Rotated D_n-lattices via number fields

Grasiele C. Jorge

Federal University of São Paulo

joint work with Sueli I. R. Costa, Agnaldo J. Ferrari and Robson R. de Araujo

ENCONTRO DE CÓDIGOS, RETICULADOS E INFORMAÇÃO

- ENCORI -

Goals

To present

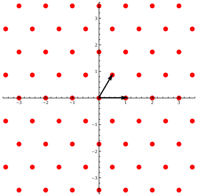
- families of rotated D_n-lattices with full diversity and
- a result on the existence of rotated D_n-lattices constructed via fractional ideals of $\mathcal{O}_{\mathbb{K}}$ when $d_{\mathbb{K}}$ is an odd number.

Lattices in $\mathbb{R}^n$

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

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

is called **lattice**.



Lattice generated by $(1,0), (1/2, \sqrt{3}/2)$

Lattices in $\mathbb{R}^n$

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

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

  is called **lattice**.
- The set $\{v_1, \ldots, v_m\}$ is called a **basis** for Λ.

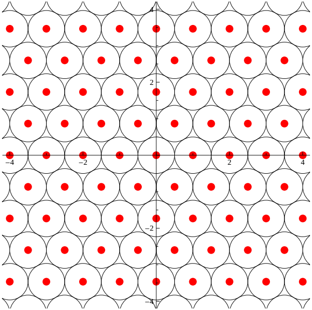
- A matrix M whose rows are these m vectors is said to be a **generator matrix** for Λ.
- The associated **Gram matrix** is $G = MM^t$.
- Gram matrices for a lattice Λ have the same determinant.
- The **determinant** of Λ, $\det(\Lambda)$, is the determinant of any Gram matrix for Λ.

Lattice parameters

- 1- Packing density
- 2 - Diversity
- 3 - Minimum product distance

1 - Packing density

The **packing density** of Λ is the proportion of the space $\mathbb{R}^n$ covered by the union of spheres of maximum radius $\rho = \frac{1}{2} min\{d(x, y); x, y \in \Lambda, x \neq y\}$ centered at the points of Λ.



Packing density

What is the densest lattice packing in $\mathbb{R}^n$?

Packing density

What is the densest lattice packing in $\mathbb{R}^n$?

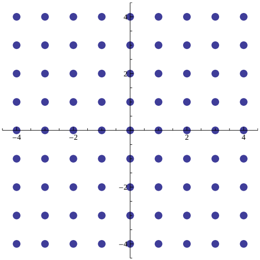
- The answer is known in dimensions from 1 to 8 and 24

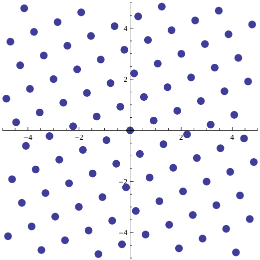
  $\mathbb{Z}$, A_2, D_3, D_4, D_5, E_6, E_7, E_8, Λ_{24}.

2 - Diversity

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

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





3 - Minimum product distance

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

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

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

Signal constellations 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.

$$D_n = \left\{ (x_1, \cdots, x_n) \in \mathbb{Z}^n ;\ \sum_{i=1}^{n} x_i \ \text{ is even } \right\}.$$

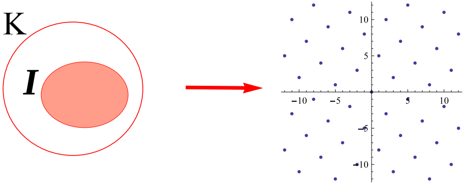
$$D_n = \left\{ (x_1, \cdots, x_n) \in \mathbb{Z}^n;\ \sum_{i=1}^{n} x_i \text{ is even} \right\}.$$

- D_n is generated by $(-1,-1,0,\dots,0)$, $(1,-1,0,\dots,0),\dots,$ $(0,1,-1,0,\dots,0),\dots,(0,0,\dots,1,-1)$.
- $\det(D_n) = 4$.

