J. Algebra Comb. Discrete Appl.
11(2) • 73–81

Received: 31 May 2021
Accepted: 27 February 2023

Journal of Algebra Combinatorics Discrete Structures and Applications

Characterization of totally real subfields of 2-power cyclotomic fields and applications to signal set design*

Research Article

Agnaldo J. Ferrari, **Antonio A. de Andrade**, **José C. Interlando**, **Carina Alves**

Abstract: A classification of all totally real subfields $\mathbb{K}$ of cyclotomic fields $\mathbb{Q}(\xi_{2^r})$, for any $r \geq 4$, and the fully-diverse related versions of the $\mathbb{Z}^n$-lattice are presented along with closed-form expressions for their minimum product distance. Any totally real subfield $\mathbb{K}$ of $\mathbb{Q}(\xi_{2^r})$ must be of the form $\mathbb{K} = \mathbb{Q}(\xi_{2^s} + \xi_{2^s}^{-1})$, where $s = r - j$ for some $0 \leq j \leq r-3$. Signal constellations for transmitting information over both Gaussian and Rayleigh fading channels (which can be useful for mobile communications) can be carved out of those lattices.

2020 MSC: 52C07, 11H31, 11H71

Keywords: Cyclotomic fields, Algebraic lattices, Signal design, Minimum product distance

1. Introduction

In this work a lattice means a discrete subgroup of Euclidean n-space. A simple, yet important example, is the n-dimensional integer lattice $\mathbb{Z}^n$, which consists of all points whose coordinates are n-tuples of integers [10]. Lattices constructed from algebraic number fields are called *algebraic lattices*. One advantage of the latter is that important parameters such as sphere packing density and minimum product distance, which are typically costly to calculate for general lattices, can be readily determined.

* *This work was supported by CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) under Grant No. 429346/2018-2. and Fapesp - 2013/25977-7.*

Agnaldo J. Ferrari (Corresponding Author); Department of Mathematics, São Paulo State University, Bauru, SP 17033-360, Brazil (email: agnaldo.ferrari@unesp.br).

Antonio A. de Andrade; Department of Mathematics, São Paulo State University, São José do Rio Preto, SP 15054-000, Brazil (email: antonio.andrade@unesp.br).

José C. Interlando; Department of Mathematics & Statistics, San Diego State University, San Diego, CA 92182, USA (email: interlan@sdsu.edu).

Carina Alves; Department of Mathematics, São Paulo State University, Rio Claro, SP 13506-900, Brazil (email: carina.alves@unesp.br).

https://doi.org/10.13069/jacodesmath.v11i2.207

ISSN 2148-838X

Lattices have been considered in different areas, especially in coding theory, more recently in cryptography [23] and from different points of view [14, 27].

Constructions of algebraic lattices have been proposed in several papers [1–9, 12, 13, 15, 16, 18–21, 24, 25, 28]. Lattices constructed from totally real algebraic number fields possess maximum diversity, a feature that makes them attractive for use over Rayleigh fading channels. Signal constellations based on $\mathbb{Z}^n$-lattices offer a good trade-off between bit labelling and constellation shaping since they are only slightly worse in terms of shaping gain but are usually easier to label [24]. Therefore, all of the above motivates the investigation of $\mathbb{Z}^n$-lattices constructed from totally real number fields. In [1, 2], rotated $\mathbb{Z}^n$-lattices were constructed from the totally real fields $\mathbb{Q}(\xi_{2^r}^{2^k} + \xi_{2^r}^{-2^k})$, with $k = 0, 1$, and their minimum product distances were computed, where ξ_{2^r} is primitive 2^r-th root of unity. Having the construction procedure of rotated $\mathbb{Z}^n$-lattices from totally real subfields of cyclotomic fields as the main motivation, in this paper we extend the constructions of [1, 2] for the totally real fields $\mathbb{Q}(\xi_{2^r}^{k} + \xi_{2^r}^{-k})$, where $k \in \mathbb{Z}$.

We conclude that, whatever the $\mathbb{Z}^n$-lattice built on totally real subfields of $\mathbb{Q}(\xi_{2^r})$, the normalized minimum product distance present in Table 1 is the best one in each dimension, since $\mathbb{K} = \mathbb{Q}(\xi_{2^s} + \xi_{2^s}^{-1})$, for $s = r - j$ $(0 \leq j \leq r - 3)$ is equivalent to $\mathbb{K} = \mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})$ for a specific $r \geq 4$, and this was precisely the case approached in [1, 6].

