Journal of Algebra 429 (2015) 218–235

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Algebraic constructions of densest lattices [☆]

Grasiele C. Jorge [a,*], Antonio A. de Andrade [b,*], Sueli I.R. Costa [c,*], João E. Strapasson [d,*]

[a] *UNIFESP – Federal University of São Paulo, 12247-014, São José dos Campos, SP, Brazil*

[b] *UNESP – São Paulo State University, 15054-000, São José do Rio Preto, SP, Brazil*

[c] *UNICAMP – University of Campinas, 13083-859, Campinas, SP, Brazil*

[d] *UNICAMP – University of Campinas, 13484-350, Limeira, SP, Brazil*

ARTICLE INFO

Article history:
Received 7 March 2014
Available online xxxx
Communicated by Eva Bayer-Fluckiger

Keywords:
Algebraic number theory
Lattices
Packing density
Diversity
Minimum product distance
Coding theory

ABSTRACT

The aim of this paper is to investigate rotated versions of the densest known lattices in dimensions 2, 3, 4, 5, 6, 7, 8, 12 and 24 constructed via ideals and free $\mathbb{Z}$-modules that are not ideals in subfields of cyclotomic fields. The focus is on totally real number fields and the associated full diversity lattices which may be suitable for signal transmission over both Gaussian and Rayleigh fading channels. We also discuss on the existence of a number field $\mathbb{K}$ such that it is possible to obtain the lattices A_2, E_6 and E_7 via a twisted embedding applied to a fractional ideal of $\mathcal{O}_{\mathbb{K}}$.

[☆] This work was partially supported by CNPq 150802/2012-9 and 312926/2013-8 and FAPESP 2013/25977-7.

[*] Corresponding author.
E-mail addresses: grasiele.jorge@unifesp.br (G.C. Jorge), andrade@ibilce.unesp.br (A.A. Andrade), sueli@ime.unicamp.br (S.I.R. Costa), joao.strapasson@fca.unicamp.br (J.E. Strapasson).

http://dx.doi.org/10.1016/j.jalgebra.2014.12.044
0021-8693/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

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 $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$ such that $\Lambda = \{\sum_{i=1}^{m} a_i \boldsymbol{v}_i;\ a_i \in \mathbb{Z},\ i = 1, \ldots, m\}$.

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 (see [9, Section I]). For this purpose the lattice parameters we consider here are packing density, diversity and minimum product distance.

The classical sphere packing problem is to find out how densely a large number of identical spheres can be packed together in the Euclidean space. The *packing density* of a lattice Λ is the proportion of the space $\mathbb{R}^n$ covered by the non-overlapping spheres of maximum radius centered at the points of Λ. The densest possible lattice packings have only been determined in dimensions 1 to 8 and 24 (see [12, p. 12] for $n = 1, 2, \ldots, 8$ and [13] for $n = 24$). It is also known that these densest lattice packings are unique.

A lattice Λ has *diversity* $k \leq n$ if k is the maximum number such that any non-zero vector $\boldsymbol{y} \in \Lambda$ has at least k non-zero coordinates. Given a full rank lattice with full diversity $\Lambda \subseteq \mathbb{R}^n$, i.e., $k = n$, the *minimum product distance* of Λ is defined as $d_{p,min}(\Lambda) = \min\{\prod_{i=1}^{n} |y_i|;\ \boldsymbol{y} \in \Lambda,\ \boldsymbol{y} \neq \boldsymbol{0}\}$.

Usually the problem of finding good signal constellations for a Gaussian channel is associated with the search for lattices with high packing density (see [12, Chapter 3]). On the other hand, for a Rayleigh fading channel the efficiency, measured by lower error probability in the transmission, is strongly related to the lattice diversity and high minimum product distance (see [9, Section III]).

In this paper, we make use of algebraic number theory for constructing rotated lattices via subfields of cyclotomic fields. Let $\mathbb{K}$ be a number field of degree n, $\mathcal{O}_{\mathbb{K}}$ its ring of integers and $\alpha \in \mathcal{O}_{\mathbb{K}}$ a totally positive real element. In [3,4] it was introduced a twisted embedding $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ such that if $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n, then $\sigma_\alpha(\mathcal{I})$ is a lattice in $\mathbb{R}^n$. These lattices are called here *algebraic lattices*. Special algebraic lattice constructions can be used to obtain certain lattice parameters such as packing density and minimum product distance, which are usually difficult to calculate for general lattices in $\mathbb{R}^n$. Some constructions and properties of algebraic lattices can be found in [1–18]. We quote particularly the paper [8], where full diversity rotated versions of the lattices A_2, E_6, E_8, K_{12} and Λ_{24} are constructed.

Let $\mathbb{K}$ be a totally real number field. When an algebraic lattice can be obtained via a free $\mathbb{Z}$-module $\mathcal{I}$ contained in $\mathcal{O}_{\mathbb{K}}$, its minimum product distance depends on the discriminant $d_{\mathbb{K}}$ of the number field considered (see [6, Section III]). In order to get greater minimum product distances, we consider number fields with small discriminants. Results on the existence of number fields $\mathbb{K}$ such that it is possible to obtain rotated A_2, E_6 and E_7-lattices via twisted embeddings applied to fractional ideals of $\mathcal{O}_{\mathbb{K}}$ are presented in Propositions 4.1, 4.7 and 4.10. Using some constructions of rotated $\mathbb{Z}^n$-lattices, we also show that there are infinitely many rotated D_3, D_5, and E_7-lattices obtained via free $\mathbb{Z}$-modules that are not ideals.

The paper is organized as follows. In Sections 2 and 3, we collect some results on number fields and algebraic lattices. In Subsections 4.1, 4.2, 4.3, 4.5, 4.6 and 4.7 explicit constructions of rotated A_2, D_4, E_6, E_8, K_{12} and Λ_{24}-lattices via principal ideals and free $\mathbb{Z}$-modules that are not ideals are presented. In Subsections 4.2 and 4.4 rotated D_3, D_5 and E_7-lattices are obtained. Finally, in Section 5, we present a comparison between relative minimum product distance and density of the lattices considered here and rotated $\mathbb{Z}^n$-lattices.

2. Basic results from algebraic number theory

In this section, we summarize some concepts and results from algebraic number theory and establish the notation to be used from now on. The results presented here can be found in [22,23].

Let $\mathbb{K}$ be a number field of degree n and $\mathcal{O}_{\mathbb{K}}$ its ring of integers. As it is well known, there are exactly n distinct $\mathbb{Q}$-homomorphisms $\sigma_i : \mathbb{K} \to \mathbb{C}$, for $i = 1, 2, \ldots, n$. A homomorphism σ_i is said to be *real* if $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ and *imaginary* otherwise. A number field $\mathbb{K}$ is said to be *totally real* if σ_i is real for all $i = 1, \ldots, n$ and *totally imaginary* if σ_i is imaginary for all $i = 1, \ldots, n$. A number field $\mathbb{K}$ is called a *CM-field* if there is a totally real number field $\mathbb{F}$ such that $\mathbb{K}$ is a totally imaginary quadratic extension of $\mathbb{F}$.

Given $x \in \mathbb{K}$, the values $N(x) = N_{\mathbb{K}|\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ and $Tr(x) = Tr_{\mathbb{K}|\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$ are called *norm* and *trace* of x in $\mathbb{K}|\mathbb{Q}$, respectively, and if $x \in \mathcal{O}_{\mathbb{K}}$, then $N(x), Tr(x) \in \mathbb{Z}$.

Every non-zero fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n. The *norm* of a free $\mathbb{Z}$-module $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ of rank n is defined as $N_{\mathbb{K}}(\mathcal{I}) = |\mathcal{O}_{\mathbb{K}}/\mathcal{I}|$. If $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{K}}$, the integer $d_{\mathbb{K}} = (\det(\sigma_j(\omega_i))_{i,j=1}^{n})^2$ is called the *discriminant* of $\mathbb{K}$ and it is an invariant under change of basis.

Let p be a prime number and $\mathcal{P} = p\mathbb{Z} \subseteq \mathbb{Z}$ a prime ideal. The ideal $\mathcal{P}\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$ can be expressed as $\mathcal{P}\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, where $\mathcal{Q}_i$'s are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$ and e_i's are positive integers. The integer e_i is called the *ramification index* of $\mathcal{Q}_i$ over $\mathcal{P}$ and it is denoted by $e(\mathcal{Q}_i|p)$. The degree $f_i = f(\mathcal{Q}_i|p) = [\mathcal{O}_{\mathbb{K}}/\mathcal{Q}_i : \mathbb{Z}/\mathcal{P}]$ is called the *residual degree* of $\mathcal{Q}_i$ over $\mathcal{P}$. We have that $\sum_{i=1}^{g} e_i f_i = n$.

A prime p is said to be *inert* in $\mathbb{K}|\mathbb{Q}$ if $g = 1$ and $e_1 = 1$, that is if $p\mathbb{Z} = \mathcal{Q}$ (and hence $f_1 = n$). A prime p *splits completely* in $\mathbb{K}|\mathbb{Q}$ if $g = n$ (and hence $e_i = f_i = 1$ for all i). p is said to be *ramified* in $\mathbb{K}|\mathbb{Q}$ if there is an $e_i \geq 2$, otherwise p is said to be *unramified.*

If $\mathbb{K}|\mathbb{Q}$ is a Galois extension, then we have that $\mathcal{P}\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e}$, where the $\mathcal{Q}_i$'s are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$, $f(\mathcal{Q}_i|p) = [\mathcal{O}_{\mathbb{K}}/\mathcal{Q}_i : \mathbb{Z}/\mathcal{P}] = f$ for all $i = 1, \ldots, g$, and $n = efg$.

Let $\zeta_m \in \mathbb{C}$ be a primitive m-th root of unity. We consider here the *cyclotomic field* $\mathbb{L} = \mathbb{Q}(\zeta_m)$ and its maximal totally real subfield $\mathbb{K} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. We have that

$[\mathbb{Q}(\zeta_m):\mathbb{Q}] = \varphi(m)$ and $[\mathbb{Q}(\zeta_m+\zeta_m^{-1}):\mathbb{Q}] = \varphi(m)/2$, where φ is the Euler function. Moreover, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_m]$ and $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_m+\zeta_m^{-1}]$.

3. Algebraic lattices

Let $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_m\}$ be a set of linearly independent vectors in $\mathbb{R}^n$ and $\Lambda = \left\{\sum_{i=1}^m a_i\boldsymbol{v}_i;\ a_i\in\mathbb{Z}\right\}$ the associated lattice. The set $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_m\}$ is called a *basis* for Λ. A matrix M whose rows are these vectors is said to be a *generator matrix* for Λ while the associated *Gram matrix* is $G = MM^t = (\langle\boldsymbol{v}_i,\boldsymbol{v}_j\rangle)_{i,j=1}^m$. The *determinant* of Λ is $\det\Lambda = \det G$ and it is an invariant under change of basis (see [12, p. 4]). A lattice Λ is said to be *integral* if $\langle\boldsymbol{x},\boldsymbol{y}\rangle\in\mathbb{Z}$ for any $\boldsymbol{x},\boldsymbol{y}\in\Lambda$. An integral lattice is said to be *even* if $\langle\boldsymbol{x},\boldsymbol{x}\rangle$ is even for any $\boldsymbol{x}\in\Lambda$ and *odd* otherwise. A *unimodular* lattice is an integral lattice with $\det(\Lambda)=1$. Two lattices Λ_1 and Λ_2 are said to be *similar* if there is an orthogonal mapping $\phi:\mathbb{R}^n\to\mathbb{R}^n$ and a real positive number c such that $c\phi(\Lambda_1)=\Lambda_2$. When $c=1$ the similar lattices Λ_1 and Λ_2 are said to be *congruent* or *isomorphic*. In this paper, as in [6,17], we will say that Λ_1 is a *rotated* Λ_2-lattice if Λ_1 and Λ_2 are congruent.

