Lattices associated with Octonion Algebras

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

***Abstract*—In this paper we propose a construction of lattices in dimension $8n$ via octonion orders over a totally real number field. To show the potential of this construction, we present rotated versions of E_8, Λ_{16}, the densest known lattices in these dimensions and a lattice with the same density of the Barnes-Wall lattice in dimension 32. Perspectives applications of these lattices based on octonion algebras are in lattice based cryptography and lattice coding for MIMO and MISO channels.**

***Index Terms*—Ideal Lattices, Lattice Coding , Octonion Algebras**

I. Introduction

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].

Algebraic number theory has been used as mathematical tool that enables the design of good coding schemes also due to coding/decoding properties. 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 [3]. 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 considered, by requiring both bigger product distance (smaller error probability) and good density (coding gain) [4].

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 [5], [6] 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 $A_p^{(k)}$ are presented.

N. G. Brasil Jr is with the Institute of Mathematics, Statistics and Computer Science (IMECC), University of Campinas (Unicamp) as a Ph.D. student (e-mail: nelson.gbrasil@gmail.com)

C. W. O. Benedito is with São Paulo State University (Unesp), Campus of São João da Boa Vista (e-mail: cintya.benedito@unesp.br)

S. I. R. Costa is with the Institute of Mathematics, Statistics and Computer Science (IMECC), University of Campinas (Unicamp) (e-mail: sueli@ime.unicamp.br).

Partial and preliminary results of this paper were presented at XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais – SBrT2017, São Pedro–SP.

This work was partially supported by CNPq 312926/2013-8, CAPES and FAPESP 2013/25977-7.

Digital Object Identifier: 10.14209/jcis.2018.24

Space-time block codes provide the bridge between the practice of wireless communication with the mathematics of quadratic forms developed by Radon and Hurwitz. The columns of the code represent different time slots and the rows the transmit antennas, and the entries are the symbols to be transmitted [7]. This connection was explored in the Alamouti space time block code for two transmit antennas in the pionner paper [8] where multiplication in the ring of quaternions was used. Maximal quaternion orders have been proposed in the context of space-time block codes in [9] and complex codes constructions based on cyclic division algebras are proposed in [10]. More recently, the E_8-lattice was constructed over an imaginary quadratic field [11]. Codewords are usually built over the complex field. However for ultra wideband communication, one needs to design them over the real field [12]. Thus, having the construction of rotated lattices as our goal, we are interested in constructing dense lattices from octonion orders over a totally real number field. In this construction we use algebraic lattice theory.

Algebraic lattices which are obtained via ideals of number fields [13] are also called ideal lattices. In [14], [15] such lattices were constructed in dimension $4n$, via maximal orders in quaternion algebras. We propose here the construction of ideal lattices in dimension $8n$ using octonion orders. To exemplify the potential of this construction we present, for $n = 1$ and 2, rotated versions of E_8 and Λ_{16} lattices (the densest known lattices in these dimensions) and for $n = 3$ a lattice with the same center density of the Barnes-Wall lattice in dimension 32. it is also meaningful to note that the division algebra of the octonions can be used in coding and decoding processes. Lattices via octonion algebras over finite fields and polynomial rings have been proposed in [16] to construct lattice-based public key cryptossystems and it was proved that such encoding based on a non-associative algebra is feasible and also more secure than the lattice-based cryptosystem NTRU.

This work is organized as follows: In Section II we review some basics concepts on lattices and algebraic number theory. In Section III some definitions and results on octonion algebras are presented. In Section IV we propose an ideal lattice construction via octonion algebras over totally positive algebraic number fields and characterize its Gram matrix. In Section V, two families of lattices in dimension 2^n, $n \geq 3$ are derived and examples of lattices in dimenson 8, 16 and 32 are presented. Conclusions and perspectives are drawn in Section VI.

II. Lattices

A **full-rank lattice** Λ is a set of $\mathbb{R}^n$ composed by all integer linear combination of n linearly independent vectors

$v_1, \cdots, v_n \in \mathbb{R}^n$. The set $\mathfrak{a} = \{v_1, \cdots, v_n\}$ is called a **basis** of Λ. The matrix $M_\mathfrak{a}$ whose rows are the vectors of $\mathfrak{a}$ is called a **generator matrix** to Λ and $G_\mathfrak{a} = M_\mathfrak{a} M_\mathfrak{a}^\top$ is the **Gram matrix** of Λ associated with $M_\mathfrak{a}$. Another set $\mathfrak{b} = \{w_1, \cdots, w_n\}$ of linearly independent vectors is also a basis of Λ if and only if $M_\mathfrak{b} = UM_\mathfrak{a}$, where U is an unimodular matrix [2] (U has integers entries and $\det(U) = \pm 1$). The **determinant** of Λ is defined by $\det(\Lambda) = \det(G_\mathfrak{a})$, where $G_\mathfrak{a}$ is any Gram matrix of Λ. The determinant of Λ is invariant under the change of basis and it measures the squared volume of the n-dimensional parallelotope generated by any lattice basis. If there is a Gram matrix G which is unimodular we say that Λ is a **unimodular lattice**.

If d_Λ is the minimum distance between two points of a lattice Λ, the **packing density**, $\Delta(\Lambda)$ is the proportion of $\mathbb{R}^n$ covered by the union of congruent and disjoint spheres with the biggest possible radius and centered at points of Λ. Due the lattice homogeneity, its packing density can be expressed as

$$\Delta(\Lambda) = \frac{\mathcal{V}olB^n(d_\Lambda/2)}{\sqrt{\det(\Lambda)}},$$

where $\mathcal{V}olB^n(r)$ is the volume of a n-dimensional ball of radius r. Another expression to be used here is the so called **center density** of a lattice, defined as

$$\delta_\Lambda = \frac{\Delta(\Lambda)}{\mathcal{V}olB^n(1)}.$$

Algebraic constructions of lattices allow explicit calculation of parameters and figures of merit of a lattice. The algebraic construction considered here is also called ideal lattice [13] and it is based on concepts and properties recalled next.

A **group** is a set G with an operation "$+$", $(G, +)$ such that for all $a, b, c, \in G$: (1) $(a + b) + c = a + (b + c)$; (2) $\exists\, e \in G$; $a + e = e + a = a$, $(e \equiv 0)$; (3) for any $a \in G$ there is $b \in G$; $a + b = b + a = e$. If $a + b = b + a$ for all $a, b \in G$ then the group G is called a commutative group. A **ring** is a set R with two operations $(R, +, \cdot)$ such that $(R, +)$ is a commutative group and for all $a, b, c \in R$: (1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$; (2) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$. An **ideal** $\mathcal{I}$ of a commutative ring R is an additive subgroup of R which is stable under multiplication by R, i.e., $a\mathcal{I} \subset \mathcal{I}$ for all $a \in R$. If the ring operation "$\cdot$" is also commutative then the ring R is a commutative ring and if there is a multiplicative identity in R (1_R) such that any nonzero element of $\mathbb{F}$ has an inverse, i.e, if for all $a \in \mathbb{F}\backslash\{0\}$ there is $b \in \mathbb{F}$ such that $ab = 1_R$ then $R = \mathbb{F}$ is a **field**. Standard examples of these concepts are the ring of integers $\mathbb{Z}$ and the fields of the rational numbers $\mathbb{Q}$, of the real numbers $\mathbb{R}$ and of the complex numbers $\mathbb{C}$.

The structure of vector spaces which are defined over fields can be generalized to **modules**. Given a ring R, a commutative group $(M, \dotplus)$ is an **R-module** if there is an operation $\varphi : R \times M \rightarrow M$ defined as $\varphi(a, m) = am$ such that (1) $a(m \dotplus n) = am \dotplus an$; (2) $(a \dotplus b)m = am \dotplus bm$; (3) $(ab)m = a(bm)$; (4) $1_R m = m$; $\forall a, b \in R$ and $m, n \in M$. Also, M is said to be a **finitely generated module** if it has a finite set of generators. A **vector space** of dimension n is a finitely generated module over a field $\mathbb{F}$.

Example 1. *Consider* $\mathbb{F}_1 = \{a + b\sqrt{2};\, a, b \in \mathbb{Z}\}$ *and* $\mathbb{F}_2 = \{a + b\sqrt{2};\, a, b \in \mathbb{Q}\}$. *Then the set* $\{1, \sqrt{2}\}$ *is a basis for both* $\mathbb{F}_1$ *and* $\mathbb{F}_2$. $\mathbb{F}_1 = \mathbb{Z}[\sqrt{2}]$ *is a module whereas* $\mathbb{F}_2$ *is a vector space of dimension* 2 *over the field* $\mathbb{Q}$ *denoted by* $\mathbb{F}_2 = \mathbb{Q}(\sqrt{2})$.

A field $\mathbb{K}$ is called an **algebraic number field** if it contains $\mathbb{Q}$ and has finite dimension n when considered as a vector space over $\mathbb{Q}$ (n is called the degree of $\mathbb{K}$). For all $y \in \mathbb{K}$ there is a monic polynomial g with coefficients in $\mathbb{Q}$ such that $g(y) = 0$ and the polynomial with this property and smallest degree is called **minimal polynomial** of y. The minimal polynomial is unique and has degree less or equal to the degree of $\mathbb{K}$. The set of all $y \in \mathbb{K}$ such that the minimal polynomial of y has integer coefficients is called the **ring of integers** of $\mathbb{K}$ and denoted by $\mathfrak{o}_\mathbb{K}$.

Example 2. $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ *is an algebraic number field of degree* 2. *The minimal polynomial of any element* $y = a + b\sqrt{2} \in \mathbb{K} = \mathbb{Q}(\sqrt{2})$ *is:* $p(x) = x - a$ *for* $b = 0$ *and* $p(x) = x^2 + 2ax + a^2 - 2b^2$ *for* $b \neq 0$. *Therefore* y *belongs to the ring of integers if and only if* a *is integer and* $b = 0$ *or* $2a$, $a^2 - 2b^2 \in \mathbb{Z}$ *what is equivalent to say that* $a, b \in \mathbb{Z}$. *Then, the ring of integers of* $\mathbb{K}$ *is the set* $\mathfrak{o}_\mathbb{K} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\, a, b \in \mathbb{Z}\}$ *and* $\{1, \sqrt{2}\}$ *is a* $\mathbb{Z}$*-basis of* $\mathfrak{o}_\mathbb{K}$.

As another example, if we consider $\mathbb{L} = \mathbb{Q}(\sqrt{5})$ *an algebraic number field of degree* 2, *the minimal polynomial of any element* $y = a + b\sqrt{5} \in \mathbb{L}$ *is:* $q(x) = x - a$ *for* $b = 0$ *and* $q(x) = x^2 - 2ax + a^2 - 5b^2$ *for* $b \neq 0$. *Since this last polynomial has integers coefficients we can assert that the the ring of integers of* $\mathbb{L}$ *is* $\mathbb{Z}[(1 + \sqrt{5})/2]$.

A **homomorphism** $\sigma : \mathbb{K}_1 \rightarrow \mathbb{K}_2$ between two fields is a map which preserves both field operations: (1) $\sigma(a + b) = \sigma(a) + \sigma(b)$ and (2) $\sigma(ab) = \sigma(a)\sigma(b)$ $\forall\, a, b \in \mathbb{K}_1$. Given an algebraic number field $\mathbb{K}$ there are exactly n field homomorphisms $\{\sigma_i : \mathbb{K} \rightarrow \mathbb{C},\ i = 1, \ldots, n \mid \sigma_i(x) = x,\ \forall x \in \mathbb{Q}\}$ [17]. The mapping $\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x))$ is called the canonical (or Minkowski) embedding of $\mathbb{K}$ in $\mathbb{C}^n$ and the signature (r_1, r_2) of $\mathbb{K}$ is defined by the number of real (r_1) and pairs of complex (r_2) embeddings ($n = r_1 + 2r_2$). If $r_2 = 0$ we say $\mathbb{K}$ is a **totally real number field**.

Let $\alpha \in \mathbb{K}$ totally positive (i.e., $\sigma_i(\alpha) = \alpha_i > 0$, $\forall i = 1, \ldots, n$), the homomorphism $\sigma_\alpha : \mathbb{K} \rightarrow \mathbb{R}^n$ where

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

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

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 $\mathfrak{o}_\mathbb{K}$, the **discriminant** of $\mathbb{K}$ is given by $d_\mathbb{K} = \left(\det(\sigma_j(w_i))_{i,j=1}^n\right)^2$. We remark that the discriminant is independent of the choice of basis [18].

It can be shown [13] that, given an ideal $\mathcal{I} \subset \mathfrak{o}_\mathbb{K}$ 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 $\{\sigma_\alpha(w_1), \cdots, \sigma_\alpha(w_n)\}$. The lattice $\Lambda = \sigma_\alpha(\mathcal{I})$

is called an **ideal lattice** associated to α and $\mathcal{I}$ with Gram matrix

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

and we will denote such lattice as $\Lambda = (\mathcal{I}, \alpha)$.

III. Octonion algebras

In this section we recall some concepts on octonion algebras and present results to be used in the following sections. We start with the most general definition of an octonion algebra.

Let $\mathbb{K}$ be a field, and V be a vector space over $\mathbb{K}$ with the usual sum and an additional operation from $V \times V$ to V called multiplication and denoted by $x \cdot y$ or simply xy. Then V is an **algebra** over $\mathbb{K}$ if the multiplication is bilinear. Classical examples of algebras are the rational numbers, the real and the complex numbers and also the set of $n \times n$ matrices with entries in some field, for some $n > 1$. Also, we say that an algebra is a **division algebra** if for any element $a \in V$ and a nonzero b in V there exist unique elements $x, y \in V$ such that $a = bx$ and $a = yb$.

Now, let $\mathbb{K}$ be a totally real algebraic number field, a, b, c nonzeros elements of $\mathbb{K}$ and C be a vector space of dimension 8 over $\mathbb{K}$ with basis $\{e_0, \ldots, e_7\}$. A product in C can be defined by setting $e_0 = 1$, the identity element, $e_1^2 = ae_0 = a$, $e_2^2 = be_0 = b$, $e_4^2 = ce_0 = c$ as described in following table:

$\cdot$	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

Definition 3. *The set C with the usual sum of vector spaces and the multiplication as described above is called an **octonion algebra** and denoted by $C = (a, b, c)_{\mathbb{K}}$.*

Note that, if we choose $\mathbb{K} = \mathbb{R}$ e $a = b = c = -1$, we will obtain the Cayley numbers, the most known octonion algebra [19]. Along this paper we consider $a = b = c = -1$, but different fields starting with $\mathbb{Q}$ (Example 2) and number fields as $\mathbb{Q}(\sqrt{2})$ and others as we will see in Section V.

We define the **conjugate** of x as $\overline{x} = x_0 - \sum_{i=1}^{7} x_i e_i$, the **reduced norm** of x by $N(x) = x\,\overline{x}$ and the **reduced trace** of x by $Trd(x) = x + \overline{x}$. In particular, we have $N(x) \in \mathbb{K}$ and $N(x) = N(\overline{x}) = \overline{x}\,x$. It can be shown that the algebra $(a, b, c)_{\mathbb{K}}$ in the Definition 3 is a nonassociative division algebra [19]. Given an octonion algebra, we can obtain an orthogonal basis to this algebra regarding to a natural inner product.

Proposition 4. *[20] In any octonion algebra $C = (a, b, c)_{\mathbb{K}}$ over a number field $\mathbb{K}$ such that $1 + 1 \neq 0$ there are elements $x, y, z \in C$ with nonzero norm such that*

$$\mathfrak{B} = \{1, x, y, xy, z, xz, yz, (xy)z\} \quad (2)$$

is an orthogonal basis of C with respect to the associate bilinear form

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

We introduce next the concept of R-**order** in the context of the octonion algebras. In particular, for the results of the next section we will assume $R = \mathfrak{o}_{\mathbb{K}}$ for some number field $\mathbb{K}$.

An R-**order** (or simply order when the ring R is clear in the context) O in the octonion algebra C ($O \subset C$) is a finitely generated module over R such that $C = \mathbb{K} \cdot O = \{\alpha \cdot x; \alpha \in \mathbb{K};\ x \in O\}$ [20].

Proposition 5. *[21] Let C be an octonion algebra and $O \subset C$. If O is an order, then every element $x \in O$ is an integer over R i.e. $Trd(x) \in R$, $N(x) \in R$.*

An order $\mathcal{M} \subset C$ is called a **maximal order** if it is not properly contained in any other order O. Every R-order is contained in a maximal R-order of C [21].

Example 6. *Consider $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ and $C = (-1, -1, -1)_{\mathbb{K}}$ an octonion algebra over $\mathbb{K}$. Any element $x \in C$ is*

$$x = x_0 + x_1 e_1 + x_2 e_2 + \cdots + x_7 e_7,$$

such that $x_i = a_i + b_i\sqrt{2}$. Note that this algebra can be seen as a vector space of dimension 16 over the field $\mathbb{Q}$ since we can write any $x \in C$ as

$$x = a_0 + b_0\sqrt{2} + \left(a_1 + b_1\sqrt{2}\right) e_1 + \cdots + \left(a_7 + b_7\sqrt{2}\right) e_7,$$

and associate x with a 16-uple $(a_0, b_0, \ldots, a_7, b_7)$.

By choosing

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

and using Proposition 4 we have a basis of C. Now taking

$$\mathfrak{W} = \left\{2e, 2x, 2y, 2xy, 2\sqrt{2}z, 2\sqrt{2}xz, 2\sqrt{2}yz, 2\sqrt{2}(xy)z\right\}, \quad (3)$$

we can generate an order O in C with basis $\mathfrak{W}$. In fact, the reduced trace and reduced norm of all elements in $\mathfrak{W}$ belongs to $\mathbb{Z}[\sqrt{2}]$. So, by Proposition 5, O is an order of C.

An ideal $\mathcal{I} \subset O$ can be obtained, for example, by selecting a basis

$$2\mathfrak{W} = \left\{4e, 4x, 4y, 4xy, 4\sqrt{2}z, 4\sqrt{2}xz, 4\sqrt{2}yz, 4\sqrt{2}(xy)z\right\}. \quad (4)$$

IV. Lattices via Octonion orders

In this section we propose an algebraic construction of lattices of dimension $8n$ via orders in octonion algebras, identifying their Gram matrix. We can define ideal lattices from octonion orders in the same way that we define ideal lattices from number fields [6].

Let $\mathbb{K}$ be a totally real algebraic number field of degree n and C an octonion algebra over $\mathbb{K}$. If $\mathcal{I} \subset O$ is an ideal of an order in C, α a totally positive element in $\mathbb{K}$ and $Q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Q}$ a positive definite quadratic form given by $Q_\alpha(x, y) = tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(x\overline{y}))$. Considering $\mathcal{I}$ an ideal on C with basis $\mathfrak{B} = \{v_1, \ldots, v_8\}$, assuming that $\mathbb{K}$ has degree n

and $\mathfrak{v}_{\mathbb{K}}$ with $\mathbb{Z}$-basis $\{u_1, \ldots, u_n\}$, we can write a basis of the lattice $\Lambda = (\mathcal{I}, \alpha) \subset \mathbb{R}^{8n}$ as

$$\mathfrak{B}' = \{\sigma(v_i u_j)\} = \{w_{11}, w_{12}, \ldots, w_{1n}, \ldots, w_{81}, \ldots, w_{8n}\},$$

where

$$w_{ij} = \left(\sqrt{2\sigma_1(\alpha)}\sigma_1(u_i v_j), \ldots, \sqrt{2\sigma_n(\alpha)}\sigma_n(u_i v_j)\right).$$

Moreover since $\mathbb{K}$ is a totally real number field, the Gram matrix associated to the basis w_{ij} of Λ is given by

$$G = tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i \overline{w}_j)). \tag{5}$$

Then, $\Lambda = (\mathcal{I}, \alpha)$ is the ideal lattice associated to the quadratic form Q_α.

The following result provides the determinant of the matrix G of the lattice $\Lambda = (\mathcal{I}, \alpha)$. The proof of this result follows similar steps as ones given in [14] for the quaternionic case.

Theorem 7. *Let $\Lambda = (\mathcal{I}, \alpha)$ be the ideal lattice with a Gram matrix G as in (5). Then the determinant of Λ can be written as*

$$\det(\Lambda) = d_{\mathbb{K}}^8 N(\alpha)^8 N_{\mathbb{K}/\mathbb{Q}}(\det(B)) \tag{6}$$

where $B = Trd(v_\ell \overline{v_{\ell'}})_{\ell,\ell'=1}^8$ and $v_\ell, v_{\ell'} \in \mathfrak{B}$ basis of $\mathcal{I}$.

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the n-homomorphism from $\mathbb{K}$ to $\mathbb{R}$. The elements of the Gram matrix of Λ, $G = (g_{ij})_{i,j=1}^8$, can be written as

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

with $tr(x) = \sum_{i=1}^n \sigma_i(x)$. We can then expand the trace form on the number field as the sum of the homomorphisms

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

Hence, the matrix G can be factorized as the product of three matrices,

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

where

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

and

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

The operation $A \otimes C$ means that if A is a matrix $m \times n$ and C a matrix $r \times s$, we have

$$A \otimes C = \begin{pmatrix} a_{11}C & a_{12}C & \cdots & a_{1n}C \\ a_{21}C & a_{22}C & \cdots & a_{2n}C \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}C & a_{m2}C & \cdots & a_{mn}C \end{pmatrix}_{mr \times ns}.$$

Therefore, the determinant of G is

$$\det(G) = \left(\sqrt{|d_{\mathbb{K}}|}\right)^{16} \det(\varphi). \tag{7}$$

To calculate the determinant of φ, we can permute rows and columns of this matrix in order to obtain block matrices as follows

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

and then $\varphi = \operatorname{diag}(\varphi_1, \ldots, \varphi_n)$.

Thus, $\det(\varphi) = \prod_{\ell=1}^n \det(\varphi_\ell)$, i.e.,

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

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

Combining (7) and (8) we have, then

$$\det(G) = (|d_{\mathbb{K}}|)^8 \left(N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right)^8 N_{\mathbb{K}/\mathbb{Q}}(\det(B)).$$

□

V. Families of lattices in dimension 2^n, $n \geq 3$

In this section, we will present two families of lattices in dimension 2^n, $n \geq 3$ by using fixed orders in octonion algebras $\mathcal{C}_n = (-1, -1, -1)_{\mathbb{K}_n}$ where $\mathbb{K}_3 = \mathbb{Q}$, $\mathbb{K}_4 = \mathbb{Q}(\sqrt{2})$ and $\mathbb{K}_n = \mathbb{Q}(\eta_n)$ where

$$\eta_n = \sqrt{2 + \eta_{n-1}},\ \eta_4 = \sqrt{2},\ n \geq 5 \tag{9}$$

Note that $\mathbb{K}_n$ has dimension 2^{n-3} over $\mathbb{Q}$.

Using the construction proposed in Section IV and choosing $\mathcal{I} = \mathcal{O}$ it is possible to obtain lattices from these fields. We remark that other choices of $\mathcal{I}$ can be taken in order to obtain different lattices in the same dimensions. In the next constructions, for $n = 3$ we obtain the lattice with optimal center density in dimension 8 and for $n = 4$ and 5 we get lattices with the same center density of the Barnes-Wall lattices, a well known family that includes the densest lattices in dimension 1, 2, 4, 8 and 16 [2], [22].

First we consider the field $\mathbb{K}_n$ for some $n \geq 3$ and construct a fixed basis of $\mathcal{C}_n$ as in Proposition 4 by choosing the elements and applying (2)

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

$$\begin{aligned} \mathfrak{A} = \Big\{1, e_1, e_2, -e_4, \frac{e_1 + e_2 + e_3 + e_4}{2}, \\ \frac{-1 - e_1 + e_4 - e_5}{2}, \frac{1 - e_1 + e_2 - e_6}{2}, \\ \frac{-1 + e_2 - e_4 + e_7}{2}\Big\}. \end{aligned} \tag{10}$$

This basis is such that the determinant of $B = (b_{ij}) = Trd(v_i \overline{v_j})$ with $v_i, v_j \in \mathfrak{A}$ in (6) is equal to 1. It can be shown that the field $\mathbb{K}_n$ has discriminant equal to $d_{\mathbb{K}_n} = 2^{(n-2)2^{(n-3)}-1}$ [23]. By using the basis $\mathfrak{A}$ and choosing the totally positive element $\alpha = 1$ for $n = 3$ and $\alpha = 2 - \eta_n$, $n \geq 4$ (9), which has norm $N(\alpha) = 2$, we can construct a family of lattices in dimension 2^n, $n \geq 3$ with determinant

$$\begin{aligned} &\det(G) = 1, \text{ for } n = 3; \\ &\det(G) = \left(2^{(n-2)2^{(n-3)}-1}\right)^8 \cdot 2^8 \cdot 1 = 2^{(n-2)2^n}, \text{ for } n \geq 4. \end{aligned}$$

We can then consider another Gram matrix G' for a scaled version of Λ by a factor $2^{\frac{n-2}{2}}$, related to G as follows

$$G' = \frac{1}{2^{(n-2)}} U^{\top} G U,$$

where U is an unimodular matrix. Therefore, $\det(G') = 1$ for all $n \geq 3$. We can also remark that since in this case every element of G described in (5) is a multiple of $2^{(n-2)}$, the scaled version of Λ is an unimodular lattice. Then, we have a family of lattices in dimension 2^n associated to the octonion algebra C_n, basis $\mathfrak{A}$ and $\alpha = 1$ if $n = 3$ and $\alpha = 2 - \eta_n$, $n \geq 4$. To exemplify and show an element of this family, we will construct a lattice in dimension 8.

Example 8. *To construct a lattice congruent to E_8, we consider $C_3 = (-1, -1, -1)_{\mathbb{K}_3}$, $\mathbb{K}_3 = \mathbb{Q}$ and the order O generated by the basis $\mathfrak{A}$. For $\alpha = 1$, applying (5) we get the following Gram matrix*

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

which is a unimodular matrix which main diagonal is even. Therefore, the lattice $\Lambda = (O, \alpha)$ is an ideal lattice congruent to the E_8 lattice.

Remark 9. *If we use the same basis $\mathfrak{A}$ to generate an octonion order in C_n for $n = 4, 5, 6$ we obtain after scaling unimodular lattices in dimension 2^n with squared minimum distance equal to 2.*

Now, instead to use the basis defined before, we can choose other triple x, y, z as

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

and

$$\mathfrak{C} = \left\{2e, 2x, 2y, 2xy, 2\sqrt{2}z, 2\sqrt{2}xz, 2\sqrt{2}yz, 2\sqrt{2}(xy)z\right\}. \quad (11)$$

In the next proposition we show that $\mathfrak{C}$ is a basis of an octonion order.

Proposition 10. *Let $\mathbb{K}_n$ be a field and the let $C_n = (-1, -1, -1)_{\mathbb{K}_n}$ be the associated octonion algebra. The set O generated by the basis $\mathfrak{C}$ is an order in C_n for all $n \geq 4$.*

Proof. We have to show that the reduced trace and reduced norm of the elements of $\mathfrak{C}$ belong to $\mathfrak{o}_{\mathbb{K}} = \mathbb{Z}[\eta_n]$, $\forall n \geq 4$.

For the reduced trace, we have

$$\begin{aligned} Trd(2) &= 4, \\ Trd\left(\sqrt{2}(1 + e_1)\right) &= 2\sqrt{2}, \\ Trd\left(\sqrt{2}(1 + e_2)\right) &= 2\sqrt{2}, \\ Trd(1 + e_1 + e_2 - e_3) &= 2, \\ Trd\left(\sqrt{2}(e_1 + e_2 + e_3 + e_4)\right) &= 0, \\ Trd(-1 + e_1 + 2e_2 + e_4 - e_5) &= -2, \\ Trd(-1 + e_2 + 2e_3 + e_4 - e_6) &= -2, \\ Trd\left(-\frac{1 + e_1 - 3e_2 - e_3 - e_4 + e_5 + e_6 - e_7}{\sqrt{2}}\right) &= -\sqrt{2}. \end{aligned}$$

And since $\sqrt{2} \in \mathbb{Z}[\eta_n]$ for all $n \geq 4$, the elements in $\mathfrak{C}$ are such that the reduced trace is an integer element. The proof regarding the reduced norm follows the same way.

$$\begin{aligned} N(2) &= 4, \\ N\left(\sqrt{2}(1 + e_1)\right) &= 4, \\ N\left(\sqrt{2}(1 + e_2)\right) &= 4, \\ N(1 + e_1 + e_2 - e_3) &= 4, \\ N\left(\sqrt{2}(e_1 + e_2 + e_3 + e_4)\right) &= 8, \\ N(-1 + e_1 + 2e_2 + e_4 - e_5) &= 8, \\ N(-1 + e_2 + 2e_3 + e_4 - e_6) &= 8, \\ N\left(-\frac{1 + e_1 - 3e_2 - e_3 - e_4 + e_5 + e_6 - e_7}{\sqrt{2}}\right) &= 8. \end{aligned}$$

So, by Proposition 5 the set O generated by the basis $\mathfrak{C}$ is an octonion order in C_n for all n. □

Now, we consider again the field $\mathbb{K}_n$ for some $n \geq 5$ and the basis $\mathfrak{C}$ of C_n as in (11). Associated to this basis we have $\det(B) = 2^{12}$ and we want to choose an appropriate $\alpha = (2 - \eta_n)^m$ for some $m \geq 0$ such that $\det(G) = 2^{k2^n}$, k integer. Computing the determinant we have

$$\det(G) = \left(2^{(n-2)2^{(n-3)}-1}\right)^8 \cdot (2^m)^8 \cdot \left(2^{12 \cdot 2^{(n-3)}}\right),$$

and $m = 2^{n-4} + 1$. This imply that we can consider an integer Gram matrix G'' of a scaled version of this lattice.

$$G'' = \frac{1}{2^n} U^{\top} G U,$$

where U is an unimodular matrix and $\det(G'') = 1$ for all $n \geq 4$. We have then constructed another family of unimodular lattices in dimension 2^n but now with basis $\mathfrak{C}$, $\alpha = (2 - \eta_n)^{(2^{n-4}+1)}$ and the field $\mathbb{K}_n$.

In the next examples we have implemented algorithms following the ideas of [24], [25]. We have used thein the Mathematica software for the Gram matrix LLL reduction and the SAGE [26] for the computation of minimum distance. In the minimum distance search we took account the Minkowski bound for this parameter

$$d_\Lambda \leq \sqrt{n}(\det G)^{\frac{1}{2n}}.$$

Using such basis we get in dimensions 32 and 64, unimodular lattices with minimum distance equal to 4. To exemplify and show an element of this family, we will present the construction of a lattice with the same center density of the Barnes-Wall lattice in dimension 32.

Example 11. *To construct a lattice in dimension* 32 *with the same center density of the Barnes-Wall lattice we choose* $\mathbb{K}_5 = \mathbb{Q}(\eta_5) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ *and* $C_5 = (-1,-1,-1)_{\mathbb{K}_5}$. *Also, we choose the basis as in* (11) *and* $\alpha = (2-\eta_5)^3$. *Using these parameters, we can construct a lattice* $\Lambda_5 = (O, \alpha)$ *in dimension* 32. *We start from the Gram matrix obtained and consider the Gram matrix of the scaled lattice*

$$G_2 = \frac{1}{2^5} U^\top G U,$$

where the unimodular matrix U *is provided by LLL algorithm [27] using the Mathematica software [28]*

$$G_2 = \begin{pmatrix} A_1 & A_2 \\ A_2^\top & A_3 \end{pmatrix},$$

where

$A_1 =$

4	0	2	-2	-2	-2	0	-2	-2	-2	0	-2	-2	0	-1	1
0	4	-2	2	-2	-2	2	0	-2	-2	2	0	0	-2	1	-1
2	-2	4	-2	0	0	0	-2	0	0	0	-2	-1	1	-2	1
-2	2	-2	4	0	0	0	2	0	0	0	2	1	-1	1	-2
-2	-2	0	0	4	2	0	0	2	2	-1	1	0	0	0	-1
-2	-2	0	0	2	4	-2	2	2	2	-1	1	0	0	1	0
0	2	0	0	0	-2	4	-2	-1	-1	2	-1	0	-1	0	-1
-2	0	-2	2	0	2	-2	4	1	1	-1	2	1	0	1	0
-2	-2	0	0	2	2	-1	1	4	2	0	0	0	0	0	-1
-2	-2	0	0	2	2	-1	1	2	4	-2	2	0	0	1	0
0	2	0	0	-1	-1	2	-1	0	-2	4	-2	0	-1	0	-1
-2	0	-2	2	1	1	-1	2	0	2	-2	4	1	0	1	0
-2	0	-1	1	0	0	0	1	0	0	0	1	4	2	0	0
0	-2	1	-1	0	0	-1	0	0	0	-1	0	2	4	-2	2
-1	1	-2	1	0	1	0	1	0	1	0	1	0	-2	4	-2
1	-1	1	-2	-1	0	-1	0	-1	0	-1	0	0	2	-2	4

$A_2 =$

4	2	0	0	0	0	0	-1	0	0	1	-2	0	-1	-1	1
2	4	-2	2	0	0	1	0	0	0	2	-1	1	-2	0	0
0	-2	4	-2	-1	0	0	0	-1	0	0	0	-1	1	-1	0
0	2	-2	4	0	1	-1	1	0	1	0	0	1	-1	0	-1
0	0	-1	0	4	2	0	0	2	1	0	0	0	0	0	0
0	0	0	1	2	4	-2	2	1	2	0	0	0	0	0	0
0	1	0	-1	0	-2	4	-2	0	-1	1	0	0	-1	0	0
-1	0	0	1	0	2	-2	4	0	1	0	1	0	0	0	-1
0	0	-1	0	2	1	0	0	4	2	0	0	1	0	0	0
0	0	0	1	1	2	-1	1	2	4	-1	1	1	0	0	0
1	2	0	0	0	0	1	0	0	-1	4	-2	0	-1	-1	0
-2	-1	0	0	0	0	0	1	0	1	-2	4	0	1	1	0
0	1	-1	1	0	0	0	0	1	1	0	0	4	1	0	0
-1	-2	1	-1	0	0	-1	0	0	0	-1	1	1	4	-1	1
-1	0	-1	0	0	0	0	0	0	0	-1	1	0	-1	4	-1
1	0	0	-1	0	0	0	-1	0	0	0	0	0	1	-1	4

and

$A_3 =$

-2	-2	2	0	-2	0	-1	1	-2	0	-1	1	-1	1	0	-1
-2	-2	0	-2	0	-2	1	-1	0	-2	-1	1	-1	1	1	0
0	0	0	2	-1	1	-2	1	-1	1	0	-1	0	0	-1	-1
0	0	-2	0	1	-1	1	-2	1	-1	-1	0	0	0	1	1
2	2	-1	1	0	0	0	-1	1	1	1	-1	2	-1	0	1
2	2	-1	1	0	0	1	0	1	1	1	-1	1	-2	-1	0
-1	-1	0	-1	0	-1	0	-1	0	-1	0	0	0	1	0	0
1	1	-1	0	1	0	1	0	1	0	0	0	0	-1	0	0
2	2	-1	1	1	1	0	0	0	0	2	-1	0	-1	-1	1
2	2	-1	1	1	1	0	0	0	0	1	-2	1	-2	0	0
-1	-1	0	-1	0	-1	0	0	0	-1	0	1	-1	1	0	0
1	1	-1	0	1	0	1	-1	1	0	-1	0	1	-1	1	0
1	1	-1	0	2	1	0	0	2	1	0	0	0	0	0	1
1	1	0	1	1	2	-1	1	1	2	0	0	0	0	0	0
0	0	0	-1	0	-1	2	-1	0	-1	0	0	0	-1	0	1
0	0	1	0	0	1	-1	2	0	1	0	0	0	0	0	-2

The squared minimum distance, computed with SageMath [26], associated to the lattice with Gram matrix G_2 *is* 4, *and the obtained lattice has then the same center density, determinant and minimum distance of the Barnes-Wall lattice in dimension* 32.

Now by using the same parameters, we will construct a lattice in dimension 16 that has the same center density and minimum distance of the Barnes-Wall lattice which is not unimodular.

Example 12. *Let* $\mathbb{K}_4 = \mathbb{Q}(\sqrt{2})$, *a number field of degree* 2, *and let* $C_4 = (-1,-1,-1)_{\mathbb{K}_4}$ *the octonion algebra over this field* $\mathbb{K}_4$ *with basis constructed as in* (11).

Now, taking $\{1, \sqrt{2}\}$, *a basis of the ring of integers* $\mathfrak{o}_{\mathbb{K}}$, *we can construct a lattice* $\Lambda = (O, 2-\sqrt{2})$ *with dimension* 16. *Its Gram matrix, after we apply the LLL algorithm [27] is*

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

where

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

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

and

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

The matrix G_1 is a Gram matrix of the lattice Λ, having $\det(G_1) = 2^8$,

$$d_\Lambda^2 = \min_{\boldsymbol{v} \in \Lambda,\ \boldsymbol{v} \neq 0} \|\boldsymbol{v}\|^2 = 4,$$

and such that

$$\delta(\Lambda) = \frac{\left(\sqrt{4}\right)^{16}}{2^{16} \cdot 2^4} = \frac{2^{16}}{2^{20}} = \frac{1}{16}.$$

Then, the lattice Λ has the same center density of the Barnes-Wall lattice Λ_{16}, and this is the biggest known center density in this dimension.

Remark 13. *It is interesting to note that in the cases analyzed above the search for the square of minimum distance found using the mentioned algorithm is an element of the diagonal of the reduced Gram matrix. This means that the LLL algorithm used in the matrix reduction provided a lattice basis which contains minimal norm vectors.*

VI. Conclusion

In this paper we have presented a construction of ideal lattices via octonion orders extending the construction using quaternion algebras [14], [15] to get lattices in dimension $8n$, $n \geq 1$. For $n = 1, 2, 4$ the obtained lattices are rotated versions of well known dense lattices. We also provide two families in dimension 2^n for $n \geq 3$ using specific basis of the octonion orders involved. A future work is to construct dense lattices in higher dimensions and also discuss advantages of this construction regarding coding/decoding processes by using octonion operations. Perspective applications of these results include lattice-based cryptography (which requires higher dimensions) and coding for MIMO and MISO channels.

VII. acknowledgment

The authors are thankful to the referees for their pertinent comments and suggestions which have contributed to improve the paper.

References

[1] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both rayleigh fading and gaussian channels," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 502–518, 1996, doi: 10.1109/18.485720.

[2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. Springer, 1988, doi: 10.1007/978-1-4757-6568-7.

[3] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the rayleigh fading channel," *IEEE Transactions on information theory*, vol. 50, no. 4, pp. 702–714, 2004, doi: 10.1109/TIT.2004.825045.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE transactions on information theory*, vol. 44, no. 2, pp. 744–765, 1998, doi: 10.1109/18.661517.

[5] E. Bayer-Fluckiger, "Definite unimodular lattices having an automorphism of given characteristic polynomial," *Commentarii Mathematici Helvetici*, vol. 59, no. 1, pp. 509–538, 1984, doi:https://doi.org/10.1007/BF0256636410.1007/BF02566364.

[6] E. Bayer-Fluckiger and I. Suarez, "Ideal lattices over totally real number fields and euclidean minima," *Archiv der Mathematik*, vol. 86, no. 3, pp. 217–225, 2006, doi: 10.1109/49.730453.

[7] A. Calderbank and A. Naguib, "Orthogonal designs and third generation wireless communication," *London Mathematical Society Lecure Note Series*, pp. 75–108, 2001, doi: 10.1017/CBO9780511721328.006.

[8] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on selected areas in communications*, vol. 16, no. 8, pp. 1451–1458, 1998, doi: 10.1109/49.730453.

[9] C. Hollanti, J. Lahtonen, and H.-F. Lu, "Maximal orders in the design of dense space-time lattice codes," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4493–4510, 2008, doi: 10.1109/TIT.2008.928998.

[10] S. Yang and J.-C. Belfiore, "Optimal space–time codes for the mimo amplify-and-forward cooperative channel," *IEEE Transactions on information theory*, vol. 53, no. 2, pp. 647–663, 2007, doi: 10.1109/IZS.2006.1649095.

[11] C. Alves and J.-C. Belfiore, "Lattices from maximal orders into quaternion algebras," *Journal of Pure and Applied Algebra*, vol. 219, no. 4, pp. 687–702, 2015, doi: 10.1016/j.jpaa.2014.04.025.

[12] B. A. Sethuraman and F. Oggier, "Constructions of orthonormal lattices and quaternion division algebras for totally real number fields," pp. 138–147, 2007, doi: 10.1007/978-3-540-77224-8_18.

[13] E. Bayer-Fluckiger, "Ideal lattices," *A panorama of number theory or the view from Baker's Garden (Zurich, 1999)*, pp. 168–184, 2002.

[14] F.-T. Tu and Y. Yang, "Lattice packing from quaternion algebras," *Algebraic Number Theory and Related Topics*, 2012.

[15] C. W. O. Benedito, C. Alves, N. G. Brasil Jr., and S. I. R. Costa, "Algebraic construction of dense lattices via maximal quaternion orders," *preprint*, 2017.

[16] E. Malekian and A. Zakerolhosseini, "A non-associative lattice-based public key cryptosystem," *Security and Communication Networks*, vol. 5, no. 2, pp. 145–163, 2012, doi: 10.1002/sec.297.

[17] D. A. Marcus, *Number fields*. Springer, vol. 1995, doi: 10.1007/978-1-4684-9356-6.

[18] I. Stewart and D. O. Tall, *Algebraic number theory*, 1979.

[19] J. Baez, "The octonions," *Bulletin of the American Mathematical Society*, vol. 39, no. 2, pp. 145–205, 2002, doi: 10.1090/S0273-0979-01-00934-X.

[20] C. Waldner, "Cycles and the cohomology of arithmetic subgroups of the exceptional group g_2," Ph.D. dissertation, uniwien, 2008.

[21] F. Van der Blij and T. Springer, "The arithmetics of octaves and of the group g2," in *Indagationes Mathematicae (Proceedings)*, vol. 62. Elsevier, 1959, pp. 406–418.

[22] R. E. M. Nebe, G. and N. J. A. Sloane, "A simple construction for the barnes-wall lattices," pp. 333–342, 2002, doi: 10.1007/978-1-4615-0895-3_19.

[23] T. J. Rivlin, "Chebyshev polynomials from approximation theory to algebra and number theory," *Pure and Applied Mathematics, John Wiley & Sons, New York, NY, USA*, 1990, doi: 10.1112/blms/23.3.311.

[24] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of computation*, vol. 44, no. 170, pp. 463–471, doi: 10.2307/2007966.

[25] G. C. Jorge, A. A. de Andrade, S. I. R. Costa, and J. E. Strapasson, "Algebraic constructions of densest lattices," *Journal of Algebra*, vol. 429, pp. 218–235, 2015, doi: 10.1016/j.jalgebra.2014.12.044.

[26] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 7.5.1)*, 2017. [Online]. Available: http://www.sagemath.org

[27] P. Q. Nguyen and B. Vallée, "The lll algorithm," *Information Security and Cryptography*, 2010, doi: 10.1007/978-3-642-02295-1.

[28] Wolfram Research, Inc., "Mathematica 11." [Online]. Available: https://www.wolfram.com

Nelson G. Brasil Junior holds a bachelor's degree in Applied Mathematics from Institute of Mathematics, Statistics and Computer Science (IMECC), University of Campinas (Unicamp) (2008–2011), Master in Applied Mathematics(2012–2014) and he is currently a PhD student at the same institute (2014–present). He has experience in Applied Mathematics with emphasis in Discrete Mathematics, Lattices and Coding Theory.

Cintya W. O. Benedito holds a bachelor's degree in Pure Mathematics from the São Paulo State University (UNESP) at the Institute of Biosciences Humanities and Exact Sciences (IBILCE), São José do Rio Preto (2004-2007), Master in Mathematics from the same institute (2008 – 2010), PhD in Electrical Engineering from School of Electrical and Computer Engineering (FEEC), University of Campinas (Unicamp) (2010 – 2014) and Post-Doctorate in Applied Mathematics at Institute of Mathematics, Statistics and Computer Science (IMECC), University of Campinas (Unicamp). She is currently Assistant Professor at the ão Paulo State University (UNESP), Campus of São João da Boa Vista. She has experience in Mathematics and Telecommunication, with emphasis on Codes and Lattice Theory, Algebraic Numbers Theory, Hyperbolic Geometry and Quaternary Algebra.

Sueli I. R. Costa Professor at the Institute of Mathematics, Statistics and Computer Science (IMECC), University of Campinas (Unicamp), received her Ph.D. from the same university and had her post-doctoral studies at the Institute for Advanced Study, Princeton. Her activities related to research development include the coordination of the thematic project Information Theory and Coding–FAPESP, invited short term visit to the Bernoulli Intertfacultaire Centre, EPFL, Lausanne, to the AT & T Research Lab NJ and serving as a co-chair of the 2011 IEEE ITW, of the 2018 Latin America Week on Coding and Information and currently as the IEEE Information Society Brazil Chapter chair. Her research topics of interest include lattice codes and applications, discrete and continuous spherical codes, coding for storage and information geometry.