Tendências em Matemática Aplicada e Computacional, **20**, N. 3 (2019), 445-456

www.scielo.br/tema
doi: 10.5540/tema.2019.020.03.0445

Rotated $\mathbb{Z}^n$-Lattices via Real Subfields of $\mathbb{Q}(\zeta_{2^r})$

A. A. ANDRADE[1*] and J. C. INTERLANDO[2]

Received on September 20, 2018 / Accepted on March 14, 2019

ABSTRACT. A method for constructing rotated $\mathbb{Z}^n$-lattices, with n a power of 2, based on totally real subfields of the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$, where $r \geq 4$ is an integer, is presented. Lattices exhibiting full diversity in some dimensions n not previously addressed are obtained.

Keywords: lattices, cyclotomic fields, modulation design, fading channels, minimum product distance.

1 INTRODUCTION

Ring theory and algebric number theory have long shown to be useful tools in the theory of information and coding [8] and [2]. In particular, lattices (discrete subgroups of the Euclidean n-space $\mathbb{R}^n$) have played a relevant role in code design for different types of channels, see for example [12], [5], [6], and [9]. One central problem in the design of signal constellations for fading channels is to construct lattices from totally real number fields with maximal minimum product distance. Using number-theoretic methods, Andrade et al. [1] and Bayer-Fluckiger et al. [12] presented constructions of algebraic lattices with full diversity and gave closed-form expressions for their minimum product distance using the corresponding algebraic properties.

The n-dimensional integer lattice, denoted by $\mathbb{Z}^n$, consists of the set of points in $\mathbb{R}^n$ whose coordinates are all integers. In [1], for any integer $r \geq 3$, rotated $\mathbb{Z}^n$-lattices, $n = 2^{r-2}$, were constructed from $\mathbb{Q}(\zeta_{2^r})^+ = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, the maximal real subfield of $\mathbb{Q}(\zeta_{2^r})$, where ζ_{2^r} is a primitive 2^r-th root of unity. In this work, we extend the method in [1] by considering a particular subfield of $\mathbb{Q}(\zeta_{2^r})^+$, namely, $\mathbb{Q}(\zeta_{2^r}^2 + \zeta_{2^r}^{-2})$, to construct lattices in dimensions that are powers of 2.

This paper is organized as follows: In Section 2, notions and results from algebraic number theory that are used in the work are reviewed. In Section 3, rotated $\mathbb{Z}^n$-lattices constructed from the totally real fields $\mathbb{Q}(\zeta_{2^r}^{2^k} + \zeta_{2^r}^{-2^k})$, with $k = 0, 1$, are presented and their minimum product distances are computed. In Section 4, the concluding remarks are drawn.

*Corresponding author: Antonio A. Andrade – E-mail: antonio.andrade@unesp.br – https://orcid.org/0000-0001-6452-2236

[1]Departamento de Matemática, Universidade do Estado de São Paulo, Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Campus São José do Rio Preto, São José do Rio Preto-SP, Brazil E-mail: antonio.andrade@unesp.br

[2]Department of Mathematics & Statistics, San Diego State University, San Diego, California, USA E-mail: interlan@sdsu.edu

2 NUMBER FIELDS BACKGROUND

If $\mathbb{F}$ be a number field of degree d (notation: $[\mathbb{F}:\mathbb{Q}]=d$), then $\mathbb{F}=\mathbb{Q}(\omega)$, for some $\omega\in\mathbb{C}$, which is a root of a monic irreducible polynomial $p(x)\in\mathbb{Z}[x]$. The d distinct roots of $p(x)$, namely, $\omega_1,\omega_2,\ldots,\omega_d$, are the conjugates of ω. The *embeddings* of $\mathbb{F}$ in $\mathbb{C}$ are the field homomorphisms $\tau_i:\mathbb{F}\to\mathbb{C}$ given by $\tau_i(\omega)=\omega_i$ and $\tau_i(a)=a$ for all $a\in\mathbb{Q}$, for $i=1,2,\ldots,d$. The latter set of embeddings is denoted by $Emb(\mathbb{F},\mathbb{C})$. If $\tau_i(\mathbb{F})\subseteq\mathbb{R}$, for $i=1,\ldots,d$, we say that $\mathbb{F}$ is totally real. The set $\{\tau\in Emb(\mathbb{F},\mathbb{C})\,|\,\tau(\mathbb{F})=\mathbb{F}\}$ is a group under composition, called the *Galois group* of $\mathbb{F}$ over $\mathbb{Q}$ and denoted by $Gal(\mathbb{F}/\mathbb{Q})$. The *norm* and the *trace* of an element $\alpha\in\mathbb{F}$ are defined, respectively, as the rational numbers

$$\mathbb{N}_{\mathbb{F}/\mathbb{Q}}(\alpha)=\prod_{i=1}^{n}\tau_i(\alpha)\ \text{ and }\ Tr_{\mathbb{F}/\mathbb{Q}}(\alpha)=\sum_{i=1}^{n}\tau_i(\alpha).$$

The set

$$\{\gamma\in\mathbb{F}\,|\,\exists m\in\mathbb{Z}_{>0}\text{ and }a_0,a_1,\ldots,a_{m-1}\in\mathbb{Z}:\gamma^m+a_{m-1}\gamma^{m-1}+\cdots+a_1\gamma+a_0=0\}$$

is a ring, called the *ring of integers* of $\mathbb{F}$ and denoted by $\mathfrak{O}_{\mathbb{F}}$; moreover, the latter is a $\mathbb{Z}$-module and it has a basis $\{\alpha_1,\ldots,\alpha_d\}$ over $\mathbb{Z}$, called an *integral basis* for $\mathbb{F}$. The *discriminant* of $\mathbb{F}$, denoted by $\Delta_{\mathbb{F}}$, is the rational integer given by $\det(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j=1}^{d}$.