The computational search for detecting if two lattices are isomorphic is in general a difficult problem. The isomorphism problem on lattices, which also has showed up in lattice applications to cryptography, is at least as hard as that on graphs and lies on complexity class SZK (see [16] and references therein). In [16, Theorem 1.1] it is derived an algorithm for solving it running in time $n^{O(n)}$ times a polynomial in the input size, where n is the rank of the lattice.

In what follows let $\mathbb{K}$ be a number field of degree $n = r_1+2r_2$. Let σ_i, for $i = 1,\dots,n$, be the n distinct $\mathbb{Q}$-homomorphisms from $\mathbb{K}$ to $\mathbb{C}$ such that $\sigma_1,\dots,\sigma_{r_1}$ are real, $\sigma_{r_1+1},\dots,\sigma_{r_1+r_2}$, $\sigma_{r_1+r_2+1},\dots,\sigma_{r_1+2r_2}$ are imaginary and $\sigma_{r_1+r_2+i}$ is the complex conjugate of σ_{r_1+i}, for all $i=1,\dots,r_2$.

Definition 3.1. (Cf. [4], Section 4.) Let $\alpha\in\mathbb{K}$ be a totally positive element (i.e., $\sigma_i(\alpha)>0$ for all $i=1,\dots,n$), and let $\alpha_i=\sigma_i(\alpha)$. The *twisted embedding* $\sigma_\alpha:\mathbb{K}\longrightarrow\mathbb{R}^n$ is defined by $\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x),\dots,\sqrt{\alpha_{r_1}}\sigma_{r_1}(x),\sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)),\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)),\dots,$ $\sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)),\sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)))$, where $\Re$ and $\Im$ represent the real and imaginary part of a complex number, respectively.

Proposition 3.2. *(Cf. [20], Corollary 2.1.) Let $\mathbb{K}$ be a number field of degree n, and let $\alpha\in\mathbb{K}$ be a totally positive element. If $\mathcal{I}\subseteq\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1,\dots,w_n\}$, then the image $\Lambda=\sigma_\alpha(\mathcal{I})$ is a lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(w_1),\dots,\sigma_\alpha(w_n)\}$.*

If $\mathbb{K}$ is a totally real number field or a CM-field, the complex conjugation commutes with all homomorphisms σ_i, $i=1,\dots,n$, and therefore the associated Gram matrix for $\sigma_\alpha(\mathcal{I})$ can be expressed in the special form described next.

Proposition 3.3. *(Cf. [20], Proposition 2.1.) Let $\mathbb{K}$ be a totally real number field or a CM-field, and let $\alpha \in \mathbb{K}$ be a totally positive element. If $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1, \ldots, w_n\}$, then $G = \left(Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_i \overline{w_j})\right)_{i,j=1}^{n}$ is a Gram matrix for $\sigma_\alpha(\mathcal{I})$.*

From now on we will consider $\mathbb{K}$ a totally real number field or a CM-field.

Proposition 3.4. *(Cf. [4], Proposition 15.) Let $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ be a free $\mathbb{Z}$-module of rank n. A lattice $\Lambda = \sigma_\alpha(\mathcal{I})$ has diversity n if $\mathbb{K}$ is totally real, and diversity $\frac{n}{2}$ if $\mathbb{K}$ is totally imaginary.*

Proposition 3.5. *(Cf. [6], Theorem 1.) Let $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ be a free $\mathbb{Z}$-module of rank n. If $\mathbb{K}$ is totally real, then $\Lambda = \sigma_\alpha(\mathcal{I})$ has minimum product distance given by $d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} \frac{1}{N_{\mathbb{K}}(\mathcal{I})} \min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)|$. In particular, if $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a principal ideal, then $\min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)| = N_{\mathbb{K}}(\mathcal{I})$.*

Definition 3.6. Let μ be the minimum Euclidean norm of a non-zero vector of a lattice Λ. The *relative minimum product distance* of Λ, denoted by $d_{p,rel}(\Lambda)$, is the minimum product distance of the scaled lattice $\frac{1}{\mu}\Lambda$.

Proposition 3.7. *(Cf. [3], Proposition 2.1.) If $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a non-zero free $\mathbb{Z}$-module of rank n, then $\det(\sigma_\alpha(\mathcal{I})) = N_{\mathbb{K}}(\mathcal{I})^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d_{\mathbb{K}}|$.*

In what follows we present a necessary condition for constructing an algebraic lattice $\Lambda = \sigma_\alpha(\mathcal{I})$ with determinant D via a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$. Proposition 3.9 is a generalization of [18, Proposition 4.3], which considers rotated D_n-lattices.

Lemma 3.8. *Let p be a prime number. Suppose that $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g} \mathcal{Q}_i^e$, where $\mathcal{Q}_i$'s are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$, and $f(\mathcal{Q}_i|p) = f$, for all $i = 1, \ldots, g$. If $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{K}}$ is an ideal and p divides $N_{\mathbb{K}}(\mathcal{B})$, then $N_{\mathbb{K}}(\mathcal{B}) = \left(p^f\right)^a b$, where $a \geq 1$ is an integer and b is an integer such that p does not divide b.*

Proof. Let $\mathcal{B} = \prod_{i=1}^{s} \mathcal{P}_i^{e_i}$, where the $\mathcal{P}_i$'s are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$. Since $p \mid N_{\mathbb{K}}(\mathcal{B})$, it follows that $p \mid N_{\mathbb{K}}(\mathcal{P}_j)$ for some j. Since $\mathcal{P}_j \cap \mathbb{Z} = r\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, it follows that r is a prime number and $\mathcal{P}_j$ lies over $r\mathcal{O}_{\mathbb{K}}$ Thus, $r = p$, the ideal $\mathcal{P}_j$ lies over $p\mathcal{O}_{\mathbb{K}}$ and $N_{\mathbb{K}}(\mathcal{P}_j) = p^f$. So, $N_{\mathbb{K}}(\mathcal{B}) = \prod_{i=1}^{s} N_{\mathbb{K}}(\mathcal{P}_i)^{e_i} = \left(p^f\right)^a b$, where $a \geq 1$ is an integer and b is an integer such that $p \nmid b$. □

Proposition 3.9. *Let $\mathbb{K}|\mathbb{Q}$ be a Galois extension and $d_{\mathbb{K}} = p^r d$, where p is a prime number, $r \geq 0$ is an integer and d is an integer such that p does not divide d. Let Λ be a lattice such that $\det(\Lambda) = p^m q$, where $m > 0$ is an integer and q is an integer such that p does not divide q. If $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g} \mathcal{Q}_i^e$, where $\mathcal{Q}_i$'s are prime ideals of $\mathcal{O}_{\mathbb{K}}$ and $f = f(\mathcal{Q}_i|p)$*

does not divide $(m-r)$*, then there does not exist any fractional ideal* $\mathcal{I}$ *of* $\mathcal{O}_{\mathbb{K}}$ *such that* $\Lambda = \sigma_\alpha(\mathcal{I})$ *for some* $\alpha \in \mathbb{K}$*.*

Proof. Suppose that there exist a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ and a totally positive element $\alpha \in \mathbb{K}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$. Thus, there exists a positive integer $t \in \mathbb{Z}$ such that $t\mathcal{I} = \mathcal{A}$ is an ideal of $\mathcal{O}_{\mathbb{K}}$, and therefore, $N_{\mathbb{K}}(\mathcal{I}) = N_{\mathbb{K}}(\mathcal{A})/t^n$. By Lemma 3.8, if p divides $N_{\mathbb{K}}(\mathcal{A})$, then $N_{\mathbb{K}}(\mathcal{A}) = \left(p^f\right)^{a_1} b_1$, where $a_1 \geq 1$ is an integer and b_1 is an integer such that $p \nmid b_1$. Otherwise, if p does not divide $N_{\mathbb{K}}(\mathcal{A})$, then $N_{\mathbb{K}}(\mathcal{A}) = \left(p^f\right)^{a_1} b_1$, where $a_1 = 0$ and b_1 is an integer such that $p \nmid b_1$. So, we can write $N_{\mathbb{K}}(\mathcal{A}) = \left(p^f\right)^{a_1} b_1$, where $a_1 \geq 0$ is an integer and b_1 is an integer such that $p \nmid b_1$ and then $N_{\mathbb{K}}(\mathcal{I}) = \left(p^f\right)^{a_1} b_1/t^n$. Given $\alpha \in \mathbb{K}$, there exists an integer s such that $s\alpha \in \mathcal{O}_{\mathbb{K}}$. We can write $N_{\mathbb{K}|\mathbb{Q}}(s\alpha) = N_{\mathbb{K}}(s\alpha\mathcal{O}_{\mathbb{K}}) = \left(p^f\right)^{a_2} b_2$, where $a_2 \geq 0$ is an integer and b_2 is an integer such that $p \nmid b_2$. Then, $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = \left(p^f\right)^{a_2} b_2/s^n$. Let $t = p^{k_1} l_1$ and $s = p^{k_2} l_2$, where $k_1, k_2 \geq 0$ are integers and l_1, l_2 are integers such that $p \nmid l_1$ and $p \nmid l_2$. From Proposition 3.7, it follows that

$$\begin{aligned} N_{\mathbb{K}}(\mathcal{I})^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d_{\mathbb{K}}| &= \frac{\left(p^f\right)^{2a_1} b_1^2}{t^{2n}} \frac{\left(p^f\right)^{a_2} b_2}{s^n} p^r |d| \\ &= p^{2fa_1 - 2k_1 n + fa_2 - k_2 n + r} \left(b_1^2 l_1^{-2n} l_2^{-n} b_2 |d|\right) = p^m q, \end{aligned}$$

and therefore, $m = 2fa_1 - 2k_1 n + fa_2 - k_2 n + r$. Since $n = efg$, it follows that $m - r = f(2a_1 - 2k_1 eg + a_2 - k_2 eg)$, that is f divides $(m-r)$, which is a contradiction. □

The next remark will be used as a tool for constructing rotated integer lattices.

Remark 3.10. Let $\Lambda \subseteq \mathbb{Z}^n$ be an integer lattice with a generator matrix M, $\mathbb{K}$ a number field of degree n, $\alpha \in \mathbb{K}$ a totally positive element, and $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ a free $\mathbb{Z}$-module of rank n. If $c\sigma_\alpha(\mathcal{I})$ is a rotated $\mathbb{Z}^n$-lattice, for some real positive number c, then there exists a generator matrix R for $c\sigma_\alpha(\mathcal{I})$ such that $RR^t = I_{n\times n}$. The matrix MR is a generator matrix for a rotated version of Λ which is contained in $c\sigma_\alpha(\mathcal{I})$. Therefore we may use the matrix MR and homomorphism properties to get the free $\mathbb{Z}$-submodule $\mathcal{J} \subseteq \mathcal{I}$ such that $\Lambda = c\sigma_\alpha(\mathcal{J})$.

