Journal of Number Theory 132 (2012) 2397–2406

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Rotated D_n-lattices ☆

Grasiele C. Jorge [a], Agnaldo J. Ferrari [b], Sueli I.R. Costa [a,*]

[a] Unicamp – University of Campinas, 13081-970, Campinas, SP, Brazil
[b] UFLA – Federal University of Lavras, 37200-000, Lavras, MG, Brazil

ARTICLE INFO

Article history:
Received 15 December 2011
Revised 24 February 2012
Accepted 1 May 2012
Available online 10 July 2012
Communicated by David Goss

Keywords:
D_n-lattices
Signal transmission
Cyclotomic fields
Minimum product distance

ABSTRACT

Based on algebraic number theory we construct some families of rotated D_n-lattices with full diversity which can be good for signal transmission over both Gaussian and Rayleigh fading channels. Closed-form expressions for the minimum product distance of those lattices are obtained through algebraic properties.

1. Introduction

A lattice $\Lambda = \Lambda^n \subseteq \mathbb{R}^n$ is a discrete set generated by integer combinations of n linearly independents vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$. Its packing density $\Delta(\Lambda)$ is the proportion of the space $\mathbb{R}^n$ covered by congruent disjoint spheres of maximum radius [9]. A lattice Λ has diversity $m \leqslant n$ if m is the maximum number such that for all $\boldsymbol{y} = (y_1, \ldots, y_n) \in \Lambda$, $\boldsymbol{y} \neq \boldsymbol{0}$ there are at least m non-vanishing coordinates. Given a full diversity lattice $\Lambda \subseteq \mathbb{R}^n$ $(m = n)$, the minimum product distance is defined as $d_{min}(\Lambda) = \min\{\prod_{i=1}^{n} |y_i|$ for all $\boldsymbol{y} = (y_1, \ldots, y_n) \in \Lambda,\ \boldsymbol{y} \neq \boldsymbol{0}\}$ [6].

Signal constellations having lattice structure have been studied as meaningful means for signal transmission over both Gaussian and single-antenna Rayleigh fading channel [8]. Usually the problem of finding good signal constellations for a Gaussian channel is associated to the search for lattices with high packing density [9]. On the other hand, for a Rayleigh fading channel the efficiency, measured by

☆ This work was partially supported by CNPq 140239/2009-0, CNPq 569966/2008-6, CNPq 309561/2009-4 and FAPESP 2007/56052-8.

* Corresponding author.
E-mail addresses: grajorge@ime.unicamp.br (G.C. Jorge), agnaldo@ime.unicamp.br (A.J. Ferrari), sueli@ime.unicamp.br (S.I.R. Costa).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.05.002

lower error probability in the transmission, is strongly related to the lattice diversity and minimum product distance [8,6]. The approach in this work, following [2,6] is the use of algebraic number theory to construct lattices which may have good performance for both channels.

For general lattices the packing density and the minimum product distance are usually hard to estimate [11]. Those parameters can be obtained in certain cases of lattices associated to number fields through algebraic properties.

In [5,6,4] some families of rotated $\mathbb{Z}^n$-lattices with full diversity and good minimum product distance are studied for transmission over Rayleigh fading channels. In [7] the lattices A_{p-1}, p prime, E_6, E_8, K_{12} and Λ_{24} were realized as full diversity ideal lattices via some subfields of cyclotomic fields. In [8] rotated n-dimensional lattices (including D_4, K_{12} and Λ_{16}), which are good for both channels, are constructed with diversity $n/2$.

In this work we also attempt to consider lattices feasible for both channels by constructing rotated D_n-lattices with full diversity n and get a closed-form for their minimum product distance. The results are obtained for $n = 2^{r-2}$, $r \geqslant 5$ and $n = (p-1)/2$, p prime and $p \geqslant 7$, in Propositions 4.3, 4.6 and 5.1. As it is known, a D_n lattice has better packing density $\delta(D_n)$ than $\mathbb{Z}^n$ (D_n has the best lattice packing density for $n = 3, 4, 5$ and $\lim_{n\longrightarrow\infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0$) and also has a very efficient decoding algorithm [9]. The relative minimum product distances $d_{p,rel}(D_n)$ of the rotated D_n-lattices obtained here are smaller than the minimum product distance $d_{p,rel}(\mathbb{Z}^n)$ of rotated $\mathbb{Z}^n$-lattices constructed for the Rayleigh channels in [1] and [6], but, as it is shown in Sections 4 and 5, $\lim_{n\longrightarrow\infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2}$, what offers a good trade-off.

In Sections 2 and 3 we summarize some definitions and results on Algebraic Number Theory. Sections 4 and 5 are devoted to the construction of full diversity rotated D_n-lattices through cyclotomic fields and the deduction of their minimum product distance.

2. Number fields

In this section we summarize some concepts and results of algebraic number theory and establish the notation to be used from now on. The results presented here can be found in [10,12–14].

Let $\mathbb{K}$ be a number field of degree n and $\mathcal{O}_{\mathbb{K}}$ its ring of integers. It can be shown that every nonzero fractionary ideal I of $\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n.

