Construction-A Lattices with Number Fields

Joseph J. Boutros

Texas A&M University at Qatar

10 May 2017
UCL, Kings Cross, London

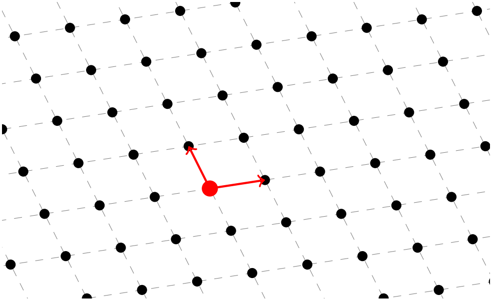
Outline of my talk

- Construction A and codes on graphs
- Alphabet size without diversity
- Construction A from number fields
- Ideals in quadratic fields for double diversity
- Ideals in cubic fields for triple diversity

Definition of a point lattice in the Euclidean space

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$:

- There are n basis vectors, $\Lambda = \mathbf{v_1}\mathbb{Z} + \mathbf{v_2}\mathbb{Z} + \ldots + \mathbf{v_n}\mathbb{Z}$.
- The lattice is given by all their integer linear combinations.
- Lattices are the real Euclidean counterpart of error-correcting codes.
  - Codes are vector spaces over a finite field.
  - Lattices are modules over a real or a complex ring, e.g. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$.



Construction A and Codes on Graphs (1)

- Low-density lattices codes [Sommer, Feder, Shalvi, 2008], by Meir Feder and his team, brought new tools from modern coding theory to lattices.
- Recent success in building high-dimensional fast-decodable LDA and GLD lattices motivated us to investigate Construction A for full-diversity lattices.
    - 0.3 dB from Poltyrev limit [Boutros, di Pietro, Huang, ITA'2015].
    - 0.8 dB from Shannon limit [di Pietro, Boutros, arXiv Nov. 2016].
- Construction A by Leech and Sloane (1971)

$$p\mathbb{Z}^n \quad \subset \quad \Lambda = \Phi(C[n,k]_p) + p\mathbb{Z}^n \quad \subset \quad \mathbb{Z}^n.$$

- Λ has rank n in $\mathbb{R}^n$, p is a prime integer, and $C[n,k]_p$ is a linear code of length n and dimension k over $\mathbb{F}_p$. The map $\Phi : \mathbb{F}_p \rightarrow \mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}$ is a group homomorphism that embeds $\mathbb{F}_p$ in $\mathbb{Z}$.

Construction A and Codes on Graphs (1)

- Low-density lattices codes [Sommer, Feder, Shalvi, 2008], by Meir Feder and his team, brought new tools from modern coding theory to lattices.

- Recent success in building high-dimensional fast-decodable LDA and GLD lattices motivated us to investigate Construction A for full-diversity lattices.
  - 0.3 dB from Poltyrev limit [Boutros, di Pietro, Huang, ITA'2015].
  - 0.8 dB from Shannon limit [di Pietro, Boutros, arXiv Nov. 2016].

- Construction A by Leech and Sloane (1971)

$$p\mathbb{Z}^n \quad \subset \quad \Lambda = \Phi(C[n,k]_p) + p\mathbb{Z}^n \quad \subset \quad \mathbb{Z}^n.$$

- Λ has rank n in $\mathbb{R}^n$, p is a prime integer, and $C[n,k]_p$ is a linear code of length n and dimension k over $\mathbb{F}_p$. The map $\Phi : \mathbb{F}_p \to \mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}$ is a group homomorphism that embeds $\mathbb{F}_p$ in $\mathbb{Z}$.

Construction A and Codes on Graphs (2)

Two sufficient conditions should be met for finite lattice constellations in order to attain Shannon capacity [Erez, Zamir, 2004-2005]:

1. Gaussian goodness which is equivalent to lattices attaining Poltyrev limit given by the highest noise variance $\sigma^2_{max} = \frac{vol(\Lambda)^{2/n}}{2\pi e}$ [Poltyrev, 1994].
2. Covering goodness which is equivalent to spherically shaped constellations in high dimensions.