4. Algebraic constructions for densest lattices

In this section, we discuss the possibility of constructing rotated A_2, E_6 and E_7-lattices via twisted embeddings applied to fractional ideals of the ring of integers of a number field $\mathbb{K}$. Constructions of rotated A_2, D_3, D_4, D_5, E_6, E_7, E_8, K_{12} and Λ_{24}-lattices via ideals and free $\mathbb{Z}$-modules that are not ideals are also presented. Full diversity rotated A_2, E_6, E_8, K_{12} and Λ_{24}-lattices are obtained via $\mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$, $\mathbb{Q}(\zeta_{36} + \zeta_{36}^{-1})$, $\mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$, $\mathbb{Q}(\zeta_{84} + \zeta_{84}^{-1})$ and $\mathbb{Q}(\zeta_{140} + \zeta_{140}^{-1})$, respectively, the same number fields considered in [8, Section 3] where the authors construct these lattices by shifting ideal lattices constructed over cyclotomic fields in [3, Section 3] to maximal totally real subfields of cyclotomic fields.

4.1. Rotated A_2-lattice

The classical A_2-lattice in $\mathbb{R}^2$ is generated by the basis $\{(1,0),(-1/2,\sqrt{3}/2)\}$. We consider next the scaled lattice Λ_2 with basis $\{\sqrt{2}(1,0),\sqrt{2}(-1/2,\sqrt{3}/2)\}$ which has minimum squared Euclidean norm 2 and $\det(\Lambda_2)=3$. In the next result, we obtain a necessary condition for constructing a rotated A_2-lattice via a twisted embedding applied to a fractional ideal of $\mathcal{O}_{\mathbb{K}}$. A related result, through a different approach, can be found in [7, Theorem 3.3].

Proposition 4.1. *Let $\mathbb{K}$ be a quadratic number field. If 3 is inert in $\mathbb{K}|\mathbb{Q}$, then there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\sigma_\alpha(\mathcal{I})$ is a rotated A_2-lattice, scaled by $\sqrt{c^*}$, with $c^*\in\mathbb{Z}$, for any $\alpha\in\mathbb{K}$ totally positive.*

Proof. Suppose that there exist a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ and a totally positive element α such that $\Lambda=\sigma_\alpha(\mathcal{I})$ is a rotated Λ_2-lattice, scaled by $\sqrt{c}$ with $c\geq 0$ an integer. Then, $\det(\Lambda)=3c^2$, where $c=3^a b$ with $a\geq 0$ an integer and $b\geq 1$ an integer such that $3\nmid b$. So, $\det(\Lambda)=3^{1+2a}b^2$. Since 3 is inert in $\mathbb{K}|\mathbb{Q}$, we have that $3\mathcal{O}_{\mathbb{K}}=\mathcal{P}$, $e(\mathcal{P}|3)=1$, $f=f(\mathcal{P}|3)=2$ and 3 does not divide the discriminant $d_{\mathbb{K}}$. By Proposition 3.9, since $f=2$ does not divide $(m-r)=(1+2a-0)$, it follows that there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\Lambda=\sigma_\alpha(\mathcal{I})$ is a rotated Λ_2-lattice, scaled by $\sqrt{c}$, with $c\in\mathbb{Z}$, for any $\alpha\in\mathbb{K}$. Since $A_2=\frac{\sqrt{2}}{2}\Lambda_2$ the last assertion holds also for the lattice A_2. □

Example 4.2. Note that $[\mathbb{Q}(\zeta_m):\mathbb{Q}]=2$ if and only if $m=3,4$ and 6 and $[\mathbb{Q}(\zeta_m+\zeta_m^{-1}):\mathbb{Q}]=2$ if and only if $m=5,8,10$ and 12. Let $\mathbb{K}_1=\mathbb{Q}(\zeta_4)=\mathbb{Q}\left(\sqrt{-1}\right)$, $\mathbb{K}_2=\mathbb{Q}(\zeta_5+\zeta_5^{-1})=\mathbb{Q}(\zeta_{10}+\zeta_{10}^{-1})=\mathbb{Q}\left(\sqrt{5}\right)$ and $\mathbb{K}_3=\mathbb{Q}(\zeta_8+\zeta_8^{-1})=\mathbb{Q}\left(\sqrt{2}\right)$. Through a direct computation, we have that 3 is inert in $\mathbb{K}_i|\mathbb{Q}$ for $i=1,2,3$. By Proposition 4.1, it follows that there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}_i}$, for $i=1,2,3$, such that $\Lambda=\sigma_\alpha(\mathcal{I})$ is a rotated A_2-lattice, scaled by $\sqrt{c}$ with $c\in\mathbb{Z}$, for any $\alpha\in\mathbb{K}_i$ totally positive.

Algebraic constructions of rotated A_2-lattices with diversity 1 via $\mathbb{Q}(\zeta_3)=\mathbb{Q}(\zeta_6)=\mathbb{Q}(\sqrt{-3})$ appear in [3, p. 76] and [9, p. 508]. In what follows we present a construction of a rotated A_2-lattice, which is full diversity as the one presented in [8, Section 3], via a principal ideal of the ring of integers of $\mathbb{Q}(\zeta_{12}+\zeta_{12}^{-1})=\mathbb{Q}(\sqrt{3})$.

A rotated A_2-lattice via an ideal of $\mathbb{Z}[\zeta_{12}+\zeta_{12}^{-1}]$: If $\mathbb{K}=\mathbb{Q}(\zeta_{12}+\zeta_{12}^{-1})=\mathbb{Q}(\sqrt{3})$, $\mathcal{I}=\left\langle 1+\sqrt{3}\right\rangle$ and $\alpha=1$, then the lattice $\Lambda=\frac{1}{2}\sigma_\alpha(\mathcal{I})$ is a rotated A_2-lattice and $\sqrt{d_{p,rel}(\Lambda)}=0.5$. In fact, since $d_{\mathbb{K}}=12=2^2 3$, consider the factorization $2\mathcal{O}_{\mathbb{K}}=\mathcal{P}^2$, where $\mathcal{P}=\left\langle 2,1+\sqrt{3}\right\rangle=\left\langle 1+\sqrt{3}\right\rangle$ and $N_{\mathbb{K}}(\mathcal{P})=2$. Taking $\mathcal{I}=\mathcal{P}$ and $\alpha=1$, a straightforward computation shows that the Gram matrix for $\frac{1}{2}\sigma_\alpha(\mathcal{I})$, related to the $\mathbb{Z}$-basis $\{1+\sqrt{3},3+\sqrt{3}\}$ of $\mathcal{I}$, has only even numbers in its diagonal. Therefore, $\frac{1}{2}\sigma_\alpha(\mathcal{I})$ is an even lattice with determinant 3. Since A_2 is up to equivalence the only lattice with this property in dimension 2, it follows that $\frac{1}{2}\sigma_\alpha(\mathcal{I})$ a rotated A_2-lattice. Since the minimum Euclidean norm of $\frac{1}{2}\sigma_\alpha(\mathcal{I})$ is $\sqrt{2}$, its relative minimum product distance satisfies $\sqrt{d_{p,rel}(\Lambda)} = \sqrt{\frac{\frac{1}{2^2}}{\sqrt{2}^2}\sqrt{N_{\mathbb{K}|\mathbb{Q}}(\alpha)N_{\mathbb{K}}(\mathcal{I})^2}} = \sqrt{0.25} = 0.5$.

The rotated A_2-lattices presented above and in [8, Section 3] have the same relative minimum product distance (Proposition 3.5) and, as it can be seen next, this is the maximum possible value for a rotated A_2-lattice.

Proposition 4.3. *The maximum relative minimum product distance for a rotated A_2-lattice is* 0.25*. Moreover, up a coordinate axis reflection, there is a unique rotated A_2-lattice with this relative minimum product distance.*

Proof. Since an orthogonal transformation in the plane is either a rotation or a reflection R_1 on the x-axis composed with a rotation, any lattice congruent to A_2 is obtained by a rotation. Let $Rot(A_2, \theta)$ be the rotation of A_2 by an angle θ, i.e., $Rot(A_2, \theta) = \{k_1(\cos(\theta), \sin(\theta)) + k_2(\cos(\theta + \frac{\pi}{3}), \sin(\theta + \frac{\pi}{3})),\ k_1, k_2 \in \mathbb{Z}\}$. Taking into account the symmetry of A_2 we can consider only $\frac{-\pi}{6} < \theta \leq \frac{\pi}{6}$. Moreover, since we also have that $Rot(A_2, -\theta) = R_1(Rot(A_2, \theta))$ and $Rot(A_2, \frac{\pi}{6} - \theta) = R_2(Rot(A_2, \theta))$, where $R_2(x, y) = (y, x)$, we can restrict our analysis to $0 \leq \theta \leq \frac{\pi}{12}$. The absolute value of the product of the coordinates of a point in $Rot(A_2, \theta)$ is $f(k_1, k_2, \theta) = \left|\frac{1}{2}k_1^2 \sin(2\theta) + \frac{1}{2}k_2^2 \sin(2\theta + \frac{2\pi}{3}) + k_1 k_2 \sin(2\theta + \frac{\pi}{3})\right|$. Since $f(k_1, 0, \theta) = \left|\frac{1}{2}k_1^2 \sin(2\theta)\right| \leq \left|\frac{1}{2}k_1^2 \sin(\frac{\pi}{6})\right| = \frac{1}{4}k_1^2$, it follows that $\frac{1}{4}$ an upper bound for $f(k_1, k_2, \theta)$ which is not reachable for $\theta \neq \frac{\pi}{12}$. On the other hand $f(k_1, k_2, \frac{\pi}{12}) = \frac{1}{4}\left|k_1^2 + k_2^2 + 4k_1k_2\right| \neq 0$, for $k_1, k_2 \in \mathbb{Z}$, $k_1 k_2 \neq 0$, what implies that the relative minimum product distance of $Rot(A_2, \frac{\pi}{12})$ is $\frac{1}{4}$, the biggest possible. The same holds for $Rot(A_2, -\frac{\pi}{12}) = R_1(Rot(A_2, \theta))$. □

4.2. Rotated D_3, D_4 and D_5-lattices

For $n \geq 3$, the n-dimensional lattice D_n in $\mathbb{R}^n$ is described, in its standard form, as $D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n;\ \sum_{i=1}^n x_i \text{ is even}\}$. The set $\beta = \{(-1, -1, 0, \ldots, 0), (1, -1, 0, \ldots, 0), (0, 1, -1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1, -1)\}$ is a basis for D_n, the minimum squared Euclidean norm of this version of D_n is 2 and $\det(D_n) = 4$ for all n.