The paper is organized as follows. Section 2 reviews definitions and results from algebraic number theory and cyclotomic fields that are relevant to the work. A classification of all totally real subfields of the cyclotomic field $\mathbb{Q}(\xi_{2^r})$ is presented. Section 3 reviews ideal lattices, in particular calculation of their minimum product distance. Section 4 contains the main contribution of the paper, namely, a method for constructing rotated $\mathbb{Z}^n$-lattices from *any* totally real subfield $\mathbb{K}$ of $\mathbb{Q}(\xi_{2^r})$; it turns out that, in each possible dimension, the minimum product distance of the obtained lattice is the same as the one previously obtained in [1, 2]. Formulas for the normalized minimum product distances of the obtained lattices are presented as well. Rotation matrices for constructing $\mathbb{Z}^n$-lattices in the same dimensions and with the same normalized minimum product distances were presented in [11], however, no rationale was provided therein for how the matrices were obtained. Finally, in Section 5, the concluding remarks are drawn.

2. Background on algebraic number theory and cyclotomic fields

In this section we review some facts about number fields, and in particular, cyclotomic fields. We recall only the results that are needed for subsequent sections. The reader interested in further details is referred to [26] and [29]. Let $\mathbb{L}$ be a number field of degree n, $\mathcal{O}_{\mathbb{L}}$ its ring of integers, and $\sigma_1, \ldots, \sigma_n$ the monomorphisms of $\mathbb{L}$ into $\mathbb{C}$. The embedding σ_i is called real if $\sigma_i(\mathbb{L})$ is contained in $\mathbb{R}$, and is called complex otherwise. The field $\mathbb{L}$ is said to be totally real if all of its embeddings are real.

Given $x \in \mathcal{O}_{\mathbb{L}}$, the (rational) integers $N(x) = N_{\mathbb{L}/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ and $Tr(x) = Tr_{\mathbb{L}/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ are called *norm* and *trace* of x in $\mathbb{L}/\mathbb{Q}$, respectively. The *norm* of a free $\mathbb{Z}$-module $\mathcal{A}$ of rank n contained in $\mathcal{O}_{\mathbb{L}}$ is defined as $N(\mathcal{A}) = N_{\mathbb{L}}(\mathcal{A}) = |\mathcal{O}_{\mathbb{L}}/\mathcal{I}|$. If $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbb{L}}$, then the (rational) integer $d_{\mathbb{L}} = (\det(\sigma_j(\omega_i))_{i,j=1}^{n})^2$, which is invariant under change of basis, is called the *discriminant* of $\mathbb{L}$. Throughout this work, $\mathbb{Z}_m$ will denote the (cyclic) group of integers modulo m and $\mathbb{Z}_m^*$ the group of invertible integers modulo m with $m \geq 2$ an integer.

Proposition 2.1. *[22, 29] For any integer $r \geq 3$, let $\mathbb{L}$ denote the cyclotomic field $\mathbb{Q}(\xi_{2^r})$ and $\mathbb{L}^+$ its maximal real subfield, namely, $\mathbb{L}^+ = \mathbb{L} \cap \mathbb{R} = \mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})$. One has:*

(i) $[\mathbb{L} : \mathbb{Q}] = 2^{r-1}$ *and* $[\mathbb{L}^+ : \mathbb{Q}] = 2^{r-2}$.

(ii) The ring of algebraic integers of $\mathbb{L}^+$ *is* $\mathbb{Z}[\xi_{2^r} + \xi_{2^r}^{-1}]$.

(iii) $\{1, \xi_{2^r} + \xi_{2^r}^{-1}, \xi_{2^r}^{2} + \xi_{2^r}^{-2}, \cdots, \xi_{2^r}^{2^{r-2}-1} + \xi_{2^r}^{-2^{r-2}+1}\}$ *is an integral basis for* $\mathbb{L}^+$.

(iv) $\mathbb{L}/\mathbb{Q}$ *is a Galois extension whose Galois group* $Gal(\mathbb{L}/\mathbb{Q})$ *is isomorphic to* $\mathbb{Z}_{2^r}^*$.

(v) $\mathbb{L}^+/\mathbb{Q}$ *is a Galois extension whose Galois group* $Gal(\mathbb{L}^+/\mathbb{Q})$ *is cyclic and generated by* σ*, the automorphism defined by* $\sigma(\xi_{2^r} + \xi_{2^r}^{-1}) = \xi_{2^r}^5 + \xi_{2^r}^{-5}$*. Moreover,* $Gal(\mathbb{L}^+/\mathbb{Q})$ *is isomorphic to* $\mathbb{Z}^*_{2^{r-2}}$*.*

(vi) $d_{\mathbb{L}^+} = 2^{(r-1)2^{r-2}-1}$.

Proposition 2.2. *For each* $0 \leq j \leq r-2$*, there exists a unique subfield* $\mathbb{K}$ *of* $\mathbb{L}^+$ *such that* $[\mathbb{K} : \mathbb{Q}] = 2^{r-j-2}$.

