



Construção do reticulado laminado E_6 via ordem maximal no anel dos inteiros algébricos

Agnaldo José Ferrari

*Unesp - Universidade Estadual Paulista; Faculdade de Ciências; Departamento de Matemática
agnaldo.ferrari@unesp.br*

João Eloir Strapasson

*Unicamp - Universidade Estadual de Campinas; Faculdade de Ciências Aplicadas
joao.strapasson@fca.unicamp.br*

Resumo: Neste trabalho apresentamos um método para construir reticulados baseado nos trabalhos de Taussky e Krüskemper, que computa a matriz geradora de um reticulado integral, dada a sua matriz Gram. Isso produz um reticulado algébrico, no sentido de que o reticulado é construído através dos mergulhos em um corpo de números totalmente real, que possui diversidade máxima. Pelo método, existe o controle do discriminante do corpo e da ordem no anel dos inteiros algébricos, que impactam na distância produto mínima dos reticulados construídos, sendo este um parâmetro importante quando associamos um reticulado a uma constelação de sinais para transmissão via o canal com desvanecimento do tipo Rayleigh.

Palavras-chave: Matemática Discreta. Reticulado. Discriminante. Distância produto

Introdução

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ é um conjunto discreto gerado por combinações lineares inteiras de n vetores linearmente independentes $v_1, v_2, \dots, v_n \in \mathbb{R}^n$. Um reticulado Λ tem diversidade $m \leq n$ se m é o número máximo tal que para todos $y = (y_1, \dots, y_n) \in \Lambda$, $y \neq 0$, existem no mínimo m coordenadas não nulas. Dado um reticulado de diversidade máxima $\Lambda \subseteq \mathbb{R}^n$ ($m = n$), a distância produto mínima é definida como $d_{\min}(\Lambda) = \min\{\prod_{i=1}^n |y_i|\}$, for all $y = (y_1, \dots, y_n) \in \Lambda$, $y \neq 0$ (FLUCKIGER, 2004).

Constelações de sinais tendo a estrutura de reticulados vêm sendo estudadas como uma maneira significativa para transmissão de sinais sobre os canais Gaussiano e com desvanecimento do tipo Rayleigh (BOUTROS, 1996). Usualmente o problema de encontrar boas constelações de sinais para o canal Gaussiano está associado à busca por reticulados com alta densidade de empacotamento (CONWAY, 1999). Por outro lado, para o canal com desvanecimento do tipo Rayleigh a eficiência, medida pela baixa probabilidade de erro na transmissão, está fortemente relacionada à diversidade e à distância produto mínima (FLUCKIGER, 2004). Em geral, a distância produto mínima de reticulados é usualmente difícil de estimar (MICCIANCIO, 2002). Este parâmetro pode ser obtido, em certos casos, de reticulados associados a corpos de números através de propriedades algébricas.

A abordagem neste trabalho, seguindo Conner (1984) e Krüskemper (1996), é o uso da Teoria Algébrica dos Números para construir um reticulado que possui boa performance em ambos os canais. Mais especificamente, faremos uso de um algoritmo que computa a matriz geradora de um reticulado integral dada sua matriz de Gram, produzindo um reticulado algébrico no sentido de que o reticulado é construído via mergulhos em um corpo de números. Por este método, Oggier et al (2003) construíram reticulados $\mathbb{Z}^n$, para n de 2 a 7, sobre corpos totalmente reais com discriminante mínimo, resultando em constelações de sinais com diversidade máxima e a melhor distância produto mínima possível. Também através deste método, Ferrari (2018) apresenta uma construção do reticulado hexagonal via corpos totalmente reais.



Neste trabalho, usando essas ideias, construímos o reticulado laminado E_6 via uma ordem maximal no anel dos inteiros algébricos de um corpo totalmente real. Para a construção implementamos algoritmos computacionais que buscam por matrizes geradoras do reticulado, sempre tendo o controle do discriminante do corpo, que deve ser, de preferência o de menor valor possível, e pelas ordens nos anéis dos inteiros algébricos que devem ser ordens maximais.

