Construções de reticulados algébricos para transmissão de sinais

Grasiele C. Jorge[a], Antonio A. de Andrade[b] e Sueli I. R. Costa[a]

***Resumo*— Neste trabalho, apresentamos um método para construir constelações de reticulados que são adequadas para transmissão de sinais sobre os canais gaussiano e com desvanecimento do tipo Rayleigh via subcorpos totalmente reais de um corpo ciclotômico. Essas construções exibem diversidade máxima e boa distância produto mínima.**

***Palavras-Chave*— Reticulados rotacionados, diversidade, densidade de empacotamento, distância produto mínima.**

***Abstract*— In this paper, we present a method for constructing rotated lattice constellations which are suitable for signal transmission over both Gaussian and Rayleigh fading channels via totally real subfields of a cyclotomic field. These constructions exhibit full diversity and good minimum product distance.**

***Keywords*— Rotated lattices, diversity, packing density, minimum product distance.**

I. Introdução

Constelações de sinais tendo estrutura de reticulado têm sido utilizadas como suporte para transmissão de sinais sobre os canais gaussianos e com desvanecimento do tipo Rayleigh [6], [9]. Assim, bons reticulados têm sido construídos via teoria algébrica dos números no que tangea densidade de centro e também em relação à distância produto.

Um *reticulado* $\Lambda \subseteq \mathbb{R}^n$ é um subgrupo aditivo discreto do $\mathbb{R}^n$ gerado por combinações lineares inteiras de n vetores linearmente independentes $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$, isto é, $\Lambda = \{\sum_{i=1}^n a_i \boldsymbol{v}_i : \ a_i \in \mathbb{Z}, \text{ para todo } i = 1, 2, \cdots, n\}$, onde $\alpha = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\}$ é uma *base* para Λ. Uma matriz M cujas linhas são estes vetores é dita ser uma *matriz geradora* para Λ e a matriz $G = MM^t$ é chamada de *matriz de Gram*. O *determinante* de Λ é definido como $\det \Lambda = \det G$ e é um invariante sob mudança de base [7].

Um *empacotamento reticulado* é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que duas destas esferas tenham no máximo um ponto em comum e que o conjunto de seus centros forma um reticulado $\Lambda \subseteq \mathbb{R}^n$. A densidade de empacotamento de um reticulado Λ, $\Delta(\Lambda)$, é a proporção do espaço $\mathbb{R}^n$ coberto pelo empacotamento de raio máximo associado a esse reticulado. Devido a homogeneidade de distribuição de pontos em um reticulado, a *densidade de empacotamento* é dada por $\Delta(\Lambda) = \frac{\rho^n vol(B(1))}{(\det \Lambda)^{1/2}}$, onde ρ é metade da norma mínima euclidiana do reticulado e $vol(B(1))$ é o volume euclidiano da esfera unitária n-dimensional [7].

a-Departamento de Matemática, Universidade Estadual de Campinas, Campinas - SP, Brasil, E-mails: grajorge@gmail.com, sueli@ime.unicamp.br

b-Departamento de Matemática, Universidade Estadual Paulista, São José do Rio Preto - SP, Brasil, E-mail: andrade@ibilce.unesp.br

Este trabalho teve o apoio do CNPq 150802/2012-9, 309561/2009-4 e da Fapesp 2013/04124-6.

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. A diversidade de um elemento não nulo $\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in \Lambda$ é definida por $div(\boldsymbol{x}) = \min\{i : x_i \neq 0\}$, e a diversidade do reticulado Λ é definida por $div(\Lambda) = \min\{div(\boldsymbol{x}); \boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0}\}$. Se a diversidade do reticulado Λ é máxima ($div(\Lambda) = n$), a *distância produto mínima* de Λ é definida como $d_{min}(\Lambda) = \min\{\prod_{i=1}^n |y_i|; \ \boldsymbol{y} = (y_1, \cdots, y_n) \in \Lambda, \boldsymbol{y} \neq \boldsymbol{0}\}$ [4].

O problema de encontrar boas constelações de sinais para o canal gaussiano está associado à densidade de empacotamento do reticulado na métrica euclidiana [7], quanto maior for a densidade de empacotamento, menor é a probabilidade de erros na transmissão. Já para um canal com desvanecimento do tipo Rayleigh, uma probabilidade de erros mais baixa está associada à diversidade máxima (que pode ser obtida aplicando uma rotação no reticulado de forma que seus pontos não toquem os eixos coordenados) e a uma distância produto mínima grande [6].

Em [4], [9], considerando canais com desvanecimento do tipo Rayleigh e os parâmetros diversidade e distância produto mínima, foi proposta a construção de reticulados $\mathbb{Z}^n$-rotacionados, isto é, versões rotacionadas do reticulado $\mathbb{Z}^n$. Além de eficiente algoritmo de decodificação, a família de reticulados $\mathbb{Z}^n = \{(x_1, \cdots, x_n); x_i \in \mathbb{Z} \text{ para todo } i = 1, \cdots, n\}$ apresenta facilidade de rotulamento e boa forma na constelação. O problema que surge é como calcular a distância produto mínima dessas versões rotacionadas.

Na busca por resultados tanto para o problema da densidade de empacotamento (que possui solução apenas nas dimensões 1 a 8 e 24) quanto para o cálculo da diversidade e distância produto mínima tem-se utilizado construções algébricas de reticulados, pois estas, em geral, facilitam estimar tais parâmetros. Para o cálculo da densidade de empacotamento por exemplo, é necessário determinar o vetor de norma mínima, o que é um problema difícil (a conjectura é que seja NP-Hard [14]) para reticulados gerais.

