Number Fields and Modulations for the Fading Channels

Joseph Boutros and Emanuele Viterbo

E.N.S.T, Paris, France
and
Politecnico di Torino, Torino, Italy

The Fading Channel Model

We define a simple model for mobile radio transmission channels.

- A **signal constellation** S is a set of M points $\mathbf{x} = (x_1, \ldots x_n) \in \mathbf{R}^n$. Each point represents a signal of an n-dimensional modulation scheme.
- Each transmitted point can be labeled with $\log_2 M$ bits.
- The **Rayleigh Fading Channel** outputs

$$y_i = g_i x_i + n_i, \quad i = 1, \ldots n \qquad \text{or} \qquad \mathbf{y} = \mathbf{g} \odot \mathbf{x} + \mathbf{n}$$

where:
– $g_i \geq 0$ are the **Fading Coefficients**: real independent Rayleigh distributed random variables with $E\{g_i^2\} = 1$
– n_i **Additive White Gaussian Noise** (AWGN) with zero mean and variance σ^2.

The receiver

- The receiver uses $\mathbf{y}$ and $\mathbf{g}$ (perfect channel state information) to obtain the *Maximum Likelihood* (ML) decision on the transmitted constellation point by

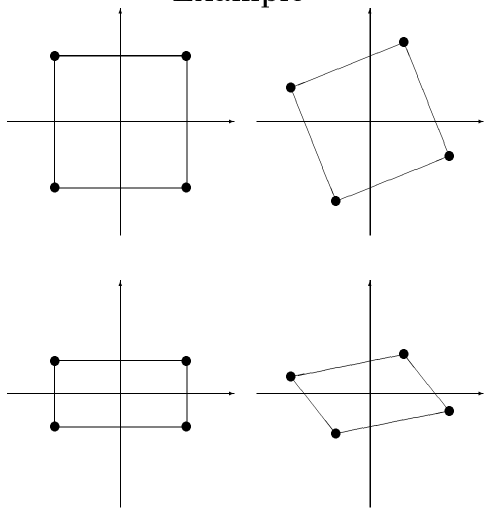
$$\min_{\mathbf{x} \in S} \|\mathbf{y} - \mathbf{g} \odot \mathbf{x}\|^2 .$$

- If all $g_i = 1$ we have the well known AWGN channel and ML detection corresponds to the minimum Euclidean distance decoding, i.e., finding the closest point of S to the received point $\mathbf{y}$.
- In the case of fading ML detection is obtained by the minimum Euclidean distance decoder applied to the "compressed" signal constellation $S_{\mathbf{g}}$ with the points $\mathbf{g} \odot \mathbf{x}$.
- The error probability is higher with fading than with AWGN channel.

Example

S

AWGN

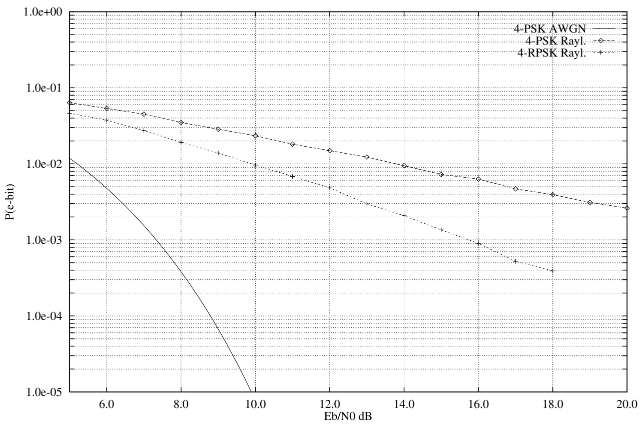


$S_{\mathbf{g}}$

Fading

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

Bit error rate 4-PSK vs. 4-RPSK



Error Probability

- **AWGN Channel**

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

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

- **Rayleigh Fading Channel**

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

where $d_p^{(l)}(\mathbf{x},\mathbf{y}) = \Pi^{(l)}_{x_i \neq y_i} |x_i - y_i|$ is the *l-product distance*.

