Reticulados associados a álgebra dos octônios

Nelson G. Brasil Jr, Cintya W. O. Benedito, Sueli I. R. Costa

***Resumo*— Neste trabalho, propomos uma construção de reticulados em dimensões $8n$ a partir de ordens em álgebras dos octônios definidas sobre um corpo de números totalmente real. Através de tal construção, apresentamos versões rotacionadas dos reticulados E_8 e Λ_{16}, que são os reticulados mais densos nas dimensões 8 e 16, respectivamente.**

***Palavras-Chave*— Reticulado Ideal, Teoria dos Números Algébricos, Álgebras de Divisão, Álgebra dos Octônios**

***Abstract*— In this paper, we propose a construction of lattices in dimension $8n$ via orders in an octonion algebra over a totally real number field. Using this construction, we present rotated versions of E_8 and Λ_{16} lattices that are the densest lattices in dimension 8 and 16, respectively.**

***Keywords*— Ideal Lattices, Algebraic Number Theory, Division Algebra, Octonion Algebra**

I. Introdução

Um *reticulado* Λ é um subgrupo aditivo discreto do espaço $\mathbb{R}^n$ gerado pela combinação linear inteira de n vetores linearmente independentes $v_1, \cdots, v_n \in \mathbb{R}^n$.

Constelações de sinais tendo a estrutura de reticulado tem sido estudados como ferramentas significativas para transmissão de dados via canais Gaussianos e canais com uma antena com desvanecimento do tipo Rayleigh [1]. O problema de encontrar uma boa constelação de sinais para canais gaussianos é associado à busca por reticulados com boa densidade de empacotamento [9]. Em um reticulado, a *densidade de empacotamento* é a proporção do espaço $\mathbb{R}^n$ coberto por esferas de maior raio possível, centradas em pontos de Λ e que não se tocam. Os reticulados mais densos são apenas determinados em dimensões 1 a 8 [9] e 24 [2].

Na busca por reticulados que podem ser base para a obtenção de códigos para os canais gaussiano e do tipo Rayleigh, tem sido estudados os chamados reticulados algébricos rotacionados. Em [1], foram construídos versões rotacionadas dos reticulados D_4, K_{12} e Λ_{16} via ideais de $\mathbb{Q}(\zeta_n)$, para $n = 8, 21$ e 40, respectivamente, e em [3], [4] versões rotacionadas da família A_{p-1}, onde p é um número primo ímpar, D_4, E_6, E_8, K_{12}, Λ_{24} e os reticulados de Craig $A_p^{(k)}$ são apresentados.

Existem diversas maneiras de se construir reticulados algebricamente e também geometricamente. As construções algébricas possibilitam o cálculo de invariantes tais como densidade e distância produto mínima, que são importantes nas aplicações em códigos corretores de erros e em esquemas criptográficos baseados em reticulados. A construção utilizando ideais em corpos de números dão origem aos chamados reticulados ideais [13] ou reticulados do tipo traço [18], os quais são obtidos por uma construção traço escalonada.

Assim como vem sendo obtidos reticulados ideais via corpos de números [13], podemos também construir reticulados ideais através de álgebras de divisão. Em [11], foram construídos reticulados ideais, em dimensões múltiplas de 4, via uma ordem maximal em uma álgebra dos quatérnios definida sobre um corpo de números totalmente real. Neste caso, o traço reduzido, $Trd(\,.\,)$, definido sobre os elementos da álgebra dos quatérnios nos fornece uma forma bilinear simétrica, e portanto, utilizando tal função e um ideal em uma ordem maximal dos quatérnios podemos obter reticulados por uma construção traço escalonada, ou seja, um reticulado ideal. A estrutura quaterniônica vem sendo usada na proposta STBC (*space-time block code*) desde a introdução dos códigos de Alamouti para duas antenas transmissoras [5].

Baseados na construção usando álgebra dos quatérnios, propomos neste trabalho uma construção de reticulados ideais via uma ordem (ou uma ordem maximal) em uma álgebra dos octônios definida sobre um corpo de números totalmente real. Utilizando a construção proposta podemos obter reticulados ideais em dimensões $8n$. Para exemplificar, fixando $n = 1$ e $n = 2$, obtemos versões rotacionadas dos reticulados E_8 e Λ_{16} que são os reticulados mais densos nas dimensões 8 e 16, respectivamente.

