

Rotated D_n -lattices in dimensions power of 3^*

Research Article

Agnaldo J. Ferrari, Grasielle C. Jorge, Antonio A. de Andrade

Abstract: In this work, we present constructions of families of rotated D_n -lattices which may be good for signal transmission over both Gaussian and Rayleigh fading channels. The lattices are obtained as sublattices of a family of rotated $\mathbb{Z} \oplus \mathcal{A}_2^k$ lattices, where \mathcal{A}_2^k is a direct sum of $k = \frac{3^{r-1}-1}{2}$ copies of the A_2 -lattice, using free \mathbb{Z} -modules in $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$.

2010 MSC: 11H06, 11R18, 94B12

Keywords: Lattices, Cyclotomic fields, Signal transmission

1. Introduction

A lattice $\Lambda \subseteq \mathbb{R}^n$ is a discrete set generated by integer combinations of n linearly independent vectors in \mathbb{R}^n over \mathbb{R} . Its packing density $\Delta(\Lambda)$ is the proportion of the space \mathbb{R}^n covered by congruent disjoint spheres of maximum radius [8]. A lattice Λ has diversity $m \leq n$ if m is the maximum number such that for all $\mathbf{y} = (y_1, \dots, y_n) \in \Lambda$, with $\mathbf{y} \neq \mathbf{0}$, there are at least m non-zero coordinates. Given a full diversity lattice $\Lambda \subseteq \mathbb{R}^n$, with $m = n$, the minimum product distance is defined as $d_{min}(\Lambda) = \inf\{\prod_{i=1}^n |y_i| \text{ for all } \mathbf{y} = (y_1, \dots, y_n) \in \Lambda, \text{ with } \mathbf{y} \neq \mathbf{0}\}$ [5].

Lattices have been considered in different areas, especially in coding theory, and they have been studied in several papers, from different points of view [1–7, 9, 10, 12, 13, 15]. Signal constellations having lattice structure have been studied for signal transmission over both Gaussian and single-antenna Rayleigh fading channel [7]. Usually the problem of finding good signal constellations for a Gaussian

* This work was supported by CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) under Grants No. 432735/2016-0 and 429346/2018-2 and Fapesp (Fundação de Amparo à Pesquisa do Estado de São Paulo) under Grant No. 2013/25977-7.

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

Grasielle C. Jorge; Institute of Science and Technology, Federal University of São Paulo, São José dos Campos, SP 12247-014, Brazil (email: grasielle.jorge@unifesp.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).

channel is associated to the search for lattices with high packing density [8]. On the other hand, for a Rayleigh fading channel the efficiency is strongly related to the lattice diversity and minimum product distance [5, 7]. The approach in this work, following [12] and [13] is the use of algebraic number theory to construct rotated D_n -lattices with full diversity via free \mathbb{Z} -modules.

In [1, 4, 5] some families of rotated \mathbb{Z}^n -lattices for $n = \frac{p-1}{2}$, where $p \geq 5$ is a prime number, and $n = 2^s$, for $s \geq 1$, with full diversity and good minimum product distance are studied for transmission over Rayleigh fading channels. In [12, 13] are studied some families of rotated D_n -lattices with full diversity and good minimum product distance for transmission over both Gaussian and Rayleigh fading channels. In [12] are constructed rotated D_n -lattices for $n = (p-1)/2$, where $p \geq 7$ is a prime and $n = 2^k$, for $k \geq 2$ integer, and in [13] families of rotated D_n -lattices for $n = 2^k(p-1)$, with $k \geq 0$ integer and $p \geq 5$ a prime, and $n = (p-1)(q-1)/4$, where $p, q \geq 5$ are distinct prime numbers.

In this work, we construct families of rotated D_n -lattices with full diversity n for $n = 3^s$, $s \geq 1$, (Propositions 3.4 and 3.5). A D_n -lattice has better packing density $\delta(D_n)$ when compared to \mathbb{Z}^n , i.e., D_n has the best lattice packing density for $n = 3, 4, 5$ and $\lim_{n \rightarrow \infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0$, and also a very efficient decoding algorithm [8].

2. Algebraic lattices

Let $\{v_1, \dots, v_m\}$ be a set of linearly independent vectors in \mathbb{R}^n and $\Lambda = \{\sum_{i=1}^m a_i v_i; a_i \in \mathbb{Z}\}$ the associated lattice. The set $\{v_1, \dots, v_m\}$ 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 $G = MM^t = (\langle v_i, v_j \rangle)_{i,j=1}^m$. The *determinant* of Λ is $\det \Lambda = \det G$ and it is an invariant under change of basis (see [8, p. 4]). Two lattices Λ_1 and Λ_2 are said to be *similar* if there is an orthogonal mapping $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ 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 [5, 12], we will say that Λ_1 is a *rotated* Λ_2 -lattice if Λ_1 and Λ_2 are congruent.

Let \mathbb{K} be a totally real number field of degree n and $\mathcal{O}_{\mathbb{K}}$ its ring of integes. Let σ_i , for $i = 1, \dots, n$, be the n distinct \mathbb{Q} -homomorphisms from \mathbb{K} to \mathbb{R} . The *canonical embedding* $\sigma : \mathbb{K} \rightarrow \mathbb{R}^n$ is defined by $\sigma(x) = (\sigma_1(x), \dots, \sigma_n(x))$ [14, 16]. It can be shown that 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 $\Lambda = \sigma(\mathcal{I})$ is a lattice in \mathbb{R}^n with basis $\{\sigma(w_1), \dots, \sigma(w_n)\}$ [16, Chapter 8] and it has full diversity [2, 5]. A Gram matrix for $\sigma(\mathcal{I})$ is $G = (Tr_{\mathbb{K}|\mathbb{Q}}(w_i w_j))_{i,j=1}^n$, where $Tr_{\mathbb{K}|\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$ for any $x \in \mathbb{K}$ [5]. In what follows let $q(u_i, u_j) = Tr_{\mathbb{K}|\mathbb{Q}}(u_i u_j)$ for any $u_i, u_j \in \mathbb{K}$.