Fundamentação Teórica

Seja $\{v_1, \dots, v_n\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$ e $\Lambda = \{\sum_{i=1}^n a_i v_i; a_i \in \mathbb{Z}\}$ um reticulado. O conjunto $\{v_1, \dots, v_n\}$ é chamado uma *base* para Λ . Uma matriz M cujas linhas são estes vetores é dita uma *matriz geradora* para Λ , enquanto a *matriz de Gram* associada é $G = MM^T = (\langle v_i, v_j \rangle)_{i,j=1}^n$. O *determinante* de Λ é $\det(\Lambda) = \det(G)$. Se T é uma matriz inteira tal que $\det(T) = \pm 1$, então TM é outra base para Λ . O *determinante* de Λ é invariante sob mudança de base (CONWAY, 1999). O reticulado Λ é chamado *integral* quando o produto interno entre os vetores do reticulado é um número inteiro.

Seja $\mathbb{K}$ um corpo de números de grau n , isto é, $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta \in \mathbb{C}$ uma raiz de um polinômio monico irreduzível $p(x) \in \mathbb{Z}[x]$. As n raízes distintas de $p(x)$, a saber, $\theta_1, \theta_2, \dots, \theta_n$, são os conjugados de θ . Os *mergulhos* em $\mathbb{K}$ são homomorfismos $\sigma_i(\theta) = \theta_i$, para todo $i = 1, 2, \dots, n$. Assim, os mergulhos σ_i , para $i = 1, \dots, n$, são os n distintos $\mathbb{Q}$ -homomorfismos de $\mathbb{K}$ em $\mathbb{C}$ tal que $\sigma_1, \dots, \sigma_{r_1}$ são reais e $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \dots, \sigma_{r_1+2r_2}$ são imaginários, onde $\sigma_{r_1+r_2+i}$ é o complexo conjugado de σ_{r_1+i} , para todo $i = 1, \dots, r_2$. Neste caso, $n = r_1 + 2r_2$. Se todos os mergulhos em $\mathbb{K}$ forem reais, neste caso $r_1 = n$ e $r_2 = 0$, (resp., complexos, neste caso, $r_1 = 0$ e $2r_2 = n$), $\mathbb{K}$ é dito totalmente real (resp. totalmente complexo).

O conjunto $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \text{existe um polinômio mônico } f(x) \in \mathbb{Z}[x] \text{ tal que } f(\alpha) = 0\}$ é chamado de *anel dos inteiros algébricos* de $\mathbb{K}$. Pode ser mostrado que $\mathcal{O}_{\mathbb{K}}$, como um $\mathbb{Z}$ -módulo, tem uma base $\{\omega_1, \dots, \omega_n\}$ sobre $\mathbb{Z}$, onde n é o grau de $\mathbb{K}$. Além disso, se $\{\omega_1, \dots, \omega_n\}$ é $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}}$, o inteiro $d_{\mathbb{K}} = (\det[\sigma_j(\omega_i)]_{i,j=1}^n)^2$ é chamado de *discriminante* de $\mathbb{K}$ e é invariante sob mudança de base. A *norma* e o *traço* de um elemento $\alpha \in \mathbb{K}$ é definido como o número racional $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ e $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$, respectivamente.

Sejam $\mathbb{K}$ um corpo de números totalmente real de grau n , e denote por σ_i , $i = 1, \dots, n$ seus n mergulhos em $\mathbb{R}^n$ e $\alpha \in \mathbb{K}$ satisfazendo $\sigma_i(\alpha) > 0$, $\forall i$ e $\mathcal{A}$ o ideal fracionário de $\mathbb{K}$ com uma $\mathbb{Z}$ -base $\{v_1, \dots, v_n\}$, isto é, $\mathcal{A} = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$. Um *reticulado ideal* é um reticulado integral cuja matriz geradora é $M = ND$, onde $N = \sigma_j(v_i)_{i,j=1}^n$ e $D = \text{diag}(\sqrt{\sigma_k(\alpha)})$ que satisfaz $MM^T = (Tr_{\mathbb{K}/\mathbb{Q}}(\alpha v_i v_j))_{i,j=1}^n$ (FLUCKIGER, 2005). Pode ser mostrado que um reticulado construído sobre corpos totalmente reais possui diversidade máxima.

