New results on signal constellation designs for transmission over Rayleigh fading channels

(joint work with Eva Bayer-Fluckiger and Frédérique Oggier)

EPFL Workshop on "Algebra and Communications"

January 16-17th, 2003

Emanuele Viterbo

Dipartimento di Elettronica

Politecnico di Torino, Italy

viterbo@polito.it

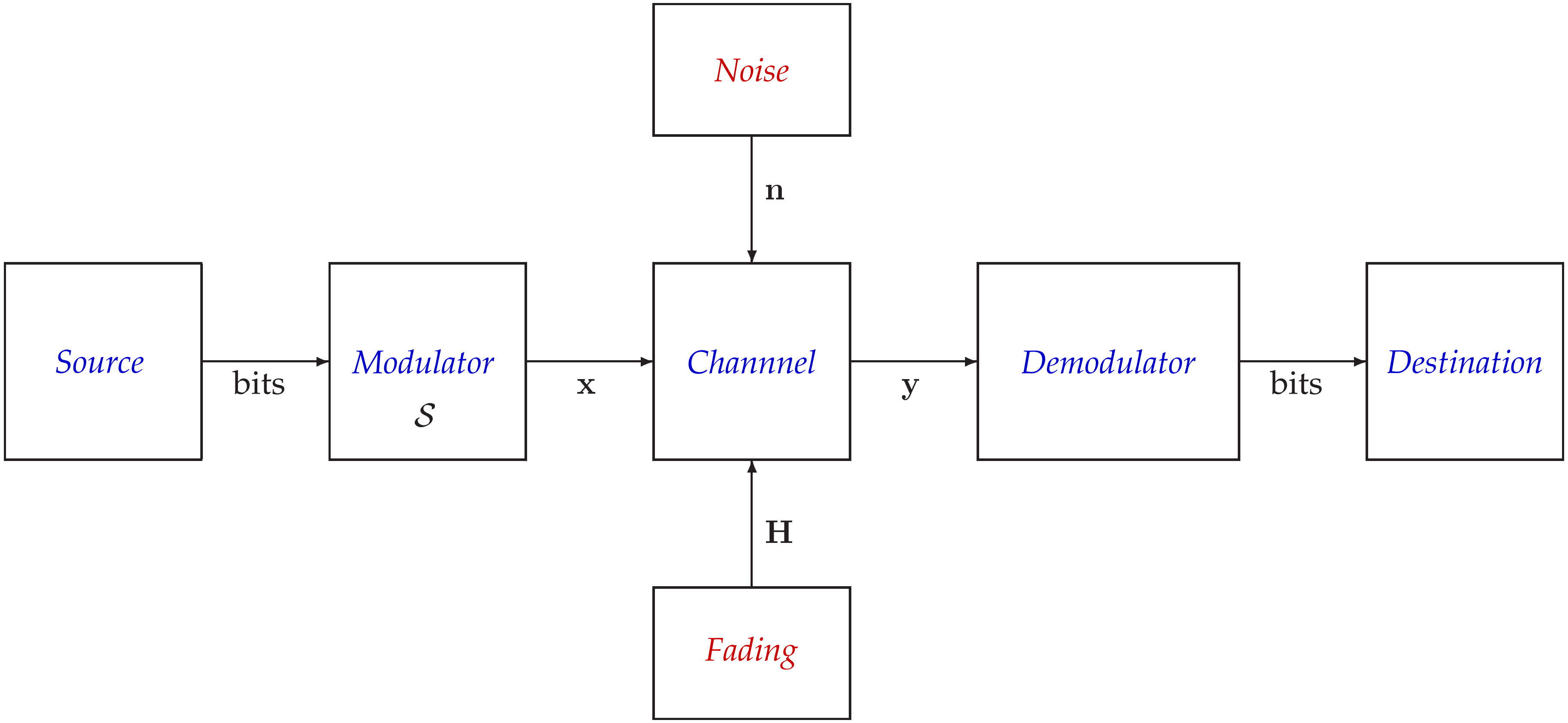
Slides available at:

http://www.tlc.polito.it/~viterbo/slides.html

Outline

- Digital transmission channel
- Coding and decoding
- Signal space diversity
- Lattices and lattice decoding
- Algebraic construction of high diversity constellations
- New constructions of high diversity rotated cubic lattices

A digital transmission system



The codebook

- Digital transmission over band-limited channels is commonly modeled in the n-dimensional Euclidean space $\mathbf{R}^n$.
- The *codebook* or *signal constellation* is a set of M points (vectors) in $\mathbf{R}^n$

$$\mathcal{S} = \{\mathbf{x}_i\}_1^M$$

- A *codeword* $\mathbf{x} = (x_1, \dots, x_n) \in \mathcal{S}$ conveniently represents a band-limited signal to be transmitted by the modulator.
- The source labels each point with $\log_2(M)$ bits (*bit labelling*).
- The finite signal constellation is usually constrained such that the points are within a bounded region centered around the origin (*constellation shaping*).

Channel Models

- Different types of channels may be described using the following model

$$\mathbf{y} = \mathbf{x}\mathbf{H} + \mathbf{n}$$

- $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbf{R}^n$ received signal vector
- $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{R}^n$ transmitted codeword taken from a codebook $\mathcal{S}$
- $\mathbf{n} \sim \mathcal{N}(\mathbf{0}, \frac{N_0}{2}\mathbf{I})$ real Gaussian random vector with i.i.d. components
- $\mathbf{H} = \mathrm{diag}(h_1, \ldots, h_n)$ diagonal channel fading matrix:
  1. *AWGN*: $\mathbf{H} = \mathbf{I}$ additive white Gaussian noise channel (no fading).
  2. *Slow (or block) fading*: $\mathbf{H} = h\mathbf{I}$ and h changes independently from one transmitted codeword to the next.
  3. *Fast fading*: h_i change independently in each component (usually Rayleigh distributed).

ML decoding

- Assuming that the channel state information (i.e. $\mathbf{H}$) is known at the receiver, ML detection is given by
$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathcal{S}} \|\mathbf{y} - \mathbf{x}\mathbf{H}\|^2 = \arg\min_{\mathbf{x}'\in\mathcal{S}'} \|\mathbf{y} - \mathbf{x}'\|^2$$
where $\mathbf{x}' = \mathbf{x}\mathbf{H}$ and $\mathcal{S}' = \mathbf{H}\mathcal{S}$ is the "faded signal constellation".

- The complexity of the ML receiver greatly depends on the structure of the code $\mathcal{S}$.

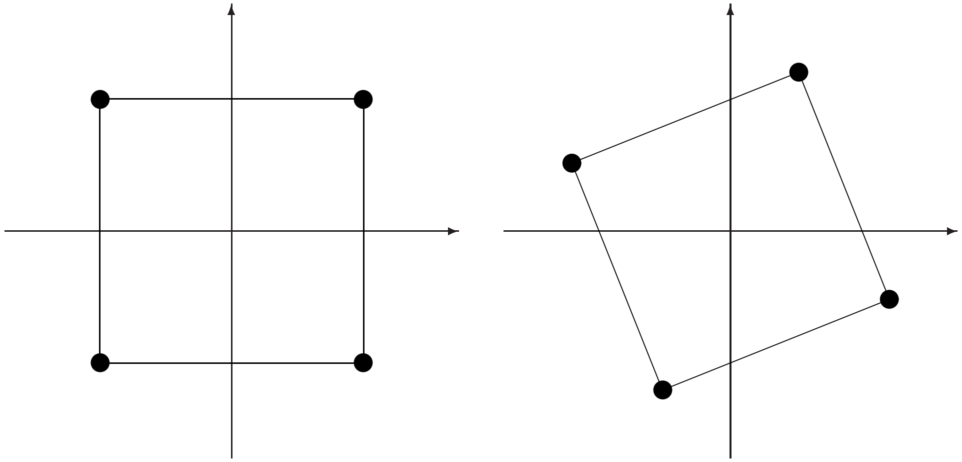
- In the case of AWGN and slow fading the error probability is asymptotically dependent on the *minimum Euclidean distance* of the signal set.