We want to construct full diversity rotated D_n-lattices and calculate their minimum product distances.

Algebraic lattices

Algebraic lattices are lattices in $\mathbb{R}^n$ obtained as the image of a homomorphism applied to a free $\mathbb{Z}$-module contained in a number field $\mathbb{K}$.



This association between number fields and lattices allows to derive certain lattice parameters (diversity, minimum product distance) which are usually difficult to calculate for general lattices.

Number Fields

- Let $\mathbb{K}$ be a number field such that $[\mathbb{K} : \mathbb{Q}] = n$ and $\mathcal{O}_{\mathbb{K}}$ its ring of integers.

Number Fields

- Let $\mathbb{K}$ be a number field such that $[\mathbb{K} : \mathbb{Q}] = n$ and $\mathcal{O}_{\mathbb{K}}$ its ring of integers.
- There are exactly n distinct $\mathbb{Q}$-homomorphisms $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$.

Number Fields

- Let $\mathbb{K}$ be a number field such that $[\mathbb{K} : \mathbb{Q}] = n$ and $\mathcal{O}_{\mathbb{K}}$ its ring of integers.
- There are exactly n distinct $\mathbb{Q}$-homomorphisms $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$.
- Let r_1 be the number of real homomorphisms (that is, with image in $\mathbb{R}$), and r_2 the number of pairs of imaginary homomorphisms. We have $n = r_1 + 2r_2$.

$$\{\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \cdots, \sigma_{r_1+2r_2}\}$$

$$\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}.$$

Twisted embedding

$$\{\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \cdots, \sigma_{r_1+2r_2}\}$$

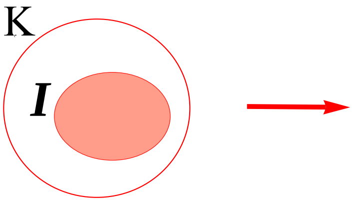
Let $\alpha \in \mathbb{K}$ such that $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$ and $\sigma_i(\alpha) > 0$ for all $i = 1, \cdots, n$. The **twisted embedding** is the map

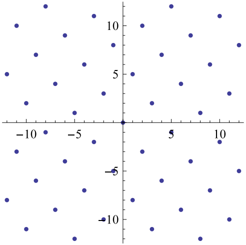
$$\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$$

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)),$$
$$\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \cdots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)))$$

- E. Bayer-Fluckiger, *Lattices and number fields*, Contemporary Mathematics, vol. 241, pp. 69-84, 1999.
- E. Bayer-Fluckiger, *Ideal lattices,* Proceedings of the conference Number theory and Diophantine Geometry, Zurich, 1999, Cambridge Univ. Press 2002, pp. 168-184.

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





Determinant

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

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

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

Diversity

The lattice $\sigma_\alpha(\mathcal{I})$ has diversity

- n, if $\mathbb{K}$ is totally real ($r_2 = 0$),
- $\frac{n}{2}$, if $\mathbb{K}$ is totally imaginary ($r_1 = 0$).

Minimum product distance

If $\mathbb{K}$ is a totally real number field, then $\Lambda = \sigma_\alpha(\mathcal{I})$ has minimum product distance

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} \frac{1}{N(\mathcal{I})} min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)|.$$

If $\mathcal{I}$ is a principal ideal of $\mathcal{O}_{\mathbb{K}}$, then

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\sigma_\alpha(\mathcal{I}))}{d_{\mathbb{K}}}}.$$

Cyclotomic Fields

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

Rayleigh fading channel

- Full diversity rotated $\mathbb{Z}^n$-lattices have been proposed to be used in signal transmission over Rayleigh fading channels.
- Our goal is to construct rotated D_n-lattices with full diversity since we want to construct lattices with a greater packing density.

