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

Grasiele C. Jorge - Unicamp-Brazil

Sueli I. R. Costa - Unicamp-Brazil

Algebraic and Combinatorial Coding Theory

ACCT 2012

Goals

- To present a family of rotated D_n-lattices with full diversity via $\mathbb{Z}$-modules of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, p prime;
- To show that it is impossible to construct these lattices via ideals of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Lattices in $\mathbb{R}^n$

- Let $\{v_1, \cdots, v_m\}$, $m \leq n$, be a set of linearly independent vectors in $\mathbb{R}^n$. The set

$$\Lambda = \left\{ \sum_{i=1}^{m} a_i v_i, \text{ where } a_i \in \mathbb{Z}, \ i = 1, \cdots, m \right\}$$

is called lattice.

- The set $\{v_1, \cdots, v_m\}$ is called a basis of Λ.

Determinant

- A matrix M whose rows are these m vectors is said to be a generator matrix of Λ.
- The associated Gram matrix is $G = MM^t$.
- The determinant of Λ is $\det(\Lambda) = \det(G)$.

D_n-lattice

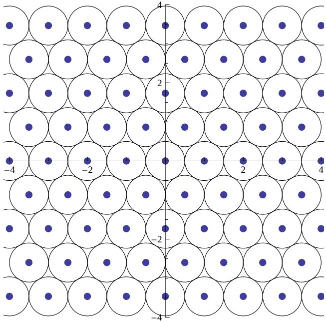
The D_n-**lattice** is defined as

$$D_n = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \text{ is even}\}$$

Packing density

The packing density of a lattice Λ is the proportion of the space $\mathbb{R}^n$ covered by congruent disjoint spheres of maximum radius

$$\rho = \frac{1}{2} min\{d(\mathbf{x}, \mathbf{0}); \mathbf{x} \in \Lambda, \mathbf{x} \neq \mathbf{0}\}.$$



Diversity

Given $\Lambda \subseteq \mathbb{R}^n$ a lattice and $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$.

- The **diversity** of $\mathbf{x}$ is the number of x_i's nonzero.
- The diversity of Λ is $div(\Lambda) = min\{div(\mathbf{x});\ \mathbf{x} \in \Lambda,\ \mathbf{x} \neq \mathbf{0}\}$.
- A full diversity lattice is a lattice such that $div(\Lambda) = n$.

Minimum product distance

Let $\Lambda \subseteq \mathbb{R}^n$ be a full diversity lattice and $\boldsymbol{x} \in \Lambda$.

- The **product distance** of x is $d_p(\boldsymbol{x}) = \prod_{i=1}^{n} |x_i|$.
- The **minimum product distance** of Λ is

$$d_{p,min}(\Lambda) = min\{d_p(\boldsymbol{x}) \mid \boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0}\}.$$

- The relative minimum product distance of Λ, denoted by $d_{p,rel}(\Lambda)$, is the minimum product distance of a scaled version of Λ with minimum Euclidean norm equal to one.

Signal constelattions having structure of lattices can be used for signal transmission over both Gaussian and Rayleigh fading channels.

- Gaussian channel $\Longrightarrow$ high packing density.
- Rayleigh fading channel $\Longrightarrow$ full diversity and high minimum product distance.

In this work we attempt to consider lattices which are feasible for both channels by constructing full diversity rotated D_n-lattices.

- E.B. Fluckiger, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel"
- J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiori, "Good lattice constellations for both Rayleigh fading and Gaussian channels"

First Goal

To construct a family of rotated D_n-lattices via free $\mathbb{Z}$-modules $I \subseteq \mathcal{O}_{\mathbb{K}}$ of rank $n = [\mathbb{K} : \mathbb{Q}]$, $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Number Fields

- A number field $\mathbb{K}$ is a finite extension of $\mathbb{Q}$.
- If $[\mathbb{K} : \mathbb{Q}] = n$, then there are n distinct $\mathbb{Q}$-homomorphisms $\{\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}\}_{i=1}^{n}$.
- If $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ for all $i = 1, \cdots, n$ the number field $\mathbb{K}$ is said totally real.

