de algum polinômio não-nulo $f \in \mathbb{K}[X]$.

Definição 1.4.8. Um corpo $\mathbb{K}$ é chamado de corpo de números se for uma extensão finita de $\mathbb{Q}$. Se a dimensão de $\mathbb{K}$ como $\mathbb{Q}$ -espaço vetorial é n , dizemos que $\mathbb{K}$ é um corpo de números de grau n .

Teorema 1.4.2. [36] Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\theta)$ para algum número algébrico $\theta \in \mathbb{K}$.

Teorema 1.4.3. [36] Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n . Então existem exatamente n monomorfismos distintos $\sigma_i : \mathbb{K} \mapsto \mathbb{C}$, $i = 1, 2, \dots, n$. Os elementos $\sigma_i(\theta) = \theta_i$ são os zeros em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.

Definição 1.4.9. Sejam $\mathbb{L}$ uma extensão de $\mathbb{K}$ e $f \in \mathbb{K}[X]$. Dizemos que $\mathbb{L}$ é um corpo de raízes de f se $\mathbb{L}$ é o menor corpo contendo $\mathbb{K}$ e todas as raízes de f . Denotamos $\mathbb{L} = \mathbb{K}(R_f)$.

Definição 1.4.10. Seja $f \in \mathbb{K}[X] \setminus \mathbb{K}$ um polinômio. Dizemos que f é separável em $\mathbb{K}[X]$ se todas as suas raízes são simples no seu corpo de raízes.

Definição 1.4.11. Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. Dizemos que $\mathbb{L}$ é uma extensão galoisiana de $\mathbb{K}$ se $\mathbb{L} = \mathbb{K}(R_f)$, para algum $f \in \mathbb{K}[X]$ separável.

Definição 1.4.12. Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. O grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ é dado por

$$\text{Gal}(\mathbb{L}/\mathbb{K}) = \{\sigma \in \text{Aut}(\mathbb{L}); \sigma(x) = x, \forall x \in \mathbb{K}\}.$$

Definição 1.4.13. *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. A extensão é dita abeliana (resp. cíclica) se é uma extensão galoisiana e o grupo de Galois $\text{Gal}(\mathbb{L}/\mathbb{K})$ é abeliano (resp. cíclico).*

Definição 1.4.14. *Sejam $\mathbb{L}$ uma extensão finita sobre $\mathbb{K}$ e $H \subset \text{Aut}(\mathbb{L})$. O corpo*

$$\mathbb{L}^H = \{\alpha \in \mathbb{L}; \sigma(\alpha) = \alpha, \forall \sigma \in H\}.$$

é chamado de corpo fixo pelo conjunto H .

Definição 1.4.15. *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. O fecho de Galois de $\mathbb{L}/\mathbb{K}$ é um corpo $\mathbb{M} \supset \mathbb{L}$ que é uma extensão de Galois de $\mathbb{K}$ e é minimal neste sentido, isto é, nenhum subcorpo próprio de $\mathbb{M}$ contendo $\mathbb{L}$ é o corpo de decomposição de algum polinômio $p \in \mathbb{L}[X]$.*

Definição 1.4.16. *Sejam $\mathbb{Q} \subset \mathbb{L}$ com $[\mathbb{L} : \mathbb{Q}] = n$, e $\sigma_1, \dots, \sigma_n$ os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Dado um elemento $\alpha \in \mathbb{L}$, define-se a norma e o traço de α relativamente a extensão $\mathbb{L}/\mathbb{Q}$, como sendo respectivamente:*

$$\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha),$$

$$\text{Tr}_{\mathbb{L}/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

Observação 1.4.1. *Quando não houver dúvida quanto à extensão que contém o elemento α , usaremos $\mathcal{N}(\alpha)$ ao invés de $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)$.*

Observação 1.4.2. *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos, $[\mathbb{L} : \mathbb{K}] = n$, $x, y \in \mathbb{L}$ e $a \in \mathbb{K}$. Valem as seguintes propriedades:*

$$1. \text{Tr}_{\mathbb{L}/\mathbb{K}}(x + y) = \text{Tr}_{\mathbb{L}/\mathbb{K}}(x) + \text{Tr}_{\mathbb{L}/\mathbb{K}}(y);$$

$$2. \text{Tr}_{\mathbb{L}/\mathbb{K}}(ax) = a\text{Tr}_{\mathbb{L}/\mathbb{K}}(x);$$

$$3. \text{Tr}_{\mathbb{L}/\mathbb{K}}(a) = na;$$

$$4. N_{\mathbb{L}/\mathbb{K}}(xy) = N_{\mathbb{L}/\mathbb{K}}(x) \cdot N_{\mathbb{L}/\mathbb{K}}(y);$$

5. $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$.

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

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

Em particular, se $x \in \mathbb{L}$, então

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

Teorema 1.4.4. [46] *Sejam $\mathbb{M}$ e $\mathbb{F}$ extensões galoisianas sobre $\mathbb{K}$ e assumamos que $\mathbb{M}$ e $\mathbb{F}$ são subcorpos de algum outro corpo, então:*

- (i) $\mathbb{M}\mathbb{F} \mid \mathbb{F}$ é Galois.
- (ii) $\mathbb{M} \mid \mathbb{M} \cap \mathbb{F}$ é Galois.
- (iii) Se H é o grupo de Galois de $\mathbb{M}\mathbb{F}$ sobre $\mathbb{F}$, G é o grupo de Galois de $\mathbb{M}$ sobre $\mathbb{K}$ e $\sigma \in H$, então a restrição de σ a $\mathbb{M}$ pertence a G , e a aplicação $\sigma \mapsto \sigma|_{\mathbb{M}}$ nos dá um isomorfismo de H no grupo de Galois de $\mathbb{M}$ sobre $\mathbb{M} \cap \mathbb{F}$.

Corolário 1.4.1. *Sejam $\mathbb{M}$ e $\mathbb{F}$ extensões galoisianas sobre $\mathbb{K}$ e assumamos que $\mathbb{M}$ e $\mathbb{F}$ são subcorpos de algum outro corpo. Dado $\alpha \in \mathbb{M}$, se $\mathbb{M} \cap \mathbb{F} = \mathbb{K}$ então*

$$Tr_{\mathbb{M}\mathbb{F}/\mathbb{F}}(\alpha) = Tr_{\mathbb{M}/\mathbb{K}}(\alpha)$$

Demonstração: Segue diretamente do Teorema 1.4.4. □

Definição 1.4.17. *Seja $\mathbb{K}$ um corpo de números de grau n . Um elemento $\alpha \in \mathbb{K}$ é chamado um inteiro algébrico do corpo $\mathbb{K}$ se existe um polinômio mônico f com coeficientes inteiros tal que $f(\alpha) = 0$. Pode ser mostrado que o conjunto $\mathcal{O}_{\mathbb{K}}$ formado pelos inteiros algébricos de $\mathbb{K}$ é um anel, chamado anel dos inteiros algébricos do corpo $\mathbb{K}$.*

Teorema 1.4.5. [36] Se $\alpha \in \mathbb{K}$ é um inteiro algébrico, então $\mathcal{N}(\alpha)$ e $Tr(\alpha)$ são números inteiros.

Teorema 1.4.6. [57] Se $\mathbb{K}$ é um corpo de números de grau n , $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros algébricos do corpo $\mathbb{K}$ e $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{A}$ e $\mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$ -módulos livres de posto n .

Definição 1.4.18. Uma base para $\mathcal{O}_{\mathbb{K}}$ como $\mathbb{Z}$ -módulo é chamada de base integral de $\mathbb{K}$ (ou de $\mathcal{O}_{\mathbb{K}}$).

Definição 1.4.19. Sejam $\{\omega_1, \dots, \omega_n\}$ uma base integral de $\mathcal{O}_{\mathbb{K}}$ e $\sigma_1, \dots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. O discriminante de $\mathbb{K}$ é definido como $d_{\mathbb{K}} = \det[\sigma_i(\omega_j)]^2$.

Definição 1.4.20. Sejam $\mathbb{K}$ um corpo de números de grau n , $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$ e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Definimos a Norma do ideal $\mathcal{A}$ como sendo o número de elementos do anel quociente $\mathcal{O}_{\mathbb{K}}/\mathcal{A}$, isto é, $\mathcal{N}(\mathcal{A}) = \#\mathcal{O}_{\mathbb{K}}/\mathcal{A}$

Teorema 1.4.7. [36] Se $\mathcal{A} = \langle \alpha \rangle$ é um ideal principal, então $\mathcal{N}(\mathcal{A}) = |\mathcal{N}(\alpha)|$

Definição 1.4.21. Seja $\mathbb{K}$ um corpo de números. Dizemos que $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal fracionário se $\mathcal{A}$ é um $\mathcal{O}_{\mathbb{K}}$ -módulo e existe $d \in \mathcal{O}_{\mathbb{K}} - \{0\}$ tal que $d\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$. Em particular, os ideais do anel $\mathcal{O}_{\mathbb{K}}$ são ideais fracionários.

Definição 1.4.22. O conjunto

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1} = \{x \in \mathbb{K}; Tr_{\mathbb{K}/\mathbb{Q}}(x\alpha) \in \mathbb{Z}, \forall \alpha \in \mathcal{O}_{\mathbb{K}}\}$$

é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ chamado de codiferente.

1.4.3 Corpos ciclotômicos

Uma classe especial de corpos de números é a classe dos corpos ciclotômicos. Nesta seção apresentamos suas propriedades, é sobre estes corpos e subcorpos que está pautado o nosso trabalho.

Definição 1.4.23. 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, $\text{mdc}(m, n) = 1$, isto é, o número de raízes primitivas n -ésimas da unidade é dado por

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

onde φ é a função de Euler.

Definição 1.4.24. Dizemos que $\mathbb{L}$ é o n -ésimo corpo ciclotômico se $\mathbb{L}$ é resultante da adjunção de $\mathbb{Q}$ e uma raiz primitiva n -ésima da unidade, $L = \mathbb{Q}(\zeta_n)$, e $[\mathbb{L} : \mathbb{Q}] = \varphi(n)$.

Teorema 1.4.8. [17] O anel dos inteiros de $\mathbb{L} = \mathbb{Q}(\zeta_n)$ é $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}\}$ é uma base integral de $\mathcal{O}_{\mathbb{L}}$.

Teorema 1.4.9. [53] Seja $\zeta_n \in \mathbb{C}$ uma raiz primitiva n -ésima da unidade. Então $\mathbb{L} = \mathbb{Q}(\zeta_n)$ é uma extensão galoisiana de $\mathbb{Q}$, cujo grupo de Galois $\text{Aut}(\mathbb{L}/\mathbb{Q})$ é canonicamente isomorfo a $(\mathbb{Z}_n)^*$, e portanto abeliano de ordem $\varphi(n)$.

Teorema 1.4.10. [56] A extensão $\mathbb{L} = \mathbb{Q}(\zeta_n)$ é cíclica se, e somente se, $n = 2, 4, p^r, 2p^r$, onde p é um primo ímpar e $r \geq 0$ é um inteiro.

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

Dado um corpo $\mathbb{L}$, o subcorpo de $\mathbb{L}$ fixado ponto-a-ponto pela conjugação complexa é chamado o subcorpo maximal real de $\mathbb{L}$.

Proposição 1.4.1. [15] *Seja $\mathbb{L} = \mathbb{Q}(\zeta_n)$, com ζ_n uma raiz primitiva n -ésima da unidade, temos que*

- (i) $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal real de $\mathbb{L}$;
- (ii) O anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$;
- iii) $1, \zeta_n + \zeta_n^{-1}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1}$ formam uma base integral de $\mathbb{K}$.

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

Teorema 1.4.11. [48] *Se $\mathbb{K}$ é uma extensão finita e abeliana dos racionais, então $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, para algum n .*

Observação 1.4.3. *O menor n na qual vale o Teorema de Kronecker-Weber é chamado de condutor de $\mathbb{K}$.*

Teorema 1.4.12. [48] *O discriminante de $\mathbb{L} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

$$d_{\mathbb{L}} = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Como consequência segue que

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

Teorema 1.4.13. [64] *Sejam p um número primo ímpar, r um inteiro positivo e $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{p^r})$, tal que $[\mathbb{K} : \mathbb{Q}] = up^j$ e u divide $p-1$. Então*

$$d_{\mathbb{K}} = \pm p^v$$

onde $v = u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}] - 1$

Corolário 1.4.2. [64] *O discriminante de $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ sobre $\mathbb{Q}$ é dado por*

$$(i) \ d_{\mathbb{K}} = p^{\frac{p-3}{2}}, \text{ se } n = p \geq 5;$$

$$(ii) \ d_{\mathbb{K}} = p^{\frac{(r+1)(p-1)p^{r-1}-p^r-1}{2}}, \text{ se } n = p^r, p \neq 2, r > 1.$$

Teorema 1.4.14. [44] *O discriminante do corpo $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ sobre $\mathbb{Q}$ é dado por*

$$d_{\mathbb{K}} = 2^{(r-1)2^{r-2}-1}$$

Os resultados que seguem têm por objetivo o cálculo do discriminante de $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ para $n = 2^r.3.5$, $r \geq 1$.

Teorema 1.4.15. [60] *Se n e m são dois números inteiros tais que $n, m \geq 1$ e $\text{mdc}(n, m) = 1$, então*

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

Teorema 1.4.16. [40] *Sejam $m = \prod_{i=1}^k p_i^{\alpha_i}$, onde os p_i 's são primos distintos, e $\mathbb{K}$ um corpo de números abeliano de condutor m . Então*

$$|d_{\mathbb{K}}| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^k p_i^{\sum_{r=1}^{\alpha_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_m/p_i^r):\mathbb{Q}]}}$$

Os próximos lemas, Proposição 1.4.2 (que será usada no último capítulo do trabalho), Proposição 1.4.5 e corolário são de nossa autoria.

Lema 1.4.1. *Se $n = 2^r.3.5$ ($r \geq 1$), $m = 2^{r-k}.3.5$ ($1 \leq k \leq r$), $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ e $\mathbb{M} = \mathbb{Q}(\zeta_m)$, então $\mathbb{K} \cap \mathbb{M} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.*

Demonstração: Observe que $\mathbb{K} = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ e $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$. Portanto,

$$\mathbb{K} \cap \mathbb{M} = \mathbb{Q}(\zeta_n) \cap \mathbb{R} \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m) \cap \mathbb{R} = \mathbb{Q}(\zeta_m + \zeta_m^{-1}).$$

□

Lema 1.4.2. *Se $n = 2^r.3.5$ ($r \geq 1$), $m = 2^r.5$, $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ e $\mathbb{M} = \mathbb{Q}(\zeta_m)$, então $\mathbb{K} \cap \mathbb{M} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.*

Demonstração: Análoga à demonstração do Lema 1.4.1.

□

Lema 1.4.3. *Se $n = 2^r.3.5$ ($r \geq 1$), $m = 2^r.3$, $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ e $\mathbb{M} = \mathbb{Q}(\zeta_m)$, então $\mathbb{K} \cap \mathbb{M} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.*

Demonstração: Análoga à demonstração do Lema 1.4.1.

□

Proposição 1.4.2. *Se $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $n = 2^r.3.5$, $r \geq 1$, então*

$$|d_{\mathbb{K}}| = 2^{(r-1)2^{r+1}} 3^{2^r} 5^{3 \cdot 2^{r-1}}$$

Demonstração: Se $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, onde $n = 2^r.3.5$, $r \geq 1$, então pelo Teorema 1.4.11 e pela Observação 1.4.3, temos que $\mathbb{K}$ é um corpo de números abeliano de condutor $2^r.3.5$, assim pelo Teorema 1.4.16, segue que

$$|d_{\mathbb{K}}| = \frac{(2^r.3.5)^{[\mathbb{K}:\mathbb{Q}]}}{2^{\beta_1} 3^{\beta_2} 5^{\beta_3}} \quad (1.4.17)$$

onde

$$\beta_1 = \sum_{k=1}^r [\mathbb{K} \cap \mathbb{Q}(\zeta_{n/2^k}) : \mathbb{Q}]$$

$$\beta_2 = [\mathbb{K} \cap \mathbb{Q}(\zeta_{n/3}) : \mathbb{Q}]$$

$$\beta_3 = [\mathbb{K} \cap \mathbb{Q}(\zeta_{n/5}) : \mathbb{Q}]$$

Mas usando o Lema 1.4.1, podemos escrever

$$\begin{aligned}
\beta_1 &= \sum_{k=1}^r [\mathbb{K} \cap \mathbb{Q}(\zeta_{n/2^k}) : \mathbb{Q}] = \sum_{k=1}^r [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^{r-k}.3.5}) : \mathbb{Q}] = \\
&= [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^{r-1}.3.5}) : \mathbb{Q}] + [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^{r-2}.3.5}) : \mathbb{Q}] + \cdots + [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^2.3.5}) : \mathbb{Q}] + \\
&\quad + [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^1.3.5}) : \mathbb{Q}] + [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^0.3.5}) : \mathbb{Q}] = \\
&= [\mathbb{Q}(\zeta_{2^{r-1}.3.5} + \zeta_{2^{r-1}.3.5}^{-1}) : \mathbb{Q}] + [\mathbb{Q}(\zeta_{2^{r-2}.3.5} + \zeta_{2^{r-2}.3.5}^{-1}) : \mathbb{Q}] + \cdots + [\mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1}) : \mathbb{Q}] + \\
&\quad + [\mathbb{Q}(\zeta_{30} + \zeta_{30}^{-1}) : \mathbb{Q}] + [\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}) : \mathbb{Q}] = \\
&= 2^r + 2^{r-1} + \cdots + 2^3 + 2^2 + 2^2 = 2^{r+1}.
\end{aligned}$$

Pelo Lema 1.4.2, temos que

$$\beta_2 = [\mathbb{K} \cap \mathbb{Q}(\zeta_{n/3}) : \mathbb{Q}] = [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^r.5}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^r.5} + \zeta_{2^r.5}^{-1}) : \mathbb{Q}] = 2^r.$$

Pelo Lema 1.4.3, temos que

$$\beta_3 = [\mathbb{K} \cap \mathbb{Q}(\zeta_{n/5}) : \mathbb{Q}] = [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^r.3}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^r.3} + \zeta_{2^r.3}^{-1}) : \mathbb{Q}] = 2^{r-1}.$$

Agora,

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^r.3.5} + \zeta_{2^r.3.5}^{-1}) : \mathbb{Q}] = 2^{r+1}.$$

Substituindo $\beta_1, \beta_2, \beta_3$ e $[\mathbb{K} : \mathbb{Q}]$ na Equação 1.4.17 segue o resultado. $\square$

Os resultados que seguem têm por objetivo o cálculo do Traço de elementos sobre as extensões $\mathbb{L}/\mathbb{Q}$, onde $\mathbb{L}$ é um corpo ciclotômico.

Proposição 1.4.3. [62] *Dados $n = p_1 p_2 \dots p_{k+1}$, onde os p_i 's, $i = 1, 2, \dots, k+1$ são primos distintos, $a = p_1 p_2 \dots p_k$ e $b = p_{k+1}$, $\mathbb{M} = \mathbb{Q}(\zeta_b)$ e $\mathbb{F} = \mathbb{Q}(\zeta_a)$, então*

- (i) $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}(\zeta_a)$ e $\mathbb{Q}(\zeta_b) \mid \mathbb{Q}$ são extensões galoisianas.
- (ii) Se $G = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\rho \in \text{Aut}(\mathbb{Q}(\zeta_n)); \rho(x) = x, \forall x \in \mathbb{Q}\}$ e $H = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)) = \{\sigma \in \text{Aut}(\mathbb{Q}(\zeta_n)); \sigma(x) = x, \forall x \in \mathbb{Q}(\zeta_a)\}$, dado $\sigma \in H$, temos que

$$\rho : H \longrightarrow \text{Gal}(\mathbb{Q}(\zeta_b) / \mathbb{Q})$$

$$\sigma \longmapsto \sigma|_{\mathbb{Q}(\zeta_b)}$$

é um isomorfismo.

Corolário 1.4.3. [62] Se $\alpha \in \mathbb{Q}(\zeta_b)$, então $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)}(\alpha) = Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\alpha)$.

Lema 1.4.4. [62] Sejam k, n números inteiros. Se $mdc(k, n) = d$ então

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^k) = \frac{\varphi(n)}{\varphi(n/d)} Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{k/d})$$

onde φ é a função de Euler.

Lema 1.4.5. [62] Sejam k, a_i números inteiros, $a_i \geq 1$ e p_i um número primo tal que $mdc(k, p_i^{a_i}) = 1$. Então

$$Tr_{\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q}}(\zeta_{p_i^{a_i}}^k) = \begin{cases} -1, & \text{se } a_i = 1. \\ 0, & \text{se } a_i > 1. \end{cases}$$

Definição 1.4.25. Seja $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$, onde $a_j \geq 1$, para $j = 1, 2, \dots, s$, definimos

$$\mu(n) = \begin{cases} (-1)^s, & \text{se } a_j = 1, \text{ para todo } j. \\ 1, & \text{se } n = 1. \\ 0, & \text{se } a_j > 1, \text{ para algum } j. \end{cases}$$

μ é chamada função de Möbius.

Lema 1.4.6. [62] Sejam $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$, onde $a_j \geq 1$, para $j = 1, 2, \dots, s$, k um número inteiro e $mdc(k, n) = d$, então

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^k) = \frac{\varphi(n)}{\varphi(n/d)} \cdot \mu(n/d)$$

onde μ é a função de Möbius.

Proposição 1.4.4. [62] Se $\mathbb{L} = \mathbb{Q}(\zeta_{2^r})$ então

$$Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^k) = \begin{cases} 0, & \text{se } mdc(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & \text{se } mdc(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & \text{se } mdc(k, 2^r) > 2^{r-1}. \end{cases}$$

Corolário 1.4.4. [62] Se $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ então

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}) = \begin{cases} 0, & \text{se } mdc(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & \text{se } mdc(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & \text{se } mdc(k, 2^r) > 2^{r-1}. \end{cases}$$

Proposição 1.4.5. *Se $\mathbb{L} = \mathbb{Q}(\zeta_{2^r.3.5})$ então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^k) = \begin{cases} -2^{r-1}, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}; \\ 2^{r-1}, & \text{se } mdc(k, 2^r.3.5) = 2^r; \\ 2^r, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}.3; \\ 2^{r+1}, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}.5; \\ -2^r, & \text{se } mdc(k, 2^r.3.5) = 2^r.3; \\ -2^{r+1}, & \text{se } mdc(k, 2^r.3.5) = 2^r.5; \\ -2^{r+2}, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}.3.5; \\ 2^{r+2}, & \text{se } mdc(k, 2^r.3.5) = 2^r.3.5; \\ 0, & \text{se } mdc(k, 2^r.3.5) = 1 \ (r > 1) \\ & e \text{ demais casos;} \end{cases}$$

Demonstração: Segue diretamente do Lema 1.4.6. □

Corolário 1.4.5. *Se $\mathbb{K} = \mathbb{Q}(\zeta_{2^r.3.5} + \zeta_{2^r.3.5}^{-1})$ então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r.3.5}^k + \zeta_{2^r.3.5}^{-k}) = \begin{cases} -2^{r-1}, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}; \\ 2^{r-1}, & \text{se } mdc(k, 2^r.3.5) = 2^r; \\ 2^r, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}.3; \\ 2^{r+1}, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}.5; \\ -2^r, & \text{se } mdc(k, 2^r.3.5) = 2^r.3; \\ -2^{r+1}, & \text{se } mdc(k, 2^r.3.5) = 2^r.5; \\ -2^{r+2}, & \text{se } mdc(k, 2^r.3.5) = 2^{r-1}.3.5; \\ 2^{r+2}, & \text{se } mdc(k, 2^r.3.5) = 2^r.3.5; \\ 0, & \text{se } mdc(k, 2^r.3.5) = 1 \ (r > 1) \\ & e \text{ demais casos;} \end{cases}$$

Demonstração: Pela transitividade do traço temos

$Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^k) + Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^{-k}) = Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^k + \zeta_{2^r.3.5}^{-k}) = Tr_{\mathbb{K}/\mathbb{Q}}(Tr_{\mathbb{L}/\mathbb{K}}(\zeta_{2^r.3.5}^k + \zeta_{2^r.3.5}^{-k})) =$
 $2Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r.3.5}^k + \zeta_{2^r.3.5}^{-k}).$ Como $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^k) = Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^{-k})$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r.3.5}^k + \zeta_{2^r.3.5}^{-k}) =$
 $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r.3.5}^k)$ e pela Proposição 1.4.5 o resultado segue. □

CAPÍTULO 2

RETICULADOS

2.1 Conceitos básicos

Nesta seção apresentamos o conceito de reticulados enfocando suas principais propriedades.

Definição 2.1.1. *Sejam $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ um conjunto de vetores linearmente independentes no espaço vetorial $\mathbb{R}^n$, tal que $m \leq n$. O conjunto*

$$\Lambda = \left\{ \sum_{i=1}^m \alpha_i \mathbf{v}_i : \alpha_i \in \mathbb{Z} \right\}.$$

é chamado um reticulado de posto m , e o conjunto $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ é chamado uma base do reticulado Λ .

Definição 2.1.2. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$. O conjunto*

$$\mathcal{P}_B = \left\{ \mathbf{x} \in \mathbb{R}^n : \mathbf{x} = \sum_{i=1}^n \lambda_i \mathbf{v}_i, 0 \leq \lambda_i < 1 \right\},$$

é chamado de paralelotopo fundamental ou região fundamental de Λ com relação à base B .

Exemplo 2.1.1. O reticulado $\mathbb{Z}^2$ possui uma base $B = \{(1, 0), (0, 1)\}$ e região fundamental P descrita na figura abaixo.

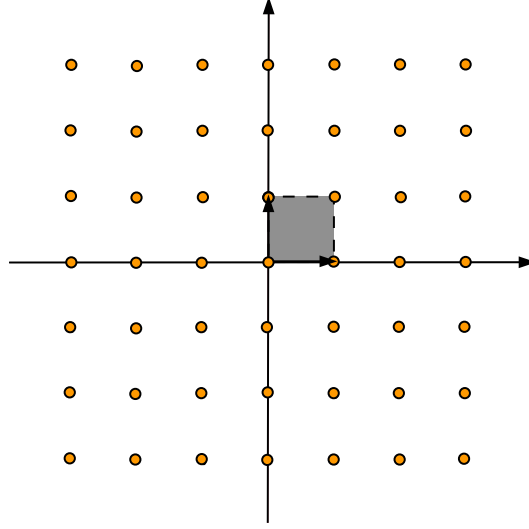


Figura 2.1: Reticulado $\mathbb{Z}^2$ com uma região fundamental.

Observação 2.1.1. O paralelotopo fundamental quando transladado por vetores do reticulado cobre todo o $\mathbb{R}^n$, de modo que cada cópia da região contém um único ponto do reticulado.

Definição 2.1.3. Seja $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ uma base para o reticulado Λ tal que $\mathbf{v}_i = (v_{i1}, v_{i2}, \dots, v_{in})$, para $i = 1, \dots, m$. Então a matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

é chamada uma matriz geradora para o reticulado Λ .

Observação 2.1.2. Seja M uma matriz geradora para o reticulado Λ . Então, Λ pode ser escrito na forma matricial por

$$\Lambda = \{\mathbf{x}M \mid \mathbf{x} \in \mathbb{Z}^m\}$$

Duas matrizes M_1 e M_2 geram o mesmo reticulado se, e somente se, $M_1 = AM_2$, onde A é uma matriz com elementos inteiros e determinante ± 1 .

Definição 2.1.4. *Seja M uma matriz geradora para o reticulado Λ . A matriz*

$$G = MM^t$$

é chamada uma matriz de Gram para o reticulado, onde t denota a transposição.

Observação 2.1.3. *Como a matriz geradora M contém os vetores $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$, vetores da base do reticulado, então a (i, j) -ésima entrada da matriz G é o produto interno $\langle \mathbf{v}_i, \mathbf{v}_j \rangle$. Assim, as entradas da matriz de Gram G guardam informações métricas importantes, pois referem-se às posições relativas dos vetores da base do reticulado.*

Definição 2.1.5. *O determinante do reticulado Λ é definido como sendo o determinante da matriz G*

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

Observação 2.1.4. *Um reticulado é dito de posto máximo se $m = n$, e neste caso M é uma matriz quadrada. Assim,*

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

Definição 2.1.6. *Dado um reticulado Λ , então seu volume é definido por*

$$\text{vol}(\Lambda) = \sqrt{\det(\Lambda)}$$

que é o volume de um paralelepípedo fundamental.

Observação 2.1.5. *O volume do reticulado independe da base escolhida, pois vimos que as bases de um mesmo reticulado diferem pelo produto de uma matriz invertível com entradas inteiras. Dessa forma, faz sentido definir o volume do reticulado como sendo o volume de um paralelepípedo fundamental.*

Definição 2.1.7. *Dizemos que um reticulado $\Lambda \subseteq \mathbb{R}^n$ é racional (respec. integral) se uma (portanto todas) de suas matrizes de Gram possuir todas as entradas racionais (respec. inteiras).*

Definição 2.1.8. *Seja B uma matriz de ordem n com entradas inteiras. Um sub-reticulado de Λ é dado por*

$$\Lambda' = \{\alpha BM; \alpha \in \mathbb{Z}^n\}$$

onde M é a matriz geradora do reticulado Λ .

Note que um reticulado Λ é um grupo aditivo abeliano livre e um sub-reticulado Λ' é um subgrupo de Λ . A próxima proposição apresenta uma relação para a cardinalidade do grupo quociente Λ/Λ' .

Proposição 2.1.1. *[36] Sejam G um grupo abeliano livre de posto r e H um subgrupo de G . Temos que G/H é finito se, e somente se, $\text{posto}(G) = \text{posto}(H)$. Se $\{x_1, x_2, \dots, x_n\}$ é uma $\mathbb{Z}$ -base para G e $\{y_1, y_2, \dots, y_n\}$ é uma $\mathbb{Z}$ -base para H tal que $y_i = \sum_{j=1}^n a_{ij}x_j$ para $a_{ij} \in \mathbb{Z}$, para todo $i = 1, 2, \dots, n$, então $|G/H| = |\det(a_{ij})|$.*

Observação 2.1.6. *[32] A proposição 2.1.1 no caso $G = \Lambda$ e $H = \Lambda'$, onde $\Lambda' \subset \Lambda$ são reticulados, afirma que $|\Lambda/\Lambda'| < \infty$ se, e somente se, $\dim(\Lambda) = \dim(\Lambda')$. Além disso, se Λ e Λ' tem posto máximo e M é uma matriz geradora para Λ e N é uma matriz geradora para Λ' , existe uma matriz B com entradas inteiras tal que $N = BM$. Assim, pela mesma proposição, temos*

$$|\Lambda/\Lambda'| = |\det(B)| = |\det(N)/\det(M)| = \det(\Lambda')^{1/2}/\det(\Lambda)^{1/2}.$$

Definição 2.1.9. *Se Λ é um reticulado no $\mathbb{R}^n$, então o reticulado dual de Λ , denotado por Λ^* , é definido por*

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n; \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}, \forall \mathbf{v} \in \Lambda\}.$$

Definição 2.1.10. *Um reticulado é chamado de 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.*

Definição 2.1.11. *Dizemos que um reticulado Λ' é uma versão escalonada do reticulado Λ com fator de escala $\sqrt{c}$, $c \in \mathbb{R}$, se $\Lambda' = \sqrt{c}\Lambda$.*

Definição 2.1.12. *Se um reticulado pode ser obtido de outro pela composição de uma rotação ou reflexão com multiplicação por um fator de escala, dizemos que eles são equivalentes na métrica euclidiana. Ou seja, Λ_1 e Λ_2 , reticulados com matrizes geradoras M_1 e M_2 , respectivamente, são equivalentes se, e somente se,*

$$M_1 = \sqrt{c}AM_2R,$$

onde A é matriz mudança de base do reticulado (com entradas inteiras e determinante ± 1), R é matriz ortogonal e $\sqrt{c}$ é o fator de escala.

Proposição 2.1.2. *Sejam G_1 e G_2 matrizes de Gram dos reticulados Λ_1 e Λ_2 , respectivamente. Então, o reticulado Λ_1 é uma versão escalonada e rotacionada do reticulado Λ_2 com fator de escala $\sqrt{c}$ se, e somente se,*

$$G_1 = cAG_2A^t$$

onde a matriz A é uma matriz com entradas inteiras e determinante ± 1 , e t denota a transposição.

Demonstração: Temos que

$$\begin{aligned} G_1 &= M_1M_1^t = (\sqrt{c}AM_2R)(\sqrt{c}AM_2R)^t = cAM_2RR^tM_2^tA^t = \\ &= cAM_2IM_2^tA^t = cAM_2M_2^tA^t = cAG_2A^t. \end{aligned}$$

Reciprocamente, se $G_1 = cAG_2A^t$, então

$$G_1 = cAG_2A^t$$

$$M_1M_1^t = cAM_2M_2^tA^t$$

$$I = M_1^{-1}cAM_2M_2^tA^t(M_1^t)^{-1}$$

$$I = cM_1^{-1}AM_2M_2^tA^t(M_1^{-1})^t$$

$$I = (\sqrt{c}M_1^{-1}AM_2)(\sqrt{c}M_1^{-1}AM_2)^t$$

Tomando $R = \sqrt{c}M_1^{-1}AM_2$, temos que $RR^t = I$, ou seja, R é uma matriz de rotação, e consequentemente R^{-1} também é uma matriz de rotação, pois como $R^t = R^{-1}$ segue que

$$(R^{-1})(R^{-1})^t = R^t(R^t)^t = R^tR = R^{-1}R = I.$$

Agora,

$$\frac{1}{\sqrt{c}}A^{-1}M_1R = \frac{1}{\sqrt{c}}A^{-1}M_1(\sqrt{c}M_1^{-1}AM_2) = A^{-1}M_1M_1^{-1}AM_2 = A^{-1}IAM_2 = A^{-1}AM_2 = IM_2 = M_2.$$

Assim,

$$\begin{aligned} M_2 &= \frac{1}{\sqrt{c}}A^{-1}M_1R \\ \sqrt{c}M_2 &= A^{-1}M_1R \\ A\sqrt{c}M_2 &= M_1R \\ \sqrt{c}AM_2R^{-1} &= M_1 \end{aligned}$$

onde A é uma matriz com entradas inteiras e determinante ± 1 , a matriz R^{-1} é uma matriz de rotação, e M_1 e M_2 são as matrizes geradoras dos reticulados Λ_1 e Λ_2 , respectivamente. Portanto, o reticulado Λ_1 é uma versão escalonada e rotacionada do reticulado Λ_2 , com fator de escala $\sqrt{c}$, o que conclui a demonstração. $\square$

2.2 Empacotamento esférico

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n -dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis. A referência clássica para estas duas próximas seções é [42] e provas mais detalhadas podem também ser encontradas em [47].

Definição 2.2.1.

1. *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.

2. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ do $\mathbb{R}^n$.
3. Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ com base $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, definimos a sua densidade de empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Estamos interessados no empacotamento associado a um reticulado Λ em que as esferas tenham raio máximo, chamado raio de empacotamento, conforme definição a seguir

Definição 2.2.2. O raio de empacotamento de um reticulado Λ é o maior raio ρ tal que $B_\rho(\mathbf{u}) \cap B_\rho(\mathbf{v}) = \emptyset$, para quaisquer $\mathbf{u}, \mathbf{v} \in \Lambda$, $\mathbf{u} \neq \mathbf{v}$.

Uma definição importante relacionada ao raio de empacotamento é a norma mínima de um vetor não nulo do reticulado que tem o mesmo valor da distância mínima entre dois pontos distintos deste.

Definição 2.2.3. A norma mínima η de um reticulado Λ é dada por

$$\eta = \min\{\|\mathbf{x}\|^2; \mathbf{x} \in \Lambda, \mathbf{x} \neq 0\}$$

Proposição 2.2.1. O raio de empacotamento ρ de um reticulado Λ é igual à metade da distância mínima d entre os pontos do reticulado.

O resultado a seguir estabelece o cálculo da densidade de empacotamento de um reticulado.

Definição 2.2.4. Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ com base $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ e raio de empacotamento ρ , definimos a densidade de empacotamento de Λ por

$$\Delta(\Lambda) = \frac{\text{Volume da esfera de raio } \rho}{\text{Volume do reticulado}} = \frac{\text{Vol}(\mathcal{B}(\rho))}{\text{Vol}(\Lambda)} = \frac{\text{Vol}(\mathcal{B}(1))\rho^n}{\text{Vol}(\Lambda)}$$

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

Podemos reduzir o problema ao estudo de um outro parâmetro, definido a seguir.

Definição 2.2.5. *Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ com base $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ e raio de empacotamento ρ , definimos a densidade de centro de Λ por*

$$\delta(\Lambda) = \frac{\rho^n}{Vol(\Lambda)}$$

Se o raio das esferas em um empacotamento no $\mathbb{R}^n$ 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 pertence à união das esferas, e este raio é definido a seguir.

Definição 2.2.6. *O raio de cobertura R de um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ é o menor raio associado às esferas que resulta em uma cobertura do espaço gerado pelo reticulado.*

O problema da cobertura consiste em encontrar a melhor cobertura do espaço por esferas sobrepostas. Para medir a melhor cobertura de um empacotamento associado a um reticulado, temos uma taxa análoga à densidade de empacotamento: a densidade de cobertura (thickness), definida a seguir.

Definição 2.2.7. *Considere um arranjo de esferas de raio R centradas nos pontos do reticulado Λ cobrindo todo o $\mathbb{R}^n$. A densidade de cobertura Θ é dada por*

$$\Theta = \frac{\text{Volume da esfera de raio } R}{\text{Volume do reticulado } \Lambda} = \frac{Vol(\mathcal{B}(R))}{Vol(\Lambda)} = \frac{Vol(\mathcal{B}(1))R^n}{Vol(\Lambda)}$$

onde R é o raio de cobertura.