Proof. The statement is an immediate consequence of the fact that the extension $\mathbb{L}^+/\mathbb{Q}$ is Galois: The intermediate fields between $\mathbb{L}^+$ and $\mathbb{Q}$ are in one-to-one correspondence with the subgroups of $Gal(\mathbb{L}^+/\mathbb{Q})$, which is cyclic (and hence for every divisor d of the group order, there is exactly one subgroup of order d). □

Proposition 2.3. *If* $\mathbb{K}$ *is a totally real subfield of* $\mathbb{L} = \mathbb{Q}(\xi_{2^r})$*, then* $\mathbb{K} \subseteq \mathbb{L}^+$*.*

Proof. The field $\mathbb{K}$ must be contained in both $\mathbb{L}$ and $\mathbb{R}$. Hence, $\mathbb{K}$ must be contained in $\mathbb{L}^+$. □

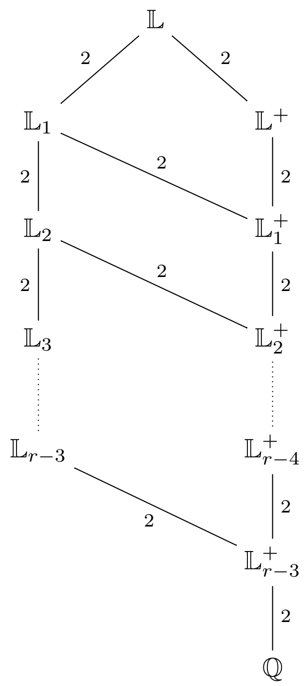
Proposition 2.4. *Let* $\mathbb{L} = \mathbb{Q}(\xi_{2^r})$*,* $\theta_j = \xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1}$*,* $\mathbb{L}_j = \mathbb{Q}(\xi_{2^{r-j}})$ *and* $\mathbb{L}_j^+ = \mathbb{Q}(\theta_j)$*, where* $j = 0, 1, \ldots, r-3$*. Then:*

(i) $[\mathbb{L}_j : \mathbb{L}_j^+] = 2$ *and* $\mathbb{L}_{j+1} \subset \mathbb{L}_j$*.*

(ii) $[\mathbb{L}_j^+ : \mathbb{Q}] = 2^{r-j-2}$.

(iii) $\mathbb{L}_{j+1}^+ \subset \mathbb{L}_j^+$ *and* $[\mathbb{L}_j^+ : \mathbb{L}_{j+1}^+] = 2$.

(iv) $[\mathbb{L}_j : \mathbb{L}_{j+1}] = 2$.



Proof.

(i) Obviously $[\mathbb{L}_j : \mathbb{L}_j^+] = 2$ since $\mathbb{L}_j^+$ is the maximal real subfield of $\mathbb{L}_j$. Notice that $\mathbb{L}_0 = \mathbb{L}$ and $\mathbb{L}_0^+ = \mathbb{L}^+ = \mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})$. Since $\xi_{2^{r-j-1}} = \xi_{2^{r-j}}^2 \in \mathbb{Q}(\xi_{2^{r-j}})$, one has $\mathbb{L}_{j+1} = \mathbb{Q}(\xi_{2^{r-j-1}}) \subset \mathbb{Q}(\xi_{2^{r-j}}) = \mathbb{L}_j$.

(ii) $[\mathbb{L}_j^+ : \mathbb{Q}] = \frac{\varphi(2^{r-j})}{2} = 2^{r-j-2}$ as $\mathbb{L}_j^+ = \mathbb{Q}(\xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1})$.

(iii) Since $\mathbb{L}_j^+ = \mathbb{L}_j \cap \mathbb{R}$ and $\mathbb{L}_{j+1} \subset \mathbb{L}_j$ (see (i)), it follows that

$$\mathbb{L}_j^+ \cap \mathbb{L}_{j+1} = (\mathbb{L}_j \cap \mathbb{R}) \cap \mathbb{L}_{j+1} = (\mathbb{L}_j \cap \mathbb{L}_{j+1}) \cap \mathbb{R} = \mathbb{L}_{j+1} \cap \mathbb{R} = \mathbb{L}_{j+1}^+,$$

and therefore, $\mathbb{L}_{j+1}^+ \subset \mathbb{L}_j^+$. The second assertion follows from $[\mathbb{L}_{j+1}^+ : \mathbb{Q}] = 2^{r-j-3}$ (see (ii)) and $[\mathbb{L}_j^+ : \mathbb{Q}] = [\mathbb{L}_j^+ : \mathbb{L}_{j+1}^+] \cdot [\mathbb{L}_{j+1}^+ : \mathbb{Q}]$.

(iv) From (i), (iii), and the fact that $[\mathbb{L}_j : \mathbb{L}_j^+] \cdot [\mathbb{L}_j^+ : \mathbb{L}_{j+1}^+] = [\mathbb{L}_j : \mathbb{L}_{j+1}] \cdot [\mathbb{L}_{j+1} : \mathbb{L}_{j+1}^+]$, it follows that $[\mathbb{L}_j : \mathbb{L}_j^+] = [\mathbb{L}_{j+1} : \mathbb{L}_{j+1}^+] = 2$ and $[\mathbb{L}_j^+ : \mathbb{L}_{j+1}^+] = 2$, respectively. Therefore, $[\mathbb{L}_j : \mathbb{L}_{j+1}] = 2$.

