Some Wireless Communication problems involving Lattices

Jean-Claude Belfiore
Télécom ParisTech

March, 19 2013
École de Printemps d'Informatique Théorique

Autrans

Parts

Part I

Introduction to Communication Systems

Outline of current Part

1. **Signal Space and Coded Modulation**

2. Modulation - Code

The transmission problem

- Connection between **signal space** and transmitted **analog signal** through an orthogonal basis of signals

The transmission problem

- Connection between **signal space** and transmitted **analog signal** through an orthogonal basis of signals

Standard serial transmission

Transmitted signal is

$$x(t) = \sum_k x_k h(t - kT)$$

where x_k are the transmitted complex symbols and $\{h(t - kT)\}_k$ is a family of orthogonal signals (h is a Nyquist root).

The transmission problem

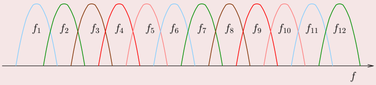
- Connection between **signal space** and transmitted **analog signal** through an orthogonal basis of signals

Standard serial transmission

Transmitted signal is

$$x(t) = \sum_k x_k h(t - kT)$$

where x_k are the transmitted complex symbols and $\{h(t-kT)\}_k$ is a family of orthogonal signals (h is a Nyquist root).



OFDM transmission

Transmitted signal is

$$x(t) = \sum_k \sum_{q=-N/2}^{N/2} x_{k,q} h(t - kT)\, e^{i\frac{2\pi k}{N+1}\Delta f t}$$

where $x_{k,q}$ are the transmitted complex symbols and $\left\{h(t-kT)\, e^{i\frac{2\pi q}{N+1}\Delta f t}\right\}_{k,q}$ is a doubly indexed family of orthogonal signals (for instance,

$$h(t) = \mathrm{rect}_T(t)$$

with $\Delta f = \frac{1}{T}$).

Complex symbols and Signal Space

- We define vector
$$\boldsymbol{x} = (x_1, x_2, \ldots, x_m)^\top$$
as a vector living in a $m-$dimensional complex space or a $n-$dimensional real space ($n = 2m$).

Complex symbols and Signal Space

- We define vector
$$\boldsymbol{x} = (x_1, x_2, \ldots, x_m)^\top$$
as a vector living in a $m-$dimensional complex space or a $n-$dimensional real space $(n = 2m)$.
- Complex symbols used in practice are QAM symbols, components of vector $\boldsymbol{x}$.

Complex symbols and Signal Space

- We define vector
$$\boldsymbol{x} = (x_1, x_2, \ldots, x_m)^\top$$
as a vector living in a m−dimensional complex space or a n−dimensional real space ($n = 2m$).
- Complex symbols used in practice are QAM symbols, components of vector $\boldsymbol{x}$.
- We need to introduce coding $\longrightarrow$ **structure** the QAM symbols.

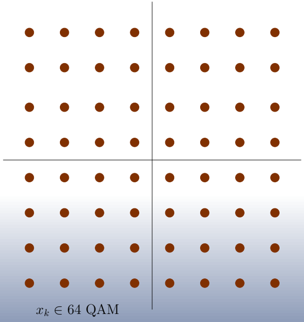


Figure: Symbol from a 64 QAM

Outline of current Part

Modulation + Code = Lattice ? ...

Modulation + Code = Lattice ? ...

What a lattice element could be

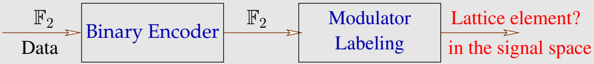


Figure: Encoder and Modulator

Modulation + Code = Lattice ? ...

What a lattice element could be

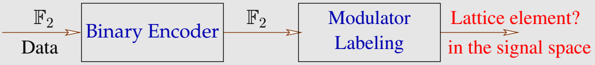


Figure: Encoder and Modulator

Requirements

- Encoder must be **linear.**
- Modulation should be **QAM** for instance.
- **Labeling** (modulator) between **binary codewords** and **modulated symbols** has to respect some criteria.

An example: the D_4 lattice (partition)

QAM Partition à la Ungerboeck

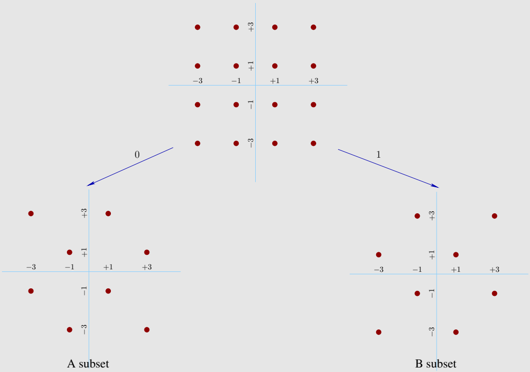


Figure: Labeling of subsets A and B

An example: the D_4 lattice (coding)

Encoder

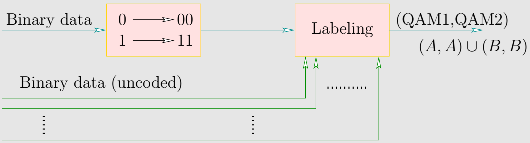


Figure: D_4 −based encoder

An example: the D_4 lattice (coding)

Encoder

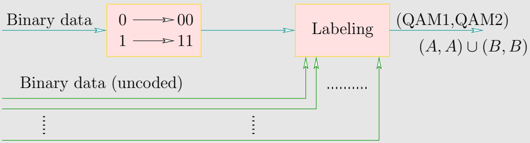


Figure: D_4−based encoder

- The binary code is the $(2, 1)$ repetition code (**linear**)
- Modulation is **QAM,** labeling is the **Ungerboeck** labeling

An example: the D_4 lattice (coding)

Encoder

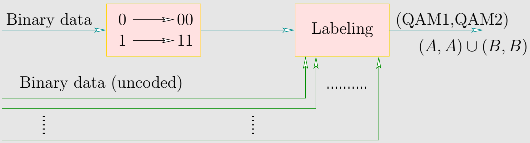


Figure: D_4−based encoder

- The binary code is the $(2,1)$ repetition code (**linear**)
- Modulation is **QAM,** labeling is the **Ungerboeck** labeling

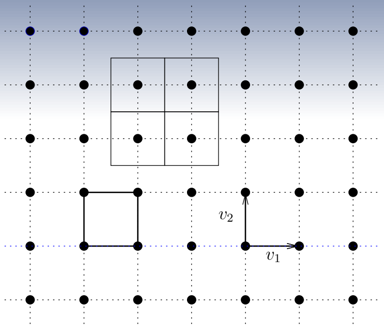
$$D_4=(1+\imath)\mathbb{Z}[\imath]^2+(2,1)_{\mathbb{F}_2} \iff D_4 \Big/ (1+\imath)\mathbb{Z}[\imath]^2 \simeq \{(0,0),(1,1)\}$$

$$\iff D_4=(1+\imath)\mathbb{Z}[\imath]^2\cup(1+\imath)\mathbb{Z}[\imath]^2+(1,1)$$

Part II

Constructing Lattices

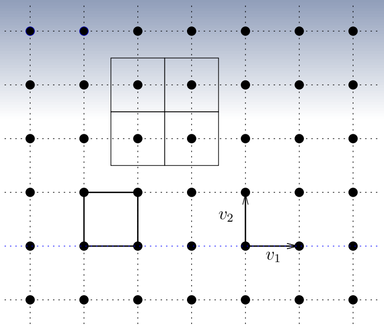
$\mathbb{Z}^2$ lattice



$\mathbb{Z}^2$ lattice

●	Lattice Point
(v_1, v_2)	Lattice Basis
◇	Fundamental Parallelotope
◇	Voronoi region

$\mathbb{Z}^2$ lattice



$\mathbb{Z}^2$ lattice

Lattice Point

(v_1, v_2) Lattice Basis

Fundamental Parallelotope

Voronoi region

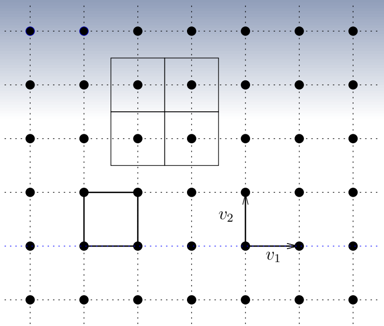
Properties

- Generator matrix is

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- A **QAM constellation** is a finite part of $\mathbb{Z}^2$.

$\mathbb{Z}^2$ lattice



$\mathbb{Z}^2$ lattice

- Lattice Point
- (v_1, v_2) Lattice Basis
- Fundamental Parallelotope
- Voronoi region

Properties

- Generator matrix is

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- A **QAM constellation** is a finite part of $\mathbb{Z}^2$.

Principal Ideal Domain

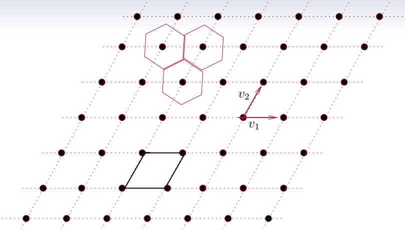
As a lattice,

$$\mathbb{Z}^2 \simeq \mathbb{Z}[\imath]$$

which is a **PID**. We will use, e.g.

$$\mathbb{Z}[\imath]\,/(1+\imath)\mathbb{Z}[\imath] \simeq \mathbb{F}_2.$$

A_2 lattice



The A_2 lattice

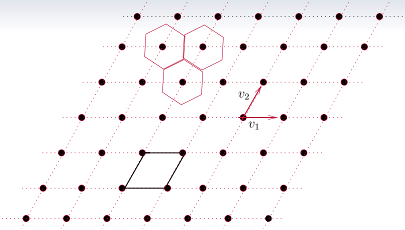
Lattice point

(v_1, v_2) Lattice basis

Fundamental parallelotope

Voronoi region

A_2 lattice



The A_2 lattice

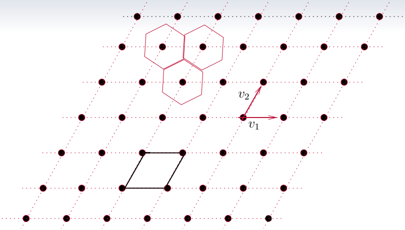
Properties

- Generator matrix is

$$M = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

- An **HEX constellation** is a finite part of A_2, the hexagonal lattice.

A_2 lattice



The A_2 lattice

Properties

- Generator matrix is

$$M = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

- An **HEX constellation** is a finite part of A_2, the hexagonal lattice.

Principal Ideal Domain

As a lattice,

$$A_2 \simeq \mathbb{Z}[\omega]$$

which is a **PID**. We will use, e.g.

$$\mathbb{Z}[\omega] \Big/ \sqrt{-3}\mathbb{Z}[\omega] \simeq \mathbb{F}_3$$

or

$$\mathbb{Z}[\omega] / 2\mathbb{Z}[\omega] \simeq \mathbb{F}_4.$$

Outline of current Part

3 **Construction A**

4 Nested lattices


CONSTRUCTION A
KEEP OUT
Sellen
Sell

Construction A

Construction A using $\mathbb{Z}$

Let q be an integer. Then, $\mathbb{Z}/q\mathbb{Z}$ is a finite field if q is a prime and a finite ring otherwise. For a linear code $\mathscr{C}$ of length n defined on $\mathbb{Z}/q\mathbb{Z}$, lattice Λ is given by

$$\Lambda = q\mathbb{Z}^n + \mathscr{C} \triangleq \bigcup_{\boldsymbol{x}\in\mathscr{C}} \left(q\mathbb{Z}^n + \boldsymbol{x}\right).$$

Construction A

Construction A using $\mathbb{Z}$

Let q be an integer. Then, $\mathbb{Z}/q\mathbb{Z}$ is a finite field if q is a prime and a finite ring otherwise. For a linear code $\mathscr{C}$ of length n defined on $\mathbb{Z}/q\mathbb{Z}$, lattice Λ is given by

$$\Lambda = q\mathbb{Z}^n + \mathscr{C} \triangleq \bigcup_{\boldsymbol{x}\in\mathscr{C}} \left(q\mathbb{Z}^n + \boldsymbol{x}\right).$$

Construction of D_4

D_4 is obtained as

$$D_4 = 2\mathbb{Z}^4 + (4,3,2)_{\mathbb{F}_2} = (1+i)\mathbb{Z}[i]^2 + (2,1,2)_{\mathbb{F}_2}$$

where $(4,3,2)_{\mathbb{F}_2}$ is the binary parity-check code.