Algebraic constructions of rotated D_4-lattices with diversity 2 were presented in [3, p. 76] and [9, p. 512] via $\mathbb{Q}(\zeta_8)$, and algebraic constructions of full diversity rotated D_3, D_4 and D_5-lattices were presented in [17, Propositions 4.6 and 5.1] via $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ and $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$, respectively. The lattice D_4 was obtained via a principal ideal of $\mathbb{Z}[\zeta_{16} + \zeta_{16}^{-1}]$ whereas the lattices D_3 and D_5 were obtained via free $\mathbb{Z}$-modules in $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ and $\mathbb{Z}[\zeta_{11} + \zeta_{11}^{-1}]$, respectively, that are not ideals. If it were possible to construct such rotated D_3 and D_5-lattices via principal ideals of $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ and $\mathbb{Z}[\zeta_{11} + \zeta_{11}^{-1}]$, respectively, their minimum product distances would be twice those obtained in such constructions via $\mathbb{Z}$-modules. However, in [18, Proposition 2.7] it was shown that if $\mathbb{K}$ is a totally real Galois extension with $d_{\mathbb{K}}$ an odd integer, then it is impossible to construct rotated D_n-lattices via fractional ideals of $\mathcal{O}_{\mathbb{K}}$. In particular, it is impossible to construct rotated D_3, D_4 and D_5-lattices via fractional ideals of any Galois extension $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$ with m odd.

In what follows we discuss some possibilities for constructing a full diversity rotated D_4-lattice and present a construction of D_4 via a principal ideal of $\mathbb{Z}[\zeta_{12}]$ and via a free $\mathbb{Z}$-module in $\mathbb{Z}[\zeta_{15} + \zeta_{15}^{-1}]$.

Example 4.4. Note that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = 4$ if and only if $m = 5, 8, 10$ and 12 and $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = 4$ if and only if $m = 15, 16, 20, 24$ and 30. Let $\mathbb{K}_1 = \mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_{10})$ and $\mathbb{K}_2 = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}) = \mathbb{Q}(\zeta_{30} + \zeta_{30}^{-1})$. Since $d_{\mathbb{K}_i}$ is odd for $i = 1, 2$, there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}_i}$, for $i = 1, 2$, such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated D_4-lattice, scaled by $\sqrt{c}$ with $c \in \mathbb{Z}$, for any $\alpha \in \mathbb{K}_i$ totally positive.

A rotated D_4-lattice via an ideal of $\mathbb{Z}[\zeta_{12}]$: Let $e_i = \zeta_{12}^i + \zeta_{12}^{-i}$ for all $i \in \mathbb{N}$. If $\mathbb{K} = \mathbb{Q}(\zeta_{12})$, $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$ and $\alpha = (1-e_1)e_5$, then $\frac{1}{6}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is a rotated D_4-lattice. In fact, since $d_{\mathbb{K}} = 2^4 3^2$, consider the factorizations $3\mathcal{O}_{\mathbb{K}} = \mathcal{P}^2$, where $\mathcal{P} = \langle e_5 \rangle$ and $N_{\mathbb{K}}(\mathcal{P}) = 2^2$ and $2\mathcal{O}_{\mathbb{K}} = \mathcal{Q}^2$, where $\mathcal{Q} = \langle 1 - e_1 \rangle$ and $N_{\mathbb{K}}(\mathcal{Q}) = 2^2$. Taking $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$ and $\alpha = (1-e_1)e_5$ a totally positive element, a straightforward computation shows that the Gram matrix for $\frac{1}{6}\sigma_\alpha(\mathcal{I})$, related to the $\mathbb{Z}$-basis $\{1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3\}$ of $\mathcal{O}_{\mathbb{K}}$, has only even numbers in its diagonal. So, the lattice $\Lambda = \frac{1}{6}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is an even lattice with determinant 4. Since D_4 is, up to congruence, the only lattice with this property, it follows that $\frac{1}{6}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is a rotated D_4-lattice.

By considering only the values of m such that $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = 4$ and reordering the list from the minimum to the maximum discriminant, we have $m = 15, 20, 16$ and 24. The case $m = 15$ is considered next.

A rotated D_4-lattice via a $\mathbb{Z}$-module in $\mathbb{Z}[\zeta_{15} + \zeta_{15}^{-1}]$: Let $e_i = \zeta_{15}^i + \zeta_{15}^{-i}$ for all $i \in \mathbb{N}$ and $\mathbb{K} = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$. Since m is odd, there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\sigma_\alpha(\mathcal{I})$ is a rotated and scaled D_4-lattice for any $\alpha \in \mathbb{K}$ totally positive. If $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$ and $\alpha = (1 + e_1)(1 + e_1 + e_2)e_1$, then the lattice $\Lambda = \frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is a rotated $\mathbb{Z}^4$-lattice. In fact, since $d_{\mathbb{K}} = 3^2 5^3$, consider the factorizations $3\mathcal{O}_{\mathbb{K}} = \mathcal{P}^2$, where $\mathcal{P} = \langle 1 + e_1 + e_2 \rangle$ and $N_{\mathbb{K}}(\mathcal{P}) = 3^2$, and $5\mathcal{O}_{\mathbb{K}} = \mathcal{Q}^4$, where $\mathcal{Q} = \langle 1 + e_1 \rangle$ and $N_{\mathbb{K}}(\mathcal{Q}) = 5$. Taking $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$, $\alpha = (1 + e_1)(1 + e_1 + e_2)e_1$ a totally positive element and calculating a Gram matrix for $\Lambda = \frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$, we have that Λ is an odd unimodular lattice in dimension 4, i.e., Λ is a rotated $\mathbb{Z}^4$-lattice. Using Remark 3.10, we obtain the $\mathbb{Z}$-module $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ with $\mathbb{Z}$-basis $\{e_1, 2e_2, e_3, e_4\}$ such that $\Lambda_1 = \frac{1}{\sqrt{15}}\sigma_\alpha(\mathcal{I})$ is a rotated D_4-lattice. Since the minimum Euclidean norm of D_4 is $\sqrt{2}$, $N_{\mathbb{K}}(\mathcal{I}) = 2$ and $N_{\mathbb{K}|\mathbb{Q}}(e_1) = 1$, the relative minimum product distance of Λ_1 satisfies $\sqrt[4]{d_{p,rel}(\Lambda_1)} = \sqrt[4]{\frac{1}{\sqrt{2}^4}\frac{1}{\sqrt{15}^4}\sqrt{(3^2\,5)\,2^2}\,\frac{1}{2}} = 0.29383$.

Remark 4.5. Although the discriminants of $\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$ and $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ are 1125 and 2048, respectively, the relative minimum product distance of the rotated D_4-lattice Λ_2 obtained in [17, Proposition 4.6] via a principal ideal of $\mathbb{Z}[\zeta_{16} + \zeta_{16}^{-1}]$ satisfies

$\sqrt[4]{d_{p,rel}(\Lambda_2)} = 0.324210$ and is greater than the relative minimum product distance obtained via the free $\mathbb{Z}$-module considered above in $\mathbb{Z}[\zeta_{15}+\zeta_{15}^{-1}]$. It is also worth noticing that, in certain cases, the relative minimum product distances obtained via free $\mathbb{Z}$-modules can be greater than some obtained via principal ideals. For example, the rotated D_8-lattice Λ_3 obtained in [17, Proposition 5.1] via a free $\mathbb{Z}$-module in $\mathbb{Z}[\zeta_{17}+\zeta_{17}^{-1}]$ has relative minimum product distance satisfying $\sqrt[8]{d_{p,rel}(\Lambda_3)} = 0.20472$ whereas the rotated D_8-lattice Λ_4 obtained in [17, Proposition 4.6] via an ideal of $\mathbb{Z}[\zeta_{32}+\zeta_{32}^{-1}]$ has relative minimum product distance satisfying $\sqrt[8]{d_{p,rel}(\Lambda_4)} = 0.201311$.

In the next proposition, we show that the lattices D_3 and D_5 can be obtained from infinitely many free $\mathbb{Z}$-modules contained in subfields of cyclotomic fields.

Proposition 4.6. *There exist infinitely many prime numbers p and number fields $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p+\zeta_p^{-1})$ and a full diversity rotated D_3-lattice (D_5-lattice) can be obtained via a twisted embedding applied to a free $\mathbb{Z}$-module of rank 3 (rank 5) contained in $\mathcal{O}_{\mathbb{K}}$.*

Proof. By Dirichlet's Theorem, it follows that there exist infinitely many prime numbers p such that $p \equiv 1 \ (mod\, 3)$. Since 3 divides $p-1$ and $G = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ is cyclic, it follows that there is a unique subgroup $H \subseteq G$ such that $|H| = (p-1)/3$. By Galois Correspondence Theorem, it follows that there is a unique field $\mathbb{K}$ contained in $\mathbb{Q}(\zeta_p)$ which is cyclic of degree 3 over $\mathbb{Q}$. Now, since 3 is odd, it follows that 3 divides $(p-1)/2$ and $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p+\zeta_p^{-1})$. Using the cyclic construction of [6, Section V] we obtain a rotated $\mathbb{Z}^3$-lattice via $\mathcal{O}_{\mathbb{K}}$. Since $D_3 \subseteq \mathbb{Z}^3$, the result follows from Remark 3.10. A similar proof holds for D_5. □

4.3. Rotated E_6-lattice

Algebraic constructions of rotated E_6-lattices were presented in [3, p. 77] and [10, p. 48] via $\mathbb{Q}(\zeta_9)$ with diversity 3, and in [8, Section 3] via $\mathbb{Q}(\zeta_{36}+\zeta_{36}^{-1})$ with full diversity. In what follows we discuss some possibilities for constructing a full diversity rotated E_6-lattice, present a construction of a rotated E_6-lattice via a principal ideal of $\mathbb{Z}[\zeta_{36}+\zeta_{36}^{-1}]$, and calculate its minimum product distance.

The 6-dimensional densest lattice E_6 is an even lattice with minimum squared Euclidean norm 2 and $\det(E_6) = 3$. E_6 can be defined by the basis $(1,1,0,0,0,0)$, $(-1,1,0,0,0,0)$, $(0,-1,1,0,0,0)$, $(0,0,-1,1,0,0)$, $(0,0,0,-1,1,0)$ and $(1/2,-1/2,-1/2,-1/2,-1/2,\sqrt{3}/2)$.

Note that the generator matrix M defined by the basis above (and hence any other generator matrix for E_6 in dimension 6) is not a matrix with only rational entries, up to a scalar factor. So, we cannot use the same strategy of Remark 3.10 for constructing a rotated E_6-lattice.

Proposition 4.7. *Let $\mathbb{K} = \mathbb{Q}(\theta)$ be a Galois extension with $[\mathbb{K} : \mathbb{Q}] = 6$. Let $3\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g} \mathcal{Q}_i^e$, where $\mathcal{Q}_i$'s are prime ideals of $\mathcal{O}_{\mathbb{K}}$, $e(\mathcal{Q}_i|3) = e$ and $f(\mathcal{Q}_i|3) = f$, for all*

$i = 1, \ldots, g$. If 3 does not divide $d_{\mathbb{K}}$, then there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated E_6-lattice, scaled by $\sqrt{c}$ with $c \in \mathbb{Z}$, for any $\alpha \in \mathbb{K}$ totally positive.

