Tendências em Matemática Aplicada e Computacional, **20**, N. 3 (2019), 561-570

www.scielo.br/tema
doi: 10.5540/tema.2019.020.03.0561

A Construction of Rotated Lattices via Totally Real Subfields of the Cyclotomic Field $\mathbb{Q}(\zeta_p)$

A. A. ANDRADE[1*], E. L. OLIVEIRA[2] and J. C. INTERLANDO[3]

Received on March 14, 2019 / Accepted on August 6, 2019

ABSTRACT. The theory of lattices have shown to be useful in information theory and rotated lattices with high modulation diversity have been extensively studied as an alternative approach for transmission over a Rayleigh-fading channel, where the performance of this modulation schemes essentially depends on the modulation diversity and on the minimum product distance to achieve substantial coding gains. The maximum diversity of a rotated lattice is guaranteed when we use totally real number fields and the minimum product distance is optimized by considering fields with minimum discriminant. In this paper, we present construction of a full diversity rotated lattice for the Rayleigh fading channel in Euclidean space with full diversity, where this construction is through a totally real subfield $\mathbb{K}$ of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where p is an odd prime, obtained by endowing their ring of integers.

Keywords: lattices, cyclotomic fields, algebraic number field, rotated lattice.

1 INTRODUCTION

Algebraic number theory has recently raised a great interest for their new role in algebraic lattice theory and for application in coding and modulation. The problem of finding algebraic lattices with maximal minimum product distance has been studied in last years and this has motivated special attention of many researchs in considering ideals of certain rings [5], [2] and [1]. Eva Bayer et al. [7] and Andrade et al. [1] have presented families of rotated $\mathbb{Z}^n$-lattices based on algebraic number theory. We know that totally real algebraic number fields result in the maximum diversity, equal to the dimension of the lattice [3]. This motivates the investigation on lattices over totally real number fields.

*Corresponding author: Antonio Aparecido de Andrade – E-mail: antonio.andrade@gmail.com – https://orcid.org/0000-0001-6452-2236
[1]Departamento de Matemática, Universidade do Estado de São Paulo, São José do Rio Preto-SP, Brazil – E-mail: antonio.andrade@gmail.com
[2]Departamento de Matemática, Universidade Federal do Mato Grosso do Sul, Campo Grande-MS, Brazil – E-mail: everton.luiz@ufms.br
[3]Department of Mathematics & Statistics, San Diego State University, San Diego-CA, USA – E-mail: interlan@sdsu.edu

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$, equivalently, $\Lambda \subseteq \mathbb{R}^n$ is a lattice iff there are linearly independent vectors $v_1, v_2, \cdots, v_m \in \mathbb{R}^n$ such that

$$\Lambda = \{\sum_{i=1}^{m} a_i v_i : a_i \in \mathbb{Z}, \text{ for } i = 1, 2, \cdots, m\}.$$

The set $\{v_1, v_2, \cdots, v_n\}$ is a $\mathbb{Z}$-basis and a matrix M whose rows are these vectors is said to be a generator matrix for Λ and the associated Gram matrix is given by $G = MM^t = (< v_i, v_j >)_{i,j=1}^n$. Lattices have been considered in different areas, especially in coding theory and more recently in cryptography. In this paper, we attempt to construct lattices with full rank, i.e., $m = n$, which may be suitable for signal transmission over both Gaussian and Rayleigh fading channels [3]. For this purpose the tattice parameters we consider here are diversity and minimum product distance.

In [1], for any integer $r \geq 4$, rotated $\mathbb{Z}^n$-lattices, $n = 2^{r-2}$ and $n = 2^{r-3}$, were constructed from $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, the maximal real subfield of $\mathbb{Q}(\zeta_{2^r})$, and over $\mathbb{Q}(\zeta_{2^r}^2 + \zeta_{2^r}^{-2})$, where ζ_{2^r} is a primitive 2^r-th root of unity. In this work, having the construction procedure of a rotated lattice over the maximal real subfield of a cyclotomic field as the main motivation, we make use of algebraic number theory for constructing rotated lattices via totally real subfields of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where p is an odd prime number.