Construction A

Construction A using $\mathbb{Z}$

Let q be an integer. Then, $\mathbb{Z}/q\mathbb{Z}$ is a finite field if q is a prime and a finite ring otherwise. For a linear code $\mathscr{C}$ of length n defined on $\mathbb{Z}/q\mathbb{Z}$, lattice Λ is given by

$$\Lambda = q\mathbb{Z}^n + \mathscr{C} \triangleq \bigcup_{\boldsymbol{x}\in\mathscr{C}} \left(q\mathbb{Z}^n + \boldsymbol{x}\right).$$

Construction of D_4

D_4 is obtained as

$$D_4 = 2\mathbb{Z}^4 + (4,3,2)_{\mathbb{F}_2} = (1+i)\mathbb{Z}[i]^2 + (2,1,2)_{\mathbb{F}_2}$$

where $(4,3,2)_{\mathbb{F}_2}$ is the binary parity-check code.

Construction of E_8

E_8 is obtained as

$$E_8 = 2\mathbb{Z}^8 + (8,4,4)_{\mathbb{F}_2} = \bigcup_{\boldsymbol{x}\in(8,4)_{\mathbb{F}_2}} \left(2\mathbb{Z}^8 + \boldsymbol{x}\right)$$

where $(8,4,4)_{\mathbb{F}_2}$ is the extended binary Hamming code $(7,4,3)_{\mathbb{F}_2}$.

Construction A (quaternary)

Construction A of the Leech lattice

The **Leech lattice** can be obtained as

$$\Lambda_{24} = 4\mathbb{Z}^{24} + (24,12)_{\mathbb{Z}_4}$$

where $(24,12)_{\mathbb{Z}_4}$ is the quaternary self-dual code obtained by extending the quaternary cyclic Golay code over $\mathbb{Z}_4$.

Construction A (quaternary)

Construction A of the Leech lattice

The **Leech lattice** can be obtained as

$$\Lambda_{24} = 4\mathbb{Z}^{24} + (24,12)_{\mathbb{Z}_4}$$

where $(24,12)_{\mathbb{Z}_4}$ is the quaternary self-dual code obtained by extending the quaternary cyclic Golay code over $\mathbb{Z}_4$.

Other constructions

Construction A can be generalized. Constructions B, C, D or E for instance. But one can show that all these constructions are equivalent to construction A with a suitable alphabet.

Outline of current Part

Sublattice

Definition

Let Λ be a lattice, then a sublattice of Λ is a lattice $\Lambda_s \subset \Lambda$. The number of copies of Λ_s in Λ is the **index**.

Sublattice

Definition

Let Λ be a lattice, then a sublattice of Λ is a lattice $\Lambda_s \subset \Lambda$. The number of copies of Λ_s in Λ is the **index**.

Toy example

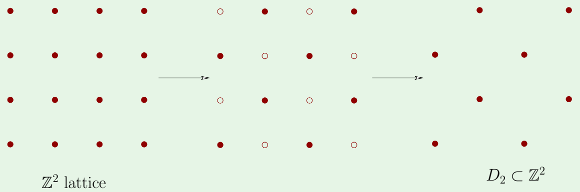


Figure: D_2 as a sublattice of $\mathbb{Z}^2$. Index is 2.

Construction A

$$D_2 = 2\mathbb{Z}^2 + (2,1,2)_{\mathbb{F}_2}.$$

An example in dimension 8

Chain of nested lattices

$$\mathbb{Z}^8 \supset D_8 \supset D_4^2 \supset L_8 \supset E_8 \supset L_8^\star \supset D_4^{2\star} \supset D_8^\star \supset 2\mathbb{Z}^8.$$

Binary codes from construction A are respectively

$$(8,8,1) \supset (8,7,2) \supset (4,3,2)^2 \supset (8,5,2) \supset (8,4,4) \supset (8,3,4) \supset (4,1,4)^2 \supset (8,1,8) \supset (8,0,\infty)$$

We have constructed a chain of **nested lattices**. All relative indices are 2.

Notation: construction A

We have, here,

$$\Lambda = 2\mathbb{Z}^8 + (8, k, d_{\min})$$

Construction D: Barnes-Wall Lattices

- A family of lattices of dimension 2^{m+1}, $m \geq 2$ can be constructed by construction D.

Barnes-Wall Lattices

Constructed as $\mathbb{Z}[i]-$ lattices,

$$\mathsf{BW}_m = (1+i)^m \mathbb{Z}[i]^{2^m} + \sum_{r=0}^{m-1} (1+i)^r \mathsf{RM}(m,r)$$

where $\mathsf{RM}(m,r)$ is the binary Reed-Müller code of length $n = 2^m$, dimension $k = \sum_{l=0}^{r} \binom{m}{l}$ and minimum Hamming distance $d = 2^{m-r}$. BW_m is a $\mathbb{Z}-$lattice of dimension 2^{m+1}.

Construction D: Barnes-Wall Lattices

- A family of lattices of dimension 2^{m+1}, $m \geq 2$ can be constructed by construction D.

Barnes-Wall Lattices

Constructed as $\mathbb{Z}[i]-$ lattices,

$$\mathsf{BW}_m = (1+i)^m \mathbb{Z}[i]^{2^m} + \sum_{r=0}^{m-1} (1+i)^r \mathsf{RM}(m,r)$$

where $\mathsf{RM}(m,r)$ is the binary Reed-Müller code of length $n = 2^m$, dimension $k = \sum_{l=0}^{r} \binom{m}{l}$ and minimum Hamming distance $d = 2^{m-r}$. BW_m is a $\mathbb{Z}-$lattice of dimension 2^{m+1}.

Another construction of E_8

We have

$$E_8 = (1+i)^2 \mathbb{Z}[i]^4 + (1+i)(4,3,2)_{\mathbb{F}_2} + (4,1,4)_{\mathbb{F}_2}$$

as E_8 is also a Barnes-Wall lattice.

Part III

Lattice Codes for the Gaussian channel

Outline of current Part

5 **Coding and Shaping**

6 Capacity achieving lattice codes $n \to +\infty$

What are Lattice Codes? An example

Toy example: the $4-$QAM

A code with 4 codewords

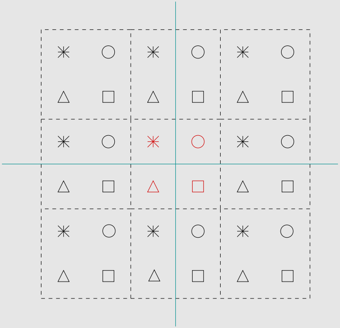


Figure: The 4 codewords are in red. Structure is $\mathbb{Z}^2/2\mathbb{Z}^2$.

What are Lattice Codes? Voronoi Constellations

Take a lattice Λ_c (**coding**) and a sublattice $\Lambda_s \subset \Lambda_c$ (**shaping**) of finite index M. Each point $\boldsymbol{x} \in \Lambda_c + \boldsymbol{c}$ can be written as

$$\boldsymbol{x} = \boldsymbol{x}_s + \boldsymbol{x}_q + \boldsymbol{c}$$

where $\boldsymbol{x}_s \in \Lambda_s$ and $\boldsymbol{x}_q$ is a a representative of $\boldsymbol{x}$ in Λ_c/Λ_s of smallest length . $\boldsymbol{c}$ is a constant vector which ensures that the overall lattice code has zero mean.

What are Lattice Codes? Voronoi Constellations

Take a lattice Λ_c (**coding**) and a sublattice $\Lambda_s \subset \Lambda_c$ (**shaping**) of finite index M. Each point $\boldsymbol{x} \in \Lambda_c + \boldsymbol{c}$ can be written as

$$\boldsymbol{x} = \boldsymbol{x}_s + \boldsymbol{x}_q + \boldsymbol{c}$$

where $\boldsymbol{x}_s \in \Lambda_s$ and $\boldsymbol{x}_q$ is a a representative of $\boldsymbol{x}$ in Λ_c/Λ_s of smallest length . $\boldsymbol{c}$ is a constant vector which ensures that the overall lattice code has zero mean.

Lattice Codes

Lattice codewords are the representatives of Λ_c/Λ_s, with **smallest length**, shifted so that the overall constellation has **zero mean**.

What are Lattice Codes? Voronoi Constellations

Take a lattice Λ_c (**coding**) and a sublattice $\Lambda_s \subset \Lambda_c$ (**shaping**) of finite index M. Each point $\boldsymbol{x} \in \Lambda_c + \boldsymbol{c}$ can be written as

$$\boldsymbol{x} = \boldsymbol{x}_s + \boldsymbol{x}_q + \boldsymbol{c}$$

where $\boldsymbol{x}_s \in \Lambda_s$ and $\boldsymbol{x}_q$ is a a representative of $\boldsymbol{x}$ in Λ_c/Λ_s of smallest length . $\boldsymbol{c}$ is a constant vector which ensures that the overall lattice code has zero mean.

Lattice Codes

Lattice codewords are the representatives of Λ_c/Λ_s, with **smallest length**, shifted so that the overall constellation has **zero mean**.

Benchmark

Lattice codes will be compared to the uncoded 2^m- QAM constellation which is $\mathbb{Z}^n/2^{\frac{m}{2}}\mathbb{Z}^n$ (m even). Vector $\boldsymbol{c}$ is the all-1/2 vector.

Coding: Minimum of Λ_c

The Coding Lattice Λ_c

We want to characterize the performance of Λ_c. Suppose that Λ_s is a scaled version of $\mathbb{Z}^n$ (separation). On the Gaussian channel, error probability is dominated by the maximal pairwise error probability

$$\max_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}} P(\boldsymbol{x}\to\boldsymbol{t}) = \max_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}} Q\left(\frac{\|\boldsymbol{x}-\boldsymbol{t}\|}{2\sqrt{N_0}}\right) = Q\left(\frac{\min_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}}\|\boldsymbol{x}-\boldsymbol{t}\|}{2\sqrt{N_0}}\right)$$

where $Q(x)$ is the error function

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}}\,du$$

and N is the noise variance.

Coding: Minimum of Λ_c

The Coding Lattice Λ_c

We want to characterize the performance of Λ_c. Suppose that Λ_s is a scaled version of $\mathbb{Z}^n$ (separation). On the Gaussian channel, error probability is dominated by the maximal pairwise error probability

$$\max_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}} P(\boldsymbol{x}\to\boldsymbol{t}) = \max_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}} Q\left(\frac{\|\boldsymbol{x}-\boldsymbol{t}\|}{2\sqrt{N_0}}\right) = Q\left(\frac{\min_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}}\|\boldsymbol{x}-\boldsymbol{t}\|}{2\sqrt{N_0}}\right)$$

where $Q(x)$ is the error function

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}}\, du$$

and N is the noise variance.

Minimum distance

We define the minimum of the lattice Λ as

$$d_{\min}(\Lambda) = \min_{\boldsymbol{x}\in\Lambda\setminus\{0\}} \|\boldsymbol{x}\|$$

Coding Gain

- Compare lattice codes (cubic shaping) with uncoded QAM with same spectral efficiency (same number of points)$\Rightarrow \alpha\mathbb{Z}^n$ with a carefully chosen α.

Coding Gain

- Compare lattice codes (cubic shaping) with uncoded QAM with same spectral efficiency (same number of points)$\Rightarrow \alpha\mathbb{Z}^n$ with a carefully chosen α.

- Dominant term of the error probability is

$$Q\left(\frac{\min_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}} \|\boldsymbol{x}-\boldsymbol{t}\|}{2\sqrt{N_0}}\right) = Q\left(\sqrt{m\frac{d^2_{\min}}{E_s}\cdot\frac{E_b}{N_0}}\right)$$

m being the **spectral efficiency,** E_b the energy per bit and $E_s = mE_b$, the energy per symbol.
Compare $\frac{d^2_{\min}}{E_s}$ of the lattice code with the one of $\mathbb{Z}^n/2^{\frac{m}{2}}\mathbb{Z}^n$.

Coding Gain

- Compare lattice codes (cubic shaping) with uncoded QAM with same spectral efficiency (same number of points)$\Rightarrow \alpha\mathbb{Z}^n$ with a carefully chosen α.

- Dominant term of the error probability is

$$Q\left(\frac{\min_{\boldsymbol{x},\boldsymbol{t}\in\mathscr{C}}\|\boldsymbol{x}-\boldsymbol{t}\|}{2\sqrt{N_0}}\right)=Q\left(\sqrt{m\frac{d^2_{\min}}{E_s}\cdot\frac{E_b}{N_0}}\right)$$

m being the **spectral efficiency,** E_b the energy per bit and $E_s = mE_b$, the energy per symbol.

