Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

Uma nota sobre reticulados rotacionados para o canal com desvanecimento do tipo Rayleigh.

Agnaldo J. Ferrari
Depto. de Matemática, FC, UNESP,
17033-360, Bauru, SP
E-mail: ferrari@fc.unesp.br,

Antonio A. de Andrade
Depto. de Matemática, IBILCE, UNESP,
15054-000, São José do Rio Preto, SP
E-mail: andrade@ibilce.unesp.br.

Resumo: *Neste trabalho, apresentamos a construção de uma família de reticulados $\mathbb{Z}^n$ rotacionados em dimensão 3^{r-1}, onde r é par, obtidos via $\mathbb{Z}$-módulos, com diversidade máxima, representando constelações de sinais que são boas para o canal com desvanecimento do tipo Rayleigh. Uma expressão para a distância produto destes reticulados é obtida através de propriedades algébricas e, apresentamos um limitante inferior para a distância produto mínima nesta família. A escolha por constelações cúbicas se deve ao fato de que os reticulados $\mathbb{Z}^n$ são ligeiramente piores em termos de ganho de forma, uma vez que estes reticulados não são os mais densos em suas dimensões, ou seja, apresentam maior ganho de forma os reticulados que possuem maior densidade de empacotamento, apesar disso, os reticulados $\mathbb{Z}^n$ são usualmente mais fáceis de rotular e decodificar, assim, oferecem um bom equilibrio entre boa forma e facilidade de rotulamento.*

Palavras-chave: *Reticulados, Diversidade, Distância produto, Canal, Transmissão de sinais.*

Introdução

Recentemente tem-se observado um grande avanço na área das Telecomunicações, cuja finalidade é desenvolver sistemas que forneçam serviços de excelente qualidade, a altas taxas de transmissão/armazenamento e com baixa probabilidade de erro.

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 destinatário usando um canal de comunicação. Um canal é um meio físico por onde a informação é transmitida/armazenada e está sujeito a vários tipos de ruídos, imperfeições e interferências que geram distorções. Um canal muito usado na transmissão de sinais é o canal com desvanecimento do tipo Rayleigh, caracterizado pela propagação por múltiplos percursos formados pela reflexão e/ou difração do sinal transmitido.

Em relação à probabilidade de erro na transmissão de sinais, pela Teoria dos Códigos Corretores de Erros [12], ao transmitirmos uma informação podemos ter um ruído, fazendo com que a mensagem recebida seja diferente da enviada. Desse modo, a teoria dos códigos corretores de erros surgiu da necessidade de detectar erros e recuperar a mensagem enviada ao receptor, construindo, desta forma, códigos com pequena probabilidade de ocorrerem erros. Uma maneira de projetar uma constelação de sinais é representar cada sinal como um ponto em um espaço euclidiano n-dimensional. O processo de projetar um conjunto de palavras-código pode ser redu-

zido a um problema geométrico de alocação de pontos em uma região de um espaço. Os códigos construídos a partir de reticulados constituem numa das técnicas de alocação de pontos.

Constelações de sinais tendo a estrutura de reticulados são consideradas importantes para a transmissão de sinais pois as estruturas algébricas e geométricas dos reticulados facilitam no processo de codificação e decodificação. Usualmente o problema de encontrar boas constelações de sinais para o canal com desvanecimento do tipo Rayleigh está associado a busca por reticulados com diversidade máxima e distância produto mínima grande ([2], [6]).

Exposição do problema

Para os reticulados em geral, a distância produto mínima é usualmente dificil de calcular. Nosso objetivo é trabalhar com reticulados associados a corpos de números que possuam diversidade máxima, pois nestes casos uma expressão para a distância produto mínima pode ser obtida através das propriedades algébricas dos referidos corpos. A seguir apresentamos conceitos básicos relativos a reticulados e teoria algébrica dos números que são necessários para o desenvolvimento do nosso trabalho [6], [11], [13] e [15].

Definição 1*:* Sejam $v_1, v_2, \cdots, v_m$ um conjunto de vetores linearmente independentes no espaço vetorial $\mathbb{R}^n$. O conjunto

$$\Lambda = \left\{ \sum_{i=1}^{m} \alpha_i v_i;\ \alpha_i \in \mathbb{Z} \right\}$$

é chamado um *reticulado* de posto m, e o conjunto $\{v_1, v_2, \cdots, v_m\}$ é chamado uma base do reticulado Λ.