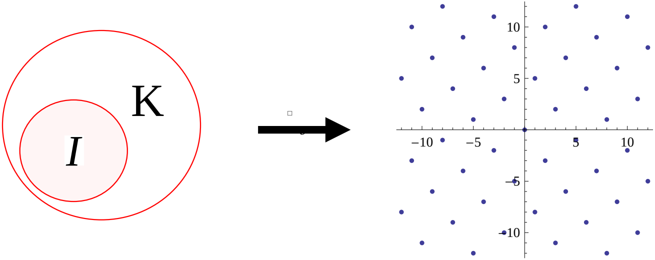
Twisted homomorphism

Let $\mathbb{K}$ be a totally real number field of degree n and $\alpha \in \mathbb{K}$ such that $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$ and $\sigma_i(\alpha) > 0$ for all $i = 1, \cdots, n$. The twisted homomorphism is the map

$$\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$$

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

If $[\mathbb{K} : \mathbb{Q}] = n$ and $I \subseteq \mathbb{K}$ is a free $\mathbb{Z}$-module with rank n and $\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$, then the image $\sigma_\alpha(I)$ is a lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(v_1), \ldots, \sigma_\alpha(v_n)\}$.



Determinant

If $I \subseteq \mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n and $\Lambda = \sigma_\alpha(I)$, then

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

where $N(I) = |\mathcal{O}_{\mathbb{K}}/I|$, $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ and $d_{\mathbb{K}}$ is the discriminant of $\mathbb{K}|\mathbb{Q}$.

If $\mathbb{K}$ is a totally real number field, then:

- $\Lambda = \sigma_\alpha(I) \subseteq \mathbb{R}^n$ has full diversity n.
- The minimum product distance of $\Lambda = \sigma_\alpha(I)$ is

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

where $N_{\mathbb{K}|\mathbb{Q}}(y) = \prod_{i=1}^{n} \sigma_\alpha(y)$ for all $x \in \mathbb{K}$.

Cyclotomic Fields

- Let $\zeta = \zeta_m = e^{\frac{2\pi i}{m}}$
- The field $\mathbb{K} = \mathbb{Q}(\zeta)$ is called cyclotomic field.
- The subfield $\mathbb{L} = \mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{Q}(\zeta)$ is called maximal real subfield of $\mathbb{Q}(\zeta)$ and it is a totally real number field.

Rotated $\mathbb{Z}^n$-lattices, $n = \frac{p-1}{2}$, p prime

Let $\zeta = \zeta_p$, p prime, $p \geq 5$, $\mathbb{K} = \mathbb{Q}(\zeta_p + {\zeta_p}^{-1})$ and $e_i = \zeta^i + \zeta^{-i}$.

Proposition

If $I = \mathcal{O}_{\mathbb{K}}$ and $\alpha = 2 - e_1$, then the lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}}) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ is a rotated $\mathbb{Z}^{\frac{p-1}{2}}$-lattice.

- E.B. Fluckiger, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel"

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

Let p prime, $p \geq 7$, $\zeta = \zeta_p$, $\mathbb{K} = \mathbb{Q}(\zeta_p + {\zeta_p}^{-1})$ and $e_i = \zeta^i + \zeta^{-i}$.

Proposition

If $I \subseteq \mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module with $\mathbb{Z}$-basis

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

and $\alpha = 2 - e_1$, then the lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$ is a rotated D_n-lattice.

We have that $D_n \subseteq \mathbb{Z}^n$

Let B be the generator matrix for D_n

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

Rotated $\mathbb{Z}^n$-lattices, $n = \frac{p-1}{2}$, p prime

Let $\zeta = \zeta_p$, p prime, $p \geq 5$, $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p{}^{-1})$ and $e_i = \zeta^i + \zeta^{-i}$.

