

Constructions of Dense Lattices of Full Diversity

A. A. ANDRADE^{1*}, A. J. FERRARI², J. C. INTERLANDO³ and R.R. ARAUJO⁴

Received on June 13, 2019 / Accepted on March 19, 2020

ABSTRACT. A lattice construction using \mathbb{Z} -submodules of rings of integers of number fields is presented. The construction yields rotated versions of the laminated lattices Λ_n for $n = 2, 3, 4, 5, 6$, which are the densest lattices in their respective dimensions. The sphere packing density of a lattice is a function of its packing radius, which in turn can be directly calculated from the minimum squared Euclidean norm of the lattice. Norms in a lattice that is realized by a totally real number field can be calculated by the trace form of the field restricted to its ring of integers. Thus, in the present work, we also present the trace form of the maximal real subfield of a cyclotomic field. Our focus is on totally real number fields since their associated lattices have full diversity. Along with high packing density, the full diversity feature is desirable in lattices that are used for signal transmission over both Gaussian and Rayleigh fading channels.

Keywords: sphere packings, algebraic lattices, number fields, cyclotomic fields.

1 INTRODUCTION

Lattices are discrete subgroups of Euclidean n -space, \mathbb{R}^n , and they have been considered in different applied areas, especially in coding/modulation theory and more recently in cryptography. Algebraic lattices are those obtained via number fields and they have been studied in several papers and from different points of view, see [1, 2, 3, 5, 6, 10]. These algebraic lattices are constructed through the canonical homomorphism via \mathbb{Z} -modules of the ring of algebraic integers of a number field. Having the construction of algebraic lattices as our goal, in this paper, we focus on the construction of algebraic lattices with special features, known in the literature, via maximal real subfields of cyclotomic fields. In digital communications, the lattice parameters of interest are its

*Corresponding author: Antonio Aparecido de Andrade – E-mail: antonio.andrade@unesp.br

¹Departamento de Matemática, Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista “Júlio de Mesquita Filho” (Unesp), Campus de São José do Rio Preto, SP, Brasil – E-mail: antonio.andrade@unesp.br <https://orcid.org/0000-0001-6452-2236>.

²Departamento de Matemática, Faculdade de Ciências (FC), Universidade Estadual Paulista “Júlio de Mesquita Filho” (Unesp), Campus de Bauru, SP, Brasil – E-mail: agnaldo.ferrari@unesp.br <https://orcid.org/0000-0002-1422-1416>

³Department of Mathematics & Statistics, San Diego State University, San Diego, California, USA – E-mail: interlan@sdu.edu <https://orcid.org/0000-0003-4928-043X>.

⁴Instituto Federal de São Paulo, Cubatão, SP, Brasil – E-mail: dearaujobonricardo@gmail.com <https://orcid.org/0000-0002-1357-9926>

sphere packing density and minimum product distance. The performance in terms of minimum product distance is given by number field discriminant, i.e., minimizing the discriminant. The question of find totally real number fields with minimal discriminant is a hard problem. Those parameters can be obtained in certain cases of lattices associated to number fields through algebraic properties [6]. From [4, Theorem 4.1], we can to give a lower (and upper) bound on the minimum product distance. The higher those two parameters are the more attractive the lattice becomes to be used for data transmission over Gaussian and fading channels.

We can find, in literature, several constructions of full diversity rotated \mathbb{Z}^n -lattices [5, 6, 7, 8]. In [6], it was shown that algebraic lattices obtained via totally real number fields have full diversity. In [8] the authors presented constructions of algebraic lattices over totally real fields and in [7] the authors presented constructions of lattices and the trace form for $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$. In this work, we focus our construction on totally real number fields and we present the trace form for $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, where $n \geq 5$, where we present constructions of algebraic lattices of full diversity and optimal packing density. In full diversity algebraic lattices, the minimum product distance depends on the minimum of the algebraic norm of nonzero elements in the lattice. This gives an advantage provided by the algebraic tools, once to calculate the minimum product distance in a general lattice is a hard problem.

In this paper, we present constructions of algebraic lattices of optimal center density and full diversity, that is, we present constructions of algebraic lattices on totally real number fields. In the first construction, the fields are the maximal real subfields of cyclotomic fields, and in the second construction, the fields \mathbb{K} are extensions of \mathbb{Q} of degree p where p is an odd ramified prime in $\mathcal{O}_{\mathbb{K}}$, the ring of integers of \mathbb{K} . In Section 2, we review necessary concepts from number fields and lattices. In Section 3, we present explicit trace forms over the maximal totally real subfield of cyclotomic fields. In Section 4, we present constructions of laminated algebraic lattices in dimensions 2 up to 6 with optimal center density. In Section 5 we give our conclusions.

2 BASIC RESULTS OVER ALGEBRAIC LATTICES AND NUMBER FIELDS

In this section, we briefly review the definitions and results that will be needed subsequently. Many of them will be assumed known to the reader; those interested in further details are referred to [10, 14].

Let Λ be a full lattice in \mathbb{R}^n , that is, Λ is the set of all integral linear combinations of some basis of the vector space \mathbb{R}^n . Let τ denote half the minimal distance between (distinct) lattice points. We can then immediately construct a sphere packing from Λ by centering an n -dimensional sphere with radius τ at each lattice point. The obtained arrangement is called the sphere packing associated to Λ . The proportion of the space that is occupied by the spheres is called the sphere packing density of Λ , denoted by $\Delta(\Lambda)$. For comparison purposes, a more used parameter is the center density of the packing, denoted by $\delta(\Lambda)$, which in turn equals $\Delta(\Lambda)$ divided by V_n , the volume of an n -dimensional sphere of radius 1.