Theorem 1. *[14, Ch. 2] If $L=\mathbb{Q}(\zeta_{2^r})$, with $r\geq 3$, then*

1. *$[L:\mathbb{Q}]=\phi(2^r)=2^{r-1}$, where ϕ denotes Euler's totient function;*
2. *$\mathfrak{O}_L=\mathbb{Z}[\zeta_{2^r}]$ and $\{1,\zeta_{2^r},\zeta_{2^r}^2,\ldots,\zeta_{2^r}^{2^{r-1}-1}\}$ is an integral basis for L;*
3. *$[L:L^+]=2$ and $[L^+:\mathbb{Q}]=2^{r-2}$, where $L^+=\mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})$ is the maximal real subfield of L;*
4. *$\mathfrak{O}_{L^+}=\mathbb{Z}[\zeta_{2^r}+\zeta_{2^r}^{-1}]$ and $\{1,\zeta_{2^r}+\zeta_{2^r}^{-1},\zeta_{2^r}^2+\zeta_{2^r}^{-2},\ldots,\zeta_{2^r}^{2^{r-2}-1}+\zeta_{2^r}^{-2^{r-2}+1}\}$ is an integral basis for L^+.*

Corollary 2. *The degree of $\mathbb{Q}(\zeta_{2^r}^2+\zeta_{2^r}^{-2})$ over $\mathbb{Q}$ equals 2^{r-3}, with $r\geq 4$.* **Proof.** Observe that $\zeta_{2^r}^2=\zeta_{2^{r-1}}$ and use part 3 of Theorem 1. □

Corollary 3. *If $K=\mathbb{Q}(\zeta_{2^r}^2+\zeta_{2^r}^{-2})$, with $r\geq 4$, then*

1. *the ring of integers of K, namely, $\mathfrak{O}_K$, is given by $\mathfrak{O}_K=\mathbb{Z}[\zeta_{2^r}^2+\zeta_{2^r}^{-2}]$;*
2. *$\{1,\zeta_{2^r}^2+\zeta_{2^r}^{-2},\ldots,\zeta_{2^r}^{2(n-1)}+\zeta_{2^r}^{-2(n-1)}\}$ is an integral basis for K, with $n=2^{r-3}$.*

Proof. Observe that $\zeta_{2^r}^2=\zeta_{2^{r-1}}$ and use part 4 of Theorem 1. □

Proposition 4. *[13, Theorem 9.12, p. 364] The order of* 5 *modulo* 2^r *is* 2^{r-2}.

$Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{r-2}\mathbb{Z})$ and is of order 2^{r-1} [14, Theorem 2.5, p. 11]. For any odd integer i, let σ_i be the automorphism of $\mathbb{Q}(\zeta_{2^r})$ given by $\sigma_i(\zeta_{2^r}) = \zeta_{2^r}^i$. Furthermore, let $\langle\sigma_i\rangle$ denote the cyclic subgroup of $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ generated by σ_i. The fixed field of $\langle\sigma_{-1}\rangle$ is $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$. Observe that $\zeta_{2^r}^{2^{r-2}} = \zeta_4$ is the imaginary unit and so the fixed field of $\langle\sigma_5\rangle$ is $\mathbb{Q}(\zeta_{2^r}^{2^{r-2}})$. With the latter two observations in mind, refer to Figure 1, where the group indicated along each line represents the Galois group of the respective field extension. By Galois theory and more specifically, by [10, Theorem 1.1, Ch. VI], $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})) = \langle\sigma_{-1}\rangle$ and $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}(\zeta_{2^r}^{2^{r-2}})) = \langle\sigma_5\rangle$; furthermore, by [10, Theorem 1.12, Ch. VI], it follows that $Gal(\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})/\mathbb{Q}) = \langle\sigma_5\rangle$. Lastly, by [10, Theorem 1.14, Ch. VI], it follows that $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}) = \langle\sigma_{-1}\rangle\langle\sigma_5\rangle$.

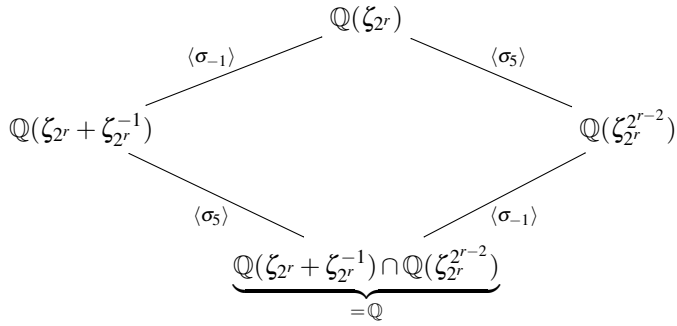

Figure 1: Relevant subfields of $\mathbb{Q}(\zeta_{2^r})$.

3 CONSTRUCTION OF IDEAL LATTICES

Let K be a totally real number field of degree n. An *ideal lattice* Λ is a lattice $(\mathscr{A}, q_\alpha)$, where $\mathscr{A} \subseteq \mathfrak{O}_K$ is an ideal,

$$q_\alpha : \mathscr{A} \times \mathscr{A} \to \mathbb{Z} \text{ is given by } q_\alpha(x,y) = Tr_{K/\mathbb{Q}}(\alpha xy), \text{ for all } x, y \in \mathscr{A},$$

and $\alpha \in K$ is totally positive, that is, $\sigma_i(\alpha) > 0$, for all $i = 1, 2, \ldots, n$. If $\{w_1, w_2, \ldots, w_n\}$ is a $\mathbb{Z}$-basis for $\mathscr{A}$, then the generator matrix R of Λ is given by

$$R = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(w_1) & \sqrt{\sigma_2(\alpha)}\sigma_2(w_1) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(w_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\sigma_1(\alpha)}\sigma_1(w_n) & \sqrt{\sigma_2(\alpha)}\sigma_2(w_n) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(w_n), \end{pmatrix}.$$

The Gram matrix of Λ is given by $G = RR^t = (Tr(\alpha w_i w_j))_{i,j=1}^n$, where R^t denotes the transpose of R.