- In the case of fast Rayleigh fading the performance of the signal set is dominated by the minimum Hamming distance between any two signal vectors, also known as *modulation diversity*, denoted by L.

- Another important parameter the case of fast Rayleigh fading is the *minimum product distance*.

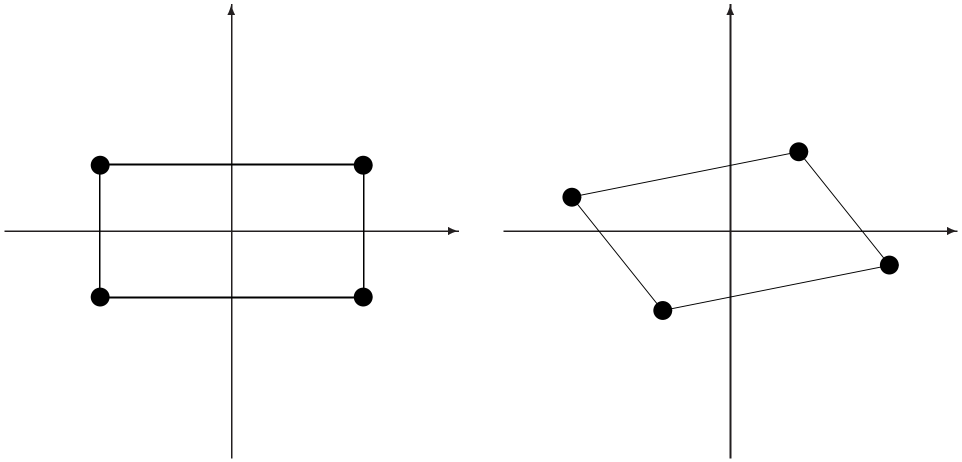
An example of modulation diversity

S



AWGN

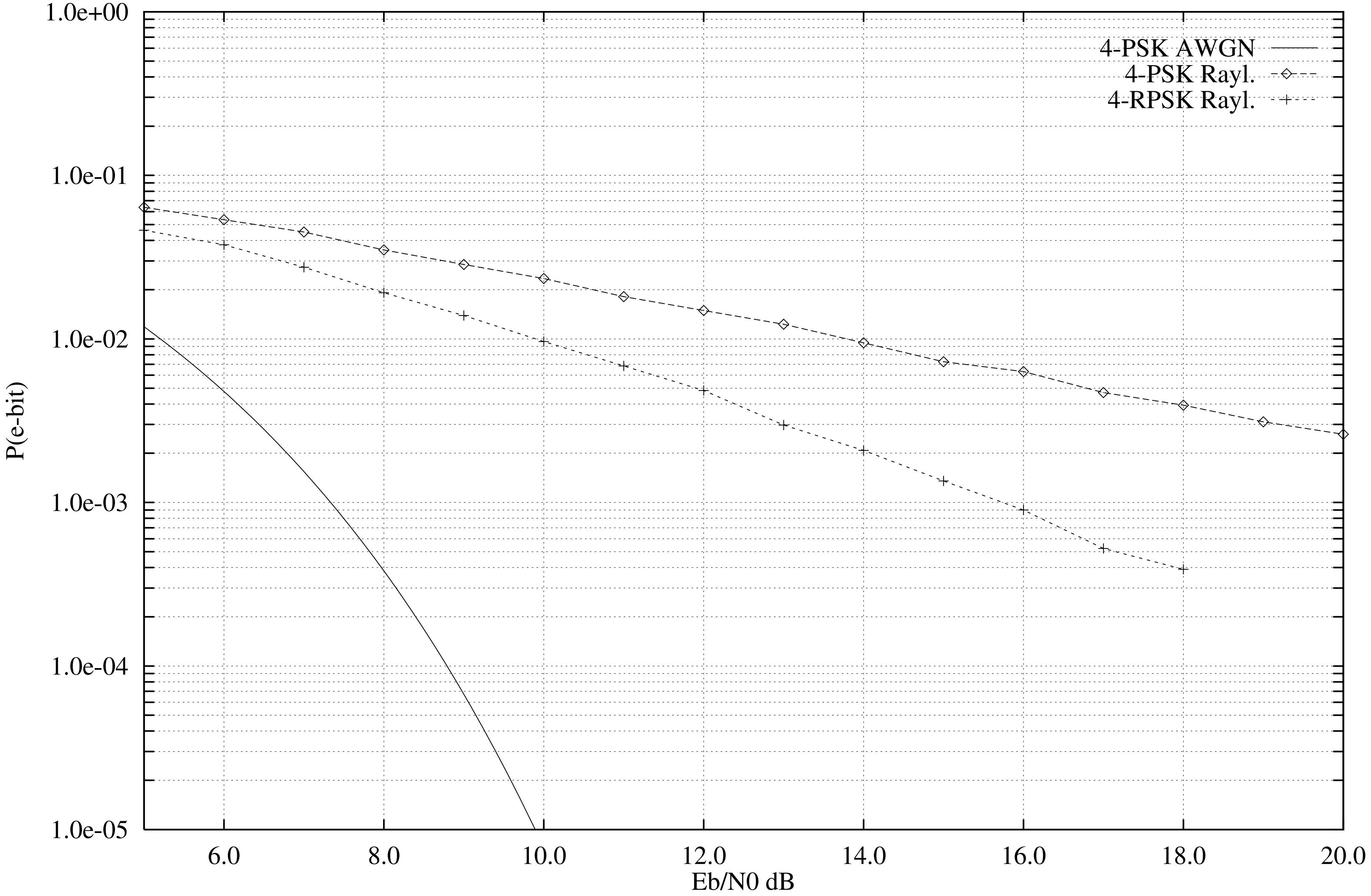
S'



Fading

$\mathbf{h} = (1, 0.5)$

Bit error rate 4-PSK vs. 4-RPSK



Error Probability

- *AWGN Channel*

$$P(\mathbf{x} \to \mathbf{w}) = \frac{1}{2}\mathrm{erfc}\left(\frac{d_E(\mathbf{x}, \mathbf{w})}{2\sigma\sqrt{2}}\right)$$

where $d_E(\mathbf{x}, \mathbf{w}) = \|\mathbf{x} - \mathbf{w}\|$ is the Euclidean distance between $\mathbf{x}, \mathbf{w} \in S$.

- *Rayleigh Fading Channel*

$$P(\mathbf{x} \to \mathbf{w}) \leq \frac{[16\sigma]^l}{d_p^{(l)}(\mathbf{x}, \mathbf{w})}$$

where $d_p^{(l)}(\mathbf{x}, \mathbf{w}) = \prod_{x_i \neq w_i}^{(l)} |x_i - w_i|$ is the *l-product distance*.

