Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 168–172*

Rotated D_n-lattices via $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, p prime [1]

Grasiele C. Jorge grajorge@ime.unicamp.com
University of Campinas, São Paulo, Brazil
Sueli I. R. Costa sueli@ime.unicamp.br
University of Campinas, São Paulo, Brazil

Abstract. We construct a family of rotated D_n-lattices with full diversity via $\mathbb{Z}$-modules of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, p prime, and obtain a closed-form for their minimum product distance. These lattices can be good for signal transmission over both Gaussian and Rayleigh fading channels. We show also that for some values of p it is impossible to construct these lattices via ideals of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

1 Introduction

Signal constellations having lattice structure have been studied as meaningful means for signal transmission over both Gaussian and single-antenna Rayleigh fading channel [1]. Usually the problem of finding good lattice signal constellations for a Gaussian channel is associated to the search for high packing density [2] and for a Rayleigh fading channel the efficiency, measured by a lower error probability in the transmission, is strongly related to the lattice diversity and its minimum product distance [5].

A lattice $\Lambda \subseteq \mathbb{R}^n$ is a discrete additive group. Its packing density is the proportion of the space covered by congruent disjoint spheres of maximum radius. Its diversity m is the maximum number such that there are at least m nonzero coordinates in each nonzero vector. For a full diversity lattice, the minimum product distance is the minimum among all product of the absolute values of the nonzero vector coordinates. For general lattices, the packing density and product distance are usually hard to estimate. They can be obtained in certain cases of algebraic lattices through algebraic properties.

In this work we attempt to consider lattices which are feasible for both channels by constructing rotated D_n-lattices in $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ via $\mathbb{Z}$-modules $I \subseteq \mathcal{O}_{\mathbb{K}}$ of rank $n = [\mathbb{K} : \mathbb{Q}]$, with full diversity and get a closed-form for their minimum product distance. We prove that these modules I are not ideals and that also for some values of p it is impossible to reproduce such rotated D_n-lattices via ideals of $\mathcal{O}_{\mathbb{K}}$. If it was possible to reproduce these lattices via principal ideals we would have twice the minimum product distance obtained in our construction.

[1]This work was partially supported by CNPq 140239/2009-0, CAPES 2548/2010, CNPq 309561/2009-4 and FAPESP 2007/56052-8

As it is known, a D_n lattice has better packing density when compared to $\mathbb{Z}^n$ and we could show for these constructions a good trade-off concerning the packing density versus the product distance when compared to previous constructed rotated $\mathbb{Z}^n$-lattices.

2 Number fields and ideal lattices

We summarize next some concepts and results of algebraic number theory and ideal lattices. The results presented here can be found in [7], [8], [9], [3] and [4].

Let $\mathbb{K}$ be a number field of degree n and $\mathcal{O}_{\mathbb{K}}$ its ring of integers. 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 $i = 1, \cdots, n$.

Given $x \in \mathbb{K}$, the value $N(x) = \prod_{i=1}^n \sigma_i(x)$ is called, *norm* of x in $\mathbb{K}|\mathbb{Q}$. It can shown that if $x \in \mathcal{O}_{\mathbb{K}}$, then $N(x) \in \mathbb{Z}$. The *norm* of an ideal $I \subseteq \mathcal{O}_{\mathbb{K}}$ is defined as $N(I) = |\mathcal{O}_{\mathbb{K}}/I|$.

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 $\mathbb{K}$.

For $\zeta = \zeta_m \in \mathbb{C}$ 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 remark that $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(m)/2$, where φ is the Euler function, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$ and $d_{\mathbb{K}} = p^{\frac{p-3}{2}}$ if $m = p$, p prime.

The construction of ideal lattices presented here was introduced in [3] and [4]. 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 $i = 1, \cdots, n$. 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.*

It can be shown that if $I \subseteq \mathbb{K}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1, \ldots, w_n\}$, then the image $\Lambda = \sigma_\alpha(I)$ is a lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(w_1), \ldots, \sigma_\alpha(w_n)\}$, or equivalently with generator matrix $\boldsymbol{M} = (\sigma_\alpha(w_{ij}))_{i,j=1}^n$ where $w_i = (w_{i1}, \cdots, w_{in})$ for all $i = 1, \cdots, n$.