In this paper, we focus on the maximal totally real subfields of the cyclotomic fields $\mathbb{Q}(\zeta_{3^r})$, where ζ_{3^r} is a primitive 3^r -th root of unity, with $r \geq 3$ a positive integer [17].

3. Rotated D_n -lattices via $\mathbb{K} = \mathbb{Q}(\zeta_{3^r} + \zeta_{3^r}^{-1})$, where $r \geq 3$ and $n = 3^{r-1}$

In [13, 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_n -lattices via fractional ideals of $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$ since $d_{\mathbb{K}} = 3^{\frac{2(r+1)3^{r-1}-3^r-1}{2}}$ by [11]. Thus, in this section, we present some families of rotated D_n -lattices using free \mathbb{Z} -modules in $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$. Our strategy is to construct these lattices as sublattices of a family of rotated $\mathbb{Z} \oplus \mathcal{A}_2^k$ -lattices, where \mathcal{A}_2^k is a direct sum of $k = \frac{3^{r-1}-1}{2}$ copies of the A_2 -lattice. In [3] is presented a family of rotated $\mathbb{Z} \oplus \mathcal{A}_2^k$ -lattices as the image of a twisted embedding [2] applied to $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$. In Proposition 3.3, we construct a family of rotated $\mathbb{Z} \oplus \mathcal{A}_2^k$ -lattices using the canonical embedding, where the Lemma 3.1 and Proposition 3.2 are support for the proof of Proposition 3.3.

Lemma 3.1. [9] Consider $e_0 = 1$ and $e_i = \zeta_{3^r}^i + \zeta_{3^r}^{-i}$, for $i = 1, 2, \dots, 3^{r-1} - 1$.

1. If $i = 0, \dots, 3^{r-1} - 1$, then $q(e_i, e_i) = \begin{cases} 3^{r-1} & \text{if } i = 0, \\ 2 \cdot 3^{r-1} & \text{otherwise.} \end{cases}$
2. If $i = 1, 2, \dots, 3^{r-1} - 1$, then $q(e_i, e_0) = 0$.
3. If $i, j = 1, \dots, 3^{r-1} - 1$, with $i \neq j$, then

$$q(e_i, e_j) = \begin{cases} -3^{r-1} & \text{if } i + j = 3^{r-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.2. Consider $u_0 = e_0$, $u_1 = e_1$ and for $i = 2, 3, \dots, 3^{r-1} - 1$

$$u_i = \begin{cases} e_{\frac{i+1}{2}} & \text{if } i \equiv 1 \pmod{2}, \\ e_{3^{r-1} - \frac{i}{2}} & \text{otherwise.} \end{cases}$$

1. If $i = 0, \dots, 3^{r-1} - 1$, then $q(u_i, u_i) = \begin{cases} 3^{r-1} & \text{if } i = 0, \\ 2 \cdot 3^{r-1} & \text{otherwise.} \end{cases}$
2. If $i = 1, 2, \dots, 3^{r-1} - 1$, then $q(u_i, u_0) = 0$.
3. If $i, j = 1, \dots, 3^{r-1} - 1$, with $i \neq j$, then

$$q(u_i, u_j) = \begin{cases} -3^{r-1} & \text{if } i + j \equiv 3 \pmod{4} \text{ and } |i - j| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. From Lemma 3.1, it follows that $q(u_0, u_0) = q(e_0, e_0) = 3^{r-1}$ and for $i = 1, 2, \dots, 3^{r-1} - 1$, it follows that $q(u_i, u_i) = 2 \cdot 3^{r-1}$ and $q(u_i, u_0) = q(u_i, e_0) = 0$, for $u_i \in \{e_1, e_2, \dots, e_{3^{r-1}-1}\}$. If $i, j = 1, 2, \dots, 3^{r-1} - 1$, with $i \neq j$, then

$$q(u_i, u_j) = \begin{cases} q(e_{\frac{i+1}{2}}, e_{\frac{j+1}{2}}) & \text{if } i, j \equiv 1 \pmod{2}, \\ q(e_{\frac{i+1}{2}}, e_{3^{r-1} - \frac{j}{2}}) & \text{if } i \equiv 1 \text{ and } j \equiv 0 \pmod{2}, \\ q(e_{3^{r-1} - \frac{i}{2}}, e_{\frac{j+1}{2}}) & \text{if } i \equiv 0 \text{ and } j \equiv 1 \pmod{2}, \\ q(e_{3^{r-1} - \frac{i}{2}}, e_{3^{r-1} - \frac{j}{2}}) & \text{if } i, j \equiv 0 \pmod{2}. \end{cases}$$