- Good constellations for the fading channel

1. Maximize the *modulation diversity* $L = \min_{\mathbf{x},\mathbf{w} \in S}(l)$, since when $L \to \infty$ performance approaches the AWGN case.
2. Maximize the *minimum L-product distance* $d_{p,min} = d_{p,min}^{(L)} = \prod_{x_i \neq w_i}^{(L)} |x_i - w_i|$.

under the average signal energy constraint $E\{\|\mathbf{x}\|^2\} = constant$.

Why Lattices?

- To increase the modulation diversity L we must consider high-dimensional modulation schemes.
- Lattice constellations (or codes) are finite sets of points carved from a lattice $\Lambda = \{\mathbf{x} = \mathbf{z}\mathbf{M} | \mathbf{z} \in \mathbf{Z}^n\}$ with generator matrix $\mathbf{M}$.
- On the AWGN channel the error probability is related to the *Hermite constant* of the lattice:

$$\gamma(\Lambda) = \frac{d_{E,min}^2}{[vol(\Lambda)]^{2/n}} \,.$$

- In some cases the lattice structure gives a simple bit labeling, so that no lookup table is needed.
- We can use a *universal lattice decoding algorithm (sphere-decoder)* for ML detection: in fact, if $\mathcal{S}$ is a lattice with generator matrix $\mathbf{M}$ then $\mathcal{S}'$ is also a lattice with generator matrix $\mathbf{M}\mathbf{H}$.
- Algebraic number theory is the mathematical tool which enables to construct lattices with high diversity and good $d_{p,min}$.

Canonical Embedding of a number field $K = \mathbf{Q}(\theta)$

- The *minimal polynomial* $\mu_\theta(x)$ has r_1 real roots and $2r_2$ complex roots

$$n = r_1 + 2r_2$$

- There are exactly n *field homomorphisms*

$$\sigma_i : K \to \mathbf{C}, \quad \sigma_i(\theta) = \theta_i$$

completely identified by the roots $\theta_i \in \mathbf{C}$ of $\mu_\theta(x)$.

- The *canonical embedding* $\sigma : K \to \mathbf{R}^n$ is defined by

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \ldots \Re\sigma_{r_1+r_2}(\alpha), \Im\sigma_{r_1+r_2}(\alpha)) \in \mathbf{R}^n$$

- Let $(\omega_1, \omega_2, \ldots \omega_n)$ be an *integral basis* of K, i.e., $O_K = \mathbf{Z}[\omega_1, \omega_2, \ldots \omega_n]$.

- An *algebraic lattice* $\Lambda = \sigma(O_K)$ is obtained by applying the canonical embedding to the ring of integers O_K. The lattice generator matrix contains the n generators $\sigma(\omega_1), \ldots, \sigma(\omega_n)$.

Algebraic Lattices

- The *generator matrix* of the canonical embedding of the ring of integers is

$$\mathbf{M} = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \ldots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \ldots & \sigma_{r_1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \ldots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \ldots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix}$$

- The *fundamental volume* of the lattice $\Lambda = \sigma(O_K)$ is

$$vol(\Lambda) = |\det(\mathbf{M})| = 2^{-r_2} \times \sqrt{|d_K|}$$

where $d_K = \det[\sigma_j(\omega_i)]^2$ is the *absolute discriminant* of the field.

Modulation Diversity of Algebraic Lattices

- *Theorem.* The lattices obtained from the previous generator matrix exhibit a diversity

$$L = r_1 + r_2 \; .$$

- *Proof.* Let $\mathbf{x} \neq \mathbf{0}$ be an arbitrary point of Λ

$$\mathbf{x} = (x_1, x_2, \dots x_n) = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i$$

with $\lambda_i \in \mathbf{Z}$ and $\mathbf{v}_i = (v_{ij})$ the rows of the lattice generator matrix M.

$$\prod_{i=1}^{n} |x_i| = \prod_{j=1}^{r_1} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| \times \prod_{j=r1+1}^{r_1+r_2} \left| \Re \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| \times \prod_{j=r1+1}^{r_1+r_2} \left| \Im \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right|$$

  - $\sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \neq 0 \Rightarrow L \geq r_1 + r_2$
  - $\beta = 1 \in O_K \Rightarrow L = r_1 + r_2$

The totally real case

- The lattice Λ constructed in this case attains the maximum degree of diversity $L = n$ (*full diversity*). Its generator matrix is given by

$$\mathbf{M} = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \dots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \dots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \dots & \sigma_n(\omega_n) \end{pmatrix}$$

- The *n-product distance* of $\mathbf{x}$ from $\mathbf{0}$ is

$$\begin{aligned} d_p^{(n)}(\mathbf{0}, \mathbf{x}) &= \prod_{j=1}^{n} |x_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i) \right| \\ &= \prod_{j=1}^{n} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = \left| N \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = |N(\beta)| \geq 1 \end{aligned}$$

- It is useful to maximize the *minimum product distance* in the lattice $d_{p,min} = \min_{\mathbf{x} \in \Lambda} d_p^{(n)}(\mathbf{0}, \mathbf{x})$.

Rotated Cubic Lattices $\mathbf{Z}_{n,L}$

For application it is convenient to work with cubic lattice constellations since bit labelling and constellation shaping become very simple. Examples of constructions of Rotated Cubic Lattices

- Algebraic construction of *totally complex lattices* $\mathbf{Z}_{n,n/2}$.

$$\mathbf{Z}_{n,n/2} = \sigma(\mathbf{Z}[i][\theta]) \qquad \theta = e^{i2\pi/N}$$

$$\mu_\theta(x) = x^n + \epsilon\, x^{n/2} + 1$$

$$\epsilon = 0 \;\; if \;\; n = 2^{e_1} \quad and \quad \epsilon = -1 \;\; if \;\; n = 2^{e_1}3^{e_2}$$

  The generator matrix of $\mathbf{Z}_{n,n/2}$ is a rotation matrix.
  Examples : $\mathbf{Z}_{4,2}$, $\mathbf{Z}_{6,3}$, $\mathbf{Z}_{8,4}$, $\mathbf{Z}_{12,6}$, $\mathbf{Z}_{16,8}$, $\mathbf{Z}_{24,12}$, $\mathbf{Z}_{32,16}$.

- Algebraic construction of *totally real lattices* $\mathbf{Z}_{n,n}$

$$\mathbf{Z}_{n,n} = \sigma(I) \quad I \subset O_K \quad K = \mathbf{Q}(2\cos(2\pi/N))$$

  The lattice dimension $n = \phi(N)/2$
  Examples : $\mathbf{Z}_{3,3}$, $\mathbf{Z}_{5,5}$, $\mathbf{Z}_{9,9}$, $\mathbf{Z}_{11,11}$, $\mathbf{Z}_{15,15}$.

- Some more systematic constructions of $\mathbf{Z}_{n,n}$ will be shown in the following.

Ideal lattices

- *Definition*. Let K be a totally real number field of degree n. An *ideal lattice* is an integral lattice $(\mathcal{I}, q_\alpha)$, where $\mathcal{I}$ is an O_K-ideal (which may be fractional) and

$$q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbf{Z}, \quad q_\alpha(x, y) = \mathrm{Tr}\,(\alpha x y), \;\; \forall x, y \in \mathcal{I}$$

where $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbf{Q}}$ is the trace and $\alpha \in K$ is totally positive (i.e. $\sigma_i(\alpha) > 0 \; \forall i$).