Uma ordem $\mathfrak{D}$ em $\mathbb{K}$ é um subanel de $\mathbb{K}$ que como um $\mathbb{Z}$ -módulo é finitamente gerado e de posto máximo $n = [\mathbb{K} : \mathbb{Q}]$. Podemos mostrar que $\mathfrak{D} \subseteq \mathcal{O}_{\mathbb{K}}$ para qualquer ordem de $\mathbb{K}$, tal que $\mathcal{O}_{\mathbb{K}}$ é chamada de *ordem maximal* de $\mathbb{K}$.

Seja $\mathfrak{D}$ uma ordem em $\mathbb{K}$ e $\mathcal{A}$ um ideal de $\mathfrak{D}$. A *distância produto mínima* de um reticulado ideal $\Lambda = (\mathcal{A}, b_{\alpha})$, onde $b_{\alpha} = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha v_i v_j)$, de determinante $\det(B)$ é

$$d_{p,\min}(\Lambda) = \sqrt{\frac{\det(B)}{d_{\mathbb{K}} [\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]}} \quad (1)$$

onde $\min(\mathcal{A}) = \min_{0 \neq x \in \mathcal{A}} \frac{|N(x)|}{N(\mathcal{A})}$ e $[\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]$ é o índice de $\mathfrak{D}$ em $\mathcal{O}_{\mathbb{K}}$ (OGGIER, 2005).

A *distância produto mínima relativa* de Λ , denotada por $d_{p,\text{rel}}(\Lambda)$, é a distância produto mínima de uma versão escalonada de Λ com vetor de norma mínima unitário, isto é, se a norma mínima de Λ é μ



então

$$d_{p,rel}(\Lambda) = \frac{1}{(\sqrt{\mu})^n} \sqrt{\frac{\det(B)}{d_{\mathbb{K}}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathcal{D}]} \quad (2)$$

A fim de comparar distância produto mínima relativa em diferentes dimensões, trabalhamos com a distância produto mínima relativa normalizada $\sqrt[n]{d_{p,rel}(\Lambda)}$.

Seja $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu anel dos inteiros algébricos. Se $I_{\mathbb{K}}$ denota o grupo dos ideais fracionários de $\mathbb{K}$ e $P_{\mathbb{K}}$ denota o subgrupo de $\mathbb{K}$ formado por ideais principais, então o *ideal class group*, denotado por $Cl(\mathbb{K})$, é $Cl(\mathbb{K}) = I_{\mathbb{K}}/P_{\mathbb{K}}$. O *class number* de $\mathbb{K}$, denotado por $h(\mathbb{K})$, é a cardinalidade de $Cl(\mathbb{K})$. Em particular, se $\mathcal{O}_{\mathbb{K}}$ é um ideal principal, então $h(\mathbb{K}) = 1$. O *class number* de um corpo $\mathbb{K}$ pode ser entendido como a medida de quão principal um anel dos inteiros é, ou seja, qual a proporção dos ideais principais entre todos os ideais.

Se $\mathcal{A}$ é um ideal principal, então $\min\{\mathcal{A}\} = 1$ e consequentemente, a distância produto mínima de Λ é

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_{\alpha})}{d_{\mathbb{K}}}} \frac{1}{[\mathcal{O}_{\mathbb{K}} : \mathcal{D}]} \quad (3)$$

Neste trabalho, para calcular $[\mathcal{O}_{\mathbb{K}} : \mathcal{D}]$ e $h(\mathbb{K})$, usamos os softwares Mathematica e Pari (BATUT), respectivamente.

Método de Kruskemper

Nesta seção apresentamos alguns resultados que provam que qualquer reticulado integral pode ser construído com um reticulado ideal de alguma álgebra $\mathbb{Z}[X]/(f(X))$, onde $f(X) \in \mathbb{Z}[X]$ é mônico e irredutível.