There are exactly n distinct $\mathbb{Q}$-homomorphisms $\{\sigma_i\}_{i=1}^{n}$ of $\mathbb{K}$ in $\mathbb{C}$. A homomorphism σ_i is said *real* if $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, and the field $\mathbb{K}$ is said *totally real* if σ_i is real for all $i = 1, \ldots, n$.

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

Let $\{\omega_1, \ldots, \omega_n\}$ be 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 $\mathbb{K}$.

The *norm* of an ideal $I \subseteq \mathcal{O}_{\mathbb{K}}$ is defined as $N(I) = |\mathcal{O}_{\mathbb{K}}/I|$.

The *codifferent* from $\mathbb{K}|\mathbb{Q}$ is the fractionary ideal $\Delta(\mathbb{K}|\mathbb{Q})^{-1} = \{x \in \mathbb{K};\ \forall\alpha \in \mathcal{O}_{\mathbb{K}},\ Tr_{\mathbb{K}|\mathbb{Q}}(x\alpha) \in \mathbb{Z}\}$ of $\mathcal{O}_{\mathbb{K}}$.

Let $\zeta = \zeta_m \in \mathbb{C}$ be a primitive m-th root of unity. We consider here the *cyclotomic field* $\mathbb{Q}(\zeta)$ and its subfield $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$. We have that $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(m)/2$, where φ is the Euler function; $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$; $d_{\mathbb{K}} = p^{\frac{p-3}{2}}$ if $m = p$, p prime, $p \geqslant 5$ and $d_{\mathbb{K}} = 2^{(r-1)2^{r-2}-1}$ if $m = 2^r$.

3. Ideal lattices

The construction of ideal lattices presented here was introduced in [2] and [3].

From now on, let $\mathbb{K}$ be a totally real number field. Let $\alpha \in \mathbb{K}$ such that $\alpha_i = \sigma_i(\alpha) > 0$ for all $i = 1, \ldots, n$. The homomorphism

$$\begin{aligned} \sigma_\alpha : \mathbb{K} &\longrightarrow \mathbb{R}^n \\ x &\longmapsto \left(\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x)\right) \end{aligned}$$

is called *twisted homomorphism*. When $\alpha = 1$ the twisted homomorphism is the *Minkowski homomorphism*.

It can be shown that if $I \subseteq \mathbb{K}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1, \dots, w_n\}$, then the image $\Lambda = \sigma_\alpha(I)$ is a lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(w_1), \dots, \sigma_\alpha(w_n)\}$, or equivalently with generator matrix $\boldsymbol{M} = (\sigma_\alpha(w_{ij}))_{i,j=1}^n$ where $w_i = (w_{i1}, \dots, w_{in})$ for all $i = 1, \dots, n$. Moreover, if $\alpha I\bar{I} \subseteq \Delta(\mathbb{K}|\mathbb{Q})^{-1}$ where $\bar{I}$ denote the complex conjugation of I, then $\sigma_\alpha(I)$ is an integer lattice. Since $\mathbb{K}$ is totally real, the associated Gram matrix of $\sigma_\alpha(I)$ is $\boldsymbol{G} = \boldsymbol{M}.\boldsymbol{M}^t = (Tr_{\mathbb{K}|\mathbb{Q}}(\alpha w_i \overline{w_j}))_{i,j=1}^n$ [6].

Proposition 3.1. *(See [2].) If $I \subseteq \mathbb{K}$ is a fractional ideal, then for $\Lambda = \sigma_\alpha(I)$ and $det(\Lambda) = det(G)$, we have:*

$$det(\Lambda) = det(G) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d_{\mathbb{K}}|. \tag{1}$$

Proposition 3.2. *Let $\mathbb{K}$ be a totally real field number with $[\mathbb{K}:\mathbb{Q}] = n$ and $I \subseteq \mathbb{K}$ a free $\mathbb{Z}$-module of rank n. The minimum product distance of $\Lambda = \sigma_\alpha(I)$ is*

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

Proof. The proof is straightforward. □

Proposition 3.3. *(See [6].) If $\mathbb{K}$ is a totally real field number and $I \subseteq \mathcal{O}_{\mathbb{K}}$ is a principal ideal then*

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

Definition 3.4. The *relative minimum product distance* of Λ, denoted by $\boldsymbol{d}_{p,rel}(\Lambda)$, is the minimum product distance of a scaled version of Λ with unitary minimum norm vector.

4. Rotated D_n-lattices for $n = 2^{r-2}$, $r \geqslant 5$ via $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$

In this section we will present some families of rotated D_n-lattices using ideals and modules in the totally real number field $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$. One of the strategies to construct these lattices was to start from the standard characterization of D_n as generated by the basis

$$\beta = \{(-1, -1, 0, \dots, 0), (1, -1, 0, \dots, 0), \dots, (0, 0, \dots, 1, -1)\}. \tag{4}$$

We derive in 4.2 a rotated D_n-lattice as a sublattice of the rotated $\mathbb{Z}^n$ algebraic constructions presented in [1,6,5]. Another strategy explored next in 4.1 is to investigate the necessary condition given in Proposition 3.1, for the existence of rotated D_n-lattices.

