Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Sobre Versões Rotacionadas dos Reticulados $\mathbb{Z}^n$ para Codificação em Sistemas de Transmissão

Fabiano Pinto Tavares[1]
DEMAT/IFMA, São Luís, MA
João Eloir Strapasson[2]
FCA/UNICAMP, Limeira, SP
Sueli Irene Rodrigues Costa[3]
IMECC/UNICAMP, Campinas, SP

Resumo. Este trabalho consiste numa investigação sobre versões rotacionadas dos reticulados $\mathbb{Z}^n$ com baixa dimensão. Nas dimensões 2 e 3, de modo alternativo aos conhecidos reticulados algébricos, exibimos as construções das versões rotacionadas de reticulados com diversidade máxima, que possuem máximas distâncias produtos mínimas. Nas dimensões $3, 5$ e 8, fixado um reticulado, obtivemos um outro reticulado com a mesma distância produto mínima e com uma densidade de empacotamento maior do que o original.

Palavras-chave. Reticulados, distância produto mínima, torção generalizada.

1 Introdução

Em canais com desvanecimento do tipo Rayleigh são consideradas constelações de sinais n-dimensionais esculpidas no conjunto de pontos de um reticulado $\Lambda \subset \mathbb{R}^n$. Visando minimizar a probabilidade de erro na decodificação de uma palavra-código devemos encontrar reticulados com diversidade máxima e máxima distância produto mínima. Conforme podemos ver em [2, 9], essas constelações de sinais podem ser obtidas a partir de rotações do $\mathbb{Z}^n$.

Construções de reticulados rotacionados com diversidade máxima e boas distâncias produtos geralmente são feitas via teoria algébrica dos números. Em [1, 7–10] encontram-se construções de reticulados rotacionados nesse formato.

Construímos em [11], a partir da álgebra dos complexos, uma versão rotacionada do $\mathbb{Z}^2$ e demonstramos que esta possui a maior distância produto mínima possível. Construímos também, a partir da álgebra dos quatérnios, uma versão rotacionada do $\mathbb{Z}^3$ e demonstramos que esta possui a maior distância produto mínima possível, quando consideramos as rotações em torno da reta com vetor diretor $(1, 1, 1)$. A vantagem dessa abordagem é que podemos descrever as rotações que geram tais reticulados, o que em geral pode ser difícil no caso dos reticulados algébricos.

Em canais de ruído branco gaussiano também são consideradas constelações de sinais n-dimensionais esculpidas no conjunto de pontos de um reticulado $\Lambda \subset \mathbb{R}^n$. Conforme podemos ver em [4, 5] para minimizarmos a probabilidade de erro de decodificação devemos maximizar as densidades de empacotamento dos reticulados considerados. Assim, se um reticulado possuir boa distância produto mínima e boa densidade de empacotamento, o mesmo pode ser útil a canais com desvanecimento do tipo Rayleigh e a canais gaussianos simultaneamente.

[1]fabiano.tavares@ifma.edu.br
[2]strapass@unicamp.br
[3]sueli@unicamp.br

A partir daí, definimos torção generalizada de um reticulado qualquer e observamos que tal versão torcida preserva a distância produto mínima de reticulados com diversidade máxima. Conjecturamos que não existe versão torcida da rotação "ótima" do $\mathbb{Z}^2$ com densidade superior a do próprio $\mathbb{Z}^2$. Encontramos versões torcidas das rotações "ótimas" do $\mathbb{Z}^3, \mathbb{Z}^5$ e $\mathbb{Z}^8$ que possuem "boas" densidades, já que estas podem ser úteis simultaneamente a canais do tipo Rayleigh e a canais gaussianos.

Este trabalho está subdividido nas seguintes secões: Preliminares (nesta seção iremos introduzir os elementos essenciais deste trabalho), Versões Rotacionadas dos Reticulados $\mathbb{Z}^2$ e $\mathbb{Z}^3$, (aqui exibimos as nossas construções das versões rotacionadas "ótimas" do $\mathbb{Z}^2$ e do $\mathbb{Z}^3$ via álgebras dos complexos e dos quatérnios respectivamente), e Torção Generalizada (aqui construímos versões torcidas mais densas das versões rotacionadas "ótimas" do $\mathbb{Z}^3$, $\mathbb{Z}^5$ e $\mathbb{Z}^8$).