Enquanto o problema do empacotamento esférico procura os empacotamentos mais densos por esferas que se tangenciam, o problema da cobertura procura os empacotamentos menos densos por esferas que cobrem todo o espaço. Num reticulado, a densidade de cobertura é dada pelas esferas de menor raio que, centradas no reticulado cobrem todo o espaço. As densidades de empacotamento e de cobertura satisfazem:

$$\Delta \leq 1 \leq \Theta$$

ou seja, o volume de uma esfera com raio de empacotamento ρ é sempre menor do que ou igual ao determinante do reticulado, enquanto o volume de uma esfera com raio de cobertura R é sempre maior do que ou igual ao determinante do reticulado.

Um outro parâmetro importante a ser estudado é o problema do “kissing number” ou “número de vizinhos” de um empacotamento esférico, definido a seguir.

Definição 2.2.8. *O “kissing number” τ de um empacotamento esférico é o número de esferas idênticas que tocam uma outra esfera idêntica central.*

Para um empacotamento reticulado, τ é o mesmo para toda esfera, mas para um empacotamento arbitrário τ pode variar de uma esfera para outra. A versão n -dimensional do problema do “kissing number” pergunta qual o número máximo de esferas idênticas n -dimensionais que tocam uma outra esfera idêntica central.

A seguir definimos um outro tipo de região fundamental de um reticulado, ou seja, uma região que “ladrilha” todo o espaço gerado por ele.

Definição 2.2.9. *Dado $\mathbf{v} \in \Lambda$, a região de Voronoi associada a $\mathbf{v}$, denotada por $R(\mathbf{v})$, é o subconjunto do $\mathbb{R}^n$ dado por*

$$R(\mathbf{v}) = \{\mathbf{x} \in \mathbb{R}^n; \|\mathbf{v} - \mathbf{x}\| \leq \|\mathbf{u} - \mathbf{x}\|, \forall \mathbf{u} \in \Lambda\}.$$

Nota-se que $R(\mathbf{v})$ é o conjunto dos pontos que estão mais próximos de $\mathbf{v}$ do que de $\mathbf{u}$, para qualquer $\mathbf{u} \in \Lambda$.

Exemplo 2.2.1. *Regiões de Voronoi associadas ao reticulado Λ gerado pelos vetores $(1, 3)$ e $(3, 2)$.*

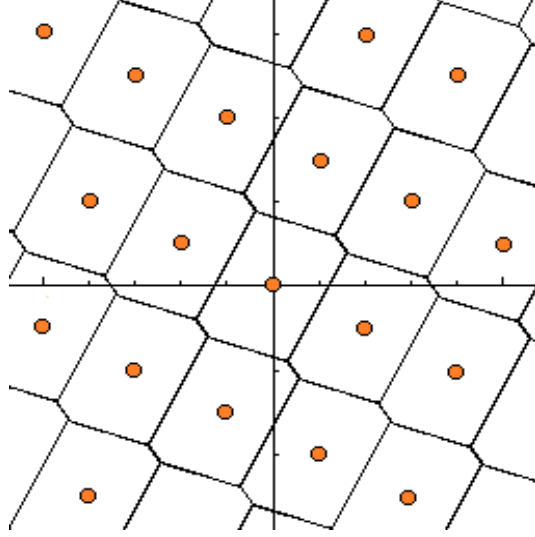


Figura 2.2: Regiões de Voronoi associadas ao reticulado Λ .

2.3 Alguns reticulados especiais e suas propriedades

Reticulado $\mathbb{Z}^n$

Para todo $n \geq 1$, temos que

$$\mathbb{Z}^n = \{(x_1, x_2, \dots, x_n) : x_j \in \mathbb{Z}\}$$

é um reticulado n -dimensional e possui uma matriz geradora $M = I_n$ (Matriz identidade de ordem n). Temos que $\det(\mathbb{Z}^n) = 1$, raio de empacotamento $\rho = 1/2$, norma mínima $\eta = 1$, densidade de centro $\delta = 2^{-n}$, densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2}}{(\frac{n}{2})! 2^n}, & \text{se } n \text{ é par.} \\ \frac{2^n \pi^{(n-1)/2} ((n-1)/2)!}{n! 2^n}, & \text{se } n \text{ é ímpar.} \end{cases},$$

raio de cobertura $R = \sqrt{n}/2$, e kissing number $\tau = 2n$. Os vetores minimais são todas as permutações do vetor $(0, \dots, \pm 1, \dots, 0)$.

Reticulado A_n

Para todo $n \geq 1$, temos que

$$A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} : x_0 + x_1 + \dots + x_n = 0\}$$

é um reticulado n -dimensional em $\mathbb{R}^{n+1}$. Por definição, A_n pertence ao hiperplano $\sum_{i=0}^n x_i = 0$, possui uma matriz geradora M , dada por:

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{pmatrix}.$$

Temos que $\det(A_n) = n + 1$, raio de empacotamento $\rho = \sqrt{2}/2$, norma mínima $\eta = 2$, densidade de centro $\delta = \frac{2^{-n/2}}{\sqrt{n+1}}$, densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2} \cdot 2^{-n/2}}{(\frac{n}{2})! \sqrt{n+1}}, & \text{se } n \text{ é par.} \\ \frac{2^n \pi^{(n-1)/2} ((n-1)/2)! 2^{-n/2}}{n! \sqrt{n+1}}, & \text{se } n \text{ é ímpar.} \end{cases},$$

raio de cobertura

$$R = \rho \left\{ \frac{2a(n+1-a)}{n+1} \right\}^{1/2},$$

onde a é a parte inteira de $(n+1)/2$, e kissing number $\tau = n(n+1)$. Os vetores minimais são todas as permutações do vetor $(1, -1, 0, \dots, 0)$.

Exemplo 2.3.1. O reticulado A_2 é um reticulado bidimensional no $\mathbb{R}^3$, com matriz geradora dada por

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

e possui a maior densidade de empacotamento na dimensão 2.

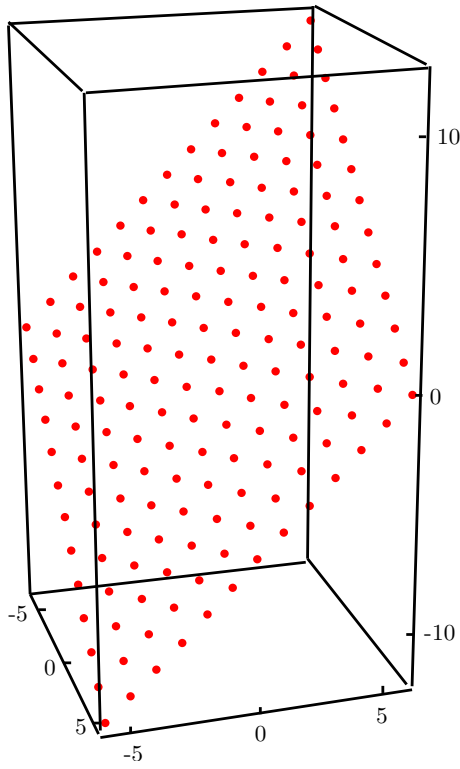


Figura 2.3: Reticulado A_2 .

Reticulado hexagonal

O reticulado hexagonal Λ é um reticulado bidimensional equivalente ao reticulado A_2 , com uma matriz geradora dada por

$$M = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

Temos que $\det(\Lambda) = 3/4$, raio de empacotamento $\rho = 1/2$, norma mínima $\eta = 1$, densidade de empacotamento $\Delta = \pi/\sqrt{12}$, densidade de centro $\delta = 1/\sqrt{12}$, raio de cobertura $R = 2\rho/\sqrt{3}$ e kissing number $\tau = 6$. O reticulado recebe este nome pelo fato das regiões de Voronoi serem hexágonos.

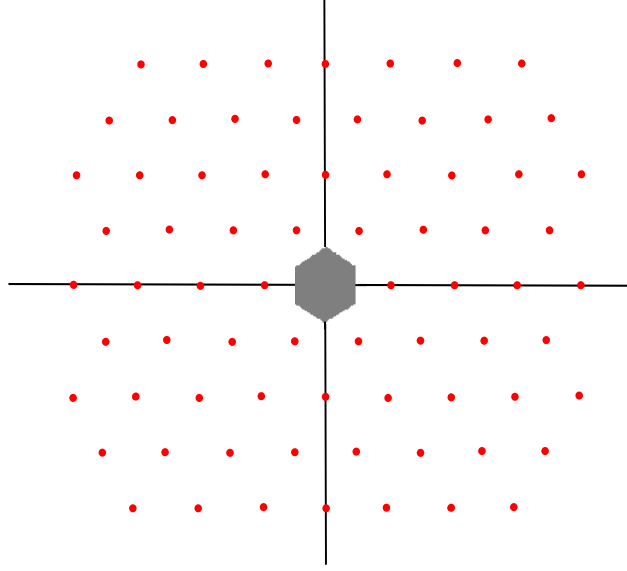


Figura 2.4: Reticulado hexagonal com região de Voronoi associada à origem.

Reticulado fcc

O reticulado fcc (cubo de face centrada) é um reticulado tridimensional equivalente ao A_3 e ao D_3 , que será definido adiante. O empacotamento referente a este reticulado é normalmente encontrado em bancas de frutas, pirâmide de laranjas (Figura 2.5).

O reticulado é formado por todos os pontos $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que $x_1 + x_2 + x_3$ é um número par. Uma matriz geradora para o fcc é dada por:

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

Temos que $\det(\Lambda) = 4$, raio de empacotamento $\rho = \sqrt{2}/2$, norma mínima $\eta = 2$, densidade de empacotamento $\Delta = \pi/\sqrt{18}$, densidade de centro $\delta = 2^{-5/2}$, raio de cobertura $R = 1$ e kissing number $\tau = 12$. Os vetores minimais são todas as permutações do vetor $(\pm 1, \pm 1, 0)$.

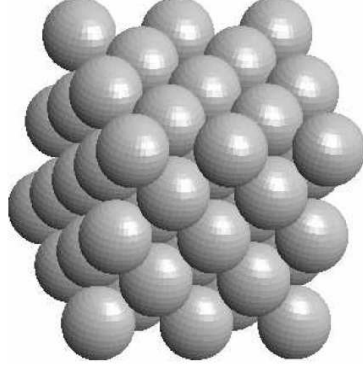


Figura 2.5: Empacotamento do reticulado fcc.

Reticulado bcc

O reticulado bcc (body-centered cubic) é um reticulado tridimensional equivalente ao A_3^* (dual do A_3) e ao D_3^* (dual do D_3). O reticulado é formado por todos os pontos $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que x_1, x_2 e x_3 são todos pares ou todos ímpares. Uma matriz geradora para o bcc é dada por:

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

Temos que $\det(\Lambda) = 16$, raio de empacotamento $\rho = \sqrt{3}/2$, norma mínima $\eta = 3$, densidade de empacotamento $\Delta = \pi\sqrt{3}/8$, densidade de centro $\delta = 3\sqrt{3}/32$, raio de cobertura $R = \sqrt{5}/2$ e kissing number $\tau = 8$. Os vetores minimais são $(\pm 1, \pm 1, \pm 1)$.

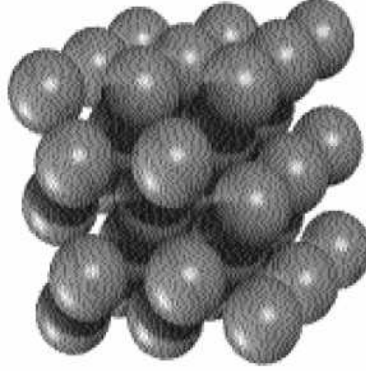


Figura 2.6: Empacotamento do reticulado bcc.

Reticulado mcc

O reticulado mcc (mean-centered cubic) é um reticulado isodual tridimensional. Uma matriz geradora para o mcc é dada por:

$$M = \begin{pmatrix} \sqrt{\frac{1}{2}} & \sqrt[4]{\frac{1}{2}} & 0 \\ \sqrt{\frac{1}{2}} & 0 & \sqrt[4]{\frac{1}{2}} \\ 0 & \sqrt[4]{\frac{1}{2}} & \sqrt[4]{\frac{1}{2}} \end{pmatrix}$$

Temos que $\det(\Lambda) = 1$, raio de empacotamento $\rho = \frac{1}{2} \sqrt[4]{\frac{1}{2} + \sqrt{\frac{1}{2}}}$, norma mínima $\sqrt{\frac{1}{2} + \sqrt{\frac{1}{2}}}$, densidade de empacotamento $\Delta = 0.6940 \dots$, densidade de centro $\delta = 0.1657 \dots$, raio de cobertura $R = \sqrt{3}/\sqrt[4]{32}$ e kissing number $\tau = 8$.

Reticulado D_n

O reticulado D_n , $n \geq 3$, é definido por

$$D_n = \{(x_1, x_2, \dots, x_n) \in \mathbb{Z}^n : x_1 + x_2 + \dots + x_n \text{ é par}\}.$$

Possui uma matriz geradora M , dada por

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

Temos que $\det(D_n) = 4$, raio de empacotamento $\rho = \sqrt{2}/2$, norma mínima $\eta = 2$, densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2} \cdot 2^{-(n+2)/2}}{(\frac{n}{2})!}, & \text{se } n \text{ é par.} \\ \frac{2^n \pi^{(n-1)/2} ((n-1)/2)! \cdot 2^{-(n+2)/2}}{n!}, & \text{se } n \text{ é ímpar.} \end{cases},$$

densidade de centro $\delta = 2^{-(n+2)/2}$, raio de cobertura $R = \rho\sqrt{2}$ ($n = 3$) ou $R = \rho\sqrt{n/2}$ ($n \geq 4$), e kissing number $\tau = 2n(n-1)$. Os vetores minimais são todas as permutações de $(\pm 1, \pm 1, 0, \dots, 0)$. O reticulado D_n é o reticulado mais denso conhecido para $n = 4$ e $n = 5$.

Reticulado E_8

O reticulado E_8 é um reticulado 8-dimensional definido por

$$E_8 = \{(x_1, x_2, \dots, x_8) \in \mathbb{R}^8 : \forall x_i, x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + 1/2, \sum x_i \equiv 0(\text{mod}2)\}$$

Uma matriz geradora é dada por

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Temos que $\det(E_8) = 1$, raio de empacotamento $\rho = \sqrt{2}/2$, norma mínima $\eta = 2$, densidade de empacotamento $\Delta = \pi^4/384$, densidade de centro $\delta = 1/16$, raio de cobertura $R = 1$ e kissing number $\tau = 240$. O reticulado E_8 é o reticulado mais denso conhecido em dimensão 8.

Reticulado E_7

O reticulado E_7 é um reticulado 7-dimensional definido por

$$E_7 = \{(x_1, x_2, \dots, x_8) \in E_8; \sum_{i=1}^8 x_i = 0\},$$

ou seja, E_7 é um sub-reticulado de E_8 . Uma matriz geradora é dada por

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Temos que $\det(E_7) = 2$, raio de empacotamento $\rho = \sqrt{2}/2$, norma mínima $\eta = 2$, densidade de empacotamento $\Delta = \pi^3/105$, densidade de centro $\delta = 1/16$, raio de cobertura $R = \sqrt{3/2}$ e kissing number $\tau = 126$. O reticulado E_7 é o reticulado mais denso conhecido em dimensão 7.

Reticulado E_6

O reticulado E_6 é um reticulado 6-dimensional definido por

$$E_6 = \{(x_1, x_2, \dots, x_8) \in E_8; x_1 + x_8 = x_2 + \dots + x_7 = 0\},$$

ou seja, E_6 é um sub-reticulado de E_8 . Uma matriz geradora é dada por

$$M = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Temos que $\det(E_6) = 3$, raio de empacotamento $\rho = \sqrt{2}/2$, norma mínima $\eta = 2$, densidade de empacotamento $\Delta = \pi^3/48\sqrt{3}$, densidade de centro $\delta = 1/8\sqrt{3}$, raio de cobertura $R = \rho\sqrt{8/3}$ e kissing number $\tau = 72$. O reticulado E_6 é o reticulado mais denso conhecido em dimensão 6.

Reticulado de Coxeter-Todd K_{12}

O reticulado K_{12} é um reticulado 12-dimensional e foi descrito por Coxeter e Todd em 1954. Uma matriz geradora é dada por

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & 0 & 1 & 0 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 1 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & -\frac{\sqrt{3}}{2} & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} & 0 \end{pmatrix}.$$

Temos que $\det(K_{12}) = 729$, raio de empacotamento $\rho = 1$, norma mínima $\eta = 4$, densidade de empacotamento $\Delta = \pi^6/19440$, densidade de centro $\delta = 1/27$, raio de cobertura $R = \sqrt{8/3}$ e kissing number $\tau = 756$. O reticulado K_{12} é o reticulado mais denso conhecido em dimensão 12.

Reticulado de Barnes-Wall Λ_{16}

O reticulado Λ_{16} é um reticulado 16-dimensional e foi descrito por Barnes e Wall em 1959. Uma matriz geradora é dada por

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Temos que $\det(\Lambda_{16}) = 256$, raio de empacotamento $\rho = 1$, norma mínima $\eta = 4$, densidade de empacotamento $\Delta = \pi^8/16.8!$, densidade de centro $\delta = 1/16$, raio de cobertura $R = \sqrt{3}$ e kissing number $\tau = 4320$. O reticulado Λ_{16} é o reticulado mais denso conhecido em dimensão 16.

Reticulado de Leech Λ_{24}

O reticulado Λ_{24} é um reticulado 24-dimensional e foi descrito por Leech em 1965. Uma matriz geradora é dada por

[illegible]

Temos que $\det(\Lambda_{24}) = 1$, raio de empacotamento $\rho = 1$, norma mínima $\eta = 4$, densidade de empacotamento $\Delta = \pi^{12}/12!$, densidade de centro $\delta = 1$, raio de cobertura $R = \sqrt{2}$ e kissing number $\tau = 196560$. O reticulado Λ_{24} é o reticulado mais denso conhecido em dimensão 24.

CAPÍTULO 3

RETICULADOS ALGÉBRICOS

Neste capítulo estabelecemos os conceitos relativos à reticulados obtidos via Teoria Algébrica dos Números. Dado $\mathbb{K}$ um corpo de números, a imagem de um ideal $\mathcal{A}$, contido no anel dos inteiros algébricos do corpo $\mathbb{K}$, pelo homomorfismo canônico $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ ou pela perturbação do homomorfismo canônico $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ é um reticulado no $\mathbb{R}^n$, chamado reticulado algébrico. Tais reticulados constituem a classe dos reticulados ideais, que são reticulados dotados com uma forma traço. Uma importante aplicação dos reticulados está relacionada à Modulação, Criptografia e Codificação de fonte e canal. Constelações de sinais com estrutura de reticulados são consideradas boas para transmissão de sinais, pois a estrutura linear e simétrica dos reticulados simplifica a tarefa de geração e demodulação. As referências utilizadas foram [11], [12], [23], [25], [26], [30], [31], [32] e [57].

3.1 Conceitos básicos

Sejam $\mathbb{K}$ um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_j : \mathbb{K} \rightarrow \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$ diz-se que σ_j é real, caso contrário, σ_j é dito imaginário. Quando todos os monomorfismos são reais diz-se que $\mathbb{K}$ é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um corpo totalmente complexo.

Se $\alpha : \mathbb{C} \rightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \dots, n$, 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, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \dots, \sigma_n$ de tais modo que $\sigma_1, \dots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \dots, r_2$. Então $n - r_1$ é um número par, assim podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \rightarrow \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ definido por

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

é um homomorfismo injetivo de anéis, chamado de *homomorfismo canônico* de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. O par (r_1, r_2) é chamado a *assinatura* de $\mathbb{K}$. 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

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \Re \sigma_{r_1+1}(x), \Im \sigma_{r_1+1}(x), \dots, \Re \sigma_{r_1+r_2}(x), \Im \sigma_{r_1+r_2}(x)),$$

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

Observação 3.1.1. Podemos definir um mergulho similar se considerarmos ao invés da extensão $\mathbb{K}/\mathbb{Q}$ a extensão relativa $\mathbb{L}/\mathbb{K}$.

Exemplo 3.1.1. Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_5)$, 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 $\mathbb{K}$ em $\mathbb{C}$. Como $\mathbb{K}$ 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 $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 \in \mathbb{K}$, com $a, b, c, d, e \in \mathbb{Q}$, temos que $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x), \Re\sigma_2(x), \Im\sigma_2(x))$.

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 $\mathbb{K}$. Isto pode ser visto de maneira formal no resultado que segue.

Teorema 3.1.1. [57] Sejam $\{w_1, \dots, w_n\}$ uma base integral de $\mathbb{K}$ e $\sigma : \mathbb{K} \rightarrow \mathbb{C}$ o homomorfismo canônico. Os n vetores $\mathbf{v}_i = \sigma(w_i) \in \mathbb{R}^n, i = 1, \dots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado reticulado algébrico de posto máximo, $\Lambda = \sigma(\mathcal{O}_{\mathbb{K}})$.

Proposição 3.1.1. [57] Seja $\mathbb{K}$ um corpo de números de grau n e M um $\mathbb{Z}$ -submódulo livre de $\mathbb{K}$ 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 $\mathbb{R}^n$.

Concluimos assim, que o ingrediente chave para a construção de reticulados algébricos tem sido a existência de uma $\mathbb{Z}$ -base livre em $\mathbb{K}$. Como $\mathcal{O}_{\mathbb{K}}$ 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

$$M = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_{r_1}(w_1) & \Re\sigma_{r_1+1}(w_1) & \cdots & \Im\sigma_{r_1+r_2}(w_1) \\ \vdots & & & & \vdots & \\ \sigma_1(w_n) & \cdots & \sigma_{r_1}(w_n) & \Re\sigma_{r_1+1}(w_n) & \cdots & \Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}, \quad (3.1.1)$$

onde $\{w_1, \dots, w_n\}$ é aqui uma base de $\mathcal{O}_{\mathbb{K}}$.

Um reticulado algébrico Λ' construído a partir de um ideal $\mathcal{A} \subset \mathcal{O}_{\mathbb{K}}$ fornece um sub-reticulado ([26],[42]) do reticulado algébrico Λ construído a partir de $\mathcal{O}_{\mathbb{K}}$. Se $\mathcal{A} = \mathfrak{a}\mathcal{O}_{\mathbb{K}}$, então a matriz geradora M é dada por

$$M = \begin{pmatrix} \sigma_1(\mathfrak{a}w_1) & \cdots & \sigma_{r_1}(\mathfrak{a}w_1) & \Re\sigma_{r_1+1}(\mathfrak{a}w_1) & \cdots & \Im\sigma_{r_1+r_2}(\mathfrak{a}w_1) \\ \vdots & & & & & \vdots \\ \sigma_1(\mathfrak{a}w_n) & \cdots & \sigma_{r_1}(\mathfrak{a}w_n) & \Re\sigma_{r_1+1}(\mathfrak{a}w_n) & \cdots & \Im\sigma_{r_1+r_2}(\mathfrak{a}w_n) \end{pmatrix} \quad (3.1.2)$$

onde $\{w_1, \dots, w_n\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$. Equivalentemente, a matriz (3.1.2) é a matriz (3.1.1) 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

$$\begin{aligned} \det(\Lambda) &= |\det(M)|^2 \\ &= |\det[\sigma_j(\mathfrak{a}w_i)]|^2 \\ &= 2^{-r_2} |\mathcal{N}(\mathfrak{a})|^2 |\det[\sigma_j(w_i)]|^2 \\ &= 2^{-r_2} |\mathcal{N}(\mathfrak{a})|^2 d_{\mathbb{K}}. \end{aligned}$$

3.2 Reticulado ideal

Esta seção é dedicada aos reticulados ideais, que são reticulados dotados com uma forma traço. As referências utilizadas foram [3], [4], [5], [8], [26], [29].

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

Definição 3.2.1. *Um corpo de números $\mathbb{K}$ é chamado um corpo CM (Complex Multiplication) se existe um corpo de números totalmente real $\mathbb{F}$ tal que $\mathbb{K}$ é uma extensão quadrática totalmente imaginária de $\mathbb{F}$.*

Observação 3.2.1. Denotamos por $\mathbb{K}^{Gal}$ o fecho de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ (Definição 1.4.15). Note que se $\mathbb{K}$ é um corpo CM, então a conjugação complexa comuta com todos os elementos de $Gal(\mathbb{K}^{Gal}/\mathbb{Q})$.

Definição 3.2.2.

1. Uma involução $\mathbb{Q}$ -linear $\bar{\cdot} : \mathbb{K} \longrightarrow \mathbb{K}$ é uma aplicação aditiva e multiplicativa tal que $\bar{\bar{x}} = x$, para $\forall x \in \mathbb{K}$.
2. O conjunto $\mathbb{F} = \{x \in \mathbb{K} \mid \bar{x} = x\}$ é um corpo, chamado corpo fixo da involução.

Definição 3.2.3. Um reticulado inteiro é um par (L, b) , onde L é um $\mathbb{Z}$ -módulo livre de posto n e $b : L \times L \rightarrow \mathbb{Z}$ é uma forma $\mathbb{Z}$ -bilinear simétrica.

Definição 3.2.4. Seja $\{v_1, v_2, \dots, v_n\}$ 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 , pois o determinante independe da escolha da base.

Definição 3.2.5. Seja $\mathcal{A}$ um ideal de $\mathcal{O}_K$, e seja $\alpha \in \mathbb{F}$ tal que $\alpha\mathcal{A}\bar{\mathcal{A}} \subset \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$. Um reticulado ideal é um reticulado inteiro $(\mathcal{A}, b_\alpha)$, onde

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

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

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

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

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

Proposição 3.2.1. [23] Seja $(\mathcal{A}, b_\alpha)$ um reticulado ideal, então $|det(b)| = |d_{\mathbb{K}}| \mathcal{N}(\mathcal{A})^2 \mathcal{N}(\alpha)$.

3.3 Retiçulados via a perturbação do homomorfismo canônico

Nesta seção apresentamos uma perturbação do homomorfismo canônico e a geração de retiçulados a partir dela.

Definição 3.3.1. *Seja α um elemento totalmente real e totalmente positivo de $\mathbb{K}$, isto é, $\sigma_i(\alpha)$ é real e totalmente positivo para todo i .*

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

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

onde $\alpha_i = \sigma_i(\alpha) > 0$, para $i = 1, \dots, n$, é chamado uma perturbação do homomorfismo canônico.

Corolário 3.3.1. *[30] Seja G um $\mathbb{Z}$ -módulo livre de posto n de $\mathcal{O}_{\mathbb{K}}$ com $\mathbb{Z}$ -base $\{w_1, \dots, w_n\}$. Então a imagem de $\sigma_\alpha(G)$ de G em $\mathbb{R}^n$ é um retiçulado com geradores $\{\sigma_\alpha(w_1), \dots, \sigma_\alpha(w_n)\}$.*

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

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

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

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 3.3.2. *Seja $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}$ -base de $\mathcal{A}$. O retiçulado $\sigma_\alpha(\mathcal{A})$ 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 3.3.1. [30] *Seja $\mathbb{K}$ um corpo de números totalmente real ou CM. Então o reticulado $\sigma_\alpha(\mathcal{A})$ é um reticulado ideal.*

Demonstração: Para mostrar que $\sigma_\alpha(\mathcal{A})$ 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

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

A segunda igualdade vale pois a conjugação complexa comuta com todos os σ_i , $i = 1, \dots, n$, (ver Observação (3.2.1)). Provamos assim que as entradas da matriz G são da forma traço. Agora, como $\{w_1, \dots, w_n\}$ é uma $\mathbb{Z}$ -base de $\mathcal{A}$, para $\forall x, y \in \mathcal{A}$ temos

$$b_\alpha(x, y) = b_\alpha\left(\sum_{i=1}^n a_i w_i, \sum_{j=1}^n b_j w_j\right) = \sum_{i=1}^n \sum_{j=1}^n a_i b_j b_\alpha(w_i, w_j)$$

$$\begin{aligned}
&= \sum_{i=1}^n \sum_{j=1}^n a_i b_j \operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha w_i \overline{w_j}) = \operatorname{Tr}_{\mathbb{K}/\mathbb{Q}} \left(\alpha \sum_{i=1}^n a_i w_i \sum_{j=1}^n b_j \overline{w_j} \right) \\
&= \operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha x \overline{y}),
\end{aligned} \tag{3.3.3}$$

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

Observação 3.3.1. *Pela Proposição 3.3.1, se $\{w_1, \dots, w_n\}$ é uma $\mathbb{Z}$ -base de $\mathcal{A}$, então o reticulado ideal $\sigma_\alpha(\mathcal{A})$ tem matriz de Gram $G = (g_{ij})_{i=1}^n$ dada por*

$$g_{ij} = \operatorname{Tr}(\alpha w_i \overline{w_j}).$$

Observação 3.3.2. *Daqui em diante denotaremos o reticulado ideal $\sigma_\alpha(\mathcal{A})$ por $(\mathcal{A}, b_\alpha)$.*

Note a hipótese sobre α , comparada à Definição (3.2.5). Aqui α não é mais tomado satisfazendo $\alpha \mathcal{A} \overline{\mathcal{A}} \subseteq \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$. 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 reticulados ideais tem a vantagem de que os pontos do reticulado são imagens de inteiros algébricos através do homomorfismo canônico aplicado em $\mathcal{O}_{\mathbb{K}}$. Deste modo, a correspondência entre os pontos $\mathbf{x} \in \Lambda \subseteq \mathbb{R}^n$ e os inteiros algébricos permite obter parâmetros associados a Λ , como a densidade e a distância produto, que para reticulados gerais são problemas difíceis.

Usando a matriz geradora dada na Definição (3.3.2), um ponto do reticulado pode ser expresso como

$$\begin{aligned}
\mathbf{x} &= (x_1, \dots, x_{r_1}, x_{r_1+1}, \dots, x_{r_1+r_2}) \\
&= \left(\sum_{i=1}^n \lambda_i \sqrt{\alpha_1} \sigma_1(w_i), \dots, \sum_{i=1}^n \lambda_i \sqrt{2\alpha_{r_1+1}} \Re(\sigma_{r_1+1}(w_i)), \dots, \sum_{i=1}^n \lambda_i \sqrt{2\alpha_{r_1+r_2}} \Im(\sigma_{r_1+r_2}(w_i)) \right),
\end{aligned}$$

$$\lambda_i \in \mathbb{Z}, \quad i = 1, \dots, n.$$

$$= (\sqrt{\alpha_1}\sigma_1(\sum_{i=1}^n \lambda_i w_i), \dots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(\sum_{i=1}^n \lambda_i w_i), \dots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(\sum_{i=1}^n \lambda_i w_i)).$$

Portanto,

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

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

3.3.1 Diversidade

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

Lembramos que dados dois vetores $\mathbf{x}$ e $\mathbf{y}$ 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

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

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

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

Teorema 3.3.1. [30] *Os reticulados ideais $\Lambda = (\mathcal{A}, b_\alpha)$ exibem uma diversidade $\text{div}(\Lambda) = r_1 + r_2$, onde (r_1, r_2) é a assinatura de $\mathbb{K}$.*

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

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

com $x \in \mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$. 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 $\text{div}(\Lambda) \geq r_1 + r_2$. Agora, se $x = 1$, então $\sigma_j(1) = 1$, para $\forall j = 1, \dots, r_1 + r_2$, e portanto $\sigma_\alpha(1)$ fornece $r_1 + r_2$ coeficientes não nulos, o que conclui a demonstração. $\square$

3.3.2 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

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

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

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

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

Pelo Teorema (3.3.1) 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 3.3.4. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n e $\mathbf{x} = (x_1, \dots, x_n) \in \Lambda$. A distância produto mínima de Λ é*

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

Seja $\mathbb{K}$ um corpo de números totalmente real de grau n com discriminante $d_{\mathbb{K}}$. A distância produto mínima de um reticulado ideal está relacionada com propriedades algébricas do corpo de números.

Teorema 3.3.2. [30] *Seja $\mathcal{A}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. A distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{A}, b_{\alpha})$ de determinante $\det(\Lambda)$ é*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} \min(\mathcal{A})$$

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

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

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

Como, pela Proposição 3.2.1, $\det(\Lambda) = \mathcal{N}(\alpha) \mathcal{N}(\mathcal{A})^2 d_{\mathbb{K}}$, segue que $\sqrt{\mathcal{N}(\alpha)} = \frac{\sqrt{\det(\Lambda)}}{\sqrt{d_{\mathbb{K}} \mathcal{N}(\mathcal{A})}}$. Logo concluímos que

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

□

Corolário 3.3.2. [30] *Se $\mathcal{A}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$ então a distância produto mínima de Λ é*

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

Demonstração: De acordo com o Teorema 3.3.2, precisamos provar que $\min_{0 \neq x \in \mathcal{A}} \mathcal{N}(x) = \mathcal{N}(\mathcal{A})$. Como $\mathcal{A}$ é um ideal principal, segue que $\mathcal{A} = (\mathfrak{a})$, para $\mathfrak{a} \in \mathcal{A}$, e

$\mathcal{N}(\mathcal{A}) = |\mathcal{N}(\mathfrak{a})|$. Se $x \in \mathcal{A}$, $x \neq 0$, então $x = \mathfrak{a}z$ para algum $z \in \mathcal{O}_{\mathbb{K}}$. Assim,

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

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 $\min(\mathcal{A}) = \min_{0 \neq x \in \mathcal{A}} \frac{|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{A})} = \frac{\mathcal{N}(\mathcal{A})}{\mathcal{N}(\mathcal{A})} = 1$, segue que $d_{p,\min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}}$. $\square$

Observação 3.3.3. Se $\det(\Lambda) = 1$, então

$$d_{p,\min}(\Lambda) = \frac{1}{\sqrt{d_{\mathbb{K}}}},$$

ou seja, a distância produto mínima depende somente do discriminante do corpo $\mathbb{K}$.

Limitante superior para a distância produto mínima

Pela Observação 3.3.3 nota-se que maximizar a distância produto mínima é equivalente a minimizar o discriminante do corpo. Isto já foi observado, por exemplo em [31], onde foram construídos reticulados $\mathbb{Z}^n$ rotacionados sobre corpos totalmente reais com discriminante mínimo, nas dimensões 2 a 7. Para $n \geq 8$, muitas famílias de $\mathbb{Z}^n$ rotacionados foram construídas resultando nas melhores performances conhecidas, mas nenhuma prova de otimalidade foi dada. A razão é que para $n \geq 8$ encontrar corpos de números totalmente reais com discriminante pequeno é uma questão difícil. Mas existem limitantes inferiores para o discriminante de corpos de números, como por exemplo o limitante de Odlyzko [[11], [12]] que veremos a seguir, e será usado para encontrar um limitante superior para a distância produto mínima. O resultado diz que assintoticamente para $n \rightarrow \infty$, temos o seguinte limitante inferior para a raiz n -ésima do discriminante

$$d_{\mathbb{K}}^{1/n} \geq (60.8395 \dots)^{r_1/n} (22.3816 \dots)^{2r_2/n} - o(n^{-2/3}) = C_n$$

Assim, a distância produto mínima normalizada é limitada superiormente por

$$\sqrt[n]{d_{p,\min}(\Lambda)} = \left(\frac{1}{\sqrt{d_{\mathbb{K}}}} \right)^{1/n} \leq \frac{1}{\sqrt{C_n}}.$$

Distância produto mínima para ideais não principais

Vimos pelo Teorema 3.3.2 que dado $\mathcal{A}$ um ideal de $\mathcal{O}_{\mathbb{K}}$, a distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{A}, b_{\alpha})$ de determinante $\det(\Lambda)$ é dada por

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} \min(\mathcal{A})$$

onde $\min(\mathcal{A}) = \min_{0 \neq x \in \mathcal{A}} \frac{|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{A})}$. Temos que $\min(\mathcal{A}) > 1$ se $\mathcal{A}$ é um ideal não principal [32].

De fato, se $x \in \mathcal{A}$ temos que

$$|\mathcal{N}(x)| = \left| \frac{\mathcal{O}_{\mathbb{K}}}{x\mathcal{O}_{\mathbb{K}}} \right| = \left| \frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}} \right| \cdot \left| \frac{\mathcal{A}}{x\mathcal{O}_{\mathbb{K}}} \right| = \mathcal{N}(\mathcal{A}) \cdot \left| \frac{\mathcal{A}}{x\mathcal{O}_{\mathbb{K}}} \right| > \mathcal{N}(\mathcal{A}),$$

pois $\left| \frac{\mathcal{A}}{x\mathcal{O}_{\mathbb{K}}} \right| = 1$ se, e somente se, $\mathcal{A}$ é um ideal principal.

Sejam $\mathbb{K}$ e $\mathbb{K}'$ corpos de números totalmente reais de grau n distintos, $\mathcal{A}$ um ideal de $\mathcal{O}_{\mathbb{K}}$, onde $\mathcal{O}_{\mathbb{K}}$ é um anel não principal, e $\mathcal{A}'$ um ideal de $\mathcal{O}_{\mathbb{K}'}$, onde $\mathcal{O}_{\mathbb{K}'}$ é um anel principal. O que é conhecido (de um argumento usado em [30]) é que nestas condições

$$d_{\mathbb{K}} > d_{\mathbb{K}'},$$

ou seja, o discriminante do corpo cujo anel dos inteiros é não principal é maior do que o discriminante do corpo cujo anel dos inteiros é principal, e consequentemente temos

$$\frac{1}{\sqrt{d_{\mathbb{K}}}} < \frac{1}{\sqrt{d_{\mathbb{K}'}}}.$$

Suponhamos que os reticulados ideais $\sigma_{\alpha}(\mathcal{A})$ e $\sigma_{\alpha'}(\mathcal{A}')$ sejam versões rotacionadas do reticulado $\mathbb{Z}^n$. Em [25] é conjecturado que

$$d_{p,min}(\sigma_{\alpha}(\mathcal{A})) = \frac{1}{\sqrt{d_{\mathbb{K}}}} \min(\mathcal{A}) < \frac{1}{\sqrt{d_{\mathbb{K}'}}} = d_{p,min}(\sigma_{\alpha'}(\mathcal{A}')),$$

ou seja, quando trabalhamos em corpos de números distintos, apesar de termos um ganho na distância produto mínima do reticulado $\sigma_{\alpha}(\mathcal{A})$ representado por $\min(\mathcal{A}) > 1$, este ganho não é suficiente para inverter a relação de ordem entre as duas distâncias produto, e isto acontece

porque $\min(\mathcal{A})$ cresce muito menos do que o discriminante $d_{\mathbb{K}}$. Assim, a conjectura é que reticulados gerados por ideais não principais não representam ganho na distância produto quando comparamos com reticulados gerados por ideais principais em um corpo distinto.