Let $\zeta = \zeta_{2^r}$ be a primitive 2^r-th root of unity, $m = 2^r$, $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$ and $n = [\mathbb{K}:\mathbb{Q}] = 2^{r-2}$.

4.1. A first construction

Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ and $I \subseteq \mathcal{O}_{\mathbb{K}}$ an ideal. If $\sigma_\alpha(I)$ is a rotated D_n-lattice scaled by $\sqrt{c}$, then $det(\sigma_\alpha(I)) = 4c^n$. Based on Proposition 3.1, taking $I = \mathcal{O}_{\mathbb{K}}$ and $c = 2^{r-1}$, since $d_{\mathbb{K}} = 2^{(r-1)2^{r-2}-1}$ and $n = 2^{r-2}$ it follows that a necessary condition to construct a rotated D_n-lattice $\sigma_\alpha(I)$ is to find an element $\alpha \in \mathcal{O}_{\mathbb{K}}$ such that $N(\alpha) = 8$. Table 1 shows some elements $\alpha \in \mathcal{O}_{\mathbb{K}}$ such that $N(\alpha) = 8$ in low dimensions. From it we got the suggestion for a general expression for α as

$$\alpha = 4 + (\zeta_{2^r} + \zeta_{2^r}^{-1}) - 2(\zeta_{2^r}^2 + \zeta_{2^r}^{-2}) - (\zeta_{2^r}^3 + \zeta_{2^r}^{-3}) \tag{5}$$

and then derive Proposition 4.3.

Table 1
Some elements $\alpha \in \mathcal{O}_{\mathbb{K}}$ such that $N(\alpha) = 8$.

r	α	$N(\alpha)$
4	$4 + (\zeta_{16} + \zeta_{16}^{-1}) - 2(\zeta_{16}^2 + \zeta_{16}^{-2}) - (\zeta_{16}^3 + \zeta_{16}^{-3})$	8
5	$4 + (\zeta_{32} + \zeta_{32}^{-1}) - 2(\zeta_{32}^2 + \zeta_{32}^{-2}) - (\zeta_{32}^3 + \zeta_{32}^{-3})$	8
6	$4 + (\zeta_{64} + \zeta_{64}^{-1}) - 2(\zeta_{64}^2 + \zeta_{64}^{-2}) - (\zeta_{64}^3 + \zeta_{64}^{-3})$	8

To prove that $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I)$ is a rotated D_n-lattice we need the next preliminary results.

Proposition 4.1. *(See [1].) If $\zeta = \zeta_{2^r}$ and $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, then*

$$Tr_{\mathbb{K}|\mathbb{Q}}\left(\zeta^k + \zeta^{-k}\right) = \begin{cases} 0, & \text{if } gcd(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & \text{if } gcd(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & \text{if } gcd(k, 2^r) = 2^r. \end{cases}$$

Proposition 4.2. *If $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, $e_0 = 1$ and $e_i = \zeta^i + \zeta^{-i}$ for $i = 1, \ldots, 2^{r-2} - 1$, then*

(a)

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i e_i) = \begin{cases} 2^r, & \text{if } i = 0, 1; \\ 2^{r+1}, & \text{if } 2 \leqslant i < 2^{r-2} - 1; \\ 3.2^r, & \text{if } i = 2^{r-2} - 1. \end{cases}$$

(b)

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i e_0) = \begin{cases} 2^{r-1}, & \text{if } i = 1; \\ -2^r, & \text{if } i = 2; \\ -2^{r-1}, & \text{if } i = 3; \\ 0, & \text{if } 3 < i \leqslant 2^{r-2} - 1. \end{cases}$$

(c) *If $0 < i < j \leqslant 2^{r-2} - 1$ then*

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i e_j) = \begin{cases} 2^{r-1}, & \text{if } |i-j| = 1 \text{ and } (i, j) \notin \{(1, 2), (2^{r-2} - 2, 2^{r-2} - 1)\}; \\ -2^r, & \text{if } |i-j| = 2; \\ -2^{r-1}, & \text{if } |i-j| = 3; \\ 2^r, & \text{if } (i, j) = (2^{r-2} - 2, 2^{r-2} - 1); \\ 0, & \text{otherwise}. \end{cases}$$