Compare $\frac{d^2_{\min}}{E_s}$ of the lattice code with the one of $\mathbb{Z}^n/2^{\frac{m}{2}}\mathbb{Z}^n$.

Fundamental Volume and Coding gain

The obtained gain (called the "**Coding Gain**") is

$$\gamma_c(\Lambda)=\frac{d^2_{\min}}{\mathrm{Vol}(\Lambda)^{\frac{2}{n}}}.$$

Obvious relation with the **Hermite constant**.

Coding Gain: Examples

Dimension 4

The checkerboard lattice D_4 has generator matrix

$$\boldsymbol{M}_{D_4} = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

with $\det\left(\boldsymbol{M}_{D_4}\right) = 2$ and $d^2_{\min} = 2$.

$$D_4 = 2\mathbb{Z}^4 + (4,3,2).$$

Coding gain is

$$\gamma_c(D_4) = \frac{d^2_{\min}}{\operatorname{vol}(D_4)^{\frac{1}{2}}} = \frac{2}{\sqrt{2}} = \sqrt{2}.$$

Coding Gain: Examples

Dimension 8

The Gosset lattice E_8 has generator matrix

$$\boldsymbol{M}_{E_8} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{bmatrix}$$

with $\det\left(\boldsymbol{M}_{E_8}\right) = 1$ and $d^2_{\min} = 2$. $E_8 = 2\mathbb{Z}^8 + (8,4,4)$.
Coding gain is

$$\gamma_c(E_8) = \frac{d^2_{\min}}{\operatorname{vol}(E_8)^{\frac{1}{4}}} = 2.$$

Normalized Second Order Moment

Energy

Performance of Λ_s is related to the **energy minimization** of the lattice code. All points of the lattice code are in the **Voronoï region** of Λ_s. Energy per dimension

$$E = \frac{1}{n}\mathbb{E}\left(\|\boldsymbol{x}\|^2\right) = \frac{1}{n}\int_{\mathcal{V}_{\Lambda_s}(\mathbf{0})} \frac{1}{\mathrm{Vol}\left(\Lambda_s\right)} \|\boldsymbol{x}\|^2 \, d\boldsymbol{x}$$

Normalized Second Order Moment

Energy

Performance of Λ_s is related to the **energy minimization** of the lattice code. All points of the lattice code are in the **Voronoï region** of Λ_s. Energy per dimension

$$E = \frac{1}{n}\mathbb{E}\left(\|\boldsymbol{x}\|^2\right) = \frac{1}{n}\int_{\mathcal{V}_{\Lambda_s}(\mathbf{0})} \frac{1}{\mathrm{Vol}\left(\Lambda_s\right)} \|\boldsymbol{x}\|^2 \, d\boldsymbol{x}$$

Normalized Second Order Moment

The parameter

$$G\left(\Lambda_s\right) = \left(\frac{1}{n}\frac{\int_{\mathcal{V}_{\Lambda_s}(\mathbf{0})} \|\boldsymbol{x}\|^2 \, d\boldsymbol{x}}{\mathrm{Vol}\left(\Lambda_s\right)}\right) \mathrm{Vol}\left(\Lambda_s\right)^{-\frac{2}{n}}$$

is called the normalized second order moment of the lattice. It has to be minimized.

Normalized Second Order Moment

Energy

Performance of Λ_s is related to the **energy minimization** of the lattice code. All points of the lattice code are in the **Voronoï region** of Λ_s. Energy per dimension

$$E = \frac{1}{n}\mathbb{E}\left(\|\boldsymbol{x}\|^2\right) = \frac{1}{n}\int_{\mathcal{V}_{\Lambda_s}(\mathbf{0})} \frac{1}{\mathrm{Vol}\left(\Lambda_s\right)} \|\boldsymbol{x}\|^2 \, d\boldsymbol{x}$$

Normalized Second Order Moment

The parameter

$$G\left(\Lambda_s\right) = \left(\frac{1}{n}\frac{\int_{\mathcal{V}_{\Lambda_s}(\mathbf{0})} \|\boldsymbol{x}\|^2 \, d\boldsymbol{x}}{\mathrm{Vol}\left(\Lambda_s\right)}\right) \mathrm{Vol}\left(\Lambda_s\right)^{-\frac{2}{n}}$$

is called the normalized second order moment of the lattice. It has to be minimized.

Shaping Gain

The ratio

$$\gamma_s\left(\Lambda_s\right) = \frac{G\left(\mathbb{Z}^n\right)}{G\left(\Lambda_s\right)} = \frac{1}{12} G\left(\Lambda_s\right)^{-1}$$

is called the **shaping gain** of Λ. Its value is upperbounded by the shaping gain of the $n-$dimensional sphere which tends to $\frac{\pi e}{6}$ ($\simeq 1.5\,\mathrm{dB}$) when $n \to \infty$.

Coding Gain and Shaping Gain

Dominant term of the Error Probability

The error probability of a lattice code using Λ_c as the coding lattice and Λ_s as the shaping lattice is dominated by the term

$$\boxed{Q\left(\sqrt{\frac{3mE_b}{N_0}\cdot\gamma_c\left(\Lambda_c\right)\cdot\gamma_s\left(\Lambda_s\right)}\right)}$$

Coding Gain and Shaping Gain

Dominant term of the Error Probability

The error probability of a lattice code using Λ_c as the coding lattice and Λ_s as the shaping lattice is dominated by the term

$$\boxed{Q\left(\sqrt{\frac{3mE_b}{N_0}\cdot\gamma_c\left(\Lambda_c\right)\cdot\gamma_s\left(\Lambda_s\right)}\right)}$$

Validity

This analysis remains valid whenever the dimension is **small to medium**. For a high dimension analysis, we only have, up to now a probabilistic analysis.

Lattice Codes : an example

Voronoi Constellations

Let's give an example of a Lattice Code (or Voronoi Constellation).

- Connection with error-correcting codes.
- It gives an embedding between the **signal space** and **binary packets**.

Lattice Codes : an example

Voronoi Constellations

Let's give an example of a Lattice Code (or Voronoi Constellation).

- Connection with error-correcting codes.
- It gives an embedding between the **signal space** and **binary packets**.

Example

Choose $\Lambda_c = E_8$ and $\Lambda_s = 2E_8$. From

$$E_8 = 2\mathbb{Z}^8 + (8,4,4)_{\mathbb{F}_2},$$

we obtain

$$E_8/2E_8 = 2(8,4)^{\nabla}_{\mathbb{F}_2} + (8,4,4)_{\mathbb{F}_2}$$

where $(8,4)^{\nabla}_{\mathbb{F}_2}$ is the quotient group of coset representatives of the extended Hamming code. In this case, take the coset representatives with **smallest Hamming weight**.

Outline of current Part

5 Coding and Shaping

6 **Capacity achieving lattice codes $n \to +\infty$**

A quick digest of Erez and Zamir work

Coding/Decoding strategy

Ingredients are:

- Use **nested lattices** $\Lambda_s \subset \Lambda_c$ of high dimension
- Use **MMSE** coefficient at the receiver
- Use **dithering** and modulo Λ decoding of the scaled received vector

A quick digest of Erez and Zamir work

Coding/Decoding strategy

Ingredients are:

- Use **nested lattices** $\Lambda_s \subset \Lambda_c$ of high dimension
- Use **MMSE** coefficient at the receiver
- Use **dithering** and modulo Λ decoding of the scaled received vector

What is achievable

Rate per real dimension for a given P_e is

$$\begin{aligned} R &= \frac{1}{n}\log_2\left(\frac{\mathrm{Vol}(\Lambda_s)}{\mathrm{Vol}(\Lambda_c)}\right) = \frac{1}{2}\log_2\left(\frac{P/G(\Lambda_s)}{\mu(\Lambda_c,P_e)\,\frac{P\cdot N}{P+N}}\right) \\ &= C - \frac{1}{2}\log_2\left(G(\Lambda_s)\,\mu(\Lambda_c,P_e)\right) \end{aligned}$$

where $\mu(\Lambda_c,P_e) = \mathrm{Vol}(\Lambda_c)/N_e$ and N_e is the noise variance guaranteeing a probability P_e that the received point does not go outside the Voronoi cell of the transmitted lattice point.

A quick digest of Erez and Zamir work

Coding/Decoding strategy

Ingredients are:

- Use **nested lattices** $\Lambda_s \subset \Lambda_c$ of high dimension
- Use **MMSE** coefficient at the receiver
- Use **dithering** and modulo Λ decoding of the scaled received vector

What is achievable

Rate per real dimension for a given P_e is

$$\begin{aligned} R &= \frac{1}{n}\log_2\left(\frac{\mathrm{Vol}\left(\Lambda_s\right)}{\mathrm{Vol}\left(\Lambda_c\right)}\right) = \frac{1}{2}\log_2\left(\frac{P/G\left(\Lambda_s\right)}{\mu\left(\Lambda_c,P_e\right)\frac{P\cdot N}{P+N}}\right) \\ &= C - \frac{1}{2}\log_2\left(G\left(\Lambda_s\right)\mu\left(\Lambda_c,P_e\right)\right) \end{aligned}$$

where $\mu\left(\Lambda_c,P_e\right) = \mathrm{Vol}\left(\Lambda_c\right)/N_e$ and N_e is the noise variance guaranteeing a probability P_e that the received point does not go outside the Voronoi cell of the transmitted lattice point.

Good lattices

We can find nested lattices such that, when $n \to \infty$,

$$\begin{cases} G\left(\Lambda_s\right) & \to \frac{1}{2\pi e} \\ \mu\left(\Lambda_c,P_e\right) & \to 2\pi e \end{cases}$$

for any value of $P_e > 0$ by using construction A over big alphabets $\mathbb{Z}/p\mathbb{Z}$, p prime.

Part IV

Lattices for Fading Channels

Outline of current Part

Paths recombination

- Each path is characterized by its magnitude α_i, its phase θ_i and its delay, τ_i.

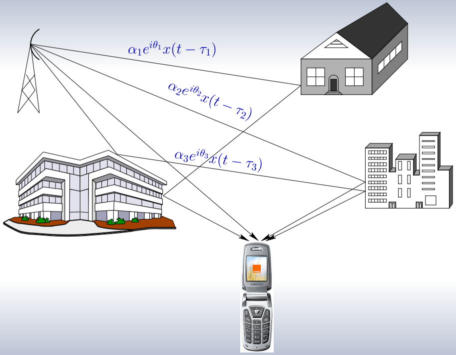


Figure: Destructive recombination due to phases $\longrightarrow$ **fadings** (here, $x(t)$ is the transmitted signal)

Phases dependencies

- Fadings vary as a function of
  - frequency.
  - antennas position (since τ_i are different from one antenna to the other one).
  - time (obstacles and terminals may move.

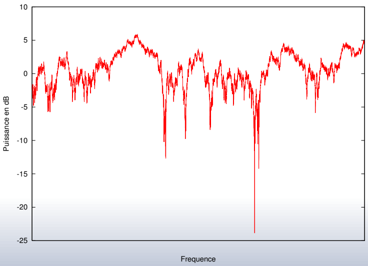


Figure: Received power as a function of the frequency

OFDM frequency diversity

OFDM

Radio channel is frequency selective. Interleaver is used to decorrelate channel coefficients.

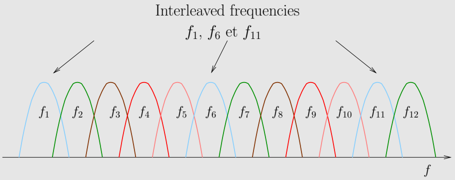


Figure: Interleaved frequencies: Here fadings on frequencies f_1, f_6 and f_{11} are assumed independent.

Outline of current Part

Channel model

Received signal

Received signal is the vector

Transmitted vector

$$\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{Z}$$

Received vector

Noise vector (i.i.d.)

Diagonal channel matrix

with $\mathbf{H} = \mathrm{diag}(h_1, h_2, \ldots, h_n)$.

Channel model

Received signal

Received signal is the vector

Transmitted vector

$$\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{Z}$$

Received vector

Noise vector (i.i.d.)

Diagonal channel matrix

with $\mathbf{H} = \mathrm{diag}\,(h_1, h_2, \ldots, h_n)$.

Assumptions

1. Channel coefficients h_i are assumed decorrelated
2. Each h_i is the channel complex attenuation on a subcarrier

Channel model

Received signal

Received signal is the vector

Transmitted vector

$$\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{Z}$$

Received vector

Noise vector (i.i.d.)

