Lattices from maximal quaternion orders over totally real number fields

Cintya W.O. Benedito, Carina Alves and Sueli I.R. Costa

***Abstract*— In this paper we propose a framework to construct space-time codes over lattices in dimensions $4n$ via ideals from maximal orders of a quaternion algebra whose center is a totally real number field. For $n = 1$ and $n = 2$ it was possible to construct rotated versions of the densest lattices in their dimensions, D_4 and E_8. These constructions provide explicit forms for the generator matrix and other algebraic invariants allowing to analyze meaningful performance parameters for coding such as density, diversity and minimal product distance.**

***Keywords*— Lattices, ideal lattices, quaternion algebras, maximal orders, space-time codes.**

I. Introduction

A *lattice* Λ is a discrete additive subgroup of $\mathbb{R}^n$ generated by integer combinations of n linearly independents vectors $v_1, \cdots, v_n \in \mathbb{R}^n$.

Signal constellations having a lattice structure have been studied as meaningful tools for transmitting data over both Gaussian and single-antenna Rayleigh fading channels [1]. The problem of finding good signal constellations for a Gaussian channel is associated to the search for lattices with high packing density [2].

The *packing density* of a lattice is the proportion of the space $\mathbb{R}^n$ covered by the non-overlapping spheres of maximum radius centered at the points of Λ. The densest possible lattice packing have only be determined in dimensions 1 to 8 [2] and 24 [13].

If we consider the Rayleigh fading channel, a design criterion can be provided by lattices with good minimum product distance and full diversity [1], [4].

A lattice $\Lambda \subseteq \mathbb{R}^n$ has *diversity* $k \leq n$ if k is the maximum number of non-vanishing coordinates of any non-zero vector in Λ. If $div(\Lambda) = n$, the lattice Λ is called *full diversity* and, in this case, we can define the *minimum product distance* of Λ by $d_{p,min}(\Lambda) = min\left\{\prod_{i=1}^{n} |x_i|; x = (x_1, \cdots, x_n) \in \Lambda, x \neq 0\right\}$.

The algebraic number theory has been used as mathematical tool that enables the design of good coding schemes for such channels.

For example, it has been shown that algebraic lattices, i.e., lattices constructed via the canonical embedding of an algebraic number field, provide an efficient tool for designing lattice codes for transmission over the single-antenna Rayleigh fading channel [4]. The reason is that the two main design parameters, namely the modulation diversity and the minimum product distance, can be related to properties of the underlying number field: the maximal diversity is guaranteed when using totally real number fields and the minimum product distance can be related to the field discriminant [1].

In the search for lattices which can be the support for design codes for both Gaussian and Rayleigh channels, algebraic rotated lattices can be studied. In [1] was constructed rotated versions of lattices D_4, K_{12} and Λ_{16} via ideals of $\mathbb{Q}(\zeta_n)$, for $n = 8, 21$ and 40, respectively, and in [14] and [5] rotated versions of lattices A_{p-1}, where p is an odd prime number, D_4, E_6, E_8, K_{12}, Λ_{24} and Craig's lattices $A_p^{(k)}$ is presented.

Quaternion structure has been used to propose STBC (*space-time block code*) since the introduction of Alamouti code for two transmit antennas [15]. From probability point of view [6], designing a space-time block code requires the maximization of two parameters: *diversity gain* and *coding gain*. In the context of lattice, maximizing the coding gain is equivalent to maximizing the density of the corresponding lattice. Maximal orders have been proposed in the context of space-time block codes in [7] and complex codes constructions based on cyclic division algebras are proposed in [16]. More recently, the E_8-lattice was constructed using quaternion algebras over an imaginary quadratic field [3]. Codewords are usually (in narrow band systems) built over the complex field. However for ultra wideband communication, one needs to design them over the real field [18]. Thus, having the construction of rotated lattices as our goal, we are interested in constructing dense lattices from maximal orders of the division algebras over a totally real number field. To do this construction we use the ideal lattice theory.

