Introduction aux communications numériques: une application de la théorie algébrique des nombres

Séminaire de Théorie des Nombres, Algorithmique et Cryptographie

Emanuele Viterbo

Dipartimento di Elettronica

Politecnico di Torino, Italy

`viterbo@polito.it`

Slides available at:

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

The codebook

- Digital transmission over the 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 $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{S}$ conveniently represents a band-limited signal to be transmitted by the source.
- The source labels each point with $\log_2(M)$ bits (bit labelling).
- The 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

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

- $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbf{R}^n$ received signal vector
- $\mathbf{x} = (x_1, \ldots, x_n)$ 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*: $\mathbf{H} = \mathbf{I}$
2. *Slow (or block) fading*: $\mathbf{H} = h\mathbf{I}$ and h changes independently from one 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 is available at the receiver, ML detection is given by
$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathcal{S}} \|\mathbf{y} - \mathbf{H}\mathbf{x}\|^2 = \arg\min_{\mathbf{x}'\in\mathcal{S}'} \|\mathbf{y} - \mathbf{x}'\|^2$$
where $\mathcal{S}' = \mathbf{H}\mathcal{S}$ is the "faded signal constellation".

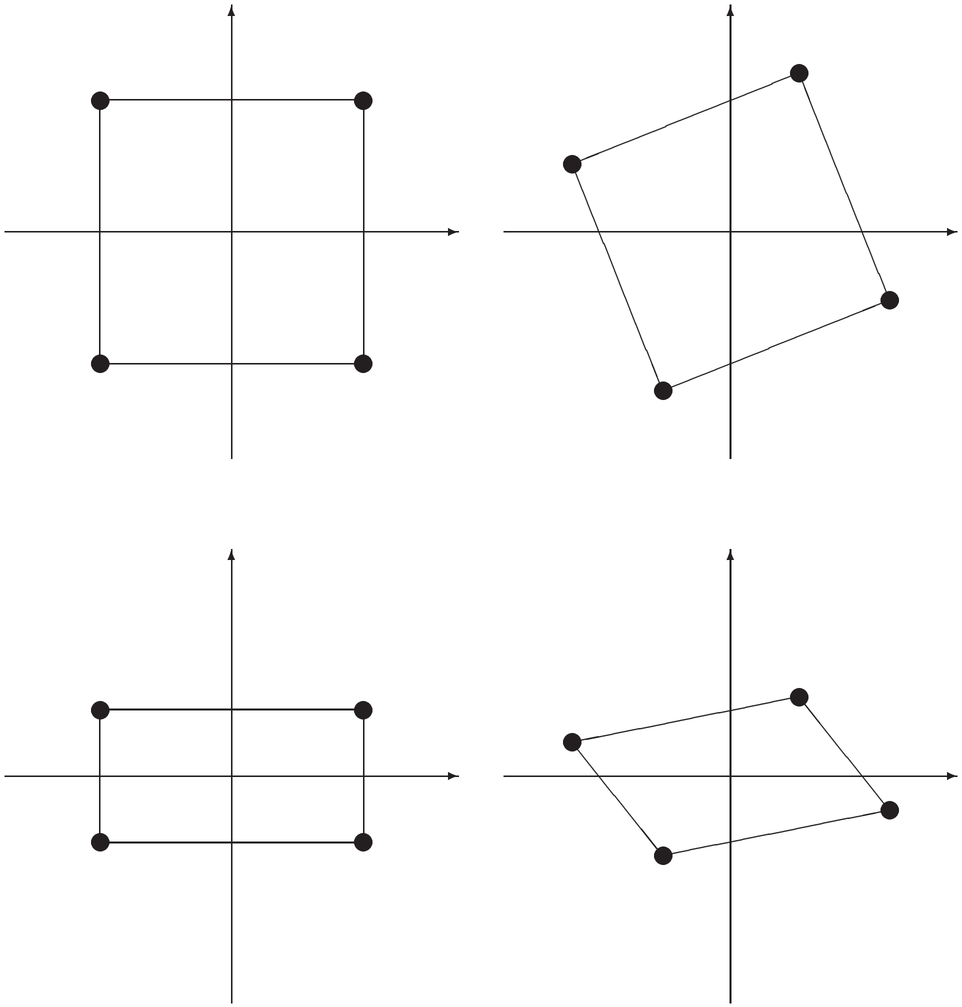
- The complexity of the ML receiver greatly depends on the structure of the code $\mathcal{S}$.

- 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*.