The minimum product distance of Λ is defined as

$$d_{p,\min}(\Lambda) = \min \left\{ \prod_{i=1}^n |x_i| : \mathbf{0} \neq (x_1, \dots, x_n) \in \Lambda \right\}.$$

Lattice Λ is said to be of full diversity if $d_{p,\min}(\Lambda) \neq 0$. In the present work, we will only be concerned with constructing lattices with a high sphere packing density and full diversity.

A number field \mathbb{K} is said to be Abelian (cyclic) if the extension \mathbb{K}/\mathbb{Q} is Galois and its Galois group, $Gal(\mathbb{K}/\mathbb{Q})$, is Abelian (cyclic). Let \mathbb{K} be a number field of degree n and signature $[r_1, r_2]$. The \mathbb{Q} -monomorphisms of \mathbb{K} into \mathbb{C} whose images are contained in \mathbb{R} are denoted by $\sigma_1, \dots, \sigma_{r_1}$, and those whose images are not contained in \mathbb{R} are denoted by $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$.

The set $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \text{there is a monic polynomial } f(x) \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0\}$ is called the ring of algebraic integers of \mathbb{K} . If $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a \mathbb{Z} -basis of $\mathcal{O}_{\mathbb{K}}$, the integer $d_{\mathbb{K}} = (\det(\sigma_j(\alpha_i))_{i,j=1}^n)^2$ is an invariant over change of basis and is called the discriminant of \mathbb{K} . The trace of any element $x \in \mathcal{O}_{\mathbb{K}}$ is defined by $Tr_{\mathbb{K}/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$.

If $\Re(x)$ and $\Im(x)$ denote, respectively, the real and imaginary parts of $x \in \mathbb{K}$, then the canonical homomorphism $\sigma : \mathbb{K} \rightarrow \mathbb{R}^n$ is defined by

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \dots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))),$$

for every $x \in \mathbb{K}$. If \mathcal{M} is a \mathbb{Z} -module of \mathbb{K} of rank n , the set $\Lambda = \sigma(\mathcal{M})$ is an n -dimensional lattice in \mathbb{R}^n . If either $r_1 = 0$ or $r_2 = 0$, then the center density of Λ is given by

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

where $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ denotes the index of \mathcal{M} in $\mathcal{O}_{\mathbb{K}}$, and

$$t = c_k \min \{ Tr_{\mathbb{K}/\mathbb{Q}}(x\bar{x}) : x \in \mathcal{M}, x \neq 0 \}$$

with $c_k = 1$ or 2^{-1} according to whether $r_2 = 0$ or $r_1 = 0$, respectively. The quantity $2^n [\mathcal{O}_{\mathbb{K}} : \mathcal{M}] \sqrt{|d_{\mathbb{K}}|}$ is equal to the volume of $\sigma(\mathcal{M})$. Lattices constructed from totally real number fields, i.e., those with $r_2 = 0$, always have full diversity, a desirable property for practical applications as already observed.

3 TRACE FORMS OVER SUBFIELDS OF CYCLOTOMIC FIELDS

In this section, we present an explicit trace form over maximal real subfield of $\mathbb{Q}(\zeta_n)$ that allow us to find the packing radius of algebraic lattices. In Subsection 3.1, we present explicit trace forms over the maximal totally real subfield of cyclotomic field $\mathbb{Q}(\zeta_n)$. Thus, in Theorem 2, we present the trace form for any n , in the Corollaries 1, 2 and 3, for $n = p^r$, $n = 2p^r$ and $n = pq$, respectively, where p and q are prime numbers and r an integer such that $r \geq 1$. We present it again in the Subsection 3.2, since it will be used in the next section for the constructions of laminated lattices.

3.1 Trace form over maximal real subfield of $\mathbb{Q}(\zeta_n)$

A number field \mathbb{L} is said to be cyclotomic if $\mathbb{L} = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n -th root of unity. Furthermore, $[\mathbb{L} : \mathbb{Q}] = \varphi(n)$, where φ is Euler’s phi function, the ring of algebraic integers of \mathbb{L} is given by $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n]$ and $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\varphi(n)-1}\}$ is an integral basis for \mathbb{L} . If $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$, then $[\mathbb{K} : \mathbb{Q}] = \varphi(n)/2$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ and $\{\zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \dots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{-\frac{\varphi(n)}{2}}\}$ is an integral basis of $\mathcal{O}_{\mathbb{K}}$ [14].

Let $n = p_1 p_2 \dots p_{k+1}$, where the p_i are distinct prime numbers, $a = p_1 p_2 \dots p_k$ and $b = p_{k+1}$. Observe that $\zeta_a = \zeta_n^b$ and $\zeta_b = \zeta_n^a$, whence $\mathbb{Q}(\zeta_a, \zeta_b) \subseteq \mathbb{Q}(\zeta_n)$. On the other hand, since $\gcd(a, b) = 1$, one has $au + bv = 1$ for some $u, v \in \mathbb{Z}$. Thus,

$$\zeta_n = \zeta_n^{au+bv} = \zeta_n^{au} \zeta_n^{bv} = \zeta_b^u \zeta_a^v$$

and $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_a, \zeta_b)$, that is, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_a, \zeta_b)$. Furthermore, $\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}$ because $\gcd(a, b) = 1$. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an Abelian extension, it follows that $\mathbb{Q}(\zeta_n)/\mathbb{F}$ and \mathbb{F}/\mathbb{Q} , for any $\mathbb{F} \subseteq \mathbb{Q}(\zeta_n)$, are Abelian extensions. Finally, the mapping

$$\begin{aligned} \sigma : Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)) &\longrightarrow Gal(\mathbb{Q}(\zeta_b)/\mathbb{Q}) \\ \sigma &\longmapsto \sigma|_{\mathbb{Q}(\zeta_b)} \end{aligned}$$

is an isomorphism. Furthermore, if $\alpha \in \mathbb{Q}(\zeta_b)$, then

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)}(\alpha) = Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\alpha).$$