This paper is organized as follows. In Section II we collect some result on ideal lattices, the Section III is devoted to recall definitions and some properties of quaternion algebras and quaternion orders. In Section IV a method to construct lattices from maximal quaternion orders over totally real number fields is presented. Finally, in Section V we describe constructions of rotated versions of D_4-lattice and E_8-lattice.

II. Ideal Lattices

The theory of ideal lattices gives a general framework for algebraic lattice constructions. We present this notion in the case of totally real algebraic number fields.

Let $\mathbb{K}$ be a totally real algebraic number field of degree n and let $\mathbb{O}_{\mathbb{K}}$ be its ring of integers. There are exactly n real embeddings $\sigma_i : \mathbb{K} \to \mathbb{R}$, for $i =, \cdots, n$.

Cintya W de O. Benedito and Sueli I.R. Costa, Institute of Mathematics, University of Campinas, Campinas-SP, Brazil, E-mails: cwinktc@hotmail.com, sueli@ime.unicamp.br.

Carina Alves, Department of Mathematics, Sao Paulo State University, UNESP/Rio Claro-SP, Brazil, E-mail: carina@rc.unesp.br

Acknowledgements: To CNPQ 151318/2014-0, 312926/2013-8 and FAPESP 2013/25977-7 for financial support.

Given $x \in \mathbb{K}$, the values $N_{\mathbb{K}/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ and $Tr_{\mathbb{K}/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ are called *norm* and *trace* of x in $\mathbb{K}/\mathbb{Q}$, respectively. If $\{w_1, \cdots, w_n\}$ is a $\mathbb{Z}$-basis of $\mathbb{O}_{\mathbb{K}}$, the *discriminant* of $\mathbb{K}$ is $d_{\mathbb{K}} = \left(\det(\sigma_j(w_i))_{i,j=1}^{n}\right)^2$.

An *ideal lattice* is a lattice $\Lambda = (\mathcal{I}, q_\alpha)$, where $\mathcal{I}$ is an ideal of $\mathbb{O}_{\mathbb{K}}$ and $q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}$ is such that

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

where $\alpha \in \mathbb{K}$ is totally positive (i.e., $\sigma_i(\alpha) > 0 \, \forall i$). The *rank* of an ideal lattice is the degree n of the number field $\mathbb{K}$.

Let $\alpha \in \mathbb{K}$ such that $\alpha_i = \sigma_i(\alpha) > 0$ for all $i = 1, \cdots, n$. The embedding $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ where

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

is called a *twisted embedding*. When $\alpha = 1$, the twisted embedding is the *canonical embedding*.

It can be shown that if $\mathcal{I} \subseteq \mathbb{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1, \cdots, w_n\}$, then the image $\Lambda = \sigma_\alpha(\mathcal{I})$ is a lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(w_1), \cdots, \sigma_\alpha(w_n)\}$. Moreover, since $\mathbb{K}$ is totally real, the associated Gram matrix of $\Lambda = \sigma_\alpha(\mathcal{I})$ is

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

The determinant of Λ is $det\Lambda = detG$ and it is an invariant under change of basis [2]. In the case of ideal lattices, the determinant of Λ is related to $d_{\mathbb{K}}$.

Proposition 2.1: [9] If $\mathcal{I} \subseteq \mathbb{O}_{\mathbb{K}}$ is a fractional ideal, then

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

where $N(\mathcal{I}) = |\mathbb{O}_{\mathbb{K}}/\mathcal{I}|$ is the norm of the ideal $\mathcal{I}$.

III. Quaternion Algebra and Quaternion Order

A *quaternion algebra* $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ over a field $\mathbb{K}$ is a central simple algebra of dimension 4 with basis $\{1, i, j, k\}$ satisfying $i^2 = \alpha$, $j^2 = \beta$ and $k = ij = -ji$, where $\alpha, \beta \in \mathbb{K}/\{0\}$.

Example 3.1: The standard example of quaternion algebra over real number field is the Hamilton's quaternions $\mathcal{H} = (-1, -1)_{\mathbb{R}}$.