Este trabalho é organizado como segue. Na Seção II fazemos uma pequena revisão dos conceitos básicos de reticulados. Na Seção III, apresentamos algumas definições e resultados sobre álgebra dos octônios. Na Seção IV, propomos uma construção de reticulados ideais via álgebra dos octônios sobre corpos de números totalmente reais e caracterizamos a matriz de Gram de tais reticulados. Na Seção V, construções de versões rotacionadas dos reticulados E_8 e Λ_{16} são apresentadas. Finalmente, na Seção V, apresentamos nossa conclusão.

II. Reticulados

Um **reticulado com posto completo** Λ é um subgrupo aditivo discreto do $\mathbb{R}^n$gerado pela combinação linear inteira de n vetores linearmente independentes $v_1, \cdots, v_n \in \mathbb{R}^n$. O conjunto $\{v_1, \cdots, v_n\}$ é chamado então de uma **basis** para Λ. A matriz M cujas linhas são os vetores da base de Λ é chamada de uma **matriz geradora** para Λ e $G = MM^\top$ é a **matriz de Gram** de Λ. Além disso, o **determinante** de Λ é dado por $\det(\Lambda) = \det(G)$.

A **densidade de empacotamento**, $\Delta(\Lambda)$, de um reticulado Λ é a proporção do espaço $\mathbb{R}^n$ coberto pela união de esferas congruentes e disjuntas com maior raio possível e centrada em pontos de Λ.

Agora, seja $\mathbb{K}$ um corpo de números algébricos totalmente real, de grau n and let $\mathfrak{o}_\mathbb{K}$ o seu anel de inteiros. Então, existem exatamente n mergulhos reais $\sigma_i : \mathbb{K} \to \mathbb{R}$, para $i = 1, \ldots, n$.

Instituto de Matemática Estatística e Computação Científica, Unicamp, Campinas-SP, Universidade Estadual Paulista, Unesp – São João da Boa Vista-SP, Brasil, E-mails: nelson.gbrasil@gmail.com, cintya.benedito@sjbv.unesp.br, sueli@ime.unicamp.br. Este trabalho foi parcialmente financiado pelo CNPq 312926/2013-8 e CAPES.

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 de *norma* e *traço* de x em $\mathbb{K}/\mathbb{Q}$, respectivamente. Se $\{w_1, \cdots, w_n\}$ é uma $\mathbb{Z}$-base de $\mathfrak{o}_{\mathbb{K}}$, 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 $\mathfrak{o}_{\mathbb{K}}$ 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 (i.e., $\sigma_i(\alpha) > 0 \, \forall i$). O *posto* 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 um *homomorfismo torcido*. Quando $\alpha = 1$, o homomorfismo torcido é exatamente o *homomorfismo canônico*.

Pode ser mostrado que, se $\mathcal{I} \subseteq \mathfrak{o}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo 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 de $\Lambda = \sigma_\alpha(\mathcal{I})$ é

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

O determinante de Λ é um invariante sobre a mudanças de base [9]. No caso de reticulados ideais, o determinante de Λ está relacionado ao valor $d_{\mathbb{K}}$.

Proposição II.1. *[13] Se $\mathcal{I} \subseteq \mathfrak{o}_{\mathbb{K}}$ é um ideal fracionário, então*

$$\det(\sigma_\alpha(\mathcal{I})) = |d_{\mathbb{K}}| N(\mathcal{I})^2 N_{\mathbb{K}/\mathbb{Q}}(\alpha),$$

onde $N(\mathcal{I}) = |\mathfrak{o}_{\mathbb{K}}/\mathcal{I}|$ é a norma do ideal $\mathcal{I}$.

III. Álgebra dos Octônios

Nesta seção definimos alguns conceitos sobre a álgebra dos octônios e apresentaremos alguns resultados que serão fundamentais para o desenvolvimento deste trabalho. A idéia é definir estruturas integrais para estas álgebras e, posteriormente, definir reticulados ideais via tais álgebras. Iniciamos com a definição mais geral de uma álgebra dos octônios.