Lemma 1. [11] *Let j and n be integers. If $\gcd(j, n) = d$, then*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{\varphi(n)}{\varphi(n/d)} Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}).$$

Lemma 2. [11] *If i, j and p are integers with $i \geq 1$, p prime and $\gcd(j, p) = 1$, then*

$$Tr_{\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}}(\zeta_{p^i}^j) = \begin{cases} -1 & \text{if } i = 1, \\ 0 & \text{if } i > 1. \end{cases}$$

Lemma 3. [11] *Let $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ with $a_k \geq 1$ for $k = 1, 2, \dots, s$. If j is prime and $\gcd(j, n) = d$, then*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{\varphi(n)}{\varphi(n/d)} \mu(n/d),$$

where μ is the Möbius function.

Lemma 4. [11] *Let $n = p_1^{a_1} \dots p_s^{a_s}$, where $a_k \geq 1$ for $k = 1, 2, \dots, s$. If i is an integer such that $i < \varphi(n)$ and $d = \gcd(i, n)$, then*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) \neq 0 \Leftrightarrow d = (n/P)t_j \text{ and } i = (n/P)j,$$

where $P = p_1 \cdots p_s$, $t_j = \gcd(j, P)$ and $j = 1, 2, \dots, \varphi(P) - 1$.

Theorem 5. [11] Let $n = p_1^{a_1} \cdots p_s^{a_s}$, with $a_k \geq 1$, for $k = 1, 2, \dots, s$, $m = \varphi(n)$. If $x = a_0 + a_1 \zeta_n + \cdots + a_{m-1} \zeta_n^{m-1}$ is an element of $\mathbb{Z}[\zeta_n]$, then

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x\bar{x}) = \frac{n}{P} \left\{ \varphi(P) \sum_{i=0}^{m-1} a_i^2 + 2 \sum_{j=1}^{\varphi(P)-1} \mu \left(\frac{P}{t_j} \right) \varphi(t_j) A_{\frac{n}{P}j} \right\},$$

where $P = p_1 \cdots p_s$, $t_j = \gcd(j, P)$ for $j = 1, 2, \dots, \varphi(P) - 1$, and $A_i = a_0 a_i + a_1 a_{i+1} + \cdots + a_{m-1-i} a_{m-1}$ for $i = 1, 2, \dots, m - 1$. In the next result, we present an explicit trace form over the ring of algebraic integers of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Theorem 6. Let $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, where $n = p_1^{a_1} \cdots p_s^{a_s}$, with $a_j \geq 1$ for $j = 1, 2, \dots, s$ and $m = \varphi(n)$. If $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{\frac{\varphi(n)}{2}}(\zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{-\frac{\varphi(n)}{2}})$ is an element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, then

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = m \sum_{i=1}^{m/2} a_i^2 + \frac{n}{P} \left(\sum_{\substack{i=u \\ 2 \mid \frac{n}{P}i}}^{\varphi(P)} \rho(t_i) a_{\frac{n}{2P}i}^2 + 2 \sum_{i=1}^s \rho(t_i) A_{\frac{n}{P}i} + 2 \sum_{i=v}^{\varphi(P)-1} \rho(t_i) B_{\frac{n}{P}i} \right),$$

where $P = p_1 \cdots p_s$, $t_i = \gcd(i, P)$, $\lfloor y \rfloor$ is the greatest integer less than or equal to y , $\lceil y \rceil$ is the smallest integer greater than or equal to y , $u = \lceil \frac{2P}{n} \rceil$, $s = \lfloor \frac{\varphi(P)}{2} - 1 \rfloor$, $v = \lceil \frac{3P}{n} \rceil$, $\rho(t_i) = \mu \left(\frac{P}{t_i} \right) \varphi(t_i)$, $A_j = a_1 a_{j+1} + a_2 a_{j+2} + \cdots + a_{\frac{m}{2}-j} a_{\frac{m}{2}}$ and $B_j = \sum_{\substack{k \geq 1 \\ k < j-k \leq \frac{m}{2}}} a_k a_{j-k}$. **Proof.** If $x \in \mathcal{O}_{\mathbb{K}}$,

then

$$x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{\frac{m}{2}}(\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}})$$

where $a_i \in \mathbb{Z}$, for $i = 1, 2, \dots, \frac{\varphi(n)}{2}$. Therefore,

$$\begin{aligned} x^2 &= (a_1 \zeta_n + a_1 \zeta_n^{-1} + \cdots + a_{\frac{m}{2}} \zeta_n^{-\frac{m}{2}})(a_1 \zeta_n + a_1 \zeta_n^{-1} + \cdots + a_{\frac{m}{2}} \zeta_n^{-\frac{m}{2}}) \\ &= [(a_1 \zeta_n + a_2 \zeta_n^2 + \cdots + a_{\frac{m}{2}} \zeta_n^{\frac{m}{2}}) + (a_1 \zeta_n^{-1} + a_2 \zeta_n^{-2} + \cdots + a_{\frac{m}{2}} \zeta_n^{-\frac{m}{2}})]^2 \\ &= A^2 + \bar{A}^2 + 2A\bar{A}, \end{aligned}$$