Denotamos por M o $\mathbb{Z}$ -módulo livre finitamente gerado de posto n e por $b : M \times M \rightarrow \mathbb{Z}$ uma forma bilinear simétrica. Seja $f(X) \in \mathbb{Z}[X]$ um polinômio mônico irredutível de grau n e θ uma raiz de f . Então $\mathbb{Z}[X]/(f(X)) = \mathbb{Z}[\theta]$ com base $\{1, \theta, \dots, \theta^{n-1}\}$. Se $\mathcal{A}$ é um ideal em $\mathbb{Z}[\theta]$, definimos $\mathcal{A}^{\#} = \{c \in \mathbb{Q}(\theta) \mid Tr(c\mathcal{A}) \subseteq \mathbb{Z}\}$. O número algébrico θ é a raiz do polinômio característico da matriz A e as componentes do autovetor correspondente v_{θ} pode ser escolhido para formar a base de um ideal no anel formado pelos polinômios em θ com coeficientes inteiros (TAUSSKY, 1949). Seja A a matriz que corresponde ao *ideal class* determinado pelo ideal $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ e seja A^t que corresponde ao ideal $\mathcal{B} = (\beta_1, \dots, \beta_n)$, então $\mathcal{B}$ pertence à classe inversa de $\mathcal{A}$ (TAUSSKY, 1957). Sejam $B \in M_n(\mathbb{Z})$ uma matriz simétrica não singular e $A \in M_n(\mathbb{Z})$ tal que seu polinômio característico χ_A é irredutível e $B^{-1}AB = A^t$, então B é a matriz de um reticulado ideal. Seja (M, b) um reticulado integral, então existe um inteiro algébrico θ , um ideal $\mathcal{A}$ de $\mathbb{Z}[\theta]$ e $\alpha \in (\mathcal{A}^2)^{\#} \subseteq \mathbb{Q}(\theta)$ tal que b é isomorfo a $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy)$, onde $x, y \in \mathcal{A}$ e $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy) \in \mathbb{Z}$. Além disso, podemos assumir que θ é totalmente real (OGGIER, 2005).

Algoritmo de construção

Apresentamos um algoritmo que toma como entrada a matriz de Gram B de um reticulado integral e tem como saída a matriz geradora do reticulado. Mais precisamente, o algoritmo computa um conjunto de elementos $\{v_1, \dots, v_n\}$ e um elemento α tal que $\mathcal{A} = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ e o reticulado ideal $(\mathcal{A}, b_{\alpha})$, onde $b_{\alpha} : \mathcal{A} \times \mathcal{A} \rightarrow \mathbb{Z}$ definido por $b_{\alpha}(x, y) = Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy)$, tem matriz de Gram B . Os passos do algoritmo são explicados em detalhes em Oggier (2005).

Passo 1: Computação da matriz A



Uma matriz $A \in M_n(\mathbb{Z})$ satisfazendo $B^{-1}AB = A^T$ cujo polinômio característico é irreduzível pode ser obtida randomicamente ou possivelmente construída de modo a obter um corpo de números específico com polinômio minimal χ_A .

Passo 2: Computação de uma $\mathbb{Z}$ -base do $\mathcal{A}$

Segundo Taussky (1949), existe um autovetor v_θ de A associado a θ , uma raiz de χ_A , tal que $\mathcal{A} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$. Pode ser mostrado que $v_j := (-1)^{i+j} \Delta_{ij}(A - \theta I_n)$, onde Δ_{ij} é o j -ésimo menor de uma linha fixada, digamos a i -ésima linha, de $(A - \theta I_n)$. Pode ser mostrado que este vetor é de fato um autovetor de A .

Passo 3: Computação de α

Segundo Oggier (2005), existe um autovetor $v'_\theta = (v'_1, \dots, v'_n)^T$ de A^T associado a θ , com $v'_i \in \mathbb{Q}(\theta)$ e tal que $\text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(v_i v'_j) = \delta_{ij}, \forall i, j$. Pode ser mostrado que $v'_j = \sum_{i=1}^n m_{ij} \theta^{i-1}$, onde $(m_{ij})_{i,j=1}^n = G^{-1}(V^T)^{-1}$ com $G = (\text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1} \theta^{j-1}))_{i,j=1}^n$ e $V = (v_1, \dots, v_n)$ é a matriz das coordenadas de $v_1, \dots, v_n$ na base $\{1, \theta, \dots, \theta^{n-1}\}$. O elemento α é obtido de $\sum_{j=1}^n b_{ij} v'_j = \alpha v_i, \forall i$. Se B é diagonal é suficiente computar um dos v_i 's.