Definição III.1. *Seja a, b, $c \in \mathbb{K}$, diferentes de zero e seja $\mathcal{C}$ um espaço vetorial de dimensão 8 sobre um corpo de números totalmente real $\mathbb{K}$ com base $\{e_0, \ldots, e_7\}$ e uma multiplicação bilinear definida de tal forma que $e_0 = 1$ é o elemento identidade e $e_1^2 = a$, $e_2^2 = b$ e $e_4^2 = c$.*

A adição de dois octônios é feita da maneira usual. Além disso, a multiplicação entre os elementos da álgebra é dada em termos dos elementos da base, da seguinte tabela:

$\cdot$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	a	$-e_4$	ae_7	e_2	ae_6	e_5	$-ae_3$
e_2	e_2	e_4	b	$-be_5$	$-e_1$	e_3	be_7	$-be_6$
e_3	e_3	$-ae_7$	be_5	ab	$-e_6$	ae_2	$-be_4$	abe_1
e_4	e_4	$-e_2$	e_1	e_6	c	ce_7	ce_3	$-ce_5$
e_5	e_5	$-ae_6$	$-e_3$	$-ae_2$	$-ce_7$	ac	ce_1	ace_4
e_6	e_6	$-e_5$	$-be_7$	be_4	$-ce_3$	$-ce_1$	bc	bce_2
e_7	e_7	ae_3	be_6	$-abe_1$	ce_5	$-ace_4$	$-bce_2$	abc

Uma álgebra $\mathcal{C}$ com estes parâmetros será denotada por $\mathcal{C} = (a, b, c)_{\mathbb{K}}$.

Note que, escolhendo $\mathbb{K} = \mathbb{Q}$ e $a = b = c = 1$, obtemos os chamados inteiros de Cayley, que é a álgebra dos octônios mais conhecida.

Agora, seja $x \in \mathcal{C}$, $x = x_0 + \sum_{i=1}^{7} x_i e_i$. Definimos o *conjugado* de x como sendo $\overline{x} = x_0 - \sum_{i=1}^{7} x_i e_i$. Além disso, podemos definir a *norma reduzida* de x por $N(x) = x\,\overline{x}$ e o *traço reduzido* de x por $Trd(x) = x + \overline{x}$.

Em particular, temos $N(x) \in \mathbb{K}$ e $N(x) = N(\overline{x}) = \overline{x}\,x$.

Teorema III.2. *[7] A álgebra $\mathcal{C}$ da Definição III.1 é uma álgebra de divisão.*

Agora dada uma álgebra dos octônios, podemos obter uma outra base para esta álgebra usando o resultado a seguir.

Proposição III.3. *[15] Para uma álgebra dos octônios $\mathcal{C} = (a, b, c)_{\mathbb{K}}$ sobre um corpo de números $\mathbb{K}$, com característica diferente de 2, existem elementos x, y, $z \in \mathcal{C}$ com norma não nula tais que*

$$\mathfrak{B} = \{1,\, x,\, y,\, xy,\, z,\, xy,\, yz,\, (xy)z\} \tag{1}$$

forma uma base para $\mathcal{C}$, e esta base é ortogonal com relação ao produto interno

$$\langle u,\, v\rangle = N(u + v) - N(u) - N(v).$$

Para definir uma estrutura integral nas álgebras dos octônios, observamos que os resultados apresentados em [8], [11], [14], que são válidos para as álgebras dos quatérnios, ainda são válidos para as álgebras dos octônios. Vamos reproduzir a seguir tais resultados, considerando $R = \mathfrak{o}_{\mathbb{K}}$, ou um domínio de Dedekind.

Definição III.4. *[15] Seja $\mathcal{C}$ uma $\mathbb{K}$-álgebra. Uma R-**ordem** $\mathcal{O}$ em $\mathcal{C}$ sobre R é um módulo finitamente gerado sobre R de modo que $\mathcal{C} = \mathbb{K} \cdot \mathcal{O}$.*

Proposição III.5. *[17] Seja $\mathcal{C}$ uma álgebra dos octônios e $\mathcal{O} \subseteq \mathcal{C}$. Se $\mathcal{O}$ é uma ordem, então todo elemento $x \in \mathcal{O}$ é inteiro sobre R, ou seja, se $Trd(x)$, $N(x) \in R$.*

Definição III.6. *[17] Seja R um anel com corpo de frações $\mathbb{K}$. Uma **ordem maximal** dos octônios, denotada por $\mathcal{M}$ contida em uma álgebra dos octônios $\mathcal{C}$ é uma R-ordem que não está propriamente contida em nenhuma outra ordem.*

Teorema III.7. *[15] Toda R-ordem em uma álgebra dos octônios $\mathcal{C}$ está contida em uma R-ordem maximal de $\mathcal{C}$.*

IV. Reticulados a partir de Ordens dos Octônios

Assim como foi proposto para álgebra dos quatérnios em [11] podemos, utilizando álgebra dos octônios, construir um reticulado a partir de uma ordem e de uma forma bilinear da seguinte forma.

