Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 5, N. 1, 2017.

Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Construção de Reticulados Unimodulares via Álgebra dos Quatérnios

Cintya Wink de O. Benedito[1]
IMECC - Universidade Estadual de Campinas, UNICAMP, Campinas, SP
Carina Alves[2]
Departamento de Matemática, UNESP, Rio Claro, SP
Sueli I. R. Costa[3]
IMECC - Universidade Estadual de Campinas, UNICAMP, Campinas, SP
Nelson Gomes Brasil Jr.[4]
IMECC - Universidade Estadual de Campinas, UNICAMP, Campinas, SP

Resumo. Neste trabalho, propomos uma ferramenta algébrica para construir reticulados a partir de ordens maximais nas álgebras dos quatérnios cujo centro é um corpo de números totalmente real. Em particular, usando a teoria e resultados obtidos, apresentamos uma construção dos reticulados unimodulares E_8 e Λ_{24}.

Palavras-chave. Reticulado Ideal, Álgebra dos Quatérnios, Ordem Maximal

1 Introdução

Um reticulado Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$ gerado por combinações de n vetores linearmente independentes em $\mathbb{R}^n$. Λ é dito unimodular se for integral e se $\det(\Lambda) = 1$. Constelações de sinais tendo a estrutura de reticulados são consideradas importantes para a transmissão de sinais pois a estrutura algébrica e geométrica dos reticulados facilita no processo de codificação e decodificação.

A estrutura da álgebra dos quatérnios tem sido proposta para STBC (*Space-Time Block Code*) desde a introdução do código de Alamout para duas antenas transmissoras [1]. No contexto de STBC, reticulados tem sido construídos usando ordens maximais em álgebra de divisão cíclica [7].

Motivados pela construção de reticulados, neste trabalho estamos interessados em construir os reticulados unimodulares E_8 e Λ_{24} via ordens maximais nas álgebras de divisão de índice 2 sobre corpos de números totalmente reais. A menos de isometria, E_8 e Λ_{24} são os únicos reliculados unimodulares pares e com maior densidade de empacotamento nas dimensões 8 e 24, respectivamente.

[1]cintyawink@gmail.com
[2]carina@rc.unesp.br
[3]sueli@ime.unicamp.br
[4]nelson.gbrasil@gmail.com

Este trabalho é organizado como segue. Na Seção 2, selecionamos alguns resultados básicos da teoria de reticulados ideais. Na Seção 3, apresentamos conceitos e resultados envolvendo álgebra dos quatérnios e ordens maximais. Na Seção 4, expomos um método de construir reticulados via álgebra dos quatérnios sobre corpos de números totalmente reais e caracterizamos a matriz geradora de tais reticulados. Na Seção 5, construções dos reticulados E_8 e Λ_{24} são apresentadas. Finalmente, na Seção 6, apresentamos nossa conclusão.

2 Reticulados Ideais

A teoria de reticulados ideais fornece uma forma de construir reticulados algébricos. Como nosso foco é a construção de reticulados sobre corpos de números totalmente reais, apresentamos alguns resultados e conceitos dessa teoria para corpos nestas condições.

Seja $\mathbb{K}$ um corpo de números totalmente real de grau n e seja $\mathbb{O}_{\mathbb{K}}$ seu anel dos inteiros. Então, existem n homomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{R}$, para $i =, \cdots, n$.

Dado $x \in \mathbb{K}$, os valores $N_{\mathbb{K}/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ e $Tr_{\mathbb{K}/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ são chamados *norma* e *traço* de x em $\mathbb{K}/\mathbb{Q}$, respectivamente. Se $\{w_1, \cdots, w_n\}$ é uma $\mathbb{Z}$-base de $\mathbb{O}_{\mathbb{K}}$, então o *discriminante* de $\mathbb{K}$ é dado por $d_{\mathbb{K}} = \left(\det(\sigma_j(w_i))_{i,j=1}^{n}\right)^2$.

Um *reticulado ideal* é um reticulado $\Lambda = (\mathcal{I}, q_\alpha)$, onde $\mathcal{I}$ é um ideal de $\mathbb{O}_{\mathbb{K}}$ e $q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}$ é tal que

$$q_\alpha(x, y) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x y),$$

onde $\alpha \in \mathbb{K}$ é totalmente positivo, ou seja, $\sigma_i(\alpha) > 0 \, \forall i$. A *dimensão* de um reticulado ideal é o grau n do corpo de números $\mathbb{K}$.

