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

Versões rotacionadas dos reticulados K_{12} e Λ_{24} com diversidade máxima

Grasiele C. Jorge
Instituto de Ciência e Tecnologia, UNIFESP
12231-280, São José dos Campos, SP
E-mail: grasiele.jorge@unifesp.br

Antonio A. Andrade
Departamento de Matemática, IBILCE, UNESP
15.054-000, São José do Rio Preto, SP
E-mail: andrade@ibilce.unesp.br

Sueli I. R. Costa*
Departamento de Matemática, UNICAMP
13083-859, Campinas, SP
E-mail: sueli@ime.unicamp.br

João E. Strapasson†
Faculdade de Ciências Aplicadas, UNICAMP
13484-350, Limeira, SP
E-mail: joao.strapasson@fca.unicamp.br

Resumo: *Reticulados com boa densidade, diversidade máxima e distância produto mínima grande são utilizados em codificações eficientes para transmissão de sinais sobre os canais gaussiano e com desvanecimento do tipo Rayleigh. Neste trabalho construímos versões rotacionadas com diversidade máxima dos reticulados mais densos conhecidos nas dimensões* 12 *e* 24*. Tais construções foram feitas com o auxílio de subcorpos de corpos ciclotômicos e de algoritmos computacionais utilizados no software Mathematica.*

Palavras-chave: *Reticulados algébricos, Densidade de empacotamento, Diversidade, Distância produto mínima, Códigos corretores de erros*

1 Introdução

Um *reticulado* Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$. Equivalentemente, $\Lambda \subseteq \mathbb{R}^n$ é um reticulado se, e somente se, existem vetores linearmente independentes $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$ tal que $\Lambda = \{\sum_{i=1}^m a_i \boldsymbol{v}_i;\ a_i \in \mathbb{Z}\}$. O conjunto $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ é dito uma *base* para Λ. Uma matriz M cujas linhas são estes vetores é dita uma *matriz geradora* para Λ enquanto que a matriz associada $G = MM^t = (\langle v_i, v_j \rangle)_{i,j=1}^m$ é dita uma *matriz de Gram*. O *determinante* de Λ é $\det \Lambda = \det G$ e é um invariante sobre mudança de base. Um reticulado Λ é dito *integral* se $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}$ para todo $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$ e um reticulado integral é dito *par* se $\langle \boldsymbol{x}, \boldsymbol{x} \rangle$ é par para todo $\boldsymbol{x} \in \Lambda$. Um reticulado *unimodular* é um reticulado integral com $\det(\Lambda) = 1$ [7]. No que se segue $m = n$.

A *densidade de empacotamento* de um reticulado $\Lambda \subseteq \mathbb{R}^n$, $\Delta(\Lambda)$, é a proporção do espaço $\mathbb{R}^n$ coberto pela união de esferas congruentes disjuntas de raio máximo, centradas nos pontos de Λ. 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 euclidiana mínima* do reticulado e $vol(B(1))$ é o volume euclidiano da esfera unitária n-dimensional [7].

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ tem *diversidade* $m \leq n$ se m é o número máximo tal que para todo $\boldsymbol{y} = (y_1, \cdots, y_n) \in \Lambda$, $\boldsymbol{y} \neq \boldsymbol{0}$, existem no mínimo m coordenadas não nulas em $\boldsymbol{y}$. Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$ com diversidade máxima ($m = n$), a *distância produto mínima* de Λ é definida como $d_{min}(\Lambda) = \min\{\prod_{i=1}^n |y_i| \text{ para todo } \boldsymbol{y} = (y_1, \cdots, y_n) \in \Lambda, \boldsymbol{y} \neq \boldsymbol{0}\}$ [3]. Para estabelecer uma comparação entre reticulados de normas mínimas diferentes, a *distância produto mínima relativa* é obtida multiplicando a distância produto mínima do reticulado por $\frac{1}{\lambda^n}$ onde λ é o valor da norma mínima euclidiana do reticulado.

*CNPQ proc: 309561/2009-4
†FAPESP proc: 2011/01096-6

Constelações de sinais tendo estrutura de reticulado são utilizadas na codificação para transmissão de sinais em canais gaussiano e com desvanecimento do tipo Rayleigh. A eficiência na transmissão está associada a propriedades específicas dos reticulados. Para utilização em canais gaussianos, bons reticulados são aqueles que apresentam alta densidade de empacotamento [7] e para utilização em canais com desvanecimento do tipo Rayleigh são aqueles com diversidade máxima e com alta distância produto mínima [5].