Proof. The proof is straightforward by calculating the $gcd(k, 2^r)$ for some values of k and applying Proposition 4.1. For $0 < i < j \leqslant 2^{r-2} - 1$ we have:

$$\begin{aligned} Tr(\alpha e_i e_i) = {} & Tr(8) + 4\,Tr\left(\zeta^{2i} + \zeta^{-2i}\right) + 2\,Tr\left(\zeta + \zeta^{-1}\right) + Tr\left(\zeta^{2i+1} + \zeta^{-2i-1}\right) \\ & + Tr\left(\zeta^{2i-1} + \zeta^{-(2i-1)}\right) - 4\,Tr\left(\zeta^2 + \zeta^{-2}\right) - 2\,Tr\left(\zeta^{2i+2} + \zeta^{-(2i+2)}\right) \\ & - 2\,Tr\left(\zeta^{2i-2} + \zeta^{-(2i-2)}\right) - 2\,Tr\left(\zeta^3 + \zeta^{-3}\right) \\ & - Tr\left(\zeta^{2i+3} + \zeta^{-(2i+3)}\right) - Tr\left(\zeta^{2i-3} + \zeta^{-(2i-3)}\right). \end{aligned}$$

For $2 \leqslant i < 2^{r-2} - 1$ since $gcd(k, 2^r) < 2^{r-1}$ for $k = 2i, 2i \pm 1, 2i \pm 2, 2i \pm 3$ it follows that $Tr(\alpha e_i e_i) = 2^{r+1}$. For $i = 1, 2^{r-2} - 1$ the development is analogous. For $i = 0$ we have:

$$Tr(\alpha e_0 e_0) = Tr(4) + Tr\big(\zeta + \zeta^{-1}\big) - 2\,Tr\big(\zeta^2 + \zeta^{-2}\big) - Tr\big(\zeta^3 + \zeta^{-3}\big) = 2^r$$

and then it follows (a).

$$\begin{aligned} Tr(\alpha e_i e_0) = {} & 4\,Tr\big(\zeta^{i} + \zeta^{-i}\big) + Tr\big(\zeta^{i+1} + \zeta^{-(i+1)}\big) + Tr\big(\zeta^{i-1} + \zeta^{-(i-1)}\big) \\ & - 2\,Tr\big(\zeta^{i+2} + \zeta^{-(i+2)}\big) - 2\,Tr\big(\zeta^{i-2} + \zeta^{-(i-2)}\big) \\ & - Tr\big(\zeta^{i+3} + \zeta^{-(i+3)}\big) - Tr\big(\zeta^{i-3} + \zeta^{-(i-3)}\big). \end{aligned}$$

For $i \neq 1, 2, 3$, since $gcd(k, 2^r) < 2^{r-1}$ for $k = i, i \pm 1, i \pm 2, i \pm 3$ then $Tr(\alpha e_i e_0) = 0$.

For $i = 1, 2, 3$ using $Tr(\zeta^0 + \zeta^0) = 2^{r-1}$ it follows (b).

$$\begin{aligned} Tr(\alpha e_i e_j) = {} & 4\,Tr\big(\zeta^{i+j} + \zeta^{-(i+j)}\big) + 4\,Tr\big(\zeta^{i-j} + \zeta^{-(i-j)}\big) + Tr\big(\zeta^{i+j+1} + \zeta^{-(i+j+1)}\big) \\ & + Tr\big(\zeta^{i-j+1} + \zeta^{-(i-j+1)}\big) + Tr\big(\zeta^{i+j-1} + \zeta^{-(i+j-1)}\big) + Tr\big(\zeta^{i-j-1} + \zeta^{-(i-j-1)}\big) \\ & - 2\,Tr\big(\zeta^{i+j+2} + \zeta^{-(i+j+2)}\big) - 2\,Tr\big(\zeta^{i-j+2} + \zeta^{-(i-j+2)}\big) - 2\,Tr\big(\zeta^{i+j-2} + \zeta^{-(i+j-2)}\big) \\ & - 2\,Tr\big(\zeta^{i-j-2} + \zeta^{-(i-j-2)}\big) - Tr\big(\zeta^{i+j+3} + \zeta^{-(i+j+3)}\big) - Tr\big(\zeta^{i-j+3} + \zeta^{-(i-j+3)}\big) \\ & - Tr\big(\zeta^{i+j-3} + \zeta^{-(i+j-3)}\big) - Tr\big(\zeta^{i-j-3} + \zeta^{-(i-j-3)}\big). \end{aligned}$$

Since $gcd(k, 2^r) < 2^{r-1}$ for $k = i \pm j, i + j \pm 1, i + j \pm 2$; $gcd(i + j + 3, 2^r) < 2^{r-1}$ for $i + j \neq 2^{r-1} - 3$; $gcd(i + j + 3, 2^r) = 2^{r-1}$, for $i + j = 2^{r-1} - 3$; $gcd(i + j - 3, 2^r) < 2^{r-1}$, for $i + j \neq 3$ and

$$Tr\big(\zeta^{i-j+1} + \zeta^{-(i-j+1)}\big) + Tr\big(\zeta^{i-j-1} + \zeta^{-(i-j-1)}\big) = \begin{cases} 2^{r-1}, & \text{if } |i-j| = 1; \\ 0, & \text{otherwise}, \end{cases}$$

$$Tr\big(\zeta^{i-j+2} + \zeta^{-(i-j+2)}\big) + Tr\big(\zeta^{i-j-2} + \zeta^{-(i-j-2)}\big) = \begin{cases} 2^{r-1}, & \text{if } |i-j| = 2; \\ 0, & \text{otherwise}, \end{cases}$$