Seja $\alpha \in \mathbb{K}$ tal que $\alpha_i = \sigma_i(\alpha) > 0$ para todo $i = 1, \cdots, n$. O homomorfismo $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ onde

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \cdots, \sqrt{\alpha_n}\sigma_n(x))$$

é chamado de *homomorfismo torcido*. Quando $\alpha = 1$, o homomorfismo é chamado de *homomorfismo canônico*.

Pode-se mostrar que se $\mathcal{I} \subseteq \mathbb{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-modulo livre de posto n com $\mathbb{Z}$-base $\{w_1, \cdots, w_n\}$, então a imagem $\Lambda = \sigma_\alpha(\mathcal{I})$ é um reticulado em $\mathbb{R}^n$ com base $\{\sigma_\alpha(w_1), \cdots, \sigma_\alpha(w_n)\}$. Além disso, como $\mathbb{K}$ é totalmente real, a matriz de Gram associada ao reticulado $\Lambda = \sigma_\alpha(\mathcal{I})$ é

$$G = \left(Tr_{\mathbb{K}/\mathbb{Q}}(\alpha w_i \overline{w_j})\right)_{i,j=1}^{n},$$

e o determinante de Λ é $det\Lambda = detG$.

3 Álgebra dos Quatérnios e Ordem dos Quatérnios

Uma *álgebra dos quatérnios* $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ sobre um corpo $\mathbb{K}$ é uma álgebra central simples de dimensão 4 com base $\{1, i, j, k\}$ satisfazendo $i^2 = \alpha$, $j^2 = \beta$ e $k = ij = -ji$, onde $\alpha, \beta \in \mathbb{K}/\{0\}$.

Example 3.1. *Um exemplo clássico de álgebra dos quatérnios sobre o corpo dos números reais é a álgebra dos quatérnios de Hamilton* $\mathcal{H} = (-1, -1)_{\mathbb{R}}$.

Se $x \in \mathcal{A}$, $x = x_1 + x_2 i + x_3 j + x_4 k$ com $x_1, x_2, x_3, x_4 \in \mathbb{K}$, então $\overline{x} = x_1 - x_2 i - x_3 j - x_4 k$ é chamado de *conjugado* de x. Para $x \in \mathcal{A}$, o *traço reduzido* e *norma reduzida* de x são definidos como

$$Trd(x) = x + \overline{x} \quad \text{e} \quad Nrd(x) = x\overline{x},$$

respectivamente.

Uma álgebra dos quatérnios $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ é uma álgebra de divisão se, e somente se, $\forall x \in \mathcal{A} \setminus \{0\}$, $Nrd(x) \neq 0$ e $\mathcal{A}$ é definida se, e somente se, a forma quadrática $Trd(x\overline{y})$ em $\mathcal{A}$ é definida positiva, para todo $x, y \in \mathcal{A}$, ou seja, $Trd(x\overline{x}) \geq 0$, $Trd(x\overline{y})$ em $\mathcal{A}$ é definida positiva, para todo $x \in \mathcal{A}$.

Seja R um anel com corpo de frações $\mathbb{K}$ e seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. Uma *ordem* $\mathcal{O}$ em $\mathcal{A}$ é um subanel de $\mathcal{A}$ contendo a unidade, ou equivalentemente, se $\mathcal{O}$ é um R-modulo finitamente gerado tal que $\mathcal{A} = \mathbb{K}\mathcal{O}$. Logo, considerando R um anel de $\mathbb{K}$ e a álgebra $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$, com $\alpha, \beta \in R$, então $\mathcal{O} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in R\}$ é uma ordem em $\mathcal{A}$ denotada por $\mathcal{O} = (\alpha, \beta)_R$.

Se $\mathcal{I}$ é um ideal na álgebra dos quatérnios $\mathcal{A}$ e $\mathcal{O}$ é uma ordem de $\mathcal{A}$, dizemos que $\mathcal{I}$ é um *ideal à esquerda* de $\mathcal{O}$ se $\mathcal{O}\mathcal{I} \subset \mathcal{I}$ e $\mathcal{I}$ é um *ideal à direita* de $\mathcal{O}$ se $\mathcal{I}\mathcal{O} \subset \mathcal{I}$. A norma reduzida de $\mathcal{I}$, denotada por $Nrd(\mathcal{I})$, é o R-ideal fracionário grado por $\{Nrd(x) : x \in \mathcal{I}\}$.