Example

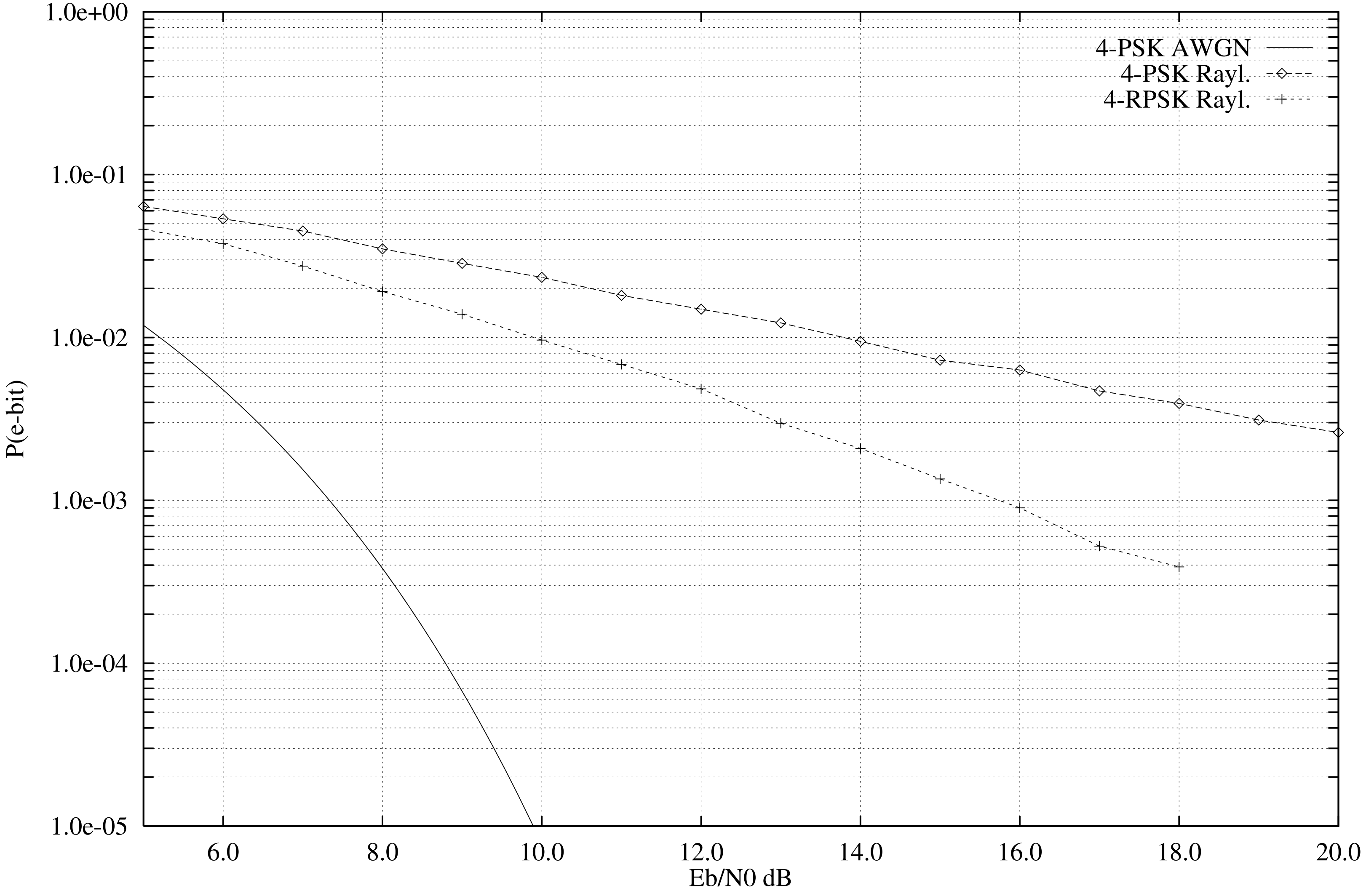


S *AWGN*

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

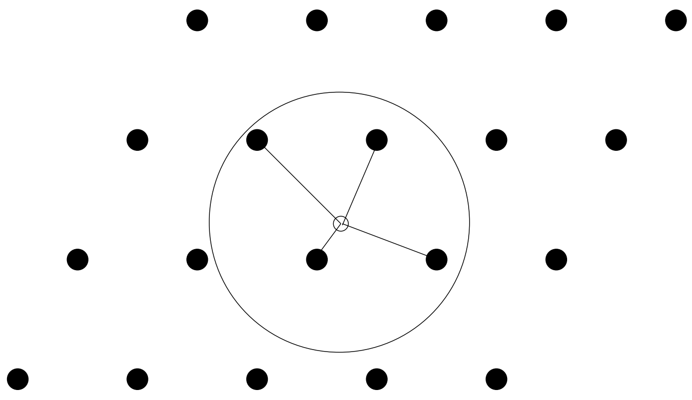
1. Maximize the *modulation diversity* $L = \min_{\mathbf{x},\mathbf{w} \in S}(l)$, since when $L \to \infty$ performance approaches the AWGN case.
2. Maximize the *minimum L-product distance* $d_{p,min}^{(L)} = \prod_{x_i \neq w_i}^{(L)} |x_i - w_i|$.