Let $x=(x_1,\ldots,x_n)\in\mathbb{R}^n$ be an element of Λ. The *product distance* of x from the origin is defined as

$$d_p(x)=\prod_{i=1}^{n}|\,x_i\,|,$$

and the *minimum product distance* of Λ is defined as

$$d_{p,\min}(\Lambda)=\min_{x\in\Lambda,x\neq 0}d_p(x).$$

When $\mathscr{A}$ is a principal ideal of $\mathfrak{O}_K$, the minimum product distance of Λ is given by

$$d_{p,\min}(\Lambda)=\sqrt{\frac{\det(\Lambda)}{\Delta_K}},$$

where $\det(\Lambda)=\det G$, see [12, Theorem 1].

Let $\mathscr{A}$ and $\mathscr{A}'$ be two ideals in $\mathfrak{O}_K$. Lattices $(\mathscr{A},q)$ and $(\mathscr{A}',q')$ are said to be isomorphic (notation: $(\mathscr{A},q)\simeq(\mathscr{A}',q')$) [4] if there exists $\beta\in K\setminus\{0\}$ such that $\mathscr{A}'=\beta\mathscr{A}$ and $q'(\beta x,\beta y)=q(x,y)$, for all $x,y\in\mathscr{A}$.

3.1 Construction from the subfield $\mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})$

Let L be the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$ and $K=\mathbb{Q}(\theta)$, where $\theta=\zeta_{2^r}+\zeta_{2^r}^{-1}$ and where $r\geq 3$. Throughout this section, let $n=[K:\mathbb{Q}]=2^{r-2}$. From [3, Theorem 2.2], one has $\Delta_K=2^{(r-1)2^{r-2}-1}$. The lattices in this section will be built from the ring of integers of K, whose an integral basis is given by $\{1,\zeta_{2^r}+\zeta_{2^r}^{-1},\ldots,\zeta_{2^r}^{n-1}+\zeta_{2^r}^{-(n-1)}\}$.

Let $\Lambda=(\mathfrak{O}_K,q_\alpha)$ be an ideal lattice and c a positive integer. Since the Gram matrix of $(\sqrt{c}\mathbb{Z})^n$ is cI_n, a necessary but not sufficient condition for Λ to be isomorphic to $(\sqrt{c}\mathbb{Z})^n$, a scaled version of $\mathbb{Z}^n$, is that $\det(\Lambda)=c^n$, see [4, 12]. Thus, the first step when verifying whether $\Lambda\simeq\mathbb{Z}^n$ is to find $\alpha\in\mathfrak{O}_K$ such that $\mathbb{N}_{K/\mathbb{Q}}(\alpha)\Delta_K$ is a perfect nth power. Since

$$2\mathbb{Z}[\zeta_{2^r}]=(1-\zeta_{2^r})^{2^{r-1}}\mathbb{Z}[\zeta_{2^r}],$$

one has $\mathbb{N}_{L/\mathbb{Q}}(1-\zeta_{2^r})=2$. Using the transitivity of the norm, it follows that

$$\begin{aligned}2 &= \mathbb{N}_{L/\mathbb{Q}}(1-\zeta_{2^r})=\mathbb{N}_{K/\mathbb{Q}}(\mathbb{N}_{L/K}(1-\zeta_{2^r}))\\ &= \mathbb{N}_{K/\mathbb{Q}}((1-\zeta_{2^r})(1-\zeta_{2^r}^{-1}))=\mathbb{N}_{K/\mathbb{Q}}(2-(\zeta_{2^r}+\zeta_{2^r}^{-1}))=\mathbb{N}_{K/\mathbb{Q}}(2-\theta).\end{aligned}$$

Thus $\alpha=\mathbb{N}_{L/\mathbb{K}}(1-\zeta_{2^r})=2-\theta$ is an element of $\mathfrak{O}_K$ of norm 2.

Proposition 1. *[1] If $K=\mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})$, then*

$$Tr_{K/\mathbb{Q}}(\zeta_{2^r}^k+\zeta_{2^r}^{-k})=\begin{cases}0 & \text{if } \gcd(k,2^r)<2^{r-1};\\ -2^{r-1} & \text{if } \gcd(k,2^r)=2^{r-1};\\ 2^{r-1} & \text{if } \gcd(k,2^r)>2^{r-1}.\end{cases}$$

Proposition 2. *[1] Let $K=\mathbb{Q}(\theta)$, $e_0=1$ and $e_i=\zeta_{2^r}^i+\zeta_{2^r}^{-i}$, for $i=1,2,\ldots,n-1$.*

1. *If* $i = 0,1,\ldots,n-1$, *then* $q_\alpha(e_i,e_i) = \begin{cases} 2n & \text{if } i = 0; \\ 4n & \text{if } i \neq 0. \end{cases}$

2. *If* $i \neq 0$, *then* $q_\alpha(e_i,e_0) = \begin{cases} -2n & \text{if } i = 1; \\ 0 & \text{if } i \neq 1. \end{cases}$

3. *If* $i \neq 0$, $j \neq 0$ *and* $i \neq j$, *then* $q_\alpha(e_i,e_j) = \begin{cases} -2n & \text{if } \mid i-j \mid = 1; \\ 0 & \text{otherwise.} \end{cases}$

Corollary 3. *If* $Q(x,y) = \frac{1}{2^{r-1}} Tr_{K/\mathbb{Q}}(\alpha xy)$, *then the matrix of* Q *in the basis* $\{e_0,e_1,\ldots,e_{n-1}\}$ *is given by*

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

Proof. It follows directly by Proposition 2. □

Matrix G of Corollary 3 is the Gram matrix of a rotated $\mathbb{Z}^n$-lattice relative to the basis $\{w_0, w_2, \ldots, w_{n-1}\}$, where $w_0 = E_0$, $w_i = -E_{i-1} + E_i$, for $i = 1,2,\cdots,n-1$, and $\{E_j\}_{j=0}^{n-1}$ is the canonical basis of $\mathbb{Z}^n$. Thus $\varphi(e_i) = w_i$, for $i = 0,1,\ldots,n-1$, is an isomorphism of the $\mathbb{Z}^n$-lattice. The basis which corresponds to the canonical basis of $\mathbb{Z}^n$ through this isomorphism is then given by $f_i = \varphi^{-1}(E_i) = \sum_{j=0}^{i} e_j$, for $i = 0,1,\cdots,n-1$. Hence, it follows the following result.