If $x \in \mathcal{A}$, let us say $x = x_1 + x_2 i + x_3 j + x_4 k$, with $x_1, x_2, x_3, x_4 \in \mathbb{K}$. Then $\overline{x} = x_1 - x_2 i - x_3 j - x_4 k$ is called *conjugated* of x. For $x \in \mathcal{A}$, the *reduced trace* and *reduced norm* of x are defined as

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

respectively.

A quaternion algebra $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ is a division algebra if and only if $\forall x \in \mathcal{A} \setminus \{0\}$, $Nrd(x) \neq 0$, and $\mathcal{A}$ is definite if and only if the quadratic form $Trd(x\overline{y})$ on $\mathcal{A}$ is positive definite, for all $x, y \in \mathcal{A}$.

Let R be a ring with field of fractions $\mathbb{K}$, and let $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ be a quaternion algebra over $\mathbb{K}$. An *order* $\mathcal{O}$ in $\mathcal{A}$ is a subring of $\mathcal{A}$ containing 1, equivalently, it is a finitely generated R-module such that $\mathcal{A} = \mathbb{K}\mathcal{O}$. Hence, considering R as a ring of $\mathbb{K}$ and the algebra $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$, with $\alpha, \beta \in R$, then $\mathcal{O} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in R\}$, is an order in $\mathcal{A}$ denoted by $\mathcal{O} = (\alpha, \beta)_R$.

If $\mathcal{I}$ is an ideal in a quaternion algebra $\mathcal{A}$ and $\mathcal{O}$ is an order of $\mathcal{A}$, we say that $\mathcal{I}$ is a *left ideal* of $\mathcal{O}$ if $\mathcal{O}\mathcal{I} \subset \mathcal{I}$ and $\mathcal{I}$ is a *right ideal* of $\mathcal{O}$ if $\mathcal{I}\mathcal{O} \subset \mathcal{I}$. The reduced norm of $\mathcal{I}$, denoted by $Nrd(\mathcal{I})$, is the R-fractional ideal generated by $\{Nrd(x) : x \in \mathcal{I}\}$.

Proposition 3.1: [12] Let $\mathcal{O}$ be an R-quaternion order in a quaternion algebra $\mathcal{A}$. If $x \in \mathcal{O}$, then $Trd(x), Nrd(x) \in R$.

Let $\mathcal{O}$ be an R-order in a quaternion algebra $\mathcal{A}$. The *reduced discriminant of* $\mathcal{O}$, $\mathcal{D}(\mathcal{O})$, is an ideal generated by $\{\{x_1, x_2, x_3\} : x_1, x_2, x_3 \in \mathcal{O}\}$, where

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

An order $\mathcal{M}$ in a quaternion algebra $\mathcal{A}$ is *maximal* if $\mathcal{M}$ is not properly contained in another order of $\mathcal{A}$.

Lemma 3.1: [12] Every order is contained in a maximal order.

It was shown in [8] that in order to maximize the number of codewords in the available signal space, one should look for cyclic division algebras having maximal orders with minimal discriminants.

Proposition 3.2: [11] If $\mathcal{M}$ is a maximal order in $\mathcal{A}$ containing another order $\mathcal{O}$, then the discriminant satisfies

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

Conversely, if $\mathcal{D}(\mathcal{O}) = \mathcal{D}(\mathcal{A})$, then $\mathcal{O}$ is a maximal order in $\mathcal{A}$.

IV. Lattices from Maximal Quaternion Orders

In this section we propose an algebraic construction of lattices of dimension $4n$ via maximal orders of quaternion algebras, identifying their Gram and generator matrix. We can define ideal lattices from maximal quaternion orders in the same way that we define ideal lattices from number fields.

Let $\mathbb{K}$ be a totally real number field with degree n and $\mathcal{A}$ be a definite quaternion algebra over $\mathbb{K}$. If $\mathcal{I}$ is an ideal in $\mathcal{A}$ and α is a totally positive element in $\mathbb{K}$, then we have a positive definite quadratic form $Q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Q}$ given by $Q_\alpha(x, y) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(x\overline{y}))$.