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 lattices are constructed from totally real subfields of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where p is an odd prime number. In Section 4, an algorithm to the construction of rotated lattices is presented and we present examples in terms of center density and minimum product distance.

2 BASIC RESULTS FROM NUMBER THEORY

A number field is a field $\mathbb{L}$ that is a finite degree extension n of $\mathbb{Q}$. An element $\alpha \in \mathbb{L}$ is called an algebraic integer if there is a monic polynomial $f(x)$ with integer coefficients such that $f(\alpha) = 0$. The set

$$\mathscr{O}_{\mathbb{L}} = \{\alpha \in \mathbb{L} : \alpha \text{ is an algebraic integer}\}$$

is a ring called ring of algebraic integers of $\mathbb{L}$. The ring $\mathscr{O}_{\mathbb{L}}$ is a $\mathbb{Z}$-module of rank n and a $\mathbb{Z}$-basis $\{\alpha_1, \cdots, \alpha_n\}$ of $\mathscr{O}_{\mathbb{L}}$ is called an integral basis of $\mathbb{L}$ (or of $\mathscr{O}_{\mathbb{L}}$). Furthermore, $\mathbb{L} = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of a monic irreducible polynomial $p(x) \in \mathbb{Q}[x]$. The n distinct roots $\alpha_1, \alpha_2, \cdots, \alpha_n$ of $p(x)$ are the conjugates of α. If $\sigma_i : \mathbb{L} \to \mathbb{C}$ is a $\mathbb{Q}$-homomorphism, then $\sigma_i(\alpha) = \alpha_i$ for some $i = 1, 2, \cdots, n$, and there are exactly n $\mathbb{Q}$-homomorphism $\sigma_i : \mathbb{L} \to \mathbb{C}$, for $i = 1, 2, \cdots, n$. A homomorphism σ_i is said to be real if $\sigma_i(\mathbb{L}) \subseteq \mathbb{R}$ and imaginary otherwise. A number field $\mathbb{L}$ is said to be totally real if σ_i is real for all $i = 1, 2, \cdots, n$ and totally imaginary if σ_i is imaginary for all $i = 1, 2, \cdots, n$. The trace of any element $\alpha \in \mathbb{L}$ is defined as the rational number

$$T_{\mathbb{L}:\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

and if $\alpha \in \mathscr{O}_{\mathbb{L}}$, then $T_{\mathbb{L}:\mathbb{Q}}(\alpha) \in \mathbb{Z}$. The discriminant of L, denoted by $\Delta_{\mathbb{L}}$, is the rational integer given by $\det(Tr_{\mathbb{L}:\mathbb{Q}}(\alpha_i\alpha_j))$.

A cyclotomic field is a number field $\mathbb{L}$ such that $\mathbb{L} = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. Also, $[\mathbb{L}:\mathbb{Q}] = \varphi(n)$, where φ is the Euler function, $\mathscr{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Z}[\zeta_n]$, and the field $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the maximal real subfield of $\mathbb{L}$, where $[\mathbb{L}:\mathbb{K}] = 2$ and $\mathscr{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ [6], [8].

3 CONSTRUCTION OF A ROTATED LATTICE

If ζ_p is a primitive p-th root of unity, where p is an odd prime number, then $\mathbb{L} = \mathbb{Q}(\zeta_p)$ is a cyclic extension of degree $p-1$ over $\mathbb{Q}$ that contains the real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, which is cyclic of degree $l = (p-1)/2$ over $\mathbb{Q}$. If $G = Gal(\mathbb{L}:\mathbb{Q})$ is the Galois group (cyclic) of $\mathbb{L}$ over $\mathbb{Q}$ with generator σ_r (or σ), then $\sigma_r(\zeta_p) = \zeta_p^r$, where r is a generator of $\mathbb{Z}_p^*$, and $r^l \equiv -1(mod\ p)$, that is, r is a primitive element modulo p.