$$Tr\big(\zeta^{i-j+3} + \zeta^{-(i-j+3)}\big) + Tr\big(\zeta^{i-j-3} + \zeta^{-(i-j-3)}\big) = \begin{cases} 2^{r-1}, & \text{if } |i-j| = 3; \\ 0, & \text{otherwise}, \end{cases}$$

it follows (c). □

Proposition 4.3. *The lattice* $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}}) \subseteq \mathbb{R}^{2^{r-2}}$, $\alpha = 4 + (\zeta_{2^r} + \zeta_{2^r}^{-1}) - 2(\zeta_{2^r}^2 + \zeta_{2^r}^{-2}) - (\zeta_{2^r}^3 + \zeta_{2^r}^{-3})$ *is a rotated* D_n*-lattice for* $n = 2^{r-2}$.

Proof. The Gram matrix for $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ related to the $\mathbb{Z}$-basis $\{e_0, e_1, \ldots, e_{n-1}\}$ is

$$\boldsymbol{G} = \begin{pmatrix} 2 & 1 & -2 & -1 & 0 & \cdots & & & & \cdots & 0 \\ 1 & 2 & 0 & -2 & -1 & 0 & & & & & \vdots \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 & \vdots \\ & & & & \ddots & 0 & -1 & -2 & 1 & 4 & 2 \\ 0 & \vdots & & & & \cdots & 0 & -1 & -2 & 2 & 6 \end{pmatrix}$$

and it is easy to see that $\boldsymbol{G}$ is the Gram matrix for D_n related to the generator matrix $\boldsymbol{TB}$ where $\boldsymbol{T} = (t_{ij})$ of order $2^{r-2} \times 2^{r-2}$ is defined as

$$t_{ij} = \begin{cases} (-1)^{j+1}, & \text{if } i = 2^{r-2} - j + 1,\ 1 \leqslant j \leqslant 2^{r-2}; \\ (-1)^j, & \text{if } i = 2^{r-2} - j + 3,\ 3 \leqslant j \leqslant 2^{r-2}; \\ -1, & \text{if } (i, j) = (2^{r-2}, 2); \\ 0, & \text{otherwise}, \end{cases}$$

$$\boldsymbol{T} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & -1 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & -1 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $\boldsymbol{B}$ is the standard generator matrix for D_n given by basis β (4). So, since lattices with the same Gram matrix must be Euclidean equivalent, then $\sigma_\alpha(I)$ is a rotated D_n-lattice. □

We determine next the relative minimum product distance of the rotated D_n-lattice considered in Proposition 4.3.

Using Propositions 3.1 and 4.3 we conclude:

Corollary 4.4. *If $m = 2^r$, $r \geqslant 4$, $\mathbb{K} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ and $\alpha = 4 + (\zeta_{2^r} + \zeta_{2^r}^{-1}) - 2(\zeta_{2^r}^2 + \zeta_{2^r}^{-2}) - (\zeta_{2^r}^3 + \zeta_{2^r}^{-3})$ then $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = 8$.*

Proposition 4.5. *For $n = 2^{r-2}$, if $\Lambda = \frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ and α as in (5) then the lattice relative minimum product distance is*

$$\boldsymbol{d}_{p,rel}\left(\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})\right) = 2^{\frac{3-rn}{2}}.$$

Proof. The minimum norm of the standard D_n is $\sqrt{2}$. Since $\mathcal{O}_{\mathbb{K}}$ is a principal ideal, using Proposition 3.3 we have $d_{p,min}(\sigma_\alpha(\mathcal{O}_{\mathbb{K}})) = \sqrt{N(\alpha)N(\mathcal{O}_{\mathbb{K}})^2}$. Since $N(\alpha) = 8$ and $N(\mathcal{O}_{\mathbb{K}}) = 1$, then

$$\boldsymbol{d}_{p,rel}\left(\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})\right) = \frac{1}{\sqrt{2}^n}\frac{1}{\sqrt{2^{r-1}}^n}\sqrt{8} = \frac{\sqrt{8}}{2^{r\frac{n}{2}}} = 2^{\frac{3-rn}{2}}. \qquad \square$$

4.2. A second construction

In [5] and [1] families of rotated $\mathbb{Z}^n$-lattices obtained as image of a twisted homomorphism applied to $\mathbb{Z}[\zeta + \zeta^{-1}]$ and having full diversity are constructed. Those constructions consider $\alpha = 2 + e_1$ and $\alpha = 2 - e_1$, respectively, and generate equivalent lattices in the Euclidean metric by permutations and coordinate signal changes.

We will use in our construction the rotated $\mathbb{Z}^n$-lattice $\Lambda = \frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I)$ with $\alpha = 2 + e_1$ and $I = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$, and then consider D_n as a sublattice of Λ.