Dado um reticulado qualquer, em geral é difícil calcular sua densidade de empacotamento pois é necessário determinar o vetor de norma mínima, o que para reticulados gerais é um problema difícil (a conjectura é que seja NP-Hard [17]). A mesma dificuldade ocorre no cálculo da distância produto mínima. Utilizando teoria algébrica dos números, podemos obter reticulados como imagem de um homomorfismo torcido aplicado a certos $\mathbb{Z}$-módulos contidos em corpos de números [2], os quais chamamos de *reticulados algébricos*. Através de propriedades específicas dos corpos de números utilizados na construção de cada reticulado algébrico, podemos calcular a densidade de empacotamento, a diversidade e a distância produto mínima do reticulado em questão.

Em [12] utilizando a teoria de reticulados algébricos e algoritmos de busca exaustiva no software Mathematica foram construídas versões rotacionadas com diversidade máxima dos reticulados A_2, D_3, D_4, D_5, E_7 e E_8, que são os reticulados mais densos possíveis nas dimensões $2, 3, 4, 5, 7$ e 8, respectivamente. Um interesse prático em reproduzir reticulados densos com diversidade máxima é que tais constelações podem ser usadas na transmissão de dados entre um receptor móvel e uma base ou entre um receptor móvel e um satélite através do mesmo sistema de modulação/demodulação [5].

Neste trabalho, também com o auxílio da teoria de reticulados algébricos e algoritmos computacionais construímos versões rotacionados com diversidade máxima dos reticulados mais densos conhecidos nas dimensões 12 e 24. Até o momento apenas nas dimensões 1 a 8 e 24 foram determinados os empacotamentos reticulados mais densos, que são respectivamente, A_2, D_3, D_4, D_5, E_6, E_7, E_8 e Λ_{24} [7, 9]. Para a dimensão 12 conjectura-se que o reticulado K_{12} seja o mais denso possível [8].

Quando passamos a trabalhar em dimensões mais altas como a 24, por exemplo, precisamos de algoritmos computacionais diferentes dos até então utilizados para dimensões menores, pois o tempo de execução torna-se inviável. Neste trabalho, adaptamos um algoritmo descrito por Fincke e Post em 1984 e que inspirou o bem conhecido algoritmo de decodificação para reticulados "Sphere Decoder" [19].

Uma questão interessante a ser explorada é qual é a maior distância produto mínima relativa possível para cada um dos reticulados A_2, D_3, D_4, D_5, E_7, E_8, K_{12} e Λ_{24}. Em [12] e neste trabalho apresentamos versões rotacionadas de tais reticulados e calculamos a respectiva distância produto mínima relativa para cada construção, mas não sabemos se estes valores os são os maiores possíveis para os reticulados considerados construídos como reticulados algébricos.

2 Reticulados algébricos

Os resultados sobre teoria algébrica dos números podem ser encontrados em [18, 14].

Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Existem exatamente n $\mathbb{Q}$-homomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$, para $i = 1, 2, \ldots, n$. Um corpo de números $\mathbb{K}$ é dito *totalmente real* se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, para todo $i = 1, \ldots, n$. Um elemento $\alpha \in \mathbb{K}$ é dito *totalmente positivo* se $\sigma_i(\alpha) > 0$ para todo $i = 1, \cdots, n$. Pode ser mostrado que todo ideal não nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.

Dado $x \in \mathbb{K}$, os valores $N(x) = N_{\mathbb{K}|\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ e $Tr(x) = Tr_{\mathbb{K}|\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ são chamados de *norma* e *traço* de x em $\mathbb{K}|\mathbb{Q}$, respectivamente. Se $x \in \mathcal{O}_{\mathbb{K}}$, então $N(x), Tr(x) \in \mathbb{Z}$. A *norma* de um ideal não nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ é definida como $N_{\mathbb{K}}(\mathcal{I}) = |\mathcal{O}_{\mathbb{K}}/\mathcal{I}|$. Se $\{\omega_1, \ldots, \omega_n\}$ é uma $\mathbb{Z}$-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 um invariante sobre mudança de base.

DOI: 10.5540/03.2015.003.01.0236

De agora em diante, sejam $\mathbb{K}$ um corpo de números totalmente real de grau n e $\sigma_i : \mathbb{K} \to \mathbb{R}$ para $i = 1, 2, \ldots, n$ seus n $\mathbb{Q}$-homomorfismos distintos.