where $A = a_1 \zeta_n + a_2 \zeta_n^2 + \cdots + a_{\frac{m}{2}} \zeta_n^{\frac{m}{2}}$. So,

$$x^2 = \sum_{j=1}^{m/2} a_j^2 (\zeta_n^{2j} + \zeta_n^{-2j}) + 2 \left(\sum_{j=3}^{m-1} B_j \beta_j \right) + 2 \left(\sum_{j=1}^{m/2} a_j^2 + \sum_{j=1}^{m/2-1} A_j \beta_j \right),$$

where $A_j = a_1 a_{j+1} + a_2 a_{j+2} + \cdots + a_{\frac{m}{2}-j} a_{\frac{m}{2}}$, $B_j = \sum_{\substack{k \geq 1 \\ k < j-k \leq \frac{m}{2}}} a_k a_{j-k}$, and $\beta_j = \zeta_n^j + \zeta_n^{-j}$. Since

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x^2) = [\mathbb{Q}(\zeta_n) : \mathbb{K}] Tr_{\mathbb{K}/\mathbb{Q}}(x^2),$$

it follows that

$$t = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) = \frac{1}{2} \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x^2).$$

Thus,

$$\begin{aligned} t &= \frac{1}{2} \left[\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \left(2 \sum_{j=1}^{m/2} a_j^2 + 2 \sum_{j=1}^{m/2-1} A_j \beta_j + \sum_{j=1}^{m/2} a_j^2 (\zeta_n^{2j} + \zeta_n^{-2j}) + 2 \sum_{j=3}^{m-1} B_j \beta_j \right) \right] \\ &= m \sum_{j=1}^{m/2} a_j^2 + \sum_{j=1}^{m/2} a_j^2 \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{2j}) \\ &\quad + 2 \left(\sum_{j=1}^{m/2-1} A_j \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) + \sum_{j=3}^{m-1} B_j \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) \right). \end{aligned}$$

From Lemmas 3 and 4, it follows that

$$\begin{aligned} \sum_{j=1}^{m/2} a_j^2 \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{2j}) &= \frac{n}{P} \sum_{\substack{i=u \\ 2 \mid \frac{n}{P} i}}^{\varphi(P)} \mu \left(\frac{P}{t_i} \right) \varphi(t_i) a_{\frac{n}{2P} i}^2, \\ \sum_{j=1}^{m/2-1} A_j \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) &= \frac{n}{P} \sum_{i=1}^s \mu \left(\frac{P}{t_i} \right) \varphi(t_i) A_{\frac{n}{P} i}, \\ \sum_{j=3}^{m-1} B_j \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) &= \sum_{i=v}^{\varphi(P)-1} \mu \left(\frac{P}{t_i} \right) \varphi(t_i) B_{\frac{n}{P} i}, \end{aligned}$$

where $u, s,$ and v are as in the theorem statement. Therefore,

$$\text{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) = m \sum_{i=1}^{m/2} a_i^2 + \frac{n}{P} \left(\sum_{\substack{i=u \\ 2 \mid \frac{n}{P} i}}^{\varphi(P)} \rho(t_i) a_{\frac{n}{2P} i}^2 + 2 \sum_{i=1}^s \rho(t_i) A_{\frac{n}{P} i} + 2 \sum_{i=v}^{\varphi(P)-1} \rho(t_i) B_{\frac{n}{P} i} \right),$$

as desired. □

Corollary 7. *Let $n = p^r$, with p an odd prime number and r a positive integer. If $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \dots + a_{\frac{\varphi(p^r)}{2}}(\zeta_n^{\frac{\varphi(p^r)}{2}} + \zeta_n^{-\frac{\varphi(p^r)}{2}})$ is an element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, then*

$$\text{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) = \varphi(p^r) \sum_{i=1}^{\frac{\varphi(p^r)}{2}} a_i^2 - p^{r-1} \left(\sum_{\substack{i=u \\ 2 \mid \frac{n}{P} i}}^{p-1} a_{i p^{r-1}}^2 + 2 \sum_{i=1}^{\frac{p-3}{2}} A_{i p^{r-1}} + 2 \sum_{i=v}^{p-2} B_{i p^{r-1}} \right),$$

where $u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$, $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$, $A_j = a_1 a_{j+1} + a_2 a_{j+2} + \dots + a_{\frac{\varphi(p^r)}{2}-j} a_{\frac{\varphi(p^r)}{2}}$ and $B_j = \sum_{k \geq 1} a_k a_{j-k}$. **Proof.** Since $P = p$, it follows that $\frac{n}{P} = p^{r-1}$ and $\varphi(P) = p - 1$. Thus, from

Theorem 6, it follows that $u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$, $s = \frac{p-3}{2}$, and $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$. Now, $t_i = \text{gcd}(i, P) = \text{gcd}(i, p) = 1$, because $1 \leq i \leq p - 1$, hence $\rho(t_i) = \mu \left(\frac{P}{t_i} \right) \varphi(t_i) = \mu(p) \varphi(1) = -1$. The result now follows from Theorem 6. □

Corollary 8. Let $n = 2p^r$, where p is an odd prime number and r is a positive integer. If $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \dots + a_{\frac{\varphi(2p^r)}{2}}(\zeta_n^{\frac{\varphi(2p^r)}{2}} + \zeta_n^{-\frac{\varphi(2p^r)}{2}})$ is an element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, then