Diagonal channel matrix

with $\mathbf{H} = \operatorname{diag}(h_1, h_2, \ldots, h_n)$.

Assumptions

1. Channel coefficients h_i are assumed decorrelated
2. Each h_i is the channel complex attenuation on a subcarrier

Detection

All h_i are assumed perfectly known at the receiver.

Product distance

- Consider a pair of points $(\mathbf{X},\mathbf{T})$ of the constellation. Pairwise Error Probability for fast fading channels is

$$p(\mathbf{X}\to\mathbf{T}) \le \frac{1}{2}\prod_{x_i\neq t_i}\frac{4N_0}{\left|x_i-t_i\right|^2} = \frac{1}{2}\frac{\left(4N_0\right)^l}{d_p^{(l)}(\mathbf{X},\mathbf{T})^2}$$

where $d_p^{(l)}(\mathbf{X},\mathbf{T})$ is the $l-$product distance produit evaluated when points $\mathbf{X}$ and $\mathbf{T}$ differ in l symbols (or components).

Product distance

- Consider a pair of points $(\mathbf{X}, \mathbf{T})$ of the constellation. Pairwise Error Probability for fast fading channels is

$$p(\mathbf{X} \to \mathbf{T}) \leq \frac{1}{2} \prod_{x_i \neq t_i} \frac{4N_0}{|x_i - t_i|^2} = \frac{1}{2} \frac{(4N_0)^l}{d_p^{(l)}(\mathbf{X}, \mathbf{T})^2}$$

  where $d_p^{(l)}(\mathbf{X}, \mathbf{T})$ is the $l-$product distance produit evaluated when points $\mathbf{X}$ and $\mathbf{T}$ differ in l symbols (or components).

Product distance

The $l-$product distance is

$$\boxed{d_p^{(l)}(\mathbf{X}, \mathbf{T}) = \prod_{x_i \neq t_i} |x_i - t_i|}$$

Product distance

- Consider a pair of points $(\mathbf{X},\mathbf{T})$ of the constellation. Pairwise Error Probability for fast fading channels is

$$p(\mathbf{X} \to \mathbf{T}) \leq \frac{1}{2} \prod_{x_i \neq t_i} \frac{4N_0}{|x_i - t_i|^2} = \frac{1}{2} \frac{(4N_0)^l}{d_p^{(l)}(\mathbf{X},\mathbf{T})^2}$$

where $d_p^{(l)}(\mathbf{X},\mathbf{T})$ is the $l-$product distance produit evaluated when points $\mathbf{X}$ and $\mathbf{T}$ differ in l symbols (or components).

Product distance

The $l-$product distance is

$$\boxed{d_p^{(l)}(\mathbf{X},\mathbf{T}) = \prod_{x_i \neq t_i} |x_i - t_i|}$$

Dominant term

In the global error probability expression, dominant term is $d_{p,\min} = \min d_p^{(L)}$ where $L = \min(l)$ is the diversity order of the constellation (also named “modulation diversity”).

Construction by optimisation

Aim and methodology

Construct the optimal constellation (in the sense of the product distance), in a 2-dimensional space, with a diversity order equal to 2.

Construction by optimisation

Aim and methodology

Construct the optimal constellation (in the sense of the product distance), in a 2-dimensional space, with a diversity order equal to 2.

1. Choose a constellation such that the product distance $d_p^{(2)}(\mathbf{X},\mathbf{T}) \geq 1$ for all $\mathbf{X} \neq \mathbf{T}$ in the constellation.
2. Start with point 0, then construct a point $\mathbf{X}_1$ respecting constraint $d_p^{(2)}(\mathbf{X}_1, 0) \geq 1$ such that the average energy of the constellation is minimized. Then construct $\mathbf{X}_2$ such that $d_p^{(2)}(\mathbf{X}_2, 0) \geq 1$ and $d_p^{(2)}(\mathbf{X}_1, \mathbf{X}_2) \geq 1$ and such that the average energy of the constellation is minimized, ...
3. We get

Optimized constellation

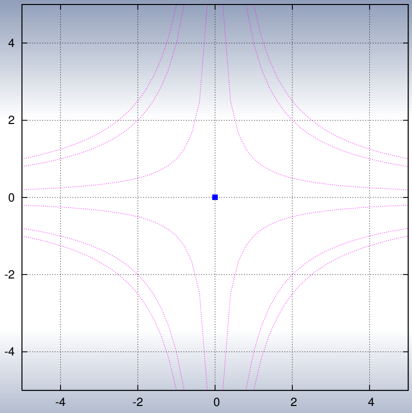


Figure: Construction of the constellation by iterating (iteration 0)

Optimized constellation

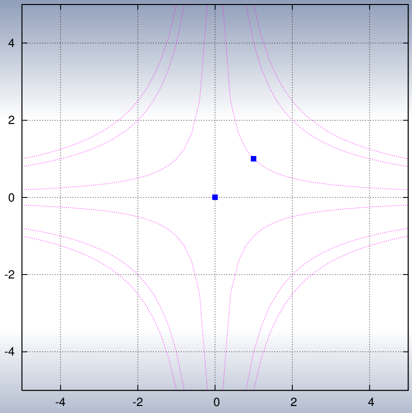


Figure: Construction of the constellation by iterating (iteration 1)

Optimized constellation

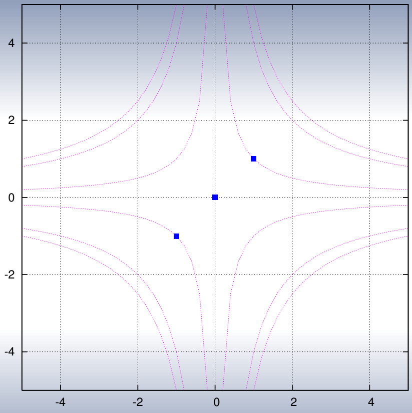


Figure: Construction of the constellation by iterating (iteration 2)

Optimized constellation

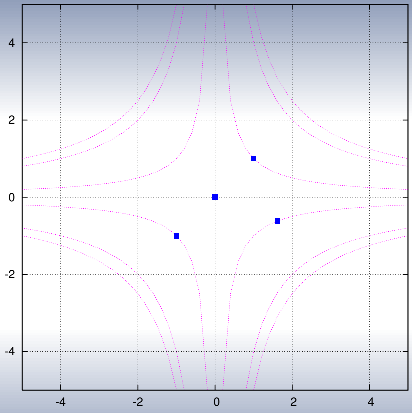


Figure: Construction of the constellation by iterating (iteration 3)

Optimized constellation

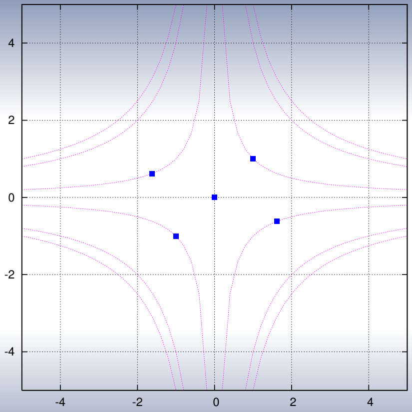


Figure: Construction of the constellation by iterating (iteration 4)

Optimized constellation

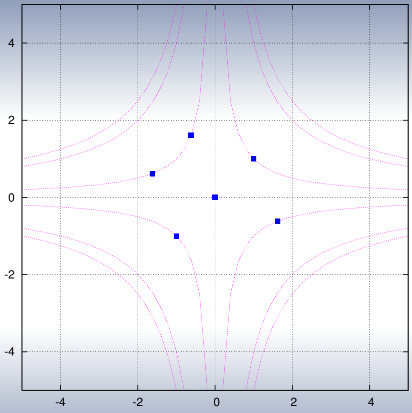


Figure: Construction of the constellation by iterating (iteration 5)

Optimized constellation

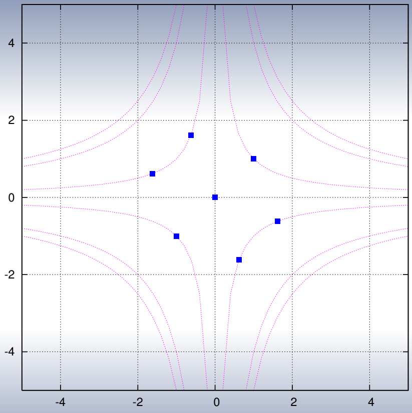


Figure: Construction of the constellation by iterating (iteration 6)

Optimized constellation

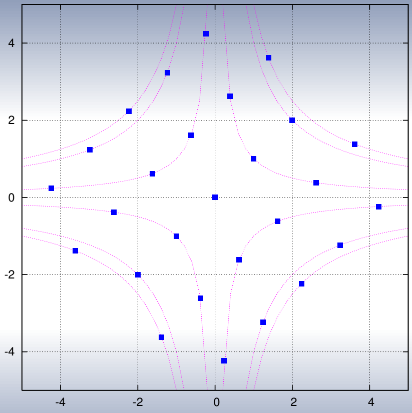


Figure: Construction of the constellation by iterating (iteration 36)

Lattice from an algebraic number field

- By iterating the optimization process, we obtain all points

$$\begin{pmatrix} a+b\frac{1+\sqrt{5}}{2} \\ a+b\frac{1-\sqrt{5}}{2} \end{pmatrix}$$

with a and b in $\mathbb{Z}$.

Generator matrix

The points of the infinite constellation may be written as

$$\begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$$

with $a, b \in \mathbb{Z}$. This infinite constellation is a lattice and

$$M = \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix} \tag{1}$$

is its generator matrix.

- Number $\varphi = \frac{1+\sqrt{5}}{2}$ is the **Golden Ratio** and $\bar{\varphi} = \frac{1-\sqrt{5}}{2}$ is its conjugate.

Outline of current Part

Extension and algebraic integers

Definitions

Golden ratio φ is in the number field $\mathbb{Q}\left(\sqrt{5}\right)$.

- $\mathbb{Q}\left(\sqrt{5}\right)$ is the set of all numbers $p+q\sqrt{5}$ with $p,q\in\mathbb{Q}$.
- Minimal polynomial of φ is X^2-X-1

Algebraic integer

An algebraic integer is an algebraic number whose minimal polynomial has its coefficients in $\mathbb{Z}$.

Examples

1. $\varphi=\frac{1+\sqrt{5}}{2}$ is an algebraic **integer**: $\mu_{\varphi}(X)=X^2-X-1$
2. $\sqrt{5}$ is an algebraic **integer**: $\mu_{\sqrt{5}}(X)=X^2-5$
3. $\beta=\frac{1+\sqrt{2}}{2}$ is not an algebraic **integer**: $\mu_{\beta}(X)=X^2-X-\frac{1}{4}$

Ring of integers and integer basis

Definitions

Integers of $\mathbb{Q}\left(\sqrt{5}\right)$ are $a + b\varphi$ with $a, b \in \mathbb{Z}$.

- $\left(1, \varphi\right)$ is an integer basis of $\mathbb{Q}\left(\sqrt{5}\right)$
- The norm is the product of an algebraic number with its conjugate. Conjugate of φ is $\bar{\varphi}$. Conjugate of 1 is 1.

Discriminant

We define matrix

$$\mathbf{\Omega} = \begin{bmatrix} 1 & \varphi \\ 1 & \bar{\varphi} \end{bmatrix}$$

which is the generator matrix of lattice (1). Discriminant of $\mathbb{Q}\left(\sqrt{5}\right)$ is

$$d_{\mathbb{Q}\left(\sqrt{5}\right)} = \left(\det \mathbf{\Omega}\right)^2 = 5$$

- Discriminant is related to the **energy** of a constellation carved from the infinite lattice. 5 is the **smallest discriminant** that a real number field can have. That is why the best constellation for the fast fading channel is related to the **Golden Ratio**.

Outline of current Part

7 Wireless Communications

8 Fast fading channel

9 Number Fields

10 Lattices from Number Fields

11 Rotations

Number fields

Base field

We consider 3 base fields $\mathbb{F}$ in what follows,

1. $\mathbb{F} = \mathbb{Q}$. $\mathscr{O}_{\mathbb{F}} = \mathbb{Z}$.
2. $\mathbb{F} = \mathbb{Q}(i)$ with $\mathbb{Q}(i) = \left\{x + iy,\ x, y \in \mathbb{Q}\right\}$; $\mathscr{O}_{\mathbb{F}} = \mathbb{Z}[i]$.
3. $\mathbb{F} = \mathbb{Q}(\omega)$ with $\mathbb{Q}(\omega) = \left\{x + \omega y,\ x, y \in \mathbb{Q}\right\}$; $\mathscr{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$. ω is a primitive third root of unity.