Passo 4: Computação da matriz geradora do reticulado

Temos que a matriz geradora do reticulado é $M = ND$, onde $N = \sigma_j(v_i)_{i,j=1}^n$ e $D = \text{diag}(\sqrt{\alpha_k})$, com $\alpha_k = \sigma_k(\alpha)$.

Passo 5: Computação do discriminante do corpo $\mathbb{K}$

Tomando $\alpha = 1$, pelo passo anterior temos que $D = I_n$, assim

$$\begin{aligned} d_{\mathbb{K}} &= (\det[\sigma_i(\theta^{j-1})]_{i,j=1}^n)^2 = \det(M)^2 = \det(M) \det(M) = \det(M) \det(M^T) = \\ &= \det(MM^T) = \det(\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\theta^{i-1} \theta^{j-1}))_{i,j=1}^n = \det(G), \end{aligned}$$

uma vez que $G = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\theta^{i-1} \theta^{j-1})_{i,j=1}^n$.

Resultados

Para a realização geométrica do reticulado laminado E_6 via método de Krüskemper, implementamos o algoritmo de construção descrito acima no software Mathematica. A fim de obter uma versão rotacionada deste reticulado com a maior distância produto mínima possível (Equação 1), devemos:

- utilizar uma ordem $\mathfrak{D} = \mathbb{Z}[\theta]$ que seja maximal, isto é, $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$.
- trabalhar em corpos de números cujo anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ seja um domínio de ideais principais, ou seja, $h(\mathbb{K}) = 1$ e consequentemente $\min\{\mathcal{A}\} = 1$;
- trabalhar em corpos de números com menor discriminante possível.

Construção

Uma matriz geradora para o reticulado E_6 é dada por $M = \{(0, -2, 2, 0, 0, 0, 0, 0), (0, 0, -2, 2, 0, 0, 0, 0), (0, 0, 0, -2, 2, 0, 0, 0), (0, 0, 0, 0, -2, 2, 0, 0), (1, 1, 1, 1, -1, -1, -1, -1)\}$, onde a matriz de Gram associada é $B = \{(8, -4, 0, 0, 0, 0), (-4, 8, -4, 0, 0, 0), (0, -4, 8, -4, 0, 0), (0, 0, -4, 8, -4, 0), (0, 0, 0, -4, 8, 0), (0, 0, -4, 0, 0, 8)\}$. Considere o corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$ tal que θ é raiz do polinômio $x^6 + 2x^5 - 9x^4 - 24x^3 - 8x^2 + 8x - 1$. A matriz $A = \{(-1, 0, -1, 1, 1, 0),$



$(1, 0, 1, 0, 0, 0), (-1, 1, 1, -1, -1, -1), (1, 0, 0, 0, 1, 2), (0, -1, -2, -1, -2, -1), (0, -1, -1, 2, 1, 0)$ satisfaz $\chi_A(X) = x^6 + 2x^5 - 9x^4 - 24x^3 - 8x^2 + 8x - 1$, onde χ_A é irredutível sobre $\mathbb{Q}$ e $B^{-1}AB = A^T$. Computamos as matrizes V e G da seguinte forma: $v_\theta = (v_1, v_2, \dots, v_6)^T$, onde $v_j = (-1)^{i+j} \Delta_{ij}(A - \theta I_6)$, tomando $i = 1$, temos $v_1 = -2 + \theta + 13\theta^2 + 8\theta^3 - \theta^4 - \theta^5$, $v_2 = -4 + 10\theta + 10\theta^2 - \theta^4$, $v_3 = 2 - 5\theta - 3\theta^2 + 2\theta^3 + \theta^4$, $v_4 = -1 - 4\theta + 4\theta^2 - \theta^3 - \theta^4$, $v_5 = -2\theta - \theta^2$ e $v_6 = 1 - 4\theta^2 - 2\theta^3$. Seja $V = (v_{ij})_{i,j=1}^6$ e $(1, \theta, \dots, \theta^5)V = (v_1, v_2, \dots, v_6)$, então $V = \{(-2, -4, 2, -1, 0, 1), (1, 10, -5, 4, -2, 0), (13, 10, -3, 4, -1, -4), (8, 0, 2, -1, 0, -2), (-1, -1, 1, -1, 0, 0), (-1, 0, 0, 0, 0, 0)\}$ e consequentemente $(V^T)^{-1} = \{(0, 2, 4, 2, 4, 3), (0, -3, -5, -2, -7, -4), (0, 6, 10, 4, 13, 8), (0, -11, -18, -7, -24, -15), (0, 21, 34, 12, 44, 28), (-1, -38, -61, -22, -82, -54)\}$, assim $G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^6 = \{(6, -2, 22, 10, 162, 238), (-2, 22, 10, 162, 238, 1420), (22, 10, 162, 238, 1420, 3092), (10, 162, 238, 1420, 3092, 13546), (162, 238, 1420, 3092, 13546, 35434), (238, 1420, 3092, 13546, 35434, 134872)\}$, uma vez que

$Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^k) = \sum_{j=1}^6 \sigma_j^k(\theta)$ e como θ é uma raiz de χ_A , o conjunto das raízes de χ_A é dado por $\{-2.4585, -1.8667, -1.3712, 0.1687, 0.2908, 3.2368\}$, isto significa que os homomorfismos reais de θ são $\sigma_1(\theta) = -2.4585$, $\sigma_2(\theta) = -1.8667$, $\sigma_3(\theta) = -1.3712$, $\sigma_4(\theta) = 0.1687$, $\sigma_5(\theta) = 0.2908$ e $\sigma_6(\theta) = -2.4585$. O discriminante do corpo $\mathbb{K}$ é dado por $d_{\mathbb{K}} = \det(G) = 14631616$, e consequentemente $G^{-1} = \frac{1}{457238} \{b_1, b_2, b_3, b_4, b_5, b_6\}$, onde

$$\begin{aligned} b_1 &= (2127173, -5545424, -10433050, -3366545, 898698, 395827), \\ b_2 &= (-5545424, 16912958, 29045703, 8686501, -2539411, -1039443), \\ b_3 &= (-10433050, 29045703, 58312277, 20437045, -4940707, -2378808), \\ b_4 &= (-3366545, 8686501, 20437045, 8159663, -1676156, -933202), \\ b_5 &= (898698, -2539411, -4940707, -1676156, 421990, 195898), \\ b_6 &= (395827, -1039443, -2378808, -933202, 195898, 107044). \end{aligned}$$

Seja $v'_\theta = (v'_1, v'_2, \dots, v'_6)^T$, onde $v'_k = \sum_{i=1}^6 m_{ik} \theta^{i-1}$, para $k = 1, 2, \dots, 6$ e $(m_{ij})_{i,j=1}^6 = G^{-1}(V^T)^{-1} = \frac{1}{457238} \{m_1, m_2, m_3, m_4, m_5, m_6\}$, com

$$\begin{aligned} m_1 &= (-395827, -844455, -1086593, -745009, -421012, -614124), \\ m_2 &= (1039443, 3064188, 4419575, 2855355, 2045955, 2806419), \\ m_3 &= (2378808, 3702815, 5418495, 4277579, 189548, 2576415), \\ m_4 &= (933202, 335784, 533849, 941019, -1650314, -283684), \\ m_5 &= (-195898, -373231, -546533, -399394, -126854, -292350), \\ m_6 &= (-107044, -51457, -79073, -116470, 173657, 17587). \end{aligned}$$