In this case, we let $\Lambda = (\mathcal{I}, \alpha)$ denote the lattice associated to the quadratic form Q_α. Notice that, if the number field $\mathbb{K}$ over $\mathbb{Q}$ is of degree n then the lattice has rank $4n$, $n \geq 1$.

Let $\mathcal{M}$ be a maximal quaternion order of $\mathcal{A}$ with basis $B = \{y_1, y_2, y_3, y_4\}$. If $[\mathbb{K} : \mathbb{Q}] = n$ and $\mathbb{O}_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$ then $\{u_1, \cdots, u_n\}$ is a $\mathbb{Z}$-basis of $\mathbb{O}_{\mathbb{K}}$. Considering $\mathcal{I} = \mathcal{M}$ ideal of $\mathcal{A}$ with basis B and α an totally real and totally positive element of $\mathbb{K}$ then $\Lambda = (\mathcal{I}, \alpha)$ is an ideal lattice of rank $4n$ with basis

$$B' = \{y_i x_j\} = \{w_1, \cdots, w_{4n}\},\ i = 1, \cdots, 4 \text{ and } j = 1, \cdots, n.$$

Moreover, since $\mathbb{K}$ is a totally real number field, the associated Gram matrix of $\Lambda = (\mathcal{I}, \alpha)$ is

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

where $w_i, w_j \in B'$. In the same way, the determinant of Λ is $det\Lambda = detG$.

Proposition 4.1: [10] Let $\mathbb{K}$ be a totally real number field and $\mathcal{A}$ be a definite quaternion algebra over $\mathbb{K}$. If $\mathcal{I} \subseteq \mathcal{M}$ is an ideal of a maximal quaternion order $\mathcal{M}$ of $\mathcal{A}$ and α is a totally positive element in $\mathbb{K}$ so that $\Lambda = (\mathcal{I}, \alpha)$ is a lattice, then

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

where G is the Gram matrix of Λ.

A necessary but not sufficient condition for Λ to be a rotated version of a lattice Λ' with scale $c \in \mathbb{Z}$, $(\sqrt{c}\Lambda')^n$, is that

$$det(\Lambda) = c^n det(\Lambda'), \qquad (2)$$

since the Gram matrix of $(\sqrt{c}\Lambda')^n$ is cM, where M is the generator matrix of Λ'.

Using the Equations (1) and (2) we can construct rotated version of a known densest lattice with Gram matrix G. The construction proposed here, differently from [10], allows also an explicit form for a generator matrix. We remark that, in order to analyze the density it may be enough to know the lattice Gram matrix, but to analyze parameters such as diversity and the minimum product distance is also necessary to know a generator matrix of the lattice.

If we consider $\{u_1, \cdots, u_n\}$ the $\mathbb{Z}$-basis of $\mathbb{O}_{\mathbb{K}}$ then the generator matrix to the lattice $\sigma_{2\alpha}(\mathbb{O}_{\mathbb{K}})$ obtained by a twisted embedding is

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

Hence, expanding M_1 into a $4n \times 4n$ matrix we have the following matrix:

$$\phi_1 = \begin{pmatrix} M_1 & 0 & 0 & 0 \\ 0 & M_1 & 0 & 0 \\ 0 & 0 & M_1 & 0 \\ 0 & 0 & 0 & M_1 \end{pmatrix}. \qquad (3)$$

Now we consider the matrix whose rows are the coefficients of $B = \{y_1, y_2, y_3, y_4\}$ (basis of $\mathcal{I} = \mathcal{M}$), where $y_s = y_{s1} + y_{s2}i + y_{s3}j + y_{s4}k$, for $s = 1, \cdots, 4$, i.e,

$$\varphi = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} y_{11} & y_{12} & y_{13} & y_{14} \\ y_{21} & y_{22} & y_{23} & y_{24} \\ y_{31} & y_{32} & y_{33} & y_{34} \\ y_{41} & y_{42} & y_{43} & y_{44} \end{pmatrix}.$$

