5 - Os canais gaussiano e com desvanecimento do tipo Rayleigh

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. Os canais gaussiano e com desvanecimento do tipo Rayleigh. In: *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, pp. 171-188. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.

5

Os canais Gaussiano e com desvanecimento do tipo Rayleigh

5.1 Introdução

Neste capítulo, apresentamos através do trabalho de Boutros; Viterbo; Rastello; Belfiori (1996), constelações de reticulados que são eficientes para ambos os canais Gaussianos e com desvanecimento do tipo Rayleigh, enfocando a construção das versões rotacionadas dos reticulados já conhecidos na literatura: $\boldsymbol{D}_4$, $\boldsymbol{K}_{12}$ e Λ_{16}, através da matriz mudança de base de um ideal contido no anel dos inteiros de um corpo de números.

5.2 Breve histórico

O rápido crescimento da comunicação sem fio requer um aumento na capacidade e melhoria no desempenho dos sistemas de transmissão. Os canais de comunicação móvel são agrupados em

dois tipos: canal via satélite e canal terrestre. O canal de comunicação terrestre é caracterizado pelo efeito de múltiplos percursos de propagação. Tal efeito pode alterar de maneira significativa a amplitude do sinal, mesmo para uma pequena variação na distância ou orientação entre o transmissor e o receptor, comportamento que é comumente rotulado como desvanecimento. Limitações nas perdas de propagação, variação no tempo, ruído, inferência e desvanecimento fazem com que, nestes sistemas, a transmissão de dados com altas taxas de transmissão não seja uma tarefa fácil.

Para se alcançar essas altas taxas de transmissão de dados é necessário aumentar a capacidade do canal de comunicações móveis. Quando o desvanecimento compromete substancialmente a qualidade da transmissão, o aumento da capacidade do canal ou equivalentemente, a diminuição da taxa de erro é extremamente difícil.

Uma alternativa mais simples para aumentar a capacidade do canal com desvanecimento é utilizar técnicas de diversidade. Estas técnicas geralmente fornecem ao receptor réplicas da informação transmitida que experimentam desvanecimentos descorrelacionados. Neste caso, se uma componente do sinal estiver sobre um desvanecimento profundo, algumas das outras componentes terão uma grande probabilidade de sofrer uma atenuação mais leve.

A função densidade de probabilidade de Rayleigh caracteriza o desvanecimento percebido em uma comunicação móvel onde não há predominância direta entre a antena transmissora e a receptora. Esse desvanecimento indica que existe uma maior probabilidade da amplitude da envoltória do sinal recebido estar abaixo de um valor médio.

Os códigos projetados para canais com desvanecimento Ray-

leigh levam em conta dois parâmetros fundamentais: o ganho de diversidade, que descreve a diminuição exponencial da taxa de erro na decodificação em função da relação sinal-ruído na curva de desempenho e o ganho de codificação que resulta em deslocamentos à esquerda dessa curva. Os melhores valores para estes parâmetros foram obtidos maximizando-se, respectivamente, o posto mínimo e a média geométrica mínima dos autovalores, de um conjunto de matrizes complexas formadas pelas diferenças entre palavras-código tomadas duas a duas.

A principal desvantagem destes códigos é que são extremamente difíceis de se projetar, pois os critérios utilizados na sua construção baseiam-se em operações no domínio complexo das modulações em banda básica e não no domínio binário ou discreto no qual os códigos de canal são tradicionalmente projetados. Uma grande capacidade computacional é necessária para acompanhar a busca, codificação e decodificação destes códigos.

O canal de comunicação via satélite é um canal AWGN (Additive White Gaussian Noise) onde predominam fortes atenuações e muitas vezes grandes atrasos de propagação do sinal. O termo AWGN é utilizado em modulamentos matemáticos para caracterizar aqueles canais onde o tipo de ruído responsável por degradar a comunicação é um ruído branco adicionado ao sinal. Este tipo de ruído é um dos mais "bem comportados" e a teoria acerca do desenvolvimento de receptores ótimos para a utilização em canais AWGN já se tornou clássica.

O ruído branco é um sinal aleatório e tem um modelamento matemático que o considera como possuindo largura de faixa infinita, média nula e correlação nula entre suas amplitudes tomadas a instantes de tempo distintos, ou seja, o valor da amplitude do

ruído em um determinado instante independe daquele observado em outro instante de tempo qualquer. O termo gaussiano se deve ao fato desse tipo de ruído possuir uma função densidade de probabilidade gaussiana com média nula, com desvio padrão igual à sua tensão rms e variância igual à potência dissipada de um resistor de 1W. No canal gaussiano, usando esquemas convencionais de modulação e codificação de canal apropriada, pode-se reduzir a probabilidade de erro e bit de 10^{-2} a 10^{-3} por meio de um aumento da relação sinal-ruído de somente 1 ou 2 dB.