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = \varphi(2p^r) \sum_{i=1}^{\frac{\varphi(2p^r)}{2}} a_i^2 - p^{r-1} \left(\sum_{\substack{i=u \\ 2|i}}^{p-1} a_i^2 - 2U + 2V \right),$$

where $U = \sum_{\substack{i=1 \\ 2|i}}^{\frac{p-3}{2}} A_{ip^{r-1}} + \sum_{\substack{i=v \\ 2|i}}^{p-2} B_{ip^{r-1}}$, $V = \sum_{\substack{i=1 \\ 2|i}}^{\frac{p-3}{2}} A_{ip^{r-1}} + \sum_{\substack{i=v \\ 2|i}}^{p-2} B_{ip^{r-1}}$, $u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$, $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$, $A_j =$

$a_1 a_{j+1} + a_2 a_{j+2} + \dots + a_{\frac{\varphi(2p^r)}{2}-j} a_{\frac{\varphi(2p^r)}{2}}$, and $B_j = \sum_{\substack{k \geq 1 \\ k < j-k \leq \frac{\varphi(2p^r)}{2}}} a_k a_{j-k}$. **Proof.** Since $P = 2p$, it

follows that $\frac{n}{P} = p^{r-1}$, and $\varphi(P) = p - 1$. From Theorem 6, it follows that $u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$, $s = \frac{p-3}{2}$ and $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$. Also,

$$t_i = \gcd(i, P) = \gcd(i, 2p) = \begin{cases} 1 & \text{if } i \text{ is odd,} \\ 2 & \text{if } i \text{ is even.} \end{cases}$$

Therefore,

$$\rho(t_i) = \begin{cases} 1 & \text{if } i \text{ is odd,} \\ -1 & \text{if } i \text{ is even.} \end{cases}$$

Since p is odd, it follows that $\frac{n}{P} = p^{r-1}$ is odd. So, $\frac{n}{P}i$ is even if and only if i is even. The result now follows from Theorem 6. □

Corollary 9. Let $n = pq$, where p and q are distinct primes. If $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \dots + a_{\frac{\varphi(pq)}{2}}(\zeta_n^{\frac{\varphi(pq)}{2}} + \zeta_n^{-\frac{\varphi(pq)}{2}})$ is an element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, then

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = \varphi(pq) \sum_{i=1}^{\frac{\varphi(pq)}{2}} a_i^2 + U + 2V + 2W,$$

where

$$\begin{aligned}
 s &= \left\lfloor \frac{\varphi(pq) - 1}{2} \right\rfloor, \quad A_j = a_1 a_{j+1} + a_2 a_{j+2} + \dots + a_{\frac{\varphi(pq)}{2} - j} a_{\frac{\varphi(pq)}{2}}, \\
 B_j &= \sum_{\substack{k \geq 1 \\ k < j - k \leq \frac{\varphi(pq)}{2}}} a_k a_{j-k}, \\
 U &= -(p-1) \sum_{\substack{i=2 \\ 2p|i}}^{\frac{\varphi(pq)}{2}} a_{\frac{i}{2}}^2 - (q-1) \sum_{\substack{i=2 \\ 2q|i}}^{\frac{\varphi(pq)}{2}} a_{\frac{i}{2}}^2 + \sum_{\substack{i=2 \\ 2|i, \gcd(i,pq)=1}}^{\frac{\varphi(pq)}{2}} a_{\frac{i}{2}}^2, \\
 V &= -(p-1) \sum_{\substack{i=1 \\ p|i}}^s A_i - (q-1) \sum_{\substack{i=1 \\ q|i}}^s A_i + \sum_{\substack{i=1 \\ \gcd(i,pq)=1}}^s A_i, \\
 W &= -(p-1) \sum_{\substack{i=3 \\ p|i}}^{\frac{\varphi(pq)-1}{2}} B_i - (q-1) \sum_{\substack{i=3 \\ q|i}}^{\frac{\varphi(pq)-1}{2}} B_i + \sum_{\substack{i=3 \\ \gcd(i,pq)=1}}^{\frac{\varphi(pq)-1}{2}} B_i.
 \end{aligned}$$

Proof. From Theorem 5, $m = \varphi(pq) = \varphi(P)$, $\mu(P) = \mu(pq) = 1$, and $t_j = \gcd(j, P)$ with $j = 1, 2, \dots, \varphi(pq) - 1$. Thus,

$$t_j = \gcd(j, pq) = \begin{cases} p & \text{if } j \text{ is a multiple of } p \\ q & \text{if } j \text{ is a multiple of } q \\ 1 & \text{otherwise,} \end{cases}$$

and

$$\rho(t_i) = \begin{cases} -(p-1) & \text{if } j \text{ is a multiple of } p \\ -(q-1) & \text{if } j \text{ is a multiple of } q \\ 1 & \text{otherwise.} \end{cases}$$

Furthermore, $\frac{n}{p}j = j$. Thus, if $n = pq$ and $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \dots + a_{\frac{m}{2}}\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}}$ is an element of $\mathbb{Z}[\zeta_n]$. The result now follows from Theorem 6. □

3.2 Trace form over cyclic number fields of degree p

In [13], a lattice construction using cyclic number fields of degree p , where p is unramified, was presented. Lattices whose center densities are arbitrarily close to optimal values were obtained. Below we present a similar construction, in this case using cyclic number fields of degree p , where p is ramified. Let \mathbb{K} be a cyclic number field of prime degree $p > 2$. From Kronecker-Weber Theorem [14], it follows that there exists $n > 0$ such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$. The least integer n with the property $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ is called the conductor of \mathbb{K} . In this case, the discriminant of \mathbb{K} is given by $d_{\mathbb{K}} = n^{p-1}$ [9, p. 186]. If n is the conductor of a cyclic number field \mathbb{K} of odd prime degree p , then

1. p is ramified in \mathbb{K} if and only if $n = p^2$ or $n = p^2 p_1 p_2 \dots p_r$;
2. p is unramified in \mathbb{K} if and only if $n = p_1 p_2 \dots p_r$,

where $r \geq 1$ and the p_i are distinct prime numbers such that $p_i \equiv 1 \pmod{p}$.