Definição 2*:* Seja $\{v_1, v_2, \cdots, v_m\}$ uma base para o reticulado Λ. A matriz $M = (v_{ij})$, onde $v_i = (v_{i1}, \cdots, v_{in})$, para $i = 1, \cdots, m$, é chamada uma *matriz geradora* para o reticulado Λ.

Definição 3*:* Seja M uma matriz geradora para o reticulado Λ. A matriz $G = MM^t$ é chamama uma *matriz de Gram* para o reticulado Λ, onde t denota a transposição.

Definição 4*:* Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $\mathbf{x} = (x_1, \cdots, x_n) \in \Lambda$. A *diversidade* de Λ é definida por

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

Definição 5*:* Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade máxima n e $\mathbf{x} = (x_1, \cdots, x_n) \in \Lambda$. A distância produto mínima de Λ é definida por

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

Definição 6*:* Um corpo de números $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, ou seja, $\mathbb{Q} \subseteq \mathbb{K}$ e $\mathbb{K}$ é visto como um espaço vetorial de dimensão finita sobre $\mathbb{Q}$, e sua dimensão é chamado o grau de $\mathbb{K}$ sobre $\mathbb{Q}$ e denotado por $[\mathbb{K} : \mathbb{Q}] = n$.

Definição 7*:* Seja $\mathbb{K}$ um corpo de números de grau finito n. O conjunto $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha$ é raiz de um polinômio mônico sobre $\mathbb{Z}\}$ é um anel chamado anel dos inteiros algébricos do corpo $\mathbb{K}$.

Definição 8*:* Seja A um anel. Um A-módulo (ou módulo sobre o anel A) é um par (M, φ), onde M é um grupo abeliano e $\varphi : A \times M \to M$ é tal que para todo $a, b \in A$ e $m, n \in M$, temos:

DOI: 10.5540/03.2015.003.01.0225

(i) $\varphi(ab, m) = \varphi(a, bm)$.
(ii) $\varphi(a + b, m) = \varphi(a, m) + \varphi(b, m)$.
(iii) $\varphi(a, m + n) = \varphi(a, m) + \varphi(a, n)$.
(iv) $\varphi(1, m) = m$.

Definição 9*:* Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. Um ideal fracionário I de $\mathbb{K}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo de $\mathbb{K}$ tal que $\alpha\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$, para algum $\alpha \in \mathcal{O}_{\mathbb{K}}$.

Teorema 1 *[11]:* Seja $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos do corpo $\mathbb{K}$. Todo ideal fracionário não nulo $\mathcal{A}$ de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.

Teorema 2 *[13]:* Dado $\mathbb{K}$ um corpo de números de grau n, existem exatamente n homomorfismos distintos $\{\sigma_i\}_{i=1}^{n}$ de $\mathbb{K}$ em $\mathbb{C}$ que fixam o corpo $\mathbb{Q}$.

Definição 10*:* Um homomorfismo σ_i é dito *real* se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, e o corpo $\mathbb{K}$ é dito *totalmente real* se σ_i é real para todo $i = 1, 2, \cdots, n$.

Definição 11*:* Sejam $\mathbb{K}$ um corpo de números de grau n e $x \in \mathbb{K}$. Os valores

$$N(x) = N_{\mathbb{K}|\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x) \quad \text{e} \quad Tr(x) = Tr_{\mathbb{K}|\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

são chamados *norma* e *traço* de x na extensão $\mathbb{K}|\mathbb{Q}$, respectivamente.

Teorema 3 *[13]:* Se $\mathbb{K}$ é um corpo de números de grau n e $x \in \mathcal{O}_{\mathbb{K}}$, então $N(x), Tr(x) \in \mathbb{Z}$.

Definição 12*:* Seja $\{e_1, e_2, \cdots, e_n\}$ uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. O inteiro

$$d_{\mathbb{K}} = (det[\sigma_j(e_i)]_{i,j=1}^{n})^2$$

é chamado de *discriminante* do corpo $\mathbb{K}$.

Definição 13*:* Seja $\mathcal{A}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. A *norma* do ideal $\mathcal{A}$ é definida por

$$N(\mathcal{A}) = |\mathcal{O}_{\mathbb{K}}/\mathcal{A}|,$$

ou seja, é a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}$ por $\mathcal{A}$.

Observação 2*:* Se $\mathcal{A}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$, isto é, $\mathcal{A} = \alpha\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{A}) = |N(\alpha)|$.