For $i, j \equiv 1 \pmod{2}$, it follows that either $i + j \equiv 0 \pmod{4}$ or $i + j \equiv 2 \pmod{4}$ and $\frac{i+1}{2} + \frac{j+1}{2} \neq 3^{r-1}$. Otherwise, since $i \neq j$, it follows that $i = j = 3^{r-1} - 1$, which is a contradiction. Thus, $q(u_i, u_j) = 0$. For $i \equiv 1 \pmod{2}$ and $j \equiv 0 \pmod{2}$, it follows that $\frac{i+1}{2} + 3^{r-1} - \frac{j}{2} = 3^{r-1}$ if and only if $i = j - 1$. For $i \equiv 0 \pmod{2}$ and $j \equiv 1 \pmod{2}$, it follows that $3^{r-1} - \frac{i}{2} + \frac{j+1}{2} = 3^{r-1}$ if and only if $j = i - 1$. In the last two cases, as $i + j$ is odd, it follows that $i + j \equiv 3 \pmod{4}$, because if $i + j \equiv 1 \pmod{4}$, with $i = j - 1$ (respectively, $j = i - 1$), it follows that j is odd (respectively, i is odd), which is a contradiction. Therefore, $q(u_i, u_j) = -3^{r-1}$ if $i + j \equiv 3 \pmod{4}$ and $|i - j| = 1$. For $i, j \equiv 0 \pmod{2}$, it follows that either $i + j \equiv 0 \pmod{4}$ or $i + j \equiv 2 \pmod{4}$ and $3^{r-1} - \frac{i}{2} + 3^{r-1} - \frac{j}{2} \neq 3^{r-1}$. Otherwise, since $i \neq j$, it follows that $i = j = 3^{r-1} - 1$, which is a contradiction. Thus, $q(u_i, u_j) = 0$. \square

Proposition 3.3. The lattice $\frac{1}{\sqrt{3^{r-1}}}\sigma(\mathcal{O}_{\mathbb{K}})$ is a rotated version of $\mathbb{Z} \oplus \mathcal{A}_2^k$, where \mathcal{A}_2^k is a direct sum of $k = \frac{3^{r-1}-1}{2}$ copies of the A_2 -lattice.

Proof. From Proposition 3.2, it follows that $\{u_0, u_1, \dots, u_{3^{r-1}-1}\}$ is a \mathbb{Z} -basis of $\mathcal{O}_{\mathbb{K}}$ because it is a permutation of the \mathbb{Z} -basis $\{e_0, e_1, \dots, e_{3^{r-1}-1}\}$. A generator matrix of the algebraic lattice $\frac{1}{\sqrt{3^{r-1}}}\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$

$$\begin{aligned} & -u_{8j+2}; \\ \omega_{3^{r-1}+3-4j} &= u_3 + u_4 + 3u_{8j-3} + 3u_{8j-2} - u_{8j-1} - u_{8j} + u_{8j+1} \\ & + u_{8j+2}; \\ \omega_{3^{r-1}+4-4j} &= -2u_3 - 2u_4 + u_{8j-9} + u_{8j-8} - 2u_{8j-7} - 2u_{8j-6} \\ & + u_{8j-5} + u_{8j-4} - u_{8j-3} - u_{8j-2} - u_{8j+1} - u_{8j+2}. \end{aligned}$$

Therefore, $\Lambda = \frac{1}{2\sqrt{3^r}}\sigma(\mathcal{I}) \subseteq \mathbb{R}^{3^{r-1}}$ is a rotated version of the $D_{3^{r-1}}$ -lattice.

Proof. From Proposition 3.2, it follows that

$$\begin{aligned} q(\omega_0, \omega_0) &= Tr_{\mathbb{K}/\mathbb{Q}}(\omega_0\omega_0) = Tr_{\mathbb{K}/\mathbb{Q}}((-4u_0 - 2u_1 - 2u_2)(-4u_0 \\ & - 2u_1 - 2u_2)) = Tr_{\mathbb{K}/\mathbb{Q}}(16u_0u_0 + 16u_0u_1 + 16u_0u_2 \\ & + 4u_1u_1 + 8u_1u_2 + 4u_2u_2) = 16q(u_0, u_0) + 16q(u_0, u_1) \\ & + 16q(u_0, u_2) + 4q(u_1, u_1) + 8q(u_1, u_2) + 4q(u_2, u_2) \\ & = 24 \cdot 3^{r-1}. \end{aligned}$$

$$q(\omega_1, \omega_1) = 4q(u_1, u_1) + 4q(u_2, u_2) - 8q(u_1, u_2) = 24 \cdot 3^{r-1}.$$

$$q(\omega_2, \omega_2) = 16q(u_0, u_0) + 4q(u_2, u_2) = 24 \cdot 3^{r-1}.$$

$$\begin{aligned} q(\omega_3, \omega_3) &= 4q(u_0, u_0) + 4q(u_1, u_1) + 8q(u_1, u_2) + 4q(u_2, u_2) \\ & + q(u_5, u_5) - 2q(u_5, u_6) + q(u_6, u_6) + q(u_9, u_9) \\ & - 2q(u_9, u_{10}) + q(u_{10}, u_{10}) = 24 \cdot 3^{r-1}. \end{aligned}$$

$$q(\omega_0, \omega_1) = q(\omega_0, \omega_3) = q(\omega_1, \omega_3) = 0.$$

$$q(\omega_0, \omega_2) = q(\omega_1, \omega_2) = q(\omega_2, \omega_3) = q(\omega_3, \omega_4) = -12 \cdot 3^{r-1}.$$