Definição 2.1. *[2] Sejam $\alpha \in \mathbb{K}$ totalmente positivo e $\alpha_i = \sigma_i(\alpha)$ para todo i. O homomorfismo torcido é definido como $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$, onde $\sigma_\alpha(x) = \left(\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x)\right)$.*

Proposição 2.1. *[3] Se $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$, então a imagem $\Lambda = \sigma_\alpha(\mathcal{I})$ é um reticulado em $\mathbb{R}^n$ com base $\{\sigma_\alpha(w_1), \ldots, \sigma_\alpha(w_n)\}$. Mais ainda, como $\mathbb{K}$ é totalmente real, segue que Λ tem diversidade máxima e possui $G = \left(Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_i w_j)\right)_{i,j=1}^n$ como matriz de Gram.*

Proposição 2.2. *[3] Se $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n, então a distância produto mínima de $\Lambda = \sigma_\alpha(\mathcal{I})$ é dada por $d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_\mathbb{K}}} \frac{1}{N_\mathbb{K}(\mathcal{I})} \min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)|$. Em particular, se $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um ideal principal, então $\min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)| = N_\mathbb{K}(\mathcal{I})$.*

Quando um reticulado algébrico é construído via um ideal principal de $\mathcal{O}_\mathbb{K}$, sua distância produto mínima é inversamente proporcional ao discriminante $d_\mathbb{K}$ do corpo de números considerado. Em nossa abordagem, como uma distância produto mínima maior é desejada, consideramos corpos de números com discriminantes pequenos.

Proposição 2.3. *[13] Se $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n, então $\det(\sigma_\alpha(\mathcal{I})) = N_\mathbb{K}(\mathcal{I})^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha) d_\mathbb{K}$.*

Os corpos utilizados nas nossas construções são subcorpos totalmente reais maximais dos corpos ciclotômicos. Seja $\zeta_m \in \mathbb{C}$ uma raiz m-ésima primitiva da unidade. O *corpo ciclotômico* $\mathbb{L} = \mathbb{Q}(\zeta_m)$ é o menor subcorpo de $\mathbb{C}$ que possui $\mathbb{Q}$ e ζ_m. O corpo $\mathbb{L}$ pode ser caracterizado por $\mathbb{Q}(\zeta_m) = \left\{\sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i;\ a_i \in \mathbb{Q}\right\}$, onde ϕ é a função de Euler. O subcorpo $\mathbb{K} = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) = \left\{\sum_{i=0}^{\frac{\phi(m)}{2}-1} a_i(\zeta_m^i + \zeta_m^{-i});\ a_i \in \mathbb{Z}\right\}$ é um subcorpo totalmente real maximal de grau $[\mathbb{K} : \mathbb{Q}] = \frac{\phi(m)}{2}$.

Nossas construções são baseadas na fatoração de ideais do anel de inteiros como um produto de ideais primos. O Teorema de Kummer [14, p. 27] fornece uma forma explícita de tal decomposição que conta com a fatoração de polinômios em certos anéis quocientes. Para fatorar tais polinômios utilizamos o software Mathematica, sem o qual tais cálculos seriam muito trabalhosos. A decomposição obtida fornece dois geradores para nossos ideais. A fim de encontrar um único gerador (caso o ideal seja principal) utilizamos a forma normal de Hermite [9, p. 67].

2.1 Um reticulado K_{12}-rotacionado

O reticulado Coxeter-Todd K_{12}, descoberto em 1953 por Coxeter e Todd, é um reticulado 12-dimensional definido pela matriz geradora

$$M = \begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & \sqrt{3} & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & \sqrt{3} & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & \sqrt{3} & 0 & 0 & 0 \\
1 & -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\
-\frac{1}{2} & 1 & -\frac{1}{2} & 0 & 1 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 1 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & \frac{\sqrt{3}}{2} & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & \frac{\sqrt{3}}{2}
\end{pmatrix}.$$

Tal reticulado possui determinante 3^6 e vetor de norma mínima ao quadrado igual a 4, o que resulta na densidade de empacotamento $\Delta(K_{12}) = 0.04945$ [7, p. 127]. Ainda não foi provado que esta é a maior densidade possível na dimensão 12 mas a conjectura é de que seja.

Em [1, 2, 5] foram apresentadas versões rotacionadas do reticulado K_{12} via o corpo ciclotômico $\mathbb{Q}(\zeta_{21})$. Essas versões possuem diversidade 6 e, neste caso, não temos uma fórmula explícita para calcular a distância produto mínima. Em [4] foi apresentada uma versão do reticulado K_{12} com diversidade máxima via $\mathbb{Q}(\zeta_{84}+\zeta_{84}^{-1})$. Na Proposição 2.4, utilizando uma técnica diferente, apresentamos a construção de um reticulado K_{12}-rotacionado via $\mathbb{Q}(\zeta_{84}+\zeta_{84}^{-1})$ com diversidade máxima 12 e calculamos sua distância produto mínima relativa, que é a mesma do reticulado obtido em [4].

