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

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

Abstract: A classification of all totally real subfields $K$ of cyclotomic fields $\mathbb{Q}(\zeta_{2^r})$, 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 $K$ of $\mathbb{Q}(\zeta_{2^r})$ must be of the form $K = \mathbb{Q}(\zeta_{2^s} + \zeta_{2^s}^{-1})$, 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, Baauri, 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
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 \(Z\)-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 \(Z^n\)-lattices constructed from totally real number fields. In [1, 2], rotated \(Z^n\)-lattices were constructed from the totally real fields \(\mathbb{Q}(\xi_{2^r} + \xi_{2^s}^{-1})\), with \(k = 0, 1\), and their minimum product distances were computed, where \(\xi_{2^r}\) is primitive \(2^r\)-th root of unity. Having the construction procedure of rotated \(Z^n\)-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 \(\mathbb{Q}(\xi_{2^r} + \xi_{2^k}^{-1})\), where \(k \in \mathbb{Z}\).

We conclude that, whatever the \(Z^n\)-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 \(\mathbb{K} = \mathbb{Q}(\xi_{2^r} + \xi_{2^s}^{-1})\), for \(s = r - j\) \((0 \leq j \leq r - 3)\) is equivalent to \(\mathbb{K} = \mathbb{Q}(\xi_{2^r} + \xi_{2^s}^{-1})\) 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 some facts about number fields, and in particular, cyclotomic fields. We conclude that, whatever the \(Z^n\)-lattice built on totally real subfields of cyclotomic fields as the main motivation, the minimum product distances were computed, where \(\xi_{2^r}\) is primitive \(2^r\)-th root of unity. Having the construction procedure of rotated \(Z^n\)-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 \(\mathbb{Q}(\xi_{2^r} + \xi_{2^k}^{-1})\), where \(k \in \mathbb{Z}\).

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 \(L\) be a number field of degree \(n\), \(O_L\) its ring of integers, and \(\sigma_1, \ldots, \sigma_n\) the monomorphisms of \(L\) into \(C\). The embedding \(\sigma_i\) is called real if \(\sigma_i(L)\) is contained in \(\mathbb{R}\), and is called complex otherwise. The field \(L\) is said to be totally real if all of its embeddings are real.

Given \(x \in O_L\), the (rational) integers \(N(x) = N_{L/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)\) and \(Tr(x) = Tr_{L/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)\) are called norm and trace of \(x\) in \(L/\mathbb{Q}\), respectively. The norm of a free \(\mathbb{Z}\)-module \(A\) of rank \(n\) contained in \(O_L\) is defined as \(N(A) = N_L(A) = |O_L/I|\). If \(\{\omega_1, \ldots, \omega_n\}\) is a \(\mathbb{Z}\)-basis for \(O_L\), then the (rational) integer \(d_L = (\det(\sigma_i(\omega_j)))_{i,j=1}^{n}\) is called the discriminant of \(L\). Throughout this work, \(Z_m\) will denote the (cyclic) group of integers modulo \(m\) and \(Z_m^n\) 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, \(\mathbb{L}^+ = \mathbb{L} \cap \mathbb{R} = \mathbb{Q}(\xi_{2^r} + \xi_{2^2}^{-1})\). One has:

1. \([\mathbb{L} : \mathbb{Q}] = 2^{r-1}\) and \([\mathbb{L}^+ : \mathbb{Q}] = 2^{r-2}\).
2. The ring of algebraic integers of \(\mathbb{L}^+\) is \(\mathbb{Z}[\xi_{2^r} + \xi_{2^2}^{-1}]\).
3. \(\{1, \xi_{2^r} + \xi_{2^2}^{-1}, \xi_{2^r}^2 + \xi_{2^2}^{-2}, \ldots, \xi_{2^r}^{2^{r-1}} + \xi_{2^2}^{-2^{r-2}+1}\}\) is an integral basis for \(\mathbb{L}^+\).
4. \(\mathbb{L}/\mathbb{Q}\) is a Galois extension whose Galois group \(\text{Gal}(\mathbb{L}/\mathbb{Q})\) is isomorphic to \(\mathbb{Z}_{2^r}\).
(v) \( L^+/\mathbb{Q} \) is a Galois extension whose Galois group \( \text{Gal}(L^+/\mathbb{Q}) \) is cyclic and generated by \( \sigma \), the automorphism defined by \( \sigma(\xi_{2r} + \xi_{2r}^{-1}) = \xi_{2r}^5 + \xi_{2r}^{-5} \). Moreover, \( \text{Gal}(L^+/\mathbb{Q}) \) is isomorphic to \( \mathbb{Z}_{2r-2}^* \).