Proof. Suppose that there exists a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated E_6-lattice, scaled by $\sqrt{c}$ with $c \geq 0$ an integer. Then, $\det(\Lambda) = 3c^6$, where $c = 3^a b$, with $a \geq 0$ an integer and $b \geq 1$ an integer such that $3 \nmid b$. So, $\det(\Lambda) = 3^{1+6a}b^6$. By Proposition 3.9, it follows that f must divide $(1+6a-r)$. Since 3 does not divide $d_{\mathbb{K}}$, it follows that $r = 0$. We show next that $f \neq 1$ and f divides 6. Therefore, f does not divide $(m-r) = (1+6a-0) = 1+6a$ and the result follows. Let $m(x) = min_{\mathbb{Q}}(\theta)$ be the minimal polynomial of θ over $\mathbb{Q}$ and $\overline{m(x)}$ the polynomial obtained from $m(x)$ by reduction modulo $\mathbb{Z}_3[x]$. If $f = 1$, then $\overline{m(x)}$ is written as the product of irreducible polynomials of degree 1 in $\mathbb{Z}_3[x]$ and there are only three possibilities for these polynomials $\overline{m_{i+1}(x)} = \overline{x - i}$, for $i = 0, 1, 2$. If $\overline{m(x)} = \overline{m_1(x)}\,\overline{m_2(x)}\,\overline{m_3(x)}$, then $3\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3$. Since $f = 1$, it follows that $N_{\mathbb{K}}(\mathcal{Q}_1) = N_{\mathbb{K}}(\mathcal{Q}_2) = N_{\mathbb{K}}(\mathcal{Q}_3) = 3^1 = 3$. Thus, $N_{\mathbb{K}}(3\mathcal{O}_{\mathbb{K}}) = 3^3$ and this is possible only if $[\mathbb{K} : \mathbb{Q}] = 3$. Similarly, if $\overline{m(x)} = \overline{m_{i+1}(x)}$, for some $i = 0, 1, 2$, then $[\mathbb{K} : \mathbb{Q}] = 1$, and if $\overline{m(x)} = \overline{m_{i+1}(x)}\,\overline{m_{j+1}(x)}$, for some $i, j = 0, 1, 2$, with $i \neq j$, then $[\mathbb{K} : \mathbb{Q}] = 2$. Therefore, $f > 1$. Since $e\,f\,g = 6$, it follows that f divides 6. □

Example 4.8. Note that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = 6$ if and only if $m = 7, 9, 14$ and 18, and $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = 6$ if and only if $m = 13, 21, 26, 28, 36$ and 42. Set $\mathbb{K}_1 = \mathbb{Q}(\zeta_7) = \mathbb{Q}(\zeta_{14})$, $\mathbb{K}_2 = \mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1}) = \mathbb{Q}(\zeta_{26} + \zeta_{26}^{-1})$, $\mathbb{K}_3 = \mathbb{Q}(\zeta_{21} + \zeta_{21}^{-1}) = \mathbb{Q}(\zeta_{42} + \zeta_{42}^{-1})$ and $\mathbb{K}_4 = \mathbb{Q}(\zeta_{28} + \zeta_{28}^{-1})$. A straightforward computation shows that $d_{\mathbb{K}_1} = -7^5$, $d_{\mathbb{K}_2} = 13^5$, $d_{\mathbb{K}_3} = 3^3 7^5$ and $d_{\mathbb{K}_4} = 2^6 7^5$. According to Proposition 4.7, it follows that it is not possible to obtain a rotated E_6-lattice, scaled by $\sqrt{c}$ with $c \in \mathbb{Z}$, via a fractional ideal of $\mathcal{O}_{\mathbb{K}_i}$ for $i = 1, 2, 4$. For $i = 3$, we have that $3\mathcal{O}_{\mathbb{K}_2} = \mathcal{P}^2$, where $\mathcal{P}$ is a prime ideal of $\mathcal{O}_{\mathbb{K}_2}$ and $f(\mathcal{P}|3) = 3$. Following the notation of Proposition 3.9, let $p = 3$. Suppose that there exists a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}_2}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated E_6-lattice, scaled by $\sqrt{c}$ with $c > 0$ an integer. Then, $\det(\Lambda) = 3c^6$, where $c = 3^a b$ with $a \geq 0$ an integer and $b \geq 1$ an integer such that $3 \nmid b$. So, $\det(\Lambda) = 3^{1+6a}b^6$. Since $f = 3$ does not divide $(1 + 6a - 3)$, we have a contradiction.

A rotated E_6-lattice via an ideal of $\mathbb{Z}[\zeta_{36} + \zeta_{36}^{-1}]$: Let $\mathbb{K} = \mathbb{Q}(\zeta_{36} + \zeta_{36}^{-1})$ and $e_i = \zeta_{36}^i + \zeta_{36}^{-i}$. If $\alpha = e_1^4$ and $\mathcal{I} = \langle 1 + e_1 + e_1^3 \rangle$, then the lattice $\Lambda = \frac{1}{\sqrt{36}}\sigma_\alpha(\mathcal{I})$ is a rotated E_6-lattice and $\sqrt[6]{d_{p,rel}(\Lambda)} = 0.24037$. In fact, since $d_{\mathbb{K}} = 2^6 3^9$ consider the factorizations $3\mathcal{O}_{\mathbb{K}} = \mathcal{Q}^6$, where $\mathcal{Q} = \langle e_1 \rangle$ with $N_{\mathbb{K}}(\mathcal{Q}) = 3$ and $2\mathcal{O}_{\mathbb{K}} = \mathcal{P}^2$, where $\mathcal{P} = \langle 1 + e_1 + e_1^3 \rangle$ and $N_{\mathbb{K}}(\mathcal{P}) = 2^3$. Taking $\alpha = e_1^4$, $\mathcal{I} = \mathcal{P}$ and $\theta = 1 + e_1 + e_1^3$, we have that α is totally positive, $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = 3^4$, $N_{\mathbb{K}}(\mathcal{I}) = 2^3$ and a straightforward computation shows that a Gram matrix for $\frac{1}{6}\sigma_\alpha(\mathcal{I})$, associated with the $\mathbb{Z}$-basis $\{\theta e_1, \ldots, \theta e_6\}$ of $\mathcal{I}$ has only even numbers in its diagonal. Therefore, $\frac{1}{6}\sigma_\alpha(\mathcal{I})$ is an even lattice with determinant 3. Its minimum squared Euclidean norm must be 2, otherwise we would have a lattice denser than E_6 in dimension 6. Since E_6 is, up to congruence, the only even lattice with minimum squared Euclidean norm 2 and determinant 3 in dimension 6, it follows that $\frac{1}{6}\sigma_\alpha(\mathcal{I})$ is a rotated E_6-lattice. Since the minimum Euclidean norm of $\frac{1}{6}\sigma_\alpha(\mathcal{I})$ is $\sqrt{2}$, its relative minimum product distance is $d_{p,rel}(\Lambda) = \frac{1}{6^6}\frac{1}{(\sqrt{2})^6}\sqrt{2^6 3^4} = \frac{1}{2^6 3^4}$ and then $\sqrt[6]{d_{p,rel}(\Lambda)} = 0.24037$.

Example 4.9. Let $\mathbb{K} = \mathbb{Q}(\zeta_{12}+\zeta_{12}^{-1})\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ the compositum of the fields $\mathbb{Q}(\zeta_{12}+\zeta_{12}^{-1}) = \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\zeta_7+\zeta_7^{-1})$. We have that $d_{\mathbb{K}} = (2^2 3)^3(7^2)^2 = 2^6 3^3 7^4$. Consider the factorizations $3\mathbb{Z}[\zeta_7+\zeta_7^{-1}] = \mathcal{P}_1$ where $\mathcal{P}_1 = \langle 3, 2+a_1+a_1^2+a_1^3\rangle$ with $a_1 = \zeta_7+\zeta_7^{-1}$ and $3\mathcal{O}_{\mathbb{K}} = \mathcal{P}_2^2$, where $\mathcal{P}_2$ is the prime ideal of $\mathcal{O}_{\mathbb{K}}$ such that $\mathcal{P}_2 \cap \mathbb{Z}[\zeta_7+\zeta_7^{-1}] = \mathcal{P}_1$ and $f(\mathcal{P}_2|3) = 3$. Suppose that there exists a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated E_6-lattice, scaled by $\sqrt{c}$ with $c > 0$ an integer. Then, $\det(\Lambda) = 3c^6$, where $c = 3^r s$ with $r \geq 0$ an integer and $s \geq 1$ an integer such that $3 \nmid s$. So, $\det(\Lambda) = 3^{1+6r}s^6$. Since 3 does not divide $(1+6r-3)$, it follows that there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ and a totally positive element α such that $\sigma_\alpha(\mathcal{I})$ is a rotated and scaled E_6-lattice.

4.4. Rotated E_7-lattice

The 7-dimensional densest lattice E_7 is an even lattice with minimum squared Euclidean norm 2 and $\det(E_7) = 2$. A basis for $\sqrt{2}E_7$ in dimension 7 is given by the vectors $(2,0,0,0,0,0,0)$, $(0,2,0,0,0,0,0)$, $(0,0,2,0,0,0,0)$, $(0,0,0,2,0,0,0)$, $(1,1,1,0,1,0,0)$, $(0,1,1,1,0,1,0)$ and $(0,0,1,1,1,0,1)$.

In Proposition 4.10, we present a necessary condition for constructing a rotated E_7-lattice via a fractional ideal in a Galois extension. In Proposition 4.12, we show that there exist infinitely many number fields such that it is possible to obtain a scaled and rotated E_7-lattice via free $\mathbb{Z}$-modules of rank 7.

Proposition 4.10. *Let $\mathbb{K} = \mathbb{Q}(\theta)$ be a Galois extension such that $[\mathbb{K}:\mathbb{Q}] = 7$. Let $2\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g}\mathcal{Q}_i^e$, where $\mathcal{Q}_i$'s are prime ideals of $\mathcal{O}_{\mathbb{K}}$, $e(\mathcal{Q}_i|2) = e$ and $f(\mathcal{Q}_i|2) = f$, for all $i = 1,\dots,g$. If 2 does not divide $d_{\mathbb{K}}$, then there does not exist any fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated E_7-lattice, scaled by $\sqrt{c}$ with $c \in \mathbb{Z}$, for any $\alpha \in \mathbb{K}$ totally positive.*

Proof. Suppose that there exists a fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\Lambda = \sigma_\alpha(\mathcal{I})$ is a rotated E_7-lattice, scaled by $\sqrt{c}$ with $c \geq 0$ an integer. Thus, $\det(\Lambda) = 2c^7$, where $c = 2^a b$ with $a \geq 0$ an integer and $b \geq 1$ an integer such that $2 \nmid b$. So, $\det(\Lambda) = 2^{1+7a}b^7$. By Proposition 3.9, it follows that f must divide $(1+7a-r)$. Since 2 does not divide $d_{\mathbb{K}}$, it follows that $r = 0$. We show next that $f = 7$ what implies that f does not divide $(m-r) = (1+7a-0) = 1+7a$ and the result follows. Let $m(x) = min_{\mathbb{Q}}(\theta)$ be the minimal polynomial of θ over $\mathbb{Q}$ and $\overline{m(x)}$ the polynomial obtained from $m(x)$ by reduction modulo $\mathbb{Z}_2[x]$. If $f = 1$, then $\overline{m(x)}$ is written as the product of irreducible polynomials of degree 1 in $\mathbb{Z}_2[x]$ and there are only two possibilities for these polynomials:

$\overline{m_1(x)} = \bar{x}$ and $\overline{m_2(x)} = \overline{x-1}$. If $\overline{m(x)} = \overline{m_1(x)}\,\overline{m_2(x)}$, then $2\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1\mathcal{Q}_2$. Since $f = 1$, it follows that $N_{\mathbb{K}}(\mathcal{Q}_1) = N_{\mathbb{K}}(\mathcal{Q}_2) = 2^1 = 2$. Thus, $N_{\mathbb{K}}(2\mathcal{O}_{\mathbb{K}}) = 2^2$ and this is possible only if $[\mathbb{K} : \mathbb{Q}] = 2$. Similarly, if $\overline{m(x)} = \overline{m_1(x)}$ or $\overline{m(x)} = \overline{m_2(x)}$, we get $[\mathbb{K} : \mathbb{Q}] = 1$. Since $e\,f\,g = 7$, it follows that $f = 7$. □

Example 4.11. Let $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ be a Galois extension of degree 7 and m odd. Since $d_{\mathbb{K}}$ is odd, it is not possible to get a rotated E_7-lattice via a fractional ideal of $\mathcal{O}_{\mathbb{K}}$.