Theorem 1. *[10] (Dirichlet's theorem) If a,n are integers such that $1 \leq a \leq n$ and $gcd(a,n) = 1$, then the arithmetic progression $\{a, a+n, a+2n, \cdots, a+kn, \cdots\}$ contains infinitely many primes.*

If n is a positive integer, from Theorem 1, it follows that there exists a prime p such that $p \equiv 1(mod\ n)$. Since n divides $p-1$, from Galois Correspondence Theorem, it follows that there exists a unique field $\mathbb{K}$ contained in $\mathbb{Q}(\zeta_p)$ which is cyclic of degree n over $\mathbb{Q}$. If n is an even number that divides $(p-1)/2$ or if n is an odd number, then $\mathbb{K}$ is contained in the real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. In this case, $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta = Tr_{\mathbb{L}:\mathbb{K}}(\zeta_p)$,

$$Gal(\mathbb{Q}(\zeta_p):\mathbb{K}) = \langle\sigma^n\rangle = \{\sigma^n, \sigma^{2n}, \cdots, \sigma^{nm}\} = \{\sigma_{r^n}, \sigma_{r^{2n}}, \cdots, \sigma_{r^{mn}}\},$$

where $m = (p-1)/n$, $Gal(\mathbb{K}:\mathbb{Q}) = \{\sigma^0, \sigma, \cdots, \sigma^{n-1}\}$ and

$$\{\sigma_r(\theta), \sigma_{r^2}(\theta), \cdots, \sigma_{r^n}(\theta)\} = \{\theta, \sigma(\theta), \cdots, \sigma^{n-1}(\theta)\}$$

is an integral basis of $\mathbb{K}$, where $\sigma^s = \sigma_{r^s}$, for all $s \in \mathbb{Z}^+$ [6].

If $\sigma_{\mathbb{K}}$ is the canonical embedding given by

$$\begin{array}{rccl} \sigma_{\mathbb{K}} : & \mathbb{K} & \longrightarrow & \mathbb{R}^n \\ & x & \longmapsto & \sigma_{\mathbb{K}}(x) = (x, \sigma(x), \cdots, \sigma^{n-1}(x)), \end{array}$$

then $\sigma_{\mathbb{K}}(\mathscr{O}_{\mathbb{K}})$ is an algebraic lattice in $\mathbb{R}^n$ with maximum diversity. Since the set $\{\theta, \sigma(\theta), \cdots, \sigma^{n-1}(\theta)\}$ is a $\mathbb{Z}$-basis of $\mathscr{O}_{\mathbb{K}}$, it follows that

$$\{\sigma_{\mathbb{K}}(\theta), \sigma_{\mathbb{K}}(\sigma(\theta)), \cdots, \sigma_{\mathbb{K}}(\sigma^{n-1}(\theta))\} \subset \mathbb{R}^n$$

is a basis of the lattice $\sigma_{\mathbb{K}}(\mathscr{O}_{\mathbb{K}})$, whose generator matrix is given by

$$M = \begin{pmatrix} \theta & \sigma(\theta) & \cdots & \sigma^{n-1}(\theta) \\ \sigma(\theta) & \sigma^2(\theta) & \cdots & \theta \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-1}(\theta) & \theta & \cdots & \sigma^{n-2}(\theta) \end{pmatrix}.$$

Since $M = M^t$, it follows that the i-th row is given by

$$\sigma_{\mathbb{K}}(\sigma^i(\theta)) = (\sigma^i(\theta), \sigma^{i+1}(\theta), \cdots, \sigma^{i+n-1}(\theta)),$$

for $i = 0, 1, \cdots, n-1$. The Gram matrix $G = (g_{ij})_{i,j=0}^{n-1}$ of $\sigma_{\mathbb{K}}(\mathscr{O}_{\mathbb{K}})$ is given by $G = MM^t$, where

$$\begin{aligned} g_{ij} &= \langle \sigma_{\mathbb{K}}(\sigma^i(\theta)), \sigma_{\mathbb{K}}(\sigma^j(\theta)) \rangle \\ &= \sigma^i(\theta)\sigma^j(\theta) + \sigma^{i+1}(\theta)\sigma^{j+1}(\theta) + \cdots + \sigma^{i+n-1}(\theta)\sigma^{j+n-1}(\theta) \\ &= \sum_{a=0}^{n-1} \sigma^{i+a}(\theta)\sigma^{j+a}(\theta) \end{aligned}$$