If $e_0 = 1$ and $e_i = \zeta^i + \zeta^{-i}$ for $i = 1, \ldots, 2^{r-2} - 1$, by [5] a generator matrix for the rotated $\mathbb{Z}^n$-lattice $\Lambda = \frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is $\boldsymbol{M}_1 = \frac{1}{\sqrt{2^{r-1}}}\boldsymbol{N}\boldsymbol{A}$, where $\boldsymbol{N} = \sigma_j(e_{i-1})_{i,j=1}^n$ and $\boldsymbol{A} = diag(\sqrt{\sigma_k(\alpha)})$. Let $\boldsymbol{T}$ the basis change matrix

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

For $\boldsymbol{M} = \boldsymbol{T}\boldsymbol{M}_1$, $\boldsymbol{G} = \boldsymbol{M}\boldsymbol{M}^t = \boldsymbol{I}_n$ and we will consider the standard lattice $D_n \subseteq \mathbb{Z}^n$ rotated by $\boldsymbol{M}$.

Proposition 4.6. *Let $I \subseteq \mathcal{O}_{\mathbb{K}}$ be the $\mathbb{Z}$-module with $\mathbb{Z}$-basis*

$$\left\{-2e_0 + 2e_1 - 2e_2 + \cdots - 2e_{n-2} + e_{n-1}, -e_{n-1}, e_{n-2}, \ldots, (-1)^{i+1}e_{n-1-i}, \ldots, e_2, -e_1\right\}$$

and $\alpha = 2 + e_1$. The lattice $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I) \subseteq \mathbb{R}^{2^{r-2}}$ is a rotated D_n-lattice.

Proof. Let $\boldsymbol{B}$ be the generator matrix of D_n associated to the basis β (4). Using homomorphism properties, a straightforward computation shows that

$$\boldsymbol{B}\boldsymbol{M} = \frac{1}{\sqrt{2^{r-1}}}\begin{pmatrix} \sigma_1(-2e_0 + 2e_1 - 2e_2 + \cdots - 2e_{n-2} + e_{n-1}) & \cdots & \sigma_n(-2e_0 + 2e_1 - 2e_2 + \cdots - 2e_{n-2} + e_{n-1}) \\ \sigma_1(-e_{n-1}) & \cdots & \sigma_n(-e_{n-1}) \\ \sigma_1(e_{n-2}) & \cdots & \sigma_n(e_{n-2}) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_2) & \cdots & \sigma_n(-e_2) \\ \sigma_1(-e_1) & \cdots & \sigma_n(-e_1) \end{pmatrix}\boldsymbol{A}$$

is a generator matrix for $\frac{1}{\sqrt{2^{r-1}}}\sigma_\alpha(I)$. This lattice is a rotated D_n-lattice since $\boldsymbol{B}\boldsymbol{M}(\boldsymbol{B}\boldsymbol{M})^t = \boldsymbol{B}\boldsymbol{B}^t$ is the standard Gram matrix of D_n relative to the basis β. $\square$

We show next that the rotated D_n-lattice of the last proposition is associated to a principal ideal of $\mathcal{O}_{\mathbb{K}}$ and then calculate its relative minimum product distance.

Table 2
Relative product distance and center density of rotated $\mathbb{Z}^n$ and D_n-lattices, $n = 2^{r-2}$.

r	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(D_n)$
4	4	0.385553	0.324210	0.062500	0.125000
5	8	0.261068	0.201311	0.003906	0.031250
6	16	0.180648	0.133393	0.000015	0.001953
7	32	0.126361	0.091307	2.3×10^{-10}	7.6×10^{-6}
8	64	0.088868	0.063523	5.4×10^{-20}	1.1×10^{-10}
9	128	0.062669	0.044554	2.9×10^{-39}	2.7×10^{-20}

Proposition 4.7. *Let I be the $\mathbb{Z}$-module given in Proposition 4.6. Then I is a principal ideal and $I = e_1\mathcal{O}_{\mathbb{K}}$.*

Proof. It is easy to see that $I = 2e_0\mathbb{Z} + e_1\mathbb{Z} + \cdots + e_{n-1}\mathbb{Z}$. Let $x \in e_1\mathcal{O}_{\mathbb{K}}$. Then $x = e_1(a_0e_0 + a_1e_1 + a_2e_2 + \cdots + a_{n-1}e_{n-1}) = a_0(e_1) + a_1(e_2 + 2e_0) + a_2(e_3 + e_{-1}) + \cdots + a_{n-1}(e_n + e_{-n+2}) = a_1(2e_0) + (a_0 + a_2)(e_1) + (a_1 + a_3)(e_2) + \cdots + (a_{n-2})(e_{n-1}) \in I$. Now, if $x \in I$, then $x = a_0 2e_0 + a_1e_1 + \cdots + a_{n-1}e_{n-1} = (e_1)[a_0e_1 + a_1e_2 + (a_2 - a_0)e_3 + (a_3 - a_1)e_4 + (a_4 - a_2 - a_0)e_5 + (a_5 - a_3 - a_1)e_6 + \cdots + (a_{n-1})e_{n-2} + (a_{n-2} - a_{n-4} \cdots - a_0)e_{n-1}] \in e_1\mathcal{O}_{\mathbb{K}}$. So, I is a principal ideal of $\mathcal{O}_{\mathbb{K}}$. □

Remark 4.8. It follows from Proposition 3.3 and Definition 3.4 that the relative minimum product distance of D_n-lattices constructed from principal ideals in $\mathcal{O}_{\mathbb{K}} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, $m = 2^r$, $r \geqslant 5$, depends only of the determinant of D_n and of the discriminant of $\mathbb{K}$. Therefore for any construction of a rotated D_n lattice from a principal ideal I in $\mathcal{O}_{\mathbb{K}}$ the relative minimum product distance is $d_{p,rel}(\sigma_\alpha(I)) = 2^{\frac{3-rn}{2}}$.