5.3 Boas constelações para ambos os canais Gaussianos e com desvanecimento do tipo Rayleigh

Nesta seção estabelecemos condições sobre os reticulados construídos para que tenhamos boas constelações para ambos os canais Gaussianos e Rayleigh com desvanecimento.

1. **Canal Gaussiano**

   - A probabilidade de erro de símbolo é limitada superiormente por

$$P_e(\Lambda) \leq \frac{\tau}{2}\, erfc\left(\frac{d_{E\,min}/2}{\sqrt{2N_0}}\right), \tag{5.1}$$

   onde τ é o número de vizinhos, $erfc$ é a função erro, N_0 é a variância gaussiana e $d_{E\,min}$ é a distância mínima Euclidiana do reticulado Λ. O ganho de codificação do reticulado Λ é dado por

$$\gamma = \frac{d^2_{E\,min}}{Vol(\Lambda)^{2/n}}.$$

- Constelações eficientes podem ser obtidas através de reticulados com alta densidade de empacotamento. Assim, constelações com boas propriedades de simetria podem ser obtidas.
- Usando corpos de números totalmente reais e com discriminante absoluto mínimo a grande desvantagem é que a densidade de empacotamento esférico é baixa.
- Usando corpos de números totalmente complexos e com discriminante absoluto mínimo a grande vantagem é que é possível obter reticulados com alta densidade de empacotamento.

2. **Canal Rayleigh com Desvanecimento**

- A probabilidade de erro de símbolo com alta relação sinal-ruído satisfaz,

$$P_e(\Lambda) \leq \frac{1}{2} \sum_{l=L}^{n} \frac{1}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^l d_p^{(l)}(x,y)^2}, \tag{5.2}$$

onde onde E_b é a energia média por bit, $\eta = \dfrac{2m}{n}$ é a eficiência espectral e $d_p^{(l)}(x,y)^2$ é a distância l-produto normalizada de x a y, quando esses pontos diferem em l componentes e é dada por

$$d_p^{(l)}(x,y)^2 = \frac{\prod\limits_{x_i \neq y_i} (x_i - y_i)^2}{\left(\dfrac{E}{n}\right)^l}, \tag{5.3}$$

onde $E = E(\|x\|^2)$ é a energia média por ponto da constelação S.

- Constelações eficientes, ou seja, aquelas em que a probabilidade de erro é mínima, podem ser obtidas através de reticulados com diversidade máxima $L = min(l)$, menor energia média da constelação E e maior distância produto mínima $d_{p,min} = min(d_p^{(L)}(x, y))$.

- Usando corpos de números totalmente reais e com discriminante absoluto mínimo, a grande vantagem é que eles apresentam diversidade máxima.

- Usando corpos de números totalmente complexos e com discriminante absoluto mínimo a grande vantagem é que obtemos uma menor energia média da constelação.

Assim, concluímos que para obter boas constelações de reticulados para ambos os canais, procura-se construir reticulados com alta densidade de empacotamento e com diversidade máxima.

Através da família de reticulados A_n que vimos a partir de subcorpos de $\mathbb{Q}(\zeta_p)$ é possível obter constelações que têm máxima diversidade e boa densidade de empacotamento, que fazem estes reticulados úteis para uso nos canais Gaussiano e Rayleigh com desvanecimento.

Corpos de números algébricos totalmente reais com discriminante absoluto mínimo são conhecidos até a dimensão 8 e são dados na 1ª coluna da Tabela (5.3.1).

Discriminantes absolutos mínimos
(Valores com * são os melhores valores conhecidos)

n	$r_2 = 0$	$r_2 = 1$	$r_2 = 2$	$r_2 = 3$	$r_2 = 4$
2	5	-3	-	-	-
3	49	-23	-	-	-
4	725	-275	117	-	-
5	14641	-4511	1609	-	-
6	300125	-92779^*	28037^*	-9747	-
7	20134393	?	?	?	-
8	282300416	?	?	?	125778^*

Tabela (5.3.1)

Pela Tabela (5.3.1) notamos que os discriminantes absolutos dos corpos totalmente complexos são menores do que dos corpos totalmente reais. Os corpos da Tabela (5.3.1) (especialmente em dimensão acima de 4) tem sido objeto de estudos na teoria dos números algébricos computacionais.