Rotated $\mathbb{Z}^n$-lattices with full diversity n

Proposition

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

- E. Bayer-Fluckiger, G. Nebe, *On the Euclidean minimum of some real number fields*, Journal de Théorie des Nombres de Bordeaux, vol. 17, no. 2, pp. 437-454, 2005.
- A.A. Andrade, C. Alves, T.B Carlos, *Rotated lattices via the cyclotomic field* $\mathbb{Q}(\zeta_{2^r})$, International Journal of Applied Mathematics, vol. 19, no. 3, pp. 321-331, 2006.

Proposition

Let p be a prime number, $p \geq 5$, $\mathbb{K} = \mathbb{Q}(\zeta_p + {\zeta_p}^{-1})$. If $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$ and $\alpha = 2 - (\zeta_p + \zeta_p^{-1})$, 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. 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, vol. 50, no. 4, pp. 702-714, 2004.

Rotated D_n-lattices, $n = 2^{r-2}$, $r \geq 5$

Let $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, $e_0 = 1$ and $e_i = \zeta_{2^r}^i + \zeta_{2^r}^{-i}$.

Proposition

Let $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ the free $\mathbb{Z}$-module with $\mathbb{Z}$-basis

$$\{-2e_0 + 2e_1 - 2e_2 + \cdots - 2e_{n-2} + e_{n-1}, -e_{n-1}, e_{n-2}, \ldots, e_2, -e_1\}$$

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

Let $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p{}^{-1})$ and $e_i = \zeta_p^i + \zeta_p^{-i}$.

Proposition

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

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

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

In this case, $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is not an ideal of $\mathcal{O}_{\mathbb{K}}$.

If it were possible to construct these rotated D_n-lattices via principal ideals of $\mathcal{O}_{\mathbb{K}}$, their minimum product distances would be twice those obtained in our construction since $\min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)| = N(\mathcal{I})$ when $\mathcal{I}$ is a principal ideal.

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_{\mathbb{K}}}} \frac{1}{N(\mathcal{I})} min_{0 \neq y \in \mathcal{I}} |N_{\mathbb{K}|\mathbb{Q}}(y)|.$$

Proposition

For any totally real Galois extension $\mathbb{K}|\mathbb{Q}$ of degree $n \notin \{1, 2, 4\}$ and odd discriminant, it is impossible to construct a rotated D_n-lattice via a twisted embedding applied to a fractional ideal of $\mathcal{O}_{\mathbb{K}}$.

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

Corollary

It is impossible to construct rotated D_3 and D_5-lattices via fractional ideals of any Galois extension $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ with m odd.

Let $e_0 = 1$, $e_i = \zeta_{2^r}^i + \zeta_{2^r}^{-i}$ for $i = 1, \ldots, 2^{r-2} - 1$ and $b_i = \zeta_p^i + \zeta_p^{-i}$ for $i = 1, \ldots, \frac{p-1}{2}$.

Proposition

Consider $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$ the compositum of $\mathbb{K}_1$ and $\mathbb{K}_2$ where $\mathbb{K}_1 = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ and $\mathbb{K}_2 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ for $r \geq 3$ and $p \geq 5$ prime. Let $n_1 = 2^{r-2}$ and $n_2 = \frac{p-1}{2}$. If $\mathcal{I}$ is the $\mathbb{Z}$-submodule of $\mathcal{O}_\mathbb{K}$ with $\mathbb{Z}$-basis $\gamma = \{e_0 b_1, \ldots, e_0 b_{n_2 - 1}, 2e_0 b_{n_2}, e_1 b_1, \ldots, e_1 b_{n_2}, \ldots, e_{n_1 - 1} b_1, \ldots, e_{n_1 - 1} b_{n_2}\}$, then the lattice $(\sqrt{2^{r-1}p})^{-1}\sigma_\alpha(\mathcal{I}) \subseteq \mathbb{R}^n$, where $\alpha = (2 - e_1)(2 - b_1)$, is a rotated D_n-lattice.