2 Preliminares

Nesta seção vamos introduzir alguns conceitos básicos, limitados aos essenciais a este trabalho, mais detalhes vide [5, 9].

2.1 Reticulados

Sejam $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_m$ vetores LI em $\mathbb{R}^n$. Um **reticulado** $\Lambda \subset \mathbb{R}^n$ com base $\{\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_m\}$ é definido por

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

Se $n = m$, dizemos que o reticulado Λ tem o **posto completo**. Uma **matriz geradora** para um reticulado Λ é uma matriz $n \times m$ formada pelas colunas dos vetores que formam uma base deste, isto é, $B = [\mathbf{b}_1 \ \mathbf{b}_2 \ ... \ \mathbf{b}_m]$.

O reticulado hipercúbico $\mathbb{Z}^n$ é definido como $\mathbb{Z}^n = \{(x_1, x_2, ..., x_n) : x_i \in \mathbb{Z}, \ i = 1, 2, ..., n\}$. Uma base para $\mathbb{Z}^n$ é a base canônica do $\mathbb{R}^n$, $\{\mathbf{e}_1, ..., \mathbf{e}_n\}$, em que $\mathbf{e}_i = (0, ..., 1, ..., 0)$ é o vetor com 1 na i-ésima coordenada e 0 nas demais.

Dada uma matriz geradora B para um reticulado Λ, definimos sua **matriz de Gram** por $G = B^t B$.

Seja G uma matriz de Gram de um reticulado Λ. O **determinante** de Λ é dado por $\det(\Lambda) = \det(G)$ e seu **volume** por $\text{Vol}(\Lambda) = \sqrt{\det(\Lambda)}$.

A **norma mínima** de um reticulado Λ, corresponde ao mínimo entre todas as normas euclidianas dos vetores não-nulos de Λ, isto é, $\mu = \min_{\mathbf{0} \neq \mathbf{x} \in \Lambda} ||\mathbf{x}||$, em que $||\mathbf{x}|| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$.

A **densidade de empacotamento** de Λ é definida como

$$\Delta(\Lambda) = \frac{\text{Vol}(B^n((\mathbf{0}; \mu/2))}{\text{Vol}(\Lambda)},$$

em que $B^n((\mathbf{0}; \mu/2)$ é uma bola aberta em $\mathbb{R}^n$ de centro em $\mathbf{0}$ e raio $\mu/2$.

Dois reticulados $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ são **equivalentes** se existirem uma matriz ortogonal Q, um número real $c \neq 0$, matrizes geradoras B_1 e B_2 para Λ_1 e Λ_2, respectivamente, de modo que $B_1 = cQB_2$.

2.2 Reticulados Algébricos

Um reticulado Λ tem **diversidade** $L \leq n$ se L é o número máximo tal que qualquer vetor $\mathbf{0} \neq \mathbf{y} \in \Lambda$ tenha pelo menos L coordenadas diferentes de zero.

DOI: 10.5540/03.2022.009.01.0308

Conforme podemos ver em [3], reticulados algébricos construídos sobre corpos de números totalmente reais têm **diversidade máxima** $L = n$.

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto completo com diversidade máxima. A **distância produto mínima** de Λ é definida como

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

No que segue, $\mathbb{K}$ é um corpo de números totalmente real de grau n, $\{\sigma_i\}_{i=1}^n$ denotam os n mergulhos de $\mathbb{K}$ em $\mathbb{R}$.

Um **reticulado ideal** é um reticulado $\Lambda = (\mathcal{I}, q_\alpha)$ em que $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um ideal do anel de inteiros $\mathcal{O}_\mathbb{K}$ e $q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Q}$, $q_\alpha(x,y) = Tr(\alpha x y)$,[4] para todo $x, y \in \mathcal{I}$, em que $\alpha \in \mathbb{K}$ é totalmente positivo (ie, $\sigma_i(\alpha) > 0$ para todo $i = 1, ..., n$).