Let \mathbb{K} be a cyclic number field of degree p and conductor $n = p^2$ or $n = p^2 p_1 p_2 \cdots p_r$, where the p_i are distinct prime numbers such that $p_i \equiv 1 \pmod{p}$. From [12], if $t = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, then

1. $\mathbb{K} = \mathbb{Q}(t)$.
2. $\mathcal{B} = \{1, \sigma(t), \dots, \sigma^{p-1}(t)\}$ is a \mathbb{Z} -basis for $\mathcal{O}_{\mathbb{K}}$.

Theorem 10. [3] *Let \mathbb{K} be a cyclic number field of prime degree $p > 2$, $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, where $n = p^2 p_1 p_2 \cdots p_r$ with $r \geq 1$ and the p_i distinct prime numbers such that $p_i \equiv 1 \pmod{p}$. If $x = a_0 + \sum_{i=1}^{p-1} a_i \sigma^i(t) \in \mathcal{O}_{\mathbb{K}}$, where $a_i \in \mathbb{Z}$, for $i = 1, 2, \dots, p-1$, then*

$$\begin{aligned} \text{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) &= pa_0^2 + pp_1 \cdots p_r \left(-2 \sum_{1 \leq i < j \leq p-1} a_i a_j + (p-1) \sum_{i=1}^{p-1} a_i^2 \right) \\ &= pa_0^2 + pp_1 \cdots p_r \left(\sum_{i=1}^{p-1} a_i^2 + \sum_{1 \leq i < j \leq p-1} (a_i - a_j)^2 \right). \end{aligned}$$

4 CONSTRUCTIONS OF LAMINATED ALGEBRAIC LATTICES OVER NUMBER FIELDS

In this section, we explicit constructions of algebraic densest lattices in dimensions 2 up to 6. The strategy used is to search for submodules contained in the ring of algebraic integers that perform the laminated lattices via canonical homomorphism. In this sense, we use center density as a parameter, so the trace forms (Theorem 6 and Theorem 10) are important for calculating the packing radius.

4.1 The Λ_2 -laminated lattice

If $\mathbb{K} = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 2$, $\{\zeta_{12} + \zeta_{12}^{-1}, \zeta_{12}^2 + \zeta_{12}^{-2}\}$ is an integral basis for \mathbb{K} and $d_{\mathbb{K}} = 12$. If

$$\mathcal{M} = \{a_1(\zeta_{12} + \zeta_{12}^{-1}) + a_2(\zeta_{12}^2 + \zeta_{12}^{-2}) \in \mathcal{O}_{\mathbb{K}} : a_1 + a_2 \equiv 0 \pmod{2}\},$$

then \mathcal{M} is a \mathbb{Z} -submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 2 and index 2. From Theorem 6, the trace form of $\alpha \in \mathcal{M}$ is given by

$$\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 8(a_1^2 - a_1 a_2 + a_2^2).$$

Thus, $t = \min\{\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\} = 8$, which is attained at $a_1 = 1$ and $a_2 = 0$. Since the volume of lattice $\sigma(\mathcal{M})$ equals $2^2 \sqrt{|d_{\mathbb{K}}|} [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 2^4 \sqrt{3}$, it follows that

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{2^3})^2}{2^4 \sqrt{3}} = \frac{1}{2\sqrt{3}},$$

i.e., the center density of $\sigma(\mathcal{M})$ is the same as that of lattice Λ_2 .

4.2 The Λ_3 -laminated lattice

If $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 3$, $\{\zeta_9 + \zeta_9^{-1}, \zeta_9^2 + \zeta_9^{-2}, \zeta_9^3 + \zeta_9^{-3}\}$ is an integral basis for \mathbb{K} and $d_{\mathbb{K}} = 3^4$. If

$$\mathcal{M} = \{a_1(\zeta_9 + \zeta_9^{-1}) + a_2(\zeta_9^2 + \zeta_9^{-2}) + a_3(\zeta_9^3 + \zeta_9^{-3}) \in \mathcal{O}_{\mathbb{K}} : 4a_1 + 4a_2 + a_3 \equiv 0 \pmod{6} \text{ and } a_3 \equiv 0 \pmod{2}\},$$

then \mathcal{M} is a \mathbb{Z} -submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 3 and index 6. From Theorem 6, the trace form of $\alpha \in \mathcal{M}$ is given by

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 18(a_1^2 + a_1a_2 + 4a_1a_3 + a_2^2 + 4a_2a_3 + 2a_3^2).$$

Thus, $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\} = 18$, which is attained at $a_1 = 1$ and $a_2 = a_3 = 0$. Since the volume of lattice $\sigma(\mathcal{M})$ equals $2^3 \sqrt{|d_{\mathbb{K}}|} [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 2^4 \cdot 3^3$, it follows that

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{2 \cdot 3^2})^3}{2^4 \cdot 3^3} = \frac{1}{4\sqrt{2}},$$

i.e., the center density of $\sigma(\mathcal{M})$ is the same as that of lattice Λ_3 .