Na demonstração da Proposição 2.4 utilizamos o fato que se dois reticulados Λ_1 e Λ_2 possuem uma mesma matriz G como matriz de Gram, então são equivalentes na métrica euclidiana [15]. Além disso, utilizamos o algoritmo LLL de redução de base [16]. Os algoritmos de redução de base procuram por uma base do reticulado que tenha vetores aproximadamente ortogonais e de tamanho razoavelmente pequeno. O algoritmo LLL atua em tempo polinomial, mas a base encontrada pode não ser a melhor possível. A questão de encontrar a melhor base reduzida possível está relacionada ao problema de encontrar a norma mínima do reticulado.

Proposição 2.4. *Sejam* $\mathbb{K}=\mathbb{Q}(\zeta_{84}+\zeta_{84}^{-1})$ *e* $e_i=\zeta_{84}^{i}+\zeta_{84}^{-i}$, *para* $i=1,2,\cdots,12$. *Se* $\alpha=e_3e_{20}e_{19}e_2$ *e* $\mathcal{I}=\langle 1+e_2+e_3+e_5+e_6\rangle$, *então o reticulado* $\Lambda=\frac{1}{\sqrt{28}}\sigma_\alpha(\mathcal{I})$ *é um reticulado* K_{12}*-rotacionado e* $\sqrt[12]{d_{p,rel}(\Lambda)}=0.15172$.

Demonstração. Baseado na Proposição 2.3, uma condição necessária para construir um reticulado K_{12}-rotacionado, escalonado por $\sqrt{c}$ com $c\in\mathbb{Z}$, via um ideal de $\mathcal{O}_\mathbb{K}$, é a existência de um elemento totalmente positivo α tal que $3^6c^{12}=N_{\mathbb{K}|\mathbb{Q}}(\alpha)N_\mathbb{K}(\mathcal{I})^2 2^{12}3^6 7^{10}$. Utilizando o Teorema de Kummer para fatorar ideais como produto de ideais primos, segue que $2\mathcal{O}_\mathbb{K}=\mathcal{P}^2$, onde $\mathcal{P}=\langle 2,1+e_1^5+e_1^6\rangle=\langle 1+e_2+e_3+e_5+e_6\rangle$ e $N_\mathbb{K}(\mathcal{P})=2^6$ e $7\mathcal{O}_\mathbb{K}=\mathcal{S}^6$, onde $\mathcal{S}=\langle 7,4+e_1^2\rangle=\langle e_3\rangle$ e $N_\mathbb{K}(\mathcal{S})=7^2$. Tomando $\alpha^*=e_3$, segue que $N_{\mathbb{K}|\mathbb{Q}}(\alpha^*)=7^2$, e que α^* não é totalmente positivo. Através de um algoritmo de busca exaustiva conseguimos encontrar o elemento $e_{20}e_{19}e_2$ tal que se $\alpha=e_3e_{20}e_{19}e_2$, então $N_{\mathbb{K}|\mathbb{Q}}(\alpha)=7^2$ e α é totalmente positivo. Tomando $\mathcal{I}=\mathcal{P}$ e $\theta=1+e_2+e_3+e_5+e_6$, segue que uma matriz de Gram para $\frac{1}{\sqrt{28}}\sigma_\alpha(\mathcal{I})$, associada à $\mathbb{Z}$-base $\{\theta e_1,\ldots,\theta e_{12}\}$ de $\mathcal{I}$, é dada por

$$G=\begin{pmatrix}
6 & 4 & -4 & 6 & 2 & -3 & 6 & 0 & -2 & 6 & -2 & -1\\
4 & 6 & -2 & 2 & 3 & 0 & 3 & 0 & 0 & 4 & -1 & 0\\
-4 & -2 & 12 & -5 & 0 & 9 & -6 & 3 & 6 & -7 & 6 & 5\\
6 & 2 & -5 & 10 & 1 & -6 & 9 & 0 & -4 & 8 & -1 & -2\\
2 & 3 & 0 & 1 & 4 & 1 & 0 & 2 & 2 & 2 & 0 & 0\\
-3 & 0 & 9 & -6 & 1 & 10 & -6 & 2 & 8 & -6 & 3 & 6\\
6 & 3 & -6 & 9 & 0 & -6 & 12 & 0 & -6 & 9 & 0 & -3\\
0 & 0 & 3 & 0 & 2 & 2 & 0 & 4 & 1 & 0 & 3 & 0\\
-2 & 0 & 6 & -4 & 2 & 8 & -6 & 1 & 10 & -5 & 0 & 6\\
6 & 4 & -7 & 8 & 2 & -6 & 9 & 0 & -5 & 10 & -2 & -4\\
-2 & -1 & 6 & -1 & 0 & 3 & 0 & 3 & 0 & -2 & 6 & 1\\
-1 & 0 & 5 & -2 & 0 & 6 & -3 & 0 & 6 & -4 & 1 & 6
\end{pmatrix}.$$