No intuito de trabalhar com ideais não principais, as seguintes condições devem ser satisfeitas:

1. Obviamente devemos escolher um corpo $\mathbb{K}$ de grau n tal que $\mathcal{O}_{\mathbb{K}}$ não seja um domínio de ideais principais, de modo que não existam outras construções de $\mathbb{Z}^n$ rotacionados via corpos cujo anel dos inteiros seja domínio de ideais principais para a dimensão n escolhida, devido à conjectura acima.
2. Encontrar um ideal não principal $\mathcal{A} \subset \mathcal{O}_{\mathbb{K}}$ tal que o reticulado $(\mathcal{A}, b_{\alpha})$ seja uma versão rotacionada do reticulado $\mathbb{Z}^n$, e se também for possível encontrar um ideal principal $\mathcal{A}' \subset \mathcal{O}_{\mathbb{K}}$, tal que $(\mathcal{A}', b_{\alpha})$ seja uma versão rotacionada do reticulado $\mathbb{Z}^n$, como $\min(\mathcal{A}) > 1$ segue que a distância produto mínima do reticulado $(\mathcal{A}, b_{\alpha})$ será melhor do que a distância produto mínima do reticulado $(\mathcal{A}', b_{\alpha})$.

Algumas dificuldades surgem ao tentarmos satisfazer as condições acima:

1. Verificar se o anel dos inteiros de um corpo $\mathbb{K}$ é, ou não, um domínio de ideais principais pode ser uma tarefa difícil. Os resultados existentes na literatura são em relação a corpos quadráticos [52] e corpos ciclotômicos ([48], pp. 204).
2. Em [25], Bayer apresenta exemplos de reticulados $\mathbb{Z}^n$ rotacionados gerados através de ideais não principais em dimensão 2, mas dada uma dimensão n , não sabemos a dificuldade de construir reticulados $\mathbb{Z}^n$ rotacionados através de ideais não principais, principalmente se n for grande.
3. O cálculo de $\min(\mathcal{A})$ é uma tarefa difícil, principalmente se n for grande.

Definição 3.3.5. *Seja Λ um reticulado de dimensão n com norma mínima $\eta, \eta \geq 1$, obtido via um corpo de números totalmente real $\mathbb{K}$ com discriminante $d_{\mathbb{K}}$ gerado por um*

ideal principal $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$. Definimos a distância produto mínima normalizada de Λ por

$$\sqrt[n]{d_{p,min}(\Lambda)} = \frac{1}{\sqrt[n]{\eta}} \sqrt[2n]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}}$$

A distância mínima normalizada deve ser considerada, pois quando tomamos reticulados com vetor de norma mínima de tamanhos diferentes, para fazer uma comparação justa entre as distâncias produto mínimas, devemos considerar versões escalonadas desses reticulados, de forma que o vetor de menor norma das versões escalonadas seja unitário. Como o reticulado Λ deve ser escalonado para ter norma mínima 1, segue que no cálculo da distância produto mínima devemos multiplicar pelo fator $\frac{1}{(\sqrt[n]{\eta})^n}$. Assim, como $\mathcal{A}$ é um ideal principal, segue pelo Corolário 3.3.2 que

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} \cdot \frac{1}{(\sqrt[n]{\eta})^n},$$

ou seja,

$$\sqrt[n]{d_{p,min}(\Lambda)} = \left(\frac{1}{\eta^{n/2}}\right)^{1/n} \cdot \left(\left(\frac{\det(\Lambda)}{d_{\mathbb{K}}}\right)^{1/2}\right)^{1/n} = \frac{1}{\eta^{1/2}} \cdot \left(\frac{\det(\Lambda)}{d_{\mathbb{K}}}\right)^{1/2n} = \frac{1}{\sqrt[n]{\eta}} \sqrt[2n]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}}.$$

□

3.3.3 Densidade de centro

Estudamos o problema de calcular a densidade de centro de reticulados ideais. Seja Λ um reticulado em $\mathbb{R}^n$, vimos que a densidade de centro do reticulado Λ é dada por

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

onde n é a dimensão, ρ é o raio de empacotamento e $\mathcal{V}ol(\Lambda)$ é o volume do reticulado Λ . Pela Proposição 3.2.1 e pelo fato de que $\mathcal{V}ol(\Lambda) = \sqrt{\det(\Lambda)}$ segue que a densidade de centro do reticulado ideal $\Lambda = (\mathcal{A}, b_{\alpha})$ é dada por

$$\delta(\Lambda) = \frac{\rho^n}{[|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2}|\mathcal{N}(\mathcal{A})|} \quad (3.3.4)$$

As proposições a seguir são extensões dos resultados encontrados em [39] para a perturbação do homomorfismo canônico e referem-se a obtenção do raio de empacotamento e densidade de centro de um reticulado ideal.

Proposição 3.3.2. [2] *Se $\mathbb{K}$ é um corpo de números totalmente real ou CM e $x \in \mathbb{K}$ então*

$$||\sigma_\alpha(x)||^2 = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x \bar{x}),$$

onde $\bar{x}$ é o conjugado complexo de x .

Demonstração: Seja $\mathbb{K}$ um corpo de números de grau n de forma que $r_1 + 2r_2 = n$. Como $\sigma_\alpha(x) \in \mathbb{R}^n$, segue que

$$\begin{aligned} ||\sigma_\alpha(x)||^2 &= [\sqrt{\alpha_1}\sigma_1(x)]^2 + \cdots + [\sqrt{\alpha_{r_1}}\sigma_{r_1}(x)]^2 + [\sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x))]^2 + [\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x))]^2 + \\ &\quad + \cdots + [\sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x))]^2 + [\sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))]^2 = \\ &= \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2 + 2\alpha_{r_1+1}[\Re(\sigma_{r_1+1}(x))]^2 + 2\alpha_{r_1+1}[\Im(\sigma_{r_1+1}(x))]^2 + \\ &\quad + \cdots + 2\alpha_{r_1+r_2}[\Re(\sigma_{r_1+r_2}(x))]^2 + 2\alpha_{r_1+r_2}[\Im(\sigma_{r_1+r_2}(x))]^2 = \\ &= \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2 + 2\alpha_{r_1+1}[\Re(\sigma_{r_1+1}(x))]^2 + 2\alpha_{r_1+1}[\Im(\sigma_{r_1+1}(x))]^2 + \\ &\quad + \cdots + 2\alpha_{r_1+r_2}[\Re(\sigma_{r_1+r_2}(x))]^2 + 2\alpha_{r_1+r_2}[\Im(\sigma_{r_1+r_2}(x))]^2. \end{aligned}$$

Observe que $\Re(\sigma_k(x))^2 + \Im(\sigma_k(x))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\bar{x})$, para $r_1 + 1 \leq k \leq r_1 + r_2$. Assim, temos os seguintes fatos

- $r_1 = 0$

$$\begin{aligned} ||\sigma_\alpha(x)||^2 &= 2\alpha_1\sigma_1(x\bar{x}) + \cdots + 2\alpha_{r_2}\sigma_{r_2}(x\bar{x}) = 2\sigma_1(\alpha)\sigma_1(x\bar{x}) + \cdots + 2\sigma_{r_2}(\alpha)\sigma_{r_2}(x\bar{x}) = \\ &= 2\sigma_1(\alpha x \bar{x}) + \cdots + 2\sigma_{r_2}(\alpha x \bar{x}), \end{aligned}$$

como $\bar{\sigma}$ é a conjugação complexa, temos que $\sigma_{r_2+j}(\alpha x \bar{x}) = (\bar{\sigma} \circ \sigma_j)(\alpha x \bar{x}) = \sigma_j(\alpha x \bar{x})$, para $j = 1, \dots, r_2$. Logo,

$$\begin{aligned} ||\sigma_\alpha(x)||^2 &= \sigma_1(\alpha x \bar{x}) + \cdots + \sigma_{r_2}(\alpha x \bar{x}) + \sigma_{r_2+1}(\alpha x \bar{x}) + \cdots + \sigma_{r_2+r_2}(\alpha x \bar{x}) = \\ &= \sum_{i=1}^n \sigma_i(\alpha x \bar{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x \bar{x}). \end{aligned}$$

Portanto

$$||\sigma_\alpha(x)||^2 = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x \bar{x}).$$

- $r_2 = 0$

$$||\sigma_\alpha(x)||^2 = \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2$$

e como $\sigma_i(x) = (\bar{\sigma} \circ \sigma_i)(x) = \sigma_i(\bar{x})$ segue que $\sigma_i(x\bar{x}) = \sigma_i(x)\sigma_i(\bar{x}) = \sigma_i(x)\sigma_i(x) = [\sigma_i(x)]^2$ e assim,

$$\begin{aligned} ||\sigma_\alpha(x)||^2 &= \alpha_1\sigma_1(x\bar{x}) + \cdots + \alpha_{r_1}\sigma_{r_1}(x\bar{x}) = \sigma_1(\alpha)\sigma_1(x\bar{x}) + \cdots + \sigma_{r_1}(\alpha)\sigma_{r_1}(x\bar{x}) = \\ &= \sigma_1(\alpha x\bar{x}) + \cdots + \sigma_{r_1}(\alpha x\bar{x}) \end{aligned}$$

Portanto,

$$||\sigma_\alpha(x)||^2 = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x\bar{x})$$

e isto conclui a demonstração. $\square$

Corolário 3.3.3. [2] O raio de empacotamento do reticulado $\sigma_\alpha(\mathcal{A}) = (\mathcal{A}, b_\alpha)$ pode ser escrito da seguinte forma

$$\begin{aligned} \rho(\sigma_\alpha(\mathcal{A})) &= \frac{1}{2} \min\{||\sigma_\alpha(x)||, x \in \mathcal{A}, x \neq 0\} = \frac{1}{2} \min\left\{\sqrt{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x\bar{x})}, x \in \mathcal{A}, x \neq 0\right\} = \\ &= \frac{1}{2} \sqrt{\min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x\bar{x}), x \in \mathcal{A}, x \neq 0\}}. \end{aligned}$$

Proposição 3.3.3. [2] A densidade de centro do reticulado ideal $\Lambda = (\mathcal{A}, b_\alpha)$ é dada por

$$\delta(\Lambda) = \frac{1}{2^n [|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2}} \cdot \frac{t_\alpha^{n/2}}{|\mathcal{N}(\mathcal{A})|}$$

onde $t_\alpha = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x\bar{x}), x \in \mathcal{A}, x \neq 0\}$

Demonstração: Tomando $t_\alpha = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x\bar{x}), x \in \mathcal{A}, x \neq 0\}$, pelo Corolário 3.3.3 e Equação 3.3.4, segue que

$$\delta(\Lambda) = \frac{\left(\frac{\sqrt{t_\alpha}}{2}\right)^n}{[|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2}|\mathcal{N}(\mathcal{A})|} = \frac{\left(\frac{t_\alpha}{4}\right)^{\frac{n}{2}}}{[|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2}|\mathcal{N}(\mathcal{A})|} = \frac{1}{2^n [|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2}} \cdot \frac{t_\alpha^{n/2}}{|\mathcal{N}(\mathcal{A})|}.$$

$\square$

3.4 Resultados conhecidos na literatura

Nesta seção, através de um breve histórico retomamos resultados importantes conhecidos na literatura acerca de reticulados algébricos aplicados à Codificação (canal e fonte), Modulação e Criptografia, com o intuito de melhor situar a nossa contribuição neste trabalho. Os resultados são apresentados em ordem cronológica e nos limitamos a citar apenas as aplicações relacionadas a corpos ciclotômicos e corpos totalmente reais. Além disso, alguns resultados serão mais detalhados, enquanto em outros é introduzida somente a idéia central.

Resultados

1. Craig ([49], [50]) reproduz os reticulados E_8 e Λ_{24} via corpos ciclotômicos.
2. Boullé et al. [45] introduzem pela primeira vez a idéia de rotacionar uma constelação de sinais a fim de aumentar a sua diversidade, aumentando assim a sua eficiência para o Canal Rayleigh com desvanecimento, com a vantagem de manter as propriedades para o canal gaussiano, ou seja, a densidade de empacotamento não é alterada quando a constelação é rotacionada. Com base neste conceito, implementam um algoritmo que reproduz os reticulados mais densos nas dimensões 2, 3 e 5 sobre corpos totalmente reais.
3. Boutros et al. [38] reproduzem os reticulados D_4 , K_{12} e Λ_{16} via os corpos ciclotômicos $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_{21})$ e $\mathbb{Q}(\zeta_{40})$, respectivamente, e com diversidade igual à metade da dimensão. Além destes reticulados, reproduzem também uma família de reticulados variando a diversidade e comparando a performance para o canal gaussiano e Canal Rayleigh com desvanecimento. Apresentam uma tabela com o discriminante mínimo de corpos totalmente reais nas dimensões 2 a 8, conforme abaixo:

Dimensão	D_{min}
2	5
3	49
4	725
5	14641
6	300125
7	20134393
8	282300416

Tabela 3.1: Discriminante mínimo - dimensão 2 a 8

4. Boutros et al. [37] usando o corpo $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, o subcorpo maximal real de $\mathbb{Q}(\zeta_n)$, reproduzem os reticulados $\mathbb{Z}^3$ ($n = 7, 9, 14, 18$), $\mathbb{Z}^5$ ($n = 11, 22$), $\mathbb{Z}^9$ ($n = 19, 38$), $\mathbb{Z}^{11}$ ($n = 23, 46$) e $\mathbb{Z}^{15}$ ($n = 31, 62$), ou seja, constelações cúbicas com diversidade máxima.

$$\begin{array}{c}
\mathbb{L} = \mathbb{Q}(\zeta_n) \\
\left| \begin{array}{c} 2 \end{array} \right. \\
\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \longrightarrow \mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}} \\
\left| \begin{array}{c} m = \frac{\phi(n)}{2} \end{array} \right. \quad \sigma_{\mathbb{K}}(\mathcal{A}) \cong \mathbb{Z}^m \\
\mathbb{Q}
\end{array}$$

5. Bayer [23] através do corpo ciclotômico $\mathbb{Q}(\zeta_n)$ reproduz os seguintes reticulados:

Família $A_{p-1} \longrightarrow$ via $\mathbb{Q}(\zeta_p)$.

$D_4 \longrightarrow$ via $\mathbb{Q}(\zeta_8)$.

$E_6 \longrightarrow$ via $\mathbb{Q}(\zeta_9)$.

$E_8 \longrightarrow$ via $\mathbb{Q}(\zeta_{15})$, $\mathbb{Q}(\zeta_{20})$, $\mathbb{Q}(\zeta_{24})$.

$K_{12} \longrightarrow$ via $\mathbb{Q}(\zeta_{21})$.

$\Lambda_{24} \longrightarrow$ via $\mathbb{Q}(\zeta_{39})$ (Também obtido por Craig [49]).

Apresenta também um resultado que garante a existência de Λ_{24} via $\mathbb{Q}(\zeta_n)$, para $n = 35, 52, 56, 70, 78, 84$.

6. Oggier ([30],[31]) implementa um algoritmo que computa a matriz geradora de um reticulado inteiro, dada a sua matriz de Gram. Este algoritmo é baseado no método de Krüskemper, e através dele reproduz o reticulado $\mathbb{Z}^n$ nas dimensões 2 a 7 sobre corpos totalmente reais e com discriminante mínimo, otimizando assim a distância produto mínima nestas dimensões. A seguir damos uma idéia do método.

- Apresenta dois teoremas devidos a Taussky e Krüskemper que prova que qualquer reticulado inteiro pode ser construído como um reticulado ideal de alguma algebra $\mathbb{Z}[X]/(f(X)) = \mathbb{Z}[\theta]$, onde $f(X)$ é mônico e irredutível e θ é uma raiz de f .
- A entrada do algoritmo é a matriz $S = I_n$ (matriz de Gram do reticulado $\mathbb{Z}^n$), a seguir computa uma matriz A com entradas inteiras de modo que o polinômio característico de A é irredutível e $AS = SA^t$.
- Estabece mais alguns parâmetros e durante a construção tem controle sobre o discriminante $d_{\mathbb{K}}$, buscando sempre pelo discriminante mínimo, que é obtido escolhendo a matriz A de modo que o polinômio característico seja minimal.
- O algoritmo mostra como saída a matriz M , geradora do reticulado ideal.
- Trabalha em corpos totalmente reais, logo com diversidade máxima, e reproduz reticulados com discriminante mínimo e portanto obtêm distância produto mínima ótima na construção.

Podemos observar através da Tabela 3.2 que os discriminantes obtidos através do algoritmo são os discriminantes mínimos, basta compará-los à Tabela 3.1.

Dimensão	Polinômio mínimo	$d_{\mathbb{K}}$
2	$X^2 - X - 1$	5
3	$X^3 - X^2 - 2X + 1$	49
4	$X^4 - X^3 - 3X^2 + X + 1$	725
5	$X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$	14641
6	$X^6 - X^5 - 7X^4 + 2X^3 + 7X^2 - 2X - 1$	300125
7	$X^7 - X^6 - 6X^5 + 4X^4 + 10X^3 - 4X^2 - 4X + 1$	20134393
8	$X^8 + 2X^7 - 7X^6 - 8X^5 + 15X^4 + 8X^3 - 9X^2 - 2X + 1$	282300416

Tabela 3.2: Polinômio mínimo de θ , onde $\mathbb{K} = \mathbb{Q}(\theta)$ - dimensão 2 a 8.

7. Bayer et al. [26] reproduzem algumas famílias de reticulados ideais, a saber:

- Construção ciclotômica

Seja $p \geq 5$ um número primo e considere $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, o subcorpo maximal real de $\mathbb{L} = \mathbb{Q}(\zeta_p)$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ o seu anel dos inteiros algébricos. Tomando $\alpha = 2 - (\zeta_p + \zeta_p^{-1})$, temos que o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, \frac{1}{\sqrt{p}}b_{\alpha})$ é uma versão rotacionada do reticulado $\mathbb{Z}^n$, $n = \frac{p-1}{2}$.

$$\begin{array}{c}
\mathbb{L} = \mathbb{Q}(\zeta_p) \\
\left| \begin{array}{c} 2 \end{array} \right. \\
\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \longrightarrow \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}] \\
\left| \begin{array}{c} n = \frac{p-1}{2} \end{array} \right. \quad \sigma_{\alpha}(\mathcal{O}_{\mathbb{K}}) \cong \mathbb{Z}^n \\
\mathbb{Q}
\end{array}$$

- Construção cíclica

São construídos $\mathbb{Z}^n$ rotacionados sobre extensões cíclicas de $\mathbb{Q}$ de grau n primo, $n \geq 2$.

- Construção mista

Sejam $m = p_1 p_2 \cdots p_N$, onde os p_j 's são primos distintos para $j = 1, 2, \dots, N$, ζ_j a raiz p_j -ésima da unidade, $K_j = \mathbb{Q}(\zeta_j + \zeta_j^{-1})$ e $K = K_1 K_2 \cdots K_N$. Tomando $\alpha_j = (1 - \zeta_j)(1 - \zeta_j^{-1})$ é provado que o reticulado ideal

$$(\mathcal{O}_{\mathbb{K}}, \frac{1}{p_1} b_{\alpha_1} \otimes \frac{1}{p_2} b_{\alpha_2} \otimes \frac{1}{p_N} b_{\alpha_N}),$$

onde $\otimes$ denota o produto tensorial, é equivalente a $\mathbb{Z}^n$, para $n = \prod_{j=1}^N \frac{p_j - 1}{2}$.

8. Bayer et al. [28] apresentam alguns resultados que garantem a existência de reticulados equivalentes a alguns reticulados densos, obtidos via o subcorpo maximal real do corpo ciclotômico $\mathbb{Q}(\zeta_n)$. Dentre os resultados, o principal deles diz que se (I, α) é um reticulado ideal sobre a extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, então existe um reticulado ideal $(\tilde{I}, \alpha)$ equivalente a (I, α) sobre a extensão $\mathbb{Q}(\zeta_{4n} + \zeta_{4n}^{-1})/\mathbb{Q}$. Vimos por Bayer et al. [23] a obtenção dos reticulados E_6 sobre $\mathbb{Q}(\zeta_9)$, E_8 sobre $\mathbb{Q}(\zeta_{15})$, K_{12} sobre $\mathbb{Q}(\zeta_{21})$ e Λ_{24} sobre $\mathbb{Q}(\zeta_{39})$, assim existem reticulados equivalentes a E_6 sobre $\mathbb{Q}(\zeta_{36} + \zeta_{36}^{-1})$, E_8 sobre $\mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$, K_{12} sobre $\mathbb{Q}(\zeta_{84} + \zeta_{84}^{-1})$ e Λ_{24} sobre $\mathbb{Q}(\zeta_{140} + \zeta_{140}^{-1})$.
9. Bayer et al. [27] através do corpo $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, tomando $\alpha = 2 + (\zeta_{2^r} + \zeta_{2^r}^{-1})$, reproduz a família de reticulados $(\mathcal{O}_{\mathbb{K}}, \frac{1}{2^{r-1}} b_{\alpha})$ que são versões rotacionadas do reticulado $\mathbb{Z}^{r-2}$.
10. Bayer [24] apresenta alguns resultados sobre reticulados ideais obtidos via subcorpos maximais reais de corpos ciclotômicos de condutor potência de primo, a saber:

- Sejam p um primo ímpar, r um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$. O reticulado ideal $(\mathcal{O}_{\mathbb{K}}, \frac{1}{p^r} b_{\alpha})$, onde $\alpha = (1 - \zeta_{p^r}^{p^{r-1}})(1 - \zeta_{p^r}^{-p^{r-1}})$, é equivalente ao reticulado

$$\mathbb{Z}^{\frac{p-1}{2}} \oplus \mathcal{A}_p^r$$

onde $\mathcal{A}_p^r$ denota a soma direta das $\frac{p^{r-1}-1}{2}$ cópias do reticulado A_{p-1} .

- Sejam p um primo, r um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$.
 - (i) Se p é ímpar, e $\alpha = 1$, então o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, \frac{1}{p^r} b_{\alpha})$ é equivalente ao

reticulado

$$\bigoplus_{i=1,2,\dots,p^{r-1}} A_{p-1}^*$$

onde A_{p-1}^* é o dual de A_{p-1} .

(ii) Se $p = 2$ e $\alpha = 1$, então o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, \frac{1}{2^{r-1}}b_\alpha)$ é equivalente ao reticulado

$$\mathbb{Z}^{2^{r-1}}.$$

• Suponha que L é um reticulado ideal sobre $\mathbb{Z}[\zeta_m]$. Então

(i) Se p é um primo ímpar tal que $p \mid m$, então

$$\bigoplus_{i=1,2,\dots,p} L$$

é um reticulado ideal sobre $\mathbb{Z}[\zeta_{pm}]$.

(ii) Para qualquer inteiro positivo r ,

$$\bigoplus_{i=1,2,\dots,2^{r-1}} L$$

é um reticulado ideal sobre $\mathbb{Z}[\zeta_{2^r m}]$.

Exemplo 3.4.1. Para $m = 15$ vimos que E_8 é um reticulado ideal sobre $\mathbb{Z}[\zeta_m]$ (Bayer [23]), daí segue que

$$\bigoplus_{i=1,2,\dots,2^{r-1}} E_8$$

é um reticulado ideal sobre $\mathbb{Z}[\zeta_{2^r \cdot 3 \cdot 5}]$.

11. Andrade et al. [4] usando o subcorpo maximal real do corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$, $r \geq 3$, reproduzem reticulados $\mathbb{Z}^n$ rotacionados. Mais especificamente, tomando $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ e $\alpha = 2 - (\zeta_{2^r} + \zeta_{2^r}^{-1})$ é mostrado que o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, \frac{1}{2^{r-1}}b_\alpha)$ é uma versão rotacionada do reticulado $\mathbb{Z}^{r-2}$.

12. Elia et al. [54] usando as idéias da construção cíclica ([26]), onde foram construídos reticulados $\mathbb{Z}^n$ rotacionados, para n primo, estende o resultado para n ímpar. A seguir

damos uma idéia da construção.

O Teorema de Dirichlet diz que se r e s são inteiros tal que $1 \leq r \leq s$ e $\text{mdc}(r, s) = 1$, então a progressão aritmética $\{r, r + s, r + 2s, \dots, r + ks, \dots\}$ contém infinitos números primos. Assim, em particular, tomando $r = 1$ e $s = n$ um inteiro ímpar, temos que $1 + kn = p$, para algum primo p , ou seja $n \mid p - 1$. Como a extensão $\mathbb{Q}(\zeta_p)$ é cíclica (Teorema 1.4.10) e $n \mid p - 1$, segue pelo Teorema de Correspondência de Galois que existe um único corpo $\mathbb{K}$ contido em $\mathbb{Q}(\zeta_p)$ que é cíclico de grau n sobre $\mathbb{Q}$. Como n é ímpar e $n \mid \frac{p-1}{2}$ segue que $\mathbb{K}$ está contido no subcorpo maximal real $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Com base nesta idéia são construídos os $\mathbb{Z}^n$ rotacionados, para n ímpar.

13. Interlando et al. [39] reproduzem uma família de reticulados que assintoticamente são bons reticulados com relação à densidade de empacotamento, e possui um reticulado em cada dimensão $n \geq 1$.

Dado n inteiro, seja q o menor primo congruente a 1 módulo n , garantido pelo Teorema de Dirichlet. Sejam $\mathbb{L} = \mathbb{Q}(\zeta_q)$, $\mathcal{A} = (1 - \zeta_q)\mathcal{O}_{\mathbb{L}}$, $\mathbb{K}$ o subcorpo de $\mathbb{L}$ de modo que $[\mathbb{K} : \mathbb{Q}] = n$, $\mathcal{A}_{\mathbb{K}} = \mathcal{A} \cap \mathbb{K} \subset \mathbb{K}$ e m o inteiro mais próximo de $\frac{n}{2 \ln q}$. É mostrado que o reticulado $\mathcal{GC}_n = \sigma_{\mathbb{K}}(\mathcal{A}_{\mathbb{K}}^m)$ é uma generalização dos reticulados de Craig, quando $n = p - 1$.

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_p)$, $\mathcal{A} = (1 - \zeta_p)\mathcal{O}_{\mathbb{K}}$ e m o inteiro mais próximo de $\frac{p-1}{2 \ln p}$, o reticulado

$$A_{p-1}^m = \sigma_{\mathbb{K}}(\mathcal{A}^m)$$

é chamado de reticulado de Craig.

Como a família de reticulados de Craig representa reticulados densos em dimensões altas, segue que $\mathcal{GC}_n$ é assintoticamente uma família de bons reticulados em relação à densidade de empacotamento.

14. Flores et al. [10] reproduzem uma família de reticulados que representam um refinamento da família de Craig, em relação à densidade de empacotamento.

Tomando $\mathbb{K} = \mathbb{Q}(\zeta_p)$, escolhem um ideal $\mathcal{T}_p^m$ em $\mathcal{O}_{\mathbb{K}}$ de modo que o reticulado $\sigma(\mathcal{T}_p^m)$ possui densidade de centro no mínimo o dobro da densidade de centro do reticulado A_{p-1}^m , para $p \geq 59$, e no mínimo três vezes, para $p \geq 97$.

15. Flores et al. [9] reproduzem uma família de reticulados similares à família de Craig via o corpo ciclotômico $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$, com p, q primos distintos. Tomando $\mathcal{A} = (1 - \zeta_p)\mathcal{O}_{\mathbb{L}}$, $\mathcal{B} = (1 - \zeta_q)\mathcal{O}_{\mathbb{L}}$ e $\mathcal{T}_{ij} = \mathcal{A}^i \mathcal{B}^j \subseteq \mathcal{O}_{\mathbb{L}}$, com i, j inteiros, encontra-se um limitante inferior para a densidade de centro do reticulado $\sigma_{\mathbb{L}}(\mathcal{T}_{ij})$ dado por

$$\delta(\sigma_{\mathbb{L}}(\mathcal{T}_{ij})) \geq \frac{\sqrt{2pqij}}{2}, \quad i \leq \frac{p-1}{2}, \quad j \leq \frac{q-1}{2}.$$

Conclui-se também que $\delta(\sigma_{\mathbb{L}}(\mathcal{T}_{ij}))$ é similar à densidade de centro dos reticulados de Craig, assim os reticulados construídos são bons assintoticamente com relação à densidade de empacotamento.

16. Andrade et al. [5] promovendo algumas mudanças na construção feita por Elia [54], reproduzem uma família de reticulados $\mathbb{Z}^n$ rotacionados, para n par, lembrando que Bayer [23] havia construído para n primo ímpar e Elia [54] para n ímpar.

Distância produto mínima normalizada nas dimensões 2 a 30 - Resumo

Fizemos um resumo das distâncias produto mínimas normalizadas, dos reticulados $\mathbb{Z}^n$ rotacionados, obtidas dos resultados listados nesta seção para efeito de comparação nas dimensões 2 a 30 e apresentamos na Tabela 3.8.

n	A	B	C	D	E	F	G	Lim
2	0.66874	0.66874	—	—	0.59460	—	0.66874	0.66995
3	0.52275	0.52275	0.52275	—	—	0.52275	—	0.52461
4	0.43899	—	—	0.39763	0.38555	—	0.34560	0.44163
5	0.38321	0.38321	0.38321	—	—	0.38321	—	0.38794
6	0.34958	0.34344	—	0.34958	—	—	0.34344	0.35032
7	0.30080	—	0.23618	—	—	0.23618	—	0.32245
8	0.29382	0.28952	—	—	0.26106	—	0.28952	0.30093
9	—	0.27018	—	—	—	0.27018	—	0.28377
10	—	—	—	0.25627	—	—	0.18803	0.26973
11	—	0.24045	0.24045	—	—	0.24045	—	0.25801
12	—	—	—	0.22967	—	—	0.13995	0.24807
13	—	—	0.16002	—	—	0.16002	—	0.23951
14	—	0.20942	—	—	—	—	0.20942	0.23205
15	—	0.20942	—	—	—	0.20138	—	0.22548
16	—	—	—	0.19361	0.18064	—	0.11713	0.21965
17	—	—	0.11292	—	—	0.11292	—	0.21444
18	—	0.18174	—	0.18068	—	—	0.18174	0.20973
19	—	—	0.08308	—	—	0.08308	—	0.20547
20	—	0.17136	—	—	—	—	0.17136	0.20159
21	—	0.16678	—	—	—	0.16678	—	0.19803
22	—	—	—	0.16080	—	—	0.11738	0.19475
23	—	0.15859	0.15859	—	—	0.15859	—	0.19173
24	—	—	—	0.15134	—	—	0.11168	0.18892
25	—	—	—	0.10574	—	0.10912	—	0.18631
26	—	0.14825	—	—	—	—	0.14825	0.18388
27	—	—	—	0.14124	—	0.10447	—	0.18160
28	—	—	—	0.14005	—	—	0.10235	0.17947
29	—	0.13967	0.13967	—	—	0.13967	—	0.17746
30	—	0.13711	—	0.13161	—	—	0.13711	0.17556

A - Krüskemper método (Oggier [30],[31]).

B,C,D - Construções ciclotômica, cíclica e mista, respectivamente (Bayer et al. [26]).

E - Construção via $\mathbb{Q}(\zeta_{2r})$ (Andrade et al. [4]).

F - Construção cíclica, n ímpar (Elia et al [54]).

G - Construção cíclica, n par (Andrade et al. [5]).

Lim - Limitante de Odlyzko. [11]

Tabela 3.3: Distância produto mínima de reticulados $\mathbb{Z}^n$ - dimensão 2 a 30.

CAPÍTULO 4

CONSTRUÇÃO ALGÉBRICA DE RETICULADOS DENSOS - ABORDAGEM MATRICIAL

O objetivo deste capítulo é a construção de reticulados ideais sobre corpos totalmente reais, de modo que tais reticulados são versões escalonadas e rotacionadas de alguns dos reticulados obtidos no Capítulo 2. Assim, estes reticulados podem ser suporte para constelações de sinais eficientes tanto para o canal Rayleigh com desvanecimento quanto para o canal gaussiano. Para as dimensões 2, 4, 6 e 8 construímos reticulados com a mesma densidade de centro dos reticulados A_2 , D_4 , E_6 e E_8 , e como estes reticulados são os únicos reticulados mais densos em suas respectivas dimensões [42], conclui-se que nossas construções são versões rotacionadas e escalonadas destes reticulados. Para a dimensão 12, construímos um reticulado com a mesma densidade de centro do reticulado K_{12} e para provar que nossa

construção é uma versão escalonada e rotacionada do reticulado K_{12} , implementamos um algoritmo que encontra a matriz A (Proposição 2.1.2), e consequentemente podemos explicitar a matriz de rotação. Calculamos também a distância produto mínima dos reticulados obtidos e comparamos com outras construções.

4.1 Matriz mudança de base - Algoritmo de busca

Vimos pela Proposição 2.1.2 que um reticulado Λ_1 é uma versão rotacionada de um reticulado Λ_2 se, e somente se,

$$G_1 = AG_2A^t,$$

onde a matriz A é uma matriz com entradas inteiras e determinante ± 1 (matriz mudança de base), e G_1, G_2 são as matrizes de Gram de Λ_1 e Λ_2 , respectivamente. Implementamos o Algoritmo 4.1 que encontra a matriz A , e os itens abaixo detalham o método:

1. Fixamos que as entradas da matriz A podem assumir os valores $-1, 0$ ou 1 , com o intuito de tornar o algoritmo menos complexo.
2. O reticulado algébrico Λ_2 possui matriz geradora M_2 (com matriz de Gram G_2), e acredita-se que Λ_2 é uma versão rotacionada do reticulado Λ_1 (com matriz de Gram $G_1 = (g_{ij})_{i,j=1}^n$).
3. O algoritmo inicia-se buscando por um vetor $\mathbf{a}_1 = (a_{11}, a_{12}, \dots, a_{1n})$ onde $a_{1j} \in \{-1, 0, 1\}$, $j = 1, 2, \dots, n$ (totalizando 3^n possibilidades), de modo que $\mathbf{w}_1 = \mathbf{a}_1 M_2$ satisfaz $\langle \mathbf{w}_1, \mathbf{w}_1 \rangle = g_{11}$. A primeira n -upla $(a_{11}, a_{12}, \dots, a_{1n})$ satisfazendo a condição, fixa $\mathbf{a}_1$ como sendo a primeira linha da matriz A .
4. Para o passo seguinte, buscamos por um vetor $\mathbf{a}_2 = (a_{21}, a_{22}, \dots, a_{2n})$ onde $a_{2j} \in \{-1, 0, 1\}$ (totalizando 3^n possibilidades) de modo que $\mathbf{w}_2 = \mathbf{a}_2 M_2$ e $\mathbf{w}_1$ obtido no passo anterior satisfazem $\langle \mathbf{w}_2, \mathbf{w}_1 \rangle = g_{21}$ e $\langle \mathbf{w}_2, \mathbf{w}_2 \rangle = g_{22}$. A primeira

n -upla satisfazendo as condições anteriores fixam $\mathbf{a}_2$ como sendo a segunda linha da matriz A .

5. O processo se repete até que o vetor $\mathbf{a}_{n-2} = (a_{n-2,1}, a_{n-2,2}, \dots, a_{n-2,n})$ seja fixado, ou seja, $\mathbf{w}_{n-2} = \mathbf{a}_{n-2}M$ e $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_{n-3}$ obtidos nos passos anteriores satisfazem $\langle \mathbf{w}_{n-2}, \mathbf{w}_1 \rangle = g_{n-2,1}, \langle \mathbf{w}_{n-2}, \mathbf{w}_2 \rangle = g_{n-2,2}, \dots, \langle \mathbf{w}_{n-2}, \mathbf{w}_{n-2} \rangle = g_{n-2,n-2}$.
6. A busca pelos vetores $\mathbf{a}_{n-1} = (a_{n-1,1}, a_{n-1,2}, \dots, a_{n-1,n})$ e $\mathbf{a}_n = (a_{n1}, a_{n2}, \dots, a_{nn})$ é feita na mesma rotina, pois se $A = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{n-1}, \mathbf{a}_n)$, temos que exigir que $\det(A) = \pm 1$. Desta forma temos mais liberdade para que isto aconteça (3^{2n} possibilidades de combinação entre os números $-1, 0$ e 1), pois quando $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{n-2}$ foram fixados nada foi exigido em relação ao determinante da matriz A .
7. Fixados $\mathbf{a}_{n-1}$ e $\mathbf{a}_n$, o algoritmo mostra como saída a matriz $A = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{n-1}, \mathbf{a}_n)$, que possui entradas inteiras e determinante ± 1 e em seguida aborta o processo de busca.