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

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

Proof. The statement is an immediate consequence of the fact that the extension \( L^+/\mathbb{Q} \) is Galois: The intermediate fields between \( L^+ \) and \( \mathbb{Q} \) are in one-to-one correspondence with the subgroups of \( \text{Gal}(L^+/\mathbb{Q}) \), 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 \( K \) is a totally real subfield of \( L = \mathbb{Q}(\xi_{2r}) \), then \( K \subseteq L^+ \).

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

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

(i) \( [L_j : L_j^+] = 2 \) and \( L_{j+1} \subset L_j \).

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

(iii) \( L_{j+1} \subset L_j^+ \) and \( [L_j^+ : L_{j+1}] = 2 \).

(iv) \( [L_j : L_{j+1}] = 2 \).
Proof.

(i) Obviously \([L_j : L_j^+] = 2\) since \(L_j^+\) is the maximal real subfield of \(L_j\). Notice that \(L_0 = \mathbb{L}\) and \(L_0^+ = \mathbb{L}^+ = \mathbb{Q}(\xi_2 + \xi_2^{-1})\). Since \(\xi_{2r-j-1} = \xi_{2r-j}^{-1} \in \mathbb{Q}(\xi_{2r-j})\), one has \(L_{j+1} = \mathbb{Q}(\xi_{2r-j}^{-1}) \subset \mathbb{Q}(\xi_{2r-j}) = L_j\).

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

(iii) Since \(L_j^+ = L_j \cap \mathbb{R}\) and \(L_{j+1} \subset L_j\) (see (i)), it follows that
\[
L_j^+ \cap L_{j+1} = (L_j \cap \mathbb{R}) \cap L_{j+1} = (L_j \cap L_{j+1}) \cap \mathbb{R} = L_{j+1} \cap \mathbb{R} = L_{j+1}^+,
\]
and therefore, \(L_{j+1}^+ \subset L_j^+\). The second assertion follows from \([L_j^+ : \mathbb{Q}] = 2^{r-j-3}\) (see (ii)) and
\[
[L_j^+ : \mathbb{Q}] = [L_j^+ : L_{j+1}^+] \cdot [L_{j+1}^+ : \mathbb{Q}].
\]

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

\[\square\]

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

Proof. If \(K\) is a subfield of \(\mathbb{L}\) and \([K : \mathbb{Q}] = t\), 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 \(L_j^+ = \mathbb{Q}(\xi_{2r-j} + \xi_{2r-j}^{-1})\) is such that \([L_j^+ : \mathbb{Q}] = 2^{r-j-2} = 2^m\). As \(K\) is a totally real number field, \(K \subseteq L_j^+\) by Proposition 2.3. In summary, we have \(K, L_j^+ \subseteq \mathbb{L}^+\) with \([K : \mathbb{Q}] = [L_j^+ : \mathbb{Q}] = 2^{r-j-2} = 2^m\). Since by Proposition 2.2 there exists a unique subfield \(K\) of \(\mathbb{L}^+\) such that \([K : \mathbb{Q}] = 2^{r-j-2}\), one has \(K = L_j^+\).

\[\square\]

3. Ideal lattices and minimum product distance

Let \(m \leq n\) be positive integers and \(\Lambda\) a lattice with basis \(\{v_1, \ldots, v_n\}\). Let the coordinates of the basis vectors be \(v_i = (v_i, \ldots, v_in) \in \mathbb{R}^n\) for \(i = 1, \ldots, m\). The matrices \(M = (v_{ij})\) and \(G = MM^t\) are called generator and Gram matrices for \(\Lambda\), respectively, where \(t\) denotes transpose. The determinant of \(\Lambda\), 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 \(\Lambda\).

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

\[
\sigma_{\alpha}(x) = (\sqrt{\alpha_1} \sigma_1(x), \ldots, \sqrt{\alpha_n} \sigma_n(x)),
\]

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

\[
G = (Tr_{K/\mathbb{Q}}(\alpha w_i w_j))_{i,j=1}^n.
\]
respectively. The minimum product distance of \( \Lambda \) is given by
\[
d_{p,\text{min}}(\Lambda) = \sqrt{N_{\mathbb{K}/\mathbb{Q}}(\alpha)} \min_{0 \neq y \in \mathcal{A}} |N_{\mathbb{K}/\mathbb{Q}}(y)|.
\]