Seja $\mathbb{K}$ um corpo de números totalmente real de grau n e $\mathcal{C}$ uma álgebra dos octônios definida sobre $\mathbb{K}$. Se $\mathcal{O}$ é uma ordem de $\mathcal{C}$ e α um elemento totalmente positivo em $\mathbb{K}$, então existe uma forma quadrática totalmente positiva $Q_\alpha : \mathcal{O} \times \mathcal{O} \to \mathbb{Q}$ dada por $Q_\alpha(x, y) = tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(x\overline{y}))$.

Além disso, $\Lambda = (\mathcal{I}, \alpha)$ é o reticulado ideal associado à forma quadrática Q_α.

Considerando $\mathcal{I} = \mathcal{O}$, a ordem de $\mathcal{A}$ com base $\mathfrak{B} = \{v_1, \ldots, v_8\}$ e, supondo que $[\mathbb{K} : \mathbb{Q}] = n$ e $\mathfrak{o}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$ com $\mathbb{Z}$-base $\{u_1, \ldots, u_n\}$, então o reticulado Λ tem posto $8n$ e base

$$\mathfrak{B}' = \{v_i u_j\} = \{w_1, \ldots, w_{8n}\}, i = 1, \ldots, 8 \text{ e } j = 1, \ldots, n.$$

Além disso, a matriz de Gram associada ao reticulado Λ é dada por

$$G = tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i \overline{w}_j)), \tag{2}$$

O resultado a seguir nos fornece o determinante da matriz de Gram do reticulado $\Lambda = (\mathcal{I}, \alpha)$. A demonstração deste resultado segue os mesmos passos da demonstração dada em [11] para o caso de uma álgebra dos quatérnios.

Teorema IV.1. *Seja o reticulado ideal $\Lambda = (\mathcal{I}, \alpha)$, com matriz de Gram G como em (2), então o determinante do reticulado pode ser colocado em termos da álgebra como*

$$\det(\Lambda) = d_\mathbb{K}^8 N(\alpha)^8 N_{\mathbb{K}/\mathbb{Q}}(\det(B)) \tag{3}$$

sendo $B = Trd(v_\ell \overline{v_{\ell'}})_{\ell,\ell'=1}^8$.

Demonstração: Seja $\sigma_1, \ldots, \sigma_n$ os n-homomorfismo de $\mathbb{K}$ em $\mathbb{R}$. Os elementos da matriz de Gram do reticulado Λ, $G = (g_{ij})_{i,j=1}^8$ podem ser escritos como

$$g_{ij} = tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i \overline{w}_j)) = tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(v_i u_\ell u_{\ell'} \overline{v_j})),$$

onde $tr(x) = \sum_{i=1}^n \sigma_i(x)$. Assim, podemos expandir o traço no corpo de números como a soma de homomorfismos, como sendo

$$g_{ij} = \sum_{k=1}^n \sigma_k(u_\ell)\sigma_k(\alpha Trd(v_i \overline{v_j}))\sigma_k(u_{\ell'}).$$

A matriz de Gram do reticulado Λ pode ser fatorada no produto de três matrizes,

$$G = M\varphi M^\top,$$

onde

$$M = (I_{8\times 8} \otimes M_1),\ \varphi = \begin{pmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{18} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{28} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{81} & \phi_{82} & \cdots & \phi_{88} \end{pmatrix},$$

e

$$\phi_{ij} = \text{diag}\left(\sigma_k(\alpha Trd(v_i \overline{v}_j), k = 1, \ldots, n\right).$$

O determinante da matriz G é, portanto

$$\det(G) = \left(\sqrt{|d_\mathbb{K}|}\right)^{16} \det\varphi.$$

Para o cálculo do determinante de φ, uma permutação das linhas e colunas desta matriz, de modo a obter blocos da seguinte forma

$$\varphi_\ell = \sigma_\ell\left(\alpha Trd(v_i \overline{v}_j)_{i,j=1}^n\right), \text{ para } \ell = 1, \ldots, n,$$

e assim $\varphi = \text{diag}(\varphi_1, \ldots, \varphi_n)$.

Deste modo, $\det(\varphi) = \prod_{\ell=1}^n \det(\varphi_\ell)$, ou seja

$$\det(\varphi) = \left(N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right)^8 N_{\mathbb{K}/\mathbb{Q}}(\det(B)),$$

com $B = Trd(v_i \overline{v_j})_{i,j=1}^8$.