- If $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbf{Z}$-basis of $\mathcal{I}$, the generator matrix $\mathbf{M}$ of the lattice $\{\mathbf{x} = \mathbf{z}\mathbf{M} | \mathbf{z} \in \mathbf{Z}^n\}$ is given by

$$\mathbf{M} = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_1) \\ \vdots & \vdots & \ldots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{pmatrix}$$

where $\alpha_j = \sigma_j(\alpha), \; \forall j$. One easily verifies that the Gram matrix of this lattice is

$$\mathbf{M}\mathbf{M}^t = \{\mathrm{Tr}\,(\alpha\,\omega_i \omega_j)\}_{i,j=1}^n$$

Minimum product distance for ideal lattices

- *Theorem.* Let $\mathcal{I}$ be a principal ideal of O_K. The minimum product distance of an ideal lattice $(\mathcal{I}, q_\alpha)$ of determinant D defined over $\mathcal{I}$ is

$$d_{p,min}(q_\alpha) = \sqrt{\frac{D}{d_K}}.$$

- In order to compare among different lattices, we normalize the determinant D to be 1, so that

$$d_{p,min} = 1/\sqrt{d_K}$$

- It is also useful to consider $d_{p,min}^{1/n}$ in order to compare among lattices of different dimensions.

Cyclotomic construction in dimension $n = (p-1)/2$

- Let $p \geq 5$ be a prime, $n = (p-1)/2$ and $\zeta = \zeta_p = e^{-2i\pi/p}$ be a pth root of unity.
- The lattices are built via the ring of integers of $K = \mathbf{Q}(\zeta + \zeta^{-1})$, the maximal real subfield of $\mathbf{Q}(\zeta)$, whose integral basis is given by $\{e_j = \zeta^j + \zeta^{-j}\}_{j=1}^n$.
- *Proposition.* Let $\alpha = (1-\zeta)(1-\zeta^{-1})$ then
$$\frac{1}{p}\,\mathrm{Tr}\,(\alpha x y)$$
is isomorphic to the unit form $< 1, \ldots, 1 >$ of degree n.
- Using the above proposition, we constructed rotated cubic lattices for
$n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \ldots$
- By the previous Theorem, the minimum product distance is given by
$d_{p,min} = 1/\sqrt{d_K} = p^{-\frac{n-1}{2}}$, since $d_K = p^{\frac{p-3}{2}} = p^{n-1}$.

Cyclotomic construction in dimension $n = (p-1)/2$ *(cont.)*

- The lattice generated by the ring of integers has the $n \times n$ generator matrix $\mathbf{M}$ with elements $M_{k,j} = 2\cos\left(\frac{2\pi kj}{p}\right)$.

- The twisting element can be represented by the diagonal matrix

$$\mathbf{A} = \mathrm{diag}\left(\sqrt{\sigma_k(\alpha)}\right)$$

- The basis transformation matrix is given by

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

- Finally the rotated cubic lattice generator matrix is given by

$$\mathbf{R} = \frac{1}{\sqrt{p}}\mathbf{TMA}$$

Minimum product distances for the cyclotomic construction

n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$	n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$
2	$1/\sqrt{5}$	0.66874030	15	$1/31^7$	0.20138689
3	$1/7$	0.52275795	18	$1/\sqrt{37^{17}}$	0.18174408
5	$1/11^2$	0.38321537	20	$1/\sqrt{41^{19}}$	0.17136718
6	$1/\sqrt{13^5}$	0.34344479	21	$1/43^{10}$	0.16678534
8	$1/\sqrt{17^7}$	0.28952001	23	$1/47^{11}$	0.15859921
9	$1/19^4$	0.27018738	26	$1/\sqrt{53^{25}}$	0.14825905
11	$1/23^5$	0.24045444	29	$1/59^{14}$	0.13967089
14	$1/\sqrt{29^{13}}$	0.20942547	30	$1/\sqrt{61^{29}}$	0.13711677

Cyclic construction in prime dimensions

- Let K be a cyclic extension of $\mathbf{Q}$ of prime degree $n > 2$.
- Based on the work of Erez (1988) we consider lattices constructed using the ideal $\mathcal{A}$ of O_K such that its square is the codifferent, i.e.,

$$\mathcal{A}^2 = \mathcal{D}_{K/\mathbf{Q}}^{-1}.$$

- Since a Galois extension of odd degree is totally real, we construct rotated cubic lattices with full diversity $L = n$.
- The construction is based on the existence a trace form over $\mathcal{A}$, which is isomorphic to the unit form up to a scaling factor.
- Let p be an odd prime. Depending on the ramification of p in O_K, we derive three different classes of lattices:
  1. Case I: $p > n$ is the only prime which ramifies.
  2. Case II: $p = n$ is the only prime which ramifies.
  3. Case III: there are at least two primes p_1 and p_2 that ramify.

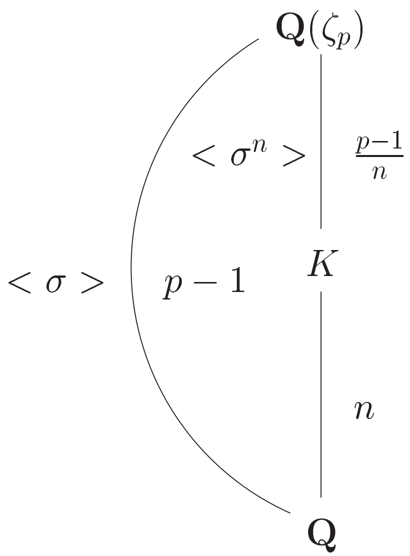
Case I

- *Proposition.* Let p such that $p \equiv 1 \pmod{n}$. Let r be a primitive element $\pmod{p}$, $\alpha = \prod_{i=0}^{m-1}(1-\zeta^{r^i})$, $m = \frac{p-1}{2}$ and let λ be such that $\lambda(r-1) \equiv 1 (\bmod\, p)$. Define $z = \zeta^{\lambda}\alpha(1-\zeta)$ and

$$x = \mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(z) = \sum_{j=1}^{\frac{p-1}{n}} \sigma^{jn}(z).$$

  Then we have $\mathrm{Tr}_{K/\mathbb{Q}}(x\sigma^t(x)) = \delta_{0,t}\, p^2$, $t = 0, \ldots, n-1$.

-

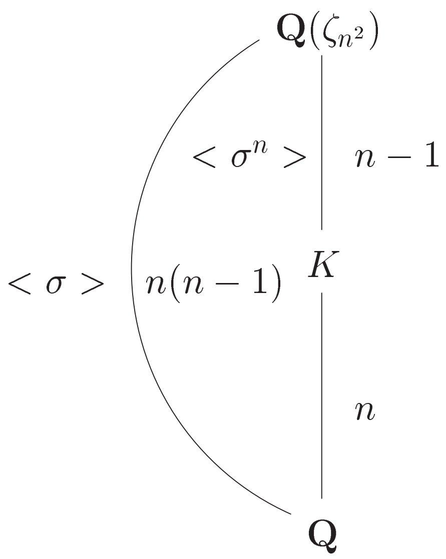


Case II

- If only the odd prime $p = n$ ramifies in K, we can embed K in $\mathbf{Q}(\zeta_{n^2})$, where $\mu = \zeta_{n^2}$ is a primitive n^2th root of unity.