Agora, devemos encontrar uma matriz mudança de base U tal que a matriz de Gram UGU^t de Λ satisfaça $UGU^t=MM^t$, que é uma matriz de Gram para K_{12}. Como a matriz M é formada por vetores pequenos (normas baixas), segue que primeiro aplicamos o algoritmo LLL [16] na matriz de Gram G, obtendo assim uma base com vetores menores para o reticulado Λ, cuja matriz de Gram associada é G_1 e a matriz mudança de base é U_1. Utilizando essa nova base, implementamos um algoritmo de busca exaustiva que varia as entradas de uma matriz U_2 em $\{-1,0,1\}$ e verifica se vale a igualdade $U_2G_1U_2^t=MM^t$. Com isso, encontramos a matriz mudança de base $U=U_2U_1$ dada por

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

tal que $UGU^t = MM^t$ é uma matriz de Gram de K_{12}. Como a norma euclidiana de $\frac{1}{\sqrt{28}}\sigma_\alpha(\mathcal{I})$ é $\sqrt{2}$, segue que sua distância produto mínima relativa satisfaz $\sqrt[12]{d_{p,rel}(\Lambda)} = \sqrt[12]{\frac{1}{\sqrt{28}^{12}}\frac{1}{2^{12}}\sqrt{2^{12}7^2}} = 0.15172$. □

2.2 Um reticulado Λ_{24}-rotacionado

O reticulado de Leech Λ_{24}, descoberto em 1965 por John Leech, é caracterizado como o único reticulado unimodular, par e com norma euclidiana mínima ao quadrado igual a 4. Tal reticulado possui portanto densidade de empacotamento $\Delta(\Lambda_{24}) = 0.001930$ e é provado ser o reticulado mais denso possível na dimensão 24 [9],[7, p. 131].

Em [6] foi apresentada a construção de um reticulado Λ_{24}-rotacionado via $\mathbb{Q}(\zeta_{39})$ e em [2] foram apresentadas construções de reticulados Λ_{24}-rotacionados via $\mathbb{Q}(\zeta_{39})$ e $\mathbb{Q}(\zeta_{35})$, ambas com diversidade 12 e, neste caso, não temos uma fórmula explícita para calcular a distância produto mínima. Em [4] foi apresentada uma versão do reticulado Λ_{24} com diversidade máxima via $\mathbb{Q}(\zeta_{140} + \zeta_{140}^{-1})$. Na Proposição 2.5, utilizando uma técnica diferente, apresentamos a construção de um reticulado Λ_{24}-rotacionado com diversidade máxima e calculamos sua distância produto mínima relativa, que é a mesma do reticulado obtido em [4].

Para provar que o reticulado da Proposição 2.5 é de fato um reticulado Λ_{24}-rotacionado vamos mostrar que o reticulado em questão não possui vetor com norma euclidiana ao quadrado igual a 2. Para este fim, implementamos no software Mathematica um algoritmo similiar ao criado por Fincke e Post em 1984 [11], que procura por vetores do reticulado com uma dada norma. Tal algoritmo é descrito brevemente na Subseção 2.2.1.

Proposição 2.5. *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_{140} + \zeta_{140}^{-1})$ *e* $e_i = \zeta_{140}^i + \zeta_{140}^{-i}$, *para* $i = 1, 2, \cdots, 24$. *Se* $\alpha = e_5e_7(e_1e_4e_{16}e_{23})$ *e* $\mathcal{I} = \langle 1 + e_7 + e_{14}\rangle$, *então o reticulado* $\Lambda = \frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ *é um reticulado* Λ_{24}*-rotacionado e* $\sqrt[24]{d_{p,rel}(\Lambda)} = 0.08594$.

Demonstração. Baseado na Proposição 2.3, uma condição necessária para construir um reticulado Λ_{24}-rotacionado, escalonado por $\sqrt{c}$ com $c \in \mathbb{Z}$, via um ideal de $\mathcal{O}_\mathbb{K}$, é a existência de um elemento totalmente positivo α tal que $c^{24} = N_{\mathbb{K}|\mathbb{Q}}(\alpha)N_\mathbb{K}(\mathcal{I})^2 2^{24}5^{18}7^{20}$. Podemos escrever $2\mathcal{O}_\mathbb{K} = \mathcal{P}^2$, onde $\mathcal{P} = \langle 2, 1 + e_1^5 + e_1^6 + e_1^7 + e_1^9 + e_1^{11} + e_1^{12}\rangle = \langle 1 + e_7 + e_{14}\rangle$ e $N_\mathbb{K}(\mathcal{P}) = 2^{12}$, $5\mathcal{O}_\mathbb{K} = \mathcal{S}^4$, onde $\mathcal{S} = \langle e_7\rangle$ e $N_\mathbb{K}(\mathcal{S}) = 5^6$ e $7\mathcal{O}_\mathbb{K} = \mathcal{R}^6$, onde $\mathcal{R} = \langle e_5\rangle$ e $N_\mathbb{K}(\mathcal{R}) = 7^4$. Tomando $\alpha^* = e_5e_7$, segue que $N_{\mathbb{K}|\mathbb{Q}}(\alpha^*) = 5^67^4$, e que α^* não é totalmente positivo. Através de um algoritmo de busca exaustiva conseguimos encontrar o elemento $e_1e_4e_{16}e_{23}$ tal que se $\alpha = e_5e_7(e_1e_4e_{16}e_{23})$, então $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = 5^67^4$ e α é totalmente positivo. Se $\mathcal{I} = \mathcal{P}$ e $\theta = 1+e_7+e_{14}$, então uma matriz de Gram para $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$, associada com a $\mathbb{Z}$-base $\{\theta e_1, \cdots, \theta e_{24}\}$ de $\mathcal{I}$, é dada por