- Good constellations for the fading channel

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

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

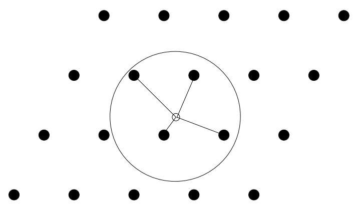
Why Lattices?

- 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 **fundamental gain**:

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

- 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 for ML detection: in fact, if S is a lattice with generator matrix G then $S_{\mathbf{g}}$ is also a lattice with generator matrix $\mathrm{diag}(\mathbf{g})G$.
- Algebraic number theory is the mathematical tool which enables to construct lattices with high diversity and good $d_{p,min}$.

Sphere Decoding Algorithm (Finke, Pohst)



- 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.

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

- Th minimal polynomial $\mu_\theta(x)$ has r_1 real roots and $2r_2$ complex roots, $n = r_1 + 2r_2$.
- There are exactly n embeddings $\sigma_i : K \to \mathbf{C}$, $\sigma_i(\theta) = \theta_i$, 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 $\sigma(\omega_1), \ldots, \sigma(\omega_n)$.

Diversity of Algebraic Lattices

- The generator matrix of the canonical embedded ring of integers is

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

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

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

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

- **Theorem** – The diversity of $\Lambda = \sigma(O_K)$ is $L = r_1 + r_2$.

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:

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

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

	$\mu_\theta(x)$	$vol(\Lambda_{n,L})$	$\gamma(\Lambda_{n,L})$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
$\Lambda_{8,4}$	$x^8 - 2x^7 + 4x^5 - 4x4 + 3x^2 - 2x + 1$	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

Dense Rotated Lattices - Craig's construction

$n = \phi(N)$	$K = \mathbf{Q}(\theta)$, $\theta = e^{2j\pi/N}$	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	$(3, \theta^3 + \theta^2 - 1)$ $(3, \theta^3 + \theta^2 + \theta + 1)$ $(13, \theta - 3)$

Lattices marked with * do not appear elsewhere in the literature, to the authors knowledge.

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

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

$$\mathbf{Z}_{n,n/2} = \sigma(\mathbf{Z}[j][\theta])$$

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

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

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 $\mathbf{Z}_{n,n}$

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

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

The direct approach

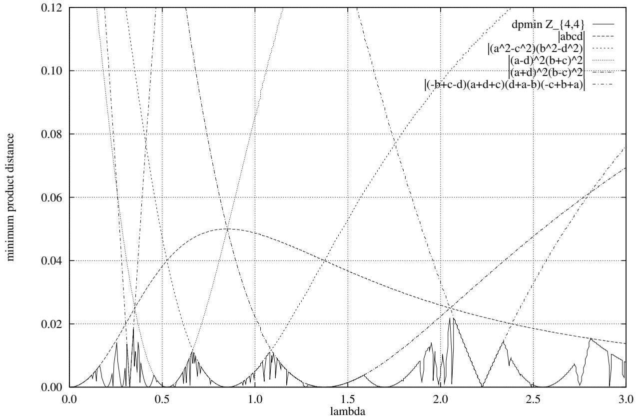
We try to build a rotation matrix M which produces a constellation with full diversity $(L = n)$ and maximum $d_{p,min}$. M must satisfy the following constraints

- $\det(M) = 1$
- The row vectors of M are orthonormal.

This constraint optimization problem has too many unknowns for a totally arbitrary matrix. We restrict ourselves to some special families of matrices.