Since $\sigma^n|_{\mathbb{K}} = \sigma^0_{\mathbb{K}}$ and $\sigma^{n-s}|_{\mathbb{K}} = \sigma^{-s}|_{\mathbb{K}}$, for all $s \in \mathbb{Z}^+$, it follows that

$$\begin{aligned} g_{ij} &= \sum_{a=0}^{n-1} \sigma^{i+a}(\theta)\sigma^{j+a}(\theta) = \sum_{a=0}^{n-1} \sigma^a(\theta)\sigma^{j+a-i}(\theta) \\ &= \sum_{a=0}^{n-1} \sigma^a(\theta\ \sigma^{j-i}(\theta)) = Tr_{\mathbb{K}:\mathbb{Q}}(\theta\ \sigma^{j-i}(\theta)), \end{aligned}$$

for $i, j = 0, 1, \cdots, n-1$. Thus,

$$G = \left(Tr_{\mathbb{K}:\mathbb{Q}}(\theta\ \sigma^{j-i}(\theta))\right)_{i,j=0}^{n-1}.$$

Since $Tr_{\mathbb{K}:\mathbb{Q}}(\sigma^i(\theta)\sigma^j(\theta)) = Tr_{\mathbb{K}:\mathbb{Q}}(\theta\ \ \sigma^{j-i}(\theta))$, for $i, j = 0, 1, \cdots, n-1$, it is sufficient to calculate $Tr_{\mathbb{K}:\mathbb{Q}}(\theta\ \sigma^t(\theta))$, for $t = 0, 1, \cdots, n-1$. Finally,

$$Tr_{\mathbb{K}/:mathbbQ}(\theta) = Tr_{\mathbb{K}:\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta_p)) = Tr_{\mathbb{Q}(\zeta_p):\mathbb{Q}}(\zeta_p) = -1$$

and

$$\begin{aligned} Tr_{\mathbb{K}:\mathbb{Q}}(\sigma^t(\theta)) &= \sum_{a=0}^{n-1} \sigma^a(\sigma^t(\theta)) = \sum_{a=0}^{n-1} \sigma^t(\sigma^a(\theta)) = \sigma^t(\sum_{a=0}^{n-1} \sigma^a(\theta)) \\ &= = \sigma^t(Tr_{\mathbb{K}:\mathbb{Q}}(\theta)) = \sigma^t(-1) = -1, \end{aligned}$$

for $t = 0, 1, \cdots, n-1$.

The following theorem, which is the main result of this work, gives us the key to constructing full diversity rotated lattice bssed on real subfields of the cyclotomic field $\mathbb{Q}(\zeta_p)$.

Theorem 2. *If $\theta = Tr_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta_p)$, then*

$$Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) = \begin{cases} p - (\frac{p-1}{n}) & if\ t = 0; \\ -(\frac{p-1}{n}) & if\ t = 1, 2, \cdots, n-1. \end{cases}$$

Proof. Since $\theta \in \mathbb{K}$, it follows that

$$Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) = \sum_{a=0}^{n-1} \sigma^a(\theta\sigma^t(\theta)),$$

for all $t = 0, 1, \cdots, n-1.$, and

$$\theta\sigma^t(\theta) = \sum_{c=1}^{\frac{p-1}{n}} \sigma^{cn}(\zeta_p) \sum_{j=1}^{\frac{p-1}{n}} \sigma^{t+jn}(\zeta_p) = \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{cn}(\zeta_p)\sigma^{t+jn}(\zeta_p),$$

because $Gal(\mathbb{Q}(\zeta_p) : \mathbb{K}) = \langle\sigma^n\rangle$, whose order is $m = (p-1)/n$. Thus,

$$\begin{aligned} Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) &= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(\zeta_p)\sigma^{a+t+jn}(\zeta_p) \\ &= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \zeta_p^{r^{a+cn}} \zeta_p^{r^{a+t+jn}} = \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \zeta_p^{r^{a+cn}+r^{a+t+jn}}. \end{aligned}$$

Since r is a generator of $\mathbb{Z}_p^*$, it follows that $r^{p-1} \equiv 1(mod\ p)$, and thus, $r^{(p-1)q} = (r^{p-1})^q \equiv 1^q = 1(mod\ p)$, for all $q \in \mathbb{Z}$. So,

$$r^{a+(mq+c)n} = r^{a+(\frac{p-1}{n}q+c)n} = r^{a+(p-1)q+cn} = r^{a+cn}r^{(p-1)q} \equiv r^{a+cn}(mod\ p).$$