Let $j = 1, 2, \dots, \frac{3^{r-1}-3}{8}$. Since $q(u_i, u_j) \neq 0$ if and only if $i + j \equiv 3 \pmod{4}$ and $|i - j| = 1$, it follows that

$$\begin{aligned} q(\omega_{4j}, \omega_{4j}) &= q(u_{8j-3}, u_{8j-3}) - 2q(u_{8j-3}, u_{8j-2}) + q(u_{8j-2}, u_{8j-2}) \\ & + q(u_{8j-1}, u_{8j-1}) - 2q(u_{8j-1}, u_{8j}) + q(u_{8j}, u_{8j}) \\ & + q(u_{8j+1}, u_{8j+1}) - 2q(u_{8j+1}, u_{8j+2}) + q(u_{8j+2}, u_{8j+2}) \\ & + q(u_{8j+3}, u_{8j+3}) - 2q(u_{8j+3}, u_{8j+4}) + q(u_{8j+4}, u_{8j+4}) \\ & = 24 \cdot 3^{r-1}. \end{aligned}$$

Similarly,

$$\begin{aligned} q(\omega_{3^{r-1}+1-4j}, \omega_{3^{r-1}+1-4j}) &= q(u_{8j-3}, u_{8j-3}) + 2q(u_{8j-3}, u_{8j-2}) \\ & + q(u_{8j-2}, u_{8j-2}) + q(u_{8j-1}, u_{8j-1}) + 2q(u_{8j-1}, u_{8j}) \\ & + q(u_{8j}, u_{8j}) + 9q(u_{8j+1}, u_{8j+1}) + 18q(u_{8j+1}, u_{8j+2}) \\ & + 9q(u_{8j+2}, u_{8j+2}) + q(u_{8j+3}, u_{8j+3}) + 2q(u_{8j+3}, u_{8j+4}) \\ & + q(u_{8j+4}, u_{8j+4}) = 24 \cdot 3^{r-1}, \end{aligned}$$

$$\begin{aligned} q(\omega_{4j+1}, \omega_{4j+1}) &= q(\omega_{4j+2}, \omega_{4j+2}) = q(\omega_{4j+3}, \omega_{4j+3}) = \\ & = q(\omega_{3^{r-1}+2-4j}, \omega_{3^{r-1}+2-4j}) = q(\omega_{3^{r-1}+3-4j}, \omega_{3^{r-1}+3-4j}) \\ & = q(\omega_{3^{r-1}+4-4j}, \omega_{3^{r-1}+4-4j}) = 24 \cdot 3^{r-1}, \end{aligned}$$

$$\begin{aligned} q(\omega_{4j}, \omega_{4j+1}) &= -q(\omega_{8j-3}, \omega_{8j-3}) + 2q(\omega_{8j-3}, \omega_{8j-2}) \\ & - q(\omega_{8j-2}, \omega_{8j-2}) - q(\omega_{8j-1}, \omega_{8j-1}) + 2q(\omega_{8j-1}, \omega_{8j}) \\ & - q(\omega_{8j}, \omega_{8j}) + q(\omega_{8j+1}, \omega_{8j+1}) - 2q(\omega_{8j+1}, \omega_{8j+2}) \\ & + q(\omega_{8j+2}, \omega_{8j+2}) - q(\omega_{8j+3}, \omega_{8j+3}) + 2q(\omega_{8j+3}, \omega_{8j+4}) \\ & - q(\omega_{8j+4}, \omega_{8j+4}) = -12 \cdot 3^{r-1}, \end{aligned}$$

$$\begin{aligned} q(\omega_{4j+1}, \omega_{4j+2}) &= q(\omega_{4j+2}, \omega_{4j+3}) = q(\omega_{4j+3}, \omega_{4(j+1)}) = \\ & = q(\omega_{3^{r-1}+1-4j}, \omega_{3^{r-1}+2-4j}) = q(\omega_{3^{r-1}+2-4j}, \omega_{3^{r-1}+3-4j}) \\ & = q(\omega_{3^{r-1}+3-4j}, \omega_{3^{r-1}+4-4j}) = -12 \cdot 3^{r-1}. \end{aligned}$$

Finally, for $k, l = 1, 2, \dots, 3^{r-1} - 2$, with $l > k + 1$, it follows that $q(\omega_k, \omega_l) = 0$. Now, $\mathcal{C} = \{\omega_0, \omega_1, \dots, \omega_{3^{r-1}-1}\}$ is a basis of a free \mathbb{Z} -module \mathcal{I} . A generator matrix of the algebraic lattice $\frac{1}{2\sqrt{3^r}}\sigma(\mathcal{I})$ is given by $M = \frac{1}{2\sqrt{3^r}}N$, where $N = (\sigma_i(\omega_{j-1}))_{i,j=1}^{3^{r-1}}$, and the associated Gram matrix is

$$G = MM^t = \frac{1}{12 \cdot 3^{r-1}} (q(\omega_i, \omega_j))_{i,j=0}^{3^{r-1}-1} =$$

$$= \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & \dots & 0 \\ -1 & -1 & 2 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Therefore, G is the Gram matrix of a $D_{3^{r-1}}$ -lattice. □

3.2. Rotated D_n -lattices for $n = 3^{r-1}$, where $r \geq 3$ is odd

In this section, we present a construction of rotated D_n -lattices using \mathbb{Z} -modules via the totally real number field $\mathbb{K} = \mathbb{Q}(\zeta_{3^r} + \zeta_{3^r}^{-1})$, where r is odd. The D_n -lattice is obtained as sublattice of $\mathbb{Z} \oplus \mathcal{A}_2^k$ using $\mathcal{B} = \{u_0, u_1, \dots, u_{3^{r-1}-1}\}$ a \mathbb{Z} -basis of $\mathcal{O}_{\mathbb{K}}$.