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 lattices.
  On the AWGN channel the error probability is related to the *Hermite constant* of the lattice:
  $$\gamma(\Lambda) = \frac{d_{E,min}^2}{[det(\Lambda)]^{2/N}} .$$
- 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 S is a lattice with generator matrix G then S' is also a lattice with generator matrix HG.
- Algebraic number theory is the mathematical tool which enables to construct lattices with high diversity and good $d_{p,min}$.

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.
- $\mathbf{x} = \mathbf{M}\mathbf{z} \in \Lambda, \quad \Lambda \subset \mathbf{R}^n$ and $\mathbf{z} \in \mathbf{Z}^n$
- $Q(\mathbf{z}) = ||\mathbf{x}||^2 = \mathbf{x}^t\mathbf{x} = \mathbf{z}^t\mathbf{G}\mathbf{z}, \qquad \mathbf{G} = \mathbf{M}^t\mathbf{M} = [g_{ij}]$ 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 :

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

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

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 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

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

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

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

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

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:

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

Modulation Diversity of Algebraic Lattices

- *Theorem.* The lattices obtained from the previous generator matrix exhibit a diversity $L = r_1 + r_2$.

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

$$\mathbf{z} = (z_1, z_2, \ldots z_n) = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i$$

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

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

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

  - $\beta = 1 \in O_K \Rightarrow L = r_1 + r_2$

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

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

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

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

- It is useful to maximize the minimum product distance in the lattice (next talk)

Lattices from Integral Ideals

- Any non-zero ideal I of O_K can be written as $I = \gamma_1 \mathbf{Z} + \gamma_2 \mathbf{Z} + \ldots + \gamma_n \mathbf{Z}$. The set $\{\gamma_i, i = 1 \ldots n\}$ is called a $\mathbf{Z}$-basis of I.

- After applying the canonical embedding to the ideal I, we obtain the lattice $\Lambda_I = \sigma(I)$ of rank n included in $\Lambda = \sigma(O_K)$.

- The generator matrix G_I of Λ_I is given by

$$G_I = \begin{pmatrix} \sigma_1(\gamma_1) & \ldots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \ldots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\gamma_n) & \ldots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{pmatrix}$$

- The fundamental volume of $\Lambda_I = \sigma(I)$ is

$$vol(\Lambda_I) = N(I) \times 2^{-r_2} \times \sqrt{|d_K|}$$

Lattices from the Ring of Integers

	$\mu_\theta(x)$	$vol(\Lambda_{n,L})$	$\gamma(\Lambda_{n,L})\mathrm{dB}$
$\Lambda_{2,1}$	$x^2 - x + 1$	0.8660	0.624
$\Lambda_{2,2}$	$x^2 - x - 1$	2.2361	-0.484
$\Lambda_{3,2}$	$x^3 - x - 1$	2.3979	0.242
$\Lambda_{3,3}$	$x^3 + x^2 - 2x - 1$	7	-0.862
$\Lambda_{4,2}$	$x^4 - x^3 - x^2 + x + 1$	2.7042	0.850
$\Lambda_{4,3}$	$x^4 - x^3 + 2x - 1$	8.2916	0.178
$\Lambda_{4,4}$	$x^4 - x^3 - 3x^2 + x + 1$	26.9258	-1.130
$\Lambda_{5,3}$	$x^5 - x^3 + x^2 + x - 1$	10.0281	0.597
$\Lambda_{5,4}$	$x^5 - 2x^3 + x^2 - 1$	33.5820	-0.083
$\Lambda_{5,5}$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	121	-1.341
$\Lambda_{6,3}$	$x^6 - 3x^5 + 4x^4 - 4x^3 + 4x^2 - 2x + 1$	12.3409	1.133
$\Lambda_{6,4}$	$x^6 - 2x^5 + 3x^3 - 2x - 1$	41.8606	0.379
$\Lambda_{6,5}$	$x^6 + x^5 - 2x^4 - 3x^3 - x^2 + 2x + 1$	152.2982	-0.285
$\Lambda_{6,6}$	$x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1$	547.8367	-1.347
$\Lambda_{7,7}$	$x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1$	4487.1364	-1.983
$\Lambda_{8,4}$	$x^8 - 2x^7 + 4x^5 - 4x^4 + 3x^2 - 2x + 1$	70.0928	1.406
$\Lambda_{8,8}$	$x^8 + 2x^7 - 7x^6 - 8x^5 + 15x^4 + 8x^3 - 9x^2 - 2x + 1$	16801.7980	-1.532

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 od the cubic lattice $\mathbf{Z}^n$.