- *Proposition.* Let $T = \mathrm{Tr}_{\mathbf{Q}(\mu)/K}(\mu) = \sum_{j=1}^{n-1} \sigma^{nj}(\mu)$. Then
$$\mathrm{Tr}_{K/\mathbf{Q}}((1+T)\sigma^t(1+T)) = \delta_{0,t} n^2, \qquad t = 0, \ldots, n-1.$$

-



Mixed construction

- *Proposition.* Let K be the compositum of N Galois extensions K_j of degree n_j, (i.e., the smallest field containing all K_j) with coprime discriminant i.e., $(d_{K_i}, d_{K_j}) = 1, \forall i \neq j$. Assume there exists an α_j such that the trace form over K_j, $\mathrm{Tr}\,(\alpha_j xy)$, is isomorphic to the unit form $< 1, \ldots, 1 >$ of degree n_j for $j = 1, \ldots, N$. Then the form over K

$$\mathrm{Tr}\,(\alpha_1 xy) \otimes \cdots \otimes \mathrm{Tr}\,(\alpha_N xy)$$

is isomorphic to the unit form $< 1, \ldots, 1 >$ of degree $n = \prod_{j=1}^{N} n_j$.

- The lattice generator matrix can be immediatly obtained as the tensor product of the generator matrices $\mathbf{M}^{(j)}$ corresponding to the forms $\mathrm{Tr}\,(\alpha_j xy)$, for $j = 1, \ldots, N$

$$\mathbf{M} = \mathbf{M}^{(1)} \otimes \cdots \otimes \mathbf{M}^{(N)}.$$

- Using as components two cyclotomic constructions we are now able to construct rotated cubic lattices in other dimensions such as $n = 10, 12, 16, 22, 24, 27, 28, \ldots$

- The case $n = 4$ can be obtained combining the two distinct rotated square lattices and the case $n = 25$ can be obtained combining the two rotated cubic lattices of dimension 5 constructed using Case I and Case II cyclic constructions.

Minimum product distance for the mixed construction

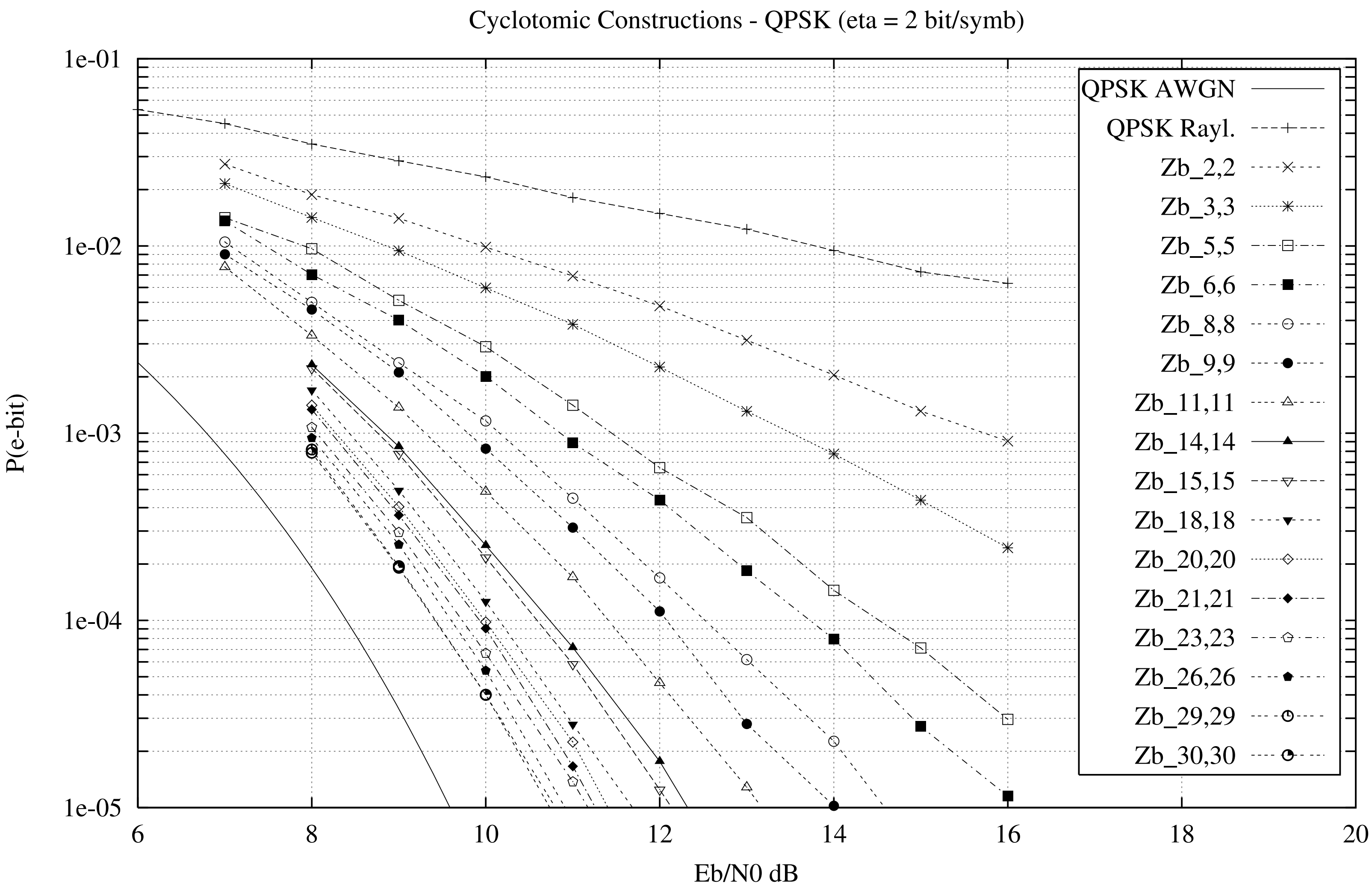
- *Proposition.* Let $K = K_1 K_2$ be the compositum of two Galois extensions of degree n_1 and n_2, with coprime discriminant. The discriminant of K is $d_K = d_{K_1}^{m_1} d_{K_2}^{m_2}$, where $m_j = [K : K_j] = n/n_j$, $j = 1, 2$.