Proposição 3.1. *[3] Seja $\mathcal{O}$ uma R-ordem em uma álgebra dos quatérnios $\mathcal{A}$. Se $x \in \mathcal{O}$, então $Trd(x), Nrd(x) \in R$.*

Seja $\mathcal{O}$ uma R-ordem em uma álgebra dos quatérnios $\mathcal{A}$. O *discriminante reduzido de* $\mathcal{O}$, $\mathcal{D}(\mathcal{O})$, é um ideal gerado por $\{\{x_1, x_2, x_3\} : x_1, x_2, x_3 \in \mathcal{O}\}$, onde

$$\{x_1, x_2, x_3\} = Trd([x_1, x_2]\overline{x_3}) = (x_1 x_2 - x_2 x_1)\overline{x_3} - x_3(\overline{x_1 x_2 - x_2 x_1}).$$

Uma ordem $\mathcal{M}$ em uma álgebra dos quatérnios $\mathcal{A}$ é *maximal* se $\mathcal{M}$ não está propriamente contida em nenhuma outra ordem de $\mathcal{A}$.

Proposição 3.2. *[5] Se $\mathcal{M}$ é uma ordem maximal em $\mathcal{A}$ contendo outra ordem $\mathcal{O}$, então o discriminante satisfaz*

$$\mathcal{D}(\mathcal{O}) = \mathcal{D}(\mathcal{M}) \cdot [\mathcal{M} : \mathcal{O}], \quad \mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}).$$

Reciprocamente, se $\mathcal{D}(\mathcal{O}) = \mathcal{D}(\mathcal{A})$, então $\mathcal{O}$ é uma ordem maximal em $\mathcal{A}$.

4 Reticulados Via Ordem Maximal da Álgebra dos Quatérnios

Nesta seção propomos uma construção algébrica de reticulados de dimensão $4n$ via ordens maximais de uma álgebra dos quatérnios, identificando sua matriz de Gram e sua matriz geradora. Podemos definir reticulados ideais via ordens maximais da mesma forma como definimos reticulados ideais via corpo de números.

DOI: 10.5540/03.2017.005.01.0237

Seja $\mathbb{K}$ um corpo de números totalmente real de grau n e $\mathcal{A}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. Se $\mathcal{I}$ é um ideal em $\mathcal{A}$ e α é um elemento totalmente positivo em $\mathbb{K}$, então temos uma forma bilinear simétrica definida positiva $Q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Q}$ dada por $Q_\alpha(x,y) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(x\overline{y}))$.

Neste caso, seja $\Lambda = (\mathcal{I}, \alpha)$ o reticulado ideal associado a Q_α. Note que, se o corpo de números $\mathbb{K}$ sobre $\mathbb{Q}$ é de grau n, então o reticulado tem dimensão $4n$, $n \geq 1$.

Seja $\mathcal{M}$ uma ordem maximal de $\mathcal{A}$ com base $B = \{v_1, v_2, v_3, v_4\}$. Se $[\mathbb{K} : \mathbb{Q}] = n$ e $\mathbb{O}_\mathbb{K}$ é o anel dos inteiros de $\mathbb{K}$ então $\{u_1, \cdots, u_n\}$ é uma $\mathbb{Z}$-base de $\mathbb{O}_\mathbb{K}$. Considerando $\mathcal{I} = \mathcal{M}$ um ideal de $\mathcal{A}$ com base B e α um elemento totalmente positivo de $\mathbb{K}$ então $\Lambda = (\mathcal{I}, \alpha)$ é um reticulado ideal de dimensão $4n$ com base

$$B' = \{v_i u_j\} = \{w_1, \cdots, w_{4n}\},\ i = 1, \cdots, 4 \text{ e } j = 1, \cdots, n.$$

Além disso, como $\mathbb{K}$ é um corpo de números totalmente real, a matriz de Gram associada a $\Lambda = (\mathcal{I}, \alpha)$ é

$$G = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i \overline{w_j})),$$

onde $w_i, w_j \in B'$. Da mesma forma, o determinante de Λ é $det\Lambda = detG$.

A proposição a seguir fornece um modo de escrever o determinante de um reticulado em termos de alguns parâmetros algébricos. Isso é de grande importância para as construções que apresentamos aqui.