□

Proposition 2.5. *With notation as in Proposition 2.4, if $\mathbb{K}$ is a totally real subfield of $\mathbb{L} = \mathbb{Q}(\xi_{2^r})$, then there is $0 \leq j \leq r-3$ such that $\mathbb{K} = \mathbb{L}_j^+$.*

Proof. If $\mathbb{K}$ is a subfield of $\mathbb{L}$ and $[\mathbb{K} : \mathbb{Q}] = t$, then $t = 2^m$ for some $1 \leq m \leq r-2$ since t divides $[\mathbb{L} : \mathbb{Q}] = 2^{r-1}$. Setting $j = r-m-2$, it follows that $0 \leq j \leq r-3$ and $\mathbb{L}_j^+ = \mathbb{Q}(\xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1})$ is such that $[\mathbb{L}_j^+ : \mathbb{Q}] = 2^{r-j-2} = 2^m$. As $\mathbb{K}$ is a totally real number field, $\mathbb{K} \subseteq \mathbb{L}_j^+$ by Proposition 2.3. In summary, we have $\mathbb{K}$, $\mathbb{L}_j^+ \subseteq \mathbb{L}^+$ with $[\mathbb{K} : \mathbb{Q}] = [\mathbb{L}_j^+ : \mathbb{Q}] = 2^{r-j-2} = 2^m$. Since by Proposition 2.2 there exists a unique subfield $\mathbb{K}$ of $\mathbb{L}^+$ such that $[\mathbb{K} : \mathbb{Q}] = 2^{r-j-2}$, one has $\mathbb{K} = \mathbb{L}_j^+$. □

3. Ideal lattices and minimum product distance

Let $m \leq n$ be positive integers and Λ a lattice with basis $\{v_1, \ldots, v_m\}$. Let the coordinates of the basis vectors be $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{R}^n$ for $i = 1, \ldots, m$. The matrices $M = (v_{ij})$ and $G = MM^t$ are called *generator* and *Gram matrices* for Λ, respectively, where t denotes transpose. The *determinant* of Λ, denoted by $\det(\Lambda)$, is defined as $\det(G)$ and it is invariant under change of basis. The quantity $\sqrt{\det(\Lambda)}$ is called the *volume* of Λ.

Let $\mathbb{K}$ be a totally real number field of degree n with monomorphisms $\sigma_1, \cdots, \sigma_n$, and $\alpha \in \mathbb{K}$ a totally positive element, that is, $\alpha_i = \sigma_i(\alpha) > 0$ for all $i = 1, \cdots, n$. The mapping $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ given by

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

is called a *twisted homomorphism* [6]. When $\alpha = 1$, the mapping becomes the *canonical embedding* of $\mathbb{K}$ into $\mathbb{R}^n$ [26, Ch. IV, Section 2]. If $\mathcal{A}$ is a $\mathbb{Z}$-module in $\mathbb{K}$ of rank n with $\mathbb{Z}$-basis $\{w_1, w_2, \cdots, w_n\}$, then $\Lambda = \sigma_\alpha(\mathcal{A})$ is a full-rank lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(w_1), \sigma_\alpha(w_2), \cdots, \sigma_\alpha(w_n)\}$. A generator and a Gram matrix for Λ are given by

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

and

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

respectively. The *minimum product distance* of Λ is given by

$$d_{p,min}(\Lambda) = \sqrt{N_{\mathbb{K}/\mathbb{Q}}(\alpha)} \min_{0\neq y\in\mathcal{A}} |N_{\mathbb{K}/\mathbb{Q}}(y)|. \tag{2}$$

In particular, if $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ is a principal ideal, then

$$d_{p,\min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{|d_{\mathbb{K}}|}}, \tag{3}$$

see [6]. The *normalized minimum product distance* of Λ, denoted by $d_{p,\text{norm}}(\Lambda)$, is the minimum product distance with normalized determinant $\det(\Lambda) = 1$, i.e.,

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

In particular, if $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ is a principal ideal then

$$d_{p,\text{norm}}(\Lambda) = \frac{1}{\sqrt{|d_{\mathbb{K}}|}}. \tag{4}$$

Theorem 3.1. *[6] Notation as above, if $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{L}}$ is a fractional ideal, then*

$$\det(\Lambda) = N(\mathcal{A})^2 N(\alpha)|d_{\mathbb{K}}|.$$

4. Construction of rotated $\mathbb{Z}^n$-lattices from $\mathbb{L}_j^+$

Henceforth, $\mathbb{L}_j$, for $0 \leq j \leq r-3$, will denote the number field defined in Section 2, Proposition 2.4. Let $\alpha \in \mathcal{O}_{\mathbb{L}_j^+}$ a totally positive element and $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{L}_j^+}$ a fractional ideal. If $\Lambda = \sigma_\alpha(\mathcal{A})$ is a rotated $\mathbb{Z}^n$-lattice scaled by $\sqrt{c}$, then $\det(\Lambda) = c^n$. In Theorem 3.1, consider $\mathbb{K} = \mathbb{L}_j^+$, $\mathcal{A} = \mathcal{O}_{\mathbb{L}_j^+}$ and $c = 2^{r-j-1}$. In this case, $n = 2^{r-j-2}$. By Proposition 2.1(v), $d_{\mathbb{L}_j^+} = 2^{(r-j-1)2^{r-j-2}-1}$. Thus, if $\sigma_\alpha(\mathcal{A})$ is a rotated $\mathbb{Z}^n$-lattice, then there is $\alpha \in \mathcal{O}_{\mathbb{L}_j^+}$ such that $N(\alpha) = 2$. Such an element α is provided by the next proposition.