- As a direct consequence, we have that for the mixed construction

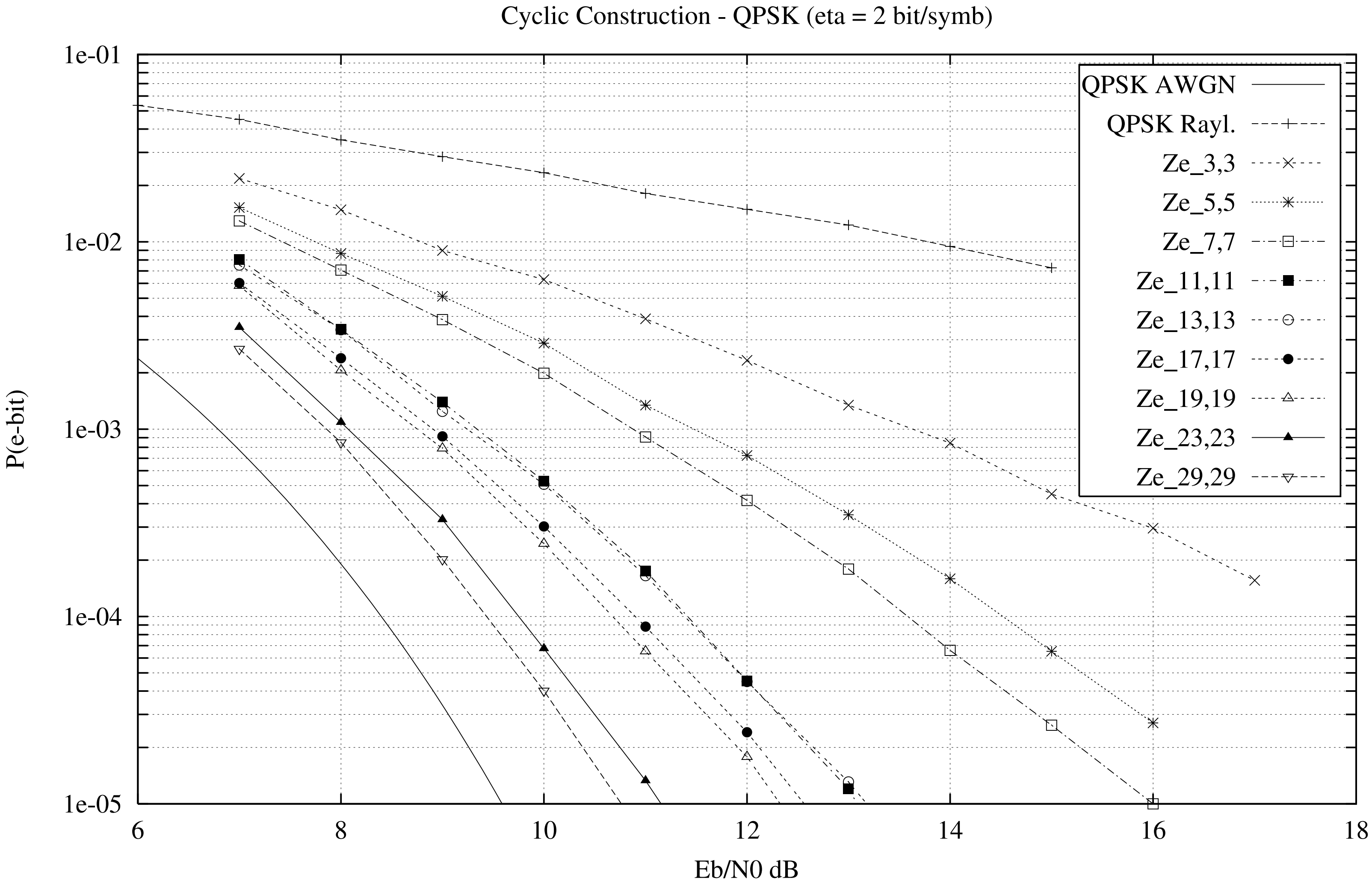
$$d_{p,min} = \frac{1}{\sqrt{d_{K_1}^{m_1} d_{K_2}^{m_2}}}.$$

n	Cyclotomic constructions	Cyclic constructions	Mixed constructions
2	0.66874030	-	-
3	0.52275795	0.52275795	-
4	-	-	0.02500000
5	0.38321537	0.38321537	-
6	0.34344479	-	0.34958931
7	-	0.23618809	-
8	0.28952001	-	-
9	0.27018738	-	-
10	-	-	0.25627156
11	0.24045444	0.24045444	-
12	-	-	0.22967537
13	-	0.16002224	-
14	0.20942547	-	-
15	0.20138689	-	0.20032888
16	-	-	0.19361370
17	-	0.11292301	-
18	0.18174408	-	0.18068519
19	-	0.08308268	-
20	0.17136718	-	-
21	0.16678534	-	-
22	-	-	0.16080157
23	0.15859921	0.15859921	-
24	-	-	0.15134889
25	-		0.10574672
26	0.14825905	-	-
27	-	-	0.14124260
28	-	-	0.14005125
29	0.13967089	0.13967089	-
30	0.13711677	-	0.13161332