Proposition 4. *Notation as above, if* $\{f_0,f_1,\ldots,f_{n-1}\}$ *is a* $\mathbb{Z}$*-basis for* $\mathfrak{O}_K$, *where* $f_i = \sum_{j=0}^{i} e_j$, *for* $i = 0,1,\ldots,n-1$, *then*

$$\frac{1}{2^{r-1}} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij},$$

i.e., the lattice $(\mathfrak{O}_K, \frac{1}{2^{r-1}} q_\alpha)$ *is isomorphic to* $\mathbb{Z}^n$.

Let $\{\sigma^0,\sigma,\ldots,\sigma^{n-1}\}$ be the Galois group of K over $\mathbb{Q}$. Thus, the generator matrix of the lattice associated to the ring of integers of K is given by

$$M = \begin{pmatrix} \sigma^0(e_0) & \cdots & \sigma^{n-1}(e_0) \\ \vdots & \ddots & \vdots \\ \sigma^0(e_{n-1}) & \cdots & \sigma^{n-1}(e_{n-1}) \end{pmatrix}.$$

Let

$$A = diag\left(\sqrt{\sigma^k(\alpha)}\right)_{k=0}^{n-1} \quad \text{and} \quad T = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix}.$$

The generator matrix of the rotated $\mathbb{Z}^n$-lattice is given by

$$R = \frac{1}{\sqrt{2^{r-1}}} TMA,$$

see [12, p. 705].

Example 3.1. *Let L be the cyclotomic field $\mathbb{Q}(\zeta_{2^3})$ and K its maximal real subfield $\mathbb{Q}(\zeta_{2^3}+\zeta_{2^3}^{-1})$. In this case, $\alpha = 2-(\zeta_{2^3}^3+\zeta_{2^3}^{-3})$, $\Delta_K = 2^3$ and $c = 2^2$. Considering the $\mathbb{Z}$-basis $\{e_0 = 1, e_1 = e_1 = \zeta_{2^3}+\zeta_{2^3}^{-1}\}$ for $\mathfrak{O}_K$ and $Q(x,y) = \frac{1}{2^2} q_\alpha(x,y) = \frac{1}{2^2} Tr_{K/\mathbb{Q}}(\alpha xy)$, it follows that the matrix of q_α is given by*

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

Matrix G is the Gram matrix of the rotated $\mathbb{Z}^2$-lattice relative to the basis $\{w_0, w_1\}$ with $w_0 = E_0$ and $w_1 = -E_0 + E_1$, where $\{E_0, E_1\}$ is the canonical basis of $\mathbb{Z}^2$. This implies that $\varphi(e_i) = w_i$, for $i = 0, 1$, is an isomorphism of the $\mathbb{Z}^2$-lattice. The basis which corresponds to the canonical basis of $\mathbb{Z}^2$ through this isomorphism is then given by $f_i = \varphi^{-1}(E_i)$, for $i = 0, 1$, i.e., $f_0 = e_0$ and $f_1 = e_0 + e_1$. Therefore, $\frac{1}{2^2} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij}$, i.e., the lattice $(\mathfrak{O}_K, \frac{1}{2^2} q_\alpha)$ is isomorphic to $\mathbb{Z}^2$.

Example 3.2. *Let L be the cyclotomic field $\mathbb{Q}(\zeta_{2^4})$ and K its maximal real subfield $\mathbb{Q}(\zeta_{2^4}+\zeta_{2^4}^{-1})$. In this case, $\alpha = \mathbb{N}_{L/K}(1-\zeta_{2^4})$, $\Delta_K = 2^{11}$ and $c = 2^6$. Considering the $\mathbb{Z}$-basis $\{e_0 = 1, e_1 = \zeta_{2^4}+\zeta_{2^4}^{-1}, e_2 = \zeta_{2^4}^2+\zeta_{2^4}^{-2}, e_3 = \zeta_{2^4}^3+\zeta_{2^4}^{-3}\}$ for $\mathfrak{O}_K$ and $Q(x,y) = \frac{1}{2^3} q_\alpha(x,y) = \frac{1}{2^3} Tr_{K/\mathbb{Q}}(\alpha xy)$, it follows that the matrix of q_α is given by*

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

The matrix G is the Gram matrix of the rotated $\mathbb{Z}^4$-lattice relative to the basis $\{w_0, w_1, w_2, w_3\}$, with $w_0 = E_0$, $w_1 = -E_0 + E_1$, $w_2 = -E_1 + E_2$ and $w_3 = -E_2 + E_3$, where $\{E_0, E_1, E_2, E_3\}$ is the canonical basis of $\mathbb{Z}^4$. This implies that $\varphi(e_i) = w_i$, for $i = 0, 1, 2, 3$, is an isomorphism on the $\mathbb{Z}^4$-lattice. The basis which corresponds to the canonical basis of $\mathbb{Z}^4$ through this isomorphism is then given by $f_i = \varphi^{-1}(E_i)$, for $i = 0, 1, 2, 3$, i.e., $f_0 = e_0, f_1 = e_0 + e_1, f_2 = e_0 + e_1 + e_2$ and $f_3 = e_0 + e_1 + e_2 + e_3$. Therefore, $\frac{1}{2^3} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij}$, i.e., the lattice $(\mathfrak{O}_K, \frac{1}{2^3} q_\alpha)$ is isomorphic to $\mathbb{Z}^4$.