Observação 4.1.1. *Com relação ao Algoritmo 4.1 nota-se:*

1. *Se os vetores $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ fossem fixados na mesma rotina, o algoritmo seria ineficiente, pois seriam 3^{n^2} combinações possíveis para as entradas da matriz, e para cada combinação diferente seria pequena a probabilidade de que $\langle \mathbf{w}_i, \mathbf{w}_j \rangle = g_{ij}$, para $i = 1, 2, \dots, n, j \leq i$, isto sem contar as outras operações que o algoritmo efetua para cada combinação.*
2. *Apesar do exposto no item anterior, a eficiência se mantém se a dimensão n não for alta, pois as 3^n possibilidades de combinações para as entradas de cada vetor é um número grande se n for grande.*

$M = (m_{ij})_{i,j=1}^n$: Matriz geradora do reticulado algebrico, onde

$$m_k = \{m_{k1}, \dots, m_{kn}\}, \quad k = 1, 2, \dots, n :$$

$G = (g_{ij})_{i,j=1}^n$: Matriz de Gram do reticulado Λ ;

inicio

```

para  $a_{1j} = -1$  até  $1$  ( $j = 1, 2, \dots, n$ ) faça
     $w_1 = \sum_{i=1}^n a_{1i} m_i$ ;  $h_{11} = \langle w_1, w_1 \rangle$ ;
    se  $h_{11} = g_{11}$  então
        para  $a_{2j} = -1$  até  $1$  ( $j = 1, 2, \dots, n$ ) faça
             $w_2 = \sum_{i=1}^n a_{2i} m_i$ ;  $h_{21} = \langle w_2, w_1 \rangle$ ;  $h_{22} = \langle w_2, w_2 \rangle$ ;
            se  $h_{21} = g_{21}$  e  $h_{22} = g_{22}$  então
                 $\vdots$ 
                 $\vdots$ 
                 $\vdots$ 
                para  $a_{(n-1),j} = -1$  até  $1$  ( $j = 1, 2, \dots, n$ ) faça
                    para  $a_{nj} = -1$  até  $1$  ( $j = 1, 2, \dots, n$ ) faça
                         $w_{n-1} = \sum_{i=1}^n a_{(n-1),i} m_i$ ;
                         $h_{(n-1),1} = \langle w_{n-1}, w_1 \rangle; \dots h_{(n-1),n} = \langle w_{n-1}, w_n \rangle$ ;
                         $w_n = \sum_{i=1}^n a_{ni} m_i$ ;  $h_{n1} = \langle w_n, w_1 \rangle; \dots h_{nn} = \langle w_n, w_n \rangle$ ;
                        se  $h_{(n-1),1} = g_{(n-1),1}$  e  $\dots$  e  $h_{(n-1),n} = g_{(n-1),n}$  e
                        e  $h_{n1} = g_{n1}$  e  $\dots$  e  $h_{nn} = g_{nn}$  então
                             $A = (a_{ij})_{i,j=1}^n$ ;
                            se  $\det(A) = \pm 1$  então
                                Imprima: A;
                                Abortar;
                            fim
                        fim
                    fim
                fim
            fim
        fim
    fim
fim

```

Algoritmo 4.1: Algoritmo de busca da matriz A

4.2 Reticulados rotacionados - condições de existência

Sejam $\mathbb{K}$ um corpo de números totalmente real de grau n , $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ um ideal de $\mathcal{O}_{\mathbb{K}}$ e α um elemento totalmente real e positivo de $\mathbb{K}$. A fim de que o reticulado $(\mathcal{A}, b_\alpha)$ seja uma versão escalonada e rotacionada de um reticulado Λ , deduzimos três condições necessárias (mas não suficientes):

1. Uma versão escalonada de Λ é da forma $\sqrt{c}M$, onde c é um inteiro e M é uma matriz geradora de Λ , tal que seu determinante é dado por

$$\det(G) = \det[(\sqrt{c}M)(\sqrt{c}M)^T] = \det[\sqrt{c}M]^2 = c^n \det[M]^2 = c^n \det(\Lambda),$$

assim pela Proposição 3.2.1 segue que

$$|d_{\mathbb{K}}| \mathcal{N}(\mathcal{A})^2 \mathcal{N}(\alpha) = c^n \det(\Lambda). \quad (4.2.1)$$

2. Uma versão escalonada do reticulado Λ possui a mesma densidade de centro de Λ , assim pela Proposição 3.3.3 segue que

$$\frac{1}{2^n [|d_{\mathbb{K}}| \mathcal{N}(\alpha)]^{1/2}} \cdot \frac{t_\alpha^{n/2}}{|\mathcal{N}(\mathcal{A})|} = \delta(\Lambda), \quad (4.2.2)$$

onde $\delta(\Lambda)$ denota a densidade de centro do reticulado Λ .

3. Como $\Lambda_1 = (\mathcal{A}, b_\alpha)$ é uma versão escalonada de Λ com fator de escala $\sqrt{c}$, segue que o raio de empacotamento $\rho(\Lambda_1)$ é dado por $\sqrt{c}\rho(\Lambda)$, onde $\rho(\Lambda)$ é o raio de empacotamento de Λ . Pelo Corolário 3.3.3 e Proposição 3.3.3 temos que $\rho(\Lambda_1) = \sqrt{t_\alpha}/2$, assim

$$t_\alpha = 4c\rho(\Lambda)^2. \quad (4.2.3)$$

As três condições acima servem como requisito inicial para a construção de versões rotacionadas de reticulados conhecidos. A seguir apresentamos a construção de alguns reticulados densos conhecidos definidos na seção anterior.

4.2.1 Reticulado A_2

A fim de que um reticulado $(\mathcal{A}, b_\alpha)$ seja uma versão escalonada e rotacionada do reticulado $\Lambda = A_2$ com fator de escala $\sqrt{c}$, as condições expressas pela Equações (4.2.1), (4.2.2) e (4.2.3) são dadas respectivamente por

$$|d_{\mathbb{K}}|N(\mathcal{A})^2N(\alpha) = 3c^2. \quad (4.2.4)$$

$$\frac{1}{2^n [|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2} \cdot |\mathcal{N}(\mathcal{A})|} = \frac{1}{2\sqrt{3}}. \quad (4.2.5)$$

$$t_\alpha = 2c. \quad (4.2.6)$$

Construção

Se considerarmos o corpo ciclotômico $\mathbb{Q}(\zeta_{12})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$ o seu subcorpo maximal real, temos que $n = [\mathbb{K} : \mathbb{Q}] = 2$ e $d_{\mathbb{K}} = 12$. As equações (4.2.4), (4.2.5) e (4.2.6) relacionam os parâmetros $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathcal{A})$, c e t_α , e a Tabela 4.1 contempla alguns valores para estes parâmetros que satisfazem as três equações.

$\mathcal{N}(\alpha)$	$\mathcal{N}(\mathcal{A})$	c	t_α
1	2	4	8
1	6	12	24
4	1	4	8
4	5	20	40
9	4	24	48
16	4	32	64

Tabela 4.1: Parâmetros do reticulado ideal rotacionado de A_2

Agora, tomando a base $\{e_0 = 1, e_1 = \zeta_{12} + \zeta_{12}^{-1}\}$ de $\mathcal{O}_{\mathbb{K}}$, o objetivo é escolher um α totalmente real e totalmente positivo e um ideal $\mathcal{A}$ que satisfaçam algum dos casos da

tabela. Depois de analisar os casos, percebemos que se escolhermos $\alpha = 1$ e $\mathcal{A} = \mathfrak{a}\mathcal{O}_{\mathbb{K}}$, onde $\mathfrak{a} = 3 + (\zeta_{12} + \zeta_{12}^{-1})$, temos $\mathcal{N}(\alpha) = 1$, $\mathcal{N}(\mathcal{A}) = 6$ e $t_{\alpha} = 24$ e consequentemente $c = 12$, satisfazendo a Equação (4.2.5), ou seja, o reticulado ideal $\Lambda = (\mathcal{A}, b_{\alpha})$, possui a mesma densidade de centro do reticulado A_2 . Como o reticulado A_2 é o único reticulado com esta densidade de centro na dimensão 2, concluímos que $(\mathcal{A}, b_{\alpha})$ é uma versão escalonada e rotacionada de A_2 .

A proposição a seguir tem por objetivo facilitar o cálculo da distância produto mínima não somente do reticulado A_2 como dos outros reticulados que serão construídos nesta seção.

Proposição 4.2.1. *Sejam Λ_1 e Λ_2 reticulados de dimensão n com normas mínimas η_1 e η_2 , respectivamente. Se Λ_1 é uma versão escalonada de Λ_2 com fator de escala $\sqrt{c}$, então*

$$\det(\Lambda_1) = c^n \det(\Lambda_2)$$

$$\eta_1 = c \eta_2$$

Demonstração: Sejam M_1 e M_2 matrizes geradores de Λ_1 e Λ_2 , respectivamente, com matrizes de Gram $G_1 = M_1 M_1^t$ e $G_2 = M_2 M_2^t$. Temos que

$$\begin{aligned} \det(\Lambda_1) &= \det(G_1) = \det(M_1 M_1^t) = \det((\sqrt{c} M_2)(\sqrt{c} M_2)^t) = \\ &= \det(c M_2 M_2^t) = \det(c G_2) = c^n \det(G_2) = c^n \det(\Lambda_2). \end{aligned}$$

Agora, se η_1 e η_2 são as normas mínimas de Λ_1 e Λ_2 , respectivamente, então $\eta_2 = \min\{\|x\|^2; x \in \Lambda_2, x \neq 0\}$ e como Λ_1 é uma versão escalonada de Λ_2 com fator de escala $\sqrt{c}$, então

$$\begin{aligned} \eta_1 &= \min\{\|\sqrt{c}x\|^2; x \in \Lambda_2, x \neq 0\} = \min\{c\|x\|^2; x \in \Lambda_2, x \neq 0\} = \\ &= c \min\{\|x\|^2; x \in \Lambda_2, x \neq 0\} = c \eta_2. \end{aligned}$$

o que conclui a demonstração. □

Distância produto mínima

Vimos que Λ é uma versão escalonada e rotacionada do reticulado A_2 com fator de escala $\sqrt{12}$, assim pela Proposição 4.2.1 temos que

$$\det(\Lambda) = 12^2 \det(A_2) = 144 \cdot 3 = 432$$

e

$$\eta_1 = 12 \quad \eta_2 = 12 \cdot 2 = 24$$

onde η_1 e η_2 são as normas mínimas de Λ e A_2 , respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt{d_{p,min}(\Lambda)} = \frac{1}{\sqrt{24}} \sqrt[4]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{24}} \sqrt[4]{\frac{432}{12}} = 0.5$$

4.2.2 Reticulado D_4

A fim de que um reticulado $(\mathcal{A}, b_\alpha)$ seja uma versão escalonada e rotacionada do reticulado $\Lambda = D_4$ com fator de escala $\sqrt{c}$, as condições expressas pela Equações (4.2.1), (4.2.2) e (4.2.3) são dadas respectivamente por

$$|d_{\mathbb{K}}| N(\mathcal{A})^2 N(\alpha) = 4c^4. \quad (4.2.7)$$

$$\frac{1}{2^n [|d_{\mathbb{K}}| \mathcal{N}(\alpha)]^{1/2}} \cdot \frac{t_\alpha^{n/2}}{|\mathcal{N}(\mathcal{A})|} = \frac{1}{8}. \quad (4.2.8)$$

$$t_\alpha = 2c. \quad (4.2.9)$$

Construção

Se considerarmos o corpo ciclotômico $\mathbb{Q}(\zeta_{16})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ o seu subcorpo maximal real, temos que $n = [\mathbb{K} : \mathbb{Q}] = 4$ e $d_{\mathbb{K}} = 2^{11}$. As equações (4.2.7), (4.2.8) e (4.2.9) relacionam os parâmetros $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathcal{A})$, c e t_α , e a Tabela 4.2 contempla alguns valores para estes parâmetros que satisfazem as três equações.

$\mathcal{N}(\alpha)$	$\mathcal{N}(\mathcal{A})$	c	t_α
2	2	8	16
2	8	16	32
8	1	8	16
8	4	16	32
8	9	24	48
18	6	24	48
18	24	48	96
32	2	16	32
32	8	32	64
50	10	40	80

Tabela 4.2: Parâmetros do reticulado ideal rotacionado de D_4

Agora, tomando a base $\{e_0 = 1, e_1 = \zeta_{16} + \zeta_{16}^{-1}, e_2 = \zeta_{16}^2 + \zeta_{16}^{-2}, e_3 = \zeta_{16}^3 + \zeta_{16}^{-3}\}$ de $\mathcal{O}_{\mathbb{K}}$, o objetivo é escolher um α totalmente real e totalmente positivo e um ideal $\mathcal{A}$ que satisfaçam algum dos casos da tabela. Depois de analisar os casos, percebemos que se escolhermos $\alpha = 4 + (\zeta_{16} + \zeta_{16}^{-1}) - 2(\zeta_{16}^2 + \zeta_{16}^{-2}) - (\zeta_{16}^3 + \zeta_{16}^{-3})$ e $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$, teremos $\mathcal{N}(\alpha) = 8$, $\mathcal{N}(\mathcal{A}) = 1$, $t_\alpha = 16$ e consequentemente $c = 8$, satisfazendo a Equação (4.2.8), ou seja, o reticulado ideal $\Lambda = (\mathcal{A}, b_\alpha)$, possui a mesma densidade de centro do reticulado D_4 . Como o reticulado D_4 é o único reticulado com esta densidade de centro na dimensão 4, concluímos que $(\mathcal{A}, b_\alpha)$ é uma versão escalonada e rotacionada de D_4 .

Distância produto mínima

Vimos que Λ é uma versão escalonada e rotacionada do reticulado D_4 com fator de escala $\sqrt{8}$, assim pela Proposição 4.2.1 temos que

$$\det(\Lambda) = 8^4 \det(D_4) = 4096 \cdot 4 = 16384$$

e

$$\eta_1 = 8 \quad \eta_2 = 8.2 = 16$$

onde η_1 e η_2 são as normas mínimas de Λ e D_4 , respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt[4]{d_{p,min}(\Lambda)} = \frac{1}{\sqrt{16}} \sqrt[8]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{16}} \sqrt[8]{\frac{16384}{2^{11}}} = 0.32421$$

4.2.3 Reticulado E_6

A fim de que um reticulado $(\mathcal{A}, b_\alpha)$ seja uma versão escalonada e rotacionada do reticulado $\Lambda = E_6$ com fator de escala $\sqrt{c}$, as condições expressas pela Equações (4.2.1), (4.2.2) e (4.2.3) são dadas respectivamente por

$$|d_{\mathbb{K}}|N(\mathcal{A})^2N(\alpha) = 3c^6. \quad (4.2.10)$$

$$\frac{1}{2^n [|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2}} \cdot \frac{t_\alpha^{n/2}}{|\mathcal{N}(\mathcal{A})|} = \frac{1}{8\sqrt{3}}. \quad (4.2.11)$$

$$t_\alpha = 2c. \quad (4.2.12)$$

Construção

Se considerarmos o corpo ciclotômico $\mathbb{Q}(\zeta_{36})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{36} + \zeta_{36}^{-1})$ o seu subcorpo maximal real, temos que $n = [\mathbb{K} : \mathbb{Q}] = 6$ e $d_{\mathbb{K}} = 2^6 3^9$. Alguns valores para $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathcal{A})$, c e t_α que satisfazem as Equações (4.2.10), (4.2.11) e (4.2.12) são listados na Tabela 4.3.

Agora, tomando a base $\{e_0 = 1, e_1 = \zeta_{36} + \zeta_{36}^{-1}, \dots, e_5 = \zeta_{36}^5 + \zeta_{36}^{-5}\}$ de $\mathcal{O}_{\mathbb{K}}$, o objetivo é escolher um α totalmente real e totalmente positivo e um ideal $\mathcal{A}$ que satisfaçam algum dos casos da tabela. Depois de analisar os casos, percebemos que se escolhermos $\alpha = 2 + (\zeta_{36}^2 + \zeta_{36}^{-2})$ e $\mathcal{A} = \mathfrak{a}\mathcal{O}_{\mathbb{K}}$, com $\mathfrak{a} = -2 - 2(\zeta_{36} + \zeta_{36}^{-1}) - 2(\zeta_{36}^2 + \zeta_{36}^{-2}) - 2(\zeta_{36}^3 + \zeta_{36}^{-3}) - (\zeta_{36}^4 + \zeta_{36}^{-4}) - (\zeta_{36}^5 + \zeta_{36}^{-5})$, temos $\mathcal{N}(\alpha) = 9$, $\mathcal{N}(\mathcal{A}) = 24$, $t_\alpha = 72$ e consequentemente $c = 36$, satisfazendo a Equação (4.2.11), ou seja, o reticulado ideal $\Lambda = (\mathcal{A}, b_\alpha)$, possui a mesma densidade de centro do

$\mathcal{N}(\alpha)$	$\mathcal{N}(\mathcal{A})$	c	t_α
1	9	18	36
1	72	36	72
4	36	36	72
9	3	18	36
9	24	36	72
16	18	36	72
36	12	36	72
64	9	36	72
81	1	18	36
81	8	36	72

Tabela 4.3: Parâmetros do reticulado ideal rotacionado de E_6

reticulado E_6 . Como o reticulado E_6 é o único reticulado com esta densidade de centro na dimensão 6, concluímos que $(\mathcal{A}, b_\alpha)$ é uma versão escalonada e rotacionada de E_6 .

Distância produto mínima

Vimos que Λ é uma versão escalonada e rotacionada do reticulado E_6 com fator de escala $\sqrt{36}$, assim pela Proposição 4.2.1 temos que

$$\det(\Lambda) = 36^6 \det(E_6) = 2^{12} \cdot 3^{12} \cdot 3 = 2^{12} \cdot 3^{13}$$

e

$$\eta_1 = 36 \quad \eta_2 = 36 \cdot 2 = 72$$

onde η_1 e η_2 são as normas mínimas de Λ e E_6 , respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt[6]{d_{p,\min}(\Lambda)} = \frac{1}{\sqrt{72}} \sqrt[12]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{72}} \sqrt[12]{\frac{2^{12} \cdot 3^{13}}{2^6 3^9}} = 0.240375$$

4.2.4 Reticulado E_8

A fim de que um reticulado $(\mathcal{A}, b_\alpha)$ seja uma versão escalonada e rotacionada do reticulado $\Lambda = E_8$ com fator de escala $\sqrt{c}$, as condições expressas pela Equações (4.2.1), (4.2.2) e (4.2.3) são dadas respectivamente por

$$|d_{\mathbb{K}}|N(\mathcal{A})^2N(\alpha) = c^8. \quad (4.2.13)$$

$$\frac{1}{2^n [|d_{\mathbb{K}}|\mathcal{N}(\alpha)]^{1/2} \cdot |\mathcal{N}(\mathcal{A})|} = \frac{1}{16}. \quad (4.2.14)$$

$$t_\alpha = 2c. \quad (4.2.15)$$

Construção

Se considerarmos o corpo ciclotômico $\mathbb{Q}(\zeta_{60})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$ o seu subcorpo maximal real, temos que $n = [\mathbb{K} : \mathbb{Q}] = 8$ e $d_{\mathbb{K}} = 2^8 3^4 5^6$. Alguns valores para $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathcal{A})$, c e t_α que satisfazem as Equações (4.2.13), (4.2.14) e (4.2.15) são listados na Tabela 4.4.

$\mathcal{N}(\alpha)$	$\mathcal{N}(\mathcal{A})$	c	t_α
1	45	30	60
9	15	30	60
16	180	60	120
25	9	30	60
36	120	60	120
64	90	60	120
81	5	30	60
100	72	60	120
144	60	60	120
2025	16	60	120

Tabela 4.4: Parâmetros do reticulado ideal rotacionado de E_8

Agora, tomando a base $\{e_0 = 1, e_1 = \zeta_{60} + \zeta_{60}^{-1}, \dots, e_7 = \zeta_{60}^7 + \zeta_{60}^{-7}\}$ de $\mathcal{O}_{\mathbb{K}}$, o objetivo é escolher um α totalmente real e totalmente positivo e um ideal $\mathcal{A}$ que satisfaçam algum dos casos da tabela. Depois de analisar os casos, percebemos que se escolhermos $\alpha = 2 - 2(\zeta_{60}^2 + \zeta_{60}^{-2}) - (\zeta_{60}^4 + \zeta_{60}^{-4}) + 3(\zeta_{60}^6 + \zeta_{60}^{-6})$ e $\mathcal{A} = \mathfrak{a}\mathcal{O}_{\mathbb{K}}$, com $\mathfrak{a} = -2 - (\zeta_{60} + \zeta_{60}^{-1}) - (\zeta_{60}^2 + \zeta_{60}^{-2}) - (\zeta_{60}^4 + \zeta_{60}^{-4}) + (\zeta_{60}^5 + \zeta_{60}^{-5}) + 2(\zeta_{60}^6 + \zeta_{60}^{-6}) + (\zeta_{60}^7 + \zeta_{60}^{-7})$, temos $\mathcal{N}(\alpha) = 2025$, $\mathcal{N}(\mathcal{A}) = 16$, $t_\alpha = 120$ e consequentemente $c = 60$, satisfazendo a Equação (4.2.14), ou seja, o reticulado ideal $\Lambda = (\mathcal{A}, b_\alpha)$, possui a mesma densidade de centro do reticulado E_8 . Como o reticulado E_8 é o único reticulado com esta densidade de centro na dimensão 8, concluímos que $(\mathcal{A}, b_\alpha)$ é uma versão escalonada e rotacionada de E_8 .

Distância produto mínima

Vimos que Λ é uma versão escalonada e rotacionada do reticulado E_8 com fator de escala $\sqrt{60}$, assim pela Proposição 4.2.1 temos que

$$\det(\Lambda) = 60^8 \det(E_8) = 2^{16} 3^8 5^8 1 = 2^{16} 3^8 5^8$$

e

$$\eta_1 = 60 \quad \eta_2 = 60.2 = 120$$

onde η_1 e η_2 são as normas mínimas de Λ e E_8 , respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt[8]{d_{p,min}(\Lambda)} = \frac{1}{\sqrt{120}} \sqrt[16]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{120}} \sqrt[16]{\frac{2^{16} 3^8 5^8}{2^8 3^4 5^6}} = 0.207766$$

4.2.5 Reticulado K_{12}

A fim de que um reticulado $(\mathcal{A}, b_\alpha)$ seja uma versão escalonada e rotacionada do reticulado $\Lambda = K_{12}$ com fator de escala $\sqrt{c}$, as condições expressas pela Equações (4.2.1), (4.2.2) e (4.2.3) são dadas respectivamente por

$$|d_{\mathbb{K}}| N(\mathcal{A})^2 N(\alpha) = 729c^{12}. \quad (4.2.16)$$

$$\frac{1}{2^n [|d_{\mathbb{K}}| \mathcal{N}(\alpha)]^{1/2}} \cdot \frac{t_\alpha^{n/2}}{|\mathcal{N}(\mathcal{A})|} = \frac{1}{27}. \quad (4.2.17)$$

$$t_\alpha = 4c. \quad (4.2.18)$$

Construção

Se considerarmos o corpo ciclotômico $\mathbb{Q}(\zeta_{84})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{84} + \zeta_{84}^{-1})$ o seu subcorpo maximal real, temos que $n = [\mathbb{K} : \mathbb{Q}] = 12$ e $d_{\mathbb{K}} = 2^{12} 3^6 7^{10}$. Alguns valores para $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathcal{A})$, c e t_α que satisfazem as Equações (4.2.16), (4.2.17) e (4.2.18) são listados na Tabela 4.5.

$\mathcal{N}(\alpha)$	$\mathcal{N}(\mathcal{A})$	c	t_α
1	7	14	56
4	224	28	112
16	112	28	112
49	1	14	56
49	64	28	112
64	56	28	112
196	32	28	112
256	28	28	112

Tabela 4.5: Parâmetros do reticulado ideal rotacionado de K_{12}

Agora, tomando a base $\{e_0 = 1, e_1 = \zeta_{84} + \zeta_{84}^{-1}, \dots, e_{11} = \zeta_{84}^{11} + \zeta_{84}^{-11}\}$ de $\mathcal{O}_{\mathbb{K}}$, o objetivo é escolher um α totalmente real e totalmente positivo e um ideal $\mathcal{A}$ que satisfaçam algum dos casos da tabela. Depois de analisar os casos, percebemos que se escolhermos $\alpha = 3 - 2(\zeta_{84}^4 + \zeta_{84}^{-4}) - (\zeta_{84}^6 + \zeta_{84}^{-6}) + (\zeta_{84}^8 + \zeta_{84}^{-8}) + (\zeta_{84}^{10} + \zeta_{84}^{-10})$ e $\mathcal{A} = \mathfrak{a}\mathcal{O}_{\mathbb{K}}$, com $\mathfrak{a} = -1 - (\zeta_{84} + \zeta_{84}^{-1}) - (\zeta_{84}^2 + \zeta_{84}^{-2}) - (\zeta_{84}^3 + \zeta_{84}^{-3}) - (\zeta_{84}^4 + \zeta_{84}^{-4}) - (\zeta_{84}^5 + \zeta_{84}^{-5}) - (\zeta_{84}^6 + \zeta_{84}^{-6}) - (\zeta_{84}^7 + \zeta_{84}^{-7}) - (\zeta_{84}^8 + \zeta_{84}^{-8}) - (\zeta_{84}^9 + \zeta_{84}^{-9}) - (\zeta_{84}^{10} + \zeta_{84}^{-10})$, teremos $\mathcal{N}(\alpha) = 49$, $\mathcal{N}(\mathcal{A}) = 64$ e $t_\alpha = 112$ satisfazendo a Equação (4.2.17), ou seja, o reticulado ideal $\Lambda = (\mathcal{A}, b_\alpha)$, possui a mesma densidade de centro do reticulado K_{12} . Assim, se fixarmos $c = 28$ teremos as três condições

(necessárias) satisfeitas, e agora vamos provar que o reticulado $\Lambda = (\mathcal{A}, b_\alpha)$ é uma versão escalonada e rotacionada do K_{12} , explicitando a matriz de rotação.

Seja $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_{12}\}$ o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$. Então o reticulado $\Lambda = (\mathcal{A}, b_\alpha)$ tem a 12×12 matriz geradora dada por

$$Q = \begin{pmatrix} \sigma_1(\mathfrak{a}e_0) & \sigma_2(\mathfrak{a}e_0) & \cdots & \sigma_{12}(\mathfrak{a}e_0) \\ \sigma_1(\mathfrak{a}e_1) & \sigma_2(\mathfrak{a}e_1) & \cdots & \sigma_{12}(\mathfrak{a}e_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\mathfrak{a}e_{11}) & \sigma_2(\mathfrak{a}e_{11}) & \cdots & \sigma_{12}(\mathfrak{a}e_{11}) \end{pmatrix}.$$

O elemento rotacionado pode ser representado pela matriz diagonal

$$D = diag(\sqrt{\sigma_k(\alpha)})_{k=1}^{12}$$

Assim, tomando $\hat{M} = QD$ e efetuando os cálculos, a matriz $\hat{M}$ (geradora do reticulado ideal Λ) é dada por

$$\begin{pmatrix} -13.2963 & 2.1445 & -4.9037 & 2.3289 & -1.5086 & -1.3379 & 1.1513 & -1.1134 & 1.2308 & 2.1394 & 0.4057 & -0.4975 \\ -26.5184 & 3.9926 & -6.6707 & 2.6239 & -0.8893 & -0.3988 & -0.3432 & 0.6563 & -1.3867 & -2.9104 & -0.7554 & 0.9922 \\ -26.2957 & 3.1441 & 0.7329 & -1.7017 & 2.4930 & 2.5569 & -2.2004 & 1.8399 & -0.8993 & -0.3197 & 0.5949 & -0.9839 \\ -25.9260 & 1.8609 & 7.6677 & -4.5411 & 2.3590 & 1.1610 & 0.9991 & -1.7410 & 2.4000 & 3.3454 & -0.3521 & 0.9700 \\ -25.4113 & 0.3205 & 9.6979 & -3.4145 & -1.1023 & -2.2108 & 1.9026 & -0.8135 & -1.8046 & -4.2311 & 0.0606 & -0.9508 \\ -24.7545 & -1.2642 & 5.5247 & 0.6942 & -3.0088 & -1.8200 & -1.5662 & 2.2206 & -0.3669 & 2.4104 & 0.2392 & 0.9262 \\ -23.9592 & -2.6742 & -2.1823 & 4.1963 & -0.6714 & 1.6683 & -1.4357 & -0.4955 & 2.2179 & 0.9521 & -0.5059 & -0.8964 \\ -23.0300 & -3.7144 & -8.4935 & 4.0338 & 2.6130 & 2.3173 & 1.9942 & -1.9285 & -2.1319 & -3.7056 & 0.7028 & 0.8617 \\ -21.9719 & -4.2412 & -9.3717 & 0.3480 & 2.2118 & -0.9775 & 0.8412 & 1.6324 & 0.1839 & 4.0888 & -0.8024 & -0.8221 \\ -20.7910 & -4.1815 & -4.2552 & -3.6417 & -1.3091 & -2.6087 & -2.2450 & 0.9662 & 1.9247 & -1.8565 & 0.7911 & 0.7779 \\ -19.4938 & -3.5438 & 3.5830 & -4.4509 & -2.9835 & 0.1999 & -0.1720 & -2.2019 & -2.3524 & -1.5632 & -0.6705 & -0.7294 \\ -18.0876 & -2.4161 & 9.1295 & -1.3729 & -0.4497 & 2.6683 & 2.2963 & 0.3318 & 0.7256 & 3.9831 & 0.4571 & 0.6767 \end{pmatrix}.$$

Nossa tarefa agora é mostrar que o reticulado ideal Λ com matriz geradora $\hat{M}$ é uma versão escalonada e rotacionada do reticulado K_{12} . Se fizermos a redução de base pelo método de redução de Minkowski [41] obtemos a matriz mudança de base

$$A_1 = \begin{pmatrix} -3 & 4 & -2 & 0 & 0 & -2 & 1 & -2 & 1 & 0 & 0 & 2 \\ -2 & 2 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -2 & 2 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -2 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 2 & -2 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -2 & 2 & -1 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 \\ 2 & -2 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -2 & 1 & 1 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & -2 \\ 2 & -2 & 2 & -1 & -1 & 1 & -1 & 1 & -1 & 0 & 1 & 0 \\ -1 & 2 & -1 & 0 & 0 & -2 & 1 & -1 & 0 & 1 & -1 & 2 \\ -2 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Assim, a base reduzida de Minkowski $M = A_1 \hat{M}$ é dada por

$$\begin{pmatrix} -0.1305 & 1.4582 & -0.7952 & -0.7451 & -2.5849 & 2.3374 & 2.7161 & 3.5024 & 1.4099 & -1.8227 & -7.7071 & 3.4884 \\ 0.2214 & -0.7311 & 2.6678 & -0.5477 & -1.3884 & -2.0747 & 2.4108 & -1.8812 & -1.0364 & -6.1148 & -3.8643 & 5.9174 \\ 0.2932 & -0.8092 & -0.6377 & 1.6744 & -2.0729 & -1.2971 & -1.5073 & 2.8087 & -3.1682 & -1.4617 & 4.2771 & -7.8383 \\ 0.6630 & -2.0924 & 6.2971 & -1.1649 & -2.2069 & -2.6931 & 1.6922 & -0.7722 & 0.1312 & 2.2034 & 3.3301 & -5.8843 \\ 0.8782 & -2.3159 & -1.5053 & 3.5609 & -3.2949 & -1.6838 & -1.0580 & 1.1529 & 0.4012 & 0.5267 & -3.6858 & 7.7945 \\ -0.0874 & 1.1008 & -1.2719 & -3.1173 & 2.3354 & -0.7647 & 0.8886 & 3.1644 & -5.8983 & 2.9152 & 5.8183 & -2.3364 \\ 1.0775 & -1.5922 & -2.0441 & -2.4543 & 4.5389 & 1.3277 & 4.2187 & -3.1327 & -0.0140 & 5.1222 & 4.1261 & -2.2052 \\ -0.1312 & 1.6922 & -2.2069 & -5.8843 & 6.2971 & -3.3301 & -2.0924 & -2.2034 & -0.6630 & 0.7722 & 2.6931 & -1.1649 \\ 3.8427 & -1.1964 & -0.1973 & -0.3053 & -2.4290 & 4.2921 & -3.4631 & -0.3519 & -4.4121 & 2.4464 & 5.3836 & -2.1894 \\ -2.3374 & 0.7952 & -3.4884 & 1.4582 & 0.7451 & 3.5024 & 2.5849 & 1.4099 & 7.7071 & -0.1305 & -1.8227 & 2.7161 \\ 1.2579 & 1.6796 & 1.2794 & 5.3696 & 1.2794 & 1.7896 & 1.6796 & 4.2336 & -1.2579 & -4.2336 & -1.7896 & 5.3696 \\ -0.1470 & 0.4346 & 0.4688 & -1.4862 & 3.5163 & 4.3517 & -5.0568 & 4.7645 & -2.8120 & -1.0745 & 2.2973 & -3.9301 \end{pmatrix}.$$

Como queremos que o reticulado Λ seja uma versão escalonada do reticulado K_{12} , segue que a matriz geradora $\hat{Q} = \frac{1}{\sqrt{28}}M$ de Λ (sem o fator de escala $\frac{1}{\sqrt{28}}$) é dada por

$$\begin{pmatrix} -0.0246 & 0.2755 & -0.1502 & -0.1408 & -0.4885 & 0.4417 & 0.5133 & 0.6618 & 0.2664 & -0.3444 & -1.4565 & 0.6592 \\ 0.0418 & -0.1381 & 0.5041 & -0.1035 & -0.2623 & -0.3920 & 0.4556 & -0.3555 & -0.1958 & -1.1555 & -0.7302 & 1.1182 \\ 0.0554 & -0.1529 & -0.1205 & 0.3164 & -0.3917 & -0.2451 & -0.2848 & 0.5307 & -0.5987 & -0.2762 & 0.8082 & -1.4813 \\ 0.1252 & -0.3954 & 1.1900 & -0.2201 & -0.4170 & -0.5089 & 0.3197 & -0.1459 & 0.0248 & 0.4164 & 0.6293 & -1.1120 \\ 0.1659 & -0.4376 & -0.2844 & 0.6729 & -0.6226 & -0.3182 & -0.1999 & 0.2178 & 0.0758 & 0.0995 & -0.6965 & 1.4730 \\ -0.0165 & 0.2080 & -0.2403 & -0.5891 & 0.4413 & -0.1445 & 0.1679 & 0.5980 & -1.1146 & 0.5509 & 1.0995 & -0.4415 \\ 0.2036 & -0.3009 & 0.3863 & -0.4638 & 0.8577 & 0.2509 & 0.7972 & -0.5920 & -0.0026 & 0.9680 & 0.7797 & -0.4167 \\ -0.0248 & 0.3197 & -0.4170 & -1.1120 & 1.1900 & -0.6293 & -0.3954 & -0.4164 & -0.1252 & 0.1459 & 0.5089 & -0.2201 \\ 0.7262 & -0.2261 & -0.0373 & -0.0576 & -0.4590 & 0.8111 & -0.6544 & -0.0665 & -0.8338 & 0.4623 & 1.0174 & -0.4137 \\ -0.4417 & 0.1502 & -0.6592 & 0.2755 & 0.1408 & 0.6618 & 0.4885 & 0.2664 & 1.4565 & -0.0246 & -0.3444 & 0.5133 \\ 0.2377 & 0.3174 & 0.2417 & 1.0147 & 0.2417 & 0.3382 & 0.3174 & 0.8000 & -0.2377 & -0.8000 & -0.3382 & 1.0147 \\ -0.0277 & 0.0821 & 0.0885 & -0.2808 & 0.6645 & 0.8224 & -0.9556 & 0.9004 & -0.5314 & -0.2030 & 0.4341 & -0.7427 \end{pmatrix}.$$

Seja G_2 a matriz de Gram relativa à matriz geradora $\hat{Q}$, usando o Algoritmo 4.1 obtemos uma matriz

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

tal que

$$AG_2A^t = \begin{pmatrix} 4 & 0 & 0 & 2 & -1 & -1 & 2 & 0 & 0 & 1 & 1 & 1 \\ 0 & 4 & 0 & -1 & 2 & -1 & 0 & 2 & 0 & 1 & 1 & 1 \\ 0 & 0 & 4 & -1 & -1 & 2 & 0 & 0 & 2 & 1 & 1 & 1 \\ 2 & -1 & -1 & 4 & 0 & 0 & 1 & -2 & -2 & 2 & 0 & 0 \\ -1 & 2 & -1 & 0 & 4 & 0 & -2 & 1 & -2 & 0 & 2 & 0 \\ -1 & -1 & 2 & 0 & 0 & 4 & -2 & -2 & 1 & 0 & 0 & 2 \\ 2 & 0 & 0 & 1 & -2 & -2 & 4 & 0 & 0 & 2 & -1 & -1 \\ 0 & 2 & 0 & -2 & 1 & -2 & 0 & 4 & 0 & -1 & 2 & -1 \\ 0 & 0 & 2 & -2 & -2 & 1 & 0 & 0 & 4 & -1 & -1 & 2 \\ 1 & 1 & 1 & 2 & 0 & 0 & 2 & -1 & -1 & 4 & 0 & 0 \\ 1 & 1 & 1 & 0 & 2 & 0 & -1 & 2 & -1 & 0 & 4 & 0 \\ 1 & 1 & 1 & 0 & 0 & 2 & -1 & -1 & 2 & 0 & 0 & 4 \end{pmatrix},$$

que é a matriz de Gram do reticulado K_{12} relativo à matriz geradora S dada por

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & 0 & 1 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 1 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & -\frac{\sqrt{3}}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} \end{pmatrix}.$$

Pela Proposição 2.1.2 segue que o reticulado Λ é uma versão escalonada e rotacionada do reticulado K_{12} com fator de escala $\sqrt{28}$. Portanto, uma outra matriz geradora para o reticulado

ideal (sem o fator de escala) é dada por $\hat{M} = A\hat{Q}$, e consequentemente,

$$\hat{M}\hat{M}^t = (A\hat{Q})(A\hat{Q})^t = A\hat{Q}\hat{Q}^tA^t = AG_2A^t = SS^t,$$

e assim,

$$(\hat{M}^{-1}S)(\hat{M}^{-1}S)^t = I_{12}.$$

Portanto, $R = \hat{M}^{-1}S$ é a matriz que rotacionada o reticulado ideal Λ no reticulado K_{12} .