4.3 The Λ_4 -laminated lattice

If $\mathbb{K} = \mathbb{Q}(\zeta_{24} + \zeta_{24}^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 4$, $\{\zeta_{24} + \zeta_{24}^{-1}, \zeta_{24}^2 + \zeta_{24}^{-2}, \zeta_{24}^3 + \zeta_{24}^{-3}, \zeta_{24}^4 + \zeta_{24}^{-4}\}$ is an integral basis for \mathbb{K} and $d_{\mathbb{K}} = 2^8 \cdot 3^2$. If

$$\mathcal{M} = \{a_1(\zeta_{24} + \zeta_{24}^{-1}) + a_2(\zeta_{24}^2 + \zeta_{24}^{-2}) + a_3(\zeta_{24}^3 + \zeta_{24}^{-3}) + a_4(\zeta_{24}^4 + \zeta_{24}^{-4}) \in \mathcal{O}_{\mathbb{K}} : 4a_1 + 3a_2 + 2a_3 + a_4 \equiv 0 \pmod{6}\},$$

then \mathcal{M} is a submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 4 and index 6. From Theorem 6, the trace form of $\alpha \in \mathcal{M}$ is given by

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 24(a_1^2 + 2a_1a_2 + 3a_1a_3 + 4a_1a_4 + 2a_2^2 + 4a_2a_3 + 6a_2a_4 + 3a_3^2 + 8a_3a_4 + 6a_4^2).$$

Thus, $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\} = 24$, which is attained at $a_0 = 1$ and $a_1 = a_2 = a_3 = 0$. Since the volume of lattice $\sigma(\mathcal{M})$ equals $2^4 \sqrt{|d_{\mathbb{K}}|} [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 2^9 \cdot 3^2$, it follows that

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{2^3 \cdot 3})^4}{2^9 \cdot 3^2} = \frac{1}{8},$$

i.e., the center density of $\sigma(\mathcal{M})$ is the same as that of the lattice Λ_4 .

4.4 The Λ_5 -laminated lattice

Let \mathbb{K} be a number field of degree $p = 5$ and conductor $n = 5^2$. In this case, the Galois group $Gal(\mathbb{K}/\mathbb{Q}) = \langle \sigma \rangle$ is cyclic of order 5, $t = Tr_{\mathbb{Q}(\zeta_{5^2})/\mathbb{K}}(\zeta_{5^2})$, and $d_{\mathbb{K}} = 5^8$. Let \mathcal{M} be the submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 5 and index 10 given by

$$\mathcal{M} = \{a_0 + a_1\sigma(t) + a_2\sigma^2(t) + a_3\sigma^3(t) + a_4\sigma^4(t) \in \mathcal{O}_{\mathbb{K}} : a_0 \equiv 0 \pmod{2}, -a_0 + a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod{5}\}.$$

From Theorem 10, it follows the trace form of \mathbb{K} restricted to \mathcal{M} is given by

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = 50(2x_0^2 + 6x_0x_1 + 6x_0x_2 + 6x_0x_3 + 8x_0x_4 + 6x_1^2 + 11x_1x_2 + 11x_1x_3 + 15x_1x_4 + 6x_2^2 + 11x_2x_3 + 15x_2x_4 + 6x_3^2 + 15x_3x_4 + 10x_4^2),$$

where x_0, \dots, x_4 are any integers. It follows that $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(x^2) : x \in \mathcal{M}\} = 50$ is attained at $a_0 = a_1 = a_2 = 0$ and $a_3 = -a_4 = 1$. Since the volume of lattice $\sigma(\mathcal{M})$ equals $2^5 \sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 2^6 \cdot 5^5$, one has

$$\delta(\sigma(\mathcal{M})) = \frac{(\sqrt{2 \cdot 5^2})^5}{2^6 \cdot 5^5} = \frac{1}{8\sqrt{2}},$$

i.e., the center density of $\sigma(\mathcal{M})$ equals that of lattice Λ_5 .

4.5 The Λ_6 -laminated lattice

If $\mathbb{K} = \mathbb{Q}(\zeta_{36} + \zeta_{36}^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 6$, $\{\zeta_{36} + \zeta_{36}^{-1}, \zeta_{36}^2 + \zeta_{36}^{-2}, \zeta_{36}^3 + \zeta_{36}^{-3}, \zeta_{36}^4 + \zeta_{36}^{-4}, \zeta_{36}^5 + \zeta_{36}^{-5}, \zeta_{36}^6 + \zeta_{36}^{-6}\}$ is a basis of \mathbb{K} and $d_{\mathbb{K}} = 2^6 \cdot 3^9$. If $\mathcal{M} = (2 + (\zeta_{36} + \zeta_{36}^{-1}) - (\zeta_{36} + \zeta_{36}^{-4}) - (\zeta_{36}^5 + \zeta_{36}^{-5}))\mathcal{O}_{\mathbb{K}}$. In this case, \mathcal{M} is a submodule of $\mathcal{O}_{\mathbb{K}}$ of rank 6 and index 72. From Theorem 6, the trace form of $\alpha \in \mathcal{M}$ is given by

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) = 72(a_0^2 + 2a_0a_1 - 2a_0a_3 - 2a_0a_4 - a_0a_5 + 2a_1^2 - 2a_1a_3 - 3a_1a_4 + a_2^2 + a_2a_3 + 2a_2a_4 + a_2a_5 + 3a_3^2 + 5a_3a_4 + 2a_3a_5 + 3a_4^2 + 2a_4a_5 + a_5^2).$$

Thus, $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha^2) : \alpha \in \mathcal{M}, \alpha \neq 0\} = 72$ which is attained at $a_0 = 1$ and $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Since volume of the lattice $\sigma(\mathcal{M})$ equals $2^6 \sqrt{|d_{\mathbb{K}}|} \cdot [\mathcal{M} : \mathcal{O}_{\mathbb{K}}] = 2^{12} \cdot 3^6 \sqrt{3}$, it follows that

$$\delta(M) = \frac{(\sqrt{2^3 \cdot 3^2})^6}{2^{12} \cdot 3^6 \sqrt{3}} = \frac{1}{8\sqrt{3}},$$

i.e., the center density of $\sigma(\mathcal{M})$ is the same of the lattice Λ_6 .