Definição 5.3.1. *A diversidade de um reticulado Λ é a distância mínima de Hamming entre quaisquer dois vetores de Λ.*

Teorema 5.3.1. *(*BoutrosS; Viterbo; Rastello; Belfiori, 1996*) Sejam $\mathbb{K}$ um corpo de números, $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ os $\mathbb{Q}$-homomorfismos de $\mathbb{K}$ em $\mathbb{C}$ e $\{w_1, w_2, \cdots, w_n\}$ uma base integral de $\mathbb{K}$. Os reticulados obtidos a partir da matriz geradora $\boldsymbol{G} =$*

$$\begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_{r_1}(w_1) & \Re\sigma_{r_1+1}(w_1) & \Im\sigma_{r_1+1}(w_1) & \cdots & \Re\sigma_{r_1+r_2}(w_1) & \Im\sigma_{r_1+r_2}(w_1) \\ \sigma_1(w_2) & \cdots & \sigma_{r_1}(w_2) & \Re\sigma_{r_1+1}(w_2) & \Im\sigma_{r_1+1}(w_2) & \cdots & \Re\sigma_{r_1+r_2}(w_2) & \Im\sigma_{r_1+r_2}(w_2) \\ \vdots & \ddots & & \vdots & & \ddots & & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_{r_1}(w_n) & \Re\sigma_{r_1+1}(w_n) & \Im\sigma_{r_1+1}(w_n) & \cdots & \Re\sigma_{r_1+r_2}(w_n) & \Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}$$

possuem diversidade $\boldsymbol{L = r_1 + r_2}$.

Demonstração. Seja $z \neq 0$ um ponto arbitrário de $\Lambda = \sigma(\mathbb{A}_{\mathbb{K}})$. Assim $z = (z_1, z_2, \cdots, z_n) = \sum_{i=1}^{n} \lambda_i v_i$, com $\lambda_i \in \mathbb{Z}$ e $v_i = (v_{ij}) = \sigma(w_i)$ são as linhas do reticulado da matriz geradora $\boldsymbol{G}$. Logo,

$$d^n(0,z) = \prod_{j=1}^{n} |z_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| =$$

$$= \prod_{j=1}^{r_1} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \times \prod_{j=r_1+1}^{r_1+r_2} \left| \Re\sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \times \prod_{j=r_1+1}^{r_1+r_2} \left| \Im\sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right|.$$

Os inteiros algébricos $\sum_{i=1}^{n} \lambda_i w_i$ são não nulos pois todos os $\lambda_i's$ são não nulos ($z \neq 0$). Isto implica que $\sigma_j(\sum_{i=1}^{n} \lambda_i w_i) \neq 0$ e assim o primeiro produto do lado direito da última igualdade contém exatamente r_1 fatores não nulos. O número mínimo de fatores não nulos no segundo e no terceiro produtos é r_2 pois as partes real e imaginária de qualquer um dos monomorfismos complexos não são ambos nulos. Assim concluímos que para tal reticulado temos uma diversidade $L \geq r_1 + r_2$. Agora, se $\alpha = 1$ em $\mathbb{A}_{\mathbb{K}}$, então $\sigma_j(1) = 1$ para $j = 1, 2, \cdots, r_1 + r_2$ e portanto $\sigma(1)$ fornece $r_1 + r_2$ componentes não nulos. Assim $L = r_1 + r_2$. ■

No caso de um corpo de números algébricos totalmente real temos que a matriz geradora $\boldsymbol{G}$ é da forma

$$\boldsymbol{G} = \begin{pmatrix} \sigma_1(w_1) & \sigma_2(w_1) & \cdots & \sigma_n(w_1) \\ \sigma_1(w_2) & \sigma_2(w_2) & \cdots & \sigma_n(w_2) \\ \vdots & & \ddots & \vdots \\ \sigma_1(w_n) & \sigma_2(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}.$$

Neste caso, o reticulado $\Lambda = \sigma(\mathbb{A}_{\mathbb{K}})$ construído atinge o grau máximo de diversidade $L = n$.

Para corpos totalmente complexos $\mathbb{K}$ temos que $r_2 = n/2$ é par e a matriz geradora do reticulado $\sigma(\mathbb{A}_{\mathbb{K}})$ é dada por

$$G = \begin{pmatrix} \Re\sigma_1(w_1) & \Im\sigma_1(w_1) & \cdots & \Re\sigma_{r_2}(w_1) & \Im\sigma_{r_2}(w_1) \\ \Re\sigma_1(w_2) & \Im\sigma_1(w_2) & \cdots & \Re\sigma_{r_2}(w_2) & \Im\sigma_{r_2}(w_2) \\ \vdots & & \ddots & & \vdots \\ \Re\sigma_1(w_n) & \Im\sigma_1(w_n) & \cdots & \Re\sigma_{r_2}(w_n) & \Im\sigma_{r_2}(w_n) \end{pmatrix}.$$

Definição 5.3.2. *Um polinômio minimal é chamado* **reduzido** *se as potências de uma de suas raízes (o elemento primitivo) é uma base integral do corpo de números.*

A Tabela (5.3.2) apresenta os polinômios minimais reduzidos dos corpos da Tabela (5.3.1) com o volume fundamental do reticulado correspondente obtido via o homomorfismo canônico, indicados por $\Lambda_{n,L}$.