Therefore, $\zeta_p^{r^{a+cn}} = \zeta_p^{r^{a+(mq+c)n}}$, for all $q \in \mathbb{Z}^+$. Now, if $s \equiv c(mod\ m)$, then $s = mq + c$, for some $q \in \mathbb{Z}$. Thus, $\zeta_p^{r^{a+sn}} = \zeta_p^{r^{a+cn}}$. So,

$$Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) = \sum_{a=0}^{n-1} \sum_{c,j\in\mathbb{Z}_m} \zeta_p^{r^{a+cn}+r^{a+t+jn}} = \sum_{c\in\mathbb{Z}_m} \sum_{a=0}^{n-1} \sum_{j\in\mathbb{Z}_m} \zeta_p^{r^{a+cn}+r^{a+t+jn}}.$$

Furthermore, if $d \equiv c - j(mod\ m)$, i.e., $c \equiv d + j(mod\ m)$, then $\zeta_p^{r^{a+cn}} = \zeta_p^{r^{a+(d+j)n}}$, and since c ranges in $\mathbb{Z}_m$, it follows that d also ranges in $\mathbb{Z}_m$. Thus,

$$\begin{aligned} Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) &= \sum_{d\in\mathbb{Z}_m} \sum_{a=0}^{n-1} \sum_{j\in\mathbb{Z}_m} \zeta_p^{r^{a+(d+j)n}+r^{a+t+jn}} \\ &= \sum_{d\in\mathbb{Z}_m} \sum_{a=0}^{n-1} \sum_{j\in\mathbb{Z}_m} \zeta_p^{(r^{dn}+r^t)r^{a+jn}} = \sum_{d=1}^{\frac{p-1}{n}} \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta_p^{(r^{dn}+r^t)r^{a+jn}}. \end{aligned}$$

Since $a \in \{0, 1, \cdots, n-1\}$ and $j \in \{1, \cdots, \frac{p-1}{n}\}$, it follows that $r^{a+jn} \equiv s(mod\ p)$, where $s = 1, \cdots, p-1$, because $\langle r\rangle = \mathbb{Z}_p^* = \{1, \cdots, p-1\}$, and thus $r^{a+jn} = s$ for some $s = 1, \cdots, p-1$. So, $\zeta_p^{r^{a+jn}} = \zeta_p^s$, for some $s = 1, \cdots, p-1$. Now, since $n(\frac{p-1}{n}) = p-1$, it follows that

$$\sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta_p^{(r^{dn}+r^t)r^{a+jn}} = \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} (\zeta_p^{r^{a+jn}})^{r^{dn}+r^t} = \sum_{s=1}^{p-1} (\zeta_p^s)^{r^{dn}+r^t} = \sum_{s=1}^{p-1} (\zeta_p^{r^{dn}+r^t})^s.$$

Thus, if $\omega_{d,t} = \zeta_p^{r^{dn}+r^t}$, then

$$Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) = \sum_{d=1}^{\frac{p-1}{n}} \sum_{s=1}^{p-1} (\omega_{d,t})^s,$$

where

$$\sum_{s=1}^{p-1} (\omega_{d,t})^s = \begin{cases} p-1 & \text{if } \omega_{d,t} = 1 \\ -1 & \text{if } \omega_{d,t} \neq 1, \end{cases}$$

for $t = 0, 1, \cdots, n-1$. The first case is trivial. Now, for $\omega_{d,t} \neq 1$, is sufficient observe that $\omega_{d,t} = \zeta_p^{r^{dn}+r^t}$ is a root of the polynomial

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1,$$

and therefore,

$$\sum_{s=1}^{p-1} (\omega_{d,t})^s = (\omega_{d,t})^{p-1} + \cdots + (\omega_{d,t})^2 + \omega_{d,t} = -1.$$