A família de reticulados $D_n = \{(x_1, \cdots, x_n); \ \sum_{i=1}^n x_i \equiv 0 \ (mod\, 2)\}$ tem densidade de empacotamento maior quando comparada com a família $\mathbb{Z}^n$ e, de fato, são esses os reticulados mais densos nas dimensões $n = 3, 4$ and 5 [7].

Em [10], [11] foi proposta a construção algébrica de reticulados D_n-rotacionados. Comparando tais reticulados com a família de reticulados $\mathbb{Z}^n$-rotacionados podemos considerá-los eficientes tanto para o canal gaussiano (pois sua densidade de empacotamento é maior) quanto para o canal com desvanecimento do tipo Rayleigh (embora sua distância produto mínima é um pouco menor).

A abordagem deste trabalho, seguindo [1], [4], [5], [6], [10], [11] faz uso de teoria algébrica dos números para construir

reticulados $\mathbb{Z}^n$ e D_n-rotacionados para valores de n que não haviam sido considerados antes e calcular suas distâncias produto mínima.

II. Resultados básicos

Nesta seção, introduzimos algumas definições e resultados sobre teoria algébrica dos números que serão utilizados no decorrer do trabalho [13], [16], [18].

Sejam $\mathbb{K}$ e $\mathbb{K}_1$ corpos. Dizemos que $\mathbb{K}$ é uma *extensão* de $\mathbb{K}_1$ de grau $n = [\mathbb{K} : \mathbb{K}_1]$ se $\mathbb{K}_1 \subseteq \mathbb{K}$ e a dimensão do espaço vetorial $\mathbb{K}$ sobre $\mathbb{K}_1$ é n. Quando $\mathbb{K}_1 = \mathbb{Q}$, dizemos que $\mathbb{K}$ é um *corpo de números*.

Proposição 1: [16] Existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{K}_1(\theta) = \{\sum_{i=1}^{n} a_i\theta^i;\ a_i \in \mathbb{K}_1\}$ e existem exatamente n homomorfismos distintos $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$ que fixam $\mathbb{K}_1$.

Dizemos que $\mathbb{K}|\mathbb{K}_1$ é uma *extensão de Galois* se $\sigma_i(\mathbb{K}) \subseteq \mathbb{K}$ para todo $i = 1, \cdots, n$ e denotamos $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_i : \mathbb{K} \longrightarrow \mathbb{K};\ i = 1, \cdots, n\}$.

Chamamos de *norma* e *traço* de x, respectivamente, os valores $N_{\mathbb{K}:\mathbb{K}_1}(x) = \prod_{i=1}^{n} \sigma_i(x)$ e $Tr_{\mathbb{K}:\mathbb{K}_1}(x) = \sum_{i=1}^{n} \sigma_i(x)$.

Proposição 2: [13] Se $\mathbb{Q} \subseteq \mathbb{K}_1 \subseteq \mathbb{K}$ são corpos, então $N_{\mathbb{K}:\mathbb{K}_1}(\alpha) = N_{\mathbb{K}_1:\mathbb{Q}}(N_{\mathbb{K}:\mathbb{K}_1}(\alpha))$ e $T_{\mathbb{K}:\mathbb{K}_1}(\alpha) = T_{\mathbb{K}_1:\mathbb{Q}}(T_{\mathbb{K}:\mathbb{K}_1}(\alpha))$.

Seja $\{\omega_1, \ldots, \omega_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{K}_1$. O *discriminante* de $\mathbb{K}|\mathbb{K}_1$ é definido como $d_{\mathbb{K}:\mathbb{K}_1} = det[\sigma_j(\omega_i)]^2$ e é um invariante sobre mudança de base.

Dizemos que um conjunto A é um *$\mathbb{Z}$-módulo livre de posto* n se A é um grupo aditivo abeliano e existem n elementos $\{a_1, \cdots, a_n\}$ em A que são linearmente independentes sobre $\mathbb{Z}$ e tal que $A = \{\sum_{i=1}^{n} \alpha_i a_i; \alpha_i \in \mathbb{Z}$ para todo $i = 1, \cdots, n\}$.

Proposição 3: [16] Se $\mathbb{K}$ é um corpo de números de grau n, então o conjunto $\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K};\ x$ é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}\}$ é um anel, chamado de *anel de inteiros* de $\mathbb{K}|\mathbb{Q}$, e todo ideal $I \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.

Dizemos que $\mathbb{K}$ é um corpo de números *totalmente real* se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ para todo $i = 1, \cdots, n$.

A seguir definimos o homomorfismo torcido e obtemos a partir do mesmo o conceito de reticuldado algébrico.

Definição 1: [2], [3] Sejam $\mathbb{K}$ um corpo de números totalmente real e $\alpha \in \mathbb{K}$ tal que $\alpha_i = \sigma_i(\alpha) > 0$ para todo $i = 1, \cdots, n$. O homomorfismo

$$\begin{aligned} \sigma_\alpha : \mathbb{K} &\longrightarrow \mathbb{R}^n \\ x &\longmapsto \left(\sqrt{\alpha_1}\sigma_1(x), \cdots, \sqrt{\alpha_n}\sigma_n(x)\right) \end{aligned}$$

é chamado de *homomorfismo torcido*.