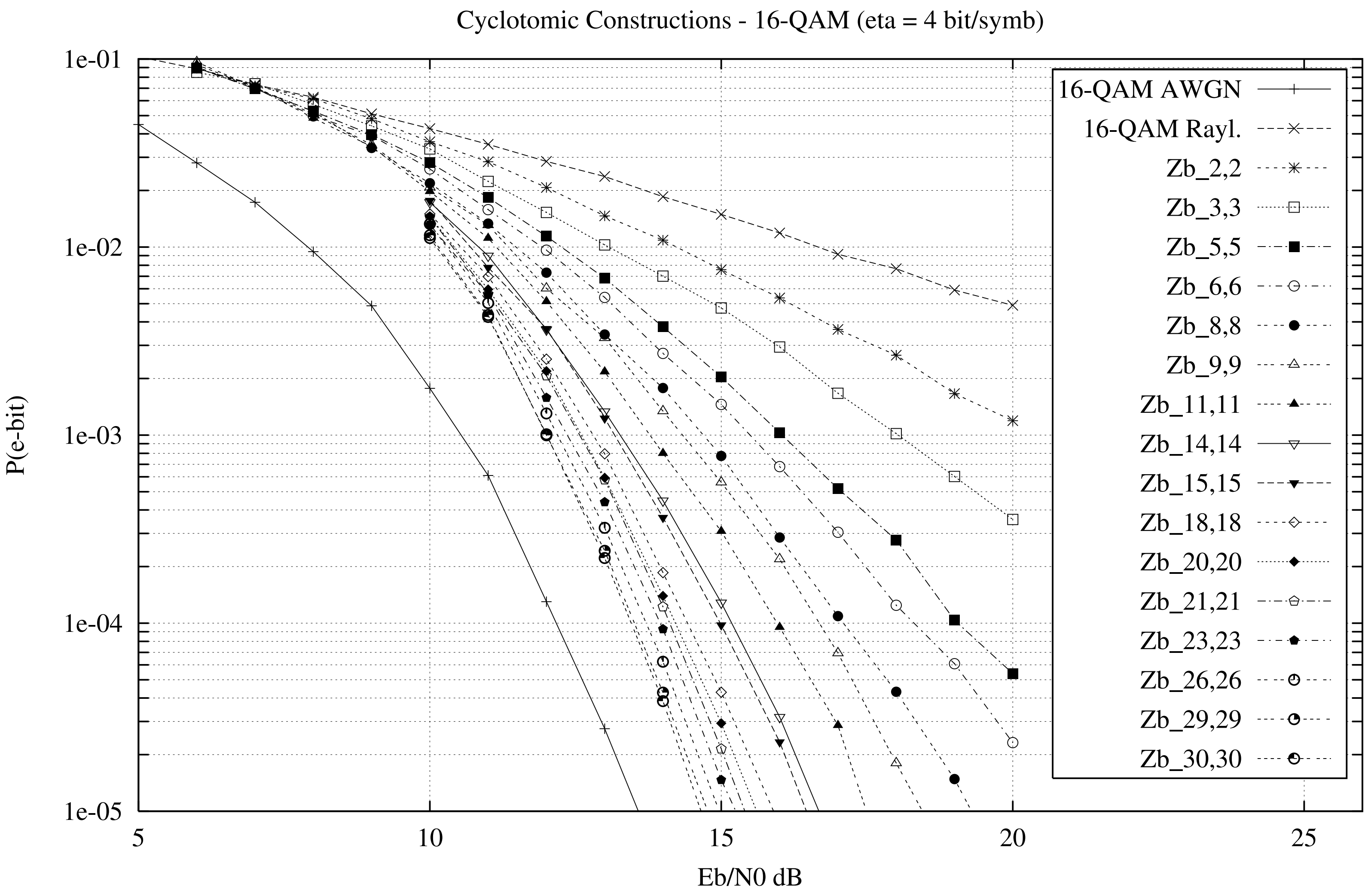
BER for $L = n$, $n =$, 2 bits/symbol



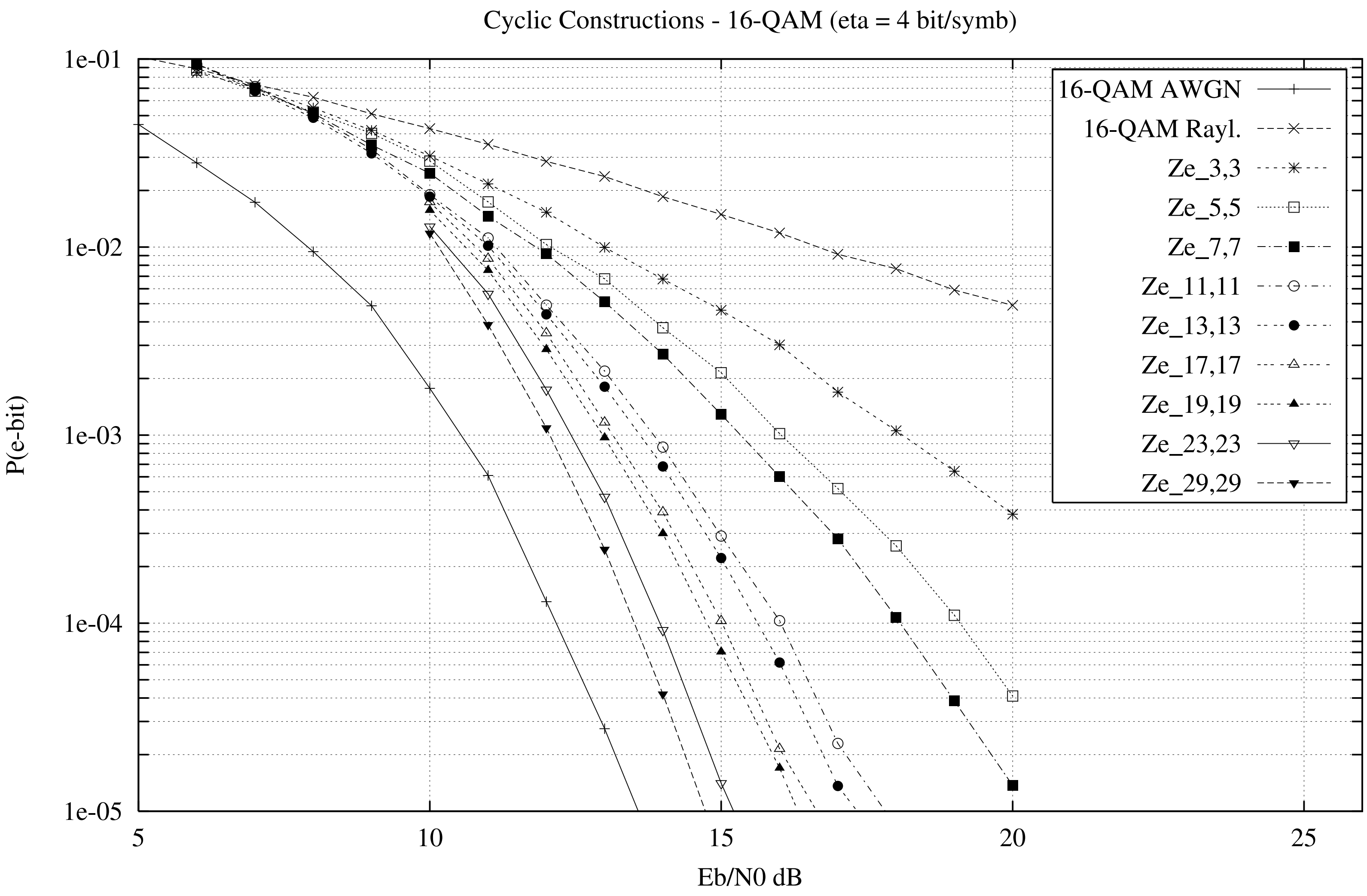
BER for $L = n$, $n =$, 2 bits/symbol



BER for $L = n$, $n =$, 4 bits/symbol



BER for $L = n$, $n =$, 4 bits/symbol



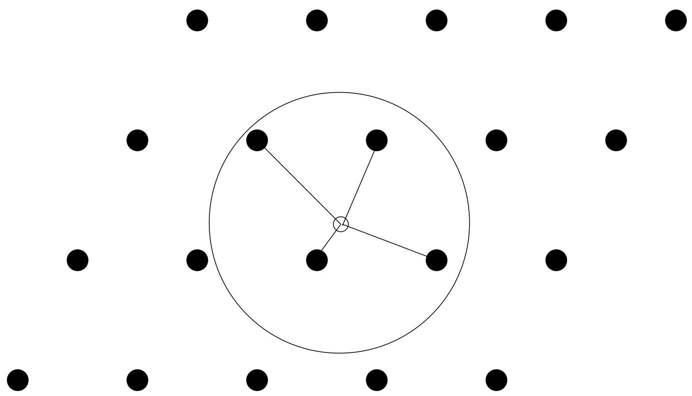
Conclusions and future research

- We have presented some new algebraic constructions of full-diversity rotated cubic lattices using the theory of ideal lattices: one based on cyclotomic fields, the other based on cyclic fields.
- We also provided a way of combining the constructions in order to obtain some missing dimensions.
- The performance in terms of minimum product distance is clearly given by means of explicit formulas related to the field discriminant.
- The cyclotomic constructions give better results in terms of $d_{p,min}$ when compared to the cyclic ones in the same dimension.
- The cyclotomic, cyclic and mixed constructions enable to build a rotated cubic lattice for all dimensions from 2 to 30.
- Future work will involve the search for maximal minimum product distance rotated cubic lattices in every dimension.

Some references

- E. Bayer-Fluckiger, "Lattices and Number Fields," *Contemporary Mathematics*, vol. 241,pp. 69–84, 1999.
- J. Boutros, E. Viterbo, C. Rastello, and J.C. Belfiore: "Good Lattice Constellations for both Rayleigh Fading and Gaussian Channels," *IEEE Transactions on Information Theory*, vol. 42, n. 2, pp. 502–518, March 1996.
- J. Boutros and E. Viterbo, "Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1453–1467, July 1998.
- B. Erez, "The Galois Structure of the Trace form in Extensions of Odd Prime Degree," *J. of Algebra*, vol. 118, pp. 438–446, 1988.
- E. Viterbo and J. Boutros: "A Universal Lattice Code Decoder for Fading Channels," *IEEE Transactions on Information Theory*, vol. 45, n. 5, pp. 1639–1642, July 1999.

Sphere Decoding Algorithm (Finke and Pohst, 1985)



- We search for the closest lattice point by enumerating all points inside a given sphere of radius $\sqrt{C}$ centered at the received point.
- The sphere radius $\sqrt{C}$ must be properly chosen to reduce the total number of operations.
- Complexity does not depend on the constellation size.
- Complexity depends only on dimension and point distribution:
  it is polynomial in n but exponential in C.

Sphere Decoding (cont.)