In particular, if \( \mathcal{A} \subseteq \mathcal{O}_K \) is a principal ideal, then
\[
d_{p,\text{min}}(\Lambda) = \frac{\sqrt{\det(\Lambda)}}{|d_{\mathbb{K}}|},
\]
see [6]. The normalized minimum product distance of \( \Lambda \), denoted by \( d_{p,\text{norm}}(\Lambda) \), is the minimum product distance with normalized determinant \( \det(\Lambda) = 1 \), i.e.,
\[
d_{p,\text{norm}}(\Lambda) = \frac{1}{\sqrt{\det(\Lambda)}} d_{p,\text{min}}(\Lambda).
\]

In particular, if \( \mathcal{A} \subseteq \mathcal{O}_K \) is a principal ideal then
\[
d_{p,\text{norm}}(\Lambda) = \frac{1}{\sqrt{|d_{\mathbb{K}}|}}.
\]

**Theorem 3.1.** [6] Notation as above, if \( \mathcal{A} \subseteq \mathcal{O}_L \) 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 \( \alpha \) 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 \( \tilde{N} = N_{\mathbb{L}_j^+}/\mathbb{L}_j^+ \). Then \( 2\tilde{N}[\xi] = (1 - \xi)^{2^{(r-j)}\mathbb{Z}[\xi]} \) in \( \mathbb{Q}[\xi] \), where \( \varphi \) is the Euler function. So, \( \tilde{N}(1 - \xi) = 2 \). Using the transitivity of the norm, we obtain
\[
2 = \tilde{N}(1 - \xi) = N(\tilde{N}(1 - \xi)) = N((1 - \xi)(1 - \xi^{-1})) = N(2 - \theta_j) = N(\alpha),
\]
which proves the result.

The condition \( N(\alpha) = 2 \) for some \( \alpha \) 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 \( \alpha \) is as in Proposition 4.1.
Proposition 4.2. [17] If \( L_j = \mathbb{Q}(\xi_{2^{r-j}}) \), then

\[
Tr_{L_j/\mathbb{Q}}(\xi_{2^{r-j}}^k) = \begin{cases} 
0 & \text{if } \gcd(k, 2^{r-j}) < 2^{r-j-1}, \\
-2^{r-j-1} & \text{if } \gcd(k, 2^{r-j}) = 2^{r-j-1}, \\
2^{r-j-1} & \text{if } \gcd(k, 2^{r-j}) > 2^{r-j-1}.
\end{cases}
\]

Corollary 4.3. If \( L_j^+ = \mathbb{Q}(\xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1}) \), then

\[
Tr_{L_j^+/\mathbb{Q}}(\xi_{2^{r-j}}^k + \xi_{2^{r-j}}^{-k}) = \begin{cases} 
0 & \text{if } \gcd(k, 2^{r-j}) < 2^{r-j-1}, \\
-2^{r-j-1} & \text{if } \gcd(k, 2^{r-j}) = 2^{r-j-1}, \\
2^{r-j-1} & \text{if } \gcd(k, 2^{r-j}) > 2^{r-j-1}.
\end{cases}
\]

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

\[
Tr_{L_j/\mathbb{Q}}(\xi_{2^{r-j}}^k) + Tr_{L_j/\mathbb{Q}}(\xi_{2^{r-j}}^{-k}) = Tr_{L_j/\mathbb{Q}}(Tr_{L_j/L_j^+}(\xi_{2^{r-j}}^k + \xi_{2^{r-j}}^{-k})) = 2Tr_{L_j/\mathbb{Q}}(\xi_{2^{r-j}}^k + \xi_{2^{r-j}}^{-k}).
\]

The result now follows from Proposition 4.2.

Proposition 4.4. Notation as in Proposition 4.1, let \( e_0 = 1 \) and \( e_k = \xi_{2^{r-j}}^k + \xi_{2^{r-j}}^{-k} \) for \( k = 1, 2, \ldots, 2^{r-j-2} - 1 \).

(i) \( Tr_{L_j^+/\mathbb{Q}}(ae_ke_k) = \begin{cases} 
2^{r-j-1} & \text{if } k = 0; \\
2^{r-j} & \text{otherwise.}
\end{cases} \)

(ii) If \( k > 0 \), then \( Tr_{L_j^+/\mathbb{Q}}(ae_ke_0) = \begin{cases} 
-2^{r-j-1} & \text{if } k = 1; \\
0 & \text{otherwise.}
\end{cases} \)

(iii) If \( 0 < i < k \), then \( Tr_{L_j^+/\mathbb{Q}}(ae_i) = \begin{cases} 
-2^{r-j-1} & \text{if } |i-k| = 1; \\
0 & \text{otherwise.}
\end{cases} \)

Proof. To simplify the notation, denote \( Tr_{L_j^+/\mathbb{Q}} \) by \( Tr \).