Teorema 2.1 ([9]). *Seja $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$,[5] em que $p \geq 5$ é primo. Então $\Lambda = (\mathcal{O}_\mathbb{K}, \frac{1}{p} q_\alpha)$, em que $\alpha = (1 - \zeta_p)(1 - \zeta_p^{-1})$ e $q_\alpha(x,y) = Tr(\alpha x y)$, é equivalente ao reticulado $\mathbb{Z}^n$, em que $n = (p-1)/2$.*

Temos, por [9], que $\{e_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^n$ é uma base integral de $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, em que $\sigma_i(e_j) = \zeta_p^{ij} + \zeta_p^{-ij} = 2\cos\left(\frac{2\pi i j}{p}\right)$ e decorre, ainda por [9], do Teorema 2.1 que

$$R = \frac{1}{\sqrt{p}} D \Sigma T \tag{1}$$

é uma *matriz geradora do reticulado $\mathbb{Z}^n$ em uma versão rotacionada*, em que D, Σ e T são matrizes quadradas de ordem n tais que $D = \mathrm{diag}(\sqrt{\sigma_1(\alpha)}, ..., \sqrt{\sigma_n(\alpha)})$, $\Sigma = [\sigma_{ij}]$, $\sigma_{ij} = \sigma_i(e_j)$ e $T = [t_{ij}]$,

$$t_{ij} = \begin{cases} 1, & \text{se} \quad i \geq j \\ 0, & \text{se} \quad i < j. \end{cases}$$

Teorema 2.2 ([9]). *Seja $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ em que $p \geq 5$ é primo. A distância produto mínima do reticulado $\Lambda = (\mathcal{O}_\mathbb{K}, \frac{1}{p} q_\alpha)$, em que $\alpha = (1 - \zeta_p)(1 - \zeta_p^{-1})$ e $q_\alpha(x,y) = Tr(\alpha x y)$, é*

$$d_{p,\min}(\Lambda) = p^{-\frac{n-1}{2}}.$$

A seguir, apresentamos construções explícitas resultantes dos Teoremas 2.1 e 2.2.

A versão rotacionada do $\mathbb{Z}^5$ é obtida quando consideramos o corpo de números $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$. Da Eq. (1), segue que sua matriz geradora R é dada por

$$\begin{bmatrix} -0.169891 & -0.455734 & -0.596885 & -0.548529 & -0.326019 \\ -0.326019 & -0.596885 & -0.169891 & 0.455734 & 0.548529 \\ -0.455734 & -0.326019 & 0.548529 & 0.169891 & -0.596885 \\ -0.548529 & 0.169891 & 0.326019 & -0.596885 & 0.455734 \\ -0.596885 & 0.548529 & -0.455734 & 0.326019 & -0.169891 \end{bmatrix}. \tag{2}$$

Do Teorema 2.2, temos que $d_{p,\min}(\mathbb{Z}^5) = \frac{1}{11^2}$.

De igual modo, a versão rotacionada do $\mathbb{Z}^8$ é obtida quando consideramos o corpo de números $\mathbb{K} = \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$. Da Eq. (1), segue que sua matriz geradora R é dada por

[4] Se $x \in \mathbb{K}$, então $Tr(x) = \sum_{i=1}^n \sigma_i(x)$.

[5] ζ_p é a $p-$ésima raiz da unidade.

$$\begin{bmatrix} -0.0891316 & -0.255357 & -0.387095 & -0.466554 & -0.483002 & -0.434218 & -0.32679 & -0.175228 \\ -0.175228 & -0.434218 & -0.466554 & -0.255357 & 0.0891316 & 0.387095 & 0.483002 & 0.32679 \\ -0.255357 & -0.483002 & -0.175228 & 0.32679 & 0.466554 & 0.0891316 & -0.387095 & -0.434218 \\ -0.32679 & -0.387095 & 0.255357 & 0.434218 & -0.175228 & -0.466554 & 0.0891316 & 0.483002 \\ -0.387095 & -0.175228 & 0.483002 & -0.0891316 & -0.434218 & 0.32679 & 0.255357 & -0.466554 \\ -0.434218 & 0.0891316 & 0.32679 & -0.483002 & 0.255357 & 0.175228 & -0.466554 & 0.387095 \\ -0.466554 & 0.32679 & -0.0891316 & -0.175228 & 0.387095 & -0.483002 & 0.434218 & -0.255357 \\ -0.483002 & 0.466554 & -0.434218 & 0.387095 & -0.32679 & 0.255357 & -0.175228 & 0.0891316 \end{bmatrix}. \tag{3}$$

Do Teorema 2.2, temos que $d_{p,\min}(\mathbb{Z}^8) = \frac{1}{17^{7/2}}$.