Método utilizado

A fim de reproduzir reticulados que sejam novas leituras de reticulados conhecidos na literatura, usamos resultados da teoria algébrica dos números. Mais especificamente, o propósito é construir reticulados via o anel dos inteiros algébricos de um corpo de números totalmente real através do *homomorfismo torcido*, pois neste caso os reticulados obtidos possuem diversidade máxima, representando assim constelações de sinais eficientes para o canal com desvanecimento do tipo Rayleigh [10] e [14].

Definição 14*:* Sejam $\mathbb{K}$ um corpo de números totalmente real e $\alpha \in \mathbb{K}$ tal que $\alpha_i = \sigma_i(\alpha) > 0$ para todo $i = 1, 2, \cdots, n$. O homomorfismo $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ dado por $\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \cdots, \sqrt{\alpha_n}\sigma_n(x))$ é chamado de *homomorfismo torcido*. Quando $\alpha = 1$ é chamado de *homomorfismo de Minkowski*.

Teorema 4 *[11]:* Se $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\{e_1, \cdots, e_n\}$, então a imagem $\Lambda = \sigma_\alpha(\mathcal{A})$ é um reticulado no $\mathbb{R}^n$ com base $\{\sigma_\alpha(e_1), \cdots, \sigma_\alpha(e_n)\}$, ou equivalentemente,

com matriz geradora $M = (\sigma_\alpha(e_{ij}))_{i,j=1}^n$, onde $e_i = (e_{i1}, \cdots, e_{in})$, para $i = 1, \cdots, n$.

Teorema 5 *[2]:* Se $\mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\mathbb{K}$ é um corpo totalmente real, então o reticulado $\Lambda = \sigma_\alpha(\mathcal{A})$ possui diversidade máxima.

Teorema 6 *[4]:* Se $\mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\mathbb{K}$ é um corpo totalmente real, então a matriz de Gram associada à matriz geradora M do reticulado $\Lambda = \sigma_\alpha(\mathcal{A})$ é dada por

$$G = MM^t = (Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i \overline{e_j}))_{i,j=1}^n.$$

Teorema 7 *[4]:* Se $\mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\mathbb{K}$ é um corpo totalmente real, então a distância produto mínima do reticulado $\Lambda = \sigma_\alpha(\mathcal{A})$ é dada por

$$d_{p,min}(\Lambda) = \sqrt{N_{\mathbb{K}|\mathbb{Q}}(\alpha)} \min_{0 \neq x \in \mathcal{A}} |N_{\mathbb{K}|\mathbb{Q}}(x)|.$$

Corolário 1 *[4]:* Se $\mathcal{A}$ é ideal principal de $\mathcal{O}_\mathbb{K}$, então

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

Resultados obtidos

Nesta seção, apresentamos a construção de uma família de reticulados $\mathbb{Z}^n$ rotacionados via $\mathbb{Z}$-módulos em dimensão 3^{r-1}, onde r é par. A construção é feita via o anel dos inteiros algébricos dos subcorpos maximais reais de corpos ciclotômicos [7], [8] e [9].

Definição 15*:* Um elemento $\zeta = \zeta_m \in \mathbb{C}$ é chamado uma raiz m-ésima da unidade se $\zeta^m = 1$, com $m \geq 1$ um inteiro, e é dito uma raiz m-ésima primitiva da unidade se $\zeta^m = 1$, com $\zeta^d \neq 1$ para qualquer $1 \leq d \leq m$.

Definição 16*:* Dizemos que $\mathbb{L}$ é o m-ésimo corpo ciclotômico se $\mathbb{L}$ é a adjunção de $\mathbb{Q}$ e uma raiz primitiva m-ésima da unidade, ou seja, $\mathbb{L} = \mathbb{Q}(\zeta)$.

Teorema 8 *[15]:* O anel dos inteiros de $\mathbb{L} = \mathbb{Q}(\zeta)$ é $\mathcal{O}_\mathbb{L} = \mathbb{Z}[\zeta]$.

Teorema 9 *[15]:* Se $\mathbb{L} = \mathbb{Q}(\zeta)$, então $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$ é o subcorpo maximal real de $\mathbb{L}$, o anel dos inteiros de $\mathbb{K}$ é $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta + \zeta^{-1}]$ e $[\mathbb{K} : \mathbb{Q}] = \varphi(m)/2$, onde φ é a função de Euler.