Let $e_i = \zeta_{p_1}^i + \zeta_{p_1}^{-i}$ for $i = 1, \ldots, n_1 = \frac{p_1 - 1}{2}$ and $b_i = \zeta_{p_2}^i + \zeta_{p_2}^{-i}$ for $i = 1, \ldots, n_2 = \frac{p_2 - 1}{2}$.

Proposition

Let $\mathbb{K}_1 = \mathbb{Q}(\zeta_{p_1} + \zeta_{p_1}^{-1})$ with $p_1 \geq 5$ and $\mathbb{K}_2 = \mathbb{Q}(\zeta_{p_2} + \zeta_{p_2}^{-1})$ with $p_2 \geq 5$ and $p_2 \neq p_1$. Set $\mathbb{K} = \mathbb{K}_1 \mathbb{K}_2$, the compositum of $\mathbb{K}_1$ and $\mathbb{K}_2$. If $\mathcal{I}$ is the $\mathbb{Z}$-submodule of $\mathcal{O}_{\mathbb{K}}$ with $\mathbb{Z}$-basis $\gamma_1 = \{e_1 b_1, e_1 b_2, \ldots, e_1 b_{n_2 - 1}, e_1 b_{n_2}, e_2 b_1, \ldots, e_2 b_{n_2}, \ldots, e_{n_1} b_1, \ldots, 2 e_{n_1} b_{n_2}\}$, then the lattice $(\sqrt{p_1 p_2})^{-1} \sigma_\alpha(\mathcal{I}) \subseteq \mathbb{R}^n$ with $\alpha = (2 - e_1)(2 - b_1)$ is a rotated D_n-lattice.

n	p	r	r_1	p_1	p_2	p_3	$\mathbb{K}_1$	$\mathbb{K}_2$	$\mathbb{K}_3$	$\mathbb{K}_4$
3	7	–	–	–	–	–	–	0.369646	–	–
4	–	4	3	5	–	–	0.324210	–	0.281171	–
5	11	–	–	–	–	–	–	0.27097	–	–
6	13	–	3	7	–	–	–	0.24285	0.219793	–
8	17	5	4	5	–	–	0.201311	0.20472	0.182317	–
10	–	–	3	11	–	–	–	–	0.161122	–
11	23	–	–	–	–	–	–	0.17003	–	–
12	–	–	3	7	–	–	–	–	0.144401	–
14	29	–	–	–	–	–	–	0.148086	–	–
15	31	–	–	–	7	11	–	0.142402	–	0.1380198
20	41	–	4	11	–	–	–	0.121175	0.104475	–
128	257	9	–	–	–	–	0.044554	0.0450746	–	–
32768	65537	17	–	–	–	–	0.00276222	0.00276258	–	–

Table: Relative minimum product distances considering

$\mathbb{K}_1 = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, $\mathbb{K}_2 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$,

$\mathbb{K}_3 = \mathbb{Q}(\zeta_{2^{r_1}} + \zeta_{2^{r_1}}^{-1})\mathbb{Q}(\zeta_{p_1} + \zeta_{p_1}^{-1})$ and $\mathbb{K}_4 = \mathbb{Q}(\zeta_{p_2} + \zeta_{p_2}^{-1})\mathbb{Q}(\zeta_{p_3} + \zeta_{p_3}^{-1})$.

- Let $n > 1$ be an odd number.

- Let $n > 1$ be an odd number.
- Due to Dirichlet's Theorem, there exists a prime number p such that $p \equiv 1 \ (mod \ n)$.

- Let $n > 1$ be an odd number.
- Due to Dirichlet's Theorem, there exists a prime number p such that $p \equiv 1 \ (mod \ n)$.
- The cyclotomic extension $\mathbb{Q}(\zeta_p)$ has cyclic Galois group, $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, generated by σ where $\sigma(\zeta_p) = \zeta_p^r$, in which r is a primitive element of the field $\mathbb{Z}_p^*$.