Explicitamente, a matriz R é dada por

$$\begin{pmatrix} -0.4135 & -0.0153 & -0.3466 & -0.1225 & -0.3986 & -0.5194 & 0.0599 & -0.4110 & 0.2334 & -0.1424 & -0.1254 & 0.0419 \\ 0.4527 & -0.0613 & -0.0806 & -0.0602 & -0.4840 & 0.0160 & -0.2579 & 0.3241 & 0.5148 & 0.1381 & -0.1931 & -0.2313 \\ 0.1804 & 0.1354 & 0.1821 & -0.7406 & -0.1018 & 0.0906 & 0.1456 & -0.3103 & -0.1435 & 0.0277 & 0.2083 & -0.4079 \\ 0.4165 & -0.0878 & 0.3607 & 0.0764 & 0.3898 & -0.5157 & 0.0336 & -0.1661 & 0.2110 & -0.4041 & -0.1504 & -0.0747 \\ 0.2263 & 0.4401 & 0.0994 & 0.1582 & 0.0013 & 0.2624 & -0.0503 & -0.5963 & 0.2095 & 0.2993 & -0.2319 & 0.3252 \\ -0.0359 & -0.0982 & -0.3840 & -0.2653 & 0.4288 & 0.2015 & -0.5198 & -0.1142 & 0.3522 & -0.1958 & 0.2960 & 0.1148 \\ -0.5198 & -0.1142 & 0.3522 & -0.1958 & 0.2960 & 0.1148 & 0.0359 & 0.0982 & 0.3840 & 0.2653 & -0.4288 & -0.2015 \\ -0.0503 & -0.5963 & 0.2095 & 0.2993 & -0.2319 & 0.3252 & -0.2263 & -0.4401 & -0.0994 & -0.1582 & -0.0013 & -0.2624 \\ -0.0336 & 0.1661 & -0.2110 & 0.4041 & 0.1504 & 0.0747 & 0.4165 & -0.0878 & 0.3607 & 0.0764 & 0.3898 & -0.5157 \\ -0.1456 & 0.3103 & 0.1435 & -0.0277 & -0.2083 & 0.4079 & 0.1804 & 0.1354 & 0.1821 & -0.7406 & -0.1018 & 0.0906 \\ -0.2579 & 0.3241 & 0.5148 & 0.1381 & -0.1931 & -0.2313 & -0.4527 & 0.0613 & 0.0806 & 0.0602 & 0.4840 & -0.0160 \\ -0.0599 & 0.4110 & -0.2334 & 0.1424 & 0.1254 & -0.0419 & -0.4135 & -0.0153 & -0.3466 & -0.1225 & -0.3986 & -0.5194 \end{pmatrix}.$$

Distância produto mínima

Vimos que Λ é uma versão escalonada e rotacionada do reticulado K_{12} com fator de escala $\sqrt{28}$, assim pela Proposição 4.2.1 temos que

$$\det(\Lambda) = 28^{12} \det(K_{12}) = 2^{24} 7^{12} \cdot 729 = 2^{24} 7^{12} 3^6$$

e

$$\eta_1 = 28 \quad \eta_2 = 28.4 = 112$$

onde η_1 e η_2 são as normas mínimas de Λ e K_{12} , respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt[12]{d_{p,min}(\Lambda)} = \frac{1}{\sqrt{112}} \sqrt[24]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{112}} \sqrt[24]{\frac{2^{24}7^{12}3^6}{2^{12}3^67^{10}}} = 0.157155$$

4.3 Distância produto mínima dos reticulados densos

- Comparação

A fim de verificar a eficiência de constelações de sinais tanto para o canal Rayleigh com desvanecimento quanto para o canal gaussiano, fazemos uma comparação entre as distâncias produto mínima dos reticulados rotacionados A_2 , D_4 , E_6 , E_8 e K_{12} , calculadas nas subseções anteriores, com o reticulado $\mathbb{Z}^n$ nas respectivas dimensões, conforme tabela abaixo

n	$\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$					$\sqrt[n]{d_{p,min}(\Lambda_n)}$	
	A	B	C	D	E	F	Lim
2	0.66874	0.66874	—	0.59460	0.66874	0.50000	0.66995
4	0.43899	—	0.39763	0.38555	0.34560	0.32421	0.44163
6	0.34958	0.34344	0.34958	—	0.34344	0.24037	0.35032
8	0.29382	0.28952	—	0.26106	0.28952	0.20776	0.30093
12	—	—	0.22967	—	0.13995	0.15715	0.24807

A - Krüskemper método (Oggier [30],[31]).

B,C - Construções ciclotômica e mista, respectivamente (Bayer et al. [26]).

D - Construção via $\mathbb{Q}(\zeta_r)$ (Andrade et al. [4]).

E - Construção cíclica, n par (Andrade et al. [5]).

F - Nossa construção dos reticulados densos, onde $\Lambda_2 = A_2$, $\Lambda_4 = D_4$, $\Lambda_6 = E_6$, $\Lambda_8 = E_8$ e $\Lambda_{12} = K_{12}$.

Lim - Limitante de Odlyzko [11].

Tabela 4.6: Distância produto mínima de A_2 , D_4 , E_6 , E_8 e K_{12} - Comparação.

Considerações

Nota-se que na maioria dos casos a distância produto mínima dos reticulados densos rotacionados que construímos é menor do que as versões rotacionadas conhecidas do reticulado

$\mathbb{Z}^n$, mas em algumas dimensões está bem próxima, como na dimensão 4. Na dimensão 12 chega a ser até maior que uma das construções de $\mathbb{Z}^n$. Considerando o “trade-off” entre diversidade, distância produto e densidade de empacotamento, os reticulados densos aqui construídos podem ser suporte para constelações de sinais eficientes para ambos os canais gaussiano e Rayleigh com desvanecimento.

CAPÍTULO 5

CONSTRUÇÃO DE RETICULADOS D_N SOBRE CORPOS TOTALMENTE REAIS

Neste capítulo reproduzimos famílias de reticulados D_n sobre corpos totalmente reais e mostramos que estas famílias apresentam bom desempenho simultaneamente para os Canais gaussianos e Canais Rayleigh com desvanecimento. As construções serão feitas de duas maneiras distintas, via reticulados ideais e via $\mathbb{Z}$ -módulos. Ressaltamos que o conteúdo deste capítulo faz parte do tema do artigo conjunto “Rotated D_n -lattices” [33], submetido em Dezembro de 2011. A nossa contribuição ao artigo é a parte correspondente à construção via reticulados ideais. A parte correspondente à construção via $\mathbb{Z}$ -módulos é contribuição da Prof^a. Dr^a. Grasielle Cristiane Jorge [32].

5.1 Via Reticulados ideais

Em [4], foram construídas famílias de reticulados $\mathbb{Z}^n$ rotacionados com diversidade máxima sobre o subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r})$, representando então constelações que são eficientes para o canal Rayleigh com desvanecimento. A seguir, usando as idéias contidas em [4] construímos uma família de reticulados D_n rotacionados sobre o subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r})$ que assintoticamente podem ser suporte para constelações de sinais eficientes para ambos os canais gaussiano e Rayleigh com desvanecimento.

Em termos de reticulado ideal, isto significa que dado n , procuramos um corpo de números $\mathbb{K}$ de grau n e um ideal $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que o reticulado $(\mathcal{A}, b_{\alpha})$ seja equivalente a D_n , $n \geq 4$. O objetivo é que seja encontrado um reticulado Λ que seja D_n escalonado e rotacionado.

5.1.1 Reticulados D_n rotacionados, $n = 2^{r-2}$, $r \geq 4$

A fim de que um reticulado $(\mathcal{A}, b_{\alpha})$ seja uma versão escalonada e rotacionada do reticulado $\Lambda = D_n$ com fator de escala $\sqrt{c}$, as condições expressas pela Equações (4.2.1), (4.2.2) e (4.2.3) são dadas respectivamente por

$$\mathcal{N}(\mathcal{A})^2 \mathcal{N}(\alpha) |d_{\mathbb{K}}| = 4c^n \quad (5.1.1)$$

$$\frac{t_{\alpha}^{n/2}}{2^n [|d_{\mathbb{K}}| \mathcal{N}(\alpha)]^{1/2}} = \frac{1}{2^{(n+2)/2}}. \quad (5.1.2)$$

$$t_{\alpha} = 2c. \quad (5.1.3)$$

Construção

Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{2^r})$ um corpo ciclotômico e $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ o subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r})$, onde r é um inteiro positivo, $r \geq 4$ e ζ_{2^r} é uma raiz primitiva 2^r -ésima da unidade. Temos que $n = [\mathbb{K} : \mathbb{Q}] = 2^{r-2}$ e $d_{\mathbb{K}} = 2^{(r-1)2^{r-2}-1}$. Assumindo $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$, os valores para

$\mathcal{N}(\alpha)$, c e t_α que satisfazem as Equações (5.1.1), (5.1.2) e (5.1.3) para $n = 2^{r-2}$ são listados abaixo

$\mathcal{N}(\alpha)$	c	t_α
8	2^{r-1}	2^r

Tabela 5.1: Parâmetros do reticulado ideal rotacionado de D_n .

Nosso objetivo agora é encontrar um elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ totalmente real e totalmente positivo que satisfaça a tabela acima. Assim, implementamos um algoritmo para encontrar α , e como a complexidade do algoritmo está relacionada ao grau da extensão $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ sobre $\mathbb{Q}$ que é 2^{r-2} , implementamos para os casos $r = 4, r = 5$ e $r = 6$, e selecionamos valores de α que sugerem um α que contemple o caso geral, conforme tabela abaixo

r	α	$\mathcal{N}(\alpha)$	c	t_α
4	$4 + (\zeta_{16} + \zeta_{16}^{-1}) - 2(\zeta_{16}^2 + \zeta_{16}^{-2}) - (\zeta_{16}^3 + \zeta_{16}^{-3})$	8	8	16
5	$4 + (\zeta_{32} + \zeta_{32}^{-1}) - 2(\zeta_{32}^2 + \zeta_{32}^{-2}) - (\zeta_{32}^3 + \zeta_{32}^{-3})$	8	16	32
6	$4 + (\zeta_{64} + \zeta_{64}^{-1}) - 2(\zeta_{64}^2 + \zeta_{64}^{-2}) - (\zeta_{64}^3 + \zeta_{64}^{-3})$	8	32	64

Tabela 5.2: Parâmetros do reticulado ideal rotacionado de D_n - dimensões 4, 8 e 16.

A tabela sugere que para o caso geral seja escolhido $\alpha = 4 + (\zeta_{2^r} + \zeta_{2^r}^{-1}) - 2(\zeta_{2^r}^2 + \zeta_{2^r}^{-2}) - (\zeta_{2^r}^3 + \zeta_{2^r}^{-3})$.

Proposição 5.1.1. *Considere $e_0 = 1$ e $e_i = \zeta_{2^r}^i + \zeta_{2^r}^{-i}$, para $i = 1, 2, \dots, 2^{r-2} - 1$.*

$$1. \text{ Se } i = 0, 1, \dots, 2^{r-2} - 1 \text{ então } b_\alpha(e_i, e_i) = \begin{cases} 2^r, & \text{se } i = 0, 1. \\ 3 \cdot 2^r, & \text{se } i = 2^{r-2} - 1. \\ 2^{r+1}, & \text{caso contrário.} \end{cases}$$

$$2. \text{ Se } i \neq 0 \text{ então } b_\alpha(e_i, e_0) = \begin{cases} 2^{r-1}, & \text{se } i = 1 \\ -2^r, & \text{se } i = 2. \\ -2^{r-1}, & \text{se } i = 3. \\ 0, & \text{caso contrário.} \end{cases}$$

$$3. \text{ Se } i \neq 0, j \neq 0 \text{ e } i < j \text{ então}$$

$$b_\alpha(e_i, e_j) = \begin{cases} 2^{r-1}, & \text{se } |i - j| = 1 \text{ e} \\ & (i, j) \notin \{(1, 2), (2^{r-2} - 2, 2^{r-2} - 1)\}. \\ -2^r, & \text{se } |i - j| = 2. \\ -2^{r-1}, & \text{se } |i - j| = 3. \\ 2^r, & \text{se } i = 2^{r-2} - 2 \text{ e } j = 2^{r-2} - 1. \\ 0, & \text{caso contrário.} \end{cases}$$

Demonstração:

Para simplificar notação chamaremos $Tr_{\mathbb{K}/\mathbb{Q}} = Tr$ e $\zeta_{2^r} = \zeta$. Pelo Corolário (1.4.4), como $mdc(i, 2^r) < 2^{r-1}$, para $i = 1, 2, 3$, segue que

$$\begin{aligned} b_\alpha(e_0, e_0) &= Tr(\alpha e_0 e_0) = Tr(\alpha) = Tr(4 + (\zeta + \zeta^{-1}) - 2(\zeta^2 + \zeta^{-2}) - (\zeta^3 + \zeta^{-3})) = \\ &= Tr(4) + Tr(\zeta + \zeta^{-1}) - 2Tr(\zeta^2 + \zeta^{-2}) - Tr(\zeta^3 + \zeta^{-3}) = \\ &= 4 \cdot 2^{r-2} = 2^r. \end{aligned}$$

Agora, para $i \neq 0$, como $mdc(2i, 2^r), mdc(2i \pm 1, 2^r), mdc(2i \pm 3, 2^r) < 2^{r-1}$ para $i = 1, 2, \dots, 2^{r-2} - 1$, e também $mdc(2i + 2, 2^r) < 2^{r-1}$, para $i = 1, 2, \dots, 2^{r-2} - 2$ e $mdc(2i + 2, 2^r) = 2^{r-1}$, para $i = 2^{r-2} - 1$ segue que

$$\begin{aligned}
b_\alpha(e_i, e_i) &= Tr(\alpha e_i e_i) = Tr(\alpha e_i^2) = \\
&= Tr([4 + (\zeta + \zeta^{-1}) - 2(\zeta^2 + \zeta^{-2}) - (\zeta^3 + \zeta^{-3})][2 + \zeta^{2i} + \zeta^{-2i}]) = \\
&= Tr(8 + 4(\zeta^{2i} + \zeta^{-2i}) + 2(\zeta + \zeta^{-1}) + (\zeta^{2i+1} + \zeta^{-(2i+1)}) + (\zeta^{2i-1} + \zeta^{-(2i-1)}) \\
&\quad - 4(\zeta^2 + \zeta^{-2}) - 2(\zeta^{2i+2} + \zeta^{-(2i+2)}) - 2(\zeta^{2i-2} + \zeta^{-(2i-2)}) - 2(\zeta^3 + \zeta^{-3}) \\
&\quad - (\zeta^{2i+3} + \zeta^{-(2i+3)}) - (\zeta^{2i-3} + \zeta^{-(2i-3)})) = \\
&= Tr(8) + 4Tr(\zeta^{2i} + \zeta^{-2i}) + 2Tr(\zeta + \zeta^{-1}) + Tr(\zeta^{2i+1} + \zeta^{-(2i+1)}) \\
&\quad + Tr(\zeta^{2i-1} + \zeta^{-(2i-1)}) - 4Tr(\zeta^2 + \zeta^{-2}) - 2Tr(\zeta^{2i+2} + \zeta^{-(2i+2)}) \\
&\quad - 2Tr(\zeta^{2i-2} + \zeta^{-(2i-2)}) - 2Tr(\zeta^3 + \zeta^{-3}) - Tr(\zeta^{2i+3} + \zeta^{-(2i+3)}) \\
&\quad - Tr(\zeta^{2i-3} + \zeta^{-(2i-3)}) = \\
&= \begin{cases} 2^r, & \text{se } i = 1. \\ 3 \cdot 2^r, & \text{se } i = 2^{r-2} - 1. \\ 2^{r+1}, & \text{caso contrário.} \end{cases}
\end{aligned}$$

Para $i \neq 0$, como $mdc(i-1, 2^r) < 2^{r-1}$ para $i = 2, 3, 4, \dots, 2^{r-2} - 1$, $mdc(i-2, 2^r) < 2^{r-1}$ para $i = 1, 3, 4, \dots, 2^{r-2} - 1$, $mdc(i-3, 2^r) < 2^{r-1}$ para $i = 1, 2, 4, \dots, 2^{r-2} - 1$, e $Tr(\zeta^0 + \zeta^0) = Tr(2) = 2^{r-1}$, segue que

$$\begin{aligned}
b_\alpha(e_i, e_0) &= Tr(\alpha e_i e_0) = Tr(\alpha e_i) = \\
&= Tr([4 + (\zeta + \zeta^{-1}) - 2(\zeta^2 + \zeta^{-2}) - (\zeta^3 + \zeta^{-3})][\zeta^i + \zeta^{-i}]) = \\
&= Tr(4(\zeta^i + \zeta^{-i}) + (\zeta^{i+1} + \zeta^{-(i+1)}) + (\zeta^{i-1} + \zeta^{-(i-1)}) - 2(\zeta^{i+2} + \zeta^{-(i+2)}) \\
&\quad - 2(\zeta^{i-2} + \zeta^{-(i-2)}) - (\zeta^{i+3} + \zeta^{-(i+3)}) - (\zeta^{i-3} + \zeta^{-(i-3)})) = \\
&= 4Tr(\zeta^i + \zeta^{-i}) + Tr(\zeta^{i+1} + \zeta^{-(i+1)}) + Tr(\zeta^{i-1} + \zeta^{-(i-1)}) - 2Tr(\zeta^{i+2} + \zeta^{-(i+2)}) \\
&\quad - 2Tr(\zeta^{i-2} + \zeta^{-(i-2)}) - Tr(\zeta^{i+3} + \zeta^{-(i+3)}) - Tr(\zeta^{i-3} + \zeta^{-(i-3)}) = \\
&= \begin{cases} 2^{r-1}, & \text{se } i = 1 \\ -2^r, & \text{se } i = 2. \\ -2^{r-1}, & \text{se } i = 3. \\ 0, & \text{caso contrário.} \end{cases}
\end{aligned}$$

Finalmente, para $i \neq 0$, $j \neq 0$ e $i < j$, como $mdc(i \pm j, 2^r), mdc(i + j \pm 1, 2^r) < 2^{r-1}$, $mdc(i + j \pm 2, 2^r) < 2^{r-1}$, $mdc(i + j + 3, 2^r) < 2^{r-1}$, se $i + j \neq 2^{r-1} - 3$, $mdc(i + j + 3, 2^r) = 2^{r-1}$,

se $i + j = 2^{r-1} - 3$ e $\text{mdc}(i + j - 3, 2^r) < 2^{r-1}$, se $i + j \neq 3$, segue que

$$\text{Tr}(\zeta^{i-j+1} + \zeta^{-(i-j+1)}) + \text{Tr}(\zeta^{i-j-1} + \zeta^{-(i-j-1)}) = \begin{cases} 2^{r-1}, & \text{se } |i - j| = 1. \\ 0, & \text{caso contrário.} \end{cases}$$

$$\text{Tr}(\zeta^{i-j+2} + \zeta^{-(i-j+2)}) + \text{Tr}(\zeta^{i-j-2} + \zeta^{-(i-j-2)}) = \begin{cases} 2^{r-1}, & \text{se } |i - j| = 2. \\ 0, & \text{caso contrário.} \end{cases}$$

$$\text{Tr}(\zeta^{i-j+3} + \zeta^{-(i-j+3)}) + \text{Tr}(\zeta^{i-j-3} + \zeta^{-(i-j-3)}) = \begin{cases} 2^{r-1}, & \text{se } |i - j| = 3. \\ 0, & \text{caso contrário.} \end{cases}$$

$$\begin{aligned} b_\alpha(e_i, e_j) &= \text{Tr}(\alpha e_i e_j) = \text{Tr}([4 + (\zeta + \zeta^{-1}) - 2(\zeta^2 + \zeta^{-2}) - (\zeta^3 + \zeta^{-3})][\zeta^i + \zeta^{-i}][\zeta^j + \zeta^{-j}]) = \\ &= \text{Tr}([4(\zeta^i + \zeta^{-i}) + (\zeta^{i+1} + \zeta^{-(i+1)}) + (\zeta^{i-1} + \zeta^{-(i-1)}) - 2(\zeta^{i+2} + \zeta^{-(i+2)}) \\ &\quad - 2(\zeta^{i-2} + \zeta^{-(i-2)}) - (\zeta^{i+3} + \zeta^{-(i+3)}) - (\zeta^{i-3} + \zeta^{-(i-3)})][\zeta^j + \zeta^{-j}]) = \\ &= \text{Tr}(4(\zeta^{i+j} + \zeta^{-(i+j)}) + 4(\zeta^{i-j} + \zeta^{-(i-j)}) + (\zeta^{i+j+1} + \zeta^{-(i+j+1)}) \\ &\quad + (\zeta^{i-j+1} + \zeta^{-(i-j+1)}) + (\zeta^{i+j-1} + \zeta^{-(i+j-1)}) + (\zeta^{i-j-1} + \zeta^{-(i-j-1)}) \\ &\quad - 2(\zeta^{i+j+2} + \zeta^{-(i+j+2)}) - 2(\zeta^{i-j+2} + \zeta^{-(i-j+2)}) - 2(\zeta^{i+j-2} + \zeta^{-(i+j-2)}) \\ &\quad - 2(\zeta^{i-j-2} + \zeta^{-(i-j-2)}) - (\zeta^{i+j+3} + \zeta^{-(i+j+3)}) - (\zeta^{i-j+3} + \zeta^{-(i-j+3)}) \\ &\quad - (\zeta^{i+j-3} + \zeta^{-(i+j-3)}) - (\zeta^{i-j-3} + \zeta^{-(i-j-3)})) = \\ &= 4\text{Tr}(\zeta^{i+j} + \zeta^{-(i+j)}) + 4\text{Tr}(\zeta^{i-j} + \zeta^{-(i-j)}) + \text{Tr}(\zeta^{i+j+1} + \zeta^{-(i+j+1)}) \\ &\quad + \text{Tr}(\zeta^{i-j+1} + \zeta^{-(i-j+1)}) + \text{Tr}(\zeta^{i+j-1} + \zeta^{-(i+j-1)}) + \text{Tr}(\zeta^{i-j-1} + \zeta^{-(i-j-1)}) \\ &\quad - 2\text{Tr}(\zeta^{i+j+2} + \zeta^{-(i+j+2)}) - 2\text{Tr}(\zeta^{i-j+2} + \zeta^{-(i-j+2)}) - 2\text{Tr}(\zeta^{i+j-2} + \zeta^{-(i+j-2)}) \\ &\quad - 2\text{Tr}(\zeta^{i-j-2} + \zeta^{-(i-j-2)}) - \text{Tr}(\zeta^{i+j+3} + \zeta^{-(i+j+3)}) - \text{Tr}(\zeta^{i-j+3} + \zeta^{-(i-j+3)}) \\ &\quad - \text{Tr}(\zeta^{i+j-3} + \zeta^{-(i+j-3)}) - \text{Tr}(\zeta^{i-j-3} + \zeta^{-(i-j-3)}) = \\ &= \begin{cases} 2^{r-1}, & \text{se } |i - j| = 1 \text{ e} \\ & (i, j) \notin \{(1, 2), (2^{r-2} - 2, 2^{r-2} - 1)\}. \\ -2^r, & \text{se } |i - j| = 2. \\ -2^{r-1}, & \text{se } |i - j| = 3. \\ 2^r, & \text{se } i = 2^{r-2} - 2 \text{ e } j = 2^{r-2} - 1. \\ 0, & \text{caso contrário.} \end{cases} \end{aligned}$$

o que conclui a demonstração. $\square$

Corolário 5.1.1. *O reticulado $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{A})$ possui matriz de Gram*

$$G = \begin{pmatrix} 2 & 1 & -2 & -1 & 0 & \cdots & \cdots & 0 \\ 1 & 2 & 0 & -2 & -1 & 0 & & \vdots \\ -2 & 0 & 4 & 1 & -2 & \ddots & \ddots & \\ -1 & -2 & 1 & 4 & 1 & \ddots & & \\ 0 & -1 & -2 & 1 & 4 & \ddots & \ddots & \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 & \vdots \\ & & \ddots & & \ddots & 4 & 1 & -2 & -1 & 0 \\ & & & & \ddots & 1 & 4 & 1 & -2 & -1 \\ & & & & \ddots & \ddots & -2 & 1 & 4 & 1 & -2 \\ \vdots & & & & & 0 & -1 & -2 & 1 & 4 & 2 \\ 0 & \cdots & & & \cdots & 0 & -1 & -2 & 2 & 6 \end{pmatrix}.$$

Demonstração: Se $\hat{M}$ é uma matriz geradora para $\sigma_\alpha(\mathcal{A})$ com respectiva matriz de Gram $\hat{G} = (\hat{g}_{ij})_{j=1}^n$, como $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$ e $\{e_0, e_1, \dots, e_n\}$, $e_0 = 1$ e $e_j = \zeta_{2^r}^j + \zeta_{2^r}^{-j}$, é uma $\mathbb{Z}$ -base para $\mathcal{A}$, segue da Observação 3.3.1 que

$$\hat{g}_{ij} = b_\alpha(e_i, e_j) = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha e_i e_j).$$

A matriz de Gram do reticulado $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{A})$ é dada por

$$G = \left(\frac{1}{\sqrt{2^{r-1}}} \hat{M} \right) \left(\frac{1}{\sqrt{2^{r-1}}} \hat{M} \right)^t = \frac{1}{2^{r-1}} \hat{M} \hat{M}^t = \frac{1}{2^{r-1}} \hat{G},$$

e pela Pela Proposição 5.1.1 segue que

$$G = \frac{1}{2^{r-1}} \hat{G} = \begin{pmatrix} 2 & 1 & -2 & -1 & 0 & \cdots & & \cdots & 0 \\ 1 & 2 & 0 & -2 & -1 & 0 & & & \vdots \\ -2 & 0 & 4 & 1 & -2 & \ddots & \ddots & & \\ -1 & -2 & 1 & 4 & 1 & \ddots & & & \\ 0 & -1 & -2 & 1 & 4 & \ddots & & \ddots & \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 & \vdots \\ & & \ddots & & & \ddots & 4 & 1 & -2 & -1 & 0 \\ & & & & & \ddots & 1 & 4 & 1 & -2 & -1 \\ & & & & \ddots & \ddots & -2 & 1 & 4 & 1 & -2 \\ \vdots & & & & & & 0 & -1 & -2 & 1 & 4 & 2 \\ 0 & \cdots & & & & \cdots & 0 & -1 & -2 & 2 & 6 \end{pmatrix},$$

o que conclui a demonstração. $\square$

Corolário 5.1.2. *O reticulado $\sigma_\alpha(\mathcal{A})$ é uma versão escalonada e rotacionada do reticulado D_n , $n = 2^{r-2}$, $r \geq 4$.*

Demonstração: A matriz A dada por

$$\begin{pmatrix} -1 & 1 & -1 & 1 & \cdots & & \cdots & -1 & 1 \\ -1 & 0 & -1 & 0 & \cdots & & \cdots & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & \cdots & \cdots & 0 & 1 & 0 & 0 \\ -1 & 0 & -1 & 0 & \cdots & 0 & -1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ -1 & 0 & -1 & 0 & -1 & 0 & \cdots & & \cdots & 0 \\ 0 & 1 & 0 & 1 & 0 & \cdots & & & \cdots & 0 \\ -1 & 0 & -1 & 0 & \cdots & & & & \cdots & 0 \\ 0 & 1 & 0 & \cdots & & & & & \cdots & 0 \\ -1 & 0 & \cdots & & & & & & \cdots & 0 \end{pmatrix},$$

possui entradas inteiras e determinante igual a 1, e pelo Corolário 5.1.1 temos

$$\frac{1}{2^{r-1}} A \hat{G} A^t = A \left(\frac{1}{2^{r-1}} \hat{G} \right) A^t = A G A^t,$$

mas

$$A G A^t = \begin{pmatrix} 2 & 0 & -1 & 0 & \cdots & \cdots & 0 \\ 0 & 2 & -1 & 0 & \ddots & & \vdots \\ -1 & -1 & 2 & -1 & 0 & \ddots & \\ 0 & 0 & -1 & 2 & -1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & 0 & -1 & 2 & -1 \\ 0 & \cdots & & \cdots & 0 & -1 & 2 \end{pmatrix},$$

que é a matriz de Gram do reticulado D_n relativo à matriz geradora padrão

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

Portanto, pela Proposição 2.1.2 o reticulado $\sigma_\alpha(\mathcal{A})$ é uma versão escalonada e rotacionada do reticulado D_n com fator de escala $\frac{1}{\sqrt{2^{r-1}}}$. $\square$

Exemplo 5.1.1. Considere o corpo ciclotômico $\mathbb{Q}(\zeta_{16})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ o seu subcorpo maximal real. Tomando a base $\{e_0 = 1, e_1 = \zeta_{16} + \zeta_{16}^{-1}, e_2 = \zeta_{16}^2 + \zeta_{16}^{-2}, e_3 = \zeta_{16}^3 + \zeta_{16}^{-3}\}$ de $\mathcal{O}_K$, a matriz geradora $\hat{M}$ do reticulado $\sigma_\alpha(\mathcal{A})$ é dada por $\hat{M} = QD$, onde

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

$$D = \begin{pmatrix} d_{11} & 0 & 0 & 0 \\ 0 & d_{22} & 0 & 0 \\ 0 & 0 & d_{33} & 0 \\ 0 & 0 & 0 & d_{44} \end{pmatrix}$$

com

$$d_{11} = \sqrt{4 + \sqrt{2 + \sqrt{2}} - 2\sqrt{2} - \sqrt{2 - \sqrt{2}}}$$

$$d_{22} = \sqrt{4 + \sqrt{2 - \sqrt{2}} + 2\sqrt{2} + \sqrt{2 + \sqrt{2}}}$$

$$d_{33} = \sqrt{4 - \sqrt{2 - \sqrt{2}} + 2\sqrt{2} - \sqrt{2 + \sqrt{2}}}$$

$$d_{44} = \sqrt{4 - \sqrt{2 + \sqrt{2}} - 2\sqrt{2} + \sqrt{2 - \sqrt{2}}}$$

e respectiva matriz de Gram $\hat{G} = \hat{M}\hat{M}^t$. Pelo Corolário 5.1.1 a matriz de Gram do reticulado $\frac{1}{\sqrt{8}}\sigma_\alpha(\mathcal{A})$ é dada por

$$G = \begin{pmatrix} 2 & 1 & -2 & -1 \\ 1 & 2 & 0 & -2 \\ -2 & 0 & 4 & 2 \\ -1 & -2 & 2 & 6 \end{pmatrix}.$$

Agora, tomando

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

segue que

$$\frac{1}{8}A\hat{G}A^t = A\left(\frac{1}{8}\hat{G}\right)A^t = AGA^t = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix},$$

que é a matriz de Gram do D_4 . Portanto, $\sigma_\alpha(\mathcal{A})$ é uma versão escalonada e rotacionada do reticulado D_4 com fator de escala $\frac{1}{\sqrt{8}}$.

A seguir calculamos a distância produto mínima dos $\mathbb{Z}^n$ rotacionados construídos em [4] e da nossa construção de D_n rotacionados, a fim de comparar o desempenho das duas constelações.

$\mathbb{Z}^n$ rotacionados

Considere o corpo ciclotômico $\mathbb{Q}(\zeta_n)$ e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ o seu subcorpo maximal real. Sejam $Gal(\mathbb{K}, \mathbb{Q}) = \{\sigma_1, \dots, \sigma_n\}$ o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ e $\{e_0, e_1, \dots, e_{n-1}\}$ uma base de $\mathcal{O}_{\mathbb{K}}$. Em [4], foram construídos reticulados Λ que são versões escalonadas e rotacionadas de $\mathbb{Z}^n$ para $n = 2^{r-2}$, com fator de escala $\sqrt{2^{r-1}}$, via $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$.

Pela Proposição 4.2.1 temos que

$$\det(\Lambda) = (2^{r-1})^{2^{r-2}} \det(\mathbb{Z}^n) = (2^{r-1})^{2^{r-2}},$$

e

$$\eta_1 = 2^{r-1} \eta_2 = 2^{r-1}$$

onde η_1 e η_2 são as normas mínimas de Λ e $\mathbb{Z}^n$, respectivamente. Assim, pela Definição 3.3.5 segue que

$$\begin{aligned} \sqrt[2^{r-2}]{d_{p,min}(\Lambda)} &= \frac{1}{\sqrt{2^{r-1}}} \sqrt[2^{r-1}]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{2^{r-1}}} \sqrt[2^{r-1}]{\frac{(2^{r-1})^{2^{r-2}}}{2^{2^{r-2}(r-1)-1}}} = \\ &= (2^{r-1})^{-\frac{1}{2}} \cdot 2^{\frac{1}{2^{r-1}}} = 2^{-\left(\frac{(r-1)2^{r-2}-1}{2^{r-1}}\right)}. \end{aligned}$$

Portanto,

$$\sqrt[2^{r-2}]{d_{p,min}(\Lambda)} = 2^{-\left(\frac{(r-1)2^{r-2}-1}{2^{r-1}}\right)}. \quad (5.1.4)$$

D_n rotacionados

Nesta seção construímos reticulados Λ que são versões escalonadas e rotacionadas dos reticulados D_n para $n = 2^{r-2}$, com fator de escala $\sqrt{2^{r-1}}$, via $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$.

Pela Proposição 4.2.1 temos que

$$\det(\Lambda) = (2^{r-1})^{2^{r-2}} \det(D_n) = (2^{r-1})^{2^{r-2}} 4 = 2^{(r-1)2^{r-2}+2},$$

e

$$\eta_1 = 2^{r-1}\eta_2 = 2^{r-1}2 = 2^r$$

onde η_1 e η_2 são as normas mínimas de Λ e D_n , respectivamente. Assim, pela Definição 3.3.5 segue que

$$\begin{aligned} \sqrt[2^{r-2}]{d_{p,min}(\Lambda)} &= \frac{1}{\sqrt{2^r}} \sqrt[2^{r-1}]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{2^r}} \sqrt[2^{r-1}]{\frac{2^{(r-1)2^{r-2}+2}}{2^{2^{r-2}(r-1)-1}}} = \\ &= (2^r)^{-\frac{1}{2}} \cdot 8^{\frac{1}{2^{r-1}}} = 2^{-\left(\frac{r2^{r-2}-3}{2^{r-1}}\right)}. \end{aligned}$$

Portanto,

$$\sqrt[2^{r-2}]{d_{p,min}(\Lambda)} = 2^{-\left(\frac{r2^{r-2}-3}{2^{r-1}}\right)}. \quad (5.1.5)$$

Podemos comparar a distância produto mínima entre as constelações $\mathbb{Z}^n$ e D_n para $n = 2^{r-2}$, $r \geq 4$. Seja γ a função que representa $\sqrt[n]{d_{p,min}(D_n)}$ em relação a $\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$, assim pelas Equações (5.1.4) e (5.1.5) temos

$$\gamma(r) = \frac{2^{-\left(\frac{(r-1)2^{r-2}-1}{2^{r-1}}\right)}}{2^{-\left(\frac{r2^{r-2}-3}{2^{r-1}}\right)}} = \frac{\sqrt{2}}{2} \sqrt[2^{r-2}]{2}$$

Nota-se que

$$\lim_{r \rightarrow +\infty} \gamma(r) = \frac{\sqrt{2}}{2} \approx 0.707107$$

ou seja, quando a dimensão tende ao infinito ($r \rightarrow +\infty$), temos que $\sqrt[n]{d_{p,min}(D_n)}$ representa aproximadamente 70.71% de $\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$, o que pode ser visto na Tabela 5.3, para $r = 4, 5, \dots, 21$.

n	$\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,min}(D_n)}$	(%)
4	0.385553	0.324210	84.089
8	0.261068	0.201311	77.110
16	0.180648	0.133393	73.841
32	0.126361	0.0913074	72.259
64	0.0888683	0.0635236	71.480
128	0.0626695	0.0445546	71.094
256	0.0442540	0.0313772	70.902
512	0.0312712	0.0221420	70.806
1024	0.0221046	0.0156409	70.758
2048	0.0156276	0.0110542	70.734
4096	0.0110495	0.00781448	70.722
8192	0.00781283	0.00552497	70.716
16384	0.00552439	0.00390650	70.713
32768	0.00390629	0.00276222	70.712
65536	0.00276215	0.00195316	70.711
131072	0.00195313	0.00138108	70.711
262144	0.00138107	0.000976566	70.710
524288	0.000976563	0.000690535	70.710

Tabela 5.3: Distâncias produto mínimas de $\mathbb{Z}^n$ e D_n - Comparação

Uma comparação entre os desempenhos das duas constelações também pode ser visto pela Figura 5.1

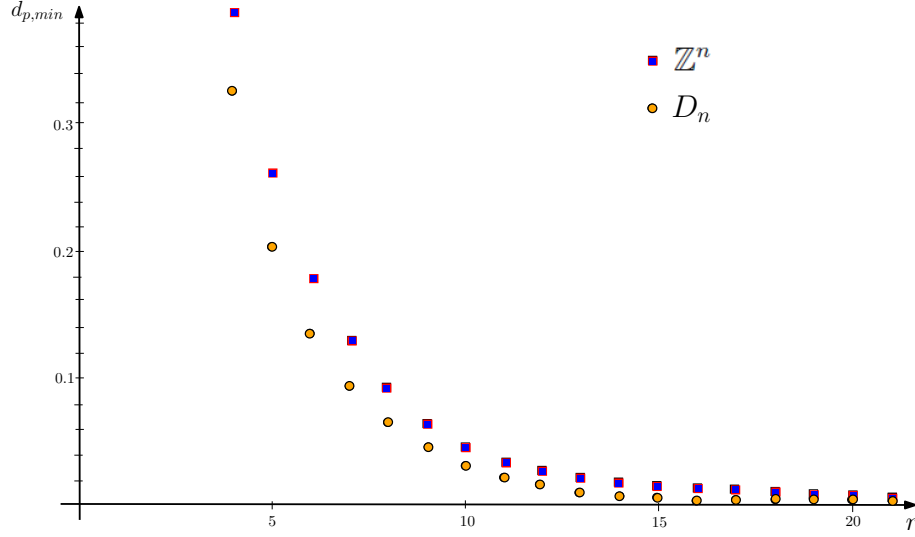


Figura 5.1: Distâncias produto mínimas de $\mathbb{Z}^n$ e D_n - Gráfico

Sejam $\delta(\mathbb{Z}^n)$ e $\delta(D_n)$ as densidades de centro dos reticulados $\mathbb{Z}^n$ e D_n , respectivamente. A fim de comparar as densidades, seja γ a função que representa $\delta(\mathbb{Z}^n)$ em relação a $\delta(D_n)$. Por [42], temos que

$$\gamma(n) = \frac{2^{-n}}{2^{-\frac{n+2}{2}}} = 2^{\frac{-n+2}{2}}.$$

Nota-se que

$$\lim_{n \rightarrow +\infty} \gamma(n) = 0,$$

ou seja, quando a dimensão tende ao infinito ($n \rightarrow +\infty$), temos que o reticulado D_n é muito mais denso do que o reticulado $\mathbb{Z}^n$.