5 CONCLUSION

A construction of algebraic lattices with special features, namely, high center density and full diversity, was presented. Each lattice was obtained as the image of the canonical homomorphism from a suitably chosen \mathbb{Z} -submodule of the ring of integers of the maximal real subfield of a cyclotomic field into \mathbb{R}^n (n -dimensional Euclidean space). The trace form of the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$ was derived explicitly so that the minimum of the associated lattice could be determined. As a result, rotated versions of full diversity of laminated lattices in dimensions 2 to 6 have been obtained. Although the constructed lattices are well known, this work helps answer the question of which lattices can be realized by a given number field, as posed in [5]. Whether the presented technique can be used to yield higher dimensional lattices with the desired features (full diversity and high packing density) is left as a research problem. Calculating or providing a good lower bound for the minimum product distance [6] of the lattices obtained by the construction technique of this work is also left as a research problem.

ACKNOWLEDGMENT

The authors thank the reviewer for carefully reading the manuscript and for all the suggestions that improved the presentation of this work. The authors also thank FAPESP 2013/25977-7 and CNPq 429346/2018-2 for its financial support.

RESUMO. Uma construção de reticulados usando \mathbb{Z} - submódulos de anéis de inteiros de corpos de números é apresentada. A construção produz versões rotacionadas dos reticulados laminados Λ_n para $n = 2, 3, 4, 5, 6$, que são os reticulados mais densos nessas dimensões. A densidade de empacotamento esférico de um reticulado é uma função do seu raio de empacotamento, o qual por sua vez pode ser diretamente calculado a partir da norma quadrada mínima do reticulado. Normas em um reticulado realizado por um corpo de números totalmente real podem ser calculadas pela forma traço do corpo restrita ao seu anel de inteiros. Portanto, no presente trabalho, apresentamos também a forma traço do subcorpo real maximal de um corpo ciclotômico. Nosso foco é em corpos de números totalmente reais pois os reticulados associados a eles possuem diversidade máxima. Juntamente com a densidade de empacotamento, a característica de diversidade máxima é desejável em reticulados que são usados para transmissão de sinais que percorrem os canais gaussiano e de desvanecimento Rayleigh.

Palavras-chave: empacotamento de esferas, reticulados algébricos, corpos de números, corpos ciclotômicos.

REFERENCES

- [1] A. A. Andrade & R. Palazzo Jr. Linear codes over finite rings, *TEMA – Trends in Applied and Computational Mathematics*, **6**(2) (2005), 207–217.
- [2] A. S. Ansari, R. Shah, Zia Ur-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] R. R. de Araujo, A. C. M. M. Chagas, A. A. Andrade & T. P. Nóbrega Neto. Trace form associated to cyclic number fields of ramified odd prime degree, accepted by *J. Algebra App.*, June, 2019.
- [4] V. Baustista-Ancora & J. Uc-Kuk. The discriminant of abelian number fields, *Journal of Mathematics*, **47**(1) (2017), 39–52.
- [5] E. Bayer-Fluckiger. Lattices and number fields, In: *Contemp. Math.*, Amer. Math. Soc., Providence (1999), 69–84.
- [6] E. Bayer-Fluckiger, F. Oggier & E. Viterbo. New algebraic constructions of rotated \mathbb{Z}^n -lattice constellations for the Rayleigh fading channel. *IEEE Trans. Inform. Theory*, **50**(4) (2004) 702–714.
- [7] E. Bayer-Fluckiger & G. Nebe. On the Euclidian minimum of some real number fields. *Journal de Théorie des Nombres de Bordeaux*, **17**(2) (2005), 437–454.
- [8] E. Bayer-Fluckiger & I. S. Atias. Ideal lattices over totally real number fields and Euclidian minima, *Archiv der Mathematik*, **86**(3) (2006), 217–225.

- [9] P. E. Conner & R. Perlis. “A Survey of Trace Forms of Algebraic Number Fields”, World Scientific Publishing Co Pte Ltd., Singapore (1984).
- [10] J. H. Conway & N. J. A. Sloane. “Sphere Packings, Lattices and Groups”, 3rd Edition, Springer Verlag, New York (1999).
- [11] J. C. Interlando, T. P. Nóbrega Neto, T. M. Rodrigues & J. O. D. Lopes. A note on the integral trace form in cyclotomic fields, *J. Algebra App.*, **14** (2015), 1550045.
- [12] G. Lettl. The ring of integers of an Abelian number field, *J. Reine Angew. Math.*, **404** (1990), 162–170.
- [13] E. L. Oliveira, J. C. Interlando, T. P. da Nóbrega Neto & J. O. D. Lopes. The integral trace form of cyclic extensions of odd prime degree, *Rocky Mountain J. Math.*, **47** (2017), 1075–1088.
- [14] L. Washington. “Introduction to cyclotomic fields”, Springer-Verlag, New York (1995).