Now, to calcule $Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta))$, we consider the cases $t = 0$ and $t \neq 0$. But,

$$\omega_{d,t} = 1 \iff t = 0 \text{ and } d = \frac{p-1}{2n}. \tag{3.1}$$

In fact, if $t = 0$ and $d = (p-1)/2n$, then $r^{p-1} \equiv 1 (mod\ p)$. Since $p-1$ is even, it follows that there exists $l \in \mathbb{Z}$ such that $p - 1 = 2l$. So, $(r^l)^2 = r^{2l} \equiv 1 (mod\ p)$, i.e., $p \mid (r^l)^2 - 1 = (r^l + 1)(r^l - 1)$. Thus, $r^l \equiv 1 (mod\ p)$ or $r^l \equiv -1 (mod\ p)$. But, since the first case is not possible because $p-1$ is the smallet positive integer with this property, it follows that $r^l \equiv -1 (mod\ p)$. Thus, $r^{\frac{p-1}{2}} + 1 \equiv 0 (mod\ p)$, and therefore,

$$\omega_{d,t} = \zeta_p^{r^{dn}+1} = \zeta_p^{r^{(\frac{p-1}{2n})n}+1} = \zeta_p^{r^{\frac{p-1}{2}}+1} = 1.$$

Reciprocally, if $\omega_{d,t} = 1$, i.e., $\zeta_p^{r^{dn}+r^t} = 1$, then

$$r^{dn} + r^t \equiv 0 (mod\ p) \Leftrightarrow r^{dn} \equiv -r^t (mod\ p).$$

Since $r^{l+t} \equiv -r^t (mod\ p)$, it follows that

$$-r^t (mod\ p) \equiv r^{dn} \equiv r^{l+t} (mod\ p).$$

From [9, Theorem 6.2], it follows that

$$r^{l+t} (mod\ p) l + t \equiv dn (mod\ p - 1).$$

Thus $p-1$ divides $l + t - dn$, i.e., there exists $k_1 \in \mathbb{Z}$ such that $t = dn - l + k_1(p-1)$. Now, $n \mid dn$, $n \mid k_1(p-1)$ (because $n \mid p-1$) and $n \mid l$ (because $n(\frac{p-1}{2n}) = l$), and thus, $n \mid t$. Since $t = 0, 1, \cdots, n-1$, it follows that $t = 0$. Thus, $dn = l - k_1(p-1)$, and therefore,

$$d = \frac{p-1}{2n} - k_1(\frac{p-1}{n}) = \frac{p-1}{2n}(1 - 2k_1) = k_2(\frac{p-1}{2n}), \text{ with } k_2 = 1 - 2k_1 \text{ odd.}$$

Since k_2 is positive, because if $k_2 < 0$, then $d \leq 0$. Thus, $k_2 = 1$ or 2, because if $k_2 \geq 3$, then $d > (p-1)/n$. But, since k_2 is odd, it follows that $k_2 = 1$. Therefore, $d = (p-1)/2n$, which concludes the proof of the equivalency of the Equation (3.1). Observe that the number $\frac{p-1}{2n}$ is integer because $n \mid (p-1)/2$. Now, for $t \neq 0$, from equivalency of the Equation (3.1), it follows that $\omega_{d,t} \neq 1$, and therefore, $\sum_{s=1}^{p-1} (\omega_{d,t})^s = -1$. Thus,

$$Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) = \sum_{d=1}^{\frac{p-1}{n}} \sum_{s=1}^{p-1} (\omega_{d,t})^s = \sum_{d=1}^{\frac{p-1}{n}} -1 = -\left(\frac{p-1}{n}\right).$$

Now, suppose $t = 0$. From equivalency of the Equation (3.1), if $d = (p-1)/2n$, then $\omega_{d,t} = 1$, and if $d \neq (p-1)/2n$, then $\omega_{d,t} \neq 1$. Therefore,

$$\begin{aligned} Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^t(\theta)) &= \sum_{d=1}^{\frac{p-1}{n}} \sum_{s=1}^{p-1} (\omega_{d,t})^s = (p-1) + \sum_{d=1, d\neq \frac{p-1}{2n}}^{\frac{p-1}{n}} -1 \\ &= (p-1) - \left(\tfrac{p-1}{n} - 1\right) = p - \left(\tfrac{p-1}{n}\right). \end{aligned}$$