Portanto, $v'_\theta = (v'_1, v'_2, \dots, v'_6)^T$ onde,

$$\begin{aligned} v'_1 &= -\frac{395827}{457238} + \frac{1039443}{457238}\theta + \frac{1189404}{228619}\theta^2 + \frac{466601}{228619}\theta^3 - \frac{97949}{228619}\theta^4 - \frac{53522}{228619}\theta^5, \\ v'_2 &= -\frac{844455}{457238} + \frac{1532094}{228619}\theta + \frac{3702815}{457238}\theta^2 + \frac{167892}{228619}\theta^3 - \frac{373231}{457238}\theta^4 - \frac{51457}{457238}\theta^5, \\ v'_3 &= -\frac{1086593}{457238} + \frac{4419575}{457238}\theta + \frac{5418495}{457238}\theta^2 + \frac{533849}{457238}\theta^3 - \frac{546533}{457238}\theta^4 - \frac{79073}{457238}\theta^5, \\ v'_4 &= -\frac{745009}{457238} + \frac{2855355}{457238}\theta + \frac{4277579}{457238}\theta^2 + \frac{941019}{457238}\theta^3 - \frac{199697}{228619}\theta^4 - \frac{58235}{228619}\theta^5, \\ v'_5 &= -\frac{210506}{228619} + \frac{2045955}{457238}\theta + \frac{94774}{228619}\theta^2 - \frac{825157}{228619}\theta^3 - \frac{63427}{228619}\theta^4 + \frac{173657}{457238}\theta^5, \end{aligned}$$



$$v'_6 = -\frac{307062}{228619} + \frac{2806419}{457238}\theta + \frac{2576415}{457238}\theta^2 - \frac{141842}{228619}\theta^3 - \frac{146175}{228619}\theta^4 + \frac{17587}{457238}\theta^5.$$

O elemento α é obtido da equação $\alpha v_\theta = Bv'_\theta$, assim computamos

$$\alpha = -\frac{2138446}{228619} + \frac{17615674}{228619}\theta - \frac{203186385}{457238}\theta^2 - \frac{31131766}{228619}\theta^3 + \frac{194030}{228619}\theta^4 + \frac{3356022}{228619}\theta^5.$$

Portanto, a matriz geradora do reticulado é $M = ND$, onde $N = \sigma_j(v_i)_{i,j=1}^n$ e $D = \text{diag}(\sqrt{\alpha_k})$, com $\alpha_k = \sigma_k(\alpha)$, assim $M = \{(1.616, -0.809, 1.586, -0.973, -0.629, -0.933), (-0.886, 0.365, -2.205, -1.387, -0.377, 0.387), (0.563, 0.127, 1.437, 0.739, 0.519, 2.186), (-1.579, -1.664, 0.071, -0.148, 0.700, -1.488), (-0.213, 2.494, 0.777, -0.250, -0.993, -0.280), (1.240, 0.711, -1.230, 0.599, 0.913, -1.801)\}$ de tal forma que a matriz de Gram $G = MM^t$ coincide com a matriz B , ou seja, o reticulado construído é uma versão rotacionada do reticulado E_6 . Agora, temos que $\det(B) = 12288$, $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$ e $h(\mathbb{K}) = 1$, logo $\min\{\mathcal{A}\} = 1$. como a norma mínima de E_6 is $\mu = 8$, segue que o reticulado construído sobre $\mathcal{O}_{\mathbb{K}}$ possui distância produto mínima relativa

$$\sqrt[6]{d_{p,rel}(E_6)} = \left(\frac{1}{(\sqrt{\mu})^6} \sqrt{\frac{\det(B)}{d_{\mathbb{K}}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]} \right)^{1/6} = \left(\frac{1}{(\sqrt{8})^6} \sqrt{\frac{12288}{14631616}} \right)^{1/6} = 0.19594$$

Na Tabela 1 apresentamos uma comparação entre as distâncias produtos mínima ($\sqrt[6]{d_{p,rel}(\Lambda)}$) e densidades de empacotamento ($\delta(\Lambda)$) relacionadas aos reticulados $\mathbb{Z}^6$, D_6 e E_6 .

Λ	$\sqrt[6]{d_{p,rel}(\Lambda)}$	$\delta(\Lambda)$
$\mathbb{Z}^6$	0.34958	0.01563
D_6	0.24285	0.06250
E_6	0.19594	0.07217

Tabela 1: Comparações entre distância produto e densidade na dimensão 6.

Conclusões

Neste trabalho construímos o reticulado E_6 , de diversidade máxima, uma vez que é construído sobre um corpo totalmente real. Nota-se, pela Tabela 1, que apesar da distância produto mínima obtida, na nossa construção, para o reticulado E_6 ser menor do que a dos reticulados $\mathbb{Z}^6$ (OGGIER, 2003) e D_6 (JORGE, 2012), a densidade de empacotamento é maior, oferecendo assim um bom “trade-off” no que se refere à utilização de um mesmo reticulado representando uma constelação de sinais eficiente para ambos os canais. Lembramos que a distância produto mínima do $\mathbb{Z}^6$ (0.34958) e a densidade de empacotamento do E_6 (0.07217) são as melhores possíveis na dimensão 6.