In all cases, the prime p increases as n^λ where λ admits a lower bound that depends on the coding rate $R = k/n$ of C.

1. For random lattices built from random non-binary codes $C[n,k]_p$, we have $\lambda > (1+R)^{-1}$ [Ordentlich et al. 2016][di Pietro et al. 2016].
2. For LDA lattices where C is a non-binary LDPC code whose Tanner graph has an expansion factor of D, λ is to be greater than $\frac{1}{1-R}$ [di Pietro et al. 2016].

Construction A and Codes on Graphs (2)

Two sufficient conditions should be met for finite lattice constellations in order to attain Shannon capacity [Erez, Zamir, 2004-2005]:

1. Gaussian goodness which is equivalent to lattices attaining Poltyrev limit given by the highest noise variance $\sigma^2_{max} = \frac{vol(\Lambda)^{2/n}}{2\pi e}$ [Poltyrev, 1994].
2. Covering goodness which is equivalent to spherically shaped constellations in high dimensions.

In all cases, the prime p increases as n^λ where λ admits a lower bound that depends on the coding rate $R = k/n$ of C.

1. For random lattices built from random non-binary codes $C[n,k]_p$, we have $\lambda > (1+R)^{-1}$ [Ordentlich et al. 2016][di Pietro et al. 2016].
2. For LDA lattices where C is a non-binary LDPC code whose Tanner graph has an expansion factor of D, λ is to be greater than $\frac{1}{1-R}$ [di Pietro et al. 2016].

Construction A and Codes on Graphs (3)

- The value of p implemented in practical iterative decoders is not as high as n^{λ}.
- Under iterative decoding, the value of p is selected large enough to guarantee that Λ is not perturbed by its sublattice $p\mathbb{Z}^n$.
- The distance inside a coset should be larger than the distance between two cosets labeled by C.

Alphabet size without diversity (1)

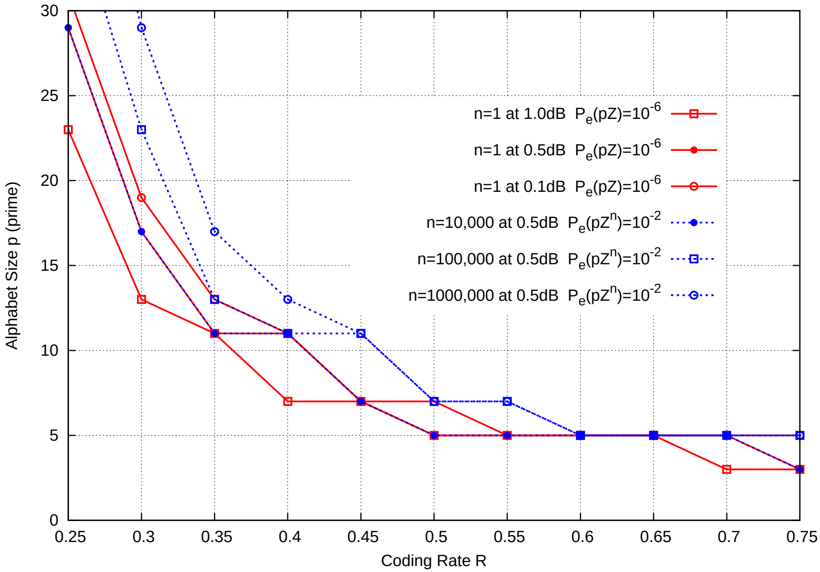
Lemma

Let $\Lambda = \Phi(C[n,k]_p) + p\mathbb{Z}^n \subset \mathbb{R}^n$ be a real lattice built via Construction A . Then, its sublattice $p\mathbb{Z}^n$ has the following error probability per dimension (per lattice coordinate) on a Gaussian channel

$$P_e(p\mathbb{Z}) = 2Q\left(\sqrt{\Delta \frac{\pi e}{2} p^{2R}}\right),$$

where $\Delta \geq 1$ is the SNR-distance to Poltyrev limit and $Q(x)$ is the Gaussian tail function.