$$G = \begin{pmatrix}
18 & 13 & 12 & 11 & 12 & 15 & 14 & 15 & 14 & 10 & 10 & 9 & 12 & 11 & 12 & 11 & 8 & 6 & 6 & 7 & 8 & 8 & 8 & 6\\
13 & 18 & 12 & 12 & 16 & 14 & 10 & 12 & 15 & 12 & 9 & 14 & 12 & 8 & 8 & 12 & 9 & 6 & 9 & 10 & 5 & 4 & 8 & 6\\
12 & 12 & 18 & 17 & 14 & 11 & 12 & 10 & 10 & 14 & 16 & 12 & 10 & 9 & 8 & 6 & 10 & 12 & 10 & 7 & 6 & 5 & 2 & 5\\
11 & 12 & 17 & 20 & 12 & 12 & 11 & 10 & 9 & 14 & 17 & 12 & 9 & 10 & 7 & 6 & 9 & 14 & 10 & 6 & 7 & 4 & 2 & 4\\
12 & 16 & 14 & 12 & 18 & 12 & 10 & 10 & 14 & 12 & 10 & 14 & 12 & 7 & 8 & 10 & 10 & 7 & 10 & 10 & 4 & 4 & 6 & 6\\
15 & 14 & 11 & 12 & 12 & 16 & 11 & 14 & 13 & 10 & 9 & 10 & 12 & 10 & 10 & 12 & 8 & 6 & 7 & 8 & 7 & 6 & 8 & 6\\
14 & 10 & 12 & 11 & 10 & 11 & 20 & 14 & 10 & 10 & 10 & 7 & 8 & 15 & 14 & 8 & 8 & 8 & 4 & 4 & 10 & 11 & 6 & 4\\
15 & 12 & 10 & 10 & 10 & 14 & 14 & 16 & 11 & 10 & 8 & 8 & 10 & 12 & 13 & 10 & 8 & 6 & 5 & 6 & 8 & 10 & 7 & 6\\
14 & 15 & 10 & 9 & 14 & 13 & 10 & 11 & 16 & 9 & 8 & 11 & 12 & 8 & 8 & 13 & 8 & 5 & 8 & 9 & 6 & 4 & 10 & 6\\
10 & 12 & 14 & 14 & 12 & 10 & 10 & 10 & 9 & 14 & 12 & 12 & 9 & 8 & 8 & 6 & 10 & 10 & 9 & 8 & 5 & 6 & 3 & 6\\
10 & 9 & 16 & 17 & 10 & 9 & 10 & 8 & 8 & 12 & 18 & 10 & 8 & 9 & 6 & 5 & 8 & 14 & 10 & 5 & 8 & 4 & 2 & 4\\
9 & 14 & 12 & 12 & 14 & 10 & 7 & 8 & 11 & 12 & 10 & 14 & 10 & 6 & 6 & 8 & 9 & 8 & 10 & 10 & 4 & 4 & 5 & 6\\
12 & 12 & 10 & 9 & 12 & 12 & 8 & 10 & 12 & 9 & 8 & 10 & 12 & 7 & 8 & 10 & 8 & 5 & 8 & 9 & 6 & 5 & 8 & 6\\
11 & 8 & 9 & 10 & 7 & 10 & 15 & 12 & 8 & 8 & 9 & 6 & 7 & 14 & 11 & 8 & 6 & 8 & 4 & 4 & 10 & 10 & 6 & 4\\
12 & 8 & 8 & 7 & 8 & 10 & 14 & 13 & 8 & 8 & 6 & 6 & 8 & 11 & 14 & 7 & 8 & 5 & 4 & 5 & 8 & 11 & 6 & 5\\
11 & 12 & 6 & 6 & 10 & 12 & 8 & 10 & 13 & 6 & 5 & 8 & 10 & 8 & 7 & 14 & 6 & 4 & 6 & 8 & 6 & 4 & 10 & 6\\
8 & 9 & 10 & 9 & 10 & 8 & 8 & 8 & 8 & 10 & 8 & 9 & 8 & 6 & 8 & 6 & 10 & 7 & 8 & 7 & 4 & 5 & 4 & 6\\
6 & 6 & 12 & 14 & 7 & 6 & 8 & 6 & 5 & 10 & 14 & 8 & 5 & 8 & 5 & 4 & 7 & 14 & 8 & 4 & 6 & 4 & 1 & 4\\
6 & 9 & 10 & 10 & 10 & 7 & 4 & 5 & 8 & 9 & 10 & 10 & 8 & 4 & 4 & 6 & 8 & 8 & 10 & 7 & 4 & 2 & 4 & 5\\
7 & 10 & 7 & 6 & 10 & 8 & 4 & 6 & 9 & 8 & 5 & 10 & 9 & 4 & 5 & 8 & 7 & 4 & 7 & 10 & 3 & 4 & 6 & 6\\
8 & 5 & 6 & 7 & 4 & 7 & 10 & 8 & 6 & 5 & 8 & 4 & 6 & 10 & 8 & 6 & 4 & 6 & 4 & 3 & 10 & 7 & 6 & 3\\
8 & 4 & 5 & 4 & 4 & 6 & 11 & 10 & 4 & 6 & 4 & 4 & 5 & 10 & 11 & 4 & 5 & 4 & 2 & 4 & 7 & 12 & 4 & 4\\
8 & 8 & 2 & 2 & 6 & 8 & 6 & 7 & 10 & 3 & 2 & 5 & 8 & 6 & 6 & 10 & 4 & 1 & 4 & 6 & 6 & 4 & 10 & 4\\
6 & 6 & 5 & 4 & 6 & 6 & 4 & 6 & 6 & 6 & 4 & 6 & 6 & 4 & 5 & 6 & 6 & 4 & 5 & 6 & 3 & 4 & 4 & 6
\end{pmatrix}$$