Tomando $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, onde $\zeta = \zeta_{3^r}$, segue que $n = [\mathbb{K} : \mathbb{Q}] = 3^{r-1}$, e assim, otem-se o seguinte resultado,

Proposição 1*:* Sejam $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, onde $\zeta = \zeta_{3^r}$, $e_0 = 1$ e $e_i = \zeta^i + \zeta^{-i}$, para $i = 1, 2, \cdots, 3^{r-1} - 1$, $\alpha = 3$.

(1) Se $i = 0, 1, \cdots, 3^{r-1} - 1$, então $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i \overline{e_i}) = \begin{cases} 3^r, & \text{se } i = 0 \\ 2.3^r, & \text{caso contrário.} \end{cases}$

(2) Se $i \neq 0$, então $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i \overline{e_0}) = 0$.

(3) Se $i \neq 0$, $j \neq 0$ e $i \neq j$, então $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i \overline{e_j}) = \begin{cases} -3^r, & \text{se } i + j = 3^{r-1} \\ 0, & \text{caso contrário.} \end{cases}$

Segue diretamente do Teorema 3.1.2 [3] e da transitividade do Traço, ou seja,
$Tr_{\mathbb{K}|\mathbb{Q}}(\zeta^i + \zeta^{-i}) = Tr_{\mathbb{L}|\mathbb{Q}}(\zeta^i)$, onde $\mathbb{L} = \mathbb{Q}(\zeta)$.

Proposição 2*:* O reticulado $\Lambda = \frac{1}{\sqrt{3^r}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ possui uma matriz geradora $M_1 = \frac{1}{\sqrt{3^r}}NA$, onde $N = (\sigma_j(e_{i-1}))_{i,j=1}^{n-1}$, $n = 3^{r-1}$, $A = diag(\sqrt{\sigma_k(\alpha)})$, e a matriz de Gram associada é dada

por

$$G_1 = M_1 M_1^t = \begin{pmatrix} 1 & & & & & & & & 0 \\ & 2 & & & & & & & -1 \\ & & 2 & & & & & -1 & \\ & & & \cdots & & & \cdots & & \\ & & & & 2 & -1 & & & \\ & & & & -1 & 2 & & & \\ & & & \cdots & & & \cdots & & \\ & & -1 & & & & & 2 & \\ 0 & -1 & & & & & & & 2 \end{pmatrix}.$$

Segue diretamente do Teorema 6 e da Proposição 1.

Lema 1*:* Se a matriz geradora do reticulado $\Lambda = \frac{1}{\sqrt{3^r}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é dada por $M_2 = \frac{1}{\sqrt{3^r}} N_1 A$, onde

$$N_1 = \begin{pmatrix} \sigma_1(e_0) & \sigma_2(e_0) & \cdots & \sigma_n(e_0) \\ \sigma_1(e_1) & \sigma_2(e_1) & \cdots & \sigma_n(e_1) \\ \sigma_1(e_{n-1}) & \sigma_2(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \\ \sigma_1(e_3) & \sigma_2(e_3) & \cdots & \sigma_n(e_3) \\ \cdots & \cdots & & \cdots \\ \sigma_1(e_{\frac{n-1}{2}}) & \sigma_2(e_{\frac{n-1}{2}}) & \cdots & \sigma_n(e_{\frac{n-1}{2}}) \\ \sigma_1(e_{n-2}) & \sigma_2(e_{n-2}) & \cdots & \sigma_n(e_{n-2}) \\ \sigma_1(e_2) & \sigma_2(e_2) & \cdots & \sigma_n(e_2) \\ \sigma_1(e_{\frac{n+1}{2}}) & \sigma_2(e_{\frac{n+1}{2}}) & \cdots & \sigma_n(e_{\frac{n+1}{2}}) \\ \cdots & \cdots & & \cdots \\ \sigma_1(e_{n-3}) & \sigma_2(e_{n-3}) & \cdots & \sigma_n(e_{n-3}) \end{pmatrix},$$

então a matriz de Gram associada é dada por

$$G_2 = M_2 M_2^t = \begin{pmatrix} W_1 & & \\ & & \\ & & W_2 \end{pmatrix},$$

onde $W_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$ e $W_2 = \begin{pmatrix} 2 & & & & & & & & -1 \\ & 2 & & & & & & -1 & \\ & & 2 & & & & -1 & & \\ & & & \cdots & & & \cdots & & \\ & & & & 2 & -1 & & & \\ & & & & -1 & 2 & & & \\ & & & \cdots & & & \cdots & & \\ & -1 & & & & & & 2 & \\ -1 & & & & & & & & 2 \end{pmatrix}$ é uma matriz quadrada de ordem $n-3$.