Since σ^{j-i} ranges in σ^t, with $t = 0, 1, \cdots, n-1$, it follows that

$$Tr_{\mathbb{K}:\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \begin{cases} p - (\frac{p-1}{n}) & \text{if } t = 0 \\ -(\frac{p-1}{n}) & \text{if } t = 1, 2, \cdots, n-1, \end{cases}$$

which concludes the proof. □

4 AN ALGORITHM OF CONSTRUCTION OF A ROTATED LATTICE

In this section, we present an algorithm to construct of a rotated lattice and we analyze if these lattices have good performance in terms of center density and minimum product distance. For this, we consider $\mathbb{K}$ a field such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where p is a prime, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = m$ and $[\mathbb{K} : \mathbb{Q}] = n$.

4.1 Algorithm

An algorithm to construct of a rotated lattice is given by:

1. Choose a dimension n.
2. Compute a prime p such that $p \equiv 1 (mod\ n)$, where n is an even number that divides $(p-1)/2$ or if n is an odd number.
3. Compute r such that r is a primitive element modulo p, i.e., r is a generator of $\mathbb{Z}_p^*$.
4. Compute $\theta = Tr_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta_p)$ and $\sigma^i(\theta)$, for $i = 1, \cdots, n-1$, with $\langle\sigma\rangle = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.

5. Compute the Gram matrix $G = (g_{ij})_{i,j=1}^{n}$, where

$$g_{i,j} = Tr_{\mathbb{K}:\mathbb{Q}}(\theta\sigma^{j-i}(\theta)) = \begin{cases} p - (\frac{p-1}{n}) & \text{if } i = j \\ -(\frac{p-1}{n}) & \text{if } i \neq j, \end{cases}$$

for $i, j = 1, \cdots, n$.

4.2 Center density and minimim distance product

If $\alpha \in \mathscr{O}_{\mathbb{K}}$, where $\alpha = a_0\sigma^0(\theta) + a_1\sigma(\theta) + \cdots + a_{n-1}\sigma^{n-1}(\theta)$, then

$$Tr_{\mathbb{K}:\mathbb{Q}}(\alpha^2) = \sum_{i=0}^{n-1} a_i^2 + m \sum_{0 \leq i < j \leq n-1} (a_i - a_j)^2.$$

If $\mathscr{M}$ is a $\mathbb{Z}$-submodule in $\mathbb{K}$ of rank n, then the set $\Lambda = \sigma_{\mathbb{K}}(\mathscr{M})$ is a lattice in $\mathbb{R}^n$ called an algebraic lattice. The center density of Λ is given by

$$\delta(\Lambda) = \frac{t^{n/2}}{2^n[\mathscr{O}_{\mathbb{K}} : \mathscr{M}]\sqrt{|\Delta_{\mathbb{K}}|}},$$

where $t = \min\left\{Tr_{\mathbb{K}:\mathbb{Q}}(\alpha^2) : \alpha \in \mathscr{M}, \alpha \neq 0\right\}$, $[\mathscr{O}_{\mathbb{K}} : \mathscr{M}]$ denotes the index of the submodule $\mathscr{M}$ and $\Delta_{\mathbb{K}} = p^{n-1}$ [**?**]. If $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is 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

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

If $\mathscr{M}$ is a principal ideal of $\mathscr{O}_{\mathbb{K}}$, then the minimum product distance of Λ is given by

$$d_{p,\min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{\Delta_{\mathbb{K}}}},$$

where $\det(\Lambda) = \det G$ [7, Theorem 1]. The normalized minimum product distance of Λ, $d_{p,norm}(\Lambda)$, is the minimum product distance of the rotated lattice $\frac{1}{\sqrt[2n]{\det(G)}}\Lambda$. Thus, the normalized minimum product distance of Λ is given by

$$d_{p,norm}(\Lambda) = \frac{1}{(\sqrt{k})^n}\frac{1}{\sqrt{\det(G)}}d_{p,min}(\Lambda) = \frac{1}{(\sqrt{k})^n}\frac{1}{\sqrt{\Lambda}},$$

where $k = min\{\| x \|^2 : 0 \neq x \in \Lambda\}$. Thus,

$$\sqrt[n]{d_{p,norm}(\Lambda)} = \frac{1}{\sqrt{k}}\frac{1}{\sqrt[2n]{\Lambda}}.$$