Proposition 4.1. *Let $\theta_j = \xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1}$ be an element of $\mathcal{O}_{\mathbb{L}_j^+}$. Then $\alpha = 2 - \theta_j$ is totally positive and $N(\alpha) = 2$.*

Proof. Clearly $\alpha = 2 - \theta_j$ is totally positive since for $k = 1, 2, \ldots, 2^{r-j-2}$,

$$\sigma_k(\alpha) = \sigma_k(2-\theta_j) = 2 - \sigma_k(\theta_j) = 2 - 2\cos\left(\frac{2\pi k}{2^{r-j}}\right) > 0.$$

Set $\xi = \xi_{2^{r-j}}$, $N = N_{\mathbb{L}_j^+/\mathbb{Q}}$, $\tilde{N} = N_{\mathbb{L}_j/\mathbb{Q}}$ and $\overline{N} = N_{\mathbb{L}_j/\mathbb{L}_j^+}$. Then $2\mathbb{Z}[\xi] = (1-\xi)^{\varphi(2^{r-j})}\mathbb{Z}[\xi]$ in $\mathbb{Q}[\xi]$, where φ is the Euler function. So, $\tilde{N}(1-\xi) = 2$. Using the transitivity of the norm, we obtain

$$2 = \tilde{N}(1-\xi) = N(\overline{N}(1-\xi)) = N((1-\xi)(1-\xi^{-1})) = N(2-\theta_j) = N(\alpha),$$

which proves the result. □

The condition $N(\alpha) = 2$ for some α totally positive is not sufficient to guarantee the existence of a rotated scaled version $\sigma_\alpha(\mathcal{A})$ of $\mathbb{Z}^n$-lattice. However, we show that such a version is obtained if α is as in Proposition 4.1.

Proposition 4.2. *[17] If $\mathbb{L}_j = \mathbb{Q}(\xi_{2^{r-j}})$, then*

$$Tr_{\mathbb{L}_j/\mathbb{Q}}(\xi^k_{2^{r-j}}) = \begin{cases} 0 & \textit{if } \gcd(k, 2^{r-j}) < 2^{r-j-1}; \\ -2^{r-j-1} & \textit{if } \gcd(k, 2^{r-j}) = 2^{r-j-1}; \\ 2^{r-j-1} & \textit{if } \gcd(k, 2^{r-j}) > 2^{r-j-1}. \end{cases}$$

Corollary 4.3. *If $\mathbb{L}_j^+ = \mathbb{Q}(\xi_{2^{r-j}} + \xi^{-1}_{2^{r-j}})$, then*

$$Tr_{\mathbb{L}_j^+/\mathbb{Q}}(\xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}}) = \begin{cases} 0 & \textit{if } \gcd(k, 2^{r-j}) < 2^{r-j-1}; \\ -2^{r-j-1} & \textit{if } \gcd(k, 2^{r-j}) = 2^{r-j-1}; \\ 2^{r-j-1} & \textit{if } \gcd(k, 2^{r-j}) > 2^{r-j-1}. \end{cases}$$

Proof. From the transitivity of the trace, it follows that

$$\begin{aligned} Tr_{\mathbb{L}_j/\mathbb{Q}}(\xi^k_{2^{r-j}}) + Tr_{\mathbb{L}_j/\mathbb{Q}}(\xi^{-k}_{2^{r-j}}) &= Tr_{\mathbb{L}_j/\mathbb{Q}}(\xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}}) \\ &= Tr_{\mathbb{L}_j^+/\mathbb{Q}}(Tr_{\mathbb{L}_j/\mathbb{L}_j^+}(\xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}})) \\ &= 2Tr_{\mathbb{L}_j^+/\mathbb{Q}}(\xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}}). \end{aligned}$$

The result now follows from Proposition 4.2. □

Proposition 4.4. *Notation as in Proposition 4.1, let $e_0 = 1$ and $e_k = \xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}}$ for $k = 1, 2, \ldots, 2^{r-j-2} - 1$.*

(i) $Tr_{\mathbb{L}_j^+/\mathbb{Q}}(\alpha e_k e_k) = \begin{cases} 2^{r-j-1} & \textit{if } k = 0; \\ 2^{r-j} & \textit{otherwise.} \end{cases}$

(ii) If $k > 0$, then $Tr_{\mathbb{L}_j^+/\mathbb{Q}}(\alpha e_k e_0) = \begin{cases} -2^{r-j-1} & \textit{if } k = 1; \\ 0 & \textit{otherwise.} \end{cases}$

(iii) If $0 < i < k$, then $Tr_{\mathbb{L}_j^+/\mathbb{Q}}(\alpha e_i e_k) = \begin{cases} -2^{r-j-1} & \textit{if } |i-k| = 1. \\ 0 & \textit{otherwise.} \end{cases}$

Proof. To simplify the notation, denote $Tr_{\mathbb{L}_j^+/\mathbb{Q}}$ by Tr.