No que se segue, seja $\mathbb{K}$ um corpo de números totalmente real.

Proposição 4: [4] Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre com $\mathbb{Z}$-base $\{w_1, \cdots, w_n\}$, então a imagem $\Lambda = \sigma_\alpha(\mathcal{I})$ é um reticulado em $\mathbb{R}^n$ com base $\{\sigma_\alpha(w_1), \cdots, \sigma_\alpha(w_n)\}$ e $G = (Tr_{\mathbb{K}:\mathbb{Q}}(\alpha w_i w_j))_{i,j=1}^{n}$ é uma matriz de Gram para Λ.

Uma matriz geradora para $\sigma_\alpha(\mathcal{I})$ é $M = M_1 D$, onde

$$M_1 = \begin{pmatrix} \sigma_1(w_1) & \sigma_2(w_1) & \cdots & \sigma_{n-1}(w_1) & \sigma_n(w_1) \\ \sigma_1(w_2) & \sigma_2(w_2) & \cdots & \sigma_{n-1}(w_2) & \sigma_n(w_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(w_n) & \sigma_2(w_n) & \cdots & \sigma_{n-1}(w_n) & \sigma_n(w_n) \end{pmatrix}$$

e

$$D = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 & \cdots & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

Proposição 5: [10] Se $\mathcal{I} \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n, então $\Lambda = \sigma_\alpha(\mathcal{I})$ é um reticulado com diversidade máxima e sua distância produto mínima é dada por $d_{p,min}(\Lambda) = \sqrt{N_{\mathbb{K}:\mathbb{Q}}(\alpha)} min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}:\mathbb{Q}}(y)|$.

Proposição 6: [4] Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal principal e $\Lambda = \sigma_\alpha(\mathcal{I})$, então $d_{p,min}(\Lambda) = \sqrt{\frac{det(\Lambda)}{d_{\mathbb{K}:\mathbb{Q}}}}$.

Proposição 7: [3] Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n e $N(\mathcal{I}) = |\mathcal{O}_{\mathbb{K}}/\mathcal{I}|$, então

$$det(\sigma_\alpha(\mathcal{I})) = N_{\mathbb{K}:\mathbb{Q}}(\mathcal{I})^2 N_{\mathbb{K}:\mathbb{Q}}(\alpha) d_{\mathbb{K}:\mathbb{Q}}. \quad (1)$$

III. Subcorpos dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um primo ímpar.

Seja $n \in \mathbb{N}^*$. Um elemento $\zeta_n \in \mathbb{C}$ é dito uma raiz n-ésima primitiva da unidade se $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$ para todo $m = 1, 2, \cdots, n-1$. O corpo $\mathbb{Q}(\zeta_n)$ é chamado de n-ésimo *corpo ciclotômico*.

Uma família de corpos muito utilizada na construção de reticulados algébricos é a dos corpos ciclotômicos [18]. Neste trabalho, vamos construir reticulados através de subcorpos $\mathbb{K}$ dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um primo ímpar.

Primeiro vamos fazer um resumo de algumas propriedades dos corpos $\mathbb{Q}(\zeta_p)$ que serão utilizadas na caracterização de seus subcorpos.

A extensão $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ é de *Galois* e $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = \{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}$ onde $\sigma_i(\zeta_p) = \zeta_p^i$ para todo $i \in \mathbb{Z}$. Temos que σ_{p-1} é a conjugação complexa e $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ é um grupo cíclico gerado por σ_a para algum $a = 1, \cdots, p-1$ [13].

Do Teorema da Correspondência de Galois segue que os subcorpos de $\mathbb{Q}(\zeta_p)$ são os corpos fixos por subgrupos H do grupo de Galois $G = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, isto é,

$$\mathbb{K} = \mathbb{Q}(\zeta_p)_H = \{\alpha \in \mathbb{Q}(\zeta_p) : \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\}.$$

Mais ainda, os subcorpos totalmente reais de $\mathbb{Q}(\zeta_p)$ são os corpos fixos pelos subgrupos H de $G = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ que contém a conjugação complexa $\sigma_{p-1} \in H$.

O seguinte diagrama pode ajudar o entendimento.

$$\begin{array}{ccc} \mathbb{Q}(\zeta) & \longleftarrow & \{id\} \\ | & & | \\ \mathbb{K} & \longleftarrow & H \\ | & & | \\ \mathbb{Q} & \longleftarrow & G \end{array}$$

No que se segue, sejam $e_i = \zeta_p^i + \zeta_p^{-i}$ para todo $i = 1, 2, \cdots, p-1$. A próxima proposição permite caracterizar alguns parâmetros de qualquer subcorpo $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$.

Proposição 8: [17] Sejam $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ com $[\mathbb{K} : \mathbb{Q}] = n$ e $\theta = T_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta_p)$. Se σ_a gera $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, então

1) $\mathbb{K} = \mathbb{Q}(\theta)$,
2) $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\{\sigma_a(\theta), \sigma_{a^2}(\theta), \cdots, \sigma_{a^n}(\theta)\}$,
3) $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_a, \sigma_{a^2}, \cdots, \sigma_{a^n}\}$,
4) $d_{\mathbb{K}:\mathbb{Q}} = p^{n-1}$.