Proposition 3.5. *Let $\mathcal{I} = \mathbb{Z}\omega_0 \oplus \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_{3^{r-1}-1}$ be a free \mathbb{Z} -module of $\mathcal{O}_{\mathbb{K}}$, where*

1. $\omega_0 = -6u_0 - 3u_1 - 3u_3; \omega_1 = 6u_0 - 3u_1 - 3u_3; \omega_2 = 6u_1;$
2. For $3 \leq j \leq \frac{3^{r-1}-3}{2}$, where j is odd,

$$\omega_j = -3u_{2j-5} + 3u_{2j-3} - 3u_{2j-1} - 3u_{2j+1};$$

$$\omega_{j+1} = 6u_{2j-1};$$
3. For $j = \frac{3^{r-1}+1}{2}$,

$$\omega_j = -u_{2j-7} - 2u_{2j-6} - 5u_{2j-5} - 4u_{2j-4} + 4u_{2j-3} + 2u_{2j-2};$$

$$\omega_{j+1} = -u_{2j-9} - 2u_{2j-8} - u_{2j-7} - 2u_{2j-6} + 3u_{2j-5} + 6u_{2j-4} - u_{2j-3} - 2u_{2j-2};$$

$$\omega_{j+2} = -u_{2j-9} - 2u_{2j-8} + 3u_{2j-7} + 6u_{2j-6} - u_{2j-5} - 2u_{2j-4} + u_{2j-3} + 2u_{2j-2};$$

$$\omega_{j+3} = 3u_{2j-9} + 6u_{2j-8} - u_{2j-7} - 2u_{2j-6} + u_{2j-5} + 2u_{2j-4} + u_{2j-3} + 2u_{2j-2};$$
4. For $j = 1, 2, \dots, \frac{3^{r-1}-9}{8}$, with $r > 3$,

$$\omega_{3^{r-1}-4j} = -u_{8j-5} - 2u_{8j-4} - 2u_{8j-3} - 4u_{8j-2} + u_{8j-1} + 2u_{8j} - u_{8j+1} - 2u_{8j+2} - u_{8j+5} - 2u_{8j+6} - 2u_{8j+7} - 4u_{8j+8};$$

$$\omega_{3^{r-1}+1-4j} = -u_{8j-7} - 2u_{8j-6} - u_{8j-5} - 2u_{8j-4} + 3u_{8j-3} + 6u_{8j-2} - u_{8j-1} - 2u_{8j};$$

$$\omega_{3^{r-1}+2-4j} = -u_{8j-7} - 2u_{8j-6} + 3u_{8j-5} + 6u_{8j-4} - u_{8j-3} - 2u_{8j-2} + u_{8j-1} + 2u_{8j};$$

$$\omega_{3^{r-1}+3-4j} = 3u_{8j-7} + 6u_{8j-6} - u_{8j-5} - 2u_{8j-4} + u_{8j-3} + 2u_{8j-2} + u_{8j-1} + 2u_{8j}.$$

Therefore, $\Lambda = \frac{1}{6\sqrt{3^{r-1}}}\sigma(\mathcal{I}) \subseteq \mathbb{R}^{3^{r-1}}$ is a rotated version of a $D_{3^{r-1}}$ -lattice.

Proof. From Proposition 3.2, it follows that

$$q(\omega_0, \omega_0) = Tr_{\mathbb{K}/\mathbb{Q}}(\omega_0\omega_0) = Tr_{\mathbb{K}/\mathbb{Q}}((-6u_0 - 3u_1 - 3u_3)(-6u_0 - 3u_1 - 3u_3)) = Tr_{\mathbb{K}/\mathbb{Q}}(36u_0u_0 + 36u_0u_1 + 36u_0u_3 + 9u_1u_1 + 18u_1u_3 + 9u_3u_3) = 36q(u_0, u_0) + 36q(u_0, u_1)$$

$$+ 36q(u_0, u_3) + 9q(u_1, u_1) + 18q(u_1, u_3) + 9q(u_3, u_3) = 72 \cdot 3^{r-1}.$$

$$q(\omega_1, \omega_1) = 36q(u_0, u_0) + 9q(u_1, u_1) + 9q(u_3, u_3) = 72 \cdot 3^{r-1}.$$

$$q(\omega_2, \omega_2) = 36q(u_1, u_1) = 72 \cdot 3^{r-1}.$$

$$q(\omega_0, \omega_1) = q(\omega_0, \omega_3) = q(\omega_1, \omega_3) = 0.$$

$$q(\omega_0, \omega_2) = q(\omega_1, \omega_2) = q(\omega_2, \omega_3) = -36 \cdot 3^{r-1}.$$

Let $3 \leq j \leq \frac{3^{r-1}-3}{2}$, with j odd. Since $q(u_i, u_j) \neq 0$ if and only if $i + j \equiv 3 \pmod{4}$ and $|i - j| = 1$, it follows that

$$q(\omega_j, \omega_j) = 9q(u_{2j-5}, u_{2j-5}) + 9q(u_{2j-3}, u_{2j-3}) + 9q(u_{2j-1}, u_{2j-1}) + 9q(u_{2j+1}, u_{2j+1}) = 72 \cdot 3^{r-1}.$$

$$q(\omega_{j+1}, \omega_{j+1}) = 36q(u_{2j-1}, u_{2j-1}) = 72 \cdot 3^{r-1}.$$

Furthermore,

$$q(\omega_j, \omega_{j+1}) = -18q(u_{2j-1}, u_{2j-1}) = -36 \cdot 3^{r-1}, \text{ and for } j < \frac{3^{r-1}-3}{2},$$

$$q(\omega_{j+1}, \omega_{j+2}) = q(6u_{2j-1}, -3u_{2(j+2)-5} + 3u_{2(j+2)-3} - 3u_{2(j+2)-1} - 3u_{2(j+2)+1}) = q(6u_{2j-1}, -3u_{2j-1} + 3u_{2j+1} - 3u_{2j+3} - 3u_{2j+5}) = -18q(u_{2j-1}, u_{2j-1}) = -36 \cdot 3^{r-1}.$$