(i) By Corollary 4.3, $Tr(\theta_j) = 0$. One has $Tr(\alpha e_0 e_0) = Tr(\alpha) = Tr(2) = Tr(2) = 2^{r-j-1}$.

(ii) Since $\gcd(k, 2^{r-j}) < 2^{r-j-1}$, for all $k = 1, 2, \ldots, 2^{r-j-2}$, it follows that

$$\begin{aligned} Tr(\alpha e_k e_0) &= Tr(\alpha e_k) = Tr((2 - (\xi_{2^{r-j}} + \xi^{-1}_{2^{r-j}}))(\xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}})) \\ &= 2Tr(\xi^k_{2^{r-j}} + \xi^{-k}_{2^{r-j}}) - Tr(\xi^{k+1}_{2^{r-j}} + \xi^{-(k+1)}_{2^{r-j}}) - Tr(\xi^{k-1}_{2^{r-j}} + \xi^{-(k-1)}_{2^{r-j}}) \\ &= Tr(\xi^{k-1}_{2^{r-j}} + \xi^{-(k-1)}_{2^{r-j}}) = \begin{cases} -2^{r-j-1}, & \text{if } k = 1. \\ 0, & \text{if } k \neq 1. \end{cases} \end{aligned}$$

Now, since $\gcd(2k, 2^{r-j}), \gcd(2k \pm 1, 2^{r-j}) < 2^{r-j-1}$ for $k = 1, 2, \ldots, 2^{r-j-2} - 1$, it follows that

$$\begin{aligned} Tr(\alpha e_k e_k) &= Tr(\alpha e_k^2) = Tr((2 - (\xi_{2^{r-j}} + \xi^{-1}_{2^{r-j}}))(\xi^{2k}_{2^{r-j}} + \xi^{-2k}_{2^{r-j}} + 2)) \\ &= 2Tr(\xi^{2k}_{2^{r-j}} + \xi^{-2k}_{2^{r-j}}) + Tr(4) - Tr(\xi^{2k+1}_{2^{r-j}} + \xi^{-(2k+1)}_{2^{r-j}}) \\ &\quad -Tr(\xi^{2k-1}_{2^{r-j}} + \xi^{-(2k-1)}_{2^{r-j}}) - 2Tr(\xi_{2^{r-j}} + \xi^{-1}_{2^{r-j}}) = 2^{r-j}. \end{aligned}$$

(iii) Under the hypotheses, $\gcd(i \pm k, 2^{r-j}), \gcd(i \pm k \pm 1, 2^{r-j}) < 2^{r-j-1}$. Then

$$\begin{aligned} Tr(\alpha e_i e_k) &= Tr((2-(\xi_{2^{r-j}}+\xi_{2^{r-j}}^{-1}))(\xi_{2^{r-j}}^{i}+\xi_{2^{r-j}}^{-i})(\xi_{2^{r-j}}^{k}+\xi_{2^{r-j}}^{-k}) \\ &= 2Tr(\xi_{2^{r-j}}^{i+k}+\xi_{2^{r-j}}^{-(i+k)})+2Tr(\xi_{2^{r-j}}^{i-k}+\xi_{2^{r-j}}^{-(i-k)}) \\ &\quad -Tr(\xi_{2^{r-j}}^{i+k+1}+\xi_{2^{r-j}}^{-(i+k+1)})-Tr(\xi_{2^{r-j}}^{i-k+1}+\xi_{2^{r-j}}^{-(i-k+1)}) \\ &\quad -Tr(\xi_{2^{r-j}}^{-i+k+1}+\xi_{2^{r-j}}^{-(-i+k+1)})-Tr(\xi_{2^{r-j}}^{i+k-1}+\xi_{2^{r-j}}^{-(i+k-1)}) \\ &= \begin{cases} -2^{r-j-1} & \text{if } |i-k|=1. \\ 0 & \text{otherwise,} \end{cases} \end{aligned}$$

as desired.