- Let $n > 1$ be an odd number.
- Due to Dirichlet's Theorem, there exists a prime number p such that $p \equiv 1 \ (mod \ n)$.
- The cyclotomic extension $\mathbb{Q}(\zeta_p)$ has cyclic Galois group, $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, generated by σ where $\sigma(\zeta_p) = \zeta_p^r$, in which r is a primitive element of the field $\mathbb{Z}_p^*$.
- Let $\mathbb{K}$ be the fixed field of the subgroup $H = \langle \sigma^n \rangle \subset Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

- The degree of $\mathbb{K}$ is n.
- $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

- Consider $\alpha = \prod_{j=0}^{m-1} \left(1 - \zeta_p^{r^j}\right) \in \mathbb{Q}(\zeta_p)$ for $m = (p-1)/2$.

- Consider $\alpha = \prod_{j=0}^{m-1} \left(1 - \zeta_p^{r^j}\right) \in \mathbb{Q}(\zeta_p)$ for $m = (p-1)/2$.
- Since $r - 1 \in \mathbb{Z}_p^*$, there exists an integer λ satisfying $\lambda(r-1) \equiv 1 \ (mod \ p)$. Also, consider the element

$$z = \zeta_p^{\lambda} \alpha (1 - \zeta_p) \in \mathbb{Q}(\zeta_p).$$

- Consider $\alpha = \prod_{j=0}^{m-1} \left(1 - \zeta_p^{r^j}\right) \in \mathbb{Q}(\zeta_p)$ for $m = (p-1)/2$.
- Since $r - 1 \in \mathbb{Z}_p^*$, there exists an integer λ satisfying $\lambda(r-1) \equiv 1 \ (mod \ p)$. Also, consider the element

$$z = \zeta_p^{\lambda}\alpha(1 - \zeta_p) \in \mathbb{Q}(\zeta_p).$$

- Since z is an algebraic integer,

$$x = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(z) = \sum_{j=1}^{\frac{p-1}{n}} \sigma^{nj}(z) \in \mathcal{O}_{\mathbb{K}}.$$

Proposition

Let $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ be the free $\mathbb{Z}$-module with $\mathbb{Z}$-basis $\{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$ and $\alpha = 1/p^2$. The algebraic lattice $\sigma_\alpha(\mathcal{I})$ is a rotated $\mathbb{Z}^n$-lattice.

- P. Elia, B.A. Sethuraman and P.V. Kumar, Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas, IEEE Transactions on Information Theory, vol. 11, pp. 722-727, 2005

Proposition

Let $\mathcal{J}$ be the $\mathbb{Z}$-module with $\mathbb{Z}$-basis

$$\{x+\sigma(x), x-\sigma(x), \sigma(x)-\sigma^2(x), \ldots, \sigma^{n-2}(x)-\sigma^{n-1}(x)\}.$$

The algebraic lattice $\sigma_\alpha(\mathcal{J})$ is a full diversity rotated D_n-lattice.

Proposition

If $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$, then the minimum product distance of $\sigma_\alpha(\mathcal{J}) \simeq D_n$ satisfies $d_{p,min}(\sigma_\alpha(\mathcal{J})) \geq p^{\frac{1-n}{2}}$.

References

- G.C. Jorge, A.J. Ferrari, S.I.R. Costa, *Rotated D_n-lattices*, Journal of Number Theory, vol. 132, pp. 2397-2406, 2012.
- G. C. Jorge, S. I. R. Costa, *On rotated D_n-lattices construct via totally real number fields*, Archiv der Mathematik, vol. 100, pp. 323-332, 2013.
- R. R. de Araujo, G. C. Jorge, *Constructions of full diversity D_n-lattices for all n*, Rocky Mountain Journal of Mathematics, vol. 50, pp. 1137-1150, 2020.