$\Lambda_{n,L}$	$\mu_\theta(x)$	$redVol(\Lambda_{n,L})$
$\Lambda_{2,1}$	$X^2 - X + 1$	0.8660
$\Lambda_{2,2}$	$X^2 - X - 1$	2.2361
$\Lambda_{3,2}$	$X^3 - X - 1$	2.3979
$\Lambda_{3,3}$	$X^3 + X^2 - 2X - 1$	7
$\Lambda_{4,2}$	$X^4 - X^3 - X^2 + X + 1$	2.7042
$\Lambda_{4,3}$	$X^4 - X^3 + 2X - 1$	8.2916
$\Lambda_{4,4}$	$X^4 - X^3 - 3X^2 + X + 1$	26.9258
$\Lambda_{5,3}$	$X^5 - X^3 + X^2 + X - 1$	10.0281
$\Lambda_{5,4}$	$X^5 - 2X^3 + X^2 - 1$	33.5820
$\Lambda_{5,5}$	$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$	121
$\Lambda_{6,3}$	$X^6 - 3X^5 + 4X^4 - 4X^3 + 4X^2 - 2X + 1$	12.3409
$\Lambda_{6,4}$	$X^6 - 2X^5 + 3X^3 - 2X - 1$	41.8606
$\Lambda_{6,5}$	$X^6 + X^5 - 2X^4 - 3X^3 - X^2 + 2X + 1$	152.2982
$\Lambda_{6,6}$	$X^6 - X^5 - 7X^4 + 2X^3 + 7X^2 - 2X - 1$	547.8367
$\Lambda_{7,7}$	$X^7 + X^6 - 6X^5 - 5X^4 + 8X^3 + 5X^2 - 2X - 1$	4487.1364
$\Lambda_{8,4}$	$X^8 - 2X^7 + 4X^5 - 4X^4 + 3X^2 - 2X + 1$	70.0928
$\Lambda_{8,8}$	$X^8 + 2X^7 - 7X^6 - 8X^5 + 15X^4 + 8X^3 - 9X^2 - 2X + 1$	16801.7980

Tabela (5.3.2)

Os passos para a construção de um reticulado a partir de um corpo de números algébricos $K = \mathbb{Q}(\theta)$ pode ser resumido do seguinte modo:

- Encontre uma base integral de $\mathbb{K}$, que identifica $\mathbb{A}_{\mathbb{K}}$.
- Encontre as n raízes de $g_\theta(X)$, que identifica os n monomorfismos $\sigma_1, \sigma_2, \cdots, \sigma_n$.
- Construa a matriz geradora aplicando o homomorfismo canônico.

Exemplo 5.3.1. *Seja* $\mathbb{K} = \mathbb{Q}(i\sqrt{3})$. *Como* $-3 \equiv 1(mod\ 4)$ *segue que a base integral de* $\mathbb{K}$ *é* $\{1, (1+i\sqrt{3})/2\}$. *Os dois monomorfismos são* $\sigma_1(i\sqrt{3}) = i\sqrt{3}$, $\sigma_2(i\sqrt{3}) = -i\sqrt{3}$ *e a matriz geradora é dada por*

$$G = \begin{pmatrix} \mathfrak{R}\sigma_1(1) & \mathfrak{I}\sigma_1(1) \\ \mathfrak{R}\sigma_1\left(\frac{1+i\sqrt{3}}{2}\right) & \mathfrak{I}\sigma_1\left(\frac{1+i\sqrt{3}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

O volume fundamental do reticulado é dado por

$$|\det(G)| = \frac{\sqrt{3}}{2} = 0,8660254.$$

A diversidade é $L = 1$ *pois* $r_1 = 0$ *e* $r_2 = 1$. *Portanto,* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *corresponde ao reticulado* $\Lambda_{2,1}$.