□

Proposition 4.5. *Notation as in Propositions 4.1 and 4.4, if $\mathcal{A} = \mathcal{O}_{\mathbb{L}_j^+}$, then $\frac{1}{\sqrt{2^{r-j-1}}}\sigma_\alpha(\mathcal{A})$ is a rotated $\mathbb{Z}^n$-lattice.*

Proof. From (1), it follows that the Gram matrix for $\frac{1}{\sqrt{2^{r-j-1}}}\sigma_\alpha(\mathcal{A})$ is given by $G_1 = \frac{1}{2^{r-j-1}}\left(Tr_{\mathbb{L}_j^+/\mathbb{Q}}(\alpha e_i e_k)\right)_{i,k=0}^{n-1}$ and by Proposition 4.4, one has

$$G_1 = \begin{pmatrix} 1 & -1 & 0 & \cdots & & & & & \\ -1 & 2 & -1 & 0 & \cdots & & & & \\ 0 & -1 & 2 & -1 & 0 & \cdots & & & \\ \cdots & 0 & -1 & 2 & -1 & 0 & \cdots & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ & & \cdots & 0 & -1 & 2 & -1 & 0 \\ & & & \cdots & 0 & -1 & 2 & -1 \\ & & & & \cdots & 0 & -1 & 2 \end{pmatrix}.$$

Let T the change of basis matrix

$$T = \begin{pmatrix} -1 & -1 & \dots & -1 & -1 & -1 \\ -1 & -1 & \dots & -1 & -1 & 0 \\ -1 & -1 & \dots & -1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ -1 & -1 & \dots & 0 & 0 & 0 \\ -1 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

Since $G = TG_1T^t = I_n$, it follows that $\frac{1}{\sqrt{2^{r-j-1}}}\sigma_\alpha(\mathcal{A})$ is a rotated $\mathbb{Z}^n$-lattice. □

Proposition 4.6. *For $r \geq 4$, let $\mathbb{K}$ be a totally real subfield of $\mathbb{Q}(\xi_{2^r})$ such that $[\mathbb{K} : \mathbb{Q}] = n$. If α is a totally positive element of $\mathcal{O}_\mathbb{K}$, then $\Lambda_n = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ is a rotated $\mathbb{Z}^n$-lattice such that*

$$d_{p,\text{norm}}(\Lambda_n) = 2^{\frac{1-(r-j-1)2^{r-j-2}}{2}}$$

and $r - j = 2 + \log_2 n$ for some $0 \leq j \leq r-3$.

Proof. If $\mathbb{K}$ is a totally real subfield of $\mathbb{Q}(\xi_{2^r})$, then by Proposition 2.2, there is $0 \leq j \leq r-3$ such that $\mathbb{K} = \mathbb{L}_j^+$ and $n = [\mathbb{K} : \mathbb{Q}] = 2^{r-j-2}$, or equivalently, with $r - j = 2 + \log_2 n$. As $\mathcal{O}_\mathbb{K}$ is a principal ideal, then from Equation (4) and Proposition 2.1 (vi),

$$d_{p,\text{norm}}(\Lambda_n) = \frac{1}{\sqrt{|d_{\mathbb{L}_j^+}|}} = \frac{1}{\sqrt{2^{(r-j-1)2^{r-j-2}-1}}} = 2^{\frac{1-(r-j-1)2^{r-j-2}}{2}},$$

which proves the result. □

5. Conclusions

This work provided a classification of all totally real subfields $\mathbb{K}$ of cyclotomic fields $\mathbb{Q}(\xi_{2^r})$ for any $r \geq 4$. It was proved that any totally real subfield $\mathbb{K}$ of $\mathbb{Q}(\xi_{2^r})$ must be of the form $\mathbb{K} = \mathbb{Q}(\xi_{2^s} + \xi_{2^s}^{-1})$, where $s = r - j$ for some $0 \leq j \leq r - 3$. As an application, for $n = 2^{r-j-2}$, the normalized minimum product distance of $\Lambda_n = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ was determined (Proposition 4.6). The obtained results are displayed in Table 1. The parameter $\sqrt[n]{d_{p,\text{norm}}(\Lambda_n)}$ was used to compare the normalized minimum product distances in different dimensions.

We conclude that when a rotated version of the $\mathbb{Z}^n$-lattice is built from a totally real subfield of $\mathbb{Q}(\xi_{2^r})$, the normalized minimum product distance presented in Table 1 is the best one in each dimension. This follows from the observation that $\mathbb{Q}(\xi_{2^s} + \xi_{2^s}^{-1})$ for $s = r - j$ $(0 \leq j \leq r - 3)$ is equal to $\mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})$ for a specific $r \geq 4$, and this was precisely the case approached in [1, 6].

Table 1. Normalized minimum product distance of rotated $\mathbb{Z}^n$-lattice over $\mathbb{K}$, a totally real subfield of the cyclotomic field $\mathbb{Q}(\xi_{2^r})$.

$r-j$	n	$\sqrt[n]{d_{p,norm}(\Lambda_n)}$
3	2	0.59460
4	4	0.38555
5	8	0.26106
6	16	0.18064
7	32	0.12636
8	64	0.08886
9	128	0.06266
10	256	0.04425
11	512	0.03127
12	1024	0.02210

References

[1] A. A. Andrade, C. Alves, T. B. Carlos, Rotated lattices via the cyclotomic field $\mathbb{Q}(\xi_{2^r})$, Int. J. Appl. Math. 19(3) (2006) 321–331.