Temos que a matriz N_1 é a matriz N da Proposição 2 com algumas linhas permutadas, assim a matriz G_2 é a matriz de Gram resultante desta permutação.

Proposição 3*:* Seja $\mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ um $\mathbb{Z}$-módulo com $\mathbb{Z}$-base

$$\{w_0, w_1, \cdots, w_{n-1}\},$$

onde
(1) $w_0 = 2e_0 + 2e_{n-1}$, $w_1 = 2e_0 + 2e_1$, $w_2 = -2e_0 + 2e_1 + 2e_{n-1}$;
(2) para $j = 3, 7, \cdots, \frac{n-13}{2}$,

$$w_j = e_j + e_{j+2} - e_{n-j-2} - e_{n-j}; \qquad w_{j+1} = e_{j+1} + e_{j+3} - e_{n-j-3} - e_{n-j-1};$$

$w_{j+2} = e_j - e_{j+2} + e_{n-j-2} - e_{n-j}$; $w_{j+3} = e_{j+1} - e_{j+3} + e_{n-j-3} - e_{n-j-1}$;

(3) para $j = \frac{n-5}{2}$,

$w_j = e_j + e_{j+2} - e_{n-j-2} - e_{n-j}$; $w_{j+1} = -e_2 + e_{j+1} - e_{n-j-1} + e_{n-2}$;

$w_{j+2} = e_j - e_{j+2} + e_{n-j-2} - e_{n-j}$; $w_{j+3} = e_2 + e_{j+1} - e_{n-j-1} - e_{n-2}$;

(4) para $j = \frac{n+3}{2}$,

$w_j = e_{j-3} + 2e_{j-2} - e_{n-2} - e_2 + 2e_{j-1} + e_j$; $w_{j+1} = e_{j-4} + 2e_{j-3} - e_{j-2} - e_{j-1} + 2e_j + e_{j+1}$;

$w_{j+2} = 2e_{j-4} - e_{j-3} - e_{n-2} - e_2 - e_j + 2e_{j+1}$; $w_{j+3} = -e_{j-4} - e_{j-2} - 2e_{n-2} - 2e_2 - e_{j-1} - e_{j+1}$;

(5) para $j = \frac{n+11}{2}, \frac{n+19}{2}, \cdots, n-4$,

$w_j = e_{n-j} + 2e_{n-j+1} - e_{n-j+2} - e_{j-2} + 2e_{j-1} + e_j$;

$w_{j+1} = e_{n-j-1} + 2e_{n-j} - e_{n-j+1} - e_{j-1} + 2e_j + e_{j+1}$;

$w_{j+2} = 2e_{n-j-1} - e_{n-j} - e_{n-j+2} - e_{j-2} - e_j + 2e_{j+1}$;

$w_{j+3} = -e_{n-j-1} - e_{n-j+1} - 2e_{n-j+2} - 2e_{j-2} - e_{j-1} - e_{j+1}$.

Se $\alpha = 3$, então o reticulado $\frac{1}{2\sqrt{3^{r+1}}}\sigma_\alpha(\mathcal{A}) \subseteq \mathbb{R}^{3^{r-1}}$, onde r é par, é um reticulado $\mathbb{Z}^{3^{r-1}}$ rotacionado.

Na demonstração é dada uma matriz T de modo que o reticulado com matriz geradora $S = (1/\sqrt{3^r})TN_1A$ (N_1 é a matriz do Lema 1 e A é a matriz da Proposição 2) possui matriz de Gram $G = 12I_{3^{r-1}}$. Portanto, $S_1 = (1/2\sqrt{3^{r+1}})TN_1A$ é a matriz geradora do reticulado $\mathbb{Z}^{3^{r-1}}$, onde

$$TN_1 = \begin{pmatrix} \sigma_1(w_0) & \sigma_2(w_0) & \cdots & \sigma_n(w_0) \\ \sigma_1(w_1) & \sigma_2(w_1) & \cdots & \sigma_n(w_1) \\ \cdots & \cdots & & \cdots \\ \sigma_1(w_{n-1}) & \sigma_2(w_{n-1}) & \cdots & \sigma_n(w_{n-1}) \end{pmatrix}$$

e segue o resultado.