Number fields

Base field

We consider 3 base fields $\mathbb{F}$ in what follows,

1. $\mathbb{F} = \mathbb{Q}$. $\mathscr{O}_{\mathbb{F}} = \mathbb{Z}$.
2. $\mathbb{F} = \mathbb{Q}(i)$ with $\mathbb{Q}(i) = \left\{x + iy,\ x, y \in \mathbb{Q}\right\}$; $\mathscr{O}_{\mathbb{F}} = \mathbb{Z}[i]$.
3. $\mathbb{F} = \mathbb{Q}(\omega)$ with $\mathbb{Q}(\omega) = \left\{x + \omega y,\ x, y \in \mathbb{Q}\right\}$; $\mathscr{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$. ω is a primitive third root of unity.

- We define

$$\mathbb{K} = \mathbb{F}(\theta) = \left\{\sum_{i=0}^{n-1} a_i \theta^i,\ a_i \in \mathbb{F}\right\}$$

where θ is some algebraic number of degree n on $\mathbb{F}$, that is, admitting a minimal polynomial of degree n with coefficients in $\mathbb{F}$.

Number fields

Base field

We consider 3 base fields $\mathbb{F}$ in what follows,

1. $\mathbb{F} = \mathbb{Q}$. $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
2. $\mathbb{F} = \mathbb{Q}(i)$ with $\mathbb{Q}(i) = \left\{x + iy,\ x, y \in \mathbb{Q}\right\}$; $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$.
3. $\mathbb{F} = \mathbb{Q}(\omega)$ with $\mathbb{Q}(\omega) = \left\{x + \omega y,\ x, y \in \mathbb{Q}\right\}$; $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$. ω is a primitive third root of unity.

- We define

$$\mathbb{K} = \mathbb{F}(\theta) = \left\{\sum_{i=0}^{n-1} a_i\theta^i,\ a_i \in \mathbb{F}\right\}$$

where θ is some algebraic number of degree n on $\mathbb{F}$, that is, admitting a minimal polynomial of degree n with coefficients in $\mathbb{F}$.

Example: $\mathbb{Q}\left(\sqrt{5}\right)$

Minimal polynomial of $\sqrt{5}$ is $X^2 - 5$. So,

$$\mathbb{Q}(\sqrt{5}) = \left\{a_0 + a_1\sqrt{5},\ a_0, a_1 \in \mathbb{Q}\right\}.$$

Algebraic Integers

- In a number field $\mathbb{K}$ on $\mathbb{F}$ of degree n, integers are of particular interest. The ring of integers is the ring of numbers in $\mathbb{K}$ whose minimal polynomial is $X^n + \sum_{i=0}^{n-1} a_i X^i$ with $a_i \in \mathscr{O}_{\mathbb{F}}$. We denote this ring $\mathscr{O}_{\mathbb{K}}$.

Algebraic Integers

- In a number field $\mathbb{K}$ on $\mathbb{F}$ of degree n, integers are of particular interest. The ring of integers is the ring of numbers in $\mathbb{K}$ whose minimal polynomial is $X^n + \sum_{i=0}^{n-1} a_i X^i$ with $a_i \in \mathcal{O}_{\mathbb{F}}$. We denote this ring $\mathcal{O}_{\mathbb{K}}$.

Basis

$(\omega_0, \omega_1, \ldots, \omega_{n-1})$ is a basis of $\mathcal{O}_{\mathbb{K}}$ **iff** any element ϕ of $\mathcal{O}_{\mathbb{K}}$ can be written as

$$\phi = \sum_{k=0}^{n-1} a_i \omega_i,\ a_i \in \mathcal{O}_{\mathbb{F}}.$$

Algebraic Integers

- In a number field $\mathbb{K}$ on $\mathbb{F}$ of degree n, integers are of particular interest. The ring of integers is the ring of numbers in $\mathbb{K}$ whose minimal polynomial is $X^n + \sum_{i=0}^{n-1} a_i X^i$ with $a_i \in \mathcal{O}_{\mathbb{F}}$. We denote this ring $\mathcal{O}_{\mathbb{K}}$.

Basis

$(\omega_0, \omega_1, \ldots, \omega_{n-1})$ is a basis of $\mathcal{O}_{\mathbb{K}}$ **iff** any element ϕ of $\mathcal{O}_{\mathbb{K}}$ can be written as

$$\phi = \sum_{k=0}^{n-1} a_i \omega_i,\ a_i \in \mathcal{O}_{\mathbb{F}}.$$

Example (cont.) $\mathbb{Q}\left(\sqrt{5}\right)$

$\sqrt{5}$ is an integer (minimal polynomial $X^2 - 5$) but $\frac{1+\sqrt{5}}{2}$ is also an integer (minimal polynomial $X^2 - X - 1$). In fact, the ring of integers of $\mathbb{Q}\left(\sqrt{5}\right)$ is

$$\mathcal{O}_{\mathbb{K}} = \left\{ a_0 + a_1 \frac{1+\sqrt{5}}{2},\ a_0, a_1 \in \mathbb{Z} \right\}$$

and $\left(1, \frac{1+\sqrt{5}}{2}\right)$ is a basis of $\mathcal{O}_{\mathbb{K}}$.

The Galois group

Definition

The group of the field morphisms ($\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$) which associates to an element of $\mathbb{K}$ its conjugates is called the Galois group of $\mathbb{K}$ and denoted $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$. If $\left|\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})\right| = n$ (the order of $\mathbb{K}$), then the extension is Galois.

The Galois group

Definition

The group of the field morphisms ($\sigma(x+y) = \sigma(x)+\sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$) which associates to an element of $\mathbb{K}$ its conjugates is called the Galois group of $\mathbb{K}$ and denoted $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$. If $\left|\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})\right| = n$ (the order of $\mathbb{K}$), then the extension is Galois.

Definition

The norm of an element of $\mathbb{K}$ is the product of all its conjugates. It is also the constant term of its minimal polynomial.

$$N_{\mathbb{K}/\mathbb{F}}(x) = \prod_{i=0}^{n-1} \sigma_i(x) \in \mathbb{F}.$$

If x is integer, then $N_{\mathbb{K}/\mathbb{F}}(x) \in \mathcal{O}_{\mathbb{F}}$ and $N_{\mathbb{K}/\mathbb{F}}(x) = 0$ **iff** $x = 0$.

The Galois group

Definition

The group of the field morphisms ($\sigma(x+y)=\sigma(x)+\sigma(y)$ and $\sigma(xy)=\sigma(x)\sigma(y)$) which associates to an element of $\mathbb{K}$ its conjugates is called the Galois group of $\mathbb{K}$ and denoted $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$. If $\left|\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})\right| = n$ (the order of $\mathbb{K}$), then the extension is Galois.

Definition

The norm of an element of $\mathbb{K}$ is the product of all its conjugates. It is also the constant term of its minimal polynomial.

$$N_{\mathbb{K}/\mathbb{F}}(x) = \prod_{i=0}^{n-1} \sigma_i(x) \in \mathbb{F}.$$

If x is integer, then $N_{\mathbb{K}/\mathbb{F}}(x) \in \mathscr{O}_{\mathbb{F}}$ and $N_{\mathbb{K}/\mathbb{F}}(x) = 0$ **iff** $x = 0$.

Product Distance

Suppose that $\mathbb{K}$ is a totally real extension on $\mathbb{Q}$. $\boldsymbol{x} = (\sigma_0(x), \sigma_1(x), \ldots, \sigma_{n-1}(x))^\top$ where $x \in \mathscr{O}_{\mathbb{K}}$. Then,

$$d_p(\boldsymbol{x}, \boldsymbol{0}) = \prod_{i=1}^{n} |x_i| = \left|N_{\mathbb{K}/\mathbb{Q}}(x)\right| \geq 1.$$

The canonical embedding (real case)

Canonical Embedding (real case)

We define the canonical embedding which maps an element of $\mathbb{K}$ onto a vector of $\mathbb{R}^n$. We have

$$\Upsilon : x \in \mathbb{K} \mapsto \boldsymbol{x} = \begin{pmatrix} \sigma_0(x) \\ \sigma_1(x) \\ \vdots \\ \sigma_{n-1}(x) \end{pmatrix} \in \mathbb{R}^n$$

The product of all components of $\boldsymbol{x}$ is the algebraic norm of x. Υ transforms $\mathcal{O}_{\mathbb{K}}$ into a lattice $\Lambda_{\mathcal{O}_{\mathbb{K}}}$.

The canonical embedding (real case)

Canonical Embedding (real case)

We define the canonical embedding which maps an element of $\mathbb{K}$ onto a vector of $\mathbb{R}^n$. We have

$$\Upsilon : x \in \mathbb{K} \mapsto \boldsymbol{x} = \begin{pmatrix} \sigma_0(x) \\ \sigma_1(x) \\ \vdots \\ \sigma_{n-1}(x) \end{pmatrix} \in \mathbb{R}^n$$

The product of all components of $\boldsymbol{x}$ is the algebraic norm of x. Υ transforms $\mathcal{O}_{\mathbb{K}}$ into a lattice $\Lambda_{\mathcal{O}_{\mathbb{K}}}$.

The case $\mathbb{K} = \mathbb{Q}\left(\sqrt{2}\right)$

An element $x = a + b\sqrt{2}$ is mapped onto the vector

$$\vec{\mathbf{x}} = \begin{pmatrix} a + b\sqrt{2} \\ a - b\sqrt{2} \end{pmatrix}$$

The canonical embedding (totally complex case)

If $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{F} = \mathbb{Q}(\omega)$ (or any **quadratic complex** field), the same definition applies. But the considered Galois group is the group

$$\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K}) = \mathrm{Gal}_{\mathbb{K}/\mathbb{Q}}(\mathbb{K}) / < \tau >$$

where τ is the complex conjugation. Vector $\boldsymbol{x}$ lies in $\mathbb{C}^n$.

The canonical embedding (totally complex case)

If $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{F} = \mathbb{Q}(\omega)$ (or any **quadratic complex** field), the same definition applies. But the considered Galois group is the group

$$\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K}) = \mathrm{Gal}_{\mathbb{K}/\mathbb{Q}}(\mathbb{K}) / < \tau >$$

where τ is the complex conjugation. Vector $\boldsymbol{x}$ lies in $\mathbb{C}^n$.

Example

Let $\mathbb{F} = \mathbb{Q}(i)$ and $\mathbb{K} = \mathbb{Q}(\zeta_8)$ where ζ_8 is some 8^{th} primitive root of unity (e.g. $\zeta_8 = \exp\left(\frac{i\pi}{4}\right)$). Then the canonical embedding maps $x = a + b\zeta_8$, with $a, b \in \mathbb{Q}(i)$, onto the vector

$$\boldsymbol{x} = \begin{pmatrix} a + b\zeta_8 \\ a - b\zeta_8 \end{pmatrix}$$

since the minimal polynomial of ζ_8 is $X^2 - i$.

The canonical embedding (totally complex case)

If $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{F} = \mathbb{Q}(\omega)$ (or any **quadratic complex** field), the same definition applies. But the considered Galois group is the group

$$\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K}) = \mathrm{Gal}_{\mathbb{K}/\mathbb{Q}}(\mathbb{K}) / < \tau >$$

where τ is the complex conjugation. Vector $\boldsymbol{x}$ lies in $\mathbb{C}^n$.

Example

Let $\mathbb{F} = \mathbb{Q}(i)$ and $\mathbb{K} = \mathbb{Q}(\zeta_8)$ where ζ_8 is some 8^{th} primitive root of unity (e.g. $\zeta_8 = \exp\left(\frac{i\pi}{4}\right)$). Then the canonical embedding maps $x = a + b\zeta_8$, with $a, b \in \mathbb{Q}(i)$, onto the vector

$$\boldsymbol{x} = \begin{pmatrix} a + b\zeta_8 \\ a - b\zeta_8 \end{pmatrix}$$

since the minimal polynomial of ζ_8 is $X^2 - i$.

Product distance

For $\boldsymbol{x} \neq \boldsymbol{0}$,

$$d_p(\boldsymbol{x}, \boldsymbol{0}) = \prod_{i=1}^{n} |x_i| = \left|N_{\mathbb{K}/\mathbb{F}}(x)\right| = \sqrt{N_{\mathbb{K}/\mathbb{Q}}(x)} \geq 1.$$

Outline of current Part

7 Wireless Communications

8 Fast fading channel

9 Number Fields

10 Lattices from Number Fields

11 **Rotations**

Finite constellation: rotate it

- We are looking for finite constellations: shaping problems.
    - **Solution:** Rotated QAM constellations.

