Construção do Reticulado E_8 via Álgebra dos Quatérnios sobre $\mathbb{Q}(\sqrt{-11})$

Carina Alves & Plínio G. Sicuti & Agnaldo J. Ferrari

Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro, São José do Rio Preto e Bauru

carina.alves@unesp.br

Instituto de Matemática Pura e Aplicada

Introdução

- Constelação de sinais tendo estrutura de reticulados tem sido estudadas para a transmissão de dados através de canais de comunicação.
- Mais recentemente, a necessidade de maior transmissão de dados levou a considerar canais de comunicação usando múltiplas antenas no transmissor e no receptor.
- Neste caso, é natural considerar reticulados construídos a partir de um ideal na ordem maximal de uma álgebra de divisão.

Reticulados e Álgebra dos Quatérnios

- Um reticulado Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$ gerado por combinações inteiras de n vetores linearmente independentes $v_1, \cdots, v_n \in \mathbb{R}^n$.
- Uma matriz M cujas linhas são esses vetores é chamada de matriz geradora para Λ e a matriz $G = MM^t$ é chamada de matriz de Gram para o reticulado Λ. O determinante de Λ é dado por $\det \Lambda = \det G$.
- A densidade de empacotamento de um reticulado é a proporção do espaço $\mathbb{R}^n$ coberta pelas esferas não sobrepostas de raio máximo centrado nos pontos de Λ. O empacotamento reticulado mais denso possível foi determinado somente nas dimensões 1 a 8 e 24.
- Uma álgebra dos quatérnios $\mathcal{A} = (a, b)_{\mathbb{F}}$ sobre um corpo de números $\mathbb{F}$ é uma álgebra de dimensão 4 com base $\{1, i, j, k\}$ satisfazendo $i^2 = a$, $j^2 = b$ e $k = ij = -ji$, onde $a, b \in \mathbb{F} \setminus \{0\}$.

Proposição 1. *[1] Uma álgebra dos quatérnios $\mathcal{A} = (a, b)_{\mathbb{F}}$ é uma álgebra de divisão se, e somente se, $b \notin N_{\mathbb{F}(\sqrt{a})/\mathbb{F}}(\mathbb{F}(\sqrt{a}))$.*

Ordem e Determinante

Definição 1. *Uma $O_{\mathbb{F}}$-ordem $\mathcal{O}$ em $\mathcal{A}$ é um subanel de $\mathcal{A}$ que tem o mesmo elemento de identidade de $\mathcal{A}$ e tal que $\mathcal{O}$ é um módulo finitamente gerado sobre $O_{\mathbb{F}}$ e gera $\mathcal{A}$ como um espaço linear sobre $\mathbb{F}$. $\mathcal{O}$ é dita ser maximal se não estiver contida propriamente em qualquer outra $O_{\mathbb{F}}$-ordem em $\mathcal{A}$.*

Seja $\Lambda_{\mathcal{I}}$ um $\mathbb{Z}$-reticulado obtido de um ideal à esquerda $\mathcal{I}$ da ordem maximal $\mathcal{O}$.

Lema 1. *[1] Seja $\mathbb{F}$ um corpo quadrático imaginário e seja $\mathcal{I}$ um ideal à esquerda da ordem maximal $\mathcal{O}$ de uma álgebra de divisão cíclica $\mathcal{A}$ de índice 2 sobre $\mathbb{F}$ com o discriminante $\delta_{\mathcal{O}}$. Então*

$$\det(\Lambda_{\mathcal{I}}) = D_{\mathbb{F}}^4 \cdot N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4, \quad (1)$$

onde $D_{\mathbb{F}}$ é o discriminante de $\mathbb{F}$ sobre $\mathbb{Q}$, $N_{\mathbb{F}/\mathbb{Q}}$ é a norma de $\mathbb{F}$ sobre $\mathbb{Q}$ e $nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I})$ denota a norma reduzida de $\mathcal{I}$.

Volume de Tamagawa

Códigos baseados em álgebras dos quatérnios tais que o volume de Tamagawa é pequeno são mais adequados para decodificação usando o método de redução algébrica [2].

Teorema 1. *(Volume de Tamagawa). Seja $\mathcal{A}$ uma álgebra dos quatérnios sobre $\mathbb{F}$ tal que $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathcal{M}_2(\mathbb{C})$ e $\mathcal{O}$ uma ordem maximal de $\mathcal{A}$. Então o volume hiperbólico é dado por*

$$Vol(\mathcal{P}_{\mathcal{O}^1}) = \frac{1}{4\pi^2}\zeta_{\mathbb{F}}(2)|D_{\mathbb{F}}|^{3/2} \prod_{p|\delta_{\mathcal{O}}} (N_p - 1),$$

onde $\mathcal{O}^1 = \{U \in \mathcal{O}^* | \det(U) = 1\}$, $\zeta_{\mathbb{F}}$ denota a função zeta de Dedekind, $D_{\mathbb{F}}$ é o discriminante de $\mathbb{F}$, $\delta_{\mathcal{O}}$ é o discriminante de $\mathcal{O}$, p varia entre os primos de $O_{\mathbb{F}}$ e $N_p = [O_{\mathbb{F}} : pO_{\mathbb{F}}]$.