Exemplo 1: Seja $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{29})$ tal que $[\mathbb{K} : \mathbb{Q}] = 7$. Utilizando o Teorema da Correspondência de Galois, segue que $\mathbb{K}$ é o corpo fixo por $H = \{\sigma_1, \sigma_{12}, \sigma_{17}, \sigma_{28}\}$, pois H é o único subgrupo de $G = \langle\sigma_2\rangle$ tal que $[G : H] = 4$. Note que $\theta = T_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta_p) = e_1 + e_{12}$ e $\mathbb{K} = \mathbb{Q}(\theta)$. Uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$ é dada por $\{\sigma_2(\theta), \sigma_{2^2}(\theta), \cdots, \sigma_{2^7}(\theta)\} = \{e_2+e_5, e_4+e_{10}, e_8+e_9, e_{13}+e_{11}, e_3+e_7, e_6+e_{14}, e_{12}+e_1\}$.

IV. Reticulados rotacionados

A construção ciclotômica de reticulados $\mathbb{Z}^n$-rotacionados foi introduzida por Eva Bayer-Fluckiger et al. em [4], onde os autores consideram o corpo de números totalmente real maximal $\mathbb{K} = \mathbb{Q}(\zeta_p+\zeta_p^{-1})$, $\alpha = 2-(\zeta_p+\zeta_p^{-1})$ e mostram que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado $\mathbb{Z}^{\frac{p-1}{2}}$-rotacionado.

Neste trabalho, vamos construir reticulados $\mathbb{Z}^n$-rotacionados via subcorpos totalmente reais de $\mathbb{Q}(\zeta_p)$, ou seja, subcorpos de $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Sejam $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ um corpo de números totalmente real com $[\mathbb{K} : \mathbb{Q}] = n$ e $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$.

Segundo a Proposição 7, uma condição necessária para a construção de um reticulado $\mathbb{Z}^n$-rotacionado, escalonado por $\sqrt{c}$, onde $c \in \mathbb{Z}$, via um $\mathbb{Z}$-módulo livre $\mathcal{I}$ de $\mathcal{O}_\mathbb{K}$, é a existência de um elemento α tal que $\sigma(\alpha) \geq 0$, para todo $\sigma \in Gal(\mathbb{K} : \mathbb{Q})$ e $c^n = N_{\mathbb{K}:\mathbb{Q}}(\alpha)N_{\mathbb{K}:\mathbb{Q}}(\mathcal{I})^2 d_\mathbb{K}$. Tomando $\mathcal{I} = \mathcal{O}_\mathbb{K}$ e $c = p$, como $d_\mathbb{K} = p^{n-1}$ pela Proposição 8, segue que uma condição necessária para construir um reticulado $\mathbb{Z}^n$-rotacionado $\frac{1}{\sqrt{c}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é encontrar um elemento $\alpha \in \mathcal{O}_\mathbb{K}$ tal que $N_{\mathbb{K}:\mathbb{Q}}(\alpha) = p$. A próxima proposição apresenta uma sugestão para α.

Proposição 9: Se $Gal(\mathbb{Q}(\zeta_p) : \mathbb{K}) = \{\psi_1, \cdots, \psi_r\}$ e $\alpha = \prod_{i=1}^r(1 - \psi_i(\zeta_p))$, então $N_{\mathbb{K}:\mathbb{Q}}(\alpha) = p$.

Demonstração: Temos que $\phi(x) = 1 + x + x^2 + \cdots + x^{p-1} = (x - \zeta)(x - \zeta^2)\cdots(x - \zeta^{p-1})$ [18]. Assim, $N_{\mathbb{Q}(\zeta_p):\mathbb{Q}}(1 - \zeta_p) = \prod_{i=1}^{p-1}\sigma_i(1 - \zeta_p) = \phi(1) = p$. Usando propriedades da norma, segue que $p = N_{\mathbb{Q}(\zeta_p):\mathbb{Q}}(1 - \zeta_p) = N_{\mathbb{K}:\mathbb{Q}}(N_{\mathbb{Q}(\zeta_p):\mathbb{K}}(1 - \zeta_p)) = N_{\mathbb{K}:\mathbb{Q}}(\prod_{i=1}^r(1 - \psi_i(\zeta_p)))$, isto é, $N_{\mathbb{K}:\mathbb{Q}}(\alpha) = p$. ■

No que se segue, vamos melhorar a maneira de representar o elemento α. Como $\mathbb{K}$ é um corpo de números totalmente real, segue que a conjugação complexa σ_{p-1} é um elemento de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{K})$. Assim, se $\sigma_i \in Gal(\mathbb{Q}(\zeta_p) : \mathbb{K})$ para algum i, então $\sigma_{p-1}\circ\sigma_i = \sigma_{p-i} \in Gal(\mathbb{Q}(\zeta_p) : \mathbb{K})$. Portanto, existem inteiros s_i para $i = 1, \cdots, r/2$ tal que $Gal(\mathbb{Q}(\zeta_p) : \mathbb{K}) =$

$$\left\{\sigma_1, \sigma_{p-1}, \sigma_{s_1}, \sigma_{p-s_1}, \cdots, \sigma_{s_{\left(\frac{r}{2}-1\right)}}, \sigma_{p-s_{\left(\frac{r}{2}-1\right)}}\right\}.$$

Assim, podemos escrever

$$\begin{aligned}\alpha &= (1 - \zeta_p)(1 - \zeta_p^{-1})\cdots\left(1 - \zeta_p^{s_{\left(\frac{r}{2}-1\right)}}\right)\left(1 - \zeta_p^{-s_{\left(\frac{r}{2}-1\right)}}\right)\\ &= (2 - e_1)(2 - e_{s_1})\cdots\left(2 - e_{s_{\left(\frac{r}{2}-1\right)}}\right).\end{aligned} \tag{2}$$

Na próxima proposição, mostramos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado unimodular, isto é, é um reticulado que possui matriz de Gram com entradas inteiras e determinante ±1. Recentemente, tais reticulados têm despertado um grande interesse, como podemos perceber através das referências [8], [15].