[2] A. A. Andrade, J. C. Interlando, Rotated $\mathbb{Z}^n$-lattices via real subfields of $\mathbb{Q}(\xi_{2^r})$, Trends in Appl. Math. and Comp. 20(3) (2019) 445–456.

[3] R. R. Araújo, S. I. R. Costa, Well-rounded algebraic lattices in odd prime dimension, Archiv der Mathematik. 112 (2019) 139–148.

[4] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. 24 (1999) 69–84.

[5] E. Bayer-Fluckiger, Ideal lattices, Proceedings of the Conference Number Theory and Diophantine Geometry. (2002) 168–184.

[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, I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, Archiv der Mathematik. 86(3) (2006) 217–225.

[8] C. W. O. Benedito, C. Alves, N. G. Brasil Jr, S. I. R. Costa, Algebraic construction of lattices via maximal quaternion orders, J. of Pure and Appl. Algebra. 224(5) (2020) 106221.

[9] J. Boutros, E. Viterbo, C. Rastello, J. C. Belfiore, Good lattice constellations for both Rayleigh fading and Gaussian channels, IEEE Trans. Inform. Theory. 42(2) (1996) 502–518.

[10] J. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups, 2^{nd} edition, Springer-Verlag, New York (1993).

[11] M. O. Damen, K. Abed-Meraim, J. C. Belfiore, Diagonal algebraic space-time block codes, IEEE Trans. Inform. Theory. 48(3) (2002) 628–636.

[12] A. J. Ferrari, A. A. Andrade, Constructions of rotated lattice constellations in dimensions power of 3, J. Algebra and its Appl. 17(09) (2018) 1850175.

[13] A. J. Ferrari, A. A. Andrade, Algebraic lattices via polynomial rings, Computational & Applied Mathematics. 38 (2019) 163.

[14] A. J. Ferrari, A. A. Andrade, R. R. Araujo, J. C. Interlando, Trace forms of certain subfields of cyclotomic fields and applications, J. Algebra Comb. Discrete Struct. Appl. 7(2) (2020) 141–160.

[15] A. J. Ferrari, G. C. Jorge, A. A. Andrade, Rotated D_n-lattices in dimensions power of 3, J. Algebra Comb. Discrete Struct. Appl. 8(3) (2021) 151–160.

[16] A. J. Ferrari, T. M. R. Souza, Rotated A_n-lattice codes of full diversity, Adv. Math. Commun. 16(3) (2022) 439-âĂŞ447.

[17] A. L. Flores, Lattices in Abelian fields, PhD Dissertation, The State University of Campinas, Campinas, Brazil (2000).

[18] O. W. Gnilke, H. T. N. Tran, A. Karrila, C. Hollanti, Well-rounded lattices for reliability and security in Rayleigh fading SISO channels, IEEE Information Theory Workshop (ITW). (2016) 359–363.

[19] J. C. Interlando, A. A. Andrade, B. G. Malaxechebarria, A. J. Ferrari, R. R. AraÃžjo, Fully-diverse lattices from ramified cyclic extensions of prime degree, Int. J. Appl. Math. 33(6) (2020) 1009–1015.

[20] G. C. Jorge, A. A. Andrade, S. I. R. Costa, J. E. Strapasson, Algebraic constructions of densest lattices, J. Algebra. 429 (2015) 218–235.

[21] G. C. Jorge, A. J. Ferrari, S. I. R. Costa, Rotated D_n-lattices, Journal of Number Theory (JNT). 132(11) (2012) 2397–2406.

[22] J. O. D. Lopes, The discriminant of subfields of $\mathbb{Q}(\xi_{2^r})$, J. Algebra and its Appl. 2(4) (2003) 463–469.

[23] D. Micciancio, S. Goldwasser, Complexity of lattice problems: a cryptographic perspective, Springer, New York (2002).

[24] F. Oggier, Algebraic methods for channel coding, PhD Dissertation, Universitede Geneve e nationalite suisse et originaire de Salquenen, Lausanne EPFL (2005).

[25] F. Oggier, E. Bayer-Fluckiger, Best rotated cubic lattice constellations for the Rayleigh fading channel, Proceedings of IEEE International Symposium on Information Theory (2003) 37.

[26] P. Samuel, Algebraic theory of numbers, Herman, Paris (1967).

[27] I. Soprunov, Lattice polytopes in coding theory, J. Algebra Comb. Discrete Struct. Appl. 2(2) (2015) 85–94.

[28] J. E. Strapasson, A. J. Ferrari, G. C. Jorge, S. I. R. Costa, Algebraic constructions of rotated unimodular lattices and direct sum of Barnes-Wall lattices, J. Algebra and its Appl. 20(3) (2021) 2150029.

[29] L. Washington, Introduction to cyclotomic fields, Springer-Verlag, New York (1982).