Considerações

Comparando os $\mathbb{Z}^n$ e D_n rotacionados em relação ao canal gaussiano, onde constelações eficientes são aquelas representadas por reticulados com boa densidade de empacotamento, e em relação ao Canal Rayleigh com desvanecimento, onde constelações eficientes são aquelas representadas por reticulados com diversidade máxima e boa distância produto mínima,

nota-se que assintoticamente os reticulados D_n rotacionados são interessantes quando o objetivo é ser eficiente em ambos os canais, pois apesar da distância produto mínima ser menor do que a dos $\mathbb{Z}^n$ rotacionados, possui diversidade máxima, o que é importante para o Canal Rayleigh. Com relação ao canal gaussiano, assintoticamente os reticulados D_n rotacionados são muito mais densos do que os $\mathbb{Z}^n$ rotacionados, evidenciando assim melhor performance para este canal.

5.2 Via $\mathbb{Z}$ -módulos

O conteúdo desta seção faz parte de [32], onde é feita a construção de famílias de reticulados D_n rotacionados, para $n = 2^{r-2}$, $r \geq 4$ e $n = \frac{p-1}{2}$, p primo.

5.2.1 Reticulados D_n rotacionados, $n = 2^{r-2}$, $r \geq 4$

Nesta seção, faremos a construção de reticulados D_n rotacionados via o subcorpo real maximal $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ dos corpos ciclotômicos $\mathbb{Q}(\zeta_{2^r})$ com $r \geq 4$. Desta forma, serão obtidos reticulados D_n rotacionados para $n = 2^{r-2}$, $r \geq 4$, isto é, $n = 4, 8, 16, 32, 64, 128, 256, 512, \dots$.

Sejam $\zeta = \zeta_{2^r}$ uma raiz 2^r -ésima primitiva da unidade, $\mathbb{L} = \mathbb{Q}(\zeta_{2^r})$ e $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$. Temos que $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 2^{r-2}$.

$$2^{r-1} \begin{pmatrix} \mathbb{Q}(\zeta) \\ |2 \\ \mathbb{Q}(\zeta + \zeta^{-1}) \\ |2^{r-2} \\ \mathbb{Q} \end{pmatrix}$$

Observação 5.2.1. Em [4, 27] são construídos reticulados $\mathbb{Z}^n$ -rotacionados no subcorpo real maximal de tais corpos ciclotômicos para $\alpha_1 = 2 - (\zeta + \zeta^{-1})$ e $\alpha_2 = 2 + (\zeta + \zeta^{-1})$, respectivamente, e $\mathcal{A} = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$. Tais reticulados, além de serem equivalentes na

métrica euclidiana, pois ambos são equivalentes ao reticulado $\mathbb{Z}^n$, são equivalentes na métrica da soma. De fato, uma matriz geradora para o reticulado $\frac{1}{\sqrt{2^{r-1}}} \sigma_{\alpha_1}(\mathcal{O}_{\mathbb{K}})$ de [27] é

$$M_1 = \frac{1}{\sqrt{2^{r-1}}} N A,$$

onde $N = (\sigma_i(e_{j-1}))_{i,j=1}^n$ e $A = \text{diag}(\sqrt{\sigma_k(\alpha_2)})$. Considere a matriz mudança de base

$$M = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix}$$

e a matriz de permutação

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

Temos que $M \left(\frac{1}{\sqrt{2^{r-1}}} N A \right) P$ é a matriz geradora para o reticulado $\frac{1}{\sqrt{2^{r-1}}} \sigma_{\alpha_2}(\mathcal{O}_{\mathbb{K}})$ obtido em [4].

Como o reticulado D_n é um sub-reticulado de $\mathbb{Z}^n$, vamos utilizar o reticulado algébrico obtido pela perturbação do homomorfismo canônico [27] e encontrar um sub-reticulado que seja D_n rotacionado.

Sejam $e_0 = 1$ e $e_j = \zeta^j + \zeta^{-j}$ para $j = 1, \dots, 2^{r-2} - 1$. Temos que $\{e_j\}_{j=0}^{2^{r-2}-1}$ é uma $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$.

Uma matriz geradora para o reticulado $\mathbb{Z}^n$ rotacionado $\frac{1}{\sqrt{2^{r-1}}} \sigma_{\alpha_1}(\mathcal{O}_{\mathbb{K}})$ de [27] é

$$M_1 = \frac{1}{\sqrt{2^{r-1}}} N A,$$

onde $N = (\sigma_i(e_{j-1}))_{i,j=1}^n$ e $A = \text{diag}(\sqrt{\sigma_k(\alpha)})$.

Consideremos a matriz mudança de base

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

Para $M = TM_1$, temos que a matriz de Gram $G = MM^t = I_n$ é uma matriz de rotação. Portanto, a matriz M leva a base canônica I_n do $\mathbb{Z}^n$ na base $I_n M$ do reticulado $\frac{1}{\sqrt{2^{r-1}}} \sigma_{\alpha_1}(\mathcal{O}_{\mathbb{K}})$.

Uma matriz geradora para o reticulado D_n é dada por

$$B = \begin{pmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}. \quad (5.2.6)$$

Proposição 5.2.1. *Sejam $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$ -módulo com $\mathbb{Z}$ -base*

$$\{-e_1, e_2, \dots, -e_{n-1}, -2e_0 + 2e_1 - 2e_2 + \cdots - 2e_{n-2} + e_{n-1}\}$$

e $\alpha = 2 + e_1$. O reticulado $\frac{1}{\sqrt{2^{r-1}}} \sigma_{\alpha}(\mathcal{A}) \subseteq \mathbb{R}^{2^{r-2}}$ é um reticulado D_n rotacionado.

Demonstração: Seja B a matriz geradora de D_n dada em (5.2.6). Usando propriedades do homomorfismo, temos que

$$\begin{aligned}
BM &= \frac{1}{\sqrt{2^{r-1}}} BTNA = \frac{1}{\sqrt{2^{r-1}}} B \begin{pmatrix} 1 & -1 & \cdots & 1 & -1 \\ 1 & -1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix} A \\
&= \frac{1}{\sqrt{2^{r-1}}} B \begin{pmatrix} \sigma_1(e_0 - e_1 + \cdots + e_{n-2} - e_{n-1}) & \cdots & \sigma_n(e_0 - e_1 + \cdots + e_{n-2} - e_{n-1}) \\ \sigma_1(e_0 - e_1 + \cdots + e_{n-2}) & \cdots & \sigma_n(e_0 - e_1 + \cdots + e_{n-2}) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_0) & \cdots & \sigma_n(e_0) \end{pmatrix} A \\
&= \frac{1}{\sqrt{2^{r-1}}} \begin{pmatrix} \sigma_1(-2e_0 + \cdots - 2e_{n-2} + e_{n-1}) & \cdots & \sigma_n(-2e_0 + \cdots - 2e_{n-2} + e_{n-1}) \\ \sigma_1(-e_{n-1}) & \cdots & \sigma_n(-e_{n-1}) \\ \vdots & \ddots & \vdots \\ \sigma_1(-e_1) & \cdots & \sigma_n(-e_1) \end{pmatrix} A
\end{aligned}$$

é uma matriz geradora para $\frac{1}{\sqrt{2^{r-1}}} \sigma_\alpha(\mathcal{A})$. Este reticulado é um reticulado D_n rotacionado, pois $BM(BM)^t = BB^t$ é a matriz de Gram padrão do reticulado D_n . $\square$

A seguir, mostraremos que os reticulados D_n rotacionados obtidos na Proposição 5.2.1 estão associados a um ideal principal de $\mathcal{O}_{\mathbb{K}}$ e calcularemos sua distância produto mínima relativa.

Proposição 5.2.2. *Seja $\mathcal{A}$ o $\mathbb{Z}$ -módulo dado na Proposição 5.2.1. $\mathcal{A}$ é um ideal principal e $\mathcal{A} = e_1 \mathcal{O}_{\mathbb{K}}$.*

Demonstração: É fácil ver que $\mathcal{A} = 2e_0\mathbb{Z} + e_1\mathbb{Z} + \cdots + e_{n-1}\mathbb{Z}$. Seja $x \in e_1 \mathcal{O}_{\mathbb{K}}$. Temos que $x = e_1(a_0e_0 + a_1e_1 + a_2e_2 + \cdots + a_{n-1}e_{n-1}) = a_0e_1 + a_1(e_2 + 2e_0) + a_2(e_3 + e_1) + \cdots + a_{n-1}(2e_0 + e_{n-2}) = a_1(2e_0) + (2a_0 + a_2)(e_1) + (a_1 + a_3)(e_2) + \cdots + (a_{n-2})(e_{n-1}) \in \mathcal{A}$. Agora, se $x \in \mathcal{A}$, então $x = a_02e_0 + a_1e_1 + \cdots + a_{n-1}e_{n-1} = (e_1)[a_0e_1 + a_1e_2 + (a_2 - a_0)e_3 + (a_3 - a_1)e_4 + (a_4 - a_2 - a_0)e_5 + (a_5 - a_3 - a_1)e_6 + \cdots + (a_{n-1})e_{n-2} + (a_{n-2} - a_{n-4} \cdots - a_0)e_{n-1}] \in e_1 \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathcal{A}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$. $\square$

Proposição 5.2.3. Se $\Lambda = \frac{1}{\sqrt{2^{r-1}}} \sigma_\alpha(\mathcal{A})$ então

$$d_{p,rel} \left(\frac{1}{2^{r-1}} \sigma_\alpha(\mathcal{A}) \right) = \frac{1}{\sqrt{2}^n} \frac{1}{\sqrt{2^{r-1}}^n} \sqrt{8} = 2^{\frac{3-rn}{2}}$$

Demonstração: Primeiro notemos que o valor da norma mínima do reticulado D_n é $\sqrt{2}$. Logo, temos que multiplicar a distância produto mínima por $\frac{1}{\sqrt{2}^n}$. Como o ideal $\mathcal{A}$ é principal, temos que $d_{p,min}(\sigma_\alpha(\mathcal{A})) = \sqrt{\mathcal{N}(\alpha)\mathcal{N}(\mathcal{A})^2}$. Agora, temos que $\mathcal{N}(\alpha) = 2$ e $\mathcal{N}(\mathcal{A}) = 2$. Portanto,

$$d_{p,rel} \left(\frac{1}{2^{r-1}} \sigma_\alpha(\mathcal{A}) \right) = \frac{1}{\sqrt{2}^n} \frac{1}{\sqrt{2^{r-1}}^n} \sqrt{8}.$$

□

A tabela seguinte mostra uma comparação entre a distância produto mínima relativa e a densidade de centro dos reticulados $\mathbb{Z}^n$ rotacionados de [27] e D_n rotacionados construídos aqui.

r	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(D_n)$
4	4	0.385553	0.324210	0.062500	0.125000
5	8	0.261068	0.201311	0.003906	0.031250
6	16	0.180648	0.133393	0.000015	0.001953
7	32	0.126361	0.091307	2.3×10^{-10}	7.6×10^{-6}
8	64	0.088868	0.063523	5.4×10^{-20}	1.1×10^{-10}
9	128	0.062669	0.044554	2.9×10^{-39}	2.7×10^{-20}

Tabela 5.4: Distância produto e densidade de centro $\mathbb{Z}^n$ e D_n via $\mathbb{Z}$ -módulos - Comparação.

Note que, para $\Lambda = \frac{1}{\sqrt{2^{r-1}}}(\sigma_\alpha(I)) \subseteq \mathbb{R}^{2^{r-2}}$, temos:

$$\lim_{n \rightarrow \infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2} \text{ e } \lim_{n \rightarrow \infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0.$$

Se o objetivo é construir reticulados com boa performance sobre os canais gaussiano e do tipo Rayleigh com desvanecimento, levando em conta o “trade-off” densidade versus

distância produto mínima relativa, existem algumas vantagens em considerar os reticulados D_n rotacionados aqui construídos ao invés dos reticulados $\mathbb{Z}^n$ rotacionados de [27] $n = 2^{r-2}$, $r \geq 5$, em altas dimensões.

5.2.2 Reticulados D_n rotacionados, $n = \frac{p-1}{2}$, p primo

Através da família de reticulados $\mathbb{Z}^n$ rotacionados construída em [30], construímos famílias de reticulados D_n rotacionados para $n = \frac{p-1}{2}$ com p primo e $p \geq 7$ [33]. Os reticulados D_n rotacionados foram construídos via $\mathbb{Z}$ -módulos de posto n que não são ideais.

Os reticulados D_n rotacionados serão construídos via o subcorpo real maximal $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ dos corpos ciclotômicos $\mathbb{L} = \mathbb{Q}(\zeta_p)$ com p primo e $p \geq 7$. Serão obtidos reticulados D_n rotacionados para $n = \frac{p-1}{2}$ com p primo e $p \geq 7$, isto é, $n = 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \dots$

Sejam p um número primo tal que $p \geq 7$, $\zeta = \zeta_p$ uma raiz p -ésima primitiva da unidade, $\mathbb{L} = \mathbb{Q}(\zeta_p)$ o p -ésimo corpo ciclotômico e $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ seu subcorpo real maximal. Temos que $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{p-1}{2}$.

$$p-1 \begin{pmatrix} \mathbb{Q}(\zeta_p) \\ |2 \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \\ |\frac{p-1}{2} \\ \mathbb{Q} \end{pmatrix}$$

Em [26, 30] são construídos reticulados $\mathbb{Z}^n$ rotacionados através do subcorpo real maximal dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, tomando $\alpha = (1 - \zeta)(1 - \zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$, $\mathcal{A} = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$ e a perturbação do homomorfismo canônico. Nós derivamos reticulados D_n rotacionados como sub-reticulados desses reticulados $\mathbb{Z}^n$ rotacionados.

Para p primo, temos que $\{e_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^{\frac{p-1}{2}}$ é uma $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Proposição 5.2.4. [30] *Sejam $e_n^* = e_n$, $e_j^* = \sum_{i=j}^n e_i$, para $j = 1, \dots, n-1$, uma $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}}$ e $\alpha = 2 - (\zeta + \zeta^{-1})$. Temos que*

$$\frac{1}{p} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_i^* e_j^*) = \delta_{ij},$$

onde δ_{ij} é o delta de Kronecker.

Segue que o reticulado ideal $\Lambda = \frac{1}{\sqrt{p}}\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$ com $\alpha = 2 - (\zeta + \zeta^{-1})$ é um reticulado $\mathbb{Z}^n$ rotacionado, pois uma matriz de Gram para $\frac{1}{\sqrt{p}}\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$ é a matriz identidade e, temos que reticulados com mesma matriz de Gram são equivalentes na métrica euclidiana.

Uma matriz geradora para o reticulado $\frac{1}{\sqrt{p}}\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$M = \frac{1}{\sqrt{p}} T N A, \text{ onde} \quad (5.2.7)$$

$$N = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \text{ e } A = \text{diag}(\sqrt{\sigma_k(\alpha)}).$$

Temos que $MM^t = I_n$, ou seja, a matriz M é uma matriz de rotação que leva a base canônica I_n do $\mathbb{Z}^n$ na base $I_n M$ do reticulado $\frac{1}{\sqrt{p}}\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$.

Seja B uma matriz geradora para o reticulado D_n como em (5.2.6).

Vamos aplicar a matriz de rotação M à matriz geradora B do reticulado D_n e obter um reticulado D_n rotacionado. A proposição seguinte mostra isso.

Proposição 5.2.5. *Considere o $\mathbb{Z}$ -módulo $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ com $\mathbb{Z}$ -base*

$$\{e_1, e_2, \dots, e_{n-1}, -e_1 - 2e_2 - \cdots - 2e_n\}$$

e $\alpha = 2 - e_1$. Temos que o reticulado $\frac{1}{\sqrt{p}}\sigma_{\alpha}(\mathcal{A})$ é um reticulado D_n rotacionado.

Demonstração: Aplicando a matriz de rotação M à matriz B , temos que

$$\begin{aligned}
BM &= \frac{1}{\sqrt{p}} BTNA = \frac{1}{\sqrt{p}} B \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix} A \\
&= \frac{1}{\sqrt{p}} B \begin{pmatrix} \sigma_1(e_1 + \cdots + e_n) & \cdots & \sigma_n(e_1 + \cdots + e_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix} A \\
&= \frac{1}{\sqrt{p}} \begin{pmatrix} \sigma_1(-e_1 - \cdots - e_n - e_2 - \cdots - e_n) & \cdots & \sigma_n(-e_1 - \cdots - e_n - e_2 - \cdots - e_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1} + e_n - e_n) & \cdots & \sigma_n(e_{n-1} + e_n - e_n) \end{pmatrix} A \\
&= \frac{1}{\sqrt{p}} \begin{pmatrix} \sigma_1(-e_1 - 2e_2 - \cdots - 2e_n) & \cdots & \sigma_n(-e_1 - 2e_2 - \cdots - 2e_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix} A.
\end{aligned}$$

Assim, note que uma matriz geradora para o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{A})$ é dada por BM . Como $BM(BM)^t = BB^t$, que é uma matriz de Gram do reticulado D_n , temos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{A})$ é um reticulado D_n rotacionado. $\square$

Proposição 5.2.6. *O $\mathbb{Z}$ -módulo $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$, dado pela proposição anterior, não é ideal de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: É fácil ver que $\{e_1, e_2, \dots, e_{n-1}, 2e_n\}$ é uma outra $\mathbb{Z}$ -base para $\mathcal{A}$. De fato, se $x \in \mathcal{A}$, então existem $a_1, \dots, a_n \in \mathbb{Z}$ tais que $x = a_1(-e_1 - 2e_2 - \cdots - 2e_n) + a_2e_2 + \cdots + a_n e_{n-1} = (a_2 - a_1)e_1 + (a_3 - 2a_1)e_2 + \cdots + (a_n - 2a_1)e_{n-1} - a_1(2e_n) \in \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1} + \mathbb{Z}2e_n$. Agora se $x \in \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1} + \mathbb{Z}2e_n$, então existem $b_1, \dots, b_n \in \mathbb{Z}$ tais que $x = b_1e_1 + b_2e_2 + \cdots + b_{n-1}e_{n-1} + b_n 2e_n = (a_1 - a_n)e_1 + \cdots + (a_{n-1} - 2a_n)e_{n-1} - a_n(-e_1 - 2e_2 - \cdots - 2e_n) \in \mathcal{A}$. Agora, temos que e_n não está em $\mathcal{A}$. De fato, se e_n estivesse em $\mathcal{A}$, teríamos $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$, mas, pela Proposição 2.1.1, $\left| \frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{A}} \right| = 1.1 \cdots 1.2 = 2$. Logo, $e_n \notin \mathcal{A}$. Mostremos que $e_{n-1}e_1$ não está em $\mathcal{A}$. Temos que $e_{n-1}e_1 = e_n + e_{n-2}$. Como $e_{n-2} \in \mathcal{A}$, se

$e_{n-1}e_1 \in \mathcal{A}$, então $e_n = e_{n-1}e_1 - e_{n-2} \in \mathcal{A}$, o que não acontece. Portanto, $\mathcal{A}$ não é ideal de $\mathcal{O}_{\mathbb{K}}$. $\square$

Os reticulados D_n rotacionados obtidos acima possuem diversidade máxima, pois o corpo $\mathbb{K}$ é totalmente real. Vamos calcular a distância produto mínima de tal família de reticulados.

Lema 5.2.1. $|\mathcal{N}_{\mathbb{K}|\mathbb{Q}}(e_1)| = 1$ para $e_1 = \zeta_p + \zeta_p^{-1}$.

Demonstração: Temos que $(\zeta + \zeta^{-1})(-\zeta^{p-1} - \zeta^{p-2} - \dots - \zeta - 1) = 1$. Assim, $\mathcal{N}(\zeta + \zeta^{-1})\mathcal{N}(-\zeta^{p-1} - \zeta^{p-2} - \dots - \zeta - 1) = \mathcal{N}(1) = 1$. Como $e_1 \in \mathcal{O}_{\mathbb{K}}$, segue que $\mathcal{N}(e_1) \in \mathbb{Z}$, logo $|\mathcal{N}(e_1)| = 1$ é a única possibilidade. $\square$

Proposição 5.2.7. Se $\Lambda = \frac{1}{\sqrt{p}}\sigma_{\alpha}(I)$ com α e I como na Proposição 5.2.5, então

$$d_{p,rel}(\Lambda) = 2^{\frac{1-p}{4}} p^{\frac{3-p}{4}}.$$

Demonstração: Primeiro, notamos que como o valor da norma mínima de D_n é $\sqrt{2}$, então devemos dividir a distância produto mínima obtida por $\sqrt{2}^n$. Além disso, como o reticulado D_n -rotacionado obtido é uma versão escalonada de D_n por $1/\sqrt{p}$ devemos dividir a distância produto mínima por $(\sqrt{p})^n$. Temos que $d_p(\sigma_{\alpha}(\mathcal{A})) = \sqrt{\mathcal{N}(\alpha)} \min_{0 \neq y \in \mathcal{A}} |\mathcal{N}(y)| = \sqrt{p}$, pois $\mathcal{N}(\alpha) = p$ e $\min_{0 \neq y \in \mathcal{A}} |\mathcal{N}(y)| = 1$. De fato, temos que $\min_{0 \neq y \in \mathcal{A}} |\mathcal{N}(y)| \geq 1$. Mas $e_1 \in \mathcal{A}$ e $|\mathcal{N}(e_1)| = 1$. Assim,

$$d_{p,rel}\left(\frac{1}{\sqrt{p}}\sigma_{\alpha}(I)\right) = \left(\frac{1}{\sqrt{p}^{\frac{p-1}{2}}}\right) \left(\frac{1}{\sqrt{2}^{\frac{p-1}{2}}}\right) \sqrt{p} = 2^{\frac{1-p}{4}} p^{\frac{3-p}{4}}.$$

$\square$

Observação 5.2.2. A distância produto mínima relativa obtida via o $\mathbb{Z}$ -módulo $\mathcal{A}$ equivale a metade da distância produto mínima que obteríamos se fosse possível construir tal família de reticulados via ideais principais.

A tabela seguinte fornece uma comparação entre a $d_{p,rel}$ e a densidade de centro δ dos reticulados $\mathbb{Z}^n$ rotacionados de [30] e D_n rotacionados construídos anteriormente.

p	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(D_n)$
5	2	0,66870	0,47287	0,25000	-
7	3	0,52275	0,36965	0,12500	0,17677
11	5	0,38321	0,27097	0,03125	0,08838
13	6	0,34344	0,24285	0,01563	0,06250
17	8	0,28952	0,20472	0,00390	0,03125
19	9	0,27187	0,19105	0,00195	0,02209
23	11	0,24045	0,17003	0,00049	0,01105

Tabela 5.5: Distância produto e densidade de centro de $\mathbb{Z}^n$ e D_n - Comparação.

Note que, para $\Lambda = \frac{1}{\sqrt{p}}(\sigma_\alpha(\mathcal{A})) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ e p primo, temos:

$$\lim_{n \rightarrow \infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2} \text{ e } \lim_{n \rightarrow \infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0.$$

Considerando o “trade-off” entre densidade de empacotamento e distância produto mínima relativa, podemos dizer que os reticulados apresentados aqui possuem melhor performance do que os reticulados $\mathbb{Z}^n$ rotacionados de [30].

CAPÍTULO 6

CONSTRUÇÃO DE RETICULADOS UNIMODULARES SOBRE CORPOS TOTALMENTE REAIS

Em [4], foram construídas famílias de reticulados $\mathbb{Z}^n$ rotacionados com diversidade máxima sobre o subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r})$, representando então constelações que são eficientes para o canal Rayleigh com desvanecimento. Neste capítulo, construímos uma família de reticulados unimodulares rotacionados sobre o subcorpo maximal real de $\mathbb{Q}(\zeta_{2^{r \cdot 3.5}})$ com um desempenho melhor para o canal Rayleigh com desvanecimento em comparação à família reproduzida em [4].

O objetivo inicial era a construção de uma família de reticulados $\mathbb{Z}^n$ escalonados e rotacionados com fator de escala $\sqrt{c}$, ou seja, o reticulado ideal $\Lambda = (\mathcal{A}, b_\alpha)$ (sem o fator de

escala) devia satisfazer as seguintes condições: $\det(\Lambda) = 1$, densidade de centro $\delta(\Lambda) = \frac{1}{2^n}$ e norma mínima $\eta = 1$. Assim, pelas Equações (4.2.1), (4.2.2) e (4.2.3), estas condições são dadas por

$$\mathcal{N}(\mathcal{A})^2 \mathcal{N}(\alpha) |d_{\mathbb{K}}| = c^n \quad (6.0.1)$$

$$\frac{t_\alpha^{n/2}}{2^n [|d_{\mathbb{K}}| \mathcal{N}(\alpha)]^{1/2}} = \frac{1}{2^n}. \quad (6.0.2)$$

$$t_\alpha = c. \quad (6.0.3)$$

O reticulado $\Lambda = \mathbb{Z}^n$ não é o único reticulado que satisfaz $\det(\Lambda) = 1$, $\delta(\Lambda) = \frac{1}{2^n}$ e $\eta = 1$. Veremos que reticulados que sejam soma direta de $\mathbb{Z}^n$ com cópias de E_8 também satisfazem as três condições.

O método que apresentaremos a seguir baseia-se na construção de reticulados ideais via o anel de inteiros algébricos do corpo $\mathbb{Q}(\zeta_{2^r.3.5} + \zeta_{2^r.3.5}^{-1})$.

Construção

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{2^r.3.5} + \zeta_{2^r.3.5}^{-1})$ o subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r.3.5})$, onde r é um inteiro positivo, $r \geq 1$ e $\zeta_{2^r.3.5}$ é uma raiz primitiva $2^r.3.5$ -ésima da unidade. Temos que $n = [\mathbb{K} : \mathbb{Q}] = 2^{r+1}$ e pela Proposição 1.4.2, $|d_{\mathbb{K}}| = 2^{(r-1)2^{r+1}} 3^{2^r} 5^{3 \cdot 2^{r-1}}$. Assumindo $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$ e trabalhando nas três primeiras dimensões, ou seja, para $n = 4$, $n = 8$ e $n = 16$, observamos algumas particularidades nos valores de $\mathcal{N}(\alpha)$ e c que satisfazem as Equações (6.0.1), (6.0.2) e (6.0.3), conforme Tabela 6.1.

n	$\mathcal{N}(\alpha)$	c
4	45	15
8	2025	30
16	4100625	60

Tabela 6.1: Parâmetros do reticulado unimodular rotacionado - dimensões 4, 8 e 16.

A tabela acima sugere que para o caso geral ($n = 2^{r+1}$) tenhamos

n	$\mathcal{N}(\alpha)$	c
2^{r+1}	$3^{2^r} 5^{2^{r-1}}$	$2^{r-1} \cdot 3 \cdot 5$

Tabela 6.2: Parâmetros do reticulado unimodular rotacionado - caso geral.

Nosso objetivo agora é encontrar um elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ totalmente real e totalmente positivo que satisfaça a tabela acima. Assim, implementamos um algoritmo para encontrar α , e como a complexidade do algoritmo está relacionada ao grau da extensão $\mathbb{Q}(\zeta_{2^r \cdot 3 \cdot 5} + \zeta_{2^r \cdot 3 \cdot 5}^{-1})$ sobre $\mathbb{Q}$ que é $n = 2^{r+1}$, implementamos para os casos $n = 4, n = 8$ e $n = 16$, e selecionamos valores de α que sugerem um α que contemple o caso geral, conforme Tabela 6.3.

n	α	$\mathcal{N}(\alpha)$
4	$2 - 2(\zeta_{30} + \zeta_{30}^{-1}) - (\zeta_{30}^2 + \zeta_{30}^{-2}) + 3(\zeta_{30}^3 + \zeta_{30}^{-3})$	45
8	$2 - 2(\zeta_{60}^2 + \zeta_{60}^{-2}) - (\zeta_{60}^4 + \zeta_{60}^{-4}) + 3(\zeta_{60}^6 + \zeta_{60}^{-6})$	2025
16	$2 - 2(\zeta_{120}^4 + \zeta_{120}^{-4}) - (\zeta_{120}^8 + \zeta_{120}^{-8}) + 3(\zeta_{120}^{12} + \zeta_{120}^{-12})$	4100625

Tabela 6.3: Elemento α do reticulado ideal unimodular - dimensões 4, 8 e 16.

A tabela sugere que para o caso geral seja escolhido

$$\alpha = 2 - 2(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{3 \cdot 2^{r-1}} + \zeta^{-3 \cdot 2^{r-1}})$$

onde $\zeta = \zeta_{2^r \cdot 3 \cdot 5}$.

Proposição 6.0.8. *Seja $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, onde $\zeta = \zeta_{2^r.3.5}$, e considere $e_0 = 1$ e $e_i = \zeta^i + \zeta^{-i}$, para $i = 1, 2, \dots, 2^{r+1} - 1$, e $\alpha = 2 - 2(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{2^{r-1}.3} + \zeta^{-2^{r-1}.3})$.*

$$1. \text{ Se } i = 0, 1, \dots, 2^{r+1} - 1, \text{ então } b_\alpha(e_i, e_i) = \begin{cases} 2^{r-1}.3.5, & \text{se } i \in \{0, 2^{r-2}, 2^r, 2^{r-2}.7\}. \\ 2^{r-1}.3^2.5, & \text{se } i \in \{2^{r-2}.3, 2^{r-2}.5\} \\ 2^r.3.5, & \text{caso contrário.} \end{cases}$$

$$2. \text{ Se } i \neq 0, \text{ então } b_\alpha(e_i, e_0) = \begin{cases} -2^{r-1}.3.5, & \text{se } i = 2^{r-1} \\ 2^{r-1}.3.5, & \text{se } i = 2^{r-1}.3 \\ 0, & \text{caso contrário.} \end{cases}$$

3. Se $i \neq 0, j \neq 0$ e $i \neq j$, então:

$$b_\alpha(e_i, e_j) = \begin{cases} -2^r.3.5, & \text{se } (i+j, |i-j|) = (2^{r+1}, 2^{r-1}) \\ -2^{r-1}.3.5, & \text{se } i+j \in \{2^{r-1}, 2^{r-1}.7\} \text{ ou} \\ & (i+j, |i-j|) \in \{(2^r, 2^{r-1}), (2^r.3, 2^{r-1})\} \text{ ou} \\ & (i+j = 2^{r+1} \text{ e } |i-j| \neq 2^{r-1}, 2^{r-1}.3) \text{ ou} \\ & (|i-j| = 2^{r-1} \text{ e } i+j \neq 2^{r-1}.3, 2^{r+1}, 2^{r-1}.5) \\ 2^{r-1}.3.5, & \text{se } (i+j = 2^{r-1}.3 \text{ e } |i-j| \neq 2^{r-1}) \text{ ou} \\ & (i+j = 2^{r-1}.5 \text{ e } |i-j| \neq 2^{r-1}) \text{ ou} \\ & (|i-j| = 2^{r-1}.3 \text{ e } i+j \neq 2^{r+1}) \\ 0, & \text{caso contrário} \end{cases}$$

Demonstração:

Para simplificar notação chamaremos $Tr_{\mathbb{K}/\mathbb{Q}} = Tr$. Pelo Corolário 1.4.5, como $Tr(\zeta^{2^{r-1}} + \zeta^{-(2^{r-1})}) = -2^{r-1}$, $Tr(\zeta^{2^r} + \zeta^{-2^r}) = 2^{r-1}$ e $Tr(\zeta^{2^{r-1}.3} + \zeta^{-2^{r-1}.3}) = 2^r$, segue que

$$\begin{aligned} b_\alpha(e_0, e_0) &= Tr(\alpha e_0 e_0) = Tr(\alpha) = \\ &= Tr(2 - 2(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{3.2^{r-1}} + \zeta^{-3.2^{r-1}})) = \\ &= Tr(2) - 2Tr(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - Tr(\zeta^{2^r} + \zeta^{-2^r}) + 3Tr(\zeta^{2^{r-1}.3} + \zeta^{-2^{r-1}.3}) = \\ &= 2.2^{r+1} - 2(-2^{r-1}) - 2^{r-1} + 3.2^r = 2^{r-1}.3.5 \end{aligned}$$

Pelo Corolário 1.4.5 temos que

$$Tr(\zeta^{2i} + \zeta^{-2i}) = \begin{cases} -2^{r-1}, & \text{se } i = 2^{r-2} \\ 2^{r+1}, & \text{se } i = 2^{r-2}.5 \\ 2^{r-1}, & \text{se } i = 2^{r-1} \text{ ou } i = 2^r \\ -2^r, & \text{se } i = 2^{r-1}.3 \\ -2^{r-1}, & \text{se } i = 2^{r-2}.7 \\ 2^r, & \text{se } i = 2^{r-2}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}+2i} + \zeta^{-(2^{r-1}+2i)}) = \begin{cases} 2^r, & \text{se } i = 2^{r-1} \\ 2^{r+1}, & \text{se } i = 2^r \\ 2^{r-1}, & \text{se } i = 2^{r-2} \text{ ou } i = 2^{r-2}.3 \text{ ou } i = 2^{r-2}.7 \\ -2^r, & \text{se } i = 2^{r-2}.5 \\ -2^{r-1}, & \text{se } i = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}-2i} + \zeta^{-(2^{r-1}-2i)}) = \begin{cases} -2^{r-1}, & \text{se } i = 2^{r-1} \\ 2^{r+2}, & \text{se } i = 2^{r-2} \\ 2^r, & \text{se } i = 2^r \\ 2^{r+1}, & \text{se } i = 2^{r-1}.3 \\ 2^{r-1}, & \text{se } i = 2^{r-2}.3 \text{ ou } i = 2^{r-2}.5 \\ -2^r, & \text{se } i = 2^{r-2}.7 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r+2i} + \zeta^{-(2^r+2i)}) = \begin{cases} 2^{r-1}, & \text{se } i = 2^{r-1} \text{ ou } i = 2^{r-1}.3 \\ 2^r, & \text{se } i = 2^{r-2} \text{ ou } i = 2^{r-2}.7 \\ -2^r, & \text{se } i = 2^r \\ 2^{r+1}, & \text{se } i = 2^{r-2}.3 \\ -2^{r-1}, & \text{se } i = 2^{r-2}.5 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r-2i} + \zeta^{-(2^r-2i)}) = \begin{cases} 2^{r+2}, & \text{se } i = 2^{r-1} \\ -2^{r-1}, & \text{se } i = 2^{r-2} \text{ ou } i = 2^{r-2}.3 \\ 2^{r-1}, & \text{se } i = 2^r \text{ ou } i = 2^{r-1}.3 \\ 2^r, & \text{se } i = 2^{r-2}.5 \\ 2^{r+1}, & \text{se } i = 2^{r-2}.7 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3+2i} + \zeta^{-(2^{r-1}.3+2i)}) = \begin{cases} 2^{r+1}, & \text{se } i = 2^{r-1} \\ -2^{r-1}, & \text{se } i = 2^r \\ 2^r, & \text{se } i = 2^{r-1}.3 \\ 2^{r-1}, & \text{se } i = 2^{r-2} \text{ ou } i = 2^{r-2}.5 \\ -2^r, & \text{se } i = 2^{r-2}.3 \\ -2^{r+1}, & \text{se } i = 2^{r-2}.7 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3-2i} + \zeta^{-(2^{r-1}.3-2i)}) = \begin{cases} 2^{r+2}, & \text{se } i = 2^{r-2}.3 \\ -2^{r-1}, & \text{se } i = 2^{r-1} \text{ ou } i = 2^r \\ 2^r, & \text{se } i = 2^{r-1}.3 \\ 2^{r-1}, & \text{se } i = 2^{r-2} \text{ ou } i = 2^{r-2}.5 \text{ ou } i = 2^{r-2}.7 \\ 0, & \text{caso contrário} \end{cases}$$

Assim, se $i \neq 0$

$$\begin{aligned}
b_\alpha(e_i, e_i) &= Tr(\alpha e_i e_i) = Tr(\alpha e_i^2) = \\
&= Tr([2 - 2(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{3 \cdot 2^{r-1}} + \zeta^{-3 \cdot 2^{r-1}})][\zeta^{2i} + \zeta^{-2i} + 2]) = \\
&= Tr(2(\zeta^{2i} + \zeta^{-2i}) + 4 - 2(\zeta^{2^{r-1}+2i} + \zeta^{-(2^{r-1}+2i)}) - 2(\zeta^{2^{r-1}-2i} + \zeta^{-(2^{r-1}-2i)}) \\
&\quad - 4(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r+2i} + \zeta^{-(2^r+2i)}) - (\zeta^{2^r-2i} + \zeta^{-(2^r-2i)}) \\
&\quad - 2(\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{2^{r-1} \cdot 3 + 2i} + \zeta^{-(2^{r-1} \cdot 3 + 2i)}) + 3(\zeta^{2^{r-1} \cdot 3 - 2i} + \zeta^{-(2^{r-1} \cdot 3 - 2i)}) \\
&\quad + 6(\zeta^{2^{r-1} \cdot 3} + \zeta^{-2^{r-1} \cdot 3})) = \\
&= 2Tr(\zeta^{2i} + \zeta^{-2i}) + Tr(4) - 2Tr(\zeta^{2^{r-1}+2i} + \zeta^{-(2^{r-1}+2i)}) - 2Tr(\zeta^{2^{r-1}-2i} + \zeta^{-(2^{r-1}-2i)}) \\
&\quad - 4Tr(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - Tr(\zeta^{2^r+2i} + \zeta^{-(2^r+2i)}) - Tr(\zeta^{2^r-2i} + \zeta^{-(2^r-2i)}) \\
&\quad - 2Tr(\zeta^{2^r} + \zeta^{-2^r}) + 3Tr(\zeta^{2^{r-1} \cdot 3 + 2i} + \zeta^{-(2^{r-1} \cdot 3 + 2i)}) + 3Tr(\zeta^{2^{r-1} \cdot 3 - 2i} + \zeta^{-(2^{r-1} \cdot 3 - 2i)}) \\
&\quad + 6Tr(\zeta^{2^{r-1} \cdot 3} + \zeta^{-2^{r-1} \cdot 3})) = \\
&= \begin{cases} 2^{r-1} \cdot 3 \cdot 5, & \text{se } i \in \{2^{r-2}, 2^r, 2^{r-2} \cdot 7\}. \\ 2^{r-1} \cdot 3^2 \cdot 5, & \text{se } i \in \{2^{r-2} \cdot 3, 2^{r-2} \cdot 5\} \\ 2^r \cdot 3 \cdot 5, & \text{caso contrário.} \end{cases}
\end{aligned}$$