Exemplo 5.3.2. *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{7+2\sqrt{5}})$. *As raízes do polinômio minimal* X^4-14X^2+29 *são* $\theta_1 = \sqrt{7+2\sqrt{5}}$, $\theta_2 = -\sqrt{7+2\sqrt{5}}$, $\theta_3 = \sqrt{7-2\sqrt{5}}$, $\theta_4 = -\sqrt{7-2\sqrt{5}}$. *O elemento primitivo é* $\theta = \theta_1$ *e os 4 monomorfismos são* $\sigma_1(\theta) = \theta_1$, $\sigma_2(\theta) = \theta_2$, $\sigma_3(\theta) = \theta_3$, *e* $\sigma_4(\theta) = \theta_4$. *Mas* $\{1, \theta, \theta^2, \theta^3\}$ *não é base integral pois* X^4-14X^2+29 *não é*

reduzido. Uma base integral é $\{1, \frac{1}{2}(1+\theta), \frac{1}{4}(3+\theta^2), \frac{1}{8}(1+\theta)(3+\theta^2)\}$. *A matriz geradora é dada por*

$$G = \begin{pmatrix} 1.000 & 1.000 & 1.000 & 1.000 \\ -1.193 & -0.294 & 1.294 & 2.193 \\ 3.618 & 1.381 & 1.381 & 8.618 \\ -4.318 & -0.407 & 1.789 & 7.936 \end{pmatrix}.$$

O volume fundamental do reticulado é $|\det(G)| = 26.92$. *A diversidade é* $L = 4$ *pois* $r_1 = 4$ *e* $r_2 = 0$. *Portanto,* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *corresponde ao reticulado* $\Lambda_{4,4}$.

5.4 Construção das versões rotacionadas dos reticulados D_4, K_{12}, e Λ_{16}

Craig (1978) como construir os reticulados E_6, E_8, Λ_{24} a partir dos corpos ciclotômicos totalmente complexos $\mathbb{K} = \mathbb{Q}(e^{i2\pi/n})$, para $n = 9, 20, 39$. Via este procedimento Boutros; Viterbo; Rastello; Belfiori (1996) encontrou D_4, K_{12} e Λ_{16} a partir das 8-ésima, 21-ésima e 40-ésima raízes da unidade. Estes reticulados são obtidos aplicando o homomorfismo canônico em ideais destes corpos ciclotômicos. Os ideais são dados na Tabela (5.3.3). Os reticulados obtidos são subreticulados de $\sigma(\mathbb{A}_{\mathbb{K}})$, mas com um ganho fundamental muito maior comparado com os reticulados presentes na Tabela (5.3.2).

Sejam $\mathbb{K}$ um corpo de números de grau n, $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$, $\mathfrak{a} \subseteq \mathbb{A}_{\mathbb{K}}$ um ideal e $\{\gamma_1, \cdots, \gamma_n\}$ uma $\mathbb{Z}$-base de $\mathfrak{a}$. Aplicando o homomorfismo canônico $\sigma_{\mathbb{K}}$ ao ideal $\mathfrak{a}$ de $\mathbb{A}_{\mathbb{K}}$, pela Proposição 3.5.2 obtemos o reticulado $\Lambda_{\mathfrak{a}} = \sigma(\mathfrak{a})$ de posto n contido em $\Lambda = \sigma(\mathbb{A}_{\mathbb{K}})$. A matriz geradora $G_{\mathfrak{a}}$ de $\Lambda_{\mathfrak{a}}$ é dada por

$$G_{\mathfrak{a}} = \begin{pmatrix} \sigma_1(\gamma_1) & \cdots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \cdots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & \ddots & & \vdots & & \ddots & & \vdots \\ \sigma_1(\gamma_n) & \cdots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{pmatrix}.$$

Comparando $\mathbb{A}_{\mathbb{K}}$ e $\mathfrak{a}$ como $\mathbb{Z}$-módulo, vemos que existe uma relação entre as matrizes $\boldsymbol{G}$ de $\sigma(\mathbb{A}_{\mathbb{K}})$ e a matriz $\boldsymbol{G}_{\mathfrak{a}}$ de $\sigma(\mathfrak{a})$. Seja $\boldsymbol{T}$ a matriz mudança de base $n \times n$ da primeira base para a segunda base, isto é,

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = T \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}.$$

Como, os $\gamma_i^{'}s$ são inteiros algébricos segue que são escritos como combinação linear dos $w_i^{'}s$, ou seja, $\gamma_i = \sum_{k=1}^{n} t_{ik} w_k$, onde $t_{ik} \in \mathbb{Z}$. Assim que $\boldsymbol{T} = [t_{ij}]$ é uma matriz inteira. A matriz $\boldsymbol{T}$ é conhecida como **matriz da representação integral** de $\mathfrak{a}$. Com isso temos a seguinte proposição.