3 Versões Rotacionadas dos Reticulados $\mathbb{Z}^2$ e $\mathbb{Z}^3$

Proposição 3.1 ([11]). *A máxima distância produto mínima para um reticulado $\mathbb{Z}^2$ rotacionado é $\frac{1}{\sqrt{5}}$.*

A matriz geradora da versão rotacionada "ótima" do $\mathbb{Z}^2$, conforme Proposição 3.1, é dada por

$$Q = \begin{bmatrix} \cos\left(\frac{1}{2}\arctan(2)\right) & -\sin\left(\frac{1}{2}\arctan(2)\right) \\ \sin\left(\frac{1}{2}\arctan(2)\right) & \cos\left(\frac{1}{2}\arctan(2)\right) \end{bmatrix} = \begin{bmatrix} 0.850651 & -0.525731 \\ 0.525731 & 0.850651 \end{bmatrix}. \tag{4}$$

Proposição 3.2 ([11]). *Seja $Rot(\mathbb{Z}^3, (1,1,1))$ o conjunto de todas as rotações possíveis do reticulado $\mathbb{Z}^3$ em torno da reta cujo vetor diretor é $(1,1,1)$. A máxima distância produto mínima para um reticulado em $Rot(\mathbb{Z}^3, (1,1,1))$ é $\frac{1}{7}$.*

A matriz geradora da versão rotacionada "ótima" do $\mathbb{Z}^3$, conforme Proposição 3.2, é dada por

$$Q = \begin{bmatrix} 0.736976 & -0.327985 & 0.591009 \\ 0.591009 & 0.736976 & -0.327985 \\ -0.327985 & 0.591009 & 0.736976 \end{bmatrix}. \tag{5}$$

Tal versão, é obtida através de uma rotação de ângulo $\frac{1}{3}\arccos\left(\frac{-13}{14}\right)$ em torno da reta cujo vetor diretor é $(1,1,1)$.

4 Torção Generalizada

Definição 4.1 (Torção Generalizada). *Sejam $(m_1, m_2, ..., m_{n-1}) \in \mathbb{R}^{n-1}$, $m_i \neq 0$, $i = 1, 2, ..., n-1$ e $\Lambda \subset \mathbb{R}^n$ um reticulado que possui uma matriz geradora A. Uma $(m_1, m_2, ..., m_{n-1})$-torção generalizada do reticulado Λ é o reticulado $\mathrm{tor}_{(m_1, m_2, ..., m_{n-1})}(\Lambda)$ com matriz geradora*

$$B = \begin{bmatrix} m_1 & & & & \\ & m_2 & & & \\ & & \ddots & & \\ & & & m_{n-1} & \\ & & & & \frac{1}{m_1 . m_2 ... m_{n-1}} \end{bmatrix} A. \tag{6}$$

Segue, da Definição 4.1, que $V(\mathrm{tor}_m(\Lambda)) = V(\Lambda)$, e ainda, se Λ tem diversidade máxima, então temos que $\mathrm{tor}_{(m_1, m_2, ..., m_{n-1})}(\Lambda)$ preserva a distância produto mínima de Λ.

Segue da Proposição 3.1 e da Definição 4.1 que qualquer reticulado da família de reticulados $\mathrm{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, em que $\mathcal{L}(\mathbb{Z}^2)$ é a versão rotacionada "ótima" do $\mathbb{Z}^2$ com matriz geradora dada por (4), possui distância produto mínima $\frac{1}{\sqrt{5}}$.

Consideramos os reticulados $\text{tor}_{m(i)}(\mathcal{L}(\mathbb{Z}^2))$, em que $m = m(i)$ foi tomado na partição $P = \left\{m = m(i) = \frac{i}{10^7}\right\}_{i=1}^{10^8}$ do intervalo $\left[\frac{1}{10^7}, 10\right]$. A partir do Algorítimo 1 proposto na Seção 2.3 de [11], verificamos que não existe i tal que $\mu_{m(i)} < \sqrt{\frac{2}{\sqrt{5}}}$ ou $\mu_{m(i)} > 1$, em que $\mu_{m(i)}$ é a norma mínima do reticulado $\text{tor}_{m(i)}(\mathcal{L}(\mathbb{Z}^2))$.

As simulações que nos levaram ao resultado do parágrafo anterior são motivações para Conjectura 4.1.