It is also interesting to note that besides being Euclidean equivalent, the lattices obtained through the first and second constructions are equivalent in the sum l_1-metric in $\mathbb{R}^n$ (which can be used in the lattice decoding process), since the isometry is a composition of permutations and coordinate signal changes.

The density $\Delta(\Lambda)$ of a lattice $\Lambda \subseteq \mathbb{R}^n$ is given by $\Delta(\Lambda) = \frac{(d/2)^n \, Vol(B(1))}{det(\Lambda)^{1/2}}$ where $Vol(B(1))$ is the volume of the unitary sphere in $\mathbb{R}^n$ and d is the minimum norm of Λ. The parameter $\delta(\Lambda) = \frac{(d/2)^n}{det(\Lambda)^{1/2}}$ is so called center density. Table 2 shows a comparison between the normalized $d_{p,rel}$ and the center density of rotated $\mathbb{Z}^n$-lattices constructed in [5] and rotated D_n-lattices constructed here via principal ideals in $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, $n = 2^{r-2}$. Asymptotically we have

$$\lim_{n \longrightarrow \infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2} \quad \text{and} \quad \lim_{n \longrightarrow \infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0. \tag{6}$$

If the goal is to construct lattices which have good performance on both Gaussian and Rayleigh channels, we may assert that taking into account the trade-off density versus product distance, there is some advantages in considering these rotated D_n-lattices instead of rotated $\mathbb{Z}^n$-lattices, $n = 2^{r-2}$, $r \geqslant 5$, in high dimensions.

5. Rotated D_n-lattices for $n = \frac{p-1}{2}$, p prime, via $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$

Let $\zeta = \zeta_p$ be a primitive p-th root of unity, p prime, $\mathbb{L} = \mathbb{Q}(\zeta)$ and $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$. We will construct a family of rotated D_n-lattices, derived from the construction of a rotated $\mathbb{Z}^n$-lattice in [6], via a $\mathbb{Z}$-module that is not an ideal. Let $e_j = \zeta^j + \zeta^{-j}$ for $j = 1, \ldots, (p-1)/2$.

By [6] a generator matrix of the rotated $\mathbb{Z}^n$-lattice $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is $\boldsymbol{M} = \frac{1}{\sqrt{p}}\boldsymbol{TNA}$, where $\boldsymbol{T} = (t_{ij})$ is an upper triangular matrix with $t_{ij} = 1$ if $i \leqslant j$, $\boldsymbol{N} = (\sigma_j(e_i))_{i,j=1}^n$ and $\boldsymbol{A} = diag(\sqrt{\sigma_k(\alpha)})$. We have $\boldsymbol{G} = \boldsymbol{MM}^t = \boldsymbol{I}_n$ [6].

Table 3
Relative product distance and center density of rotated $\mathbb{Z}^n$ and D_n-lattices, $n=(p-1)/2$, p prime.

p	n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(D_n)$
11	5	0.38321	0.27097	0.03125	0.08838
13	6	0.34344	0.24285	0.01563	0.06250
17	8	0.28952	0.20472	0.00390	0.03125
19	9	0.27187	0.19105	0.00195	0.02209
23	11	0.24045	0.17003	0.00049	0.01105

Proposition 5.1. *Let $I \subseteq \mathcal{O}_{\mathbb{K}}$ be a $\mathbb{Z}$-module with $\mathbb{Z}$-basis*

$$\{-e_1 - 2e_2 - \cdots - 2e_n, e_1, e_2, \ldots, e_{n-1}\}$$

and $\alpha = 2 - e_1$. The lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(I) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ is a rotated D_n-lattice.