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.
- Build algebraically the totally complex lattices $\mathbf{Z}_{n,n/2}$.

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

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

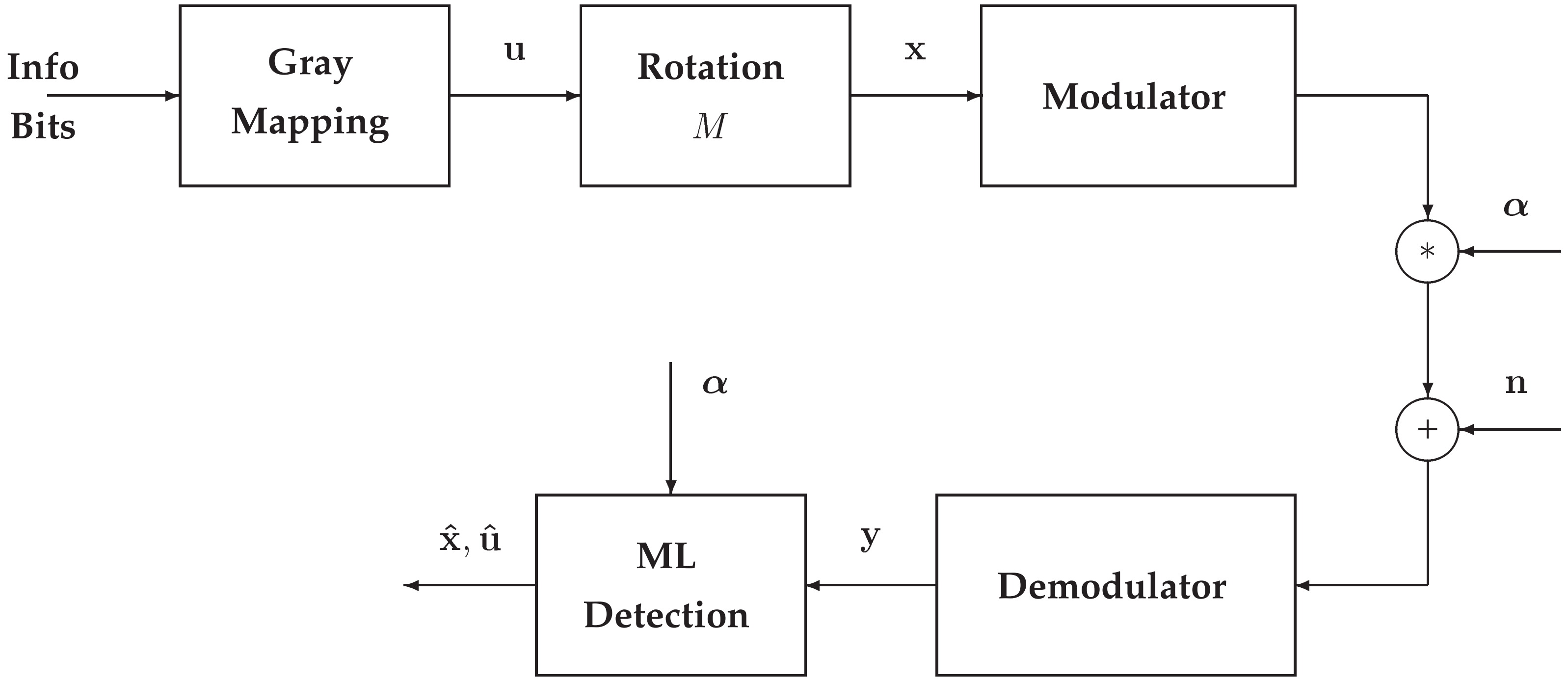
$$\epsilon = 0 \;\; if \;\; n = 2^{e_1} \quad and \quad \epsilon = -1 \;\; if \;\; n = 2^{e_1}3^{e_2}$$

  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 the totally real lattices $\mathbf{Z}_{n,n}$