3.2 Construction from the subfield $\mathbb{Q}(\zeta_{2^r}^2 + \zeta_{2^r}^{-2})$

Let $L = \mathbb{Q}(\zeta_{2^r})$, $r \geq 4$, $L^+ = \mathbb{Q}(\theta)$, where $\theta = \zeta_{2^r} + \zeta_{2^r}^{-1}$, and $K = \mathbb{Q}(\zeta_{2^r}^2 + \zeta_{2^r}^{-2})$. Throughout this section, let $n = [K : \mathbb{Q}] = 2^{r-3}$. Thus $[L^+ : \mathbb{Q}] = 2^{r-2}$, $[L^+ : K] = 2$, and $Gal(L^+/\mathbb{Q}) = \langle \sigma \rangle$, where $\sigma(\zeta_{2^r}) = \zeta_{2^r}^5$, is a cyclic group isomorphic to $\mathbb{Z}_{2^{r-2}}$. Let $Gal(K/\mathbb{Q}) = \{\sigma^0, \sigma, \ldots, \sigma^{n-1}\}$ and $Gal(L^+/\mathbb{K}) = \{\sigma^0, \sigma^{n-1}\}$. From Proposition 4, it follows that $5^n - 1 = 5^{2^{r-3}} - 1 \equiv 0$

$(\text{mod } 2^{r-1})$, i.e., $5^{2^{r-3}} = k2^{r-1}+1$, where k is an odd positive integer. Thus, $\sigma^n(\zeta_{2^r}) = \zeta_{2^r}^{5^n} = (\zeta_{2^r})^{k2^{r-1}+1} = -\zeta_{2^r}$, and therefore, $\sigma^n(\theta) = -\theta$. So,

$$\begin{aligned}\alpha &= \mathbb{N}_{L^+/K}(2-\theta) = \prod_{i=0}^{1}\sigma^{in}(2-\theta)\\ &= (2-\theta)(2-\sigma^n(\theta))\\ &= (2-\theta)(2+\theta) = 4-\theta^2 = 2-(\zeta_{2^r}^2+\zeta_{2^r}^{-2}).\end{aligned}$$

The lattices are built via the ring of integers of K, a real subfield of L^+, whose an integral basis is given by $\{1, \zeta_{2^r}^2+\zeta_{2^r}^{-2}, \ldots, \zeta_{2^r}^{2(n-1)}+\zeta_{2^r}^{-2(n-1)}\}$. Since

$$2\mathbb{Z}[\zeta_{2^r}] = (1-\zeta_{2^r})^{2^{r-1}}\mathbb{Z}[\zeta_{2^r}],$$

it follows that $\mathbb{N}_{L/\mathbb{Q}}(1-\zeta_{2^r}) = 2$. Using the transitivity of the norm, it follows that

$$\begin{aligned}\mathbb{N}_{L/\mathbb{Q}}(1-\zeta_{2^r}) &= \mathbb{N}_{K/\mathbb{Q}}(\mathbb{N}_{L/K}(1-\zeta_{2^r})) = \mathbb{N}_{K/\mathbb{Q}}(\mathbb{N}_{L^+/\mathbb{K}}(\mathbb{N}_{L/L^+}(1-\zeta_{2^r})))\\ &= \mathbb{N}_{K/\mathbb{Q}}(\mathbb{N}_{L^+/\mathbb{K}}(1-\zeta_{2^r})(1-\zeta_{2^r}^{-1}))\\ &= \mathbb{N}_{K/\mathbb{Q}}(\mathbb{N}_{L^+/\mathbb{Q}}(2-(\zeta_{2^r}+\zeta_{2^r}^{-1})))\\ &= \mathbb{N}_{K/\mathbb{Q}}(\mathbb{N}_{L^+/\mathbb{Q}}(2-\theta)) = 2.\end{aligned}$$

Thus, $\alpha = \mathbb{N}_{L^+/K}(2-\theta)$ is an element of $\mathfrak{O}_K$ whose norm is equal to 2.

Proposition 5. *Let $e_0 = 1$ and $e_i = \zeta_{2^r}^{2i}+\zeta_{2^r}^{-2i}$, for $i = 1,2,\ldots,n-1$.*

1. *If $i = 0,1,\ldots,n-1$, then $q_\alpha(e_i,e_i) = Tr_{K/\mathbb{Q}}(\alpha e_i e_i) = \begin{cases} 2n & \text{if } i=0;\\ 4n & \text{if } i\neq 0.\end{cases}$*
2. *If $i \neq 0$, then $q_\alpha(e_0,e_i) = Tr_{K/\mathbb{Q}}(\alpha e_i) = \begin{cases} -2n & \text{if } i=1;\\ 0 & \text{if } i\neq 1.\end{cases}$*
3. *If $i,j = 1,2,\ldots,n-1$, with $i \neq j$, then*

$$q_\alpha(e_i,e_j) = Tr_{K/\mathbb{Q}}(\alpha e_i e_j) = \begin{cases} -2n & \text{if } \mid i-j \mid = 1;\\ 0 & \text{otherwise}.\end{cases}$$

Proof. By the transitivity of the trace, it follows that $Tr_{L/\mathbb{Q}}(\alpha) = Tr_{K/\mathbb{Q}}(Tr_{L/\mathbb{K}}(\alpha) = 2^2 Tr_{K/\mathbb{Q}}(\alpha)$. Since $\alpha = 2-(\zeta_{2^r}^2+\zeta_{2^r}^{-2})$ and $\gcd(2,2^r) < 2^{r-1}$, it follows that

$$Tr_{K/\mathbb{Q}}(\alpha) = 2n.$$

If $e_i = \zeta_{2^r}^{2i}+\zeta_{2^r}^{-2i}$, for $i = 1,2,\ldots,n-1$, then

$$\begin{aligned}\alpha e_i &= (2-(\zeta_{2^r}^2+\zeta_{2^r}^{-2}))(\zeta_{2^r}^{2i}+\zeta_{2^r}^{-2i})\\ &= 2(\zeta_{2^r}^{2i}+\zeta_{2^r}^{-2i}) - (\zeta_{2^r}^{2(i+1)}+\zeta_{2^r}^{-2(i+1)}+\zeta_{2^r}^{2(i-1)}+\zeta_{2^r}^{-2(i-1)}).\end{aligned}$$