Proof. Let $\boldsymbol{B}$ be a generator matrix for D_n given by basis β (4). Using homomorphism properties, a straightforward computation shows that $\boldsymbol{BM}$ is a generator matrix for $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(I)$. This lattice is a rotated D_n since $\boldsymbol{BM}(\boldsymbol{BM})^t = \boldsymbol{BB}^t$ is a Gram matrix of D_n. It has full diversity since it is contained in $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ [6]. □

Proposition 5.2. *The $\mathbb{Z}$-module $I \subseteq \mathcal{O}_{\mathbb{K}}$ is not an ideal of $\mathcal{O}_{\mathbb{K}}$.*

Proof. The set $\{e_1, e_2, \ldots, e_{n-1}, 2e_n\}$ is an another $\mathbb{Z}$-basis to I. We will show that e_n is not in I. Indeed, if $e_n \in I$, then $I = \mathcal{O}_{\mathbb{K}}$, but $|\frac{\mathcal{O}_{\mathbb{K}}}{I}| = 2$. So, $e_n \notin I$. $e_{n-1}e_1$ is not in I. In fact, note that $e_{n-1}e_1 = e_n + e_{n-2}$ and $e_{n-2} \in I$. If $e_{n-1}e_1 \in I$, then $e_n = e_{n-1}e_1 - e_{n-2} \in I$, and this doesn't happen. □

Proposition 5.3. *If $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(I) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ with α and I as in Proposition 5.1, then the relative minimum product distance is*

$$\boldsymbol{d}_{p,rel}(\Lambda) = 2^{\frac{1-p}{4}} p^{\frac{3-p}{4}}.$$

Proof. First note that $|N(e_1)| = 1$. Indeed, $(\zeta + \zeta^{-1})(-\zeta^{p-1} - \zeta^{p-2} - \cdots - \zeta - 1) = 1$ and so

$$N(\zeta + \zeta^{-1})N(-\zeta^{p-1} - \zeta^{p-2} - \cdots - \zeta - 1) = N(1) = 1.$$

Since $e_1 \in \mathcal{O}_{\mathbb{K}}$, then $N(e_1) \in \mathbb{Z}$, what implies $|N(e_1)| = 1$. Now, the minimum norm in D_n is $\sqrt{2}$. By Proposition 3.2, $\boldsymbol{d}_p(\sigma_\alpha(I)) = \sqrt{N(\alpha)}\min_{0\neq y\in I}|N(y)| = \sqrt{p}$, since $\min_{0\neq y\in I}|N(y)| = 1$. Therefore, the relative minimum product distance is

$$d_{p,rel}\left(\frac{1}{\sqrt{p}}\sigma_\alpha(I)\right) = \left(\frac{1}{\sqrt{p}^{\frac{p-1}{2}}}\right)\left(\frac{1}{\sqrt{2}^{\frac{p-1}{2}}}\right)\sqrt{p} = 2^{\frac{1-p}{4}} p^{\frac{3-p}{4}}. \qquad \square$$

Table 3 shows a comparison between the normalized $d_{p,rel}$ and the center density δ of rotated $\mathbb{Z}^n$-lattices constructed in [6] and rotated D_n-lattices constructed here, $n = (p-1)/2$. As in Section 6 we also have for $\Lambda = \frac{1}{\sqrt{p}}(\sigma_\alpha(I)) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ and p prime, the following results:

$$\lim_{n\longrightarrow\infty} \frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2} \quad \text{and} \quad \lim_{n\longrightarrow\infty} \frac{\delta(\mathbb{Z}^n)}{\delta(D_n)} = 0.$$

6. Conclusion

In this work we construct some families of full diversity rotated D_n-lattices for $n = 2^{r-2}$, $r \geqslant 5$ and $n = \frac{p-1}{2}$, p prime, $p \geqslant 7$ through cyclotomic fields and derive their relative minimum product distance. A comparison between these lattices and rotated $\mathbb{Z}^n$-lattices is also presented.

Acknowledgment

The authors would like to thank the referee for the very pertinent comments and suggestions.

References

[1] A.A. Andrade, C. Alves, T.B. Carlos, Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$, Int. J. Appl. Math. 19 (3) (2006) 321–331.
[2] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. 241 (1999) 69–84.
[3] E. Bayer-Fluckiger, Ideal lattices, in: Proceedings of the Conference Number Theory and Diophantine Geometry, Zürich, 1999, Cambridge Univ. Press, 2002, pp. 168–184.
[4] E. Bayer-Fluckiger, Upper bounds for Euclidean minima of algebraic number fields, J. Number Theory 121 (2) (2006) 305–323.
[5] E. Bayer-Fluckiger, G. Nebe, On the Euclidean minimum of some real number fields, J. Theor. Nombres Bordeaux 17 (2) (2005) 437–454.
[6] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel, IEEE Trans. Inform. Theory 50 (4) (2004) 702–714.
[7] E. Bayer-Fluckiger, I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, Arch. Math. 86 (3) (2006) 217–225.
[8] 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.
[9] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag, 1988.
[10] J.O.D. Lopes, Discriminants of subfields of $\mathbb{Q}(\zeta_{2^r})$, J. Algebra Appl. 2 (2003) 463–469.
[11] D. Micciancio, S. Goldwasser, Complexity of Lattice Problems: A Cryptographic Perspective, Kluwer Internat. Ser. Engrg. Comput. Sci., vol. 671, Kluwer Academic Publishers, 2002.
[12] P. Samuel, Algebraic Theory of Numbers, Hermann, Paris, 1970.
[13] I.N. Stewart, D.O. Tall, Algebraic Number Theory, Chapman & Hall, London, 1987.
[14] L.C. Washington, Introduction to Ciclotomic Fields, Springer-Verlag, New York, 1982.