Conjectura 4.1. *Se $\mathcal{L}(\mathbb{Z}^2)$ é a versão rotacionada do $\mathbb{Z}^2$ com matriz geradora dada por (4) e μ_m é a norma mínima do reticulado $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$, então $\sqrt{\frac{2}{\sqrt{5}}} \leq \mu_m \leq 1$.*

Observamos que caso a Conjectura 4.1 seja verdadeira, isso implicará que não existe versão torcida $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$ com densidade de empacotamento superior a da versão rotacionada ótima $\mathcal{L}(\mathbb{Z}^2)$ de matriz geradora (4), ou seja, não existe reticulado $\text{tor}_m(\mathcal{L}(\mathbb{Z}^2))$ com densidade de empacotamento superior a 0.785398.

Seja $\mathcal{L}(\mathbb{Z}^n)$ a versão rotacionada "ótima" do $\mathbb{Z}^n$, que para $n = 3, 5$ e 8 as matrizes geradoras são dadas por (5), (2) e (3) respectivamente. Segue da da Definição 4.1, que as famílias $\text{tor}_{(m_1,m_2)}(\mathcal{L}(\mathbb{Z}^3))$, $\text{tor}_{(m_1,m_2,m_3,m_4)}(\mathcal{L}(\mathbb{Z}^5))$ e $\text{tor}_{(m_1,m_2,\ldots,m_7)}(\mathcal{L}(\mathbb{Z}^8))$ definem reticulados que preservam as distâncias produtos mínimas de $\mathcal{L}(\mathbb{Z}^3)$, $\mathcal{L}(\mathbb{Z}^5)$ e $\mathcal{L}(\mathbb{Z}^8)$ respectivamente, ou seja, qualquer reticulado da família $\text{tor}_{(m_1,m_2)}(\mathcal{L}(\mathbb{Z}^3))$ tem distância produto mínima $\frac{1}{7}$, qualquer reticulado da família $\text{tor}_{(m_1,m_2,m_3,m_4)}(\mathcal{L}(\mathbb{Z}^5))$ tem distância produto mínima $\frac{1}{11^2}$ e qualquer reticulado da família $\text{tor}_{(m_1,m_2,\ldots,m_7)}(\mathcal{L}(\mathbb{Z}^8))$ tem distância produto mínima $\frac{1}{17^{7/2}}$.

Consideramos os reticulados $\text{tor}_{(m_1(i_1),m_2(i_2))}(\mathcal{L}(\mathbb{Z}^3))$, em que $(m_1(i_1), m_2(i_2))$ foi tomado no subconjunto

$$P = \left\{m_1(i_1) = \frac{i_1}{20}\right\}_{i_1=1}^{50} \times \left\{m_2(i_2) = \frac{i_2}{20}\right\}_{i_2=1}^{50}$$

do quadrado $\left[\frac{1}{20}, \frac{5}{2}\right]^2$, os reticulados $\text{tor}_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))}(\mathcal{L}(\mathbb{Z}^5))$, em que $(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4))$ foi tomado no subconjunto

$$P = \left\{m_1(i_1) = \frac{i_1}{3}\right\}_{i_1=1}^{7} \times \left\{m_2(i_2) = \frac{i_2}{3}\right\}_{i_2=1}^{7} \times \left\{m_3(i_3) = \frac{i_3}{3}\right\}_{i_3=1}^{7} \times \left\{m_4(i_4) = \frac{i_4}{3}\right\}_{i_4=1}^{7}$$

do hipercubo $\left[\frac{1}{3}, \frac{7}{3}\right]^4$ e os reticulados $\text{tor}_{(m_1(i_1),m_2(i_2),\ldots,m_7(i_7))}(\mathcal{L}(\mathbb{Z}^8))$, em que $(m_1(i_1), m_2(i_2), \ldots, m_7(i_7))$ foi tomado no subconjunto

$$P = \left\{m_1(i_1) = \frac{i_1}{2}\right\}_{i_1=1}^{3} \times \left\{m_2(i_2) = \frac{i_2}{2}\right\}_{i_2=1}^{3} \times \ldots \times \left\{m_7(i_7) = \frac{i_7}{2}\right\}_{i_7=1}^{3}$$

do hipercubo $\left[\frac{1}{2}, \frac{3}{2}\right]^7$. Para tais reticulados, o algoritmo usado para o cálculo da norma mínima foi proposto por U. Fincke e M. Pohst conforme podemos ver em [6].