Since $\gcd(2i,2^r) < 2^{r-1}$, it follows that $Tr_{L/\mathbb{Q}}(\zeta_{2^r}^{2i} + \zeta_{2^r}^{-2i}) = 0$. Thus,

$$Tr_{K/\mathbb{Q}}(\alpha e_i) = \begin{cases} 2n & \text{if } i = 1; \\ 0 & \text{if } i \neq 1. \end{cases}$$

Now, for $i = 1,2,\ldots,n-1$, it follows that $e_i^2 = \zeta_{2^r}^{4i} + \zeta_{2^r}^{-4i} + 2$. Thus,

$$\begin{aligned} \alpha e_i^2 &= (2-(\zeta_{2^r}^2 + \zeta_{2^r}^{-2}))(2+(\zeta_{2^r}^{4i} + \zeta_{2^r}^{-4i})) \\ &= 4 + 2(\zeta_{2^r}^{4i} + \zeta_{2^r}^{-4i} - \zeta_{2^r}^2 - \zeta_{2^r}^{-2}) - (\zeta_{2^r}^{2(2i+1)} + \zeta_{2^r}^{-2(i+1)} + \zeta_{2^r}^{2(2i-1)} + \zeta_{2^r}^{-2(2i-1)}). \end{aligned}$$

Since $\gcd(4i,2^r)$, $\gcd(2(i+1),2^{r-1})$ and $\gcd(2(i-1),2^r) < 2^{r-1}$, it follows that

$$Tr_{L/\mathbb{Q}}(\alpha e_i^2) = 4n.$$

Finally, let $i,j = 1,2,\ldots,n-1$, with $i \neq j$. Since $e_i e_j = (\zeta_{2^r}^{2i} + \zeta_{2^r}^{-2i})(\zeta_{2^r}^{2j} + \zeta_{2^r}^{-2j}) = \zeta_{2^r}^{2(i+j)} + \zeta_{2^r}^{-2(i+j)} + \zeta_{2^r}^{2(i-j)} + \zeta_{2^r}^{-2(i-j)}$, with $i > j$, it follows that

$$\begin{aligned} \alpha e_i e_j &= (2-(\zeta_{2^r}^2 + \zeta_{2^r}^{-2}))(\zeta_{2^r}^{2(i+j)} + \zeta_{2^r}^{-2(i+j)} + \zeta_{2^r}^{2(i-j)} + \zeta_{2^r}^{-2(i-j)}) \\ &= 2(\zeta_{2^r}^{2(i+j)} + \zeta_{2^r}^{-2(i+j)} + \zeta_{2^r}^{2(i-j)} + \zeta_{2^r}^{-2(i-j)}) \\ &- (\zeta_{2^r}^{2(i+j+1)} + \zeta_{2^r}^{-2(i+j+1)} + \zeta_{2^r}^{2(i-j+1)} + \zeta_{2^r}^{-2(i-j+1)}) \\ &- (\zeta_{2^r}^{2(i+j-1)} + \zeta_{2^r}^{-2(i+j-1)} + \zeta_{2^r}^{2(i-j-1)} + \zeta_{2^r}^{-2(i-j-1)}). \end{aligned}$$

Since $\gcd(i \pm j, 2^r), \gcd(2(i \pm j), 2^r)$ and $\gcd(2(i \pm j \pm 1), 2^r) < 2^{r-1}$, it follows that

$$Tr_{L/\mathbb{Q}}(\alpha e_i e_j) = \begin{cases} -2n & \text{if } \mid i-j \mid = 1; \\ 0 & \text{otherwise,} \end{cases}$$

which proves the proposition. □

Corollary 6. *If $Q(x,y) = \frac{1}{2^{r-2}} Tr_{K/\mathbb{Q}}(\alpha xy)$, then the matrix of Q in the basis $\{e_0, e_1, \cdots, e_{n-1}\}$ is given by*

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

Proof. It follows directly from Proposition 5. □

Matrix G of Corollary 6 is the Gram matrix of a rotated $\mathbb{Z}^n$-lattice related to the basis $\{w_0, w_1, \cdots, w_{n-1}\}$, where $w_0 = E_0$, $w_i = -E_{i-1} + E_i$, for $i = 1,2,\cdots,n-1$, and $\{E_j\}_{j=0}^{n-1}$ is the canonical basis of $\mathbb{Z}^n$. Thus $\varphi(e_i) = w_i$, for $i = 0,1,\cdots,n-1$, is an isomorphism on the $\mathbb{Z}^n$-lattice. The basis which corresponds to the canonical basis of $\mathbb{Z}^n$ through this isomorphism is then given by $f_i = \varphi^{-1}(E_i) = \sum_{j=0}^{i} e_j$, for $i = 0,1,\cdots,n-1$. Hence, one has the following result.

Proposition 7. *If* $\{f_0, f_1, \cdots, f_{n-1}\}$, *where* $f_i = \sum_{j=0}^{i} e_j$, *for* $i = 0, 1, \cdots, n-1$, *is a basis of* $\mathfrak{O}_K$, *then*

$$\frac{1}{2^{r-2}} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij},$$

i.e., the lattice $(\mathfrak{O}_K, \frac{1}{2^{r-2}} q_\alpha)$ *is isomorphic to* $\mathbb{Z}^n$.