Proposição 10: Se $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ é um corpo de números totalmente real com $[\mathbb{K} : \mathbb{Q}] = n$, $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = \langle\sigma_a\rangle$ para algum $a \in \mathbb{Z}$ e se α é como da Equação (2), então o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é unimodular.

Demonstração: Seja $\theta = e_1+e_{s_1}+\cdots+e_{s_{\left(\frac{r}{2}-1\right)}}$. De [17] segue que uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$ é $\{\sigma_a(\theta), \cdots, \sigma_{a^n}(\theta)\}$ e uma matriz de Gram de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é dada por $G = (g_{ij})_{i,j=1}^n$, onde $g_{ij} = Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\sigma_{a^i}(\theta)\sigma_{a^j}(\theta)) = \sum_{k=1}^n \sigma_{a^k}(\alpha\sigma_{a^i}(\theta)\sigma_{a^j}(\theta))$. Pela Proposição 2, segue que $N_{\mathbb{K}:\mathbb{Q}}(\alpha\mathcal{O}_\mathbb{K}) = p$, e assim, $\alpha\mathcal{O}_\mathbb{K}$ é um ideal primo de $\mathcal{O}_\mathbb{K}$. Como $\alpha\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$, pelo [16, Teorema 1, p.71], segue que $\alpha\mathcal{O}_\mathbb{K}$ está sobre $p\mathcal{O}_\mathbb{K}$. Assim, $p\mathcal{O}_\mathbb{K} = (\alpha\mathcal{O}_\mathbb{K})^n$. Como $\sigma_{a^k}(\alpha\mathcal{O}_\mathbb{K})$ está sobre $p\mathcal{O}_\mathbb{K}$ para todo $k = 1, \cdots, n$, segue que $\sigma_{a^k}(\alpha\mathcal{O}_\mathbb{K}) = \alpha\mathcal{O}_\mathbb{K}$. Assim, $Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\sigma_{a^i}(\theta)\sigma_{a^j}(\theta)) \in \alpha\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$. Por construção, como $\det\sigma_\alpha(\mathcal{O}_\mathbb{K}) = p^n$, segue que $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado unimodular. ■

Proposição 11: $T_{\mathbb{K}:\mathbb{Q}}(\alpha) = p$.

Demonstração: Utilizando propriedades do traço e [4], segue que $p = T_{\mathbb{Q}(\zeta_p):\mathbb{Q}}(\zeta) = T_{\mathbb{K}:\mathbb{Q}}(T_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta)) = T_{\mathbb{K}:\mathbb{Q}}(\alpha)$. ■

De acordo com as Proposições 10 e 11, mostramos que o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado unimodular ímpar com norma mínima 1. De fato, como $1 \in \mathcal{O}_\mathbb{K}$, segue que $T_{\mathbb{K}:\mathbb{Q}}(\alpha)$ corresponde a norma do vetor $\sigma_\alpha(1)$. Portanto, tal reticulado possui a mesma densidade de empacotamento que a família de reticulados $\mathbb{Z}^n$-rotacionados, que é dada por $\Delta(\Lambda) = \frac{\rho^n vol(B(1))}{(\det\Lambda)^{1/2}} = \frac{vol(B(1))}{2^n}$.

Como $\mathcal{O}_\mathbb{K}$ é um ideal principal, segundo a Proposição 6, segue que a distância produto mínima de tal reticulado é dada por $d_{p,min}\left(\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})\right) = \frac{1}{\sqrt{d_{\mathbb{K}:\mathbb{Q}}}}$. Desta forma, fixada uma dimensão n, a maior distância produto mínima obtida através desta contrução ciclotômica é realizada no corpo de números de grau n com o menor discriminante.

Uma possibilidade para caracterizar a família de reticulados $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ como reticulados $\mathbb{Z}^n$-rotacionados é relacionar suas matrizes de Gram. É conhecido que se dois reticulados possuem a mesma matriz de Gram, então são equivalentes na métrica euclidiana [12].

A família de reticulados $\mathbb{Z}^n$-rotacionados obtida em [4, Proposição 1, p. 704] é um caso particular da família de reticulados obtida na Proposição 10. Quando $\mathbb{K} = \mathbb{Q}(\zeta_p+\zeta_p^{-1})$ é possível perceber um padrão em qualquer matriz de Gram

associada a $\mathbb{Z}$-base $\{e_1, e_2, \cdots, e_n\}$ que é dada por

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

Quando consideramos o caso mais geral, ou seja, subcorpos de $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, não obtemos o mesmo tipo de padrão como podemos perceber no próximo exemplo. Neste caso, utilizamos o software Mathematica para procurar por uma matriz mudança de base tal que a matriz de Gram associada a nova base seja a matriz identidade e então mostramos que $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é de fato um reticulado $\mathbb{Z}^9$-rotacionado.