Proposition

If $I = \mathcal{O}_{\mathbb{K}}$ and $\alpha = 2 - e_1$, then the lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}}) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ is a rotated $\mathbb{Z}^{\frac{p-1}{2}}$-lattice.

- E.B. Fluckiger, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel"

Using the generator matrix M of $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ such that $MM^t = I_{n\times n}$, we have that BM is a generator matrix for a rotated D_n-lattice. Using homomorphism properties we prove that this rotated D_n-lattice is $\frac{1}{\sqrt{p}}\sigma_\alpha(I)$.

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

Proposition

If $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(I)$, then

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

For $\Lambda = \frac{1}{\sqrt{p}}(\sigma_\alpha(I)) \subseteq \mathbb{R}^{\frac{p-1}{2}}$ and p prime:

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

Proposition

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

- If it was possible to construct these rotated D_n-lattices via ideals of $\mathcal{O}_{\mathbb{K}}$ we would have a greater relative minimum product distance than the one obtained in our construction.
- This motivated our study on the existence of such rotated D_n-lattices via ideals of $\mathcal{O}_{\mathbb{K}}$, for $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, p prime.

Second Goal

Proposition

Let p be a prime number and $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ such that $\mathbb{K}|\mathbb{Q}$ is a Galois extension and $[\mathbb{K} : \mathbb{Q}] \notin \{1, 2, 4\}$. It is impossible to construct rotated D_n-lattices via the twisted homomorphism applied to ideals of $\mathcal{O}_{\mathbb{K}}$ and $\alpha \in \mathcal{O}_{\mathbb{K}}$.

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 totally positive $\alpha \in \mathcal{O}_{\mathbb{K}}$ such that

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

Since p is odd prime, we have that $2 \nmid d_{\mathbb{K}}$, what implies that

$$\boxed{\text{either 2 divides } N(\alpha) \text{ or 2 divides } N(I).}$$

We can prove that if $A \subseteq \mathcal{O}_{\mathbb{K}}$ is an ideal and $N(A)$ is even, then

$$\boxed{N(A) = (2^f)^a b,\ \ a \geq 1, b \text{ odd}}$$

where f is the residual degree of 2.

We may write:

- $N(I) = (2^f)^{a_1} b_1,\ a_1 \geq 0,\ b_1$ odd.
- $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = (2^f)^{a_2} b_2,\ a_2 \geq 0,\ b_2$ odd.
- $c = 2^a b,\ a \geq 0,\ b$ odd.

We have

$$\boxed{4(2^a b)^n = (2^f)^{a_2} b_2((2^f)^{a_1} b_1)^2 d_{\mathbb{K}}}$$

and the powers of 2 are equal in the equality iff

$2 + aefg = 2 + an = fa_2 + 2fa_1 = f(a_2 + 2a_1)$, i.e.,

$$\boxed{2 = f(a_2 + 2a_1 - ag)}$$

Since $d_{\mathbb{K}}$ is odd and $[\mathbb{K} : \mathbb{Q}] \notin \{1, 2, 4\}$ we can prove that $f \neq 1$ and $f \neq 2$. Then, it is impossible to obtain this equality.

Rotated D_3 and D_5-lattices

Proposition

It is impossible to construct rotated D_3 and D_5-lattices via ideals of $\mathcal{O}_{\mathbb{K}}$.

- E.B. Fluckiger, F. Oggier, E. Viterbo, *New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel*, IEEE Trans. Inform. Theory, v.50, n.4, p.702-714, 2004.
- E.B. Fluckiger, G. Nebe, "On the Euclidean minimum of some real number fields", Journal de theorie des nombres de Bordeaux, 17 no. 2, p. 437-454, 2005.
- 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.

J.H. Conway and N.J.A. Sloane. "*Sphere Packings, Lattices and Groups*". Springer-Verlag, New York (1999).

Thank you!