4.3 Example

If $\mathbb{L} = \mathbb{Q}(\zeta_5)$ and $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta = \zeta_5 + \zeta_5^{-1}$, then $n = 2$, $t = 2$, $\Delta_{\mathbb{K}} = 5$,

$$G = \begin{pmatrix} 3 & -2 \\ -2 & 3 \end{pmatrix}$$

is the Gram matrix of the algebraic lattice $\sigma(\mathscr{O}_{\mathbb{K}})$, $k = 2$ and $\det(G) = 5$. In this case, the center density is given by $\delta(\Lambda) = 1/(2\sqrt{5})$ and the normalized minimum product distance. Since $k = 2$, it follows that $\sqrt{d_{p,norm}(\Lambda)} = \frac{1}{\sqrt{2}}\frac{1}{\sqrt[4]{5}} \simeq 0.47287$. In the Table 1, we summarized a comparision of the values of $\delta(\mathscr{M})$, where $\mathscr{M} = \mathscr{O}_{\mathbb{K}}$, and $\sqrt[n]{d_{p,norm}(\Lambda)}$ for some known constructions of algebraic lattices in some dimensions.

Table 1: Comparison of the values of $\delta(\mathscr{M})$ [4] and $\sqrt[n]{d_{p,norm}(\Lambda)}$ [7].

p	n	$\delta(\mathscr{M})$	known	$\sqrt[n]{d_{p,norm}(\Lambda)}$	known
5	2	0.22360	0.28868	0.47287	0.66874030
7	3	0.09278	0.17678	0.30181	0.52275795
11	5	0.01443	0.08839	0.17137	0.38321537
13	6	0.00553	0.07217	0.14021	0.34344479
13	3	0.02400	0.17678	0.24554	0.28952001
13	2	0.13867	0.28868	0.372309	0.27018738

5 ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their intuitive comentary that significantly improved the worth of this work.

RESUMO. A teoria de reticulados têm mostrado útil na teoria da informação e reticulados ideais com alta diversidade de modulação têm sido extensamente estudados como uma alternativa de transmissão via o canal de Rayleigh, onde o desempenho destes esquemas de modulação depende essencialmente da diversidade de modulação e da distância produto mínima para obter ganhos substanciais de codificação. A diversidade máxima de um reticulado rotacionado é garantida quando usamos corpos de números totalmente reais e a distância produto mínima é otimizada considerando os corpos com discriminante mínimo. Neste trabalho, apresentamos uma construção de reticulado rotacionado, onde esta construção é através de um subcorpo totalmente real $\mathbb{K}$ do p-ésimo corpo ciclotômico, onde p é um número primo ímpar, obtido via o seu anel de inteiros.

Palavras-chave: reticulados, corpos ciclotômicos, corpos de números algébricos, reticulado rotacionado.

REFERENCES

[1] A.A. Andrade & J.C. Interlando. Rotated $\mathbb{Z}^n$-lattices via real subfields of $\mathbb{Q}(\zeta_{2^r})$. *TEMA - Trends in Applied and Computational Mathematics*, **39**(3) (2019).

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

[3] 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.

[4] J.H. Conway & N.J.A. Sloane. "Sphere Packings, Lattices and Groups". Springer-Verlag (1998).

[5] A. de Andrade & R. Palazzo Jr. Linear codes over finite rings. *TEMA - Trends in Applied and Computational Mathematics*, **6**(2) (2005), 207–217.

[6] B. Erez. The Galois structure of the trace form in extensions of odd prime degree. *Journal of Algebra*, **118**(2) (1988), 438–446.

[7] F. Oggier, E. Bayer-Fluckiger & E. Viterbo. New algebraic constructions of rotated cubic lattice constellations for the Rayleigh fading channel. In "Proceedings 2003 IEEE Information Theory Workshop (Cat. No. 03EX674)". IEEE (2003), pp. 263–266.

[8] P. Ribenboim. "Classical theory of algebraic numbers". Springer Science & Business Media (2013).

[9] J.P.O. Santos. "Introduction to numbers theory, Projeto Euclides". Impa (2006).

[10] J.P. Serre. "A course in arithmetic", volume 7. Springer Science & Business Media (2012).