(i) By Corollary 4.3, \( Tr(\theta_j) = 0 \). One has \( Tr(ae_0e_0) = Tr(a) = Tr(2) = Tr(2) = 2^{r-j-1} \).

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

\[
Tr(\alpha e_k e_0) = Tr(\alpha e_k) = Tr((2 - (\xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1}))(\xi_{2^{r-j}}^k + \xi_{2^{r-j}}^{-k}))
= 2Tr(\xi_{2^{r-j}}^k + \xi_{2^{r-j}}^{-k}) - Tr(\xi_{2^{r-j}}^{2k} + \xi_{2^{r-j}}^{2k+1}) - Tr(\xi_{2^{r-j}}^{2k+1} + \xi_{2^{r-j}}^{2k})
= Tr(\xi_{2^{r-j}}^{2k-1} + \xi_{2^{r-j}}^{-2k-1}) = \begin{cases} 
-2^{r-j-1} & \text{if } k = 1; \\
0 & \text{if } k \neq 1.
\end{cases}
\]

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

\[
Tr(\alpha e_ke_k) = Tr(\alpha e_{2k}) = Tr((2 - (\xi_{2^{r-j}} + \xi_{2^{r-j}}^{-1}))(\xi_{2^{r-j}}^{2k} + \xi_{2^{r-j}}^{-2k} + 2))
= 2Tr(\xi_{2^{r-j}}^{2k} + \xi_{2^{r-j}}^{-2k}) + Tr(4) - Tr(\xi_{2^{r-j}}^{2k+1} + \xi_{2^{r-j}}^{2k+2})
- Tr(\xi_{2^{r-j}}^{2k+2} + \xi_{2^{r-j}}^{2k+1}) = 2^{r-j}.
\]
Proposition 4.5. Notation as in Propositions 4.1 and 4.4, if \( A = \mathcal{O}_{L_j} \), then \( \frac{1}{\sqrt{2^{r-j}}}, \sigma_A(A) \) is a rotated \( \mathbb{Z}^n \)-lattice.

Proof. From (1), it follows that the Gram matrix for \( \frac{1}{\sqrt{2^{r-j}}}, \sigma_A(A) \) is given by

\[
G_1 = \left( \text{Tr}_{L_j/Q}(ae, e_k) \right)_{i,k=0}^{n-1}
\]

and by Proposition 4.4, one has

\[
G_1 = \begin{pmatrix}
1 & -1 & 0 & \cdots \\
-1 & 2 & 1 & 0 & \cdots \\
0 & -1 & 2 & -1 & 0 & \cdots \\
\vdots & 0 & -1 & 2 & -1 & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\end{pmatrix}
\]

Let \( T \) the change of basis matrix

\[
T = \begin{pmatrix}
-1 & -1 & \cdots & -1 & -1 \\
-1 & -1 & \cdots & -1 & 0 \\
-1 & -1 & \cdots & -1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
-1 & -1 & \cdots & 0 & 0 \\
-1 & 0 & \cdots & 0 & 0
\end{pmatrix}
\]

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

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

\[
d_{\text{p,norm}}(\Lambda_n) = 2^{1-(r-j-1)\sigma_{r-j-2}}
\]

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

Proof. If \( K \) 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 \( K = \mathcal{O}_{L_j} \) and \( n = [K : \mathbb{Q}] = 2^{r-j-2} \), or equivalently, with \( r - j = 2 + \log_2 n \). As \( \mathcal{O}_K \) is a principal ideal, then from Equation (4) and Proposition 2.1 (vi),

\[
d_{\text{p,norm}}(\Lambda_n) = \frac{1}{\sqrt{|d_{L_j}|}} = \frac{1}{\sqrt{2^{(r-j-1)\sigma_{r-j-1}}}} = 2^{1-(r-j-1)\sigma_{r-j-2}}
\]

which proves the result.
5. Conclusions

This work provided a classification of all totally real subfields $K$ of cyclotomic fields $\mathbb{Q}(\xi_{2^r})$ for any $r \geq 4$. It was proved that any totally real subfield $K$ of $\mathbb{Q}(\xi_{2^r})$ must be of the form $K = \mathbb{Q}(\xi_{2^s} + \xi_{2^{r-1}}^{-1})$, 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 $\Lambda_n = \sigma_n(\mathcal{O}_K)$ was determined (Proposition 4.6). The obtained results are displayed in Table 1. The parameter $\sqrt{d_{p,norm}(\Lambda_n)}$ 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 $\mathbb{Q}(\xi_{2^s} + \xi_{2^{r-1}}^{-1})$ 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 $K$, a totally real subfield of the cyclotomic field $\mathbb{Q}(\xi_{2^r})$.

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

References