Alphabet size without diversity (2)



Classification of Numbers

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Monoid Ring Fields

- Integer: natural and relative (or rational integer).
- Rational: from $\mathbb{Q}$, the ring of fractions of $\mathbb{Z}$.
- Algebraic number: real or complex number that is root of a finite-degree polynomial with coefficients in $\mathbb{Q}$.
- Algebraic integer: real or complex number that is root of a finite-degree polynomial with coefficients in $\mathbb{Z}$.

$$\begin{array}{ccccc} \mathbb{Q} & \subset & \mathbb{K} = \mathbb{Q}(\theta) & \subset & \mathbb{C}, \\ \mathbb{Z} & \subset & O_{\mathbb{K}} & \subset & \mathbb{K}. \end{array}$$

- Transcendental numbers: π, e, $\log(2)$, $\sin(1)$, $2^{\sqrt{2}}$, $\sum_{n=1}^{\infty} 10^{-n!}$.

Other rings in $\mathbb{C}$ are possible: the Gaussian integers $\mathbb{Z}[i]$ and Eisenstein integers $\mathbb{Z}[\omega]$.

The ring of integers $O_{\mathbb{K}}$ is identified to a lattice $\Lambda_{O_{\mathbb{K}}}$

- θ is root of $\mu_\theta(x)$, with coefficients in $\mathbb{Z}$, irreducible, of degree $n_0 = [\mathbb{K} : \mathbb{Q}]$.
- The number field is $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q} + \theta\mathbb{Q} + \theta^2\mathbb{Q} + \ldots + \theta^{n_0-1}\mathbb{Q}$.
- Its ring of integers is $O_{\mathbb{K}} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} + \ldots + \omega_{n_0}\mathbb{Z}$. This is a free $\mathbb{Z}$-module!
- The integral basis $\{\omega_1, \ldots, \omega_{n_0}\}$ is not necessarily identical to the power basis $\{1, \theta, \ldots, \theta^{n_0-1}\}$ of $\mathbb{K}$.
- Any algebraic integer $\alpha \in O_{\mathbb{K}}$ is converted into a lattice point via a special embedding σ, i.e. $\Lambda_{O_{\mathbb{K}}} = \sigma(O_{\mathbb{K}})$. Any ideal $I \subset O_{\mathbb{K}}$ yields a sub-lattice $\Lambda_{\mathcal{I}} = \sigma(\mathcal{I}) \subset \Lambda_{O_{\mathbb{K}}}$.

Construction A from number fields

- Replace the partition chain $\mathbb{Z}^n/\Lambda/p\mathbb{Z}^n$ by $\Lambda_{O_{\mathbb{K}}}^m/\Lambda/\Lambda_{\mathcal{I}}^m$.
- $\Lambda_{O_{\mathbb{K}}} = \sigma(O_{\mathbb{K}}) \subset \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$, $\Lambda_{\mathcal{I}} = \sigma(\mathcal{I})$ such that the quotient ring has order $N(I) = |O_{\mathbb{K}}/\mathcal{I}| = p$ and $m = n/[\mathbb{K}:\mathbb{Q}] = n/n_0$.
- The canonical embedding $\sigma : O_{\mathbb{K}} \to \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ converts the ring of integers $O_{\mathbb{K}}$ and its ideals into lattices of dimension $n_0 = [\mathbb{K}:\mathbb{Q}]$.

Construction A from a number field becomes

$$\Lambda_{\mathcal{I}}^m \quad \subset \quad \Lambda = \Phi(C[m,k]_p) + \Lambda_{\mathcal{I}}^m \quad \subset \quad \Lambda_{O_{\mathbb{K}}}^m.$$

- The homomorphism $\Phi : \mathbb{F}_p \to \Lambda_{O_{\mathbb{K}}} \subset \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ embeds the prime field $\mathbb{F}_p$ in the real space $\mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$.