Proposição 4.1. *[6] Seja $\mathbb{K}$ um corpo de números totalmente real e $\mathcal{A}$ uma álgebra dos quatérnios definida sobre $\mathbb{K}$. Se $\mathcal{I} \subseteq \mathcal{M}$ é um ideal de uma ordem maximal $\mathcal{M}$ de $\mathcal{A}$ e α é um elemento totalmente positivo de $\mathbb{K}$ tal que $\Lambda = (\mathcal{I}, \alpha)$ é um reticulado, então*

$$det(G) = d_\mathbb{K}^4 N(\alpha)^4 N_\mathbb{K}(Nrd(\mathcal{I}))^4 (\mathcal{D}(\mathcal{M})^2), \tag{1}$$

onde G é a matriz de Gram de Λ.

Uma condição necessária, mas não suficiente, para um reticulado Λ seja isomorfo a um reticulado $(\sqrt{c}\Lambda')^n$, uma versão escalonada de Λ', é que

$$det(\Lambda) = c^n det(\Lambda'), \tag{2}$$

uma vez que a matriz de Gram de $(\sqrt{c}\Lambda')^n$ é cM, onde M é a matriz geradora de Λ' e $c \in \mathbb{Z}$.

Utilizando as Equações (1) e (2) podemos construir uma versão rotacionada de um reticulado conhecido na literatura com matriz de Gram G. A construção que propomos aqui, diferente de [6], nos permite explicitar além da matriz de Gram, também a matriz geradora deste reticulado rotacionado.

Seja $\{u_1, \cdots, u_n\}$ a $\mathbb{Z}$-base de $\mathbb{O}_\mathbb{K}$, então a matriz geradora do reticulado $\sigma_{2\alpha}(\mathbb{O}_\mathbb{K})$ obtido utilizando o homomorfismo torcido é

$$M_1 = \begin{pmatrix} \sqrt{2\sigma_1(\alpha)}\sigma_1(u_1) & \cdots & \sqrt{2\sigma_n(\alpha)}\sigma_n(u_1) \\ \vdots & \ddots & \vdots \\ \sqrt{2\sigma_1(\alpha)}\sigma_1(u_n) & \cdots & \sqrt{2\sigma_n(\alpha)}\sigma_n(u_n) \end{pmatrix}_{n \times n}.$$

Expandindo M_1 em uma matriz $4n \times 4n$, obtemos a seguinte matriz:

$$\phi_1 = \begin{pmatrix} M_1 & 0 & 0 & 0 \\ 0 & M_1 & 0 & 0 \\ 0 & 0 & M_1 & 0 \\ 0 & 0 & 0 & M_1 \end{pmatrix}. \tag{3}$$

Consideramos a matriz φ cujas linhas são os coeficiente de $B = \{v_1, v_2, v_3, v_4\}$ (base de $\mathcal{M}$), onde $v_s = v_{s1} + v_{s2}i + v_{s3}j + v_{s4}k$, para $s = 1, \cdots, 4$. Aplicando os n homomorfismos de $\mathbb{K}$ em $\mathbb{R}$, $\sigma_1, \cdots, \sigma_n$, nos elementos de φ obtemos a seguinte matriz $4n \times 4n$:

$$\phi_2 = (\sigma_k(\varphi_{i,j})) \quad = \quad \begin{pmatrix} \sigma_1(\varphi_{ij}) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_n(\varphi_{ij}) \end{pmatrix},$$

onde $i, j = 1, \cdots, 4$ e $k = 1, \cdots, n$. Assim, a matriz geradora do reticulado ideal $\Lambda = (\mathcal{I}, \alpha)$ é dada por $M = \phi_1 \phi_2$.

5 Construção dos Reticulados E_8 e Λ_{24}

Nesta seção, seguindo a construção proposta na Seção 4, encontramos ideais $\mathcal{I} \subseteq \mathcal{M}$ e elementos totalmente positivos $\alpha \in \mathbb{K}$ tais que o reticulado ideal $\Lambda = (\mathcal{I}, \alpha)$ seja isomorfo aos reticulados unimodulares mais densos nas dimensões 8 e 24, os reticulados E_8 e Λ_{24}, respectivamente. Nestas construções os algoritmos foram implementados nos *softwares* *Magma* e *Wolfram Mathematica*.