Proposição 5.4.1. *(*Boutros; Viterbo; Rastello; Belfiori, 1996*) A matriz geradora $\boldsymbol{G}_{\mathfrak{a}}$ do reticulado $\Lambda_{\mathfrak{a}}$ é obtida a partir da matriz geradora $\boldsymbol{G}$ do reticulado Λ pela aplicação da matriz mudança de base T entre as $\mathbb{Z}$-bases de $\mathfrak{a}$ e $\mathbb{A}_{\mathbb{K}}$, isto é, $\boldsymbol{G}_{\mathfrak{a}} = \boldsymbol{TG}$.*

Demonstração. O resultado segue diretamente da fórmula $\gamma_i = \sum_{k=1}^{n} t_{ik} w_k$, que também é válido tomando as partes real e imaginária de ambos os lados $\sigma_j(\gamma_i) = \sum_{k=1}^{n} \sigma_j(t_{ik} w_k) = \sum_{k=1}^{n} t_{ik} \sigma_j(w_k)$, e isto conclui a demonstração. ∎

Da igualdade $G_{\mathfrak{a}} = TG$ temos que $\det G_{\mathfrak{a}} = \det T \cdot \det G$, o que significa que

$$Vol(\Lambda_{\mathfrak{a}}) = |\det T| \cdot Vol(\Lambda).$$

Se $\mathfrak{a}$ é um ideal principal, isto é, $\mathfrak{a} = \alpha\mathbb{A}_{\mathbb{K}}$ então a matriz mudança de base é dada por $T = R(\alpha)$. A $\mathbb{Z}$-base do ideal principal $\mathfrak{a} = \alpha\mathbb{A}_{\mathbb{K}}$ é o conjunto $\{\alpha w_i,\ i = 1, \cdots, n\}$. Assim podemos escrever

$$\alpha \cdot \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = R(\alpha) \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}.$$

A procura de reticulados rotacionados da Tabela (5.3.3) com dimensão n e diversidade $n/2$ segue os seguintes passos:

1. Calcule o polinômio minimal de ζ_n sobre $\mathbb{Q}$ que tem grau $\phi(n)$.

2. Encontre todos os ideais $\mathfrak{a}$ de $\mathbb{A}_{\mathbb{K}}$ com norma inteira.

3. Usando a matriz mudança de base T, calcule a matriz geradora $G_{\mathfrak{a}} = TG$ e avalie os parâmetros dos reticulados, por exemplo, a densidade de centro e o número de vizinhos. Se eles são iguais aos parâmetros de D_4, E_6, E_8, Λ_{12}, Λ_{16} ou Λ_{24}, então obtemos uma versão rotacionada destes reticulados pois tais reticulados são os únicos com tais parâmetros.

   Este procedimento é aplicado sucessivamente para obter uma matriz geradora para cada um dos reticulados presentes na Tabela (5.3.3).

Alguns reticulados conhecidos dos corpos ciclotômicos:

	$\mathbb{Q}(\theta)$	n	Ideais
$D_{4,2}$	θ^4+1	8	$(2,\theta+1)$
$E_{6,3}$	$\theta^6-\theta^3+1$	9	$(3,(\theta+1)^2)$
$E_{8,4}$	$\theta^8-\theta^6+\theta^4-\theta^2+1$	20	$(5,\theta-2)$
$K_{12,6}$	$\theta^{12}-\theta^{11}+\theta^9-\theta^8+\theta^6-\theta^4+\theta^3-\theta+1$	21	$(7,\theta+3)$
$\Lambda_{16,8}$	$\theta^{16}-\theta^{12}+\theta^8-\theta^4+1$	40	$(2,\theta^4+\theta^3+\theta^2+\theta+1)$ $(5,\theta^2+2)$
$\Lambda_{24,12}$	$\theta^{24}-\theta^{23}+\theta^{21}-\theta^{20}+\theta^{18}-\theta^{17}+\theta^{15}-\theta^{14}+$ $+\theta^{12}-\theta^{10}+\theta^9-\theta^7+\theta^6-\theta^4+\theta^3-\theta+1$	39	$(3,\theta^3+\theta^2-1)$ $(3,\theta^3+\theta^2+\theta+1)$ $(13,\theta-3)$

Tabela (5.3.3)