Procuramos por uma álgebra de divisão dos quatérnios sobre $\mathbb{F} = \mathbb{Q}(\sqrt{-11})$ com menor volume de Tamagawa e na qual a construção de reticulados via tal álgebra resulte no reticulado E_8. A álgebra que satisfaz as condições acima é $\mathcal{A} = (-3, -1)_{\mathbb{F}}$. Temos que $|D_{\mathbb{F}}| = 4$, $\zeta_{\mathbb{F}} = 1,49613\cdots$, e $Vol(\mathcal{P}_{\mathcal{O}^1}) = 5,53043\cdots$.

Construção do Reticulado E_8 via $\mathcal{A} = (-3, -1)_{\mathbb{Q}(\sqrt{-11})}$

Seja $\mathbb{F} = \mathbb{Q}(\sqrt{-11})$ e $\Lambda_{\mathcal{I}}$ um reticulado, onde $\mathcal{I}$ é um ideal à esquerda da ordem maximal de $\mathcal{A}$:

$$\mathcal{O} = \mathbb{Z}[\omega] \oplus \mathbb{Z}[\omega]\frac{1+i}{2} \oplus \mathbb{Z}[\omega]j \oplus \mathbb{Z}[\omega]\frac{j+ij}{2},$$

onde $\omega = (-1 + \sqrt{-11})/2$.

Uma condição necessária (mas não suficiente) para $\Lambda_{\mathcal{I}}$ ser isomorfo a $\sqrt{c}E_8$ (uma versão em escalar de E_8 para algum inteiro c) é que $\det(\Lambda_{\mathcal{I}}) = c^8$. Para cumprir esta condição precisamos que a igualdade (1) seja satisfeita

$$D_{\mathbb{F}}^4 \cdot N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4 = c^8.$$

Neste caso, $|D_{\mathbb{F}}| = 11$ e $N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) = 3^4$. Para encontrar um ideal à esquerda $\mathcal{I}$ da ordem maximal $\mathcal{O}$ de $\mathcal{A}$ com norma reduzida $11 \cdot 3 = 33$, consideramos os subcorpos $\mathbb{K}$ de $\mathcal{A}$ que tem a forma

$$\mathbb{K} = \mathbb{F}\left(\sqrt{-3x_1^2 - x_2^2 - 3x_3^2}\right).$$

O ideal $\mathcal{I}$ será o produto de dois ideais primos $\mathcal{I}_1$ e $\mathcal{I}_2$ em $\mathcal{O}$ com respectiva norma absoluta 11 e 3. Assim, é suficiente encontrar ideais J_1, $J_2 \in O_{\mathbb{K}}$ tais que

$$\begin{cases} 11 = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(J_1)) \\ 3 = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(J_2)) \end{cases}$$

Assim, para construir $\mathcal{I}_1$ consideramos $\mathbb{K} = \mathbb{Q}(\sqrt{-11}, \sqrt{-7})$ ($x_1 = x_2 = x_3 = 1$). Neste caso, J_1 é gerado por $(-\theta + \omega - 1)$, onde $\theta = (1 + \sqrt{-7})/2$. Depois de mergulhar J_1 em $\mathcal{A}$ obtemos um ideal à esquerda $\mathcal{I}_1$ gerado por $\left((\omega - 1) - \frac{(1+i)}{2} - \frac{(j+ij)}{2}\right)$. Agora, para construir $\mathcal{I}_2$ consideramos $\mathbb{K} = \mathbb{Q}(\sqrt{-11}, \sqrt{-3})$ ($x_1 = 1$ e $x_2 = x_3 = 0$). Neste caso, J_2 é gerado por $((\omega + 1)\theta - \omega + 1)$, onde $\theta = (1 + \sqrt{-3})/2$. Depois de mergulhar J_2 em $\mathcal{A}$ obtemos um ideal à esquerda $\mathcal{I}_2$ gerado por $\left((-w + 1) + (w + 1)\frac{1+i}{2}\right)$. Assim, o ideal $\mathcal{I} = \mathcal{I}_1\mathcal{I}_2$ dá um reticulado cuja matriz de Gram tem o determinante 1 e todos os seus termos diagonais são inteiros pares. Portanto, $\Lambda_{\mathcal{I}}$ é um reticulado unimodular par de dimensão 8. Como o reticulado E_8 é o único reticulado unimodular na dimensão 8, segue que $\Lambda_{\mathcal{I}}$ coincide com o reticulado E_8.

Referências

[1] C.Alves and J-C. Belfiore. Lattices from maximal orders into quaternion algebras. *Journal of Pure and Applied Algebra*, 219:687–702, 2015.

[2] L. Luzzi, G. R-B. Othman, and J-C. Belfiore. Algebraic reduction for the golden code. *Advances in Mathematics of Communications*, 6(1):1–26, 2012.

Agradecimentos

Este trabalho foi financiado pela FAPESP Processos: 2023/06476-9 e 2019/20800-8.