Através da matriz de Gram G, podemos concluir que $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ é um reticulado unimodular par. Para mostrar que este reticulado é de fato um reticulado Λ_{24}-rotacionado precisamos

mostrar que sua norma euclidiana mínima ao quadrado é igual a 4, pois Λ_{24} é o único reticulado unimodular, par e com norma euclidiana mínima ao quadrado igual a 4 na dimensão 24, a menos de equivalência [9]. Utilizando inicialmente o algoritmo LLL e depois o algoritmo descrito na Subseção 2.2.1 conseguimos verificar que não existe um vetor com norma ao quadrado igual a 2. Portanto, o reticulado é de fato um reticulado Λ_{24}-rotacionado. Como $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ tem norma mínima euclidiana igual a 2, segue que sua distância produto mínima relativa é $\sqrt[24]{d_{p,rel}(\Lambda)} = \sqrt[24]{\frac{1}{\sqrt{140}^{24}}\frac{1}{2^{24}}\sqrt{2^{24}5^67^4}} = 0.08594$. □

2.2.1 Algoritmo

Sejam Λ um reticulado e G uma matriz de Gram para Λ. O primeiro passo é fazer uma fatoração de Cholesky em G dada por $G = RR^t$, onde

$$R = \begin{pmatrix} r_{1,1} & 0 & \cdots & 0 \\ r_{2,1} & r_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ r_{24,1} & r_{24,2} & \cdots & r_{24,24} \end{pmatrix}$$

é uma matriz triangular inferior. A matriz R pode ser vista como uma matriz geradora de um reticulado Λ_1 equivalente ao reticulado Λ. Daí, como Λ e Λ_1 são equivalentes com o mesmo determinante, segue que possuem o mesmo valor de norma mínima. Um vetor de Λ_1 é dado por $\boldsymbol{y} = \boldsymbol{x}R$, para algum $\boldsymbol{x} \in \mathbb{Z}^n$. Assim, a norma euclidiana de $\boldsymbol{y}$ ao quadrado é dada por

$$\|\boldsymbol{y}\|^2 = \left|\sum_{i=1}^{n} x_i r_{i,1}\right|^2 + \cdots + |x_{23}r_{23,23} + x_{24}r_{24,23}|^2 + |x_{24}r_{24,24}|^2.$$