Exemplo 2: Seja $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{73})$ um corpo de números totalmente real tal que $[\mathbb{K} : \mathbb{Q}] = 9$ e $Gal(\mathbb{Q}(\zeta_{73}) : \mathbb{Q}) = \langle\sigma_5\rangle$. Assim, $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = e_1 + e_{10} + e_{22} + e_{27}$. Seja $\alpha = (2-e_1)(2-e_{10})(2-e_{22})(2-e_{27})$. Uma matriz de Gram G de $\frac{1}{\sqrt{73}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ associada a $\mathbb{Z}$-base $\{e_5 + e_{23} + e_{36} + e_{11}, e_{25} + e_{31} + e_{34} + e_{18}, e_{21} + e_9 + e_{24} + e_{17}, e_{32} + e_{28} + e_{26} + e_{12}, e_{14} + e_6 + e_{16} + e_{13}, e_3 + e_{30} + e_7 + e_8, e_{15} + e_4 + e_{35} + e_{33}, e_2 + e_{20} + e_{29} + e_{19}, e_{10} + e_{27} + e_1 + e_{22}\}$ of $\mathcal{O}_\mathbb{K}$ é dada por

$$\begin{pmatrix} 36 & -9 & 14 & -19 & -20 & 6 & 0 & 2 & -2 \\ -9 & 10 & 5 & -3 & 1 & 2 & 0 & -10 & 2 \\ 14 & 5 & 24 & -18 & -16 & 9 & 1 & -15 & -2 \\ -19 & -3 & -18 & 20 & 15 & -8 & 0 & 10 & -1 \\ -20 & 1 & -16 & 15 & 16 & -6 & 0 & 5 & 1 \\ 6 & 2 & 9 & -8 & -6 & 4 & 0 & -6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & -1 \\ 2 & -10 & -15 & 10 & 5 & -6 & -1 & 16 & 0 \\ -2 & 2 & -2 & -1 & 1 & 0 & -1 & 0 & 3 \end{pmatrix}$$

Considerando a matriz mudança de base

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & -2 & -1 & -2 & 0 \\ 1 & 1 & 2 & 1 & 2 & 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & -1 & 1 \\ 2 & 2 & 3 & 2 & 3 & 1 & 1 & 2 & 2 \\ -1 & -2 & -1 & -2 & -1 & -4 & -2 & -2 & -1 \\ -3 & -5 & -5 & -4 & -5 & -6 & -4 & -6 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 4 & 6 & 4 & 5 & 3 & 3 & 5 & 4 \end{pmatrix}$$

segue que $TGT^t = I_{9\times 9}$.

Exemplo 3: Seja $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{41})$ tal que $[\mathbb{K} : \mathbb{Q}] = 10$ e $Gal(\mathbb{Q}(\zeta_{41}) : \mathbb{Q}) = \langle\sigma_6\rangle$, onde $\sigma_i(\zeta) = \zeta^i$, para $i = 1, 2, \cdots, 40$. Assim, $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = e_1 + e_9$. Seja $\alpha = (2-e_1)(2-e_9)$. Uma matriz de Gram G para $\frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é dada por

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

Neste caso, tem-se que $m = 8$. Utilizando o software Mathematica, encontramos a matriz mudança de base

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

tal que $TGT^t = I_{10\times 10}$.

Em alguns casos especiais podemos caracterizar tais reticulados sem relacionar as matrizes de Gram. É conhecido que o único reticulado unimodular ímpar nas dimensões $n \leq 8$ é um reticulado $\mathbb{Z}^n$-rotacionado [7].

Proposição 12: Se $[\mathbb{K} : \mathbb{Q}] \leq 8$, então os reticulados unimodulares da Proposição 10 são reticulados $\mathbb{Z}^n$-rotacionados.

De acordo com a natureza do problema conjecturamos que:

Conjectura 1: Os reticulados unimodulares da Proposição 10 são reticulados $\mathbb{Z}^n$-rotacionados para todo $n \in \mathbb{N}^*$.

V. O CASO $n = \frac{p-1}{4}$

Seja $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ um corpo de números totalmente real tal que $[\mathbb{K} : \mathbb{Q}] = n$ e $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = 4$. Como $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = 4$, segue que existe um elemento $\sigma_s \in Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ com ordem 4 tal que $Gal(\mathbb{Q}(\zeta_p) : \mathbb{K}) = \{\sigma_1, \sigma_{p-1}, \sigma_s, \sigma_{p-s}\}$. Da Seção IV, sejam $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = \langle\sigma_a\rangle$, $\theta = e_1 + e_s$ e $\mathbb{K} = \mathbb{Q}(\theta)$.

Proposição 13: Se $\alpha = (2 - e_1)(2 - e_s)$, então $Tr_{\mathbb{K}:\mathbb{Q}}(\sigma_{a^j}(e_1 + e_s)) = -1$ para todo $j = 1, \cdots, n$.