Construction A from number fields

- Replace the partition chain $\mathbb{Z}^n/\Lambda/p\mathbb{Z}^n$ by $\Lambda^m_{O_\mathbb{K}}/\Lambda/\Lambda^m_{\mathcal{I}}$.
- $\Lambda_{O_\mathbb{K}} = \sigma(O_\mathbb{K}) \subset \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$, $\Lambda_{\mathcal{I}} = \sigma(\mathcal{I})$ such that the quotient ring has order $N(I) = |O_\mathbb{K}/\mathcal{I}| = p$ and $m = n/[\mathbb{K}:\mathbb{Q}] = n/n_0$.
- The canonical embedding $\sigma : O_\mathbb{K} \to \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ converts the ring of integers $O_\mathbb{K}$ and its ideals into lattices of dimension $n_0 = [\mathbb{K}:\mathbb{Q}]$.

Construction A from a number field becomes

$$\Lambda^m_{\mathcal{I}} \quad \subset \quad \Lambda = \Phi(C[m,k]_p) + \Lambda^m_{\mathcal{I}} \quad \subset \quad \Lambda^m_{O_\mathbb{K}}.$$

- The homomorphism $\Phi : \mathbb{F}_p \to \Lambda_{O_\mathbb{K}} \subset \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ embeds the prime field $\mathbb{F}_p$ in the real space $\mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$.

Construction A from quadratic fields (1)

- Real quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ for $d \geq 2$. Its ring of integers is $O_{\mathbb{K}} = \mathbb{Z}[\phi]$ where $\{1, \phi\}$ is an integral basis.
- If $d \neq 1 \; mod \; 4$ then $\phi = \sqrt{d}$, its conjugate is $\bar{\phi} = -\sqrt{d}$.
- If $d = 1 \; mod \; 4$ then $\phi = (1 + \sqrt{d})/2$, its conjugate is $\bar{\phi} = (1 - \sqrt{d})/2$.
- Let $\mathcal{I} = gO_{\mathbb{K}}$ be a principal ideal with generator g.

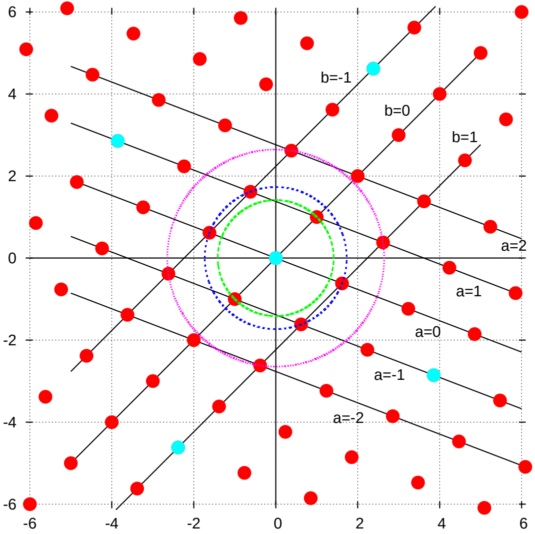
The generator matrices of $\Lambda_{O_{\mathbb{K}}} = \sigma(O_{\mathbb{K}})$ and $\Lambda_{\mathcal{I}} = \sigma(\mathcal{I})$ are

$$G_{O_{\mathbb{K}}} = \left(\begin{array}{cc} 1 & 1 \\ \phi & \bar{\phi} \end{array} \right), \qquad G_{\mathcal{I}} = \left(\begin{array}{cc} g & \bar{g} \\ g\phi & \bar{g}\bar{\phi} \end{array} \right).$$

The fundamental volume of $\Lambda_{\mathcal{I}}$ is given by (P. Samuel 1967)

$$vol(\Lambda_{\mathcal{I}}) = |\det(G_{\mathcal{I}})| = N(\mathcal{I}) \times |\det(G_{O_{\mathbb{K}}})| = p\sqrt{d_{\mathbb{K}}},$$

Construction A from quadratic fields (2)



The bidimensional double-diversity lattices $\Lambda_{O_{\mathbb{K}}}$ and $\Lambda_{\mathcal{I}}$ built from the field $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ and $O_{\mathbb{K}}/\mathcal{I}$ shown on the first three shells ($p = 11$).