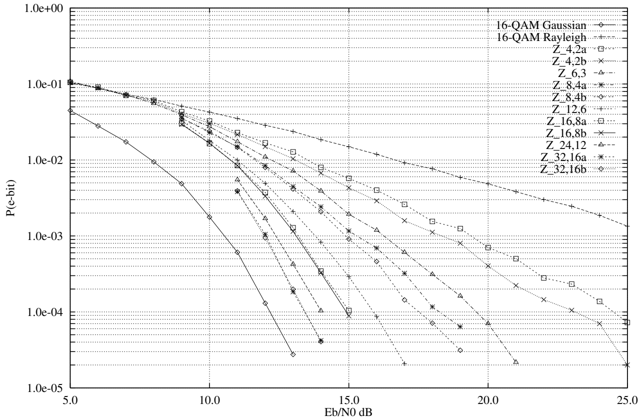
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ b & c & a \\ -c & -a & -b \end{pmatrix} \quad \begin{pmatrix} a & b & -c & -d \\ -b & a & d & -c \\ c & d & a & b \\ -d & c & -b & a \end{pmatrix} \quad \begin{pmatrix} a & b & c & -d & -e & -f \\ b & c & a & -e & -f & -d \\ -c & -a & -b & f & d & e \\ d & e & f & a & b & c \\ e & f & d & b & c & a \\ -f & -d & -e & -c & -a & -b \end{pmatrix} \quad \cdots$$

$d_{p,min}$ for a family of rotated Z_4 lattices



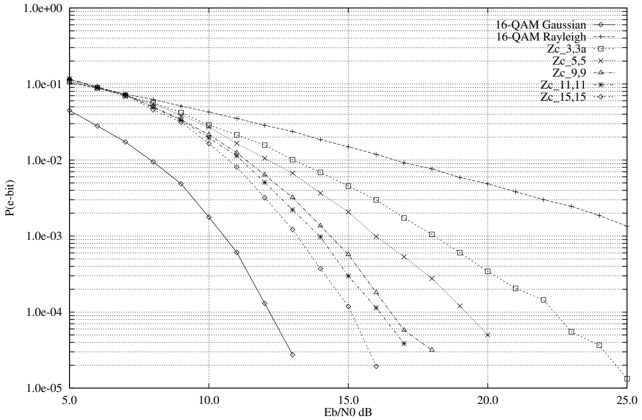
CIRM, Luminy
Sept. 30 – Oct. 4, 1996

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



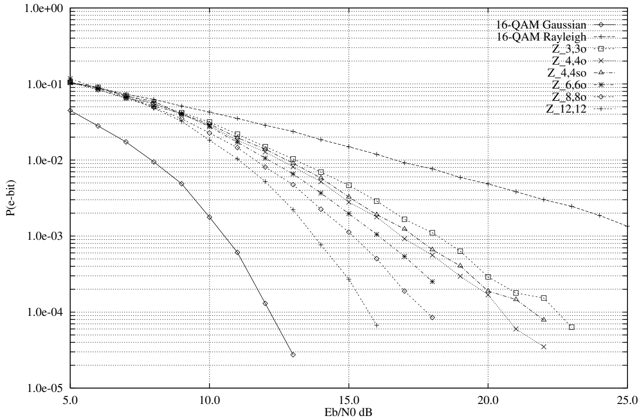
CIRM, Luminy
Sept. 30 – Oct. 4, 1996

BER for $L = n$, $n = 3, 5, 9, 11, 15$, 4 bits/symbol



CIRM, Luminy
Sept. 30 – Oct. 4, 1996

BER for $L = n$, $n = 3, 4, 6, 8, 12$, 4 bits/symbol



CIRM, Luminy
Sept. 30 – Oct. 4, 1996

Open Problems

- Give a complete classification of $Z_{n,L}$ lattices which can be obtained by some canonical embedding.
- Find other techniques to build $Z_{n,L}$ lattices.
- Reduce the lattice decoder complexity.
- Non lattice constellations.

CIRM, Luminy
Sept. 30 – Oct. 4, 1996

Euclidean lattices and modular forms