Since $\sqrt{2}\,E_7$ is an integer lattice, using Remark 3.10 and the cyclic construction of [6], the next proposition can be derived.

Proposition 4.12. *There exist infinitely many prime numbers p and number fields $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and a full diversity rotated $\sqrt{2}E_7$-lattice can be obtained via a twisted embedding and a free $\mathbb{Z}$-module of rank 7 contained in $\mathcal{O}_{\mathbb{K}}$.*

Remark 4.13. Let p be a prime number and $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ such that $[\mathbb{K} : \mathbb{Q}] = 7$. Since $d_{\mathbb{K}} = p^6$, it follows that in this case the minimum value of $d_{\mathbb{K}}$ is achieved when $p = 29$. Using the cyclic construction of [6, Section V], it follows that there exists a rotated $\mathbb{Z}^7$-lattice, $Rot(\mathbb{Z}^7)$, via a subfield $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{29} + \zeta_{29}^{-1})$ satisfying $\sqrt[7]{d_{p,rel}(Rot(\mathbb{Z}^7))} = 0.23618$. Using this rotated $\mathbb{Z}^7$-lattice, we can obtain a rotated $\sqrt{2}E_7$-lattice, $Rot(\sqrt{2}E_7)$, such that $Rot(\sqrt{2}E_7) \subseteq Rot(\mathbb{Z}^7)$. Since the minimum squared Euclidean norm of E_7 is 2, it follows that $\sqrt[7]{d_{p,rel}(Rot(\sqrt{2}E_7))} \geq \sqrt[7]{\left(\frac{1}{\sqrt{2}^7}\frac{1}{\sqrt{2}^7}(0.23618)^7\right)} = 0.11809$.

4.5. Rotated E_8-lattice

The 8-dimensional densest lattice is defined, in its standard form, as $E_8 = \{(x_1, \ldots, x_8)$ such that $x_i \in \mathbb{Z}$ for all i or $x_i \in \mathbb{Z} + 1/2$ for all i and $\sum_{i=1}^{8} x_i$ is even$\}$. The lattice E_8 is an even unimodular lattice with minimum squared Euclidean norm 2.

Algebraic constructions of rotated E_8-lattices were presented in [3, p. 77] via the cyclotomic fields $\mathbb{Q}(\zeta_{15})$, $\mathbb{Q}(\zeta_{20})$ and $\mathbb{Q}(\zeta_{24})$ and in [11, p. 52] via $\mathbb{Q}(\zeta_{20})$ and $\mathbb{Q}(\zeta_{24})$. In [15] it was shown that there exist infinitely many subfields $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{pq})$, with p, q distinct primes, such that it is possible to obtain rotated E_8-lattices via the canonical embedding applied to an ideal of $\mathcal{O}_{\mathbb{K}}$. All these rotated E_8-lattices have diversity 4. In [8, Section 3] it was presented a full diversity rotated E_8-lattice via $\mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$. In what follows we discuss some possibilities for constructing a full diversity rotated E_8-lattice and present constructions of E_8 via a principal ideal of $\mathbb{Z}[\zeta_{60} + \zeta_{60}^{-1}]$ and via a free $\mathbb{Z}$-module in $\mathbb{Z}[\zeta_{60} + \zeta_{60}^{-1}]$ that is not an ideal. In both cases we obtain the relative minimum product distance.

Note that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = 8$ if and only if $m = 15, 16, 20, 24$ and 30 and $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = 8$ if and only if $m = 17, 32, 34, 40, 48$ and 60. Reordering the last list from the minimum to the maximum discriminant we have $m = 60, 17, 40, 48$ and 32.

A rotated $\boldsymbol{E_8}$-lattice via an ideal of $\boldsymbol{\mathbb{Z}[\zeta_{60}+\zeta_{60}^{-1}]}$: Let $\mathbb{K} = \mathbb{Q}(\zeta_{60}+\zeta_{60}^{-1})$ and $e_i = \zeta_{60}^{i}+\zeta_{60}^{-i}$ for all $i \in \mathbb{N}$. If $\alpha = (e_1+e_5)e_5$ and $\mathcal{I} = \langle e_1+e_4+e_6\rangle$, then the lattice $\Lambda = \frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{I})$ is a rotated E_8-lattice and $\sqrt[8]{d_{p,rel}(\Lambda)} = 0.20776$. In fact, since $d_{\mathbb{K}} = 2^8 3^4 5^6$, consider the factorizations $2\mathcal{O}_{\mathbb{K}} = \mathcal{P}^2$, where $\mathcal{P} = \left\langle 2, 1+e_1^3+e_1^4\right\rangle = \langle e_1+e_4+e_6\rangle$ and $N_{\mathbb{K}}(\mathcal{P}) = 2^4$, $3\mathcal{O}_{\mathbb{K}} = \mathcal{Q}^2$, where $\mathcal{Q} = \left\langle 3, 2+e_1^2+e_1^4\right\rangle = \langle e_5\rangle$ and $N_{\mathbb{K}}(\mathcal{Q}) = 3^4$, and $5\mathcal{O}_{\mathbb{K}} = \mathcal{R}^4$, where $\mathcal{R} = \left\langle 5, 2+e_1^2\right\rangle = \langle e_1+e_5\rangle$ and $N_{\mathbb{K}}(\mathcal{R}) = 5^2$. Taking $\alpha = (e_1+e_5)e_5$ and $\mathcal{I} = \mathcal{P}$, it follows that α is totally positive, $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = 5^2 3^4$ and $N_{\mathbb{K}}(\mathcal{I}) = 2^4$. If $\theta = e_1+e_4+e_6$, a straightforward calculation shows that the Gram matrix for $\frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{I})$, associated with the $\mathbb{Z}$-basis $\{\theta e_1, \ldots, \theta e_8\}$ of $\mathcal{I}$, has only even numbers in its diagonal. Therefore, $\frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{I})$ is an even unimodular lattice. Since E_8 is, up to congruence, the only even unimodular lattice with minimum squared Euclidean norm 2 in dimension 8, it follows that $\frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{I})$ is a rotated E_8-lattice. Since the minimum Euclidean norm of $\frac{1}{\sqrt{60}}\sigma_\alpha(\mathcal{I})$ is $\sqrt{2}$, it follows that its relative minimum product distance satisfies $\sqrt[8]{d_{p,rel}(\Lambda)} = \sqrt[8]{\frac{1}{\sqrt{60}^8}\frac{1}{\sqrt{2}^8}\sqrt{2^8 3^4 5^2}} = 0.20776$.

A rotated $\boldsymbol{E_8}$-lattice via a free $\boldsymbol{\mathbb{Z}}$-module in $\boldsymbol{\mathbb{Z}[\zeta_{60}+\zeta_{60}^{-1}]}$: Let $\mathbb{K} = \mathbb{Q}(\zeta_{60}+\zeta_{60}^{-1})$ and $e_i = \zeta_{60}^{i}+\zeta_{60}^{-i}$ for all $i \in \mathbb{N}$. If $\alpha = (e_1+e_5)e_5$ and $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$, then the lattice $\Lambda = \frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is a rotated $\mathbb{Z}^8$-lattice and $\sqrt[8]{d_{p,rel}(\Lambda)} = 0.29382$. In fact, a straightforward calculation shows that Λ is an odd unimodular lattice in dimension 8. Therefore, $\frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is a rotated $\mathbb{Z}^8$-lattice. Since $2E_8$ is a sublattice of $\mathbb{Z}^8$, using Remark 3.10 we obtain the $\mathbb{Z}$-module $\mathcal{J}$ with $\mathbb{Z}$-basis $\{2e_1, 2e_2+2e_5, e_3+e_5+e_6+e_7+e_8, 2e_4, 4e_5, 2e_6, 2e_7, 2e_8\}$ such that $\Lambda_{\circledast} = \frac{1}{\sqrt{30}}\sigma_\alpha(\mathcal{J})$ is a rotated $2E_8$-lattice, i.e., $\Lambda_* = \frac{1}{\sqrt{120}}\sigma_\alpha(\mathcal{J})$ is a rotated E_8-lattice. The $\mathbb{Z}$-module $\mathcal{J}$ is not an ideal of $\mathcal{O}_{\mathbb{K}}$. In fact, if $\mathcal{J}$ were an ideal we would have $(2e_1)e_2 = 2e_3+2e_1 \in \mathcal{J}$ and then $(2e_3+2e_1)-2e_1 = 2e_3 \in \mathcal{J}$. Moreover, $2(e_3+e_5+e_6+e_7+e_8)-2e_3-2e_6-2e_7-2e_8 = 2e_5 \in \mathcal{J}$. Therefore, $\{2e_1, 2e_2, 2e_3, 2e_4, 2e_5, 2e_6, 2e_7, 2e_8\}$ would be a $\mathbb{Z}$-basis of a free $\mathbb{Z}$-module $\mathcal{J}_1 \subseteq \mathcal{J}$. However, $\frac{1}{\sqrt{120}}\sigma_\alpha(\mathcal{J}_1)$ is a rotated $\mathbb{Z}^8$-lattice. Since $\mathbb{Z}^8$ is not a sublattice of E_8, it follows that $\mathcal{J}$ is not an ideal of $\mathcal{O}_{\mathbb{K}}$. Since the minimum Euclidean norm of E_8 is $\sqrt{2}$ and $\min_{0\neq y\in\mathcal{J}} |N_{\mathbb{K}|\mathbb{Q}}(y)| = 2^4 = N_{\mathbb{K}|\mathbb{Q}}(e_3+e_5+e_6+e_7+e_8)$, the relative minimum product distance of Λ_* satisfies $\sqrt[8]{d_{p,rel}(\Lambda_*)} = \sqrt[8]{\frac{1}{\sqrt{120}^8}\frac{1}{\sqrt{2}^8}\sqrt{(3^4\,5^2)2^4}} = 0.146913$.