For $j = \frac{3^{r-1}+1}{2}$, it follows that

$$q(\omega_j, \omega_j) = q(u_{2j-7}, u_{2j-7}) + 4q(u_{2j-7}, u_{2j-6}) + 4q(u_{2j-6}, u_{2j-6}) + 25q(u_{2j-5}, u_{2j-5}) + 40q(u_{2j-5}, u_{2j-4}) + 16q(u_{2j-4}, u_{2j-4}) + 16q(u_{2j-3}, u_{2j-3}) + 16q(u_{2j-3}, u_{2j-2}) + 4q(u_{2j-2}, u_{2j-2}) = 72 \cdot 3^{r-1}.$$

In the same way, it follows that

$$q(\omega_{j+1}, \omega_{j+1}) = q(\omega_{j+2}, \omega_{j+2}) = q(\omega_{j+3}, \omega_{j+3}) = 72 \cdot 3^{r-1}.$$

Also,

$$q(\omega_j, \omega_{j+1}) = q(\omega_{2j-7}, \omega_{2j-7}) + 4q(\omega_{2j-7}, \omega_{2j-6}) + 4q(\omega_{2j-6}, \omega_{2j-6}) - 15q(\omega_{2j-5}, \omega_{2j-5}) - 42q(\omega_{2j-5}, \omega_{2j-4}) - 24q(\omega_{2j-4}, \omega_{2j-4}) - 4q(\omega_{2j-3}, \omega_{2j-3}) - 10q(\omega_{2j-3}, \omega_{2j-2}) - 4q(\omega_{2j-2}, \omega_{2j-2}) = -36 \cdot 3^{r-1}.$$

In the same way, it follows that

$$q(\omega_{j+1}, \omega_{j+2}) = q(\omega_{j+2}, \omega_{j+3}) = -36 \cdot 3^{r-1}, \text{ and for } k = \frac{3^{r-1}-9}{8},$$

$$q(\omega_{j+3}, \omega_{3^{r-1}-4k}) = q(\omega_{\frac{3^{r-1}+7}{2}}, \omega_{\frac{3^{r-1}+9}{2}}) = -36 \cdot 3^{r-1}.$$

For $j = 1, 2, \dots, \frac{3^{r-1}-9}{8}$, with $r > 3$,

$$q(\omega_{3^{r-1}-4j}, \omega_{3^{r-1}-4j}) = q(\omega_{8j-5}, \omega_{8j-5}) + 4q(\omega_{8j-5}, \omega_{8j-4}) + 4q(\omega_{8j-4}, \omega_{8j-4}) + 4q(\omega_{8j-3}, \omega_{8j-3}) + 16q(\omega_{8j-3}, \omega_{8j-2}) + 16q(\omega_{8j-2}, \omega_{8j-2}) + q(\omega_{8j-1}, \omega_{8j-1}) + 4q(\omega_{8j-1}, \omega_{8j}) + 4q(\omega_{8j}, \omega_{8j}) + q(\omega_{8j+1}, \omega_{8j+1}) + 4q(\omega_{8j+1}, \omega_{8j+2}) + 4q(\omega_{8j+2}, \omega_{8j+2}) + q(\omega_{8j+5}, \omega_{8j+5}) + 4q(\omega_{8j+5}, \omega_{8j+6}) + 4q(\omega_{8j+6}, \omega_{8j+6}) + 4q(\omega_{8j+7}, \omega_{8j+7}) + 16q(\omega_{8j+7}, \omega_{8j+8}) + 16q(\omega_{8j+8}, \omega_{8j+8}) = 72 \cdot 3^{r-1}.$$

In the same way, it follows that

$$q(\omega_{3^{r-1}+1-4j}, \omega_{3^{r-1}+1-4j}) = q(\omega_{3^{r-1}+2-4j}, \omega_{3^{r-1}+2-4j}) = q(\omega_{3^{r-1}+3-4j}, \omega_{3^{r-1}+3-4j}) = 72 \cdot 3^{r-1}.$$

Also,

$$q(\omega_{3^{r-1}-4j}, \omega_{3^{r-1}+1-4j}) = q(u_{8j-5}, u_{8j-5}) + 4q(u_{8j-5}, u_{8j-4}) + 4q(u_{8j-4}, u_{8j-4}) - 6q(u_{8j-3}, u_{8j-3}) - 24q(u_{8j-3}, u_{8j-2}) - 24q(u_{8j-2}, u_{8j-2}) - q(u_{8j-1}, u_{8j-1}) - 4q(u_{8j-1}, u_{8j}) - 4q(u_{8j}, u_{8j}) = -36 \cdot 3^{r-1}.$$

In the same way, it follows that

$$q(\omega_{3^{r-1}+1-4j}, \omega_{3^{r-1}+2-4j}) = q(\omega_{3^{r-1}+2-4j}, \omega_{3^{r-1}+3-4j}) = -36 \cdot 3^{r-1}.$$