Finite constellation: rotate it

- We are looking for finite constellations: shaping problems.
  - **Solution:** Rotated QAM constellations.
- Same performance on the Gaussian channel as the non rotated QAM constellation. Rotation must be chosen to maximize the **product distance**.

Finite constellation: rotate it

- We are looking for finite constellations: shaping problems.
  - **Solution:** Rotated QAM constellations.
- Same performance on the Gaussian channel as the non rotated QAM constellation. Rotation must be chosen to maximize the **product distance**.

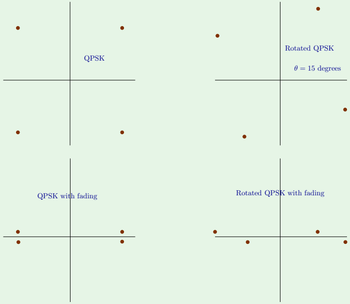


Figure: Effect of a fading on a QPSK and a rotated QPSK

Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (I)

- Construct a rotation with 2 PAM symbols. We consider the Golden field $\mathbb{Q}\left(\sqrt{5}\right)$. A PAM symbol is an integer. Let a and b in $\mathbb{Z}$. The lattice on the Golden field is defined by the application

$$\Upsilon : \boldsymbol{p} = \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \boldsymbol{x} = \begin{pmatrix} a + b\frac{1+\sqrt{5}}{2} \\ a + b\frac{1-\sqrt{5}}{2} \end{pmatrix}$$

Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (I)

- Construct a rotation with 2 PAM symbols. We consider the Golden field $\mathbb{Q}\left(\sqrt{5}\right)$. A PAM symbol is an integer. Let a and b in $\mathbb{Z}$. The lattice on the Golden field is defined by the application

$$\Upsilon : \boldsymbol{p} = \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \boldsymbol{x} = \begin{pmatrix} a + b\frac{1+\sqrt{5}}{2} \\ a + b\frac{1-\sqrt{5}}{2} \end{pmatrix}$$

So,

$$\boldsymbol{x} = \boldsymbol{M} \cdot \boldsymbol{p} = \begin{bmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{bmatrix} \cdot \boldsymbol{p}$$

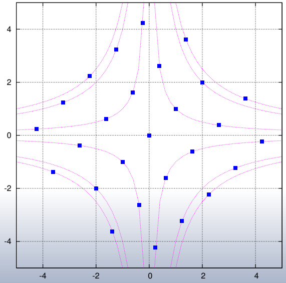
Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (I)

- Construct a rotation with 2 PAM symbols. We consider the Golden field $\mathbb{Q}\left(\sqrt{5}\right)$. A PAM symbol is an integer. Let a and b in $\mathbb{Z}$. The lattice on the Golden field is defined by the application

$$\Upsilon : \boldsymbol{p} = \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \boldsymbol{x} = \begin{pmatrix} a + b\frac{1+\sqrt{5}}{2} \\ a + b\frac{1-\sqrt{5}}{2} \end{pmatrix}$$

So,

$$\boldsymbol{x} = \boldsymbol{M} \cdot \boldsymbol{p} = \begin{bmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{bmatrix} \cdot \boldsymbol{p}$$



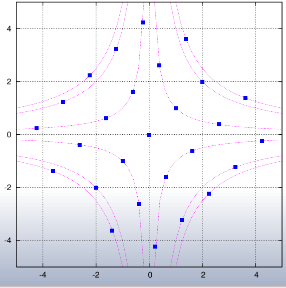
Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (I)

- Construct a rotation with 2 PAM symbols. We consider the Golden field $\mathbb{Q}\left(\sqrt{5}\right)$. A PAM symbol is an integer. Let a and b in $\mathbb{Z}$. The lattice on the Golden field is defined by the application

$$\Upsilon : \boldsymbol{p} = \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \boldsymbol{x} = \begin{pmatrix} a + b\frac{1+\sqrt{5}}{2} \\ a + b\frac{1-\sqrt{5}}{2} \end{pmatrix}$$

So,

$$\boldsymbol{x} = \boldsymbol{M} \cdot \boldsymbol{p} = \begin{bmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{bmatrix} \cdot \boldsymbol{p}$$



Problem

M is not a **rotation!** We can have problems of shaping ...

Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (II)

Gram matrix

Gram matrix of $\boldsymbol{M}$ is $\boldsymbol{G} \triangleq \boldsymbol{M}^t \cdot \boldsymbol{M}$. If $\boldsymbol{M}$ would have been a scaled rotation, we would have

$$\boldsymbol{G} = c \cdot \boldsymbol{I}$$

where c is some integer.

Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (II)

Gram matrix

Gram matrix of $\boldsymbol{M}$ is $\boldsymbol{G} \triangleq \boldsymbol{M}^t \cdot \boldsymbol{M}$. If $\boldsymbol{M}$ would have been a scaled rotation, we would have

$$\boldsymbol{G} = c \cdot \boldsymbol{I}$$

where c is some integer.

Condition on the determinant

Determinant of the Gram matrix must be

$$\det \boldsymbol{G} = c^2$$

Rotation in $\mathbb{Q}\left(\sqrt{5}\right)$ (II)

Gram matrix

Gram matrix of $\boldsymbol{M}$ is $\boldsymbol{G} \triangleq \boldsymbol{M}^t \cdot \boldsymbol{M}$. If $\boldsymbol{M}$ would have been a scaled rotation, we would have

$$\boldsymbol{G} = c \cdot \boldsymbol{I}$$

where c is some integer.

Condition on the determinant

Determinant of the Gram matrix must be

$$\det \boldsymbol{G} = c^2$$

Reality

Determinant of $\boldsymbol{M}$ is $-\sqrt{5}$, so,

$$\det \boldsymbol{G} = 5$$

which is not a square.

A rotation

1. Take $\beta = 2 + \frac{1-\sqrt{5}}{2}$. Its norm is

$$N(\beta) = \left(2 + \frac{1-\sqrt{5}}{2}\right) \cdot \left(2 + \frac{1+\sqrt{5}}{2}\right) = 5$$

A rotation

1. Take $\beta = 2 + \frac{1-\sqrt{5}}{2}$. Its norm is

$$N(\beta) = \left(2 + \frac{1-\sqrt{5}}{2}\right) \cdot \left(2 + \frac{1+\sqrt{5}}{2}\right) = 5$$

2. Consider matrix

$$\boldsymbol{A} = \begin{bmatrix} \sqrt{\beta} & 0 \\ 0 & \sqrt{\bar{\beta}} \end{bmatrix}$$

whose determinant is $\det(\boldsymbol{A}) = \sqrt{N(\beta)} = \sqrt{5}$. Equivalent to consider lattices for trace form $(x, y) = \mathrm{Tr}\left(\beta x y\right)$.

A rotation

1. Take $\beta = 2 + \frac{1-\sqrt{5}}{2}$. Its norm is

$$N(\beta) = \left(2 + \frac{1-\sqrt{5}}{2}\right) \cdot \left(2 + \frac{1+\sqrt{5}}{2}\right) = 5$$

2. Consider matrix

$$\boldsymbol{A} = \begin{bmatrix} \sqrt{\beta} & 0 \\ 0 & \sqrt{\bar{\beta}} \end{bmatrix}$$

whose determinant is $\det(\boldsymbol{A}) = \sqrt{N(\beta)} = \sqrt{5}$. Equivalent to consider lattices for trace form $(x, y) = \mathrm{Tr}\left(\beta xy\right)$.

3. Construct $\boldsymbol{P} = \boldsymbol{A} \cdot \boldsymbol{M}$ whose Gram matrix has determinant 5^2.

A rotation

1. Take $\beta = 2 + \frac{1-\sqrt{5}}{2}$. Its norm is

$$N(\beta) = \left(2 + \frac{1-\sqrt{5}}{2}\right) \cdot \left(2 + \frac{1+\sqrt{5}}{2}\right) = 5$$

2. Consider matrix

$$\boldsymbol{A} = \begin{bmatrix} \sqrt{\beta} & 0 \\ 0 & \sqrt{\bar{\beta}} \end{bmatrix}$$

whose determinant is $\det(\boldsymbol{A}) = \sqrt{N(\beta)} = \sqrt{5}$. Equivalent to consider lattices for trace form $(x, y) = \operatorname{Tr}\left(\beta x y\right)$.

3. Construct $\boldsymbol{P} = \boldsymbol{A} \cdot \boldsymbol{M}$ whose Gram matrix has determinant 5^2.
4. We can check that $\boldsymbol{P}^t \cdot \boldsymbol{P} = 5 \cdot \boldsymbol{I}$. The rotation matrix is

$$\boldsymbol{R} = \frac{1}{\sqrt{5}} \boldsymbol{P} = \frac{1}{\sqrt{5}} \begin{bmatrix} \sqrt{2+\bar{\varphi}} & \varphi\sqrt{2+\bar{\varphi}} \\ \sqrt{2+\varphi} & \bar{\varphi}\sqrt{2+\varphi} \end{bmatrix}$$

Minimum product distance of the constellation is $d_{p,\min} = \frac{1}{\sqrt{5}}$ which is the best known minimum product distance for $\mathbb{Z}^2$.

A Unitary Transform

- Same considerations apply when instead of $\mathbb{F} = \mathbb{Q}$ we consider $\mathbb{F} = \mathbb{Q}(\imath)$. Here a and b will be in $\mathbb{Z}[\imath]$.

A Unitary Transform

- Same considerations apply when instead of $\mathbb{F}=\mathbb{Q}$ we consider $\mathbb{F}=\mathbb{Q}(\imath)$. Here a and b will be in $\mathbb{Z}[\imath]$.
- The unitary matrix now is

$$\boldsymbol{U}=\frac{1}{\sqrt{5}}\begin{bmatrix}\alpha & \alpha\varphi\\ \bar{\alpha} & \bar{\alpha}\bar{\varphi}\end{bmatrix} \tag{2}$$

  where $\alpha=1+\imath-\imath\varphi$ and $\bar{\alpha}=1+\imath-\imath\bar{\varphi}$. It is the key transform in the construction of the **Golden Code** for MIMO communication.

A Unitary Transform

- Same considerations apply when instead of $\mathbb{F} = \mathbb{Q}$ we consider $\mathbb{F} = \mathbb{Q}(\imath)$. Here a and b will be in $\mathbb{Z}[\imath]$.
- The unitary matrix now is
$$\boldsymbol{U} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha & \alpha\varphi \\ \bar{\alpha} & \bar{\alpha}\bar{\varphi} \end{bmatrix} \tag{2}$$
where $\alpha = 1 + \imath - \imath\varphi$ and $\bar{\alpha} = 1 + \imath - \imath\bar{\varphi}$. It is the key transform in the construction of the **Golden Code** for MIMO communication.
- This transform gives the best product distance among all unitary transforms in dimension 2.

General case: Get a lattice with given determinant

Norm of an ideal

The norm of an ideal $\mathscr{I}$ of $\mathscr{O}_{\mathbb{K}}$ is defined as

$$N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I}) = \mathrm{Card}\left(\mathscr{O}_{\mathbb{K}}/\mathscr{I}\right).$$

Moreover, if I is principal, generated by α, then $N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I}) = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|$.

General case: Get a lattice with given determinant

Norm of an ideal

The norm of an ideal $\mathscr{I}$ of $\mathscr{O}_{\mathbb{K}}$ is defined as

$$N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I}) = \mathrm{Card}\left(\mathscr{O}_{\mathbb{K}}/\mathscr{I}\right).$$

Moreover, if I is principal, generated by α, then $N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I}) = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|$.

Determinant

Suppose that we consider the canonical embedding of an ideal $\mathscr{I}$ of absolute norm $N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I})$. Then the lattice obtained by canonical embedding has determinant,

$$\det\left(\Lambda_{\mathscr{I}}\right) = N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I})^2 \cdot d_{\mathbb{K}}$$

General case: Get a lattice with given determinant

Norm of an ideal

The norm of an ideal $\mathscr{I}$ of $\mathscr{O}_{\mathbb{K}}$ is defined as

$$N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I}) = \mathrm{Card}\left(\mathscr{O}_{\mathbb{K}}/\mathscr{I}\right).$$

Moreover, if I is principal, generated by α, then $N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I}) = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|$.