Let $Gal(K/\mathbb{Q}) = \{\sigma^0, \sigma, \ldots, \sigma^{n-1}\}$ be the Galois group of K over $\mathbb{Q}$. Thus, the generator matrix of the lattice associated to the ring of integers of K is given by

$$M = \begin{pmatrix} \sigma^0(e_0) & \cdots & \sigma^{n-1}(e_0) \\ \vdots & \ddots & \vdots \\ \sigma^0(e_{n-1}) & \cdots & \sigma^{n-1}(e_{n-1}) \end{pmatrix}.$$

Let

$$A = diag\left(\sqrt{\sigma^{2k}(\alpha)}\right)_{k=0}^{n-1} \quad \text{and} \quad T = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix}.$$

As before, the generator matrix of the rotated $\mathbb{Z}^n$-lattice is then given by

$$R = \frac{1}{\sqrt{2^{r-2}}} TMA.$$

Example 3.3. *Let* L *be the cyclotomic field* $\mathbb{Q}(\zeta_{2^4})$ *and* $K \subseteq L^+$ *its real subfield given by* $K = \mathbb{Q}(\zeta_{2^4}^2 + \zeta_{2^4}^{-2})$. *In this case,* $[L^+ : K] = 2$,

$$\begin{aligned} \alpha &= \mathbb{N}_{L/K}(1-\zeta_{2^4}) = \mathbb{N}_{L^+/K}(\mathbb{N}_{L/L^+}(1-\zeta_{2^4})) = \mathbb{N}_{L^+/K}(1-\zeta_{2^4})(1-\zeta_{2^4}^{-1}) \\ &= \mathbb{N}_{L^+/K}(2-(\zeta_{2^4}+\zeta_{2^4}^{-1})) = (2-(\zeta_{2^4}^9+\zeta_{2^4}^{-9}))(2-(\zeta_{2^4}+\zeta_{2^4}^{-1})) \\ &= 4-2(\zeta_{2^4}+\zeta_{2^4}^{-1}+\zeta_{2^4}^9+\zeta_{2^4}^{-9})+(\zeta_{2^4}^8+\zeta_{2^4}^{-8}+\zeta_{2^4}^{10}+\zeta_{2^4}^{-10}), \end{aligned}$$

$\Delta_K = 2^3$ *and* $c = 2^2$. *Considering the* $\mathbb{Z}$*-basis for* $\mathfrak{O}_K$, *namely,* $\{e_0, e_1\}$, *where* $e_0 = 1$ *and* $e_1 = \zeta_{2^4}^2 + \zeta_{2^4}^{-2}$, *and* $Q(x,y) = \frac{1}{2^2} q_\alpha(x,y) = \frac{1}{2^2} Tr_{K/\mathbb{Q}}(\alpha xy)$, *it follows that the matrix of* q_α *is given by*

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

Matrix G *is the Gram matrix of the rotated* $\mathbb{Z}^2$*-lattice relative to the basis* $\{w_0, w_1\}$ *with* $w_0 = E_0$ *and* $w_1 = -E_0 + E_1$, *where* $\{E_0, E_1\}$ *is the canonical basis of* $\mathbb{Z}^2$. *This implies that* $\varphi(e_i) = w_i$, *for* $i = 0, 1$, *is an isomorphism of the* $\mathbb{Z}^2$*-lattice. The basis which corresponds to the canonical basis of* $\mathbb{Z}^2$ *through this isomorphism is then given by* $f_i = \varphi^{-1}(E_i)$, *for* $i = 0, 1$, *i.e.,* $f_0 = e_0$ *and* $f_1 = e_0 + e_1$. *Therefore,* $\frac{1}{2^2} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij}$, *i.e., the lattice* $(\mathfrak{O}_K, \frac{1}{2^2} q_\alpha)$ *is isomorphic to* $\mathbb{Z}^2$.

Example 3.4. *Let L be the cyclotomic field $\mathbb{Q}(\zeta_{2^5})$ and $K \subseteq L^+$ its real subfield given by $K = \mathbb{Q}(\zeta_{2^5}^2 + \zeta_{2^5}^{-2})$. In this case, $[L^+ : K] = 2$,*

$$\begin{aligned}\alpha &= \mathbb{N}_{L/K}(1-\zeta_{2^5}) = \mathbb{N}_{L^+/K}(\mathbb{N}_{L/L^+}(1-\zeta_{2^5})) = \mathbb{N}_{L^+/K}(1-\zeta_{2^5})(1-\zeta_{2^5}^{-1}) \\ &= \mathbb{N}_{L^+/K}(2-(\zeta_{2^5}+\zeta_{2^5}^{-1})) = (2-(\zeta_{2^5}^{17}+\zeta_{2^5}^{-17}))(2-(\zeta_{2^5}+\zeta_{2^5}^{-1})) \\ &= 4-2(\zeta_{2^5}+\zeta_{2^5}^{-1}+\zeta_{2^5}^{17}+\zeta_{2^5}^{-17})+(\zeta_{2^5}^{16}+\zeta_{2^5}^{-16}+\zeta_{2^5}^{18}+\zeta_{2^5}^{-18}),\end{aligned}$$

$\Delta_K = 2^{11}$ and $c = 2^6$. Considering the basis $\{e_0, e_1, e_2, e_3\}$, where $e_0 = 1$, $e_1 = \zeta_{2^5}^2 + \zeta_{2^5}^{-2}$, $e_2 = \zeta_{2^5}^4 + \zeta_{2^5}^{-4}$ and $e_3 = \zeta_{2^5}^6 + \zeta_{2^4}^{-6}$, of $\mathfrak{O}_K$ and $Q(x,y) = \frac{1}{2^3} q_\alpha(x,y) = \frac{1}{2^3} Tr_{K/\mathbb{Q}}(\alpha xy)$, it follows that the matrix of q_α is given by

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

Matrix G is the Gram matrix of the rotated $\mathbb{Z}^4$-lattice relative to the basis $\{w_0, \cdots, w_3\}$, with $w_0 = E_0$, $w_1 = -E_0 + E_1$, $w_2 = -E_1 + E_2$ and $w_3 = -E_3 + E_4$, where $\{E_0, E_1, E_2, E_3\}$ is the canonical basis of $\mathbb{Z}^4$. This implies that $\varphi(e_i) = w_i$, for $i = 0, 1, 2, 3$, is an isomorphism of the $\mathbb{Z}^4$-lattice. The basis which corresponds to the canonical basis of $\mathbb{Z}^4$ through this isomorphism is then given by $f_i = \varphi^{-1}(E_i)$, for $i = 0, 1, 2, 3$, i.e., $f_0 = e_0$, $f_1 = e_0 + e_1$, $f_2 = e_0 + e_1 + e_2$ and $f_3 = e_0 + e_1 + e_2 + e_3$. Therefore, $\frac{1}{2^3} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij}$, i.e., the lattice $(\mathfrak{O}_K, \frac{1}{2^3} q_\alpha)$ is isomorphic to $\mathbb{Z}^4$.