Proposição 4: Se $\Lambda = \frac{1}{2\sqrt{3^{r+1}}}\sigma_\alpha(\mathcal{A}) \subseteq \mathbb{R}^{3^{r-1}}$, onde r é par, com α e $\mathcal{A}$ como na Proposição 3, então a distância produto mínima relativa satisfaz

$$d_{p,rel}(\Lambda) \geq 2^{-3^{r-1}}\ 3^{\frac{-r3^{r-1}}{2}}. \tag{1}$$

Dado $x \in \mathcal{A}$ temos que $N(x) \in \mathbb{Z}$, logo $min_{0\neq x\in\mathcal{A}}|N(x)| \geq 1$. Como $N(\alpha) = 3^{3^{r-1}}$, segue que $d_{p,min}(\sigma_\alpha(\mathcal{A})) = \sqrt{N(\alpha)}min_{0\neq x\in\mathcal{A}}|N(x)| \geq \sqrt{3^{3^{r-1}}}$. Portanto, a distância produto mínima relativa satisfaz

$$d_{p,rel}\left(\frac{1}{2\sqrt{3^{r+1}}}\sigma_\alpha(\mathcal{A})\right) \geq \frac{1}{(2\sqrt{3^{r+1}})^{3^{r-1}}}\sqrt{3^{3^{r-1}}} = 2^{-3^{r-1}}\ 3^{\frac{-r3^{r-1}}{2}},$$

e segue o resultado.

A Tabela 1 apresenta um limitante inferior para a distância produto mínima normalizada dado pela Inequação (1) para a familia de reticulados $\mathbb{Z}^n$ rotacionados obtidos na Proposição 3.

Conclusões

Neste trabalho, apresentamos uma nova família de reticulados $\mathbb{Z}^n$ rotacionados em dimensão $n = 3^{r-1}$, onde r é par. Como as constelações foram construídas usando $\mathbb{Z}$-módulos, o cálculo da distância produto mínima nem sempre é uma tarefa fácil, o que não aconteceria se ao invés de $\mathbb{Z}$-módulos trabalhássemos com ideais principais (Teorema 7 e Corolário 1). Assim, estabelecemos um limitante inferior para a distância produto mínima nos reticulados construídos. Uma perspectiva futura é expandir a construção para r ímpar e assim completar a dimensão potência de 3.

r	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$ $(\geq)$
2	3	0.166667
4	27	0.055555
6	243	0.018518
8	2187	0.006172
10	19683	0.002057
12	177147	0.000685
14	1594323	0.000228

Tabela 1: Limitante para a distância produto mínima relativa de $\mathbb{Z}^n$, onde $n = 3^{r-1}$ e r é par.

Referências

[1] 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, 2006.

[2] 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, 1996.

[3] A. L. Flores, "Reticulados em corpos abelianos". Tese de Doutorado, FEEC-UNICAMP, Campinas, 2012.

[4] E. B. Fluckiger, "Lattices and number fields". *Contemporary Mathematics*, v. 241, pp. 69-84, 1999.

[5] E. B. Fluckiger, G. Nebe, On the euclidean minimum of some real number fields. *Journal de Theorie des Nombres de Bordeaux*, v. 17, n. 2, pp. 437-454, 2005.

[6] 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, 2004.

[7] J. C. Interlando, J. O. D. Lopes, T. P. N. Neto, The discriminant of abelian number fields. *Journal of Algebra and its Applications*, v. 5, n. 1, pp. 35-41, 2006.

[8] C. H. S. Jesus, "Discriminante dos subcorpos de corpos ciclotômicos de condutores potência de um primo ímpar". *Tese de Doutorado*, UFPB, 2007.

[9] D. A. Marcus, "Numbers fields". *Springer-Verlag*, New York, 1977.

[10] F. Oggier, "Algebraic methods for channel coding". *Tese de doutorado*, École Polytechnique fédérale de Lausanne, 2005.

[11] P. Samuel, "Algebraic theory of numbers". *Hermann*, Paris, 1967.

[12] C. Shannon, Mathematical theory of communication. *Bell Systems Technical Journal*, v. 27, pt. I: pp. 379-423; pt. II: pp. 623-656, 1948.

[13] I. Stewart, D. Tall, "Algebric number theory". *Chapman & Hall*, New York, 1987.

[14] 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.

[15] L. Washington, "Introduction to cyclotomic fields". *Springer-Verlag*, New York, 1982.