Alphabet size with double diversity (1)

Lemma

The sublattice $\Lambda_{\mathcal{I}}^{m}$ *has error probability* $P_e(\Lambda_{\mathcal{I}})$ *per two dimensions* ($[\mathbb{K}:\mathbb{Q}]=2$) *satisfying*

$$2Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I\ p^R}\right) \le P_e(\Lambda_{\mathcal{I}}),$$

$$P_e(\Lambda_{\mathcal{I}}) \le 2Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I\ p^R}\right) + \sum_{\ell=2}^{\tau_f/2} 2Q\left(\sqrt{\Delta\frac{\pi e}{2}\frac{d_\ell^2(\mathcal{I})\ p^R}{vol(\Lambda_{\mathcal{I}})}}\right),$$

where $R=\frac{k}{m}=\frac{k}{n/2}$ *is the coding rate of* C, Δ *is the SNR-distance to Poltyrev limit, the Hermite constant is*

$$\gamma_I = \frac{d_{Emin}^2(\mathcal{I})}{vol(\Lambda_{\mathcal{I}})} \quad \text{with} \quad vol(\Lambda_{\mathcal{I}}) = N(\mathcal{I})\sqrt{d_{\mathbb{K}}},$$

and $d_{Emin}^2(\mathcal{I})$ *being the minimal squared Euclidean distance of the lattice* $\Lambda_{\mathcal{I}}$.

For a general totally real number field

Lemma

The sublattice $\Lambda_{\mathcal{I}}^m$ has error probability $P_e(\Lambda_{\mathcal{I}})$ per n_0 dimensions ($[\mathbb{K}:\mathbb{Q}] = n_0$) satisfying

$$2Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I \ p^{\frac{2R}{[\mathbb{K}:\mathbb{Q}]}}}\right) \le P_e(\Lambda_{\mathcal{I}}),$$

$$P_e(\Lambda_{\mathcal{I}}) \le 2Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I \ p^{\frac{2R}{[\mathbb{K}:\mathbb{Q}]}}}\right) + \sum_{\ell=2}^{\tau_f/2} 2Q\left(\sqrt{\Delta\frac{\pi e}{2}\frac{d_\ell^2(\mathcal{I}) \ p^{\frac{2R}{[\mathbb{K}:\mathbb{Q}]}}}{vol(\Lambda_{\mathcal{I}})^{2/n_0}}}\right),$$

where $R = \frac{k}{m} = \frac{k}{n/2}$ is the coding rate of C, Δ is the SNR-distance to Poltyrev limit, the Hermite constant is

$$\gamma_I = \frac{d^2_{Emin}(\mathcal{I})}{(vol(\Lambda_{\mathcal{I}}))^{2/n_0}} \quad \textit{with} \quad vol(\Lambda_{\mathcal{I}}) = N(\mathcal{I})\sqrt{d_{\mathbb{K}}},$$

and $d^2_{Emin}(\mathcal{I})$ being the minimal squared Euclidean distance of the lattice $\Lambda_{\mathcal{I}}$.