Example 4.14. For $m = 16$ if we consider $\mathcal{I} = \mathbb{Z}[\zeta_{16}]$ and $\alpha = 1$ we obtain a rotated $\mathbb{Z}^8$-lattice. We also get rotated $\mathbb{Z}^8$-lattices for $m = 17, 32, 40$ and 48 when we consider $\mathcal{I} = \mathbb{Z}[\zeta_m+\zeta_m^{-1}]$ and $\alpha = 2-(\zeta_{17}+\zeta_{17}^{-1}), 2-(\zeta_{32}+\zeta_{32}^{-1}), (\zeta_{40}+\zeta_{40}^{-1})(\zeta_{40}^{6}+\zeta_{40}^{-6})(\zeta_{40}^{7}+\zeta_{40}^{-7})$ and $(\zeta_{48}+\zeta_{48}^{-1})(\zeta_{48}^{4}+\zeta_{48}^{-4})(\zeta_{48}^{19}+\zeta_{48}^{-19})$, respectively. In such cases we can use Remark 3.10 to obtain rotated $2E_8$-lattices via free $\mathbb{Z}$-modules of rank 8.

4.6. Rotated K_{12}-lattice

The Coxeter–Todd lattice K_{12} is a 12-dimensional even lattice with determinant $\det(K_{12}) = 3^6$ and minimum squared Euclidean norm 4.

Algebraic constructions of rotated K_{12}-lattices with diversity 6 were presented in [3, p. 78] and [9, p. 513] via $\mathbb{Q}(\zeta_{21})$. In what follows we discuss some possibilities for constructing a full diversity rotated K_{12}-lattice with the same minimum product distance of the one constructed in [8, Section 3].

Example 4.15. Note that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = 12$ if and only if $m = 13, 21, 26, 28, 36, 42$ and $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = 12$ if and only if $m = 35, 39, 45, 52, 56, 70, 72, 78, 84$ and 90. Let $\mathbb{K}_1 = \mathbb{Q}(\zeta_{35} + \zeta_{35}^{-1}) = \mathbb{Q}(\zeta_{70} + \zeta_{70}^{-1})$, $\mathbb{K}_2 = \mathbb{Q}(\zeta_{13}) = \mathbb{Q}(\zeta_{26})$ and $\mathbb{K}_3 = \mathbb{Q}(\zeta_{28})$. A straightforward computation shows that $d_{\mathbb{K}_1} = 5^9 7^{10}$, $3\mathcal{O}_{\mathbb{K}_1} = \mathcal{Q}$ with $f(\mathcal{Q}|3) = 12$, $d_{\mathbb{K}_2} = 13^{13}$, $3\mathcal{O}_{\mathbb{K}_2} = \mathcal{R}$ with $f(\mathcal{R}|3) = 12$ and $d_{\mathbb{K}_3} = 2^{12} 7^{10}$, $3\mathcal{O}_{\mathbb{K}_3} = \mathcal{S}$ with $f(\mathcal{S}|3) = 12$. By Proposition 3.7, it follows that there does not exist any rotated K_{12}-lattice via a fractional ideal of $\mathcal{O}_{\mathbb{K}_i}$, for $i = 1, 2, 3$, since $f(\mathcal{Q}|3) = f(\mathcal{R}|3) = f(\mathcal{S}|3)$ does not divide 3^6.

Considering only the values of m such that $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = 12$ and reordering the list from the minimum to the maximum discriminant we have $m = 35, 45, 84, 39, 56,$ 72 and 52.

A rotated K_{12}-lattice via an ideal of $\mathbb{Z}[\zeta_{84} + \zeta_{84}^{-1}]$: Let $\mathbb{K} = \mathbb{Q}(\zeta_{84} + \zeta_{84}^{-1})$ and $e_i = \zeta_{84}^i + \zeta_{84}^{-i}$ for all $i \in \mathbb{N}$. If $\alpha = e_3 e_{20} e_{19} e_2$ and $\mathcal{I} = \langle 1 + e_2 + e_3 + e_5 + e_6 \rangle$, then the lattice $\Lambda = \frac{1}{\sqrt{28}} \sigma_\alpha(\mathcal{I})$ is a rotated K_{12}-lattice and $\sqrt[12]{d_{p,rel}(\Lambda)} = 0.15172$. In fact, we have that $d_{\mathbb{K}} = 2^{12} 3^6 7^{10}$, $2\mathcal{O}_{\mathbb{K}} = \mathcal{P}^2$, where $\mathcal{P} = \langle 2, 1 + e_1^5 + e_1^6 \rangle = \langle 1 + e_2 + e_3 + e_5 + e_6 \rangle$ and $N_{\mathbb{K}}(\mathcal{P}) = 2^6$ and $7\mathcal{O}_{\mathbb{K}} = \mathcal{S}^6$, where $\mathcal{S} = \langle 7, 4 + e_1^2 \rangle = \langle e_3 \rangle$ and $N_{\mathbb{K}}(\mathcal{S}) = 7^2$. Taking $\alpha = e_3 e_{20} e_{19} e_2$ and $\mathcal{I} = \mathcal{P}$, it follows that $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = 7^2$ and α is totally positive. If $\theta = 1 + e_2 + e_3 + e_5 + e_6$, then a Gram matrix for $\frac{1}{\sqrt{28}} \sigma_\alpha(\mathcal{I})$, associated with the $\mathbb{Z}$-basis $\{\theta e_1, \ldots, \theta e_{12}\}$ of $\mathcal{I}$, has only even numbers in its diagonal. Therefore, $\frac{1}{\sqrt{28}} \sigma_\alpha(\mathcal{I})$ is an even lattice with determinant 3^6. Moreover, using a full search algorithm in the software Mathematica we shown that its minimum squared Euclidean norm must be 4. Since K_{12} is up to equivalence the only even lattice with minimum Euclidean norm 2 and determinant 3^6 in dimension 12 [3], it follows that $\frac{1}{\sqrt{28}} \sigma_\alpha(\mathcal{I})$ is a rotated K_{12}-lattice. Since the minimum Euclidean norm of $\frac{1}{\sqrt{28}} \sigma_\alpha(\mathcal{I})$ is 2, its relative minimum product distance satisfies $\sqrt[12]{d_{p,rel}(\Lambda)} = \sqrt[12]{\frac{1}{\sqrt{28}^{12}} \frac{1}{2^{12}} \sqrt{2^{12} 7^2}} = 0.15172$.

4.7. Rotated Λ_{24}-lattice

The Leech lattice Λ_{24} is, up to congruence, the only even unimodular lattice in the 24-dimensional Euclidean space with minimum squared Euclidean norm 4 (cf. [13]).

Algebraic constructions of the Leech lattice were presented in [11] via $\mathbb{Q}(\zeta_{39})$ and in [3, p. 79] via $\mathbb{Q}(\zeta_{39})$ and $\mathbb{Q}(\zeta_{35})$. In [3] it was also stated in Proposition 3.4 that the Leech lattice can be obtained from $\mathbb{Q}(\zeta_m)$ if only if $m = 35, 39, 52, 56, 70, 78$ and 84. In [8, Section 3] it was presented a construction of a full diversity rotated Λ_{24}-lattice via $\mathbb{Q}(\zeta_{140} + \zeta_{140}^{-1})$. In what follows we discuss some possibilities for constructing a full diversity rotated Leech lattice via a principal ideal of $\mathbb{Q}(\zeta_m+\zeta_m^{-1})$, present a construction for $m=140$, and obtain its minimum product distance. We also present a construction of Λ_{24} via a free $\mathbb{Z}$-module in $\mathbb{Z}[\zeta_{180}+\zeta_{180}^{-1}]$.

Note that $[\mathbb{Q}(\zeta_m+\zeta_m^{-1}):\mathbb{Q}]=24$ if and only if $m=65,104,105,112,130,140,144,156,168,180$ and 210. This last list when reordered from the minimum to the maximum discriminant is $105,140,180,168,65,156,112,144$ and 104. If we could construct a Leech lattice for the case $m=105$ via a principal ideal of $\mathbb{Z}[\zeta_{105}+\zeta_{105}^{-1}]$, we would have the greater minimum product distance possible among the constructions obtained via the number fields in this list and principal ideals. However, we could not get the Leech lattice for $m=105$ using an algorithm approach similar to the one described next for $m=140$.

A rotated Λ_{24}-lattice via an ideal of $\mathbb{Z}[\zeta_{140}+\zeta_{140}^{-1}]$: Let $\mathbb{K}=\mathbb{Q}(\zeta_{140}+\zeta_{140}^{-1})$ and $e_i=\zeta_{140}^i+\zeta_{140}^{-i}$ for all $i\in\mathbb{N}$. If $\alpha=e_5e_7(e_1e_4e_{16}e_{23})$ and $\mathcal{I}=\langle 1+e_7+e_{14}\rangle$, then the lattice $\Lambda=\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ is a rotated Λ_{24}-lattice and $\sqrt[24]{d_{p,rel}(\Lambda)}=0.08594$. In fact, we have that $d_{\mathbb{K}}=2^{24}5^{18}7^{20}$, $2\mathcal{O}_{\mathbb{K}}=\mathcal{P}^2$, where $\mathcal{P}=\langle 2,1+e_1^5+e_1^6+e_1^7+e_1^9+e_1^{11}+e_1^{12}\rangle=\langle 1+e_7+e_{14}\rangle$ and $N_{\mathbb{K}}(\mathcal{P})=2^{12}$, $5\mathcal{O}_{\mathbb{K}}=\mathcal{S}^4$, where $\mathcal{S}=\langle e_7\rangle$ and $N_{\mathbb{K}}(\mathcal{S})=5^6$ and $7\mathcal{O}_{\mathbb{K}}=\mathcal{R}^6$, where $\mathcal{R}=\langle e_5\rangle$ and $N_{\mathbb{K}}(\mathcal{R})=7^4$. Taking $\alpha=e_5e_7(e_1e_4e_{16}e_{23})$ and $\mathcal{I}=\mathcal{P}$, it follows that $N_{\mathbb{K}|\mathbb{Q}}(\alpha)=5^67^4$ and α is totally positive. If $\theta=1+e_7+e_{14}$, then a Gram matrix for $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$, associated with the $\mathbb{Z}$-basis $\{\theta e_1,\dots,\theta e_{24}\}$ of $\mathcal{I}$, has only even integer numbers in its diagonal. From the Gram matrix above, it follows that $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ is an even unimodular lattice. To show that this lattice is in fact the Leech lattice Λ_{24} a fundamental result is that Λ_{24} is, up to congruence, the unique even unimodular lattice with minimum squared Euclidean norm 4 in dimension 24 [13]. In order to show that the minimum squared Euclidean norm of $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ is not 2 we implement an algorithm in the Mathematica software following the ideas of [14] (which has inspired the so called Sphere Decoder process [19,24]). Since $\frac{1}{\sqrt{140}}\sigma_\alpha(\mathcal{I})$ is an even unimodular lattice and does not have vectors with minimum squared Euclidean norm 2, it follows that this lattice is a rotated Λ_{24}-lattice. Its relative minimum product distance is $\sqrt[24]{d_{p,rel}(\Lambda)}=\sqrt[24]{\frac{1}{\sqrt{140}^{24}}\frac{1}{\sqrt{4}^{24}}\sqrt{2^{24}5^67^4}}=0.08594$.