Como uma perspectiva futura, pretendemos realizar melhorias no algoritmo tornando-o mais eficiente, uma vez que acreditamos na existência de corpos de números com valor menor para o discriminante que realizem o E_6 , sendo possível assim obter outras versões do reticulado construído com maior valor para a distância produto mínima. Encontrar um corpo de números com menor valor para o discriminante não é garantia de obtenção de maior distância produto, uma vez que para o referido corpo talvez tenhamos $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] > 1$ e/ou $\min\{\mathcal{A}\} < 1$, afetando negativamente na obtenção de uma distância produto mínima maior. Portanto, no algoritmo temos que controlar estas três variáveis: discriminante, ordem e class number.



Agradecimentos

Este trabalho é apoiado pela Fapesp - Projeto Temático 2013/25977-7 e pelo CNPq - Projeto Universal 429346/2018-2.

Referências

BATUT, C.; BELABAS, K.; BERNARDI, D.; COHEN H.; OLIVIER, M. PARI/GP-a software package for computer-aided number theory. Disponível em: math.mit.edu/~brubaker/PARI/PARItutorial.pdf. Acesso em 2019.

BOUTROS, J.; VITERBO E.; RASTELLO, C.; BELFIORE, J. C. Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels. **IEEE Transactions on Information Theory**, v. 42, n. 2, p. 502-518, 1996.

CONNER, E. P.; PERLIS, R. **A survey of trace forms of algebraic number fields**. Louisiana: Word Scientific Publishing Co Pte Ltd, 1984 .

CONWAY, J. H.; SLOANE, N. J. A. **Sphere Packings, Lattices and Groups**. New York: Springer-Verlag, 1999.

FERRARI, A. J. Construção do reticulado hexagonal via o método de Kruskemper. In: XXXVIII Congresso Nacional de Matemática Aplicada e Computacional, 2018, Campinas. **Anais do XXXVIII Congresso Nacional de Matemática Aplicada e Computacional**.

FLUCKIGER, E-BAYER.; OGGIER, F.; VITERBO, E. New Algebraic Constructions of Rotated $\mathbb{Z}^n$ -Lattice Constellations for the Rayleigh Fading Channel. **IEEE Transactions on Information Theory**. v. 50, n. 4, p. 702-714, 2004.

FLUCKIGER, E. BAYER.; NEBE, G. On the euclidean minimum of some real number fields. **Journal de theorie des nombres de Bordeaux**. v.17, n.2, p. 437-454, 2005.

JORGE, G. C.; FERRARI, A. J.; COSTA, S. I. R. Rotated D_n -lattices. **Journal of Number Theory**. v.132, n.11, p. 2397-2406, 2012.

KRÜSKEMPER, M. Algebraic construction of bilinear forms over $\mathbb{Z}$. **Pub. Math. de Besancon, Théorie des nombres**. 1996/97 - 1997/98.

MICCIANCIO, D.; GOLDWASSER, S. Complexity of Lattice Problems: A Cryptographic Perspective. **Kluwer Internat. Ser. Engrg. Comput. Sci.** v. 671, Kluwer Academic Publishers, 2002.

OGGIER, F. **Algebraic Methods for Channel Coding**. Ph.D. thesis, SB, Lausanne, 10.5075/epfl-thesis-3182, 2005.

OGGIER, F.; FLUCKIGER, E-BAYER. Best rotated cubic lattice constellations for the Rayleigh fading channel. **ISIT 2003 - International Symposium of Information Theory**. Yokohama, Japan, 2003.

TAUSSY, O. On a theorem of Latimer and Macduffee. **Canad. J. Math.**, v.1, p. 300-302, 1949.

TAUSSY, O. On matrix classes corresponding to an ideal and its inverse. **Illinois Math, J.** v.1, p. 108-113, 1957.