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

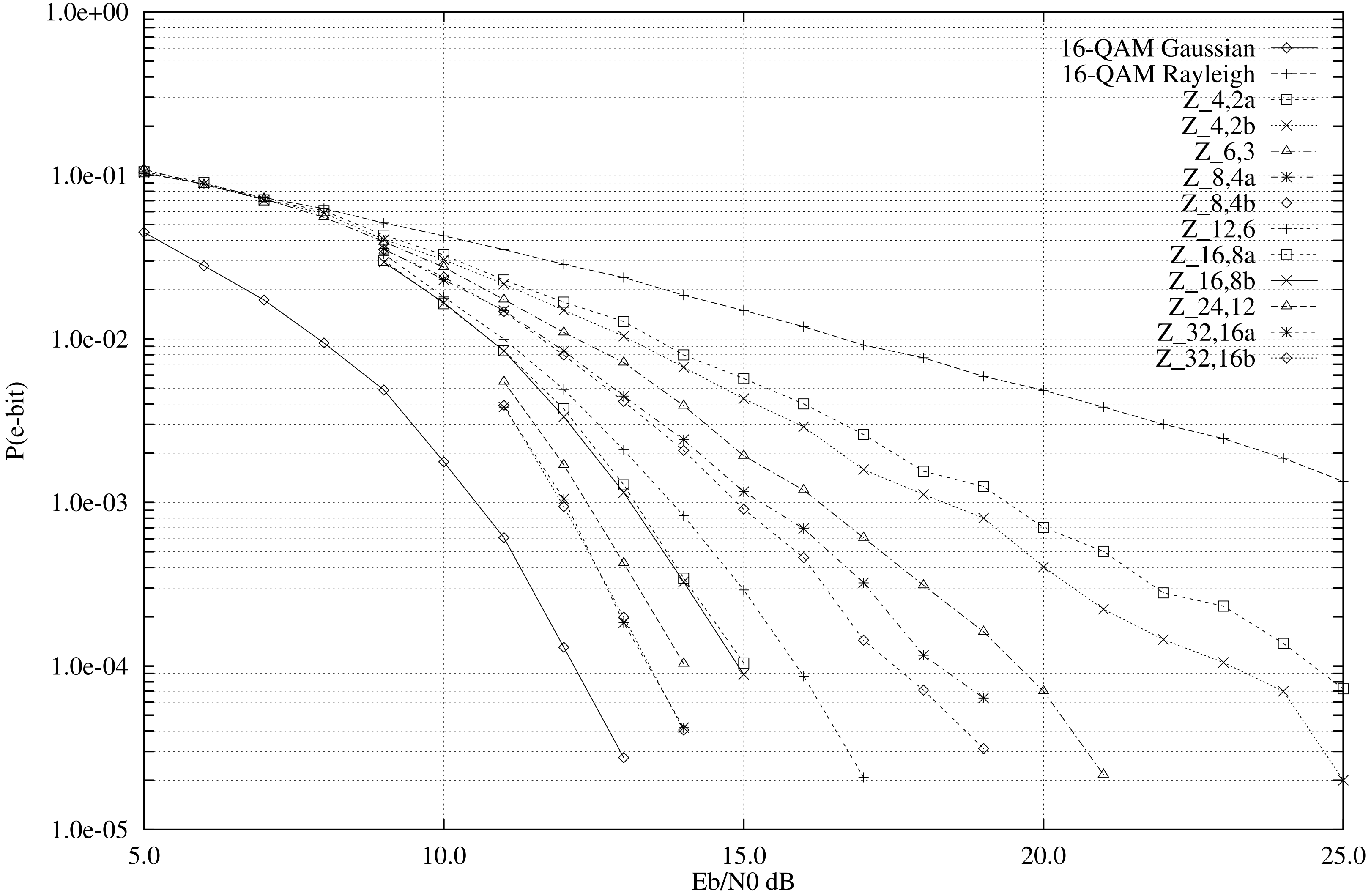
  The lattice dimension $n = \phi(N)/2$
  Examples : $\mathbf{Z}_{3,3}$, $\mathbf{Z}_{5,5}$, $\mathbf{Z}_{9,9}$, $\mathbf{Z}_{11,11}$, $\mathbf{Z}_{15,15}$.
- Some better constructions will be shown in the next talk.

System model



- $\mathbf{u} = (u_1, \ldots u_n)$ $u_i = \pm 1, \pm 3, \ldots$ is an n-dimensional QAM signal point.
- Transmitted vector $\mathbf{x} = \mathbf{u}M$ where M is the generator matrix of a rotated cubic lattice $Z_{n,L}$.

BER for $L = n/2$***,*** $n = 2^{e_1}3^{e_2}$***, 4 bits/symbol***



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