Exemplo 5.4.1. *(Construção de $D_{4,2}$). Note que $\phi(8)=4$ e que para outros valores de n tal que $\phi(n)=4$ não resultam na versão rotacionada de D_4, cuja densidade de centro é 1/8. O polinômio minimal de $\theta=\zeta_8$ sobre $\mathbb{Q}$ é dado na Tabela (5.3.2), o discriminante absoluto do corpo $\mathbb{K}=\mathbb{Q}(\zeta_8)$ é $D_{\mathbb{K}}=2^8$, $r_1=0$ e $r_2=2$. Pela Equação* (3.4) *temos que*

$$N(\mathfrak{a})=\frac{2^{4/2}}{\sqrt{2^8}}\frac{\rho^4}{\frac{1}{8}}=2^3\rho^4,$$

e para $N(\mathfrak{a})=2$ devemos tomar $\rho=\dfrac{1}{\sqrt{2}}$. O ideal $\mathfrak{a}$ com norma 2 pode ser obtido da fatoração do ideal primo (2), *que tem norma 2^4 do seguinte modo*

$$(2)=(2,\theta+1)^4=\mathfrak{a}^4.$$

Assim $\mathfrak{a}$ tem a norma desejada 2. A matriz geradora do reticulado é $G_{\mathfrak{a}}=TG$, onde T é a matriz da representação integral de $\mathfrak{a}$

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

e $\boldsymbol{G}$ *é a matriz geradora de* $\sigma(\mathbb{A}_{\mathbb{K}})$. *O reticulado gerado por* $\boldsymbol{G}_{\mathfrak{a}}$ *tem densidade de centro* $0.125 = \dfrac{1}{8}$ *e o número de vizinhos é* 24, *sendo exatamente como* $\boldsymbol{D}_4$. *Como* $\boldsymbol{D}_4$ *é o único reticulado com estes parâmetros, obtemos sua versão rotacionada com diversidade igual a 2.*

Exemplo 5.4.2. *(Construção de* $\boldsymbol{K}_{12,6}$*). Note que* $\phi(21) = 12$ *e que para outros valores de* n *tal que* $\phi(n) = 21$ *não resultam na versão rotacionada de* $\boldsymbol{K}_{12}$, *cuja densidade de centro é* 1/27. *O polinômio minimal de* $\theta = \zeta_{21}$ *sobre* $\mathbb{Q}$ *é dado na Tabela (5.3.2), o discriminante absoluto do corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{21})$ *é* $D_{\mathbb{K}} = 3^6.7^{10}$, $r_1 = 0$ *e* $r_2 = 6$. *Pela Equação* (3.4) *temos que*

$$N(\mathfrak{a}) = \frac{2^{12/2}}{\sqrt{3^6.7^{10}}} \frac{\rho^{12}}{\frac{1}{27}} = \frac{2^6\rho^{12}}{7^5},$$

e para $N(\mathfrak{a}) = 7$ *devemos tomar* $\rho = \dfrac{\sqrt{7}}{\sqrt{2}}$. *O ideal* $\mathfrak{a}$ *com norma 7 pode ser obtido da fatoração do ideal primo* (7), *que tem norma* 7^{12}, *ou seja,*

$$(7) = (7, \theta + 3)^6(7, \theta + 5)^6 = \mathfrak{a}_1^6\mathfrak{a}_2^6.$$

Como $N(\mathfrak{a}_1) = N(\mathfrak{a}_2) = 7$, *podemos escolher* $\mathfrak{a} = \mathfrak{a}_1$, *que tem a norma desejada. A matriz geradora do reticulado é* $\boldsymbol{G}_{\mathfrak{a}} = \boldsymbol{TG}$, *onde* $\boldsymbol{T}$ *é a matriz da representação integral de* $\mathfrak{a}$

$$T = \begin{pmatrix} 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

e $\boldsymbol{G}$ *é a matriz geradora de* $\sigma(\mathbb{A}_{\mathbb{K}})$. *O reticulado gerado por* $\boldsymbol{G}_{\mathfrak{a}}$ *tem densidade de centro* $\dfrac{1}{27}$ *e o número de vizinhos é* 756, *sendo exatamente como* $\boldsymbol{K}_{12}$. *Como* $\boldsymbol{K}_{12}$ *é o único reticulado com estes parâmetros, obtemos sua versão rotacionada com diversidade igual a 6.*