From [12, Theorem 1], it follows that the minimum product distance of Λ is given by

$$d_{p,\min}(\Lambda) = \frac{1}{\sqrt{\Delta_K}}.$$

To compare lattices in different dimensions, we use the parameter $\sqrt[n]{d_{p,\min}(\Lambda)}$. In the next table, we list the minimum product distance of Λ for several dimensions. The entries in the column labeled "bound" were calculated from the minimal discriminant of Abelian and totally real number fields of degree n, [11]. For $n > 32$, the minima appear to be currently unknown, which explains the missing entries.

4 CONCLUSION

A method for constructing rotated $\mathbb{Z}^n$-lattices via the ring of integers of the subfield $K = \mathbb{Q}(\zeta_{2^r}^{2^k} + \zeta_{2^r}^{-2^k})$ of the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$ with $k = 0, 1$ has been presented. The dimensions $n = 8$ and $n = 16$ were addressed in [7] using the field $\mathbb{Q}(\zeta_{8n} + \zeta_{8n}^{-1})$, and they have the same $d_{p,\min}(\Lambda)$ as our cyclotomic construction. The lattices presented in this work are all ideal lattices, which allowed us to easily evaluate their minimum product distances from field discriminants, just as in [5] and [9].

n	r	k	$\sqrt[n]{d_{p,\min}(\Lambda)}$	Bound
2	3	0	0.594604	0.668740
4	4	0	0.385553	0.438993
8	5	0	0.261068	0.296367
16	6	0	0.180648	0.214279
32	7	0	0.126361	0.167500
64	8	0	0.088868	–
128	9	0	0.062669	–
256	10	0	0.044254	–
512	11	0	0.031271	–
1024	12	0	0.022105	–
2048	13	0	0.015628	–

n	r	k	$\sqrt[n]{d_{p,\min}(\Lambda)}$	Bound
2	4	1	0.594604	0.668740
4	5	1	0.385553	0.438993
8	6	1	0.261068	0.296367
16	7	1	0.180648	0.214279
32	8	1	0.126361	0.167500
64	9	1	0.088868	–
128	10	1	0.062669	–
256	11	1	0.044254	–
512	12	1	0.031271	–
1024	13	1	0.022105	–
2048	14	1	0.015628	–

5 ACKNOWLEDGMENT

The authors thank the reviewer for carefully reading the manuscript and for all the suggestions that improved the presentation of the work. They also thank FAPESP for its financial support 2013/25977-7.

RESUMO. Um método para construir $\mathbb{Z}^n$-reticulados rotacionados, com n uma potência de 2, via subcorpos totalmente reais do corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$, onde $r \geq 4$ é um inteiro, é apresentado. Reticulados que exibem diversidade completa em algumas dimensões n não abordadas anteriormente são obtidos.

Palavras-chave: reticulados, corpos cyclotômicos, modulação, canais de desvanecimento, distância produto mínima.

REFERENCES

[1] A.A. Andrade, C. Alves & T.B. Carlos. Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$. *Internat. J. Appl. Math.*, **19** (2006), 321–331.

[2] A. Ansari, T. Shah, Z.u. Rahman & A.A. Andrade. Sequences of Primitive and Non-primitive BCH Codes. *TEMA (São Carlos)*, **19**(2) (2018), 369–389.

[3] V. Bautista-Ancona, J. Uc-Kuk *et al.* The discriminant of abelian number fields. *Rocky Mountain Journal of Mathematics*, **47**(1) (2017), 39–52.

[4] E. Bayer-Fluckiger. Lattices and number fields. volume 241. Am. Math. Soc. (1999).

[5] E. Bayer-Fluckiger, F. Oggier & E. Viterbo. Algebraic lattice constellations: Bounds on performance. *IEEE Transactions on Information Theory*, **52**(1) (2005), 319–327.

[6] J. Boutros, E. Viterbo, C. Rastello & J.C. Belfiore. Good lattice constellations for both Rayleigh fading and Gaussian channels. *IEEE Transactions on Information Theory*, **42**(2) (1996), 502–518.

[7] M.O. Damen, K. Abed-Meraim & J.C. Belfiore. Diagonal algebraic space-time block codes. *IEEE Transactions on Information Theory*, **48**(3) (2002), 628–636.

[8] A.A. de Andrade, T. Shah & A. Khan. A note on linear codes over semigroup rings. *Trends in Applied and Computational Mathematics*, **12**(2) (2011), 79–89.

[9] P. Elia, B.A. Sethuraman & P.V. Kumar. Perfect Space-Time Codes for Any Number of Antennas. *IEEE Trans. Information Theory*, **53**(11) (2007), 3853–3868.

[10] S. Lang. "Algebra. Revised third edition, Corrected forth printing". Graduate Texts in Mathematics, 3 ed. (2003).

[11] A.M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Journal de théorie des nombres de Bordeaux*, **2**(1) (1990), 119–141.

[12] F. Oggier, E. Bayer-Fluckiger & E. Viterbo. New algebraic constructions of rotated cubic Zn-lattice constellations for the Rayleigh fading channel. In "Proceedings 2003 IEEE Information Theory Workshop (Cat. No. 03EX674)". IEEE (2004), pp. 702–714.

[13] K.H. Rosen. "Elementary Number Theory and its Applications". Addison-Wesley, Reading, MA, 6 ed. (2011).

[14] L. Washington. "Introduction to Cyclotomic Fields". Springer-Verlag, New York, 2 ed. (1997).