Pelo Corolário 1.4.5, temos que

$$Tr(\zeta^i + \zeta^{-i}) = \begin{cases} -2^{r-1}, & \text{se } i = 2^{r-1} \\ 2^{r-1}, & \text{se } i = 2^r \\ 2^r, & \text{se } i = 2^{r-1} \cdot 3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}+i} + \zeta^{-(2^{r-1}+i)}) = \begin{cases} 2^{r-1}, & \text{se } i = 2^{r-1} \text{ ou } i = 2^{r-1} \cdot 3 \\ 2^r, & \text{se } i = 2^r \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}-i} + \zeta^{-(2^{r-1}-i)}) = \begin{cases} 2^{r+2}, & \text{se } i = 2^{r-1} \\ -2^{r-1}, & \text{se } i = 2^r \\ 2^{r-1}, & \text{se } i = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r+i} + \zeta^{-(2^r+i)}) = \begin{cases} 2^r, & \text{se } i = 2^{r-1} \\ 2^{r-1}, & \text{se } i = 2^r \\ 2^{r+1}, & \text{se } i = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r-i} + \zeta^{-(2^r-i)}) = \begin{cases} -2^{r-1}, & \text{se } i = 2^{r-1} \text{ ou } i = 2^{r-1}.3 \\ 2^{r+2}, & \text{se } i = 2^r \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3+i} + \zeta^{-(2^{r-1}.3+i)}) = \begin{cases} 2^{r-1}, & \text{se } i = 2^{r-1} \\ 2^{r+1}, & \text{se } i = 2^r \\ -2^r, & \text{se } i = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3-i} + \zeta^{-(2^{r-1}.3-i)}) = \begin{cases} 2^{r+2}, & \text{se } i = 2^{r-1}.3 \\ -2^{r-1}, & \text{se } i = 2^r \\ 2^{r-1}, & \text{se } i = 2^{r-1} \\ 0, & \text{caso contrário} \end{cases}$$

Assim, se $i \neq 0$

$$\begin{aligned}
b_\alpha(e_i, e_0) &= Tr(\alpha e_i e_0) = Tr(\alpha e_i) = \\
&= Tr([2 - 2(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{3 \cdot 2^{r-1}} + \zeta^{-3 \cdot 2^{r-1}})][\zeta^i + \zeta^{-i}]) = \\
&= Tr(2(\zeta^i + \zeta^{-i}) - 2(\zeta^{2^{r-1}+i} + \zeta^{-(2^{r-1}+i)}) - 2(\zeta^{2^{r-1}-i} + \zeta^{-(2^{r-1}-i)}) \\
&\quad - (\zeta^{2^r+i} + \zeta^{-(2^r+i)}) - (\zeta^{2^r-i} + \zeta^{-(2^r-i)}) + 3(\zeta^{2^{r-1} \cdot 3+i} + \zeta^{-(2^{r-1} \cdot 3+i)}) \\
&\quad + 3(\zeta^{2^{r-1} \cdot 3-i} + \zeta^{-(2^{r-1} \cdot 3-i)})) = \\
&= 2Tr(\zeta^i + \zeta^{-i}) - 2Tr(\zeta^{2^{r-1}+i} + \zeta^{-(2^{r-1}+i)}) - 2Tr(\zeta^{2^{r-1}-i} + \zeta^{-(2^{r-1}-i)}) \\
&\quad - Tr(\zeta^{2^r+i} + \zeta^{-(2^r+i)}) - Tr(\zeta^{2^r-i} + \zeta^{-(2^r-i)}) + 3Tr(\zeta^{2^{r-1} \cdot 3+i} + \zeta^{-(2^{r-1} \cdot 3+i)}) \\
&\quad + 3Tr(\zeta^{2^{r-1} \cdot 3-i} + \zeta^{-(2^{r-1} \cdot 3-i)}) = \\
&= \begin{cases} -2^{r-1} \cdot 3 \cdot 5, & \text{se } i = 2^{r-1} \\ 2^{r-1} \cdot 3 \cdot 5, & \text{se } i = 2^{r-1} \cdot 3 \\ 0, & \text{caso contrário.} \end{cases}
\end{aligned}$$

Para $i, j \neq 0$, $i \neq j$, pelo Corolário 1.4.5 temos que

$$Tr(\zeta^{i+j} + \zeta^{-(i+j)}) = \begin{cases} -2^{r-1}, & \text{se } i+j = 2^{r-1} \text{ ou } i+j = 2^{r-1} \cdot 7 \\ 2^{r-1}, & \text{se } i+j = 2^r \text{ ou } i+j = 2^{r+1} \\ 2^r, & \text{se } i+j = 2^{r-1} \cdot 3 \\ 2^{r+1}, & \text{se } i+j = 2^{r-1} \cdot 5 \\ -2^r, & \text{se } i+j = 2^r \cdot 3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}+(i+j)} + \zeta^{-(2^{r-1}+(i+j))}) = \begin{cases} 2^{r-1}, & \text{se } i+j = 2^{r-1} \text{ ou } i+j = 2^{r-1} \cdot 3 \\ & \text{ou } i+j = 2^{r-1} \cdot 7 \\ 2^r, & \text{se } i+j = 2^r \\ 2^{r+1}, & \text{se } i+j = 2^{r+1} \\ -2^r, & \text{se } i+j = 2^{r-1} \cdot 5 \\ -2^{r-1}, & \text{se } i+j = 2^r \cdot 3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}-(i+j)} + \zeta^{-(2^{r-1}-(i+j))}) = \begin{cases} 2^{r+2}, & \text{se } i+j = 2^{r-1} \\ -2^{r-1}, & \text{se } i+j = 2^r \\ 2^{r-1}, & \text{se } i+j = 2^{r-1}.3 \text{ ou } i+j = 2^{r-1}.5 \\ 2^r, & \text{se } i+j = 2^{r+1} \\ 2^{r+1}, & \text{se } i+j = 2^r.3 \\ -2^r, & \text{se } i+j = 2^{r-1}.7 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r+(i+j)} + \zeta^{-(2^r+(i+j))}) = \begin{cases} 2^r, & \text{se } i+j = 2^{r-1} \text{ ou } i+j = 2^{r-1}.7 \\ 2^{r-1}, & \text{se } i+j = 2^r \text{ ou } i+j = 2^r.3 \\ 2^{r+1}, & \text{se } i+j = 2^{r-1}.3 \\ -2^{r-1}, & \text{se } i+j = 2^{r-1}.5 \\ -2^r, & \text{se } i+j = 2^{r+1} \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r-(i+j)} + \zeta^{-(2^r-(i+j))}) = \begin{cases} -2^{r-1}, & \text{se } i+j = 2^{r-1} \text{ ou } i+j = 2^{r-1}.3 \\ 2^{r+2}, & \text{se } i+j = 2^r \\ 2^r, & \text{se } i+j = 2^{r-1}.5 \\ 2^{r-1}, & \text{se } i+j = 2^{r+1} \text{ ou } i+j = 2^r.3 \\ 2^{r+1}, & \text{se } i+j = 2^{r-1}.7 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3+(i+j)} + \zeta^{-(2^{r-1}.3+(i+j))}) = \begin{cases} 2^{r-1}, & \text{se } i+j = 2^{r-1} \text{ ou } i+j = 2^{r-1}.5 \\ 2^{r+1}, & \text{se } i+j = 2^r \\ -2^r, & \text{se } i+j = 2^{r-1}.3 \\ -2^{r-1}, & \text{se } i+j = 2^{r+1} \\ 2^r, & \text{se } i+j = 2^r.3 \\ -2^{r+1}, & \text{se } i+j = 2^{r-1}.7 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3-(i+j)} + \zeta^{-(2^{r-1}.3-(i+j))}) = \begin{cases} 2^{r-1}, & \text{se } i+j = 2^{r-1} \text{ ou } i+j = 2^{r-1}.5 \\ & \text{ou } i+j = 2^{r-1}.7 \\ -2^{r-1}, & \text{se } i+j = 2^r \text{ ou } i+j = 2^{r+1} \\ 2^{r+2}, & \text{se } i+j = 2^{r-1}.3 \\ 2^r, & \text{se } i+j = 2^r.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{i-j} + \zeta^{-(i-j)}) = \begin{cases} -2^{r-1}, & \text{se } |i-j| = 2^{r-1} \\ 2^{r-1}, & \text{se } |i-j| = 2^r \\ 2^r, & \text{se } |i-j| = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}+(i-j)} + \zeta^{-(2^{r-1}+(i-j))}) = \begin{cases} 2^{r-1}, & \text{se } |i-j| = 2^{r-1} \\ 2^r, & \text{se } |i-j| = 2^r \\ 2^{r-1}, & \text{se } |i-j| = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}-(i-j)} + \zeta^{-(2^{r-1}-(i-j))}) = \begin{cases} 2^{r+2}, & \text{se } |i-j| = 2^{r-1} \\ -2^{r-1}, & \text{se } |i-j| = 2^r \\ 2^{r-1}, & \text{se } |i-j| = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r+(i-j)} + \zeta^{-(2^r+(i-j))}) = \begin{cases} 2^r, & \text{se } |i-j| = 2^{r-1} \\ 2^{r-1}, & \text{se } |i-j| = 2^r \\ 2^{r+1}, & \text{se } |i-j| = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^r-(i-j)} + \zeta^{-(2^r-(i-j))}) = \begin{cases} -2^{r-1}, & \text{se } |i-j| = 2^{r-1} \text{ ou } |i-j| = 2^{r-1}.3 \\ 2^{r+2}, & \text{se } |i-j| = 2^r \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3+(i-j)} + \zeta^{-(2^{r-1}.3+(i-j))}) = \begin{cases} 2^{r-1}, & \text{se } |i-j| = 2^{r-1} \\ 2^{r+1}, & \text{se } |i-j| = 2^r \\ -2^r, & \text{se } |i-j| = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

$$Tr(\zeta^{2^{r-1}.3-(i-j)} + \zeta^{-(2^{r-1}.3-(i-j))}) = \begin{cases} 2^{r-1}, & \text{se } |i-j| = 2^{r-1} \\ -2^{r-1}, & \text{se } |i-j| = 2^r \\ 2^{r+2}, & \text{se } |i-j| = 2^{r-1}.3 \\ 0, & \text{caso contrário} \end{cases}$$

Assim,

$$\begin{aligned} b_\alpha(e_i, e_j) &= Tr(\alpha e_i e_j) = \\ &= Tr([2 - 2(\zeta^{2^{r-1}} + \zeta^{-2^{r-1}}) - (\zeta^{2^r} + \zeta^{-2^r}) + 3(\zeta^{3.2^{r-1}} + \zeta^{-3.2^{r-1}})][\zeta^i + \zeta^{-i}][\zeta^j + \zeta^{-j}]) = \\ &= Tr(2(\zeta^{i+j} + \zeta^{-(i+j)}) - 2(\zeta^{2^{r-1}+(i+j)} + \zeta^{-(2^{r-1}+(i+j))}) - 2(\zeta^{2^{r-1}-(i+j)} + \zeta^{-(2^{r-1}-(i+j))}) \\ &\quad - (\zeta^{2^r+(i+j)} + \zeta^{-(2^r+(i+j))}) - (\zeta^{2^r-(i+j)} + \zeta^{-(2^r-(i+j))}) \\ &\quad + 3(\zeta^{2^{r-1}.3+(i+j)} + \zeta^{-(2^{r-1}.3+(i+j))}) + 3(\zeta^{2^{r-1}.3-(i+j)} + \zeta^{-(2^{r-1}.3-(i+j))})) \\ &\quad + 2(\zeta^{i-j} + \zeta^{-(i-j)}) - 2(\zeta^{2^{r-1}+(i-j)} + \zeta^{-(2^{r-1}+(i-j))}) \\ &\quad - 2(\zeta^{2^{r-1}-(i-j)} + \zeta^{-(2^{r-1}-(i-j))}) - (\zeta^{2^r+(i-j)} + \zeta^{-(2^r+(i-j))}) \\ &\quad - (\zeta^{2^r-(i-j)} + \zeta^{-(2^r-(i-j))}) + 3(\zeta^{2^{r-1}.3+(i-j)} + \zeta^{-(2^{r-1}.3+(i-j))}) \\ &\quad + 3(\zeta^{2^{r-1}.3-(i-j)} + \zeta^{-(2^{r-1}.3-(i-j))}) = \\ &= 2Tr(\zeta^{i+j} + \zeta^{-(i+j)}) - 2Tr(\zeta^{2^{r-1}+(i+j)} + \zeta^{-(2^{r-1}+(i+j))}) - 2Tr(\zeta^{2^{r-1}-(i+j)} + \zeta^{-(2^{r-1}-(i+j))}) \\ &\quad - Tr(\zeta^{2^r+(i+j)} + \zeta^{-(2^r+(i+j))}) - Tr(\zeta^{2^r-(i+j)} + \zeta^{-(2^r-(i+j))}) \\ &\quad + 3Tr(\zeta^{2^{r-1}.3+(i+j)} + \zeta^{-(2^{r-1}.3+(i+j))}) + 3Tr(\zeta^{2^{r-1}.3-(i+j)} + \zeta^{-(2^{r-1}.3-(i+j))}) \\ &\quad + 2Tr(\zeta^{i-j} + \zeta^{-(i-j)}) - 2Tr(\zeta^{2^{r-1}+(i-j)} + \zeta^{-(2^{r-1}+(i-j))}) \\ &\quad - 2Tr(\zeta^{2^{r-1}-(i-j)} + \zeta^{-(2^{r-1}-(i-j))}) - Tr(\zeta^{2^r+(i-j)} + \zeta^{-(2^r+(i-j))}) \\ &\quad - Tr(\zeta^{2^r-(i-j)} + \zeta^{-(2^r-(i-j))}) + 3Tr(\zeta^{2^{r-1}.3+(i-j)} + \zeta^{-(2^{r-1}.3+(i-j))}) \\ &\quad + 3Tr(\zeta^{2^{r-1}.3-(i-j)} + \zeta^{-(2^{r-1}.3-(i-j))}) = \end{aligned}$$

$$= \left\{ \begin{array}{ll} -2^r.3.5, & \text{se } (i+j, |i-j|) = (2^{r+1}, 2^{r-1}) \\ -2^{r-1}.3.5, & \text{se } i+j \in \{2^{r-1}, 2^{r-1}.7\} \text{ ou} \\ & (i+j, |i-j|) \in \{(2^r, 2^{r-1}), (2^r.3, 2^{r-1})\} \text{ ou} \\ & (i+j = 2^{r+1} \text{ e } |i-j| \neq 2^{r-1}, 2^{r-1}.3) \text{ ou} \\ & (|i-j| = 2^{r-1} \text{ e } i+j \neq 2^{r-1}.3, 2^{r+1}, 2^{r-1}.5) \\ 2^{r-1}.3.5, & \text{se } (i+j = 2^{r-1}.3 \text{ e } |i-j| \neq 2^{r-1}) \text{ ou} \\ & (i+j = 2^{r-1}.5 \text{ e } |i-j| \neq 2^{r-1}) \text{ ou} \\ & (|i-j| = 2^{r-1}.3 \text{ e } i+j \neq 2^{r+1}) \\ 0, & \text{caso contrário} \end{array} \right.$$

o que conclui a demonstração. $\square$

Corolário 6.0.1. *Os reticulados $\frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{A})$ e $\frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{A})$, possuem matrizes de Gram*

$$\begin{pmatrix} 1 & -1 & 0 & 1 \\ -1 & 2 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 2 \end{pmatrix} \text{ e } \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 2 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 3 & 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 3 & 0 & -1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 1 \end{pmatrix},$$

respectivamente.

Demonstração: Se $\hat{M}$ é uma matriz geradora para $\sigma_\alpha(\mathcal{A})$ com respectiva matriz de Gram $\hat{G} = (\hat{g}_{ij})_{j=1}^n$ então pela Observação 3.3.1 temos que

$$\hat{g}_{ij} = b_\alpha(e_i, e_j) = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha e_i e_j).$$

As matrizes de Gram dos reticulados $\frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{A})$ e $\frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{A})$ são dadas respectivamente por

$$G_1 = \left(\frac{1}{\sqrt{15}} \hat{M} \right) \left(\frac{1}{\sqrt{15}} \hat{M} \right)^t = \frac{1}{15} \hat{M} \hat{M}^t = \frac{1}{15} \hat{G},$$

$$G_2 = \left(\frac{1}{\sqrt{30}} \hat{M} \right) \left(\frac{1}{\sqrt{30}} \hat{M} \right)^t = \frac{1}{30} \hat{M} \hat{M}^t = \frac{1}{30} \hat{G},$$

e pela Proposição 6.0.8 segue o resultado. $\square$

Corolário 6.0.2. *O reticulado $\frac{1}{\sqrt{2^{r-1} \cdot 3 \cdot 5}} \sigma_\alpha(\mathcal{A})$, $r \geq 3$, possui matriz de Gram, na forma genérica, dada por*

$$G = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 & -1 & 0 & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 & -1 \\ 0 & 2 & & & & 0 & & & & & 0 & & & & & 0 \\ \vdots & & 2 & 0 & -1 & & & -1 & 0 & 1 & & & & & 1 & 0 & -1 \\ \vdots & & 0 & 1 & 0 & & & 0 & 0 & 0 & & & & & 0 & 0 & 0 \\ \vdots & & -1 & 0 & 2 & & & 1 & 0 & -1 & & & & & -1 & 0 & 1 \\ 0 & & & & & 2 & 0 & 1 & & & -1 & 0 & -1 & & & & 0 \\ -1 & 0 & & & & 0 & 3 & 0 & & & 0 & -2 & 0 & & & 0 & 1 \\ 0 & & & & & 1 & 0 & 2 & & & -1 & 0 & -1 & & & & 0 \\ \vdots & & & & & & & & 2 & 0 & -1 & & & & & & \vdots \\ \vdots & & -1 & 0 & 1 & & & 0 & 1 & 0 & & & & & -1 & 0 & 1 \\ \vdots & & 0 & 0 & 0 & & & -1 & 0 & 2 & & & & & 1 & 0 & -1 \\ \vdots & & 1 & 0 & -1 & & & & & & 2 & 0 & 1 & & & & 0 \\ 0 & & & & & -1 & 0 & -1 & & & 0 & 3 & 0 & & & 0 & -1 \\ 1 & 0 & & & & 0 & -2 & 0 & & & 1 & 0 & 2 & & & 0 & 0 \\ 0 & & & & & -1 & 0 & -1 & & & & & & 2 & 0 & -1 \\ \vdots & & 1 & 0 & -1 & & & -1 & 0 & 1 & & & & & 0 & 1 & 0 \\ \vdots & & 0 & 0 & 0 & & & 0 & 0 & 0 & & & & & -1 & 0 & 2 \\ \vdots & & -1 & 0 & 1 & & & 1 & 0 & -1 & & & & & & & \vdots \\ 0 & & & & & & & 0 & & & 0 & & & & & & 0 \\ -1 & 0 & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 & -1 & 0 & \cdots & \cdots & 0 & 2 \end{bmatrix}$$

Demonstração: Se $\hat{M}$ é uma matriz geradora para $\sigma_\alpha(\mathcal{A})$ com respectiva matriz de Gram $\hat{G} = (\hat{g}_{ij})_{j=1}^n$ então pela Observação 3.3.1 temos que

$$\hat{g}_{ij} = b_\alpha(e_i, e_j) = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha e_i e_j).$$

A matriz de Gram do reticulado $\frac{1}{\sqrt{2^{r-1} \cdot 3.5}} \sigma_\alpha(\mathcal{A})$ é dada por

$$G = \left(\frac{1}{\sqrt{2^{r-1} \cdot 3.5}} \hat{M} \right) \left(\frac{1}{\sqrt{2^{r-1} \cdot 3.5}} \hat{M} \right)^t = \frac{1}{2^{r-1} \cdot 3.5} \hat{M} \hat{M}^t = \frac{1}{2^{r-1} \cdot 3.5} \hat{G},$$

e pela Proposição 6.0.8 segue o resultado. $\square$

Observação 6.0.3. *A fim de que não haja dúvida em relação à matriz de Gram, na forma genérica, dada no Corolário 6.0.2 exibimos abaixo os casos $r = 3$ (dimensão 16) e $r = 4$ (dimensão 32).*

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

6.1 Reticulados $\mathbb{Z}^4$ e $\mathbb{Z}^8$ rotacionados

Proposição 6.1.1. *Para $r = 1$ e $r = 2$ o reticulado $\frac{1}{\sqrt{2^{r-1} \cdot 3 \cdot 5}} \sigma_\alpha(\mathcal{A})$ é uma versão rotacional do reticulado $\mathbb{Z}^{2^{r+1}}$.*

Demonstração: Para $r = 1$, pelo Corolário 6.0.1, o reticulado ideal $\frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{A})$, para $\alpha = 2 - 2(\zeta_{30} + \zeta_{30}^{-1}) - (\zeta_{30}^2 + \zeta_{30}^{-2}) + 3(\zeta_{30}^3 + \zeta_{30}^{-3})$, obtido via o corpo $\mathbb{K} = \mathbb{Q}(\zeta_{30} + \zeta_{30}^{-1})$, possui matriz de Gram dada por

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

Pelo Algoritmo 4.1, obtemos uma matriz

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

que possui entradas inteiras e determinante igual a 1, tal que

$$AGA^t = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

logo pela Proposição 2.1.2, segue que $\Lambda = \sigma_\alpha(\mathcal{A})$ é uma versão escalonada e rotacionada do reticulado $\mathbb{Z}^4$, com fator de escala $\sqrt{15}$.

Para $r = 2$, pelo Corolário 6.0.1, o reticulado ideal $\frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{A})$, para $\alpha = 2 - 2(\zeta_{60}^2 + \zeta_{60}^{-2}) - (\zeta_{60}^4 + \zeta_{60}^{-4}) + 3(\zeta_{60}^6 + \zeta_{60}^{-6})$, obtido via o corpo $\mathbb{K} = \mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$,

possui matriz de Gram dada por

$$G = \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 2 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 3 & 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 3 & 0 & -1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 1 \end{pmatrix}.$$

Pelo Algoritmo 4.1, obtemos uma matriz

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

que possui entradas inteiras e determinante igual a -1 , tal que

$$AGA^t = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

logo pela Proposição 2.1.2, segue que $\Lambda = \sigma_\alpha(\mathcal{A})$ é uma versão escalonada e rotacionada do reticulado $\mathbb{Z}^8$, com fator de escala $\sqrt{30}$.

6.1.1 Distância produto mínima

Para o reticulado Λ ($\mathbb{Z}^4$ rotacionado), pela Proposição 4.2.1 temos que

$$\det(\Lambda) = 15^4 \det(\mathbb{Z}^4) = 15^4 1 = 15^4,$$

e

$$\eta_1 = 15 \quad \eta_2 = 15.1 = 15$$

onde η_1 e η_2 são as normas mínimas de Λ e $\mathbb{Z}^4$, respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt[4]{d_{p,min}(\Lambda)} = \frac{1}{\sqrt{15}} \sqrt[8]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{15}} \sqrt[8]{\frac{15^4}{2^2 3^2 5^3}} = 0.41553$$

Para o reticulado Λ ($\mathbb{Z}^8$ rotacionado), temos que

$$\det(\Lambda) = 30^8 \det(\mathbb{Z}^8) = 30^8 1 = 30^8,$$

e

$$\eta_1 = 30 \quad \eta_2 = 30.1 = 30$$

onde η_1 e η_2 são as normas mínimas de Λ e $\mathbb{Z}^8$, respectivamente. Assim, pela Definição 3.3.5 segue que

$$\sqrt[8]{d_{p,min}(\Lambda)} = \frac{1}{\sqrt{30}} \sqrt[16]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{30}} \sqrt[16]{\frac{30^8}{2^8 3^4 5^6}} = 0.29382$$

6.1.2 Distância produto mínima - Comparação com outras construções

Usando a Tabela 3.8, temos condições de comparar a distância produto mínima dos $\mathbb{Z}^n$, $n = 4, 8$ com as construções obtidas acima.

n	A	B	C	D	E	F	Lim
4	0.43899	—	0.39763	0.38555	0.34560	0.41553	0.44163
8	0.29382	0.28952	—	0.26106	0.28952	0.29382	0.30093

A - Krüskemper método (Oggier [30],[31]).
B,C - Construções ciclotômica e mista, respectivamente (Bayer et al. [26]).
D - Construção via $\mathbb{Q}(\zeta_{2^r})$ (Andrade et al. [4]).
E - Construção cíclica, n par (Andrade et al. [5]).
F - Nossa construção (via $\mathbb{Q}(\zeta_{2^r.3.5})$).
Lim - Limitante de Odlyzko [11].

Tabela 6.4: Distância produto mínima de $\mathbb{Z}^4$ e $\mathbb{Z}^8$ via $\mathbb{Q}(\zeta_{2^r.3.5})$ - Comparação.

Observação 6.1.1. *Nota-se pela tabela acima, que para a dimensão 4, a distância produto mínima da nossa construção só não é melhor que a primeira construção (Oggier [30],[31]), que é a distância produto mínima ótima para a dimensão. Para a dimensão 8, equipara-se também à primeira construção, e como a distância produto mínima está muito próxima do limitante de Odlyzko, talvez estas duas construções sejam as melhores na dimensão 8.*

6.2 Reticulados $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ rotacionados

Nesta seção veremos que os reticulados ideais $\sigma_\alpha(\mathcal{A})$ obtidos via o corpo $\mathbb{K} = \mathbb{Q}(\zeta_{2^r.3.5} + \zeta_{2^r.3.5}^{-1})$, para $r \geq 3$ correspondem às versões escalonadas e rotacionadas dos reticulados $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, onde $\mathcal{E}_8^r$ denota a soma direta das $2^{r-2} - 1$ cópias do reticulado E_8 . Além disso, comparamos as distâncias produto mínimas com as versões do reticulado $\mathbb{Z}^n$ conhecidas na literatura.

Vimos pela Proposição 6.1.1 que os reticulados $\frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{A})$ e $\frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{A})$ são versões rotacionadas dos reticulados $\mathbb{Z}^4$ e $\mathbb{Z}^8$, respectivamente. Para isso, usamos o Algoritmo 4.1, que busca pela matriz mudança de base. Para $r \geq 3$, os reticulados $\frac{1}{\sqrt{2^{r-1}.3.5}}\sigma_\alpha(\mathcal{A})$ estão nas dimensões 16, 32, 64, $\dots$, e apesar de ser possível resolver o problema na dimensão 16 com o uso do algoritmo, a partir da dimensão 32 o uso do Algoritmo 4.1 passa a ser inviável devido à complexidade.

Assim, teremos que usar outro método para mostrar que os reticulados $\frac{1}{\sqrt{2^{r-1}.3.5}}\sigma_\alpha(\mathcal{A})$

são versões rotacionadas dos reticulados $\mathbb{Z}^8 \oplus \mathcal{E}_g^r$. Faremos isto, analisando a matriz de Gram genérica apresentada no Corolário 6.0.2, e realizando operações elementares nas linhas e colunas da referida matriz. Mas, ao fazer tais operações devemos tomar o cuidado de não alterar o reticulado associado à matriz. As operações que serão realizadas na matriz de Gram e que não alteram o reticulado associado são as seguintes:

- Adicionar a Linha i à Linha j e substituir o resultado na Linha j .
(Notação: Linha $i +$ Linha $j \longrightarrow$ Linha j).
- Subtrair a Linha j da Linha i e substituir o resultado na Linha j .
(Notação: Linha $i -$ Linha $j \longrightarrow$ Linha j).
- Subtrair a Linha i da Linha j e substituir o resultado na Linha j .
(Notação: Linha $j -$ Linha $i \longrightarrow$ Linha j).

As mesmas operações são feitas com as colunas, e quando for feita uma das operações com as linhas, em seguida é feita a mesma operação com as colunas, ou seja, as operações são sempre aos pares, por exemplo

$$\text{Linha } i + \text{Linha } j \longrightarrow \text{Linha } j$$

$$\text{Coluna } i + \text{Coluna } j \longrightarrow \text{Coluna } j$$

Apresentamos agora um exemplo que ilustra tal situação.

Exemplo 6.2.1. *Suponhamos que um determinado reticulado com matriz geradora M tenha matriz de Gram dada por*

$$G = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 1 \\ -1 & 1 & 3 \end{pmatrix},$$

e o nosso objetivo seja realizar operações elementares nas linhas e colunas da matriz G a fim de zerar os elementos que estão na primeira linha e na primeira coluna, exceto o elemento

g_{11} . Nota-se que para isto basta realizar o par de operações

$$^* \text{Linha } 1 + \text{Linha } 3 \longrightarrow \text{Linha } 3$$

$$^{**} \text{Coluna } 1 + \text{Coluna } 3 \longrightarrow \text{Coluna } 3,$$

obtendo

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 1 \\ -1 & 1 & 3 \end{pmatrix} \xrightarrow{*} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \xrightarrow{**} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Denotando por $\hat{G}$ a matriz de Gram resultante, temos que $\hat{G} = AGA^t$, onde

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

é uma matriz com entradas inteiras e determinante 1. Como $G = MM^t$, segue que

$$\hat{G} = A(MM^t)A^t = (AM)(AM)^t.$$

Portanto, quando fazemos o par de operações na matriz de Gram, na verdade, obtemos como resultado uma outra matriz de Gram do reticulado, associada à mudança de base $\hat{M} = AM$, e isto acontece com qualquer par de operações dentre os tipos que estabelecemos anteriormente.

Com base nas idéias do Exemplo 6.2.1, implementamos um algoritmo que prova o seguinte resultado.

Proposição 6.2.1. *O reticulado $\frac{1}{\sqrt{2^{r-1} \cdot 3 \cdot 5}} \sigma_\alpha(\mathcal{A})$, $r \geq 3$, é uma versão rotacionada do reticulado $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, onde $\mathcal{E}_8^r$ denota a soma direta das $2^{r-2} - 1$ cópias do reticulado E_8 .*

Demonstração: A seguir apresentamos os passos do algoritmo que prova o resultado.

1. Na matriz de Gram G do reticulado $\frac{1}{\sqrt{2^{r-1} \cdot 3 \cdot 5}} \sigma_\alpha(\mathcal{A})$, $r \geq 3$, escolhemos 8 elementos na diagonal principal, a saber: g_{ii} , para $i = 1, 2^{r-2} + 1, 2^{r-1} + 1, 3 \cdot 2^{r-2} + 1$,

$2^r + 1, 5.2^{r-2} + 1, 3.2^{r-1} + 1, 7.2^{r-2} + 1$. O objetivo agora é realizar uma sequência de operações elementares (aos pares) para zerar os elementos da linha i e da coluna i , exceto g_{ii} que deve assumir o valor 1.

2. Realizamos a seguinte sequência de operações elementares:

$$\text{Linha } 1 + \text{Linha } (2^{r-1} + 1) \longrightarrow \text{Linha } (2^{r-1} + 1)$$

$$\text{Coluna } 1 + \text{Coluna } (2^{r-1} + 1) \longrightarrow \text{Coluna } (2^{r-1} + 1)$$

$$\text{Linha } 1 - \text{Linha } (3.2^{r-1} + 1) \longrightarrow \text{Linha } (3.2^{r-1} + 1)$$

$$\text{Coluna } 1 - \text{Coluna } (3.2^{r-1} + 1) \longrightarrow \text{Coluna } (3.2^{r-1} + 1)$$

$$\text{Linha } (2^{r-2} + 1) + \text{Linha } (3.2^{r-2} + 1) \longrightarrow \text{Linha } (3.2^{r-2} + 1)$$

$$\text{Coluna } (2^{r-2} + 1) + \text{Coluna } (3.2^{r-2} + 1) \longrightarrow \text{Coluna } (3.2^{r-2} + 1)$$

$$\text{Linha } (5.2^{r-2} + 1) - \text{Linha } (2^{r-2} + 1) \longrightarrow \text{Linha } (5.2^{r-2} + 1)$$

$$\text{Coluna } (5.2^{r-2} + 1) - \text{Coluna } (2^{r-2} + 1) \longrightarrow \text{Coluna } (5.2^{r-2} + 1)$$

$$\text{Linha } (7.2^{r-2} + 1) + \text{Linha } (5.2^{r-2} + 1) \longrightarrow \text{Linha } (5.2^{r-2} + 1)$$

$$\text{Coluna } (7.2^{r-2} + 1) + \text{Coluna } (5.2^{r-2} + 1) \longrightarrow \text{Coluna } (5.2^{r-2} + 1)$$

$$\text{Linha } (3.2^{r-2} + 1) - \text{Linha } (7.2^{r-2} + 1) \longrightarrow \text{Linha } (3.2^{r-2} + 1)$$

$$\text{Coluna } (3.2^{r-2} + 1) - \text{Coluna } (7.2^{r-2} + 1) \longrightarrow \text{Coluna } (3.2^{r-2} + 1)$$

3. A sequência de operações do Passo 2 atinge o objetivo estabelecido no Passo 1, ou seja, a matriz de Gram resultante apresenta as linhas i e colunas i zeradas, exceto o elemento g_{ii} que é igual a 1, para os 8 elementos escolhidos no Passo 1. Assim, os vetores v_i , para $i = 1, 2^{r-2} + 1, 2^{r-1} + 1, 3.2^{r-2} + 1, 2^r + 1, 5.2^{r-2} + 1, 3.2^{r-1} + 1, 7.2^{r-2} + 1$ da matriz geradora resultante do reticulado possuem norma mínima 1 e são ortogonais aos demais vetores da base. Agora, estes 8 vetores formam um reticulado com norma mínima 1 cuja matriz de Gram possui determinante igual a 1, e o único reticulado integral (a menos de rotação) com tal propriedade é o reticulado $\mathbb{Z}^8$.

4. Nota-se que os demais elementos da diagonal principal da matriz de Gram resul-

tante são iguais a 2. Assim, se $w_1, w_2, \dots, w_{2^{r+1}-8}$ são os vetores restantes da matriz geradora resultante do reticulado $\Lambda = \frac{1}{\sqrt{2^{r-1} \cdot 3 \cdot 5}} \sigma_\alpha(\mathcal{A})$, então $\langle w_i, w_i \rangle = 2$, para $i = 1, 2, \dots, 2^{r+1} - 8$. Afirmamos que o reticulado Λ' gerado por $w_1, w_2, \dots, w_{2^{r+1}-8}$ possui norma mínima 2. De fato, dado $w \in \Lambda'$, $w \neq 0$, temos que $w = \sum_{i=1}^{2^{r+1}-8} \alpha_i w_i$, $\alpha_i \in \mathbb{Z}$, logo

$$\|w\|^2 = \langle w, w \rangle = \left\langle \sum_{i=1}^{2^{r+1}-8} \alpha_i w_i, \sum_{i=1}^{2^{r+1}-8} \alpha_i w_i \right\rangle = \sum_{i=1}^{2^{r+1}-8} \alpha_i^2 \langle w_i, w_i \rangle + 2 \sum_{i,j=1; i < j}^{2^{r+1}-8} \alpha_i \alpha_j \langle w_i, w_j \rangle,$$

e como $\langle w_i, w_i \rangle = 2$, segue que $\|w\|^2$ é estritamente positivo e par, ou seja, $\|w\|^2 \geq 2$, assim o reticulado Λ' possui norma mínima 2.

Para concluir, observamos inicialmente que dado qualquer reticulado integral, o subreticulado gerado por vetores de norma 1 e 2 é a soma direta de reticulados raízes (Teorema de Witt, [42] - pág. 101), ou seja, é soma direta dos reticulados $\mathbb{Z}^n$, A_n , D_n , E_6 , E_7 e E_8 . O reticulado $\Lambda = \frac{1}{\sqrt{2^{r-1} \cdot 3 \cdot 5}} \sigma_\alpha(\mathcal{A})$ foi construído satisfazendo as condições impostas pelas Equações (6.0.1), (6.0.2) e (6.0.3), ou seja, possui a mesma densidade de centro do reticulado $\mathbb{Z}^n$ e acabamos de verificar que possui norma mínima 1, logo possui o mesmo raio de empacotamento do reticulado $\mathbb{Z}^n$, portanto possui o mesmo determinante, ou seja, $\det(\Lambda) = 1$. Como $\Lambda = \mathbb{Z}^8 \oplus \Lambda'$, segue que $\det(\Lambda') = 1$, pois $\det(\Lambda) = \det(\mathbb{Z}^8) = 1$.

Agora, temos que Λ' possui determinante igual a 1 e norma mínima 2, logo é soma direta de reticulados raízes (A_n , D_n , E_6 , E_7 e E_8), e como $\det(A_n) = n + 1$, $\det(D_n) = 4$, $\det(E_8) = 1$, $\det(E_7) = 2$, $\det(E_6) = 3$, segue que a única possibilidade é que Λ' seja soma direta de $2^{r-2} - 1$ cópias de E_8 , pois para qualquer outra combinação teríamos $\det(\Lambda') \neq 1$. Lembramos que o reticulado $\mathbb{Z}^n$ não foi considerado na combinação pois não existe nenhuma cópia de $\mathbb{Z}^n$ em Λ' , uma vez que a norma mínima de Λ' é 2. Daí, segue o resultado. $\square$

A seguir apresentamos um exemplo de aplicação do algoritmo, faremos o caso $r = 3$.