V. Exemplos

Nesta seção apresentamos exemplos de construções de versões rotacionadas dos reticulados E_8 e Λ_{16} via a álgebra dos octônios

Exemplo V.1. *Para construir um reticulado que é isomorfo ao E_8, vamos tomar o corpo dos racionais e escolher*

$$\begin{aligned} x &= e_1; \\ y &= e_2; \\ z &= (e_1 + e_2 + e_3 + e_4)/2 \end{aligned}$$

e construímos a base como em (1)*, dada por*

$$\begin{aligned} \mathfrak{B} = \Big\{ & 1, e_1, e_2, -e_4, \frac{e_1+e_2+e_3+e_4}{2}, \\ & \frac{-1-e_1+e_4-e_5}{2}, \frac{1-e_1+e_2-e_6}{2}, \\ & \frac{-1+e_2-e_4+e_7}{2} \Big\} \end{aligned} \tag{4}$$

e obtemos, assim um ideal $\mathcal{I}$. Depois, tomando $\alpha = 1$ e aplicando (2) *obtemos a seguinte matriz de Gram*

$$G = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & -1 & -1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 2 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & -1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 & 2 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 & 0 & 2 & 0 & 0 \\ -1 & -1 & 0 & -1 & 0 & 0 & 2 & 0 \\ 1 & -1 & 1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix},$$

que é uma matriz unimodular com diagonal par. Portanto, o reticulado $\Lambda = (\mathcal{I}, \alpha)$ é um reticulado ideal congruente ao reticulado E_8.

Exemplo V.2. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ e considere a álgebra dos octônios $\mathcal{C} = (-1, -1, -1)_\mathbb{K}$ construída sobre o corpo $\mathbb{K}$ com base construída a partir de*

$$x = \frac{1}{\sqrt{2}}(1+e_1), y = \frac{1}{\sqrt{2}}(1+e_2) \text{ e } z = \frac{1}{2}(e_1+e_2+e_3+e_4).$$

A partir da Proposição III.3 obtemos uma ordem com a seguinte base

$$\mathfrak{B} = \{2e, 2x, 2y, 2xy, 2\sqrt{2}z, 2\sqrt{2}xz, 2\sqrt{2}yz, 2\sqrt{2}(xy)z\}.$$

Agora, tomando $\{1, \sqrt{2}\}$, a base para o anel de inteiros $\mathfrak{o}_\mathbb{K}$, construímos um reticulado $\Lambda = (\mathcal{O}, 2+\sqrt{2})$ em dimensão 16. Sua matriz de Gram, após usar o algoritmo LLL [16] é escrita como

$$G_1 = \begin{pmatrix} A_1 & A_2 \\ A_2^\top & A_3 \end{pmatrix},$$

sendo

$$A_1 = \begin{pmatrix} 4 & 0 & 2 & 2 & 2 & 2 & 2 & 0 \\ 0 & 4 & 2 & -2 & 2 & -2 & 0 & 2 \\ 2 & 2 & 4 & 0 & 2 & 0 & 2 & 2 \\ 2 & -2 & 0 & 4 & 0 & 2 & 2 & -2 \\ 2 & 2 & 2 & 0 & 4 & 0 & 2 & 2 \\ 2 & -2 & 0 & 2 & 0 & 4 & 2 & -2 \\ 2 & 0 & 2 & 2 & 2 & 2 & 4 & 0 \\ 0 & 2 & 2 & -2 & 2 & -2 & 0 & 4 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} -2 & -2 & -2 & 0 & -2 & 0 & -1 & -1 \\ -2 & 2 & 0 & -2 & 0 & -2 & -1 & 1 \\ -2 & 0 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & -2 & 0 & 0 & -1 & 1 & 0 & 0 \\ -2 & 0 & -1 & -1 & -2 & -2 & -2 & 0 \\ 0 & -2 & -1 & 1 & -2 & 2 & 0 & -2 \\ -1 & -1 & -2 & 0 & -2 & 0 & -2 & -2 \\ -1 & 1 & 0 & -2 & 0 & -2 & -2 & 2 \end{pmatrix},$$

e

$$A_3 = \begin{pmatrix} 4 & 0 & 2 & 2 & 2 & 2 & 2 & 0 \\ 0 & 4 & 2 & -2 & 2 & -2 & 0 & 2 \\ 2 & 2 & 4 & 0 & 2 & 0 & 1 & 1 \\ 2 & -2 & 0 & 4 & 0 & 2 & 1 & -1 \\ 2 & 2 & 2 & 0 & 4 & 0 & 2 & 2 \\ 2 & -2 & 0 & 2 & 0 & 4 & 2 & -2 \\ 2 & 0 & 1 & 1 & 2 & 2 & 4 & 0 \\ 0 & 2 & 1 & -1 & 2 & -2 & 0 & 4 \end{pmatrix}.$$