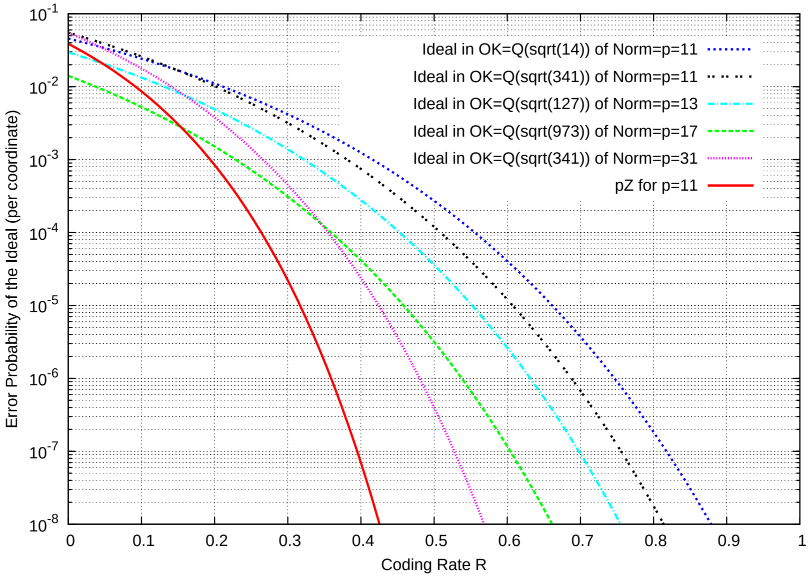
Alphabet size with double diversity (2)

p	d	$d_{\mathbb{K}}$	g	$d^2_{Emin}(\mathcal{I})$	$\gamma_I(dB)$
11	5	5	$-1+3\phi$	23	-0.29
11	14	56	$5+\phi$	78	-0.23
11	341	341	$26+3\phi$	231	0.56
13	127	508	$\pm 34+3\phi$	326	0.46
17	973	973	$-338+21\phi$	578	0.37
31	341	341	$44+5\phi$	651	0.56

Table: Parameters for good lattices $\sigma(\mathcal{I})$ where $\mathcal{I} = gO_{\mathbb{K}}$ is a principal ideal in the ring of integers $O_{\mathbb{K}}$ of quadratic number fields $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.

The ideal norm $N(\mathcal{I}) = p$, the discriminant $d_{\mathbb{K}}$, the generator g, the minimum Euclidean distance, and Hermite constant $\gamma_I(dB) = 10\log_{10}(\gamma_I)$ are given.

Alphabet size with double diversity (3)



Totally real cubic number fields

- $\mathbb{K} = \mathbb{Q}(\theta)$, θ is root of $\mu_\theta(x) = x^3 - ax + b$, where $a, b \in \mathbb{Z}$.
- $x^3 - ax + b$ irreducible and $4a^3 - 27b^2 > 0$.
- François Viète's equations for the three roots ($\theta = \theta_1$):

$$\theta_1 = \theta(a,b) = 2\sqrt{\frac{a}{3}}\ \cos\left(\frac{1}{3}\ arccos\left(-\frac{3b}{2a}\ \sqrt{\frac{3}{a}}\right)\right),$$
$$\theta_3 = -\theta(a,-b), \qquad \theta_2 = -\theta_1 - \theta_3.$$

- For a principal ideal $\mathcal{I} = gO_{\mathbb{K}}$, the generator matrix of $\Lambda_{\mathcal{I}}$ is

$$G_{\mathcal{I}} = \left(\begin{array}{ccc} \sigma_1(g\omega_1) & \sigma_2(g\omega_1) & \sigma_3(g\omega_1) \\ \sigma_1(g\omega_2) & \sigma_2(g\omega_2) & \sigma_3(g\omega_2) \\ \sigma_1(g\omega_3) & \sigma_2(g\omega_3) & \sigma_3(g\omega_3) \end{array}\right).$$

where $\sigma_1(\theta) = \theta_1$, $\sigma_2(\theta) = \theta_2$, and $\sigma_3(\theta) = \theta_3$.