Exemplo 6.2.2. O reticulado $\Lambda = \frac{1}{\sqrt{60}} \sigma_\alpha(\mathcal{A})$ é uma versão rotacionada do reticulado $\mathbb{Z}^8 \oplus E_8$.

Passos do algoritmo

1. A matriz de Gram do reticulado Λ é dada por

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 & \mathbf{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & \mathbf{3} & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 2 & 0 & -1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 2 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & \mathbf{3} & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{2} & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 2 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 2 \end{pmatrix}$$

Escolhemos 8 elementos na diagonal principal, a saber: g_{ii} , para $i = 1, 3, 5, 7, 9, 11, 13, 15$.

O objetivo agora é realizar uma sequência de operações elementares (aos pares) para zerar os elementos da linha i e da coluna i , exceto g_{ii} que deve assumir o valor 1.

2. Realizamos a seguinte sequência de operações elementares:

$\text{Linha } 1 + \text{Linha } 5 \longrightarrow \text{Linha } 5$

$\text{Coluna } 1 + \text{Coluna } 5 \longrightarrow \text{Coluna } 5$

$\text{Linha } 1 - \text{Linha } 13 \longrightarrow \text{Linha } 13$

$\text{Coluna } 1 - \text{Coluna } 13 \longrightarrow \text{Coluna } 13$

$\text{Linha } 3 + \text{Linha } 7 \longrightarrow \text{Linha } 7$

$\text{Coluna } 3 + \text{Coluna } 7 \longrightarrow \text{Coluna } 7$

$\text{Linha } 11 - \text{Linha } 3 \longrightarrow \text{Linha } 11$

$\text{Coluna } 11 - \text{Coluna } 3 \longrightarrow \text{Coluna } 11$

$\text{Linha } 15 + \text{Linha } 11 \longrightarrow \text{Linha } 11$

$\text{Coluna } 15 + \text{Coluna } 11 \longrightarrow \text{Coluna } 11$

$\text{Linha } 7 - \text{Linha } 15 \longrightarrow \text{Linha } 7$

$\text{Coluna } 7 - \text{Coluna } 15 \longrightarrow \text{Coluna } 7$

3. A matriz de Gram resultante é dada por

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 2 & 0 & -1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 2 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 2 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 2 \end{pmatrix}$$

Nota-se que os vetores v_i , para $i = 1, 3, 5, 7, 9, 11, 13, 15$ da matriz geradora resultante do reticulado possuem norma mínima 1 e são ortogonais aos demais vetores da base. Agora, estes 8 vetores formam um reticulado com norma mínima 1 cuja matriz de Gram possui determinante igual a 1, e o único reticulado integral com tal propriedade é o reticulado $\mathbb{Z}^8$.

4. Nota-se que os demais elementos da diagonal principal da matriz de Gram resultante são iguais a 2. Assim, se $w_1, w_2, \dots, w_8$ são os vetores restantes da matriz geradora resultante do reticulado $\Lambda = \frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{A})$, então $\langle w_i, w_i \rangle = 2$, para $i = 1, 2, \dots, 8$. Vimos que o reticulado Λ' gerado pelos vetores $w_1, w_2, \dots, w_8$ possui norma mínima 2.

Conclusão

Como Λ' tem determinante 1 e norma mínima 2, segue pelo Teorema de Witt, que Λ' é escrito como soma direta de reticulados raízes $(\mathbb{Z}^n, A_n, D_n, E_6, E_7 \text{ e } E_8)$, e a única possibilidade é que Λ' seja igual a E_8 , pois caso contrário teríamos $\det(\Lambda') \neq 1$. Portanto, o reticulado $\Lambda = \frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{A})$ é uma versão rotacionada do reticulado $\mathbb{Z}^8 \oplus E_8$.

6.2.1 Distância produto mínima

Como o reticulado $\Lambda = \sigma_\alpha(\mathcal{A})$ é uma versão escalonada e rotacionada do reticulado $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, com fator de escala $\sqrt{2^{r-1}.3.5}$, $\det(\mathbb{Z}^8 \oplus \mathcal{E}_8^r) = 1$ e o vetor de norma mínima de $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ é $\eta_2 = 1$, segue da Proposição 4.2.1 que

$$\det(\Lambda) = (2^{r-1}.3.5)^{2^{r+1}} \det(\mathbb{Z}^8 \oplus \mathcal{E}_8^r) = (2^{r-1}.3.5)^{2^{r+1}},$$

e

$$\eta_1 = 2^{r-1}.3.5 \quad \eta_2 = 2^{r-1}.3.5,$$

onde η_1 é a norma mínima de Λ . Assim, pela Definição 3.3.5 segue que

$$\begin{aligned} \sqrt[2^{r+1}]{d_{p,min}(\Lambda)} &= \frac{1}{\sqrt{2^{r-1}.3.5}} \sqrt[2^{r+2}]{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} = \frac{1}{\sqrt{2^{r-1}.3.5}} \sqrt[2^{r+2}]{\frac{(2^{r-1}.3.5)^{2^{r+1}}}{2^{(r-1)2^{r+1}} 3^{2^r} 5^{3 \cdot 2^{r-1}}}} = \\ &= \frac{1}{(2^{r-1}.3.5)^{\frac{1}{2}}} \left(3^{2^r} 5^{2^{r-1}} \right)^{\frac{1}{2^{r+2}}} = 2^{-(\frac{r-1}{2})}.3^{-\frac{1}{4}}.5^{-\frac{3}{8}} \end{aligned}$$

Portanto,

$$\sqrt[2^{r+1}]{d_{p,min}(\Lambda)} = 2^{-(\frac{r-1}{2})}.3^{-\frac{1}{4}}.5^{-\frac{3}{8}} \quad (6.2.4)$$

6.2.2 Distância produto mínima - Comparação com outras construções

Podemos comparar a distância produto mínima entre as constelações $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ rotacionadas e $\mathbb{Z}^n$ rotacionadas conhecidas na literatura, para $n = 2^{r+1}$, $r \geq 3$.

Para $n = 2^{r+1}$, $r = 3$, temos

n	$\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$			$\sqrt[n]{d_{p,min}(\mathbb{Z}^8 \oplus \mathcal{E}_8^r)}$	
	A	B	C	D	Lim
16	0.19361	0.18064	0.11713	0.20776	0.21965

A - Construção mista (Bayer et al. [26]).
B - Construção via $\mathbb{Q}(\zeta_{2^r})$ (Andrade et al. [4]).
C - Construção cíclica, n par (Andrade et al. [5]).
D - Nossa construção (via $\mathbb{Q}(\zeta_{2^r.3.5})$).
Lim - Limitante de Odlyzko [11].

Tabela 6.5: Distância produto mínima de $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ na dimensão 16 - Comparação.

Observação 6.2.1. *Nota-se que para a dimensão 16, a nossa construção possui melhor desempenho em comparação às outras construções, e está bem próxima do Limitante de Odlyzko.*

Para $r \geq 4$ a comparação será feita à construção via $\mathbb{Q}(\zeta_{2^r})$ [4]. Seja γ a função que representa $\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$ [4] em relação a $\sqrt[n]{d_{p,min}(\mathbb{Z}^8 \oplus \mathcal{E}_8^r)}$, $n = 2^{r+1}$, assim pelas Equações (5.1.4) e (6.2.4) temos

$$\gamma(r) = \frac{2^{-\left(\frac{(r+2)2^{r+1}-1}{2^{r+2}}\right)}}{2^{-(\frac{r-1}{2})}.3^{-\frac{1}{4}}.5^{-\frac{3}{8}}} = 2^{-\frac{3}{2}}.3^{\frac{1}{4}}.5^{\frac{3}{8}}.2^{\frac{1}{2^{r+2}}}$$

Nota-se que

$$\lim_{r \rightarrow +\infty} \gamma(r) = 2^{-\frac{3}{2}}.3^{\frac{1}{4}}.5^{\frac{3}{8}} \approx 0.850842$$

ou seja, quando a dimensão tende ao infinito ($r \rightarrow +\infty$), temos que $\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$ representa aproximadamente 85% de $\sqrt[n]{d_{p,min}(\mathbb{Z}^8 \oplus \mathcal{E}_8^r)}$, o que pode ser visto na Tabela 6.6, para $n = 2^{r+1}$, $r \geq 4$.

n	$\sqrt[n]{d_{p,min}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,min}(\mathbb{Z}^8 \oplus \mathcal{E}_8^r)}$	(%)
32	0.12636	0.14691	86.010
64	0.08886	0.10388	85.546
128	0.06266	0.07345	85.314
256	0.04425	0.05194	85.199
512	0.03127	0.03672	85.141
1024	0.02210	0.02597	85.113
2048	0.01562	0.01836	85.098
4096	0.01104	0.01298	85.091
8192	0.00781	0.00918	85.087
16384	0.00552	0.00649	85.086
32768	0.00390	0.00459	85.085
65536	0.00276	0.00324	85.084
131072	0.00195	0.00229	85.084
262144	0.00138	0.00162	85.084

Tabela 6.6: Distância produto mínima de $\mathbb{Z}^n$ e $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, $n \geq 32$ - Comparação.

Uma comparação entre as distâncias produto mínimas das duas constelações também pode ser vista na Figura 6.1.

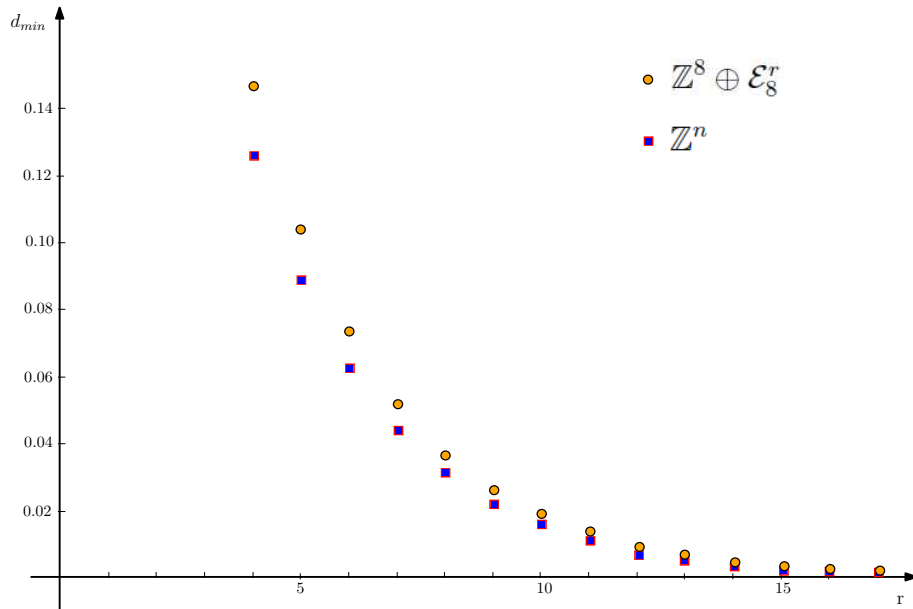


Figura 6.1: Distância produto mínima $\mathbb{Z}^n$ e $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ - gráfico.

Considerações

1. Apesar da distância produto mínima da família $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ ser maior que a distância produto mínima da família $\mathbb{Z}^n$ [4], temos que levar em conta o “trade-off” entre *distância produto mínima* e *rotulamento de bit*, pois vimos que quando consideramos uma constelação obtida de um reticulado com a forma

$$\mathcal{S} = \{\mathbf{x} = \mathbf{u}M; \mathbf{u} = (u_1, \dots, u_n) \in A\} \subset \Lambda$$

onde M é uma matriz geradora do reticulado Λ e $A \subset \mathbb{Z}^n$ é um conjunto finito, o mais simples algoritmo para rotulamento que podemos usar é obtido executando o rotulamento de bit sobre as componentes inteiras u_i do vetor $\mathbf{u}$. Se nos restringirmos ao algoritmo simples de rotulamento acima, observamos que isto induz a uma forma de constelação similar ao paralelepípedo fundamental (reticulado $\mathbb{Z}^n$), ou seja, é mais simples rotular um bit sobre uma constelação $\mathbb{Z}^n$ do que sobre uma constelação $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$.

2. Em relação ao canal gaussiano, vimos que a probabilidade de erro possui um limitante superior dado por

$$P_e(\mathcal{S}) \lesssim \frac{\nu}{2} \text{erfc} \left(\sqrt{\frac{nS}{2}} \Delta^{1/n} \right),$$

onde ν denota o kissing number, S é relação sinal ruído normalizada e Δ é a densidade de empacotamento da constelação de sinais. Agora, temos que o kissing number de $\mathbb{Z}^n$ é $2n$ e de $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ é 16, a densidade de empacotamento dos dois reticulados é a mesma, assim, assintoticamente a constelação baseada em $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ apresenta um desempenho melhor para o referido canal do que a constelação baseada em $\mathbb{Z}^n$.

6.3 Reticulados $\mathbb{Z}^8 \oplus \frac{1}{\sqrt{2}}\mathcal{E}_8^r$ rotacionados

Nesta seção fazemos uma perturbação dos reticulados $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ e analisamos o que acontece com a densidade de centro e com a distância produto mínima, com o intuito de melhorar

a eficiência da constelação em relação aos canais gaussiano e canal Rayleigh com desvanecimento. Veremos que a densidade de centro do reticulado perturbado é fixa em cada dimensão, ao contrário da densidade de centro de $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ que tende a zero quando a dimensão tende ao infinito. Veremos também, através de uma simulação na dimensão 16, que não temos controle sobre a distância produto mínima, que é extremamente pequena em relação a do reticulado $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$.

6.3.1 Densidade de centro

Vimos que $\Lambda = \frac{1}{\sqrt{2^{r-1} \cdot 3.5}} \sigma_\alpha(\mathcal{A})$ obtido via subcorpo maximal real de $\mathbb{Q}(\zeta_{2^r \cdot 3.5} + \zeta_{2^r \cdot 3.5}^{-1})$ é uma versão rotacionada de $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$, onde $\det(\Lambda) = 1$ e o vetor de norma mínima de Λ é igual a 1. Agora, seja Λ_1 o reticulado cuja matriz geradora é formada pelos vetores da base reduzida de Minkowski [41] de Λ , assim, os 8 primeiros vetores possuem norma 1 e os $2^{r+1} - 8$ vetores restantes possuem norma 2.

Agora, seja Λ_2 o reticulado cuja matriz geradora é formada pelos 8 vetores de norma 1 de Λ_1 e pelos $2^{r+1} - 8$ vetores restantes de norma 2 multiplicados pelo fator $\frac{1}{\sqrt{2}}$. Assim, podemos afirmar que Λ_2 é uma versão rotacionada do reticulado $\mathbb{Z}^8 \oplus \frac{1}{\sqrt{2}} \mathcal{E}_8^r$, logo

$$\det(\Lambda_2) = [\det(M_2)]^2 = \left[\left(\frac{1}{\sqrt{2}} \right)^{2^{r+1}-8} \det(M_1) \right]^2 = \left(\frac{1}{2^{2^{r+1}-8}} \right) [\det(M_1)]^2 = \frac{1}{2^{2^{r+1}-8}},$$

onde M_1 e M_2 são as matrizes geradoras dos reticulados Λ_1 e Λ_2 , respectivamente. Agora, a norma mínima do reticulado perturbado é a mesma do reticulado original, logo, o raio de empacotamento também é o mesmo, ou seja, $\rho = \frac{1}{2}$. Portanto, a densidade de centro de Λ_2 é dada por

$$\delta(\Lambda_2) = \frac{\rho^n}{\det(\Lambda_2)} = \frac{\left(\frac{1}{2}\right)^{2^{r+1}}}{\frac{1}{2^{2^{r+1}-8}}} = \frac{\left(\frac{1}{2}\right)^{2^{r+1}}}{\left(\frac{1}{2}\right)^{2^{r+1}-8}} = \frac{\left(\frac{1}{2}\right)^{2^{r+1}}}{\left(\frac{1}{2}\right)^{2^{r+1}} \left(\frac{1}{2}\right)^{-8}} = \frac{1}{256}.$$

Como $\delta(\Lambda_1) = \frac{1}{2^n}$, segue que a densidade de centro de Λ_1 tende a zero quando a dimensão n tende ao infinito, enquanto que a densidade de centro de Λ_2 é constante igual a $\frac{1}{256}$, ou seja, assintoticamente Λ_2 é extremamente denso em relação à Λ_1 .

6.3.2 Distância produto mínima

Para confirmar a eficiência do reticulado Λ_2 sobre Λ_1 em relação aos canais gaussianos e Rayleigh com desvanecimento simultaneamente, é preciso verificar o que acontece com a distância produto mínima quando perturbamos o reticulado Λ_1 obtendo o reticulado Λ_2 . Acabamos de verificar que em relação ao canal gaussiano, o uso de uma constelação baseada no reticulado Λ_2 é extremamente vantajosa sobre uma constelação baseada em Λ_1 , devido à densidade de empacotamento. A questão agora é: Em relação ao canal Rayleigh com desvanecimento, será que Λ_2 acompanha o desempenho de Λ_1 ? Para responder esta pergunta não dispomos de ferramentas algébricas como aquelas usadas para calcular a distância produto mínima em reticulados ideais, por exemplo o Teorema 3.3.2 e Corolário 3.3.2. Assim, fizemos uma simulação na dimensão 16 para comparar a distância produto mínima de $\Lambda_1 = \mathbb{Z}^8 \oplus E_8$ com a distância produto para alguns vetores em $\Lambda_2 = \mathbb{Z}^8 \oplus \frac{1}{\sqrt{2}}E_8$. Pela Equação 6.2.4 temos que

$$\sqrt[16]{d_{p,min}(\mathbb{Z}^8 \oplus E_8)} = 2^{-(\frac{2}{2})} \cdot 3^{-\frac{1}{4}} \cdot 5^{-\frac{3}{8}} = 0.207767$$

A simulação é feita através do Algoritmo 6.1, e os itens abaixo detalham o método:

1. A matriz M é a matriz geradora do reticulado Λ_2 , ou seja, é uma matriz geradora do reticulado $\mathbb{Z}^8 \oplus \frac{1}{\sqrt{2}}E_8$ rotacionado.
2. O objetivo do algoritmo é gerar alguns pontos do reticulado Λ_2 calculando a distância produto para poder compará-la com a distância produto mínima de Λ_1 que é identificada no algoritmo pela constante $d_{min} = 0.207767$.
3. Os vetores $\mathbf{m}_1, \mathbf{m}_2, \dots, \mathbf{m}_{16}$ geram Λ , e obtemos alguns pontos do reticulado fazendo

$$\mathbf{v} = \sum_{j=1}^{16} a_j \mathbf{m}_j; \quad a_j \in \{-1, 0, 1\},$$

ou seja, geramos 43046721 pontos.

4. Para cada ponto gerado, é calculada a distância produto, em seguida a distância produto mínima normalizada, identificada no algoritmo pela variável d_{norm} e comparada com d_{min} .
5. Se d_{norm} é menor que d_{min} , então d_{min} assume o valor de d_{norm} , o algoritmo informa d_{norm} e esta rotina é repetida para o próximo ponto gerado. Assim, o algoritmo somente informa uma distância produto se ela for menor que a obtida nos passos anteriores.

Finalizado o algoritmo os valores obtidos foram

0.206876

0.203313

0.189952

0.189557

0.179652

0.146913

0.000000005487

0.000000005398

0.000000004698

0.000000004499

Assim, podemos concluir que a distância produto mínima do reticulado Λ_2 é menor do que ou igual a 0.000000004499. Portanto, a distância produto mínima de Λ_1 é da ordem de 10^7 vezes maior que a distância produto mínima de Λ_2 (no mínimo).

Considerações

Vimos que quando perturbamos o reticulado $\mathbb{Z}^8 \oplus \mathcal{E}_8^r$ rotacionado, assintoticamente a densidade de centro do reticulado obtido é muito superior à do reticulado original. Por outro lado, pela simulação feita na dimensão 16, a distância produto mínima é muito inferior à do reticulado original. Assim, uma constelação baseada no reticulado $\mathbb{Z}^8 \oplus \frac{1}{\sqrt{2}}\mathcal{E}_8^r$ não é interessante para ser usada em ambos os canais (gaussiano e Rayleigh com desvanecimento).

$M = (m_{ij})_{i,j=1}^{16}$: Matriz geradora do reticulado $Z^8 \oplus \frac{1}{\sqrt{2}}E_8$ rotacionado , onde
 $\mathbf{m}_k = \{m_{k1}, \dots, m_{k16}\}$, $k = 1, 2, \dots, 16$.

inicio

$d_{min} = 0.207766$;

para $a_1 = -1$ até 1 **faça**

para $a_2 = -1$ até 1 **faça**

$\vdots$ $\vdots$ $\vdots$

para $a_{16} = -1$ até 1 **faça**

$\mathbf{v} = \sum_{j=1}^{16} a_j \mathbf{m}_j$, $[\mathbf{v} = (v_1, v_2, \dots, v_{16})]$;

$d_{prod} = \prod_{j=1}^{16} |v_j|$;

$d_{norm} = \sqrt[16]{d_{prod}}$;

se $d_{norm} < d_{min}$ e $d_{norm} \neq 0$ **então**

$d_{min} \leftarrow d_{norm}$;

Imprima: d_{norm} ;

fim

fim

$\vdots$ $\vdots$ $\vdots$

fim

fim

fim

Algoritmo 6.1: Distancia produto no reticulado $Z^8 \oplus \frac{1}{\sqrt{2}}E_8$.

PERSPECTIVAS FUTURAS

Delineamos a seguir algumas perspectivas em que deverão direcionar nosso trabalho futuro.

1. Extensão da família de D_n rotacionados

Durante o trabalho reproduzimos uma família de reticulados D_n rotacionados sobre corpos totalmente reais em dimensão potência de 2, e temos interesse em estender o resultado para outras dimensões. Uma possibilidade a ser explorada é usar as idéias contidas em [5] e [54] para tentar construir D_n rotacionados para qualquer dimensão n .

2. Extensão da família de $\mathbb{Z}^n$ rotacionados

Durante o trabalho reproduzimos uma família de reticulados unimodulares rotacionados em dimensão potência de 2, e temos interesse de estender esta família, preferencialmente $\mathbb{Z}^n$ rotacionados, para outras dimensões como por exemplo potência de 3 e de 5.

3. Reticulados A_2 , D_4 , E_8 e K_{12} com melhor performance para o canal Rayleigh com desvanecimento

Neste trabalho reproduzimos versões rotacionadas dos reticulados A_2 , D_4 , E_6 , E_8 e

K_{12} através de subcorpos maximais reais de corpos ciclotômicos. Temos interesse em reproduzir tais reticulados via subcorpos maximais reais com valor menor para o discriminante, assim teremos um ganho na distância produto mínima. Considerando o subcorpo maximal real $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ as possíveis opções para valores menores do discriminante são:

$$A_2 \rightarrow n = 5, 8, 10.$$

$$D_4 \rightarrow n = 15, 20, 30.$$

$$E_8 \rightarrow n = 13, 21, 26, 28, 42.$$

$$K_{12} \rightarrow n = 35, 39, 45, 70, 78, 90.$$

4. Uso de reticulados em criptossistemas pós-quânticos

Na teoria dos reticulados existem dois problemas clássicos, o SVP (Shortest Vector Problem) e CVP (Closest Vector Problem) que são problemas de alta complexidade computacional. Com o advento do computador quântico, uma linha de pesquisa de grande interesse atualmente é o uso de reticulados na implementação de criptossistemas pós-quanticos, e a idéia básica consiste no uso dos reticulados no sistema de chaves pública e privada, e a segurança do sistema consiste na complexidade do SVP e CVP, pois para o computador quântico não existe (até o momento) nenhum algoritmo em tempo polinomial que resolva tanto o SVP quanto o CVP. Assim, temos interesse em estudar sistemas criptográficos utilizando reticulados. As referências são [18], [19] e [20].

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] A. A. Andrade, A. J. Ferrari, C. Alves, T. B. Carlos, “Lattices via cyclotomic fields in dimensions 2 and 4”. *International Journal of Applied Mathematics*, v.20, pp. 1095-1105, 2007.
- [2] A. A. Andrade, A. J. Ferrari, C. W. O. Benedito, S. I. R. Costa, “Constructions of algebraic lattices”. *Computational & Applied Mathematics*, v.29, n.3, pp. 1-13, 2010.
- [3] A. A. Andrade, C. Alves, T. B. Carlos, “New constructions of rotated lattices”. *International Journal of Applied Mathematics*, v. 20, n. 8, pp. 1079 -1087, 2007.
- [4] A. A. Andrade, C. Alves, T. B. Carlos, “Rotated Lattices via the Cyclotomic Field $Q(\zeta_{2^r})$ ”. *International Journal of Applied Mathematics*, v. 19, n. 3, pp. 321-331, August 2006.
- [5] A. A. Andrade, E. D. Carvalho, “Constructions of ideal lattices with full diversity”. *Journal of Advanced Research in Mathematics*.
- [6] A. J. Ferrari, “Reticulados algébricos via corpos abelianos”. *Dissertação de Mestrado*, IBILCE-UNESP, 2008.

- [7] A. J. Ferrari, A. A. Andrade, “Families of algebraic lattices in even dimensions up to 8”. *International Journal of Pure and Applied Mathematics*, v.49, pp. 53-61, 2008.
- [8] A. L. Flores, “Reticulados em Corpos Abelianos”. *Tese de Doutorado*, FEEC - UNICAMP, Campinas, 2000.
- [9] A. L. Flores, J. C. Inerlando, T. P. Nobrega, “An extension of Craig’s family of lattices”. *Canad. Math. Bull.* , v.54, n.4, pp. 645-653, March 2011.
- [10] A. L. Flores, J. C. Interlando, T. P. Nobrega, J. O. D. Lopes, “On a refinement of Craig’s lattice”. *Journal of Pure and Applied Algebra*, v.215, pp. 1440-1442, September 2010.
- [11] A. M. Odlyzko, “Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results”. *Séminaire de Théorie des Nombres*, Bourdeaux, France, pp. 1-15, 1989.
- [12] A. M. Odlyzko, “Some analytic estimates of class numbers and discriminants”. *Invent. Math.*, v.29, pp. 275-286, 1975.
- [13] C. Alves, “Reticulados e códigos”. *Tese de Doutorado*, IMECC-UNICAMP, 2008.
- [14] C. D. Mayer, “Matrix analysis and applied linear algebra”. *SIAM*, 2000.
- [15] C. H. S. Jesus, “Discriminante dos subcorpos de corpos ciclotômicos de condutores potência de um primo ímpar”. *Dissertação de Mestrado*, UFPB, 2007.
- [16] C. Shannon, “Mathematical Theory of Communication”. *Bell Systems Technical Journal*, v. 27, pt. I: pp. 379-423; pt. II: pp. 623-656, 1948.
- [17] D. A. Marcus, “Numbers Fields”. *Springer-Verlag*, New York, 1977.
- [18] D. J. Bernstein, J. A. Buchmann, E. Dahmen, “Post-Quantum Cryptography”. *Springer-Verlag*, Berlin, 2008.

- [19] D. Micciancio, O. Regev, “Lattice-Based Cryptography em Post Quantum Cryptography”. D.J. Bernstein, J. Buchmann, E. Dahmen (eds), pp. 147-191, Springer, 2009.
- [20] D. Micciancio, S. Goldwasser, “Complexity of Lattices Problems: A Cryptographic Perspective”. *The Kluwer International Series in Engeneering as Computer Science*, vol. 671, Kluwer Academic Publishers, 2002.
- [21] E. Augustini, “Constelações de Sinais em Espaços Hiperbólicos”. *tese de doutorado*, IMECC- UNICAMP, 2002.
- [22] E. B. Fluckiger, “Ideal Lattices”. *Cambridge Univ. Press*, pp. 168-184, 2002.
- [23] E. B. Fluckiger, “Lattices and Number Fields”. *Contemp. Math.*, v. 241, pp. 69-84, 1999.
- [24] E. B. Fluckiger, “Upper bounds for euclidean minima of algebraic number fields”. *Journal of Number Theory*, 121, pp. 305-323, May 2006.
- [25] E. B. Fluckiger, F. Oggier, “Algebraic lattice constellations: Bounds and performance”. *IEEE Trans. Inform. Theory*, V.52, n.1, pp. 319-327, 2006.
- [26] E. B. Fluckiger, F. Oggier, E. Viterbo, “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.
- [27] E. B. Fluckiger, G. Nebe, “On the euclidean minimum of some real number fields”. *Journal de theorie des nombres de Bordeaux*, 17, n.2, pp. 437,454, 2005.
- [28] E. B. Fluckiger, I. Suares, “Ideal Lattices over totally real Number Fields and Euclidean Minima”. , February 2005.
- [29] E. Viterbo, F. Oggier, “Algebraic Number Theory and Code Design for Rayleigh Fading Channels”, *Foundations and Trends in Communications and Information Theory*, v. 1, n.3, 2004.

- [30] F. Oggier, “Algebraic Methods for Channel Coding”. *Tese de doutorado*, École Polytechnique fédérale de Lausanne, 2005.
- [31] F. Oggier, E. B. Fluckiger, “Best rotated cubic lattice constellations for Rayleigh fading channel”. *Proc. Int. Symposium of Information Theory - ISIT 2003*, Yokohama, Japan, July 2003.
- [32] G. C. Jorge, “Reticulados q-ários e algébricos”. *Tese de doutorado*, IMECC- UNICAMP, 2012.
- [33] G. C. Jorge, A. J. Ferrari, S. I. R. Costa, “Rotated D_n -lattices”. *Journal of Number Theory*, artigo submetido, arXiv:1111.3787v1.
- [34] G. H. Golub, C. F. V. Loan, “Matrix computations”. *The Johns Hopkins University Press*, London, 1996.
- [35] I. N. Herstein, “Tópicos de Álgebra”. *Editora Polígono S.A.*, 1970.
- [36] I. Stewart, D. Tall, “Algebraic Number Theory”. *Chapman & Hall*, New York, 1987.
- [37] J. Boutros, E. Viterbo, “Signal space diversity: A power and bandwidth-efficient diversity technique for the Rayleigh fading channel”. *IEEE Transactions on Information Theory*, v. 44, n. 4, pp. 1453-1467, July 1998.
- [38] J. Boutros, E. Viterbo, C. Rastello, J. C. Belfiore, “Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels”. *IEEE Transactions on Information Theory*, v. 42, n. 2, pp. 502-518, March 1996.
- [39] J. C. Interlando, A. L. Flores, T. P. Nobrega, “A family of asymptotically good lattices having a lattice in each dimension”. *Internacional Journal of Number Theory*, v. 4, n. 1, pp. 147-154, 2008.
- [40] J. C. Interlando, J. O. D. Lopes, T. P. Nobrega, “The discriminant of abelian number fields”. *Journal of Algebra and its Applications*, v. 5, n. 1, pp. 35-41, 2006.

- [41] J. E. Strapasson,, “Geometria Discreta e Códigos”. *Tese de Doutorado*, IMECC-UNICAMP, 2007.
- [42] J. H. Conway, N. J. A. Sloane, “Sphere Packings, Lattices and Groups”. 3rd edition *Springer-Verlag*, New York, 1999.
- [43] J. Leech, N. J. A. Sloane, “Sphere Packing and Error- Correcting Code”. *Canad. J. Math*, v. 23, pp. 718-745, 1971.
- [44] J. O. D. Lopes, “The discriminant of subfields of $\mathbb{Q}(\zeta_{2^r})$ ”. *Journal of Algebra and its Applications*, vol.2, pp. 463-469, 2003.
- [45] K. Boullé, J. C. Belfiore, “Modulation scheme design for the Rayleigh fading channel”. *Proc. Conf. Information Science and System - CISS’92*, Princeton, NJ, pp.288-293, March 1992.
- [46] L. H. J. Monteiro, “Teoria de Galois”. *7º Colóquio Brasileiro de Matemática*, IMPA, Rio de Janeiro, 1969.
- [47] L. R. B. Naves, “A densidade de empacotamentos esféricos em reticulados”. *Dissertação de Mestrado*, IMECC-UNICAMP, 2009.
- [48] L. Washington, “Introduction to cyclotomic fields”. *Springer-Verlag*, New York, 1982.
- [49] M. Craig, “A cyclotomic construction for Leech’s lattice”. *Mathematika*. 25, pp.236-241, 1978.
- [50] M. Craig, “Extreme forms and cyclotomy”. *Mathematika*. 25, pp.44-56, 1978.
- [51] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, K. Wildanger, “KANT V4”. *J. Symbolic Comp.* v. 24, pp. 267-283, 1997. Disponível em: [http : //www.math.tu – berlin.de/ ~ kant/download.html](http://www.math.tu-berlin.de/~kant/download.html).
- [52] N. J. A. Sloane, S. Plouffe, “The Encyclopedia of Integer Sequences.” *Academic Press.*, 1995. Disponível em: [http : //www.oeis.org/A003172](http://www.oeis.org/A003172).

- [53] O. Endler, “Teoria dos Números Algébricos”. *IMPA*, Rio de Janeiro, 1986.
- [54] P. Elia, B. A. Sethuraman, P. V. Kumar, “Perfect space-time codes for any number of antennas”. *IEEE Transactions on Information Theory*, v. 53, n. 11, pp. 3853-3868, November 2007.
- [55] P. Ribenboim, “Algebraic Numbers”. *Wiley - Interscience*, 1972.
- [56] P. Ribenboim, “Classical theory of algebraic numbers”. *Springer-Verlag*, New York, 1982.
- [57] P. Samuel, “Algebraic Theory of Numbers”. *Hermann*, Paris, 1967.
- [58] S. Benedetto, E. Biglieri, “Principles of Digital Transmission With Wireless Applications”. *Kluwer Academic / Plenum Publishers*, New York, 1999.
- [59] S. I. R. Costa, R. M. Siqueira, C. C. Lavor, M. M. S. Alves, “Uma Introdução à Teoria de Códigos”. *Sociedade Brasileira de Matemática Aplicada e Computacional*, São Carlos-SP, 2006.
- [60] S. Lang, “Algebra”. *Addison-Wesley Publishing Company*, New York, 1972.
- [61] T. B. Carlos, “Abordagem algébrica e geométrica de reticulados”. *Tese de Doutorado*, IMECC-UNICAMP, 2007.
- [62] T. M. Rodrigues, “Cúbicas galoisianas”. *Dissertação de Mestrado-Ibilce/Unesp*, São José do Rio Preto-SP, 2003.
- [63] T. P. Nobrega, “Cúbicas reais, Algumas aplicações.”. *Anais do VI Encontro de Álgebra*, USP-UNICAMP, 1997.
- [64] T. P. Nobrega, J. C. Interlando, J. O. D. Lopes, “On computing discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$.”. *Journal of Number Theory*, vol.96, pp. 319-325, 2002.

ÍNDICE REMISSIVO

- A -módulo, 14
 - livre, 15
- anel dos inteiros algébricos, 19
- assinatura, 50
- base integral, 19
- canônico
 - perturbação do homomorfismo, 54
- canal, 2
 - codificador de, 2
 - decodificador de, 3
 - Rayleigh com desvanecimento, 7
 - gaussiano, 4
- cobertura
 - densidade de , 34
 - raio de , 34
- codiferente, 19
- condutor, 21
- construção
 - cíclica, 69
 - ciclotômica, 69
 - mista, 70
- corpo
 - de números, 16
 - de raízes, 16
 - fixo, 17
 - CM, 52
 - fixo da involução, 53
- demodulador, 3
- densidade de centro, 34
 - de um reticulado ideal, 63, 65
- determinante, 53
- discriminante de um corpo de números , 19
- distância
 - l -produto, 9
 - produto mínima, 58
- diversidade, 9, 57
- empacotamento
 - densidade de, 33

- esférico, 32
- raio de, 33
- reticulado, 33
- extensão
 - abeliana, 17
 - cíclica, 17
 - galoisiana, 16
 - algébrica, 16
 - de corpos, 15
 - finita, 16
- fecho de Galois, 17
- fonte, 2
 - decodificador de, 3
- forma da constelação, 12
- função
 - de Möbius, 25
 - de Euler, 20
- grupo de Galois, 16, 20
- homomorfismo
 - canônico, 50
- ideal fracionário, 19
- inteiro algébrico, 19
- involução, 53
- kissing number, 35
- limitante
 - de Bhattacharyya, 6
 - de Odlyzko, 60
- método de Krüskemper, 68
- matriz
 - de Gram, 29
 - geradora, 28
- modulador, 2
- n -ésimo corpo ciclotômico, 20
- número
 - algébrico, 16
- norma, 17
 - de um ideal, 19
 - mínima de um reticulado, 33
- polinômio
 - minimal, 16
 - separável, 16
- raio de empacotamento
 - de um reticulado ideal, 65
- raiz
 - n -ésima da unidade, 20
 - n -ésima primitiva da unidade, 20
- região
 - de Voronoi, 35
 - fundamental, 28
- reticulado, 27
 - A_n , 37
 - D_n , 41
 - E_6 , 44

E_7 , 43
 E_8 , 42
 K_{12} , 45
 Λ_{16} , 46
 Λ_{24} , 47
 $\mathbb{Z}^n$, 36
 determinante de um , 29
 dual, 30
 equivalente, 31
 integral, 29
 isodual, 30
 racional, 29
 raio de empacotamento de um, 33
 volume de um , 29
 algébrico, 51
 bcc, 40
 fcc, 39
 hexagonal, 38
 ideal, 53
 inteiro, 53
 mcc, 41
 rotulamento de bit, 12
 sub-reticulado, 30
 subcorpo maximal real, 20
 submódulo, 15
 Teorema de
 Dirichlet, 72
 Kronecker-Weber, 21
 Witt, 144
 traço, 17