Applying the n embeddings of $\mathbb{K}$ in $\mathbb{R}$, $\sigma_1, \cdots, \sigma_n$, in the elements of φ we obtain the following $4n \times 4n$ matrix:

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

with $i, j = 1, \cdots, 4$ and $k = 1, \cdots, n$. Hence, a generator matrix to ideal lattice $\Lambda = (\mathcal{I}, \alpha)$ is given by

$$M = \phi_1 \phi_2. \qquad (4)$$

Moreover, we can define through $\mathcal{M}$ a $\mathbb{Z}$-basis $\{\sigma_{2\alpha}(w_1), \cdots, \sigma_{2\alpha}(w_{4n})\}$ of ideal lattice $\Lambda = (\mathcal{I}, \alpha)$, where

$$\begin{aligned} \sigma_{2\alpha}(w_i) &= \sigma_{2\alpha}(u_n y_s) \\ &= \Big(\sqrt{2\sigma_1(\alpha)}\sigma_1(u_r y_{s_1}), \cdots, \sqrt{2\sigma_n(\alpha)}\sigma_n(u_r y_{s_1}), \\ &\quad \sqrt{2\sigma_1(\alpha)}\sigma_1(u_r y_{s_2}), \cdots, \sqrt{2\sigma_n(\alpha)}\sigma_n(u_r y_{s_2}), \\ &\quad \sqrt{2\sigma_1(\alpha)}\sigma_1(u_r y_{s_3}), \cdots, \sqrt{2\sigma_n(\alpha)}\sigma_n(u_r y_{s_3}), \\ &\quad \sqrt{2\sigma_1(\alpha)}\sigma_1(u_r y_{s_4}), \cdots, \sqrt{2\sigma_n(\alpha)}\sigma_n(u_r y_{s_4})\Big) \end{aligned}$$

and $\sigma_{2\alpha}$ is an embedding of $\mathcal{A}$ in $\mathbb{R}^{4n}$.

V. Construction of lattices from maximal orders into quaternion algebras

In this section, following the schedule provided in Section IV, we find suitable ideals $\mathcal{I} \subseteq \mathcal{M}$ and totally positive elements $\alpha \in \mathbb{K}$ such that the ideal lattices $\Lambda = (\mathcal{I}, \alpha)$ are rotated versions of the densest lattices in dimensions 4 and 8, that is, the root lattices D_4 and E_8, respectively. In these constructions the algorithms were implemented in Magma and Wolfram Mathematica software.

A. Construction of D_4

Let $\mathcal{H} = (-1, -1)_{\mathbb{Q}}$ be the Hamilton quaternions over $\mathbb{Q}$ and $\mathcal{M} \supseteq \mathcal{O} = (-1, -1)_{\mathbb{Z}}$ a maximal quaternion order characterized by the basis

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

In fact, by Propositions 3.1 and 3.2, $\mathcal{M}$ characterized by B is a maximal quaternion order in $\mathcal{A}$ because

$$Trd(y_i), Nrd(y_i) \in \mathbb{Z} \text{ and } \mathcal{D}(\mathcal{M}) = \langle 2 \rangle = \mathcal{D}(\mathcal{A}),$$

for all $y_i \in B$, $i = 1, \cdots, 4$. If we take the ideal $\Lambda = \mathcal{I} = \mathcal{M}$ and considering the canonical embedding ($\alpha = 1$) we have that $\Lambda = (\mathcal{I}, 1)$ is an ideal lattice with $\mathbb{Z}$-basis B and full diversity. Moreover, the Gram matrix of $(\mathcal{I}, 1)$ is given by

$$G = Trd(w_i \overline{w_j}) = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix},$$

where $w_i, w_j \in B$.

Applying the LLL algorithm, [17], we obtain the matrix

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

that is a Gram matrix of the lattice D_4. Therefore, $\Lambda = (\mathcal{I}, 1)$ is an ideal lattice isomorphic to D_4.