Demonstração: Por propriedades do traço, segue que $-1 = Tr_{\mathbb{Q}(\zeta_p):\mathbb{Q}}(\sigma_{a^j}(\zeta_p)) = Tr_{\mathbb{K}:\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\sigma_{a^j}(\zeta_p))) = Tr_{\mathbb{K}:\mathbb{Q}}(\sigma_{a^j}(\theta))$. ■

Utilizando a proposição anterior e propriedades do traço demonstramos a seguinte proposição:

Proposição 14: Se m é um inteiro positivo tal que $\sigma_{a^m}(e_1 + e_s) = e_{s+1} + e_{s-1}$, então

$$Tr_{\mathbb{K}:\mathbb{Q}}(\alpha(\sigma_{a^j}(e_1 + e_s))^2) = \begin{cases} 6p & \text{se } j = n, \\ p & \text{se } j = n - m, \\ 2p & \text{se } 2a^j \equiv as \text{ (mod p)}, \\ 4p & \text{caso contrário.} \end{cases}$$

Proposição 15: Se $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo com $\mathbb{Z}$-base $\{\sigma_{a^j}(e_1+e_s), j = 1, \cdots, n$ e $j \neq n-m\} \cup 2\sigma_{a^{n-m}}(e_1+e_s)$, então o reticulado $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I})$ é par e $\det\Lambda = 4$. Além disso, $\Delta(\Lambda)$ é a mesma densidade dos reticulados D_n.

Demonstração: Segue da Proposição 14 que $\frac{1}{\sqrt{p}}Tr_{\mathbb{K}:\mathbb{Q}}(\alpha\sigma_{a^j}(e_1 + e_s)\sigma_{a^j}(e_1 + e_s))$ é par para todo $j \neq n - m$. Agora, para $j = n - m$, segue que $\frac{1}{\sqrt{p}}Tr_{\mathbb{K}:\mathbb{Q}}(\alpha 2\sigma_{a^{n-m}}(e_1 + e_s)2\sigma_{a^{n-m}}(e_1 + e_s)) = 4$. Portanto, o reticulado $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I})$ é um reticulado par. Como $N(\mathcal{I}) = |\mathcal{O}_\mathbb{K}/\mathcal{I}| = 2$, pela Proposição 7, segue que $\det\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I}) = N_{\mathbb{K}:\mathbb{Q}}(\alpha)N_{\mathbb{K}:\mathbb{Q}}(\mathcal{I})^2 d_{\mathbb{K}:\mathbb{Q}} = \frac{1}{p^n}(p\,2^2\,p^{n-1}) = 4$. Novamente, pela Proposição 14, segue que existe um vetor em $\det\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I})$ com norma 2. Com isso, $\Delta(\Lambda) = \frac{\rho^n vol(B(1))}{(\det\Lambda)^{1/2}} = \frac{\sqrt{2}^n vol(B(1))}{2} = 2^{\frac{-(n+2)}{2}} vol(B(1))$. ■

Todo reticulado par contido em $\mathbb{Z}^n$ também está contido em D_n [11]. Utilizando a Proposição 12 segue que o reticulado $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I})$ obtido na Proposição 15 é um D_n-rotacionado para todo $n \leq 8$, isto é, para $p = 13, 17, 29$.

Exemplo 4: Seja $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{41})$ como no Exemplo 3 e $\mathcal{I}$ o $\mathbb{Z}$-módulo da Proposição 15. Neste caso, segue que $m = 8$ e uma

$\mathbb{Z}$-base de $\mathcal{I}$ é dada por $\{\sigma_6(e_1+e_9), \sigma_{6^3}(e_1+e_9), \sigma_{6^4}(e_1+e_9), \sigma_{6^5}(e_1+e_9), \sigma_{6^6}(e_1+e_9), \sigma_{6^7}(e_1+e_9), \sigma_{6^8}(e_1+e_9), \sigma_{6^9}(e_1+e_9), \sigma_{6^{10}}(e_1+e_9)\} \cup 2\sigma_{6^2}(e_1+e_9)$. Como $\frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{I}) \subseteq \frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ e $\frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado $\mathbb{Z}^{10}$-rotacionado, segue que $\frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{I})$ é um reticulado D_{10}-rotacionado.

Exemplo 5: Seja $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{37})$ tal que $[\mathbb{K}:\mathbb{Q}] = 9$ e $Gal(\mathbb{Q}(\zeta_{37})\mathbb{Q}) = \langle\sigma_2\rangle$. Assim, $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = e_1 + e_6$. Seja $\alpha = (2-e_1)(2-e_6)$. Uma matriz de Gram de $\frac{1}{37}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é dada por

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

Neste caso, $m = 5$ e $j = n - m = 4$. Utilizando o software Mathematica, encontramos a matriz mudança de base

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & -1 & -1 & -3 & 0 & -2 & -2 & -2 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & -1 & -1 & -1 & -3 & 0 & -2 & -2 & -1 \\ -1 & -2 & -3 & -3 & -5 & -2 & -4 & -4 & -3 \\ 1 & 2 & 2 & 3 & 3 & 2 & 3 & 3 & 2 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 \end{pmatrix}$$

tal que $TGT^t = I_{9\times 9}$. Portanto, o reticulado $\frac{1}{37}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado $\mathbb{Z}^9$-rotacionado e o reticulado $\frac{1}{37}\sigma_\alpha(\mathcal{I})$ para $\mathcal{I}$ como na Proposição 15 é um reticulado D_9-rotacionado.

A *distância produto mínima relativa* de um reticulado equivale a distância produto mínima de uma versão escalonada do reticulado com vetor de norma mínima unitário e estabelece uma forma de comparar reticulados com normas mínimas diferentes [10].

Proposição 16: Se $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I})$ como na Proposição 15, então $d_{p,rel}(\Lambda) \geq 2^{\frac{1-p}{8}} p^{\frac{5-p}{8}}$.