Em relação aos reticulados $\text{tor}_{(m_1(i_1),m_2(i_2))}(\mathcal{L}(\mathbb{Z}^3))$, verificamos que $\mu_{(m_1(i_1),m_2(i_2))} \leq 1.01992$, para todo $i_1 = 1, 2, .., 50$ e $i_2 = 1, 2, .., 50$. Um ponto $(m_1(i_1), m_2(i_2))$ para o qual encontramos $\mu_{(m_1(i_1),m_2(i_2))} = 1.01992$ foi $(m_1(i_1), m_2(i_2)) = (7/4, 41/20)$. Dessa forma, temos que o reticulado $\text{tor}_{(7/4,41/20)}(\mathcal{L}(\mathbb{Z}^3))$ é mais denso que o $\mathbb{Z}^3$, cuja densidade é 0.5236 e tem a maior densidade dentre todas as versões torcidas consideradas; tal densidade é dada por

$$\Delta(\text{tor}_{(7/4,41/20)}(\mathcal{L}(\mathbb{Z}^3))) = \frac{\mu^3_{(7/4,41/20)}\pi}{6} \simeq \frac{1.01992^3\pi}{6} \simeq 0.555513.$$

Isso nos dá um ganho de aproximadamente 6.1 % na densidade.

Em relação aos reticulados $\text{tor}_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))}(\mathcal{L}(\mathbb{Z}^5))$, verificamos que $\mu_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))} \leq 1.09221$, para todo $i_j = 1, 2, .., 7$, em que $j = 1, 2, 3, 4$. Um ponto $(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4))$ para o qual encontramos $\mu_{(m_1(i_1),m_2(i_2),m_3(i_3),m_4(i_4))} = 1.09221$ foi $(m_1(i_1), m_2(i_2), m_3(i_3), m_4(i_4)) = (5/3, 7/3, 2, 1)$. Temos que o reticulado $\text{tor}_{(5/3,7/3,2,1)}(\mathcal{L}(\mathbb{Z}^5))$ é mais denso que o $\mathbb{Z}^5$ cuja densidade é 0.164493 e tem a maior densidade dentre todas as versões torcidas consideradas, essa densidade por sua vez é dada por

$$\Delta(\text{tor}_{(5/3,7/3,2,1)}(\mathcal{L}(\mathbb{Z}^5))) = \frac{\mu^5_{(5/3,7/3,2,1)}\pi^2}{60} \simeq \frac{1.09221^5\pi^2}{60} \simeq 0.255673.$$

Isso nos dá um ganho de aproximadamente 55.43 % na densidade.

Em relação aos reticulados $\text{tor}_{(m_1(i_1),m_2(i_2),...,m_7(i_7))}(\mathcal{L}(\mathbb{Z}^8))$, verificamos que $\mu_{(m_1(i_1),m_2(i_2),...,m_7(i_7))} \leq 1.1315$, para todo $i_j = 1, 2, 3$, em que $j = 1, 2, ..., 7$. Um ponto $(m_1(i_1), m_2(i_2), ..., m_7(i_7))$ para o qual encontramos $\mu_{(m_1(i_1),m_2(i_2),...,m_7(i_7))} = 1.1315$ foi $(m_1(i_1), m_2(i_2), ..., m_7(i_7)) = (1/2, 1, 3/2, 1, 1/2, 3/2, 1/2)$. Dessa forma, temos que o reticulado $\text{tor}_{(1/2,1,3/2,1,1/2,3/2,1/2)}(\mathcal{L}(\mathbb{Z}^8))$ é mais denso que o $\mathbb{Z}^8$ cuja densidade é 0.0158543 e tem a maior densidade dentre todas as versões torcidas consideradas; tal densidade é dada por

$$\Delta(\text{tor}_{(1/2,1,3/2,1,1/2,3/2,1/2)}(\mathcal{L}(\mathbb{Z}^8))) = \frac{\mu^8_{(1/2,1,3/2,1,1/2,3/2,1/2)}\pi^4}{2^8 4!} \simeq \frac{1.1315^8\pi^4}{2^8 4!} \simeq 0.0425967.$$

Isso nos dá um ganho de aproximadamente 168.67 % na densidade.

Na Tabela 1, registramos as densidades dos reticulados estudados nessa seção bem como as de suas “melhores” versões torcidas encontradas. Nas duas últimas colunas temos os reticulados com maior densidade conhecida em cada dimensão e suas respectivas densidades.