B. Construction of E_8

Let $\mathcal{A} = (-1,-1)_{\mathbb{K}}$ be a quaternion algebra over the totally real number field $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Therefore, $\mathcal{M} \supseteq \mathcal{O} = (-1,-1)_{\mathbb{O}_{\mathbb{K}}}$ is a maximal quaternion order in $\mathcal{A}$, where $\mathbb{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$, characterized by the basis

$$B = \left\{1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+k}{2}\right\}. \quad (5)$$

In fact, by Propositions 3.1 and 3.2, $\mathcal{M}$ characterized by B is a maximal quaternion order in $\mathcal{A}$ because

$$Trd(y_i), Nrd(y_i) \in \mathbb{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}] \text{ and } \mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}),$$

for all $y_i \in B$, $i = 1, \cdots, 4$. According with Proposition 4.1, in order to fulfill the condition (2) for $\Lambda' = E_8$, we need to find $\alpha \in \mathbb{K}$ totally positive and $\mathcal{I} \subseteq \mathcal{M}$ a right ideal such that

$$c^8 = 2^{12} N(\alpha)^4 N(Nrd(\mathcal{I}))^4, \quad (6)$$

since $det(E_8) = 1$, $\mathcal{D}(\mathcal{M}) = 1$ and $d_{\mathbb{K}} = 2^3$. If we take the ideal $\mathcal{I} = \mathcal{M}$ and $\alpha = 2 + \sqrt{2}$ totally positive element in $\mathbb{K}$, then $\Lambda = (\mathcal{I}, 2+\sqrt{2})$ is an ideal lattice with basis B' given by

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

that satisfies (6), for $c = 4$. Moreover, the Gram matrix of $\Lambda = (\mathcal{I}, 2+\sqrt{2})$ is given by

$$\begin{aligned} G &= Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i \overline{w_j})) \\ &= \begin{pmatrix} 8 & 8 & 4 & 8 & 4 & 8 & 4 & 4 \\ 8 & 16 & 8 & 8 & 8 & 8 & 4 & 8 \\ 4 & 8 & 8 & 8 & 4 & 4 & 4 & 8 \\ 8 & 8 & 8 & 16 & 4 & 8 & 8 & 8 \\ 4 & 8 & 4 & 4 & 8 & 8 & 4 & 8 \\ 8 & 8 & 4 & 8 & 8 & 16 & 8 & 8 \\ 4 & 4 & 4 & 8 & 4 & 8 & 8 & 8 \\ 4 & 8 & 8 & 8 & 8 & 8 & 8 & 16 \end{pmatrix}, \end{aligned} \quad (7)$$

where $w_i, w_j \in B'$ and $det(\Lambda) = det(G) = 4^8$. Applying the LLL algorithm, [17], we obtain the matrix

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

that is a Gram matrix of the lattice E_8 (E_8 is the only unimodular lattice of dimension 8 and even). Therefore, $\Lambda = (\mathcal{I}, 2+\sqrt{2})$ is an ideal lattice isomorphic to E_8.

Now consider the matrix whose rows are the coefficients of the basis given in (5):

$$\varphi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Since φ has zero entries, we have verified that the generator matrix obtained as in (4) also have zero entries, and therefore the ideal lattice obtained has not full diversity. The aim is to find a rotated version of E_8 with good minimum product distance. So, as a first approach, we have found, using the quaternion structure and a rotation matrix of φ, the following matrix

$$\Phi = \begin{pmatrix} \frac{1}{2\sqrt{2}} & \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2\sqrt{2}} \\ \frac{1}{4}(1-\sqrt{2}) & \frac{1}{4}(1+\sqrt{2}) & \frac{1}{4} & \frac{3}{4} \\ -\frac{1}{4} & \frac{1}{4}(1+\sqrt{2}) & \frac{3}{4} & \frac{1}{4}(1-\sqrt{2}) \\ \frac{1}{4}(-1-\sqrt{2}) & \frac{1}{4} & \frac{1}{4}(1+\sqrt{2}) & \frac{1}{4}+\frac{1}{\sqrt{2}} \end{pmatrix}, \quad (8)$$

whose rows give us a new basis of the lattice Λ with non-vanishing elements which improve the diversity of Λ. Applying the embeddings $\sigma_1(a+b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a+b\sqrt{2}) = a - b\sqrt{2}$, $a, b \in \mathbb{Q}(\sqrt{2})$, in the elements of Φ we obtain the following 8×8 matrix:

$$\phi_2 = \begin{pmatrix} \sigma_1(\Phi_{ij}) & 0 \\ 0 & \sigma_2(\Phi_{ij}) \end{pmatrix},$$