Demonstração: Pela Proposição 5, segue que $d_p(\sigma_\alpha(\mathcal{I})) = \sqrt{N(\alpha)} min_{0\neq y\in\mathcal{I}}|N(y)| \geq \sqrt{N(\alpha)}$ pois $|N(y)| \geq 1$. Assim, $d_{p,rel}(\Lambda) = \frac{1}{\sqrt{p}^{\frac{p-1}{4}}} \frac{1}{\sqrt{2}^{\frac{p-1}{4}}} \sqrt{p} = 2^{\frac{1-p}{8}} p^{\frac{5-p}{8}}$. ■

A Tabela I compara a densidade de centro e a distância produto mínima relativa dos reticulados $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$, $\Lambda_1 = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{I})$ quando $n = (p-1)/4$.

p	n	$\sqrt[n]{d_{p,rel}(\Lambda)}$	$\sqrt[n]{d_{p,rel}(\Lambda_1)}$ $(\geq)$	$\delta(\Lambda)$	$\delta(\Lambda_1)$
13	3	0.42529	0.30073	0.125	0.17677
17	4	0.34561	0.24438	0.0625	0.125
29	7	0.23619	0.16701	0.00781	0.04419
37	9	0.20092	0.14207	0.00195	0.02209
41	10	0.18804	0.13296	0.00098	0.01563
101	25	0.10913	0.07716	$2.980 * 10^{-8}$	0.00009

TABELA I
DENSIDADE DE EMPACOTAMENTO VERSUS DISTÂNCIA PRODUTO MÍNIMA RELATIVA

VI. CONCLUSÃO

Em [4] foi introduzida a construção ciclotômica de reticulados $\mathbb{Z}^n$-rotacionados para $n = (p-1)/2$ com p primo ímpar via os corpos $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Neste trabalho, apresentamos uma construção ciclotômica de famílias de reticulados rotacionados com diversidade máxima e mesma densidade de empacotamento que os reticulados $\mathbb{Z}^n$ e D_n para todo n via subcorpos $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Provamos que em dimensões até 8, os reticulados obtidos são de fato equivalentes a $\mathbb{Z}^n$ e D_n, os quais vem sendo considerados para transmissões de sinais sobre os canais gaussianos e com desvanecimento do tipo Rayleigh.

Como um trabalho futuro é de particular interesse uma efetiva comparação de desempenho entre as famílias aqui propostas e as que vem sendo consideradas.

REFERÊNCIAS

[1] A.A. Andrade, C. Alves, T.B. Carlos. Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$, International Journal of Applied Mathematics, v. 19, n. 3, p. 321-331, 2006.

[2] E. Bayer-Fluckiger. Ideal lattices. Proceedings of the conference number theory and diophantine geometry (Zurich, 1999), Cambridge Univ. Press, 2002, 168 - 184.

[3] E. Bayer-Fluckiger. Lattices and number fields. Contemporary Mathematics, v. 241, p. 69-84, 1999.

[4] E. Bayer-Fluckiger, F. Oggier, E. Viterbo. New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel. IEEE Trans. Inform. Theory, v. 50, n. 4, p. 702-714, 2004.

[5] E. Bayer-Fluckiger, F. Oggier, E. Viterbo. Algebraic lattice constellations: bounds on performance. IEEE Trans. Inform. Theory, v. 52, n. 1, p. 319-327, p. 2006.

[6] J. Boutros, E. Viterbo, C. Rastello, J-C. Belfiore. Good lattice constellations for both Rayleigh fading and Gaussian channels. IEEE Trans. Inform. Theory, v. 42, n. 2, p. 502-517, 1996.

[7] J.H. Conway, N.J.A. Sloane. Sphere packings, lattices and groups. New York, Springer-Verlag, 1988.

[8] J. H. Conway and N. J. A. Sloane, *A Note on Optimal Unimodular Lattices*, Journal of Number Theory, v. 72, p. 357-362, 1998.

[9] X. Giraud and J.C. Belfiore. Constellations matched to the Rayleigh fading channel. IEEE Trans. Inform. Theory, v. 42, n. 1, p. 106-115, 1996.

[10] G.C. Jorge, A.J. Ferrari, S.I.R. Costa. Rotated D_n-lattices. Journal of Number Theory, v. 132, p. 2397-2406, 2012.

[11] G. C. Jorge, S. I. R. Costa, On rotated D_n-lattices construct via totally real number fields, Archiv der Mathematik, v. 100, p. 323-332, 2013.

[12] C.C. Lavor, M.M. Alvez, R.M. Siqueira, S.I.R. Costa, *Uma introdução à teoria de códigos*, SBMAC, 2006.

[13] D.A. Marcus. Number Fields. New York, Springer-Verlag, 1977.

[14] D. Micciancio, O. Regev, *Lattice-Based Cryptography* em *Post Quantum Cryptography,* D.J. Bernstein, J. Buchmann, E. Dahmen (eds), p. 147-191, Springer, 2009.

[15] G. Nebe and B. Venkov, *Unimodular lattices with long shadow*, Journal of Number Theory, v. 99, p. 307-317, 2003.

[16] P. Samuel. Algebraic theory of numbers. Paris, Hermann, 1970.

[17] J. P. G. Vicente, Reticulados de posto 3 em corpos abelianos. Dissertação de Mestrado, Ibilce - Unesp, São José do Rio Preto - SP, Brasil, 2000.

[18] L.C. Washington. Introduction to cyclotomic fields. New York, Springer-Verlag, 1982.