Finally, for $k, l = 1, 2, \dots, 3^{r-1} - 2$, with $l > k + 1$, it follows that $q(\omega_k, \omega_l) = 0$. Now, $\mathcal{C} = \{\omega_0, \omega_1, \dots, \omega_{3^{r-1}-1}\}$ is a basis of a free \mathbb{Z} -module \mathcal{I} . A generator matrix of the algebraic

lattice $\frac{1}{6\sqrt{3^{r-1}}}\sigma(\mathcal{I})$ is given by $M = \frac{1}{6\sqrt{3^{r-1}}}N$, where $N = (\sigma_i(\omega_{j-1}))_{i,j=1}^{3^{r-1}}$, and the associated Gram matrix is

$$G = MM^t = \frac{1}{36 \cdot 3^{r-1}} (q(\omega_i, \omega_j))_{i,j=0}^{3^{r-1}-1} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & \dots & 0 \\ -1 & -1 & 2 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Therefore, G is the Gram matrix of a $D_{3^{r-1}}$ -lattice. □

4. Conclusions

In this paper, we construct full diversity rotated versions of $D_{3^{r-1}}$ -lattices via the canonical embedding and two families of \mathbb{Z} -modules of the ring of the integers $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$, for $r \geq 3$ a positive integer, since it is impossible to construct rotated D_n -lattices via fractional ideals of $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$ [13]. The lattices obtained here are sublattices of the family of rotated $\mathbb{Z} \oplus \mathcal{A}_2^k$ -lattices, where \mathcal{A}_2^k is a direct sum of $k = \frac{3^{r-1}-1}{2}$ copies of the A_2 -lattice.

In [1] and [4] families of rotated $\mathbb{Z}^{2^{r-2}}$ -lattices were obtained via the ring of integers $\mathbb{Z}[\zeta_{2^r} + \zeta_{2^r}^{-1}]$. In [5] a family of rotated $\mathbb{Z}^{(p-1)/2}$ -lattices was obtained via the ring of integers $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, with p prime. In [9] two families of rotated $\mathbb{Z}^{3^{r-1}}$ -lattices were obtained via free \mathbb{Z} -modules of $\mathbb{Z}[\zeta_{3^r} + \zeta_{3^r}^{-1}]$, one for r odd and one for r even. In [12] two families of rotated $D_{2^{r-2}}$ -lattices were obtained, one via the ring of integers $\mathbb{Z}[\zeta_{2^r} + \zeta_{2^r}^{-1}]$ and one via a principal ideal of $\mathbb{Z}[\zeta_{2^r} + \zeta_{2^r}^{-1}]$. Also in [12] a family of rotated $D_{(p-1)/2}$ -lattices was presented via free \mathbb{Z} -modules in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, with p prime, that are not ideals. In [13] considering the compositum of $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ and $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and the compositum of $\mathbb{Q}(\zeta_{p_1} + \zeta_{p_1}^{-1})$ and $\mathbb{Q}(\zeta_{p_2} + \zeta_{p_2}^{-1})$, where p, p_1 and p_2 are prime numbers with $p_1 \neq p_2$, were constructed families of rotated D_n -lattices via free \mathbb{Z} -modules of rank n that are not ideals. In Table 1, we list the number fields considered in [1, 4, 5, 9, 12, 13] and here for constructing rotated \mathbb{Z}^n and D_n -lattices for some values of n . Let $\mathbb{K}_1 = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, $\mathbb{K}_2 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where p is a prime, $\mathbb{K}_3 = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $\mathbb{K}_4 = \mathbb{Q}(\zeta_{p_1} + \zeta_{p_1}^{-1})\mathbb{Q}(\zeta_{p_2} + \zeta_{p_2}^{-1})$, with $p_1 \neq p_2$, and $\mathbb{K}_5 = \mathbb{Q}(\zeta_{3^r} + \zeta_{3^r}^{-1})$. We observe that for $r = 14, 21, 25, 26, 28, 29$ and 30 there are not p, p_1, p_2 prime numbers with $p_1 \neq p_2$ such that the degree of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $\mathbb{Q}(\zeta_{p_1} + \zeta_{p_1}^{-1})\mathbb{Q}(\zeta_{p_2} + \zeta_{p_2}^{-1})$ be 3^{r-2} .

n	\mathbb{Z}^n			D_n				
	\mathbb{K}_1	\mathbb{K}_2	\mathbb{K}_5	\mathbb{K}_1	\mathbb{K}_2	\mathbb{K}_3	\mathbb{K}_4	\mathbb{K}_5
2	$r = 3$	$p = 5$	–	–	–	–	–	–
3	–	$p = 7$	$r = 3$	–	$p = 7$	–	–	$r = 3$
4	$r = 4$	–	–	$r = 4$	–	$r = 3, p = 5$	–	–
8	$r = 5$	$p = 17$	–	$r = 5$	$p = 17$	$r = 4, p = 5$	–	–
9	–	$p = 19$	$r = 4$	–	$p = 19$	–	–	$r = 4$
16	$r = 6$	–	–	$r = 6$	–	$r = p = 5$	$p_1, p_2 \in \{5, 17\}$	–
27	–	–	$r = 5$	–	–	–	$p_1, p_2 \in \{7, 19\}$	$r = 5$
32	$r = 7$	–	–	$r = 7$	–	$r = 4, p = 17$	–	–
64	$r = 8$	–	–	$r = 8$	–	$r = 7, p = 5$	–	–
81	–	$p = 163$	$r = 6$	–	$p = 163$	–	–	$r = 6$