Proposition 2.1. *[3] If $I \subseteq \mathbb{K}$ is a fractional ideal, then for $\Lambda = \sigma_\alpha(I)$ we have $det(\Lambda) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)|d_{\mathbb{K}}|$.*

Proposition 2.2. *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 $d_{p,min}(\Lambda) = \sqrt{N_{\mathbb{K}|\mathbb{Q}}(\alpha)} min_{0 \neq y \in I} |N_{\mathbb{K}|\mathbb{Q}}(y)|$.*

Definition 2.3. 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.

3 Rotated D_n-lattices for $n = \frac{p-1}{2}$, p prime

We consider the D_n lattice generated by the standard basis

$$\beta = \{(-1,-1,0,\cdots,0),(1,-1,0,\cdots,0),\cdots,(0,0,\cdots,1,-1)\}. \quad (1)$$

Let $\zeta = \zeta_p$ be a primitive p-th root of unity, p prime, and $\mathbb{K} = \mathbb{Q}(\zeta+\zeta^{-1})$. We will construct a family of rotated D_n-lattices, derived from the construction of rotated $\mathbb{Z}^n$-lattices in [5], via a $\mathbb{Z}$-module that is not an ideal. Let $e_j = \zeta^j + \zeta^{-j}$ for $j = 1,\cdots,(p-1)/2$.

By [5], 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 $i \leq j$, $\boldsymbol{N} = (\sigma_j(e_i))_{i,j=1}^n$ and $\boldsymbol{A} = diag(\sqrt{\sigma_k(\alpha)})$. We have $\boldsymbol{G} = \boldsymbol{MM}^t = \boldsymbol{I}_n$ [5].

Proposition 3.1. *Let $I \subseteq \mathcal{O}_\mathbb{K}$ be a $\mathbb{Z}$-module with $\mathbb{Z}$-basis*

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

and $\alpha = 2 - e_1$. This $\mathbb{Z}$-module is not an ideal and 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 (1). 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. We remark that I is not an ideal since $e_{n-1}e_1 \notin I$ [6]. ∎

Proposition 3.2. *If $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(I) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ with α and I as in the Proposition 3.1, 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 $|N(e_1)| = 1$. because $(\zeta + \zeta^{-1}) \in \mathcal{O}_\mathbb{K}$ is invertible in $\mathcal{O}_\mathbb{K}$. Now, the minimum norm in D_n is $\sqrt{2}$ and by Proposition 2.2 the result follows. ∎

As a consequence we get a comparison between the minimum product distance of the lattices construct here and rotated $\mathbb{Z}^n$-lattices presented in [5]:

Proposition 3.3. *Considering the rotated $\mathbb{Z}^n$-lattices constructed in [5] and the rotated D_n-lattices constructed here, $n = (p-1)/2$, we have*

$$\lim_{n \longrightarrow \infty} \frac{\sqrt[n]{d_{p,rel}(D_n)}}{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}} = \frac{1}{\sqrt{2}}.$$

Since the packing density of D_n is much higher than the packing density of $\mathbb{Z}^n$, $\frac{\delta(D_n)}{\delta(\mathbb{Z}^n)} = \frac{2^{\frac{-n-2}{2}}}{2^{-n}} = 2^{\frac{n-2}{2}}$, we may say that the above result presents a good trade-off concerning the comparison between the product distance and packing density of the respective lattices.

In what follows we will show that it is impossible to construct rotated D_n lattices via ideals of $\mathcal{O}_{\mathbb{K}}$ for some values of p.

By Proposition (2.1), we have that a necessary condition to construct a rotated D_n-lattice, scaled by $\sqrt{c}$ with $c \in \mathbb{Z}$, via ideals of $\mathcal{O}_{\mathbb{K}}$, is the existence of an ideal $I \subseteq \mathcal{O}_{\mathbb{K}}$ and an element totaly positive α such that

$$4c^n = N(\alpha)N(I)^2|d_{\mathbb{K}}|. \tag{2}$$

Since p is prime we have that $d_{\mathbb{K}} = p^{\frac{p-3}{2}}$ is odd, what implies that

$$\text{or 2 divides } N(\alpha) \text{ or 2 divides } N(I). \tag{3}$$

Proposition 3.4. *Let $2\mathcal{O}_{\mathbb{K}}$ be a prime ideal. If $B \subseteq \mathcal{O}_{\mathbb{K}}$ is an ideal such that 2 divides $N(B)$, then $N(B) = (2^n)^a b$ where $a \geq 1$, b is odd and $n = [\mathbb{K} : \mathbb{Q}]$.*