5.1 Construção do E_8

Considere a álgebra dos quatérnios $\mathcal{A} = (-1, -1)_{\mathbb{K}}$ sobre o corpos de números totalmente real $\mathbb{K} = \mathbb{Q}(w)$, onde $w = \zeta_8 + \zeta_8^{-1}$ A ordem $\mathcal{M}$ caracterizada pela base

$$B = \left\{1, \frac{1+i}{w}, \frac{1+j}{w}, \frac{1+i+j+k}{2}\right\} \tag{4}$$

é uma ordem maximal em $\mathcal{A}$. De fato, pelas Proposições 3.1 e 3.2,

$$Trd(v_i), Nrd(v_i) \in \mathbb{O}_{\mathbb{K}} = \mathbb{Z}[w] \text{ and } \mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}),$$

para todo $v_i \in B$, $i = 1, \cdots, 4$. De acordo com a Proposição 4.1, para que a condição (2) seja satisfeita para $\Lambda' = E_8$, precisamos encontrar $\alpha \in \mathbb{K}$ totalmente positivo e $\mathcal{I} \subseteq \mathcal{M}$ um ideal a direita tal que

$$c^8 = 2^{12} N(\alpha)^4 N(Nrd(\mathcal{I}))^4, \tag{5}$$

pois $det(E_8) = 1$, $\mathcal{D}(\mathcal{M}) = 1$ and $d_{\mathbb{K}} = 2^3$. Considerando o ideal $\mathcal{I} = \mathcal{M}$, e o elemento totalmente positivo $\alpha = 2 - (\zeta_8 + \zeta_8^{-1})$ em $\mathbb{K}$ então $\Lambda = (\mathcal{I}, 2 - w)$ é um ideal reticulado com base B' dada por

$$B' = \left\{1, w, \frac{1+i}{w}, 1+i, \frac{1+j}{w}, \frac{1+i+j+k}{2}, \frac{1+i+j+k}{w}\right\},$$

DOI: 10.5540/03.2017.005.01.0237

que satisfaz (6), para $c = 4$. Além disso, a matriz de Gram de $\Lambda = (\mathcal{I}, 2 - w)$ é dada por $G = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i\overline{w_j}))$ onde $w_i, w_j \in B'$. Aplicando o algoritmo LLL [4] em G, obtemos a matriz $G^{'}$:

$$G = \begin{pmatrix} 8 & 8 & 4 & 8 & 4 & 8 & 4 & 4 \\ 8 & 16 & 8 & 8 & 8 & 8 & 4 & 8 \\ 4 & 8 & 8 & 8 & 4 & 4 & 4 & 8 \\ 8 & 8 & 8 & 16 & 4 & 8 & 8 & 8 \\ 4 & 8 & 4 & 4 & 8 & 8 & 4 & 8 \\ 8 & 8 & 4 & 8 & 8 & 16 & 8 & 8 \\ 4 & 4 & 4 & 8 & 4 & 8 & 8 & 8 \\ 4 & 8 & 8 & 8 & 8 & 8 & 8 & 16 \end{pmatrix} \quad G' = \begin{pmatrix} 2 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & -1 & 1 & -1 & 0 & 1 \\ 1 & 1 & 2 & 0 & 1 & 0 & 1 & 1 \\ 1 & -1 & 0 & 2 & 0 & 1 & 1 & -1 \\ 1 & 1 & 1 & 0 & 2 & 0 & 1 & 1 \\ 1 & -1 & 0 & 1 & 0 & 2 & 1 & -1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & -1 & 1 & -1 & 0 & 2 \end{pmatrix}.$$

Verificamos que $G^{'}$ uma matriz de Gram do reticulado E_8 pois E_8 é o único reticulado unimodular de dimensão 8 e par. Portanto, $\Lambda = (\mathcal{I}, 2 - w)$ é um reticulado ideal isomorfo a E_8.

Como $\{1, w\}$ é a $\mathbb{Z}$-base de $\mathbb{O}_{\mathbb{K}} = \mathbb{Z}[w]$ então

$$M_1 = \begin{pmatrix} \sqrt{2\sigma_1(2-w)}\sigma_1(1) & \sqrt{2\sigma_2(2-w)}\sigma_2(1) \\ \sqrt{2\sigma_1(2-w)}\sigma_1(w) & \sqrt{2\sigma_2(2-w)}\sigma_2(w) \end{pmatrix}.$$

Portanto, expandindo M_1 em uma matriz 8×8 obtemos a matriz ϕ_1 como em (3).

Agora, considerando a matriz φ cujas linhas são os coeficientes da base dada em (4) e aplicando os mergulhos $\sigma_1(a + bw) = a + bw$ e $\sigma_2(a + bw) = a - bw$, $a, b \in \mathbb{Q}(w)$, nos elementos of φ, obtemos a matriz ϕ_2 8×8 :

$$\varphi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{1}{w} & \frac{1}{w} & 0 & 0 \\ \frac{1}{w} & 0 & \frac{1}{w} & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \qquad \phi_2 = \begin{pmatrix} \sigma_1(\varphi_{ij}) & 0 \\ 0 & \sigma_2(\varphi_{ij}) \end{pmatrix}, \quad i, j = 1, \cdots, 4.$$

Portanto $M = \phi_1\phi_2$ é uma matriz geradora do reticulado ideal Λ. Além disso, usando M obtemos a matriz de Gram $G^{'}$ e portanto Λ é isomorfo a E_8.