- If we set the received point $\mathbf{y} = \mathbf{0}$: enumeration of points around the origin.
- $\mathbf{x} = \mathbf{M}\mathbf{z} \in \Lambda, \quad \Lambda \subset \mathbf{R}^n \quad$ and $\quad \mathbf{z} \in \mathbf{Z}^n$
- $Q(\mathbf{z}) = ||\mathbf{x}||^2 = \mathbf{x}^t\mathbf{x} = \mathbf{z}^t\mathbf{G}\mathbf{z}, \qquad \mathbf{G} = \mathbf{M}^t\mathbf{M} = [g_{ij}]$ is the Gram matrix.
- Solve the inequality $Q(\mathbf{z}) \leq C$, i.e. find all points $||\mathbf{x}|| \leq \sqrt{C}$.
- We apply the Fincke-Pohst algorithm to solve the above inequality.
- If d^{-1} is a lower bound for the eigenvalues of $\mathbf{G}$, the number of arithmetical operations is

$$O(n^2 \times \left(1 + \frac{n-1}{4dC}\right)^{4dC})$$

- When $\mathbf{y} \neq 0$. Minimize $||\mathbf{x} - \mathbf{y}||$ where $\mathbf{y} = \mathbf{M}\rho$ and $\rho = (\rho_1, \ldots, \rho_n) \in \mathbf{R}^n$.
  Modify the quadratic form inequality by adding ρ.

Solving $Q(x) \leq C$

$$Q(\mathbf{z}) = \sum_{i=1}^{n} \sum_{j=1}^{n} g_{ij} z_i z_j$$

and after Cholesky decomposition

$$Q(\mathbf{z}) = \sum_{i=1}^{n} q_{ii}(z_i + \sum_{j=i+1}^{n} q_{ij} z_j)^2 = \sum_{i=1}^{n} q_{ii} {Z_i}^2$$

In dimension 2, $Z_2 = z_2, Z_1 = z_1 + q_{12} z_2$ and $Q(\mathbf{z}) = q_{11} {Z_1}^2 + q_{22} {Z_2}^2 \leq C$.
In the new coordinate system, the value of each component of a point inside the ellipsiod, can be bounded as follows :

$$|Z_2| \leq \sqrt{\frac{C}{q_{22}}} \qquad |Z_1| \leq \sqrt{\frac{C - q_{22} {Z_2}^2}{q_{11}}}$$

The bounds of the integer components are :

$$-\sqrt{\frac{C}{q_{22}}} \leq z_2 \leq \sqrt{\frac{C}{q_{22}}}$$

$$-\sqrt{\frac{C - q_{22} {z_2}^2}{q_{11}}} - q_{12} z_2 \leq z_1 \leq \sqrt{\frac{C - q_{22} {Z_2}^2}{q_{11}}} - q_{12} z_2$$

Example: $\Lambda_{3,2}$ *Dimension=3 Diversity=2*

- The number field is $K = \mathbf{Q}(\theta)$ where θ is a primitive element with minimal polynomial $\mu_\theta(x) = x^3 - x - 1$.
- The field signature is $r_1 = 1$ and $r_2 = 1$.
- The roots are $\theta_1 = U + V$ and $\theta_{2,3} = -\frac{1}{2}(U+V) \pm i\frac{\sqrt{3}}{2}(U-V)$ where $U = \frac{1}{3}\sqrt[3]{\frac{9+3\sqrt{63}}{2}}$ and $V = \frac{1}{3}\sqrt[3]{\frac{9-3\sqrt{63}}{2}}$.
- $\theta = \theta_2$ and an integral basis is $1, \theta, \theta^2$.
- The 3 embeddings are $\sigma_1(\theta) = \theta_1$ (real), $\sigma_2(\theta) = \theta_2$ and $\sigma_3(\theta) = \theta_3$.
- We obtain the lattice generator matrix:

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 0 \\ (U+V) & -\frac{1}{2}(U+V) & \frac{\sqrt{3}}{2}(U-V) \\ (U+V)^2 & -\frac{1}{2}(U^2+V^2-4UV) & -\frac{\sqrt{3}}{2}(U^2-V^2) \end{pmatrix}$$

Known dense lattices from cyclotomic fields
Bayer's and Craig's constructions

$n = \phi(N)$	$K = \mathbf{Q}(\theta)$, $\theta = e^{2j\pi/N}$	N	$I = \alpha O_K + \beta O_K$
$D_{4,2}$	$\theta^4 + 1$	8	$(2, \theta + 1)$
$E_{6,3}$	$\theta^6 - \theta^3 + 1$	9	$(3, (\theta + 1)^2)$
$E_{8,4}$	$\theta^8 - \theta^6 + \theta^4 - \theta^2 + 1$	20	$(5, \theta - 2)$
$K_{12,6}$	$\theta^{12} - \theta^{11} + \theta^9 - \theta^8 +$ $+\theta^6 - \theta^4 + \theta^3 - \theta + 1$	21	$(7, \theta + 3)$
$\Lambda_{16,8}$	$\theta^{16} - \theta^{12} + \theta^8 - \theta^4 + 1$	40	$(2, \theta^4 + \theta^3 + \theta^2 + \theta + 1)$ $(5, \theta^2 + 2)$
$\Lambda_{24,12}$	$\theta^{24} - \theta^{23} + \theta^{21} - \theta^{20} + \theta^{18} - \theta^{17} + \theta^{15} - \theta^{14}$ $+\theta^{12} - \theta^{10} + \theta^9 - \theta^7 + \theta^6 - \theta^4 + \theta^3 - \theta + 1$	39	$(3, \theta^3 + \theta^2 - 1)$ $(3, \theta^3 + \theta^2 + \theta + 1)$ $(13, \theta - 3)$

- The above dense sphere packing lattices have a modulation diversity $L = n/2$.
- They are sublattices of a rotated version of the cubic lattice $\mathbf{Z}^n$.

Case III

- *Proposition.* Let K_1, K_2 be two disjoint Galois extensions of $\mathbf{Q}$, whose discriminants are relatively prime. Let $G_i =$Gal$(K_i/\mathbf{Q})$ for $i = 1, 2$ and $G_1 =< \sigma >$, $G_2 =< \tau >$ be cyclic of order n. Let $K \subseteq K_1K_2$ be another cyclic extension of order n. If there exist $x_i \in K_i$, $i = 1, 2$ which satisfy

  1. $\mathrm{Tr}_{K_1/\mathbf{Q}}(x_1\sigma^t(x_1)) = \delta_{0,t}p_1^2,\ t = 0, \ldots, n-1$
  2. $\mathrm{Tr}_{K_2/\mathbf{Q}}((x_2\tau^t(x_2)) = \delta_{0,t}p_2^2,\ t = 0, \ldots, n-1$

  then there exists $x \in K$, given by $x =\mathrm{Tr}_{K_1K_2/K}(x_1x_2)$, such that

  $$\mathrm{Tr}_{\,K/\mathbf{Q}}(x\gamma^t(x)) = \delta_{0,t}p_1^2p_2^2, \quad t = 0, \ldots, n-1$$

  where $< \gamma >= Gal(K/\mathbf{Q})$.

Examples of parameters for Case I

n	p	r	λ
3*	7	3	4
3	13	2	1
5*	11	2	1
5	31	3	16
7	29	2	1
11*	23	5	6
11	67	2	1
13	53	2	1
17	103	5	26
19	191	19	138
23*	47	5	12
29*	59	2	1