n	\mathbb{Z}^n			D_n				
	\mathbb{K}_1	\mathbb{K}_2	\mathbb{K}_5	\mathbb{K}_1	\mathbb{K}_2	\mathbb{K}_3	\mathbb{K}_4	\mathbb{K}_5
128	$r = 9$	$p = 257$	—	$r = 9$	$p = 257$	$r = 8, p = 5$	—	—
243	—	$p = 487$	$r = 7$	—	$p = 487$	—	$p_1, p_2 \in \{7, 163\}$	$r = 7$
256	$r = 10$	—	—	$r = 10$	—	$r = 7, p = 17$	$p_1, p_2 \in \{5, 257\}$	—
512	$r = 11$	—	—	$r = 11$	—	$r = 10, p = 5$	—	—
729	—	$p = 1459$	$r = 8$	—	$p = 1459$	—	$p_1, p_2 \in \{7, 487\}$ $p_1, p_2 \in \{19, 163\}$	$r = 8$
1024	$r = 12$	—	—	$r = 12$	—	$r = 9, p = 17$	$p_1, p_2 \in \{17, 257\}$	—
2048	$r = 13$	—	—	$r = 13$	—	$r = 10, p = 17$	—	—
2187	—	—	$r = 9$	—	—	—	$p_1, p_2 \in \{7, 1459\}$ $p_1, p_2 \in \{19, 487\}$	$r = 9$
4096	$r = 14$	—	—	$r = 14$	—	$r = 13, p = 5$	—	—
6561	—	—	$r = 10$	—	—	—	$p_1, p_2 \in \{19, 1459\}$	$r = 10$
8192	$r = 15$	—	—	$r = 15$	—	$r = 12, p = 17$	—	—
16384	$r = 16$	—	—	$r = 16$	—	$r = 13, p = 5$	—	—
19683	—	$p = 39367$	$r = 11$	—	$p = 39367$	—	$p_1, p_2 \in \{163, 487\}$	$r = 11$
32768	$r = 17$	$p = 65537$	—	$r = 17$	$p = 65537$	$r = 14, p = 17$	—	—
59049	—	—	$r = 12$	—	—	—	$p_1, p_2 \in \{7, 39367\}$ $p_1, p_2 \in \{163, 1459\}$	$r = 12$
65536	$r = 18$	—	—	$r = 18$	—	$r = 17, p = 5$	—	—
131072	$r = 19$	—	—	$r = 19$	—	$r = 16, p = 17$	—	—
177147	—	—	$r = 13$	—	—	—	$p_1, p_2 \in \{19, 39367\}$ $p_1, p_2 \in \{487, 1459\}$	$r = 13$
262144	$r = 20$	—	—	$r = 20$	—	$r = 13, p = 257$	—	—
524288	$r = 21$	—	—	$r = 21$	—	$r = 20, p = 5$	—	—
531441	—	—	$r = 14$	—	—	—	—	$r = 14$
1048576	$r = 22$	—	—	$r = 22$	—	$r = 19, p = 17$	—	—
1594323	—	—	$r = 15$	—	—	—	$p_1, p_2 \in \{163, 39367\}$	$r = 15$

Table 2. Rotated \mathbb{Z}^n and D_n -lattices for n powers of 2 and 3.

References

- [1] A. A. Andrade, C. Alves, T. B. Carlos, Rotated lattices via th cyclotomic field $\mathbb{Q}(\zeta_r)$, International Journal of Applied Mathematics 19(3) (2006) 321-331.
- [2] E. Bayer-Fluckiger, Lattices and number fields, Contemporary Mathematics 241 (1999) 69-84.
- [3] E. Bayer-Fluckiger, Upper bounds for Euclidean minima of algebraic number fields, Journal of Number Theory 121(2) (2006) 305-323.
- [4] E. Bayer-Fluckiger, G. Nebe, On the Euclidean minimum of some real number fields, Journal de Théorie des Nombres de Bordeaux 17(2) (2005) 437-454.
- [5] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, New algebraic constructions of rotated \mathbb{Z}^n -lattice constellations for the Rayleigh fading channel, IEEE Transactions on Information Theory 50(4) (2004) 702-714.
- [6] E. Bayer-Fluckiger, I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, Archiv der Mathematik 86(3) (2006) 217-225.
- [7] 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.
- [8] J. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups, Springer-Verlag (1988).
- [9] A. J. Ferrari, A. A. Andrade, Constructions of rotated lattice constellations in dimensions power of 3, Journal of Algebra and its Applications 17(9) (2018) 1850175-1 to 17.

- [10] A. J. Ferrari, A. A. Andrade, R. R. Araujo, J. C. Interlando, Trace forms of certain subfields of cyclotomic fields and applications, *Journal of Algebra Combinatorics Discrete Structures and Applications* 7(2) (2020) 141-160.
- [11] J. C. Interlando, J. O. D. Lopes, T. P. N. Neto, The discriminant of Abelian number fields. *Journal of Algebra and Its Applications* 5 (2006) 35-41.
- [12] G. C. Jorge, A. J. Ferrari, S. I. R. Costa, Rotated D_n -lattices, *Journal of Number Theory* 132 (2012) 2397-2406.
- [13] G. C. Jorge, S. I. R. Costa, On rotated D_n -lattices constructed via totally real number fields, *Archiv der Mathematik* 100 (2013) 323-332.
- [14] P. Samuel, *Algebraic theory of numbers*, Hermann, Paris (1970).
- [15] I. Soprunov, Lattice polytopes in coding theory, *Journal of Algebra Combinatorics Discrete Structures and Applications* 2 (2) (2015) 85-94.
- [16] I. N. Stewart, D. O. Tall, *Algebraic number theory*, Chapman & Hall, London (1987).
- [17] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York (1982).