Ideals in cubic number fields for triple diversity (1)

Two examples of very negative fundamental gain for $p = 11$.

p	$a, b, d_{\mathbb{K}}$	Integral Basis $\{\omega_1, \omega_2, \omega_3\}$	Generator g	d^2_{Emin}	$\gamma_I(dB)$
11	$5, 1, 473$	$1, \theta, -3+\theta^2$	ω_3	17	-3.55
11	$7, 5, 697$	$1, \theta, -5+\theta+\theta^2$	$\omega_1 - 2\omega_3$	17	-4.12

Table: Parameters for bad lattices $\sigma(\mathcal{I})$ where $\mathcal{I} = gO_{\mathbb{K}}$ is a principal ideal in the ring of integers $O_{\mathbb{K}}$ of a cubic number field $\mathbb{K} = \mathbb{Q}(\theta)$ defined by $\mu_\theta(x) = x^3 - ax + b$.

The ideal norm $N(\mathcal{I}) = p$, the coefficients of the minimal polynomial $\mu_\theta(x)$, the field discriminant $d_{\mathbb{K}}$, the generator g, the minimum Euclidean distance $d^2_{Emin}(\mathcal{I})$, and Hermite constant $\gamma_I(dB) = 10\log_{10}(\gamma_I)$ are given.

Ideals in cubic number fields for triple diversity (2)

p	$a, b, d_{\mathbb{K}}$	Integral Basis $\{\omega_1, \omega_2, \omega_3\}$	Generator g	d^2_{Emin}	$\gamma_I(dB)$
11	$9, 3, 2673$	$1, \theta, \theta^2 - 6$	$\omega_1 - 2\omega_2$	75	0.38
23	$22, 14, 1492$	$1, -\frac{13}{5} + \frac{3}{5}\theta + \frac{1}{5}\theta^2,$ $\frac{13}{5} + \frac{2}{5}\theta - \frac{1}{5}\theta^2$	$3\omega_1 + 2\omega_2$	103	0.47
29	$14, 16, 1016$	$1, -5 + \theta + \frac{1}{2}\theta^2, \theta$	$5\omega_1 + 2\omega_2$	107	0.52
31	$4, 1, 229$	$1, \theta, \theta^2 - 3$	$\omega_1 - 2\omega_2 - 3\omega_3$	67	0.45
41	$25, 25, 1825$	$1, -3 + \frac{1}{5}\theta^2$ $-3 + \theta + \frac{1}{5}\theta^2$	$\omega_1 + 4\omega_2 + 5\omega_3$	158	0.36
47	$12, 4, 1620$	$1, \theta, -4 + \frac{1}{2}\theta^2$	$5\omega_1 - \omega_2 - 2\omega_3$	171	0.48

Table: Parameters for good lattices $\sigma(\mathcal{I})$ where $\mathcal{I} = gO_{\mathbb{K}}$ is a principal ideal in the ring of integers $O_{\mathbb{K}}$ of a cubic number field $\mathbb{K} = \mathbb{Q}(\theta)$ defined by $\mu_\theta(x) = x^3 - ax + b$.

The ideal norm $N(\mathcal{I}) = p$, the coefficients of the minimal polynomial $\mu_\theta(x)$, the field discriminant $d_{\mathbb{K}}$, the generator g, the minimum Euclidean distance $d^2_{Emin}(\mathcal{I})$, and Hermite constant $\gamma_I(dB) = 10\log_{10}(\gamma_I)$ are given.

Conclusions

- Construction A with non-binary codes is one of the most successful recent tools for building lattices.
- The lattice diversity produced by the number field comes with a drawback. The general expression for the dominant term in $P_e(\Lambda_{\mathcal{I}})$ is

$$Q\left(\sqrt{\Delta \frac{\pi e}{2} \gamma_I \; p^{\frac{2R}{[\mathbb{K}:\mathbb{Q}]}}}\right).$$

- We searched for ideals in number fields to build Construction-A lattices that are good for both Gaussian and fading channels.
- Reasonable values are found for the alphabet size p in order to avoid error floors generated by the sublattice $p\mathbb{Z}^n$ or $\Lambda_{\mathcal{I}}^m$.
- For cubic fields and above, the search should include general ideals (non-principal).