Determinant

Suppose that we consider the canonical embedding of an ideal $\mathscr{I}$ of absolute norm $N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I})$. Then the lattice obtained by canonical embedding has determinant,

$$\det\left(\Lambda_{\mathscr{I}}\right) = N_{\mathbb{K}/\mathbb{Q}}(\mathscr{I})^2 \cdot d_{\mathbb{K}}$$

Rotation

If we want to have a chance of generating a lattice equivalent to $\mathbb{Z}^n$, then $\det\left(\Lambda_{\mathscr{I}}\right) = q^n$ for some integer q. If it is impossible, then try to use the trace form $(x,y)_\beta = \mathrm{Tr}\left(\beta xy\right)$.

Part V

Lattices for Security

Outline of current Part

The Gaussian Wiretap Channel

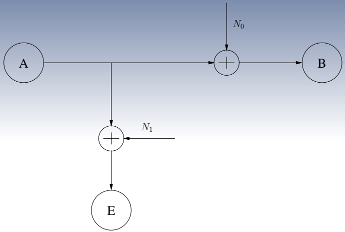


Figure: The Gaussian Wiretap Channel model

The Gaussian Wiretap Channel

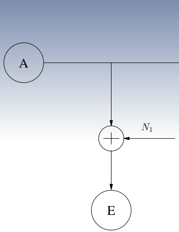


Figure: The Gaussian Wiretap Channel model

The secrecy capacity is given by

$$\boxed{C_s = [C_{A\to B} - C_{A\to E}]^+}$$

where $C_{A\to B} = \log_2\left(1+\frac{P}{N_0}\right)$ and $C_{A\to E} = \log_2\left(1+\frac{P}{N_1}\right)$ can be achieved by doing **lattice coding**.
Of course, $C_s > 0$ if $N_0 < N_1$.

Encoder Design

- The problem of Wiretap is a problem of **labelling** transmitted symbols with data bits

Encoder Design

- The problem of Wiretap is a problem of **labelling** transmitted symbols with data bits

+2 mod (4) Channel

We suppose the alphabet $\mathbb{Z}_4$ and a channel Alice$\longrightarrow$Eve that outputs

$$y = x + 2$$

with probability $1/2$ and x with same probability. The **symbol** error probability is $1/2$.

Encoder Design

- The problem of Wiretap is a problem of **labelling** transmitted symbols with data bits

$+2$ mod (4) Channel

We suppose the alphabet $\mathbb{Z}_4$ and a channel Alice$\longrightarrow$Eve that outputs

$$y = x + 2$$

with probability $1/2$ and x with same probability. The **symbol** error probability is $1/2$.

Symbol to Bits Labelling

$$s = 2b_1 + b_0$$

Bit b_1 experiences error probability $1/2$ while bit b_0 experiences error probability 0.

Encoder Design

- The problem of Wiretap is a problem of **labelling** transmitted symbols with data bits

$+2$ mod (4) Channel

We suppose the alphabet $\mathbb{Z}_4$ and a channel Alice$\hookrightarrow$Eve that outputs

$$y = x + 2$$

with probability $1/2$ and x with same probability. The **symbol** error probability is $1/2$.

Symbol to Bits Labelling

$$s = 2b_1 + b_0$$

Bit b_1 experiences error probability $1/2$ while bit b_0 experiences error probability 0.

Confidential data must be encoded through b_1. On b_0, put random bits.

Outline of current Part

Uniform Noise

Assume that **Alice** → **Eve** channel is corrupted by an additive uniform noise

Uniform Noise

Assume that **Alice** → **Eve** channel is corrupted by an additive uniform noise

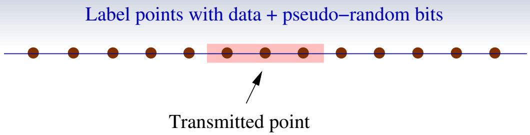


Figure: Constellation corrupted by uniform noise

Uniform Noise

Assume that **Alice** → **Eve** channel is corrupted by an additive uniform noise

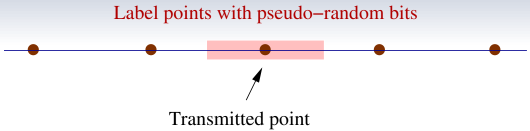


Figure: Points can be decoded **error free**: label with pseudo-random symbols

Uniform Noise

Assume that **Alice** → **Eve** channel is corrupted by an additive uniform noise

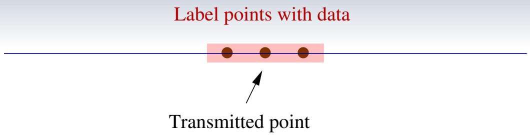


Figure: Points are **not distinguishable**: label with data

Uniform Noise

Assume that **Alice** → **Eve** channel is corrupted by an additive uniform noise

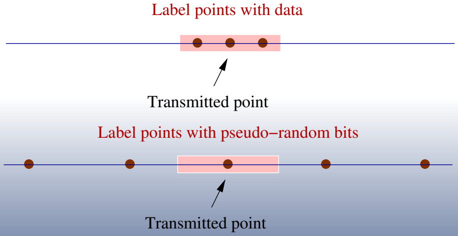


Figure: Constellation corrupted by uniform noise

Uniform Noise

Assume that **Alice** → **Eve** channel is corrupted by an additive uniform noise

Error Probability

Pseudo-random symbols are perfectly decoded by Eve when data error probability will be high.

- unfortunately **not valid** for **Gaussian** noise.

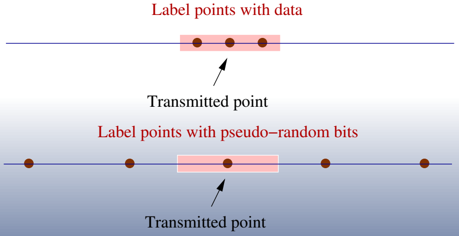


Figure: Constellation corrupted by uniform noise

Coset Coding with Integers

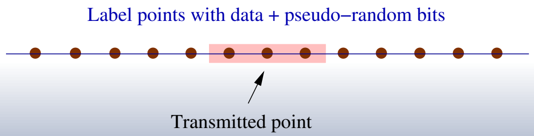


Figure: Constellation corrupted by uniform noise

Coset Coding with Integers

Example

- Suppose that points x are in $\mathbb{Z}$.
- Euclidean division

$$x = 3q + r$$

- q carries the pseudo-random symbols while r carries the data **or** "pseudo-random symbols label points in $3\mathbb{Z}$ while data label elements of $\mathbb{Z}/3\mathbb{Z}$".

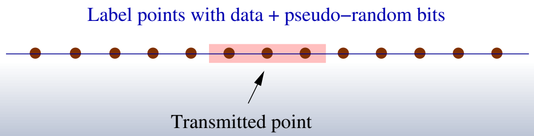


Figure: Constellation corrupted by uniform noise

Lattice Coset Coding

Gaussian noise is **not** bounded: it **needs** a $n-$dimensional approach (then let $n \to \infty$ for **sphere hardening**).

	$1-$dimensional	$n-$dimensional
Transmitted lattice	$\mathbb{Z}$	Fine lattice Λ_b
Pseudo-random symbols	$m\mathbb{Z} \subset \mathbb{Z}$	Coarse lattice $\Lambda_e \subset \Lambda_b$
Data	$\mathbb{Z}/m\mathbb{Z}$	Cosets Λ_b/Λ_e

Table: From the example to the general scheme

Lattice Coset Coding

Gaussian noise is **not** bounded: it **needs** a $n-$dimensional approach (then let $n \to \infty$ for **sphere hardening**).

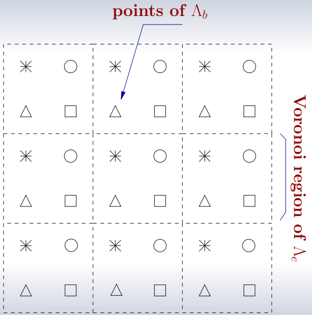


Figure: Example of coset coding

Lattice Coset Coding

Gaussian noise is **not** bounded: it **needs** a $n-$dimensional approach (then let $n \to \infty$ for **sphere hardening**).

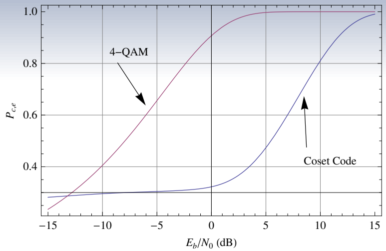


Figure: Probability of correct decoding for coset coding compared to QPSK

Probability of correct decoding is given by

$$P_{c,e} = \left[1 - \frac{1}{3}\left(5Q\left(\sqrt{\theta}\right) - 4Q\left(3\sqrt{\theta}\right) + 3Q\left(5\sqrt{\theta}\right) - 2Q\left(7\sqrt{\theta}\right) + Q\left(9\sqrt{\theta}\right)\right)\right]^2, \theta = \frac{6}{35}\frac{E_b}{N_0}$$

Outline of current Part

Eve's Probability of Correct Decision (data)

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

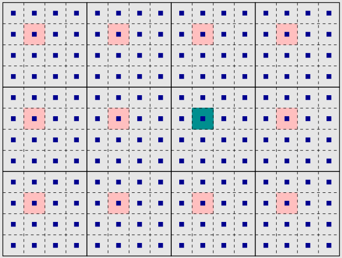


Figure: Eve correctly decodes when finding another coset representative

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

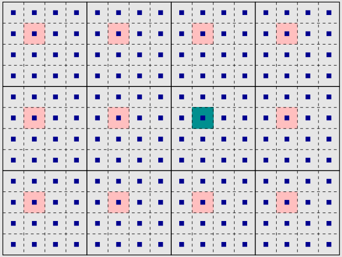


Figure: Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision

$$
\begin{aligned}
P_{c,e} &\leq \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^n \mathrm{Vol}\left(\Lambda_b\right) \sum_{\mathbf{r}\in\Lambda_e} e^{-\frac{\|\mathbf{r}\|^2}{2N_1}} \\
&= \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^n \mathrm{Vol}\left(\Lambda_b\right) \Theta_{\Lambda_e}\left(\frac{1}{2\pi\sigma^2}\right)
\end{aligned}
$$

where

$$
\Theta_\Lambda(y) = \sum_{\vec{x}\in\Lambda} q^{\|\vec{x}\|^2}, q = e^{-\pi y}, y > 0
$$

is the **theta series** of Λ and $\sigma^2 = N_1$.

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

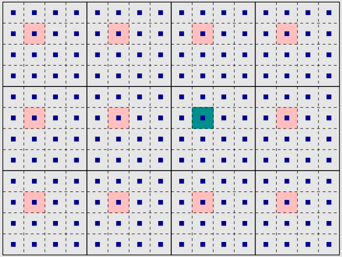


Figure: Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision

$$P_{c,e} \leq \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^n \mathrm{Vol}\left(\Lambda_b\right) \sum_{\mathbf{r}\in\Lambda_e} e^{-\frac{\|\mathbf{r}\|^2}{2N_1}}$$

$$= \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^n \mathrm{Vol}\left(\Lambda_b\right) \Theta_{\Lambda_e}\left(\frac{1}{2\pi\sigma^2}\right)$$

where

$$\Theta_\Lambda(y) = \sum_{\vec{x}\in\Lambda} q^{\|\vec{x}\|^2}, q = e^{-\pi y}, y > 0$$

is the **theta series** of Λ and $\sigma^2 = N_1$.

Problem

Find Λ minimizing

$$\boxed{\Theta_\Lambda(y)}$$

for some y.

Secrecy function

Definition

Let Λ be a $n-$dimensional lattice with fundamental volume λ^n. Its **secrecy function** is defined as,

$$\Xi_\Lambda(y) \triangleq \frac{\Theta_{\lambda\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{\vartheta_3^n\left(e^{-\pi\sqrt{\lambda}y}\right)}{\Theta_\Lambda(y)}$$

where $\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ and $y > 0$.

Secrecy function

Definition

Let Λ be a $n-$dimensional lattice with fundamental volume λ^n. Its **secrecy function** is defined as,

$$\Xi_\Lambda(y) \triangleq \frac{\Theta_{\lambda\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{\vartheta_3^n\left(e^{-\pi\sqrt{\lambda}y}\right)}{\Theta_\Lambda(y)}$$

where $\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ and $y > 0$.