5.2 Construção de Λ_{24}

Para construir o reticulado de Leech Λ_{24} consideramos $\mathcal{A} = (-1, -1)_{\mathbb{K}}$, $\mathbb{K} = \mathbb{Q}(w)$, onde $w = \zeta_{13} + \zeta_{13}^{-1}$.

De acordo com a Proposição 4.1, para que a condição (2) seja satisfeita para $\Lambda' = \Lambda_{24}$, precisamos encontrar $\alpha \in \mathbb{K}$ totalmente positivo e $\mathcal{I} \subseteq \mathcal{M}$ um ideal a direita tal que

$$c^{24} = (13^5)^4 N(\alpha)^4 N_{\mathbb{K}}(Nrd(\mathcal{I}))^4, \tag{6}$$

pois $det(\Lambda_{24}) = 1$, $\mathcal{D}(\mathcal{M}) = 1$ and $d_{\mathbb{K}} = 13^5$. Se tomarmos o ideal $\mathcal{I} = \mathbb{O}_{\mathbb{K}} < 2 - w, (2 - w)i, [(w^4 + w^3 + 2) + (w^4 + w^3 + 7)i + j]/2, [(w^4 + w^3 + 7) + (w^4 + w^3 + 2)i + k]/2 >$, $c = 13^2$ e

DOI: 10.5540/03.2017.005.01.0237

o elemento totalmente positivo $\alpha = \left(2 - (\zeta_{13} + \zeta_{13}^{-1})\right)^6$ em $\mathbb{K}$ então usando o software *Sage* verificamos através da matriz de Gram do reticulado ideal $\Lambda = (\mathcal{I}, (2-w)^6)$ que Λ possui norma mínima 4 e além disso, Λ é par e unimodular. Como a menos de isomorfismo, Λ_{24} é o único reticulado de dimensão 24 com tais características, concluímos portanto que Λ isomorfo a Λ_{24}.

6 Conclusões

Neste trabalho, apresentamos um método de construir reticulados ideais via ordens maximais das álgebras dos quatérnios sobre corpos de números totalmente reais e focamos na construção de versões rotacionadas dos reticulados unimodulares E_8 e Λ_{24}, que são os mais densos em suas dimensões. Usando corpos de números totalmente reais, reticulados $\mathbb{Z}^n$-rotacionados foram construídos em [2] para a transmissão sobre canais com desvanecimento do tipo Rayleigh. Através da construção que propomos aqui, usando a álgebra dos quatérnios, é possível construir reticulados em dimensões $4n$ e que podem ser usados em canais com múltiplas antenas transmissoras e receptoras, os quais são muito usados recentemente devido à necessidade de altas taxas de transmissão.

Agradecimentos

Esta pesquisa é financiada pelo PNPD/CAPES, CNPq processos 151318/ 2014-0, 312926/ 2013-8 e FAPESP 2013/25977-7.

Referências

[1] S. M. Alamouti, A simple transmit diversity technique for wireless communication, *IEEE J. on Select. Areas in Commun.*, 16:1451-1458, 1998.

[2] E. Bayer-Fluckiger, F. Oggier and E. Viterbo, New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel, *Trans. Inf. Theory,* 50(4):702-714, 2004.

[3] C. Maclachlan and A. W. Reid. *The arithmetic of hyperbolic 3-manifolds*. Springer-Verlag, New York, 2003.

[4] P. Q. Nguyen and B. Vallée. *The LLL Algorithm: Survey and Applications*. Springer-Verlag, Berlin Heidelberg, 2010.

[5] I. Reiner. *Maximal Orders*. Academic Press, London, 1975.

[6] F.-T. Tu and Y. Yang, Lattice packing from quaternion algebras, *RIMS K$\hat{o}$ky$\hat{u}$roku Bessatsu*, 229-237, 2012.

[7] R. Vehkalahti, C. Hollanti, J. Lahtonen and K. Ranto, On the Densest MIMO Lattices from Cyclic Division Algebras, *IEEE Trans. Inform. Theory,* 55(8):3751-3780, 2009.

DOI: 10.5540/03.2017.005.01.0237