Dado um valor r, para que $\boldsymbol{y}$ tenha norma menor ou igual a $\sqrt{r}$, devemos ter que $|x_{24}r_{24,24}|^2 \leq r$, o que produz um intervalo pequeno de possibilidades para x_{24}. Uma vez que o intervalo em que x_{24} pode variar é conhecido, procuramos o intervalo de possibilidades para x_{23} levando em conta que $|x_{23}r_{23,23} + x_{24}r_{24,23}|^2 + |x_{24}r_{24,24}|^2 \leq r$ e guardamos os pares ordenados (x_{23}, x_{24}). Notemos que os valores de x_{23} dependem dos valores de x_{24}. Seguindo o raciocínio indutivamente, obtemos 24 condições necessárias para que a norma de $\boldsymbol{y}$ seja menor ou igual a $\sqrt{r}$. Tais condições são descritas por

$$0 \leq \boldsymbol{x}_k R_k R_k^t \boldsymbol{x}_k^t \leq r, \ k = 1, \cdots, 24, \tag{1}$$

onde $\boldsymbol{x}_k = (x_k, x_{k+1}, \cdots, x_{23}, x_{24})$ e

$$R_k = \begin{pmatrix} r_{k,k} & 0 & \cdots & 0 \\ r_{k+1,k} & r_{k+1,k+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ r_{24,1} & r_{24,2} & \cdots & r_{24,24} \end{pmatrix}.$$

Em cada condição tem-se que a variação de x_k depende da variação de $(x_{k-1}, \cdots, x_{23}, x_{24})$. Após obter esses intervalos de variação, testamos os candidatos.

Observação 2.1. *Observarmos que se para Λ_{24} tivéssemos utilizado o mesmo algoritmo utilizado no caso do reticulado K_{12} para buscar por uma matriz mudança de base, mesmo variando os possíveis coeficientes da matriz mudança de base somente em $\{-1, 0, 1\}$, muito provavelmente não obteríamos uma resposta em um tempo viável.*

Referências

[1] A.A. Andrade, A.J. Ferrari, C.W.O. Benedito, S.I.R. Costa, Constructions of algebraic lattices, *Computational & Applied Mathematics*, vol. 29, n. 3, p. 493-505, 2010. 2010.

[2] E. Bayer-Fluckiger, Lattices and number fields, *Contemporary Mathematics*, vol. 241, p. 69-84, 1999.

[3] E. Bayer-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*, vol. 50, n. 4, p. 702-714, 2004.

[4] E. Bayer-Fluckiger, I. Suarez, *Ideal lattices over totally real number fields and Euclidean minima*, Archiv der Mathematik, vol. 86, n. 3, p. 217-225, 2006.

[5] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiori, Good lattice constellations for both Rayleigh fading and Gaussian channels, *IEEE Transactions on Information Theory*, vol. 42, n. 2, p. 502-517, 1996.

[6] M. Craig, A cyclotomic construction of the Leech's lattice, *Mathematika*, vol. 25, p. 236-241, 1978.

[7] J.H. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups¨, Springer-Verlag, New York, 1998.

[8] J.H. Conway, N.J.A. Sloane, What are all the best sphere packings in low dimensions?, *Discrete & Computational Geometry*, Springer-Verlag, vol. 13, n. 1, p. 383-403, 1995.

[9] H. Cohn, A. Kumar, Optimality and uniqueness of the Leech lattice among lattices, *Annals of Mathematics*, Princeton, vol. 170, p. 1003-1050, 2009.

[10] H. Cohen, "A course in Computational Algebraic Number Theory¨, Springer-Verlag, New York, 1993.

[11] U. Fincke, M. Pohst, Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis, *Mathematics of Computation*, AMS, vol, 44, n. 170, p. 463-471, 1985.

[12] G.C. Jorge, A.J. Ferrari, S.I.R. Costa, Reticulados densos nas dimensões 2,3,4,5,7 e 8 com diversidade máxima, "XXXIV Congresso Nacional de Matemática Aplicada e Computacional", Águas de Lindóia, São Paulo, 2012.

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

[14] S. Lang, "Algebraic Number Theory, Addison-Wesley Publishing Company, New York, 1970.

[15] C.C. Lavor, M.M. Alvez, R.M. Siqueira, S.I.R. Costa, Uma introdução à teoria de códigos, "Notas em Matemática Aplicada, XXVI Congresso Nacional de Matemática Aplicada e Computacional, 2006.

[16] A.K. Lenstra, H.W. Lenstra, L. Lovasz, Factoring polynomials with rational coefficients, *Math. Ann.*, vol. 261, p. 515-534, 1982.

[17] D. Micciancio, S. Goldwasser, "Complexity of Lattices Problems: A Cryptographic Perspective¨, The Kluwer International Series in Engeneering as Computer Science, vol. 671, Kluwer Academic Publishers, 2002

[18] P. Samuel, "Algebraic Theory of Numbers, Hermann, Paris, 1970.

[19] E. Viterbo and J. Boutros, A universal lattice code decoder for fading channels, *IEEE Transactions on Information Theory*, vol. 45, n. 5, p. 1639-1642, 1999.