Examples

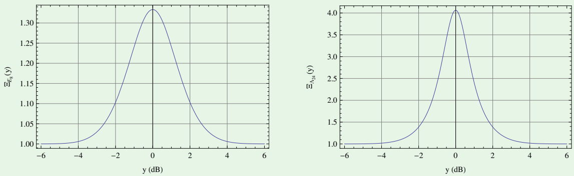


Figure: Secrecy functions of E_8 and Λ_{24}

Secrecy Gain

Definition

The **strong secrecy gain** of a lattice Λ is

$$\boxed{\chi_\Lambda^s \triangleq \sup_{y>0} \Xi_\Lambda(y)}$$

Secrecy Gain

Definition

The **strong secrecy gain** of a lattice Λ is

$$\boxed{\chi_\Lambda^s \triangleq \sup_{y>0} \Xi_\Lambda(y)}$$

- A lattice equivalent to its dual has a theta series with a **multiplicative symmetry point** at $d(\Lambda)^{-\frac{1}{n}}$ (**Poisson-Jacobi's** formula),

$$\boxed{\Xi_\Lambda\left(d(\Lambda)^{-\frac{1}{n}}y\right) = \Xi_\Lambda\left(\frac{d(\Lambda)^{-\frac{1}{n}}}{y}\right)}$$

Secrecy Gain

Definition

The **strong secrecy gain** of a lattice Λ is

$$\boxed{\chi_\Lambda^s \triangleq \sup_{y>0} \Xi_\Lambda(y)}$$

- A lattice equivalent to its dual has a theta series with a **multiplicative symmetry point** at $d(\Lambda)^{-\frac{1}{n}}$ (**Poisson-Jacobi's** formula),

$$\boxed{\Xi_\Lambda\left(d(\Lambda)^{-\frac{1}{n}} y\right) = \Xi_\Lambda\left(\frac{d(\Lambda)^{-\frac{1}{n}}}{y}\right)}$$

Definition

For a lattice Λ equivalent to its dual and of determinant (volume) $d(\Lambda)$, we define the **weak secrecy gain**,

$$\boxed{\chi_\Lambda \triangleq \Xi_\Lambda\left(d(\Lambda)^{-\frac{1}{n}}\right)}$$

Conjecture

Conjecture

If Λ is a lattice equivalent to its dual, then the strong and the weak secrecy gains coincide.

Corollary

*The strong secrecy gain of a unimodular lattice Λ is $\chi_\Lambda^s \triangleq \Xi_\Lambda(1)$ (unimodular means that the Gram matrix has **integer-valued** entries and **determinant** equal to 1).*

Conjecture

Conjecture

If Λ is a lattice equivalent to its dual, then the strong and the weak secrecy gains coincide.

Corollary

*The strong secrecy gain of a unimodular lattice Λ is $\chi_\Lambda^s \triangleq \Xi_\Lambda(1)$ (unimodular means that the Gram matrix has **integer-valued** entries and **determinant** equal to 1).*

Calculation of E_8 secrecy gain

From E_8 theta series,

$$\begin{aligned}\frac{1}{\Xi_{E_8}(1)} &= \frac{\frac{1}{2}\left(\vartheta_2(e^{-\pi})^8+\vartheta_3(e^{-\pi})^8+\vartheta_4(e^{-\pi})^8\right)}{\vartheta_3(e^{-\pi})^8}\\ &= \frac{3}{4} \quad \left(\text{since } \frac{\vartheta_2\left(e^{-\pi}\right)}{\vartheta_3\left(e^{-\pi}\right)}=\frac{\vartheta_4\left(e^{-\pi}\right)}{\vartheta_3\left(e^{-\pi}\right)}=\frac{1}{\sqrt[4]{2}}\right)\end{aligned}$$

so we get $\boxed{\chi_{E_8} = \Xi_{E_8}(1) = \frac{4}{3}}$.

Outline of current Part

Even Unimodular Lattices

Definition

An **even unimodular lattice** is a lattice whose squared length of all its vectors is always an even integer). For instance, E_8 or the Leech lattice Λ_{24} are even unimodular.

Even Unimodular Lattices

Definition

An **even unimodular lattice** is a lattice whose squared length of all its vectors is always an even integer). For instance, E_8 or the Leech lattice Λ_{24} are even unimodular.

Properties

An even unimodular lattice Λ only exists when n is a multiple of 8. The minimum squared length of any non zero vector is upperbounded

$$\delta^2 \leq 2(m+1)$$

where $n = 24m + 8k$, $k = 0, 1, 2$. A lattice achieving this upperbound is called **extremal**.

Secrecy Gain of Extremal Lattices

Secrecy Functions in dimensions 72 and 80

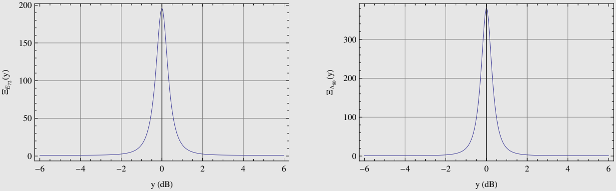


Figure: Secrecy functions of extremal lattices ($n = 72, 80$)

Secrecy Gain of Extremal Lattices

Secrecy Functions in dimensions 72 and 80

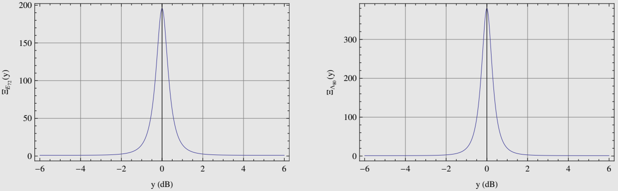


Figure: Secrecy functions of extremal lattices ($n = 72, 80$)

Secrecy gains of extremal lattices (all rational numbers !!!)

Dimension	8	24	32	48	72	80
Secrecy gain	$\frac{4}{3}$	$\frac{256}{63}$	$\frac{64}{9}$	$\frac{524288}{19467}$	$\frac{134217728}{685881} \simeq 195.7$	$\frac{536870912}{1414413} \simeq 380$

Secrecy Gain of Extremal Even Unimodular Lattices

Theorem

The secrecy gain of an even unimodular lattice is a rational number.

Secrecy Gain of Extremal Even Unimodular Lattices

Theorem

The secrecy gain of an even unimodular lattice is a rational number.

Proof.

Theta series of an even unimodular lattice Λ ($n = 24m + 8k$),

$$\Theta_\Lambda = \sum_{j=0}^{m} b_j E_4^{3(m-j)+k} \Delta^j$$

with $E_4 = \frac{1}{2}\left(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8\right)$, $\Delta = \frac{1}{256}\left(\vartheta_2\vartheta_3\vartheta_4\right)^8$ and $b_j \in \mathbb{Q}$. For an extremal lattice, the annihilation of the first terms give integer b_j. As

$$\begin{cases} \vartheta_2\left(e^{-\pi}\right) & = \vartheta_4\left(e^{-\pi}\right) \\ \vartheta_3\left(e^{-\pi}\right) & = \sqrt[4]{2}\,\vartheta_4\left(e^{-\pi}\right) \end{cases},$$

we obtain

$$E_4\left(e^{-\pi}\right) = \frac{3}{4}\vartheta_3^8\left(e^{-\pi}\right) \qquad \text{and} \qquad \Delta\left(e^{-\pi}\right) = \frac{1}{2^{12}}\vartheta_3^{24}\left(e^{-\pi}\right)$$

giving the rationality of $\Xi_\Lambda(1)$. □

Asymptotic behavior (I)

- Want to study the behavior of even unimodular lattices when n becomes large.

Question

How does the optimal secrecy gain behaves when $n \to \infty$?

Asymptotic behavior (I)

- Want to study the behavior of even unimodular lattices when n becomes large.

Question

How does the optimal secrecy gain behaves when $n \to \infty$?

First answer

Apply the Siegel-Weil formula,

$$\sum_{\Lambda \in \Omega_n} \frac{\Theta_\Lambda(q)}{|\mathrm{Aut}(\Lambda)|} = M_n \cdot E_k\left(q^2\right)$$

where

$$M_n = \sum_{\Lambda \in \Omega_n} \frac{1}{|\mathrm{Aut}(\Lambda)|}$$

and E_k is the Eisenstein series with weight $k = \frac{n}{2}$. Ω_n is the set of all inequivalent $n-$dimensional, even unimodular lattices. We get

$$\boxed{\Theta_{n,\mathrm{opt}}\left(e^{-\pi}\right) \leq E_k\left(e^{-2\pi}\right)}$$

Asymptotic behavior (II)

Maximal Secrecy gain

For a given dimension n, multiple of 8, there **exists** an even unimodular lattice whose secrecy gain is

$$\boxed{\chi_n \geq \frac{\vartheta_3^n\left(e^{-\pi}\right)}{E_k\left(e^{-2\pi}\right)} \simeq \frac{1}{2}\left(\frac{\pi^{\frac{1}{4}}}{\Gamma\left(\frac{3}{4}\right)}\right)^n \simeq \frac{1.086^n}{2}}$$

Asymptotic behavior (II)

Maximal Secrecy gain

For a given dimension n, multiple of 8, there **exists** an even unimodular lattice whose secrecy gain is

$$\boxed{\chi_n \geq \frac{\vartheta_3^n\left(e^{-\pi}\right)}{E_k\left(e^{-2\pi}\right)} \simeq \frac{1}{2}\left(\frac{\pi^{\frac{1}{4}}}{\Gamma\left(\frac{3}{4}\right)}\right)^n \simeq \frac{1.086^n}{2}}$$

Behavior of Eisenstein Series

We have

$$E_k\left(e^{-2\pi}\right) = 1 + \frac{2k}{\left|B_k\right|}\sum_{m=1}^{+\infty}\frac{m^{k-1}}{e^{2\pi m}-1}$$

B_k being the Bernoulli numbers. For k a multiple of 4, then $E_k\left(e^{-2\pi}\right)$ fastly converges to 2 ($k \to \infty$).

Asymptotic behavior (II)

Maximal Secrecy gain

For a given dimension n, multiple of 8, there **exists** an even unimodular lattice whose secrecy gain is

$$\boxed{\chi_n \geq \frac{\vartheta_3^n\left(e^{-\pi}\right)}{E_k\left(e^{-2\pi}\right)} \simeq \frac{1}{2}\left(\frac{\pi^{\frac{1}{4}}}{\Gamma\left(\frac{3}{4}\right)}\right)^n \simeq \frac{1.086^n}{2}}$$

Behavior of Eisenstein Series

We have

$$E_k\left(e^{-2\pi}\right) = 1 + \frac{2k}{|B_k|}\sum_{m=1}^{+\infty}\frac{m^{k-1}}{e^{2\pi m}-1}$$

B_k being the Bernoulli numbers. For k a multiple of 4, then $E_k\left(e^{-2\pi}\right)$ fastly converges to 2 ($k \to \infty$).

Bound from Siegel-Weil Formula vs. Extremal lattices

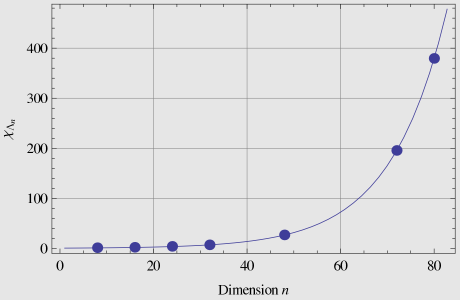


Figure: Lower bound of the minimal secrecy gain as a function of n from Siegel-Weil formula. **Points** correspond to **extremal lattices**.

Another way of analyzing the asymptotic behavior

Expression of the theta series

For a $2k$−dimensional even unimodular lattice, the Fourier decomposition gives

$$\Theta_\Lambda(z) = E_k(z) + S_k(z,\Lambda) = \sum_{m=0}^{\infty} r(m,\Lambda)\, e^{2i\pi mz}$$

where $S_k(z,\Lambda)$ is a cusp form.

Another way of analyzing the asymptotic behavior

Expression of the theta series

For a $2k$−dimensional even unimodular lattice, the Fourier decomposition gives

$$\Theta_\Lambda(z) = E_k(z) + S_k(z,\Lambda) = \sum_{m=0}^{\infty} r(m,\Lambda)\, e^{2i\pi mz}$$

where $S_k(z,\Lambda)$ is a cusp form.

Fourier coefficients

If $S_k(z,\Lambda) = \sum_{m=0}^{\infty} a(m,\Lambda)\, e^{2i\pi mz}$, then,

$$r(m,\Lambda) = \underbrace{\frac{(2\pi)^k}{\zeta(k)\Gamma(k)}\sigma_{k-1}(m)}_{E_k} + \underbrace{a(m,\Lambda)}_{S_k}$$