A matriz G obtida é a matriz de Gram de um reticulado, tendo $\det(G) = 2^8$

$$\min_{\boldsymbol{v} \in \Lambda} \|\boldsymbol{v}\|^2 = 4,$$

e de modo que G_1 é uma matriz 2*-modular.*

Portanto, o reticulado Λ é um reticulado ideal congruente ao reticulado Barnes-Wall Λ_{16}, uma vez que este é o único reticulado, a menos de congruência, em dimensão 16 *com esta mesma norma e determinante.*

VI. Conclusão

Neste trabalho apresentamos uma construção de reticulados ideias via uma ordem de uma álgebra dos octônios de maneira análoga à apresentada para álgebra dos quatérnios em [11]. A partir desta construção, é possível construir reticulados em dimensões $8n$, $n \geq 1$. Para $n = 1$ e $n = 2$, os reticulados obtidos são versões rotacionadas dos reticulados mais densos conhecidos nas dimensões 8 e 16, respectivamente. Uma perspectiva dos resultados aqui apresentados visando aplicações é a construção de reticulados com boa densidade em dimensões altas, com ganhos significativos nos processos de codificação e decodificação. Uma proposta de continuidade para este trabalho é a obtenção de reticulados para outros valores n, como por exemplo em dimensões 2^r, $r \geq 3$ e comparar os reticulados obtidos com a família de reticulados Barnes-Wall nestas dimensões [9], [12].

Referências

[1] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels", *IEEE Trans. Inform. Theory*, v. 42 (2), pp. 502-517, 2006.

[2] H. Cohn, A. Kumar, "Optimality and uniqueness of the Leech lattice among lattices," *Annals of Mathematics, Princeton,* v. 170, pp. 1003-1050, 2009.

[3] E. Bayer-Fluckiger, "Definite unimodular lattices having an automorphism of given characteristic polynomial," *Comment. Math. Helvetici,* v. 59, pp. 509-538, 1984.

[4] E. Bayer-Fluckiger, I. Suarez, "Ideal lattices over totally real number fields and Euclidean minima," *Arch. Math.,* v. 86 (3), pp. 217-225, 2006.

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

[6] V. Tarokh, N. Seshadri, A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction", *IEEE Trans. Inf. Theory,* v. 44 (2), pp. 744-765, 1998.

[7] J. Baez, *The octonions*, Bulletin of the American Mathematical Society, 39 (2002), pp. 145–205.

[8] C. W. O. Benedito, *Construção de grupos fuchsianos aritméticos provenientes de álgebras dos quatérnios e ordens maximais dos quatérnios associados a reticulados hiperbólicos*, Tese de Doutorado, 2014.

[9] J. H. Conway e N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer, 1988.

[10] I. Stewart e D. O. Tall, *Algebraic number theory*, 1979.

[11] F.-F. Tu, Y. Yang. "Lattice packing from quaternion algebras". *RIM Kôkyûroku Bessatsu*, 229-237.

[12] G. Nebe, E. M. Rains e N. J. A. Sloane. A simple construction for the Barnes-Wall lattices. In *Codes, Graphs, and Systems*, pp. 333-342. (2002)

[13] E. Bayer-Fluckiger, Ideal Lattices, In A panorama of number theory or the view from Baker's garden (Zürich, 1999), *Cambridge Univ. Press, Cambridge*, **241** (2002) 168–184.

[14] J. Voight, *The arithmetic of quaternion algebras*, (2014).

[15] C. Waldner, *Cycles and the cohomology of arithmetic subgroups of the exceptional group G_2*, PhD thesis, uniwien, 2008.

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

[17] F. Van der Blij e T. Springer, *The arithmetics of octaves and of the group G2*, in Indagationes Mathematicae, vol. 62, Elsevier, 1959, pp. 406–418.

[18] B. A. Sethuraman, F. Oggier, "Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields". *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science,* v. 4851, pp. 138-147, 2007.