Exemplo 5.4.3. *(Construção de* $\Lambda_{16,8}$*). Note que* $\phi(40) = 16$ *e que para outros valores de* n *tal que* $\phi(n) = 16$ *não resultam na versão rotacionada de* Λ_{16}, *cuja densidade de centro é* 1/16. *O polinômio minimal de* $\theta = \zeta_{40}$ *sobre* $\mathbb{Q}$ *é dado na Tabela (5.3.2), o discriminante absoluto do corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{40})$ *é* $D_{\mathbb{K}} = 2^{32}.5^{12}$, $r_1 = 0$ *e* $r_2 = 8$. *Pela Equação* (3.4) *temos que*

$$N(\mathfrak{a}) = \frac{2^{16/2}}{\sqrt{2^{32}.5^{12}}} \frac{\rho^{16}}{\frac{1}{16}} = \frac{\rho^{16}}{5^6.2^4},$$

e para $N(\mathfrak{a}) = 2^4.5^2$ *devemos tomar* $\rho = \sqrt{2.5}$. *O ideal* $\mathfrak{a}$ *com tal norma pode ser obtido da fatoração dos ideais* (2) *e* (5) *que tem*

norma 2^{16} *e* 5^{16}, *respectivamente. Assim*

$$(2) = (2, \theta^4 + \theta^3 + \theta^2 + \theta + 1)^4 = \mathfrak{a}_1^4$$
$$(5) = (5, \theta^2 + 2)^4 (5, \theta^2 + 3)^4 = \mathfrak{a}_2^4 \mathfrak{a}_3^4.$$

Como, $N(\mathfrak{a}_1) = 2^4$, $N(\mathfrak{a}_2) = 5^2$, $N(\mathfrak{a}_3) = 5^2$, *podemos escolher* $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ *que tem a norma desejada* $N(\mathfrak{a}) = N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2) = 2^4 5^2$. *A matriz geradora do reticulado é* $\boldsymbol{G}_{\mathfrak{a}} = \boldsymbol{TG}$, *onde* $\boldsymbol{T}$ *é a matriz da representação integral de* $\mathfrak{a}$ *e* $\boldsymbol{G}$ *é a matriz geradora de* $\sigma(\mathbb{A}_{\mathbb{K}})$. *O reticulado gerado por* $\boldsymbol{G}_{\mathfrak{a}}$ *tem densidade de centro* $0,0625$ *e o número de vizinhos é* 4320, *sendo exatamente como* Λ_{16}. *Como* Λ_{16} *é o único reticulado com estes parâmetros, obtemos sua versão rotacionada com diversidade igual a 8.*

5.5 Conclusão

Duas diferentes aproximações tem sido usadas para estudar duas famílias de reticulados com o objetivo de atingir bom desempenho sobre ambos os canais Gaussianos e Rayleigh com desvanecimento.

A primeira família é gerada pelo homomorfismo canônico sobre o anel dos inteiros de um corpo de números. Entre os reticulados desta família, demos importância aos reticulados obtidos a partir de corpos totalmente reais e totalmente complexos. Vimos que os reticulados obtidos a partir de corpos totalmente reais tem bom desempenho sobre o canal Rayleigh com desvanecimento com uma diversidade máxima n. Mas eles tem um ganho negativo sobre o canal Gaussiano causado pela sua baixa densidade de empacotamento. Os reticulados obtidos a partir de corpos totalmente complexos tem um acordo entre diversidade e densidade de empacotamento. Eles mostram um ganho positivo sobre o canal Gaussiano

e bom desempenho sobre o canal Rayleigh com desvanecimento com uma diversidade $\frac{n}{2}$.

A segunda família de reticulados é gerada pelo homomorfismo canônico sobre determinados ideais nos anéis dos inteiros dos corpos ciclotômicos que são corpos totalmente complexos. Esta família inclui versões dos famosos reticulados conhecidos na literatura; $\boldsymbol{D}_4$, $\boldsymbol{E}_6$, $\boldsymbol{E}_8$, $\boldsymbol{K}_{12}$, Λ_{16} e Λ_{24}. Estes reticulados atuam de modo análogo aos reticulados de diversidade $\frac{n}{2}$ sobre o canal Rayleigh e então podem atingir a diversidade de 2 até 12. Além disso, estes são os melhores reticulados para o canal Gaussiano.

O ponto importante nesta conclusão é o fato de que corpos de números com discriminante absoluto mínimos são conhecidos somente em graus menores ou iguais a 8. Assim, a diversidade de reticulados obtidos a partir de corpos totalmente reais não podem exceder 8, a menos que encontremos corpos ótimos com alto grau. Ao contrário, os reticulados da segunda família são menos limitados na diversidade, $\Lambda_{24,12}$ atinge uma diversidade 12. Naturalmente, podemos pensar em construir $\Lambda_{32,16}$ e $\Lambda_{64,32}$ que tem diversidades 16 e 32, respectivamente. Mas somos limitados pela proporção da complexidade de um sistema sobre o ganho prático. Não podemos nos esquecer também que o estudo da primeira família possibilita-nos construir e entender a segunda família.