Tabela 1: Densidade de $\mathcal{L}(\mathbb{Z}^n) \subset \mathbb{R}^n$ e densidade da melhor versão torcida encontrada

$\mathcal{L}(\mathbb{Z}^n)$	$\Delta(\mathcal{L}(\mathbb{Z}^n))$	$\Lambda = \text{tor}_{\mathbf{v}}(\mathcal{L}(\mathbb{Z}^n))$	$\Delta(\Lambda)$	M	$\Delta(M)$
$n = 3$	0.5236	$\mathbf{v} = \left(\frac{7}{4}, \frac{41}{20}\right)$	0.5555	FCC	0.7450
$n = 5$	0.1645	$\mathbf{v} = \left(\frac{5}{3}, \frac{7}{3}, 2, 1\right)$	0.2557	D_5	0.4653
$n = 8$	0.0159	$\mathbf{v} = \left(\frac{1}{2}, 1, \frac{3}{2}, 1, \frac{1}{2}, \frac{3}{2}, \frac{1}{2}\right)$	0.0426	E_8	0.2537

5 Considerações Finais

Em dimensões 2 e 3 exibimos nossas versões rotacionadas “ótimas” de reticulados com diversidade máxima e suas distâncias produtos mínimas, tais versões foram contruídas de maneira alternativa às já conhecidas versões algébricas. Em dimensões 3, 5 e 8 construímos versões torcidas de reticulados “ótimos” e exibimos suas normas mínimas e densidades.

Agradecimentos

Os autores agradecem à Universidade Estadual de Campinas, à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), pelo suporte ao grupo de pesquisa através do Projeto Temático 2013/25977-7 “Segurança e Confiabilidade da Informação: Teoria e Prática” e ao Instituto Federal de Educação, Ciência e Tecnologia do Maranhão.

Referências

[1] E. Bayer-Fluckiger. "Lattices and number Fields". Em: **Algebraic Geometry: Hirzebruch 70** 241.BOOK_CHAP (1999). URL: https://cds.cern.ch/record/458428.

[2] E. Bayer-Fluckiger, F. Oggier e E. Viterbo. "New algebraic constructions of rotated Z/sup n/-lattice constellations for the Rayleigh fading channel". Em: **IEEE Transactions on information theory** 50.4 (2004), pp. 702–714. DOI: 10.1109/TIT.2004.825045.

[3] J. Boutros et al. "Good lattice constellations for both Rayleigh fading and Gaussian channels". Em: **IEEE Transactions on Information Theory** 42.2 (1996), pp. 502–518. DOI: 10.1109/18.485720.

[4] J. H. Conway e N. J. A. Sloane. **Sphere packings, lattices and groups**. Vol. 290. Springer Science & Business Media, 2013. ISBN: 978-1-4757-2018-1.

[5] S. I. R. Costa et al. **Lattices Applied to Coding for Reliable and Secure Communications**. Springer, 2017. ISBN: 978-3-319-67881-8.

[6] U. Fincke e M. Pohst. "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis". Em: **Mathematics of computation** 44.170 (1985), pp. 463–471. DOI: 10.1090/S0025-5718-1985-0777278-8.

[7] G. C. Jorge. "Reticulados q-ários e algébricos. 2012. 164f". Tese de doutorado. Tese (Doutorado em Matemática)-Instituto de Matemática, Estatística e Computação Científica, 2012.

[8] G. C Jorge et al. "Algebraic constructions of densest lattices". Em: **Journal of Algebra** 429 (2015), pp. 218–235. DOI: 10.1016/j.jalgebra.2014.12.044.

[9] F. Oggier e E. Viterbo. **Algebraic number theory and code design for Rayleigh fading channels**. Now publishers inc, 2004. DOI: 10.1561/0100000003.

[10] J. E. Strapasson et al. "Algebraic constructions of rotated unimodular lattices and direct sum of Barnes–Wall lattices". Em: **Journal of Algebra and Its Applications** (2020), p. 2150029. DOI: 10.1142/S0219498821500298.

[11] F. P. Tavares. "Sobre Reticulados Rotacionados para Codificação em Sistemas de Transmissão. 2022. 133f". Tese de doutorado. Tese (Doutorado em Matemática)-Instituto de Matemática, Estatística e Computação Científica, 2022.