A rotated Λ_{24}-lattice via a free $\mathbb{Z}$-module in $\mathbb{Z}[\zeta_{180}+\zeta_{180}^{-1}]$: Let $\mathbb{K}=\mathbb{Q}(\zeta_{180}+\zeta_{180}^{-1})$ and $e_i=\zeta_{180}^i+\zeta_{180}^{-i}$ for all $i\in\mathbb{N}$. If $\alpha=(e_1+e_5+e_9)^3(-e_1-e_{17})(1-4e_{17}^2+e_{17}^4)$ and $\mathcal{I}=\langle -1-e_{15}+e_{22}+e_{23}\rangle$, then the lattice $\Lambda=\frac{1}{\sqrt{180}}\sigma_\alpha(\mathcal{I})$ is a rotated $E_8\oplus E_8\oplus E_8$-lattice and $\sqrt[24]{d_{p,rel}(\Lambda)}=0.119954$. In fact, we have that $d_{\mathbb{K}}=2^{24}3^{36}5^{18}$, $2\mathcal{O}_{\mathbb{K}}=\mathcal{P}^2$, where $\mathcal{P}=\langle -1-e_{15}+e_{22}+e_{23}\rangle$ and $N_{\mathbb{K}}(\mathcal{P})=2^{12}$, $5\mathcal{O}_{\mathbb{K}}=\mathcal{S}^4$, where $\mathcal{S}=\langle e_1+e_{17}\rangle$ and $N_{\mathbb{K}}(\mathcal{S})=5^6$, and $3\mathcal{O}_{\mathbb{K}}=\mathcal{R}^6$, where $\mathcal{R}=\langle e_1+e_5+e_9\rangle$ and $N_{\mathbb{K}}(\mathcal{R})=3^4$. Taking $\alpha=(e_1+e_5+e_9)^3(-e_1-e_{17})(1-4e_{17}^2+e_{17}^4)$, it follows that α is totally positive and $N_{\mathbb{K}|\mathbb{Q}}(\alpha)=5^63^{12}$. Let $\mathcal{I}=\mathcal{P}$ and $\theta=-1-e_{15}+e_{22}+e_{23}$. The Gram matrix for $\frac{1}{\sqrt{180}}\sigma_\alpha(\mathcal{I})$, associated with the $\mathbb{Z}$-basis $\{\theta e_1,\dots,\theta e_{24}\}$ of $\mathcal{I}$, has only even numbers in its diagonal. Using the LLL algorithm for reduction of basis we show that $\frac{1}{\sqrt{180}}\sigma_\alpha(\mathcal{I})$ is a rotated $E_8 \oplus E_8 \oplus E_8$-lattice. Since the minimum Euclidean norm of $E_8 \oplus E_8 \oplus E_8$ is $\sqrt{2}$, it follows that $\sqrt[24]{d_{p,rel}(\Lambda)} = \sqrt[24]{\frac{1}{\sqrt{180}^{24}} \frac{1}{\sqrt{2}^{24}} \sqrt{2^{24} 5^6 3^{12}}} = 0.119954$. Using the fact that $\sqrt{2}\Lambda_{24}$ is a sublattice of $E_8 \oplus E_8 \oplus E_8$ we found the $\mathbb{Z}$-module $\mathcal{J} \subseteq \mathcal{I}$ with $\mathbb{Z}$-basis $\{\theta(e_1 + e_{16} + e_{17} + e_{19} + e_{21} + e_{22} + e_{23}), \theta(e_2 + e_{11} + e_{16} + e_{18} + e_{19} + e_{20} + e_{23}), \theta(e_3 + e_{16} + e_{18} + e_{19} + e_{21} + e_{24}), \theta(e_4 + e_{11} + e_{12} + e_{15} + e_{17} + e_{19} + e_{23}), \theta(e_5 + e_{11} + e_{16} + e_{19} + e_{21} + e_{24}), \theta(e_6 + e_{12} + e_{15} + e_{17} + e_{19} + e_{20} + e_{22} + e_{24}), \theta(e_7 + e_{11} + e_{12} + e_{15} + e_{16} + e_{17} + e_{19} + e_{23} + e_{24}), \theta(e_8 + e_{16} + e_{21} + e_{23}), \theta(e_9 + e_{12} + e_{15} + e_{16} + e_{17} + e_{18} + e_{19} + e_{21} + e_{22} + e_{24}), \theta(e_{10} + e_{12} + e_{15} + e_{17} + e_{19} + e_{21} + e_{23} + e_{24}), 2\theta e_{11}, 2\theta e_{12}, \theta(e_{13} + e_{15} + e_{17} + e_{20} + e_{21} + e_{22}), \theta(e_{14} + e_{15} + e_{17} + e_{18} + e_{19} + e_{20} + e_{21} + e_{22} + e_{23}), 2\theta e_{15}, 2\theta e_{16}, 2\theta e_{17}, 2\theta e_{18}, 2\theta e_{19}, 2\theta e_{20}, 2\theta e_{21}, 2\theta e_{22}, 2\theta e_{23}, 2\theta e_{24}\}$. The Gram matrix for the lattice $\Lambda_1 = \frac{1}{\sqrt{360}}\sigma_\alpha(\mathcal{J})$, associated with this $\mathbb{Z}$-basis of $\mathcal{J}$ has only even integers in its diagonal. Using an algorithm in the Mathematica software we show that the minimum squared Euclidean norm of Λ_1 is 4. Then, $\frac{1}{\sqrt{360}}\sigma_\alpha(\mathcal{J})$ is a Leech lattice. Since $N_{\mathbb{K}|\mathbb{Q}}(\theta) = 2^{12}$, it follows that $\min_{0 \neq y \in \mathcal{J}} |N_{\mathbb{K}|\mathbb{Q}}(y)| \geq 2^{12}$. Now, $\boldsymbol{y} = -1 + 2e_1 + e_2 + 2e_3 + 2e_4 + 2e_5 + 2e_8 + 3e_{10} + e_{11} - 2e_{13} - e_{14} - e_{15} - e_{17} - 3e_{19} - 3e_{20} - 2e_{21} - 4e_{22} - e_{23} \in \mathcal{J}$ and $|N_{\mathbb{K}|\mathbb{Q}}(y)| = 2^{12}$. Therefore, $\sqrt[24]{d_{p,rel}(\Lambda_1)} = \sqrt[24]{\frac{1}{\sqrt{360}^{24}} \frac{1}{2^{24}} \sqrt{5^6 3^4 2^{12}}} = 0.0599771$.

5. Conclusion

In this section, we present a comparison between relative minimum product distance versus density. As mentioned in the Introduction, density and minimum product distance are lattice parameters which are associated with the efficiency in the signal transmission over Gaussian and Rayleigh fading channels, respectively.

The next Table 1 shows a comparison between the best known normalized product distance of rotated $\mathbb{Z}^n$-lattices and of the densest lattices Λ in dimensions 2 to 8, 12 and 24. The center density δ of these lattices are also displayed.

The relative minimum product distance of the rotated A_2-lattice obtained here is the maximum possible, as stated in Subsection 4.1. A broader question to be investigated is if algebraic constructions of lattices, as the ones approached here, can provide the greatest possible relative minimum product distance for rotated densest lattices in other dimensions.

Table 1
Relative minimum product distance versus center density (from [6,21,17] and the results presented here).

n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(\Lambda)}$	$\delta(\mathbb{Z}^n)$	$\delta(\Lambda)$
2	0.66870	0.5	0.25	0.28868
3	0.52276	0.36965	0.125	0.17677
4	0.43899	0.32421	0.06250	0.12500
5	0.38322	0.27097	0.03125	0.08838
6	0.34958	0.24037	0.01563	0.07217
7	0.30080	$\geq$0.11809	0.00781	0.0625
8	0.29382	0.20777	0.00391	0.0625
12	0.22967	0.15172	0.00024	0.03704
24	0.15134	0.08594	5.96×10^{-8}	1

References

[1] A.A. Andrade, E.D. Carvalho, Construction of ideal lattices with full diversity, J. Adv. Res. Appl. Math. 3 (3) (2011) 82–92.

[2] A.A. Andrade, A.J. Ferrari, C.W.O. Benedito, S.I.R. Costa, Constructions of algebraic lattices, Comput. Appl. Math. 29 (3) (2010) 493–505.

[3] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. 241 (1999) 69–84.

[4] E. Bayer-Fluckiger, Ideal lattices, in: Proceedings of the Conference Number Theory and Diophantine Geometry, Zurich, 1999, Cambridge Univ. Press, 2002, pp. 168–184.

[5] E. Bayer-Fluckiger, Determinants of integral ideal lattices and automorphisms of given characteristic polynomial, J. Algebra 257 (2002) 215–221.

[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 Euclidean minimum of some real number fields, J. Théor. Nombres Bordeaux 17 (2) (2005) 437–454.

[8] E. Bayer-Fluckiger, I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, Arch. Math. 86 (3) (2006) 217–225.

[9] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiori, Good lattice constellations for both Rayleigh fading and Gaussian channels, IEEE Trans. Inform. Theory 42 (2) (1996) 502–517.

[10] M. Craig, Extreme forms and cyclotomy, Mathematika 25 (1978) 44–56.

[11] M. Craig, A cyclotomic construction of the Leech's lattice, Mathematika 25 (1978) 236–241.

[12] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag, 1998.

[13] H. Cohn, A. Kumar, Optimality and uniqueness of the Leech lattice among lattices, Ann. of Math. 170 (2009) 1003–1050, Princeton.

[14] U. Fincke, M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, Math. Comp. 44 (170) (1985) 463–471, AMS.

[15] A.L. Flores, J.C. Interlando, T.P. Nóbrega Neto, A.L. Contiero, A new number field construction of the lattice E_8, Contrib. Algebra Geom. 56 (2012) 1–6, Springer.

[16] I. Haviv, O. Regev, On the lattice isomorphism problem, arXiv:1311.0366 [csDS], 2013.

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

[18] G.C. Jorge, S.I.R. Costa, On rotated D_n-lattices constructed via totally real number fields, Arch. Math. 100 (2013) 323–332.

[19] F. Oggier, E. Viterbo, Algebraic number theory and code design for Rayleigh fading channels, Found. Trends Commun. Inf. Theory 1 (3) (2004) 333–415.

[20] F. Oggier, Algebraic methods for channel coding, Ph.D. Thesis, École Polytechnique Fédérale de Laussane, Laussane, 2005.

[21] F. Oggier, E. Bayer-Fluckiger, Best rotated cubic lattice constellations for the Rayleigh fading channel, in: Proceedings of IEEE International Symposium on Information Theory, 2013.

[22] P. Samuel, Algebraic Theory of Numbers, Hermann, Paris, 1970.

[23] I.N. Stewart, D.O. Tall, Algebraic Number Theory, Chapman & Hall, London, 1987.

[24] E. Viterbo, J. Boutros, A universal lattice code decoder for fading channels, IEEE Trans. Inform. Theory 45 (5) (1999) 1639–1642.