Proof: Let $B = \prod_{i=1}^{t} P_i^{r_i}$ where P_i are prime ideals of $\mathcal{O}_{\mathbb{K}}$ and r_i are positive integers. Since 2 divides $N(B)$ there is a prime ideal $P \in \{P_i, i = 1, \cdots, t\}$ such that 2 divides $N(P)$. So, P is on the factorization of $2\mathcal{O}_{\mathbb{K}}$ as a product of prime ideals of $\mathcal{O}_{\mathbb{K}}$. Since $2\mathcal{O}_{\mathbb{K}}$ is a prime ideal, then $P = 2\mathcal{O}_{\mathbb{K}}$ and $N(P) = 2^n$. So, since B can have more than one ideal with even norm in its factorization, we have $N(B) = (2^n)^a b$ with $a \geq 1$ and b odd. ∎

Proposition 3.5. *Let $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $p \geq 7$ and $n = [\mathbb{K} : \mathbb{Q}]$. If $2\mathcal{O}_{\mathbb{K}}$ is a prime ideal of $\mathcal{O}_{\mathbb{K}}$, it is impossible to construct a rotated D_n-lattice via a twisted homomorphism applied to ideals of $\mathcal{O}_{\mathbb{K}}$.*

Proof: By Proposition 3.4, any ideal B of $\mathcal{O}_{\mathbb{K}}$ with even norm satisfies $N(B) = (2^n)^a b$ where $a \geq 1$ and b is odd. Note that $N(\alpha) = N(\alpha\mathcal{O}_{\mathbb{K}})$. By (3), we have that or the ideal I or the element α should have even norm. Let $N(I) = (2^n)^{a_1} b_1$ and $N(\alpha) = (2^n)^{a_2} b_2$ with $a_1, a_2 \geq 0$, ($a_1 \neq 0$ or $a_2 \neq 0$), b_1, b_2 odd. We have that

$$N(I)^2 N(\alpha)|d_{\mathbb{K}}| = (2^n)^{2a_1+a_2}(b_1^2 b_2)|d_{\mathbb{K}}| \neq 4c^n \text{ for all } c \in \mathbb{Z}.$$

In fact, if $c = 2^a b$ then $4c^n = (2^n)^a 2^2 b^n$ and the powers of 2 are equal in equality above if and only if $an + 2 = n(2a_1 + a_2)$ what implies that $2 = n(2a_1 + a_2 - a)$. So, or $n = 1$ or $n = 2$, what can not happen. Then, it is impossible to find an ideal I and an element α satisfying the necessary conditions. ∎

Corollary 3.6. *For* $\mathbb{K}_1 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $\mathbb{K}_2 = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, $\mathbb{K}_3 = \mathbb{Q}(\zeta_{14} + \zeta_{14}^{-1})$ *and* $\mathbb{K}_4 = \mathbb{Q}(\zeta_{18} + \zeta_{18}^{-1})$ *it is impossible to construct a rotated* D_3*-lattice via a twisted homomorphism applied to ideals of* $\mathcal{O}_{\mathbb{K}_i}$.

Corollary 3.7. *For* $\mathbb{K}_5 = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ *and* $\mathbb{K}_6 = \mathbb{Q}(\zeta_{22} + \zeta_{22}^{-1})$ *it is impossible to construct rotated* D_5*-lattice via the twisted homomorphism applied to ideals of* $\mathcal{O}_{\mathbb{K}_i}$.

Proof: Since in both cases $2\mathcal{O}_{\mathbb{K}_i}$ is a prime ideal in $\mathcal{O}_{\mathbb{K}_i}$ for all $i = 1, \cdots, 6$, the results follow from Proposition 3.5. ∎

References

[1] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiori, Good lattice constellations for both Rayleigh fading and Gaussian channels. IEEE Trans. Inform. Theory, v.42, n.2, p.502-517, 1996.

[2] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups. Springer-Verlag, 1988.

[3] E. Bayer-Fluckiger, Lattices and number fields, Contemporary Mathematics, v.241, p.69-84, 1999.

[4] E. Bayer-Fluckiger, Ideal lattices, Proceedings of the conference *Number theory and Diophantine Geometry*, Zurich, 1999, Cambridge Univ. Press 2002, 168-184.

[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, v.50, n.4, p.702-714, 2004.

[6] G.C. Jorge, A.J.Ferrari, S.I.R. Costa, Rotated D_n-lattices, submitted.

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

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

[9] L.C. Washington, Introduction to Ciclotomic Fields, New York, Springer-Verlag, 1982.