$i, j = 1, \cdots, 4$. If we consider the basis $\{1, \sqrt{2}\}$ of $\mathbb{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ then

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

Hence, expanding M_1 into a 8×8 matrix we have the matrix ϕ_1 as in (3). Multiplying ϕ_1 by ϕ_2 we have a generator matrix M as in (4) of the lattice Λ with non-vanishing elements. Moreover, using M we obtain the Gram matrix (7) and therefore, with the new basis (8), Λ is also isomorphic to E_8.

Constructions of lattices in dimensions $4n$, $n > 2$, are to be considered using ideals in the maximal real subfield of cyclotomic fields.

VI. Conclusions

In this paper, we construct ideal lattices from maximal orders of quaternion algebras over totally real number fields which can be used to design space-time block codes as lattices of rank $4n$. Special cases approached here are rotated versions of lattices D_4 and E_8 which makes these quaternion constructions as dense as possible in their dimensions. This is a work in progress. The perspective is to explore this construction for lattices in higher dimensions and besides density, to analyze diversity and minimum product distance using some advantages provided by the explicit form of the generator matrix and algebraic structure.

We would like to thank the reviews for their very pertinent remarks and suggestions.

References

[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] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups,* Springer-Verlag, 1988.

[3] C. Alves, J-C. Belfiore, "Lattices from maximal orders into quaternion algebras," *Journal of Pure and Applied Algebra*, v. 219 (4), pp. 687-702, 2015.
[4] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel," *Trans. Inf. Theory,* v. 50 (4), pp. 702-714, 2004.
[5] E. Bayer-Fluckiger, I. Suarez, "Ideal lattices over totally real number fields and Euclidean minima," *Arch. Math.,* v. 86 (3), pp. 217-225, 2006.
[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] C. Hollanti, J. Lahtonen, H.-f.(F.) Lu, "Maximal Orders in the Design of Dense Space-Time Lattice Codes", *IEEE Trans. Inform. Theory,* v.54 (10) pp. 4493-4510, 2008.
[8] R. Vehkalahti, C. Hollanti, J. Lahtonen, K. Ranto, "On the Densest MIMO Lattices from Cyclic Division Algebras", *IEEE Trans. Inform. Theory,* v.55 (8), pp. 3751-3780, 2009.
[9] E. Bayer-Fluckiger, *Lattices and number fields, Contemporary Mathematics,* v. 241, pp. 69-84, 1999.
[10] F.-T. Tu and Y. Yang, "Lattice packing from quaternion algebras", *RIMS Kôkyûroku Bessatsu*, pp. 229-237, 2012.
[11] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.
[12] C. Maclachlan and A. W. Reid, *The arithmetic of hyperbolic 3-manifolds*. Springer-Verlag, New York, 2003.
[13] H. Cohn, A. Kumar, "Optimality and uniqueness of the Leech lattice among lattices," *Annals of Mathematics, Princeton,* v. 170, pp. 1003-1050, 2009.
[14] E. Bayer-Fluckiger, "Definite unimodular lattices having an automorphism of given characteristic polynomial," *Comment. Math. Helvetici,* v. 59, pp. 509-538, 1984.
[15] 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.
[16] S. Yang, J.-C., Belfiore, "Optimal Space-Time Codes For The Mimo Amplify-And- Forward Cooperative Channel", *IEEE Trans. Inform. Theory,* v. 53(2), pp. 647-663, 2007.
[17] P. Q. Nguyen and B. Vallée, *The LLL Algorithm: Survey and Applications*, Springer-Verlag, Berlin Heidelberg, 2010.
[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.