International Journal of Applied Mathematics

Volume 31 No. 1 2018, 63-71
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v31i1.6

E_8-LATTICE VIA THE CYCLOTOMIC FIELD $\mathbb{Q}(\xi_{24})$

C.C. Trinca Watanabe[1 §], J.-C. Belfiore[2],
E.D. De Carvalho[3], J. Vieira Filho[4]

[1]Department of Communications (DECOM)
Campinas State University
Campinas – SP, 13083-852, BRAZIL

[2]Department of Communications and Electronics
Télécom ParisTech
Paris, 75013, FRANCE

[3]Department of Mathematics
São Paulo State University
Ilha Solteira – SP, 15385-000, BRAZIL

[4]Telecommunications Engineering
São Paulo State University
São João da Boa Vista – SP, 13876-750, BRAZIL

Abstract: Lattices can be applied in different areas of research, particularly, they can be applied in information theory and encryption schemes. Signal constellations having lattice structure have been used as a support for signal transmission over the Gaussian and Rayleigh fading channels.

The problem to find a good signal constellation for Gaussian channels is associated to the search of lattices which present a good packing density, that is, dense lattices. In this way, we propose an algebraic framework to construct the dense lattice E_8 from the principal ideal $\Im = ((1 + \xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2)$ of the cyclotomic field $\mathbb{Q}(\xi_{24})$, where ξ_3 and ξ_{24} are the third and 24-th root of unity, respectively.

The advantage of obtaining lattices from this method is the identification of the lattice points with the elements of a number field. Consequently, it is possible to utilize some properties of number fields in the study of such lattices.

Received: December 8, 2017

§Correspondence author

AMS Subject Classification: 06B05, 06B10, 11R18, 13F10
Key Words: E_8-lattice; dense lattice, cyclotomic field, principal ideal

1. 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]. Usually the problem of finding good signal constellations for a Gaussian channel is associated to the search for lattices with high packing density [2]. On the other hand, for a Rayleigh fading channel, a design criterion obtained by minimizing the error probability at the receiver is strongly related to what has been named lattice diversity and minimum product distance [1],[3].

For general lattices the packing density and the minimum product distance are usually hard to calculate [4]. Nevertheless, those parameters can be obtained in some cases, when ideal lattices associated to number fields are used [5].

In the literature, there exist several ways to construct algebraically and geometrically lattices. Algebraic constructions enable the computation of invariants such as packing density (density) and minimum product distance which are important for applications related to error correcting codes and encryption schemes based on lattices.

The E_8-lattice is the densest lattice and the best quantizer in dimension 8 [6]. In [7], the author proposes the trace construction to obtain the E_8-lattice via the ring of integers of the cyclotomic fields $\mathbb{Q}(\xi_{24})$, $\mathbb{Q}(\xi_{20})$ and $\mathbb{Q}(\xi_{15})$, where ξ_{24}, ξ_{20} and ξ_{15} are the 24, 20 and 15-th roots of unity, respectively. In [8], the E_8-lattice is constructed as a full diversity ideal lattice via some subfield of cyclotomic field. In [9], the E_8-lattice is constructed as a space-time code with full diversity and high coding gain. In [10], the authors propose four new constructions of the E_8-lattice from left ideals of maximal orders of some quaternion algebras with centers $\mathbb{Q}(\sqrt{-d})$, $d = 1, 2, 3, 7$, and, in [11], the E_8-lattice is constructed via an order in an octonion algebra over a totally real number field.

In this work we present a new construction of the dense lattice E_8. In this construction, we obtain the E_8-lattice via the principal ideal $\Im = ((1 + \xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2)$ of the cyclotomic field $\mathbb{Q}(\xi_{24})$, where ξ_3 and ξ_{24} are the third and 24-th root of unity, respectively.

2. Lattice Theory

Lattices have been very useful in applications in communication theory and, in this work, we have the construction of the dense lattice E_8 via the cyclotomic field $\mathbb{Q}(\xi_{24})$. In this section we present basic concepts of the lattice theory.

Definition 1. Let $v_1, v_2, \ldots, v_m$ be a set of linearly independent vectors in $\mathbb{R}^n$ such that $m \leq n$. The set of the points

$$\Lambda = \{x = \textstyle\sum_{i=1}^{m} \lambda_i v_i, \text{ where } \lambda_i \in \mathbb{Z}\}$$

is called a *lattice* of rank m and $\{v_1, v_2, \ldots, v_m\}$ is called a basis of the lattice.

So we have that a real *lattice* Λ is simply a discrete set of vectors (points (n-tuples)) in real Euclidean n-space $\mathbb{R}^n$ that forms a group under ordinary vector addition, i.e., the sum or difference of any two vectors in Λ is in Λ. Thus Λ necessarily includes the all-zero n-tuple 0 and if λ is in Λ, then so is its additive inverse $-\lambda$.

As an example, the set $\mathbb{Z}$ of all integers is the only one-dimensional real lattice, up to scaling, and the prototype of all lattices. The set $\mathbb{Z}^n$ of all integer n-tuples is an n-dimensional real lattice, for any n, and its corresponding $\frac{n}{2}$-dimensional complex lattice is given by $\mathbb{Z}[i]^{\frac{n}{2}}$.

A sublattice Λ' of Λ is a subset of the points of Λ which is itself an n-dimensional lattice. The sublattice induces a partition Λ/Λ' of Λ into $|\Lambda/\Lambda'|$ cosets of Λ', where $|\Lambda/\Lambda'|$ is the order of the partition.

The coset code $\mathcal{C}(\Lambda/\Lambda'; C)$ is the set of all sequences of signal points that lie within a sequence of cosets of Λ' that could be specified by a sequence of coded bits from C. Some lattices, including the most useful ones, can be generated as lattice codes $\mathcal{C}(\Lambda/\Lambda'; C)$, where C is a binary block code. If C is a convolutional encoder, then $\mathcal{C}(\Lambda/\Lambda'; C)$ is a trellis code [12].

A lattice code $\mathcal{C}(\Lambda/\Lambda'; C)$, where C is a binary block code, is defined as the set of all coset leaders in Λ/Λ', i.e.,

$$\mathcal{C}(\Lambda/\Lambda'; C) = \Lambda \bmod \Lambda' = \{\lambda \bmod \Lambda' \ : \ \lambda \in \Lambda\}.$$

Definition 2. The parallelotope formed by the points

$$\theta_1 v_1 + \cdots + \theta_m v_m, \text{ where } 0 \leq \theta_i < 1,\ i = 1, \ldots, m,$$

is called a fundamental parallelotope or fundamental region of the lattice.

Definition 3. A sphere packing is a distribution of spheres in $\mathbb{R}^n$ that have the same radius and the intersection of two of them is, at most, formed by one point. A lattice packing is a sphere packing in which the set of the centers of the spheres form a lattice Λ in $\mathbb{R}^n$.

Definition 4. Let Λ be a lattice. The packing density of Λ is defined by

$$\triangle(\Lambda) = \frac{\textit{volume of the region covered by an sphere}}{\textit{volume of the fundamental region}}.$$

One of the problems related to sphere packing of a lattice in $\mathbb{R}^n$ is to find a sphere packing which has the greatest packing density. It is known and proved that the packing density of the lattices $A_1, A_2, D_3, D_4, D_5, E_6, E_7, E_8$ and Λ_{24} in dimensions from 1 through 8 and 24, respectively, is great, that is, they are dense lattices in their dimension.

Besides the lattice E_8 be the densest lattice in dimension 8, it is the only even and unimodular lattice in its dimension. The lattice E_8 (E_8-lattice) is an 8-dimensional lattice defined by

$$E_8 = \{(x_1, \ldots, x_8) \mid \text{either } x_i \in \mathbb{Z} \text{ or } x_i \in \mathbb{Z} + \tfrac{1}{2},$$
$$\forall\, i = 1, \ldots, 8, \text{ and } \textstyle\sum_{i=1}^{8} x_i \equiv 0 \pmod 2\}.$$

3. Construction of the Dense Lattice E_8 from an Ideal of the Cyclotomic Field $\mathbb{Q}(\xi_{24})$

In this section we show that the dense lattice E_8 can be obtained from an ideal of the cyclotomic field $\mathbb{Q}(\xi_{24})$. Therefore we consider the following Galois extensions:

$$\begin{array}{c} \mathbb{Q}(\xi_{24}) \\ \Big| 4 \\ \mathbb{Q}(\xi_3) \\ \Big| 2 \\ \mathbb{Q} \end{array}$$

Let $\xi_3 = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{3}i}{2}$ and $\xi_{24} = e^{\frac{2\pi i}{24}}$ be the third root of unity and the 24-th root of unity, respectively. We can notice that $\xi_3^2 + \xi_3 + 1 = 0$ and $\xi_3^2 = -\xi_{24}^4$, then we have $\xi_{24}^4 + \xi_3^2 = 0$. Observe that $x^2 + x + 1$ and

$x^4 + \xi_3^2$ are monic and irreducible polynomials over $\mathbb{Q}$ and $\mathbb{Q}(\xi_3)$, respectively. As $[\mathbb{Q}(\xi_{24}) : \mathbb{Q}] = \phi(24) = 8$, where ϕ is the Euler function, and $[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2$, then we have $[\mathbb{Q}(\xi_{24}) : \mathbb{Q}(\xi_3)] = 4 = n$.

Since $\{1, \xi_{24}, \ldots, \xi_{24}^7\}$ is an integral basis of $\mathbb{Z}[\xi_{24}]$, the ring of integers of $\mathbb{Q}(\xi_{24})$, and $\xi_{24} = -\xi_3^2$, it follows that $\mathbb{Z}[\xi_{24}]$ is a free $\mathbb{Z}[\xi_3]$-module of rank 4 and

$$\{1, \xi_{24}, \xi_{24}^2, \xi_{24}^3\}$$

is a $\mathbb{Z}[\xi_3]$-basis of $\mathbb{Z}[\xi_{24}]$.

Let $2 + \xi_3 = \sqrt{-3} = i\sqrt{3} \in \mathbb{Z}[\xi_3]$, where $\mathbb{Z}[\xi_3]$ is the ring of integers of $\mathbb{Q}(\xi_3)$. Observe that $N_{\mathbb{Q}(\xi_3)/\mathbb{Q}}(2 + \xi_3) = (2 + \xi_3)(2 + \xi_3^2) = 4 + 2\xi_3^2 + 2\xi_3 + \xi_3^3 = 2(\xi_3^2 + \xi_3) + 5 = -2 + 5 = 3$, since $\xi_3^2 + \xi_3 + 1 = 0$, and $(2+\xi_3)^2 = -3\xi_3^2 = 3(-\xi_3^2)$. Then 3 is totally ramified in $\mathbb{Q}(\xi_3)$.

Therefore we have that 3 is totally ramified in $\mathbb{Q}(\xi_{24})$ and $3\mathbb{Z}[\xi_{24}] = (3) = \Im^8$, where $\Im = ((1+\xi_3)\xi_{24} + \xi_3\xi_{24}^2 + \xi_3\xi_{24}^3)$. Then we have that $\Im$ is the principal ideal in $\mathbb{Z}[\xi_{24}]$ generated by $(1 + \xi_3)\xi_{24} + \xi_3\xi_{24}^2 + \xi_3\xi_{24}^3$.

Observe that $\xi_{24} \in \mathbb{Z}[\xi_{24}]$ and $(1+\xi_3)\xi_{24} + \xi_3\xi_{24}^2 + \xi_3\xi_{24}^3 = \xi_{24}((1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2)$. Since ξ_{24} is a unity in $\mathbb{Z}[\xi_{24}]$, it follows that the principal ideal $\Im$ is also generated by $\mu = (1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2$. Then $\Im = ((1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2) = (\mu)$.

The next theorem shows us that the dense lattice E_8 can be obtained from the principal ideal $\Im = ((1+\xi_3) + \xi_3\xi_{24} + \xi_{24}\xi_{24}^2)$ via the cyclotomic field $\mathbb{Q}(\xi_{24})$.

Theorem 5. *The dense lattice E_8 can be constructed from the principal ideal $\Im = ((1 + \xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2)$ in $\mathbb{Z}[\xi_{24}]$, where $\mathbb{Z}[\xi_{24}]$ is the ring of integers of the cyclotomic field $\mathbb{Q}(\xi_{24})$.*

Proof. We have $\xi_{24}^4 = -\xi_3^2$, $\frac{\mathbb{Z}[\xi_3]}{(2+\xi_3)\mathbb{Z}[\xi_3]} \simeq \mathbb{F}_3 = \{0, 1, -1\}$ and $\xi_3^2 \equiv 1$ (modulo $(2 + \xi_3)$), since $\xi_3^2 = -(1 + \xi_3) \equiv 1$ (modulo $(2 + \xi_3)$).

Let $v \in \mathbb{Z}[\xi_{24}]$, then $v = a_0 + a_1\xi_{24} + a_2\xi_{24}^2 + a_3\xi_{24}^3$, where $a_k \in \mathbb{Z}[\xi_3]$, $k = 0, 1, 2, 3$, and $\xi_{24}^4 = -\xi_3^2$.

Since $\frac{\mathbb{Z}[\xi_3]}{(2+\xi_3)\mathbb{Z}[\xi_3]} \simeq \mathbb{F}_3 = \{0, 1, -1\}$ and $a_k \in \mathbb{Z}[\xi_3]$, we have $a_k = (2+\xi_3)b_k + c_k$, where $b_k \in \mathbb{Z}[\xi_3]$ and $c_k = 0, 1$ or -1. Thereby,

$$v = ((2+\xi_3)b_0 + c_0) + ((2+\xi_3)b_1 + c_1)\xi_{24} + ((2+\xi_3)b_2 + c_2)\xi_{24}^2 + ((2+\xi_3)b_3 + c_3)\xi_{24}^3$$

$$= [(2+\xi_3)b_0 + (2+\xi_3)b_1\xi_{24} + (2+\xi_3)b_2\xi_{24}^2 + (2+\xi_3)b_3\xi_{24}^3] + [c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3]$$

$$= (2 + \xi_3)(b_0 + b_1\xi_{24} + b_2\xi_{24}^2 + b_3\xi_{24}^3) + (c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3).$$

Let $w = (2+\xi_3)(b_0 + b_1\xi_{24} + b_2\xi_{24}^2 + b_3\xi_{24}^3)$, then $w \in (2+\xi_3)\mathbb{Z}[\xi_{24}] \subset \mathbb{Z}[\xi_{24}]$ and

$$v = w + (c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3), \text{ where } c_k \in \mathbb{F}_3 = \{0, 1, -1\}.$$

Therefore $v - w = c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3$, where $c_k \in \mathbb{F}_3 = \{0, 1, -1\}$.

We have $\xi_{24}^4 = -\xi_3^2 \equiv (-1)$ (modulo $(2 + \xi_3)$), then $\xi_{24}^4 = -1$ over the field $\mathbb{F}_3 = \{0, 1, -1\}$. Let $x = \xi_{24}$, then $x^4 = -1$ over $\mathbb{F}_3$ and it follows that $v(x) - w(x) = c_0 + c_1x + c_2x^2 + c_3x^3$ (modulo $x^4 - 1$).

Since $3 < 4$, we can conclude that $[v(x) - w(x)] = \{c_0 + c_1x + c_2x^2 + c_3x^3$, where $c_k \in \mathbb{F}_3 = \{0, 1, -1\}\} \simeq \mathbb{F}_3^4$.

By using the fact that $v \in \mathbb{Z}[\xi_{24}]$ is an arbitrary element, it follows that $\frac{\mathbb{Z}[\xi_{24}]}{(2+\xi_3)\mathbb{Z}[\xi_{24}]} \simeq \mathbb{F}_3^4$. Besides, since $\frac{\mathbb{Z}[\xi_3]}{(2+\xi_3)\mathbb{Z}[\xi_3]} \simeq \mathbb{F}_3$, we have $\mathbb{Z}[\xi_3]^4 = (2 + \xi_3)\mathbb{Z}[\xi_3]^4 + (4, 4, 1)_{\mathbb{F}_3}$, where $C_0 = (4, 4, 1)_{\mathbb{F}_3}$ is the universal code. Therefore $\mathbb{Z}[\xi_{24}] \simeq \mathbb{Z}[\xi_3]^4$.

Now observe that $\Im = (\mu) = ((1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2) = \{((1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2)(a_0 + a_1\xi_{24} + a_2\xi_{24}^2 + a_3\xi_{24}^3)$, where $a_k \in \mathbb{Z}[\xi_3]$, $k = 0, 1, 2, 3$, and $\xi_{24}^4 = -\xi_3^2$ over $\mathbb{Q}(\xi_3)\}$.

Let $u \in \Im$, then $u = \mu(a_0 + a_1\xi_{24} + a_2\xi_{24}^2 + a_3\xi_{24}^3)$, where $a_k \in \mathbb{Z}[\xi_3]$, $k = 0, 1, 2, 3$, and $\xi_{24}^4 = -\xi_3^2 \equiv (-1)$ (modulo $(2 + \xi_3)$).

Since $\frac{\mathbb{Z}[\xi_3]}{(2+\xi_3)\mathbb{Z}[\xi_3]} \simeq \mathbb{F}_3 = \{0, 1, -1\}$ and $a_k \in \mathbb{Z}[\xi_3]$, we have $a_k = (2+\xi_3)b_k + c_k$, where $b_k \in \mathbb{Z}[\xi_3]$ and c_k=0,1 or -1. Therefore,

$$u = \mu[((2+\xi_3)b_0+c_0)+((2+\xi_3)b_1+c_1)\xi_{24}+((2+\xi_3)b_2+c_2)\xi_{24}^2+((2+\xi_3)b_3+c_3)\xi_{24}^3)]$$

$$= \mu[(2+\xi_3)b_0+(2+\xi_3)b_1\xi_{24}+(2+\xi_3)b_2\xi_{24}^2+(2+\xi_3)b_3\xi_{24}^3]+\mu[c_0+c_1\xi_{24}+c_2\xi_{24}^2+c_3\xi_{24}^3]$$

$$= \mu(2 + \xi_3)(b_0 + b_1\xi_{24} + b_2\xi_{24}^2 + b_3\xi_{24}^3) + \mu(c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3)$$

$$= (2 + \xi_3)\mu(b_0 + b_1\xi_{24} + b_2\xi_{24}^2 + b_3\xi_{24}^3) + \mu(c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3).$$

Let $w_1 = (2+\xi_3)\mu(b_0+b_1\xi_{24}+b_2\xi_{24}^2+b_3\xi_{24}^3)$. Since $\xi_{24}^4 = -\xi_3^2$ and $b_k \in \mathbb{Z}[\xi_3]$, we have $w_1 \in (2 + \xi_3)\mathbb{Z}[\xi_{24}] \subset \mathbb{Z}[\xi_{24}]$, where $(2 + \xi_3)\mathbb{Z}[\xi_{24}] \simeq (2 + \xi_3)\mathbb{Z}[\xi_3]^4$, and $u = w_1 + \mu(c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3)$, where $c_k \in \mathbb{F}_3 = \{0, 1, -1\}$.

Observe that $\frac{\mathbb{Z}[\xi_3]}{(2+\xi_3)\mathbb{Z}[\xi_3]} \simeq \mathbb{F}_3 = \{0, 1, -1\}$ and let σ be an isomorphism between $\mathbb{Z}[\xi_{24}]$ and the $\mathbb{Z}[\xi_3]^4$-lattice. Thereby

$$u - w_1 = \mu(c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3)$$
$$= ((1 + \xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2)(c_0 + c_1\xi_{24} + c_2\xi_{24}^2 + c_3\xi_{24}^3),$$

where $c_k \in \mathbb{F}_3 = \{0, 1, -1\}$.

As $\mu = ((1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2) \in \mathbb{Z}[\xi_{24}]$, then we have

$$((1+\xi_3) + \xi_3\xi_{24} + \xi_3\xi_{24}^2) \equiv (-1 + \xi_{24} + \xi_{24}^2) \text{ (modulo } (2+\xi_3)),$$

since $(1+\xi_3) \equiv -1$ (modulo $(2+\xi_3)$) and $\xi_3 \equiv 1$ (modulo $(2+\xi_3)$).

We have $\xi_{24}^4 = -\xi_3^2 \equiv (-1)$ (modulo $(2+\xi_3)$), then $\xi_{24}^4 = (-1)$ over the field $\mathbb{F}_3 = \{0, 1, -1\}$. Let $x = \xi_{24}$, then $x^4 = (-1)$ $(x^4 + 1 = 0)$ over $\mathbb{F}_3$ and it follows that

$$u(x) - w_1(x) = (x^2 + x - 1)(c_0 + c_1x + c_2x^2 + c_3x^3) \text{ (modulo } x^4 + 1).$$

So we can conclude that

$$[u(x) - w_1(x)] = \{(x^2 + x - 1)(c_0 + c_1x + c_2x^2 + c_3x^3) \\ \text{(modulo } x^4 + 1) \ ; \ c_k \in \mathbb{F}_3\} = (x^2 + x - 1),$$

which corresponds to the ideal in $\frac{\mathbb{F}_3[x]}{(x^4+1)}$ generated by $(x^2 + x - 1)$.

Therefore, we have $u \in \Im = (\mu)$ an arbitrary element and, after the quotient, we have the identification with the ideal in $\frac{\mathbb{F}_3[x]}{(x^4+1)}$ generated by $(x^2 + x - 1)$. Then it follows that $\sigma(\Im) = (2+\xi_3)\mathbb{Z}[\xi_3]^4 + C_1$, where C_1 is the negacyclic code called *Tetracode* which has dimension 2 and generator polynomial $x^2 + x - 1$. The Tetracode C_1 is given by

$$C_1 = \{(0,0,0,0); (0,-1,1,1); (0,1,-1,-1); (1,-1,-1,0);$$

$$(-1,1,1,0); (1,1,0,1); (1,0,1,-1); (-1,-1,0,-1); (-1,0,-1,1)\}$$

and its respective generator matrix is given by

$$\begin{pmatrix} 1 & -1 & -1 & 0 \\ 0 & -1 & 1 & 1 \end{pmatrix}.$$

Consequently, by [2], page 200, we have

$$\sigma(\Im) = (2+\xi_3)\mathbb{Z}[\xi_3]^4 + C_1 = (2+\xi_3)\mathbb{Z}[\xi_3]^4 + (4,2,3)_{\mathbb{F}_3} = E_8.$$

Thereby we can conclude that the lattice E_8 can be obtained from an ideal via the cyclotomic field $\mathbb{Q}(\xi_{24})$. □

Then we can conclude that the dense lattice E_8 can be constructed from an ideal via the cyclotomic field $\mathbb{Q}(\xi_{24})$.

4. Conclusion

In [7], the author proposes the trace construction to obtain the E_8-lattice via the ring of integers of the cyclotomic field $\mathbb{Q}(\xi_{24})$, where ξ_{24} is the 24-th root of unity. In this work, we present a way to construct the dense E_8-lattice from a principal ideal of the cyclotomic field $\mathbb{Q}(\xi_{24})$.

Acknowledgment

This work has been supported by the following Brazilian Agencies: FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) under grant No. 2013/03976-9 and CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) under grant No. 6562-10-8.

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*, **42**, No 2 (2006), 502-517.

[2] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York (1999).

[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*, **50**, No 4 (2004), 702-714.

[4] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Springer International Ser. in Engineering and Computer Science, Kluwer Academic Publishers (2002).

[5] F. Oggier and E. Viterbo, Algebraic number theory and code design for Rayleigh fading channels, *Foundations and Trends in Communications and Information Theory*, **1**, No 3 (2004), 333-415.

[6] J.H. Conway and N.J.A. Sloane, Fast quantizing and decoding algorithms for lattice quantizers and codes, *IEEE Transactions on Information Theory*, **28**, No 2 (1982), 227-232.

[7] E. Bayer-Fluckiger, *Lattices and Number Fields*, Contemporary Mathematics (1999).

[8] E. Bayer-Fluckiger and I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, *Archiv der Mathematik*, **86**, No 3 (2006), 217-225.

[9] C. Hollanti, J. Lahtonen and H.-f.(F.) Lu, Maximal orders in the design of dense space-time lattice codes, *IEEE Transactions on Information Theory*, **54**, No 10 (2008), 4493-4510.

[10] C. Alves and J.-C. Belfiore, Lattices from maximal orders into quaternion algebras, *Journal of Pure and Applied Algebra*, (2014), 1-16.

[11] N.G. Brasil Jr., C.W.O. Benedito and S.I.R. Costa, Reticulados associados a álgebra dos octônios, In: *XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT2017)* (2017).

[12] G.D. Forney, Coset codes - Part I: Introduction and geometrical classification, *IEEE Transactions on Information Theory*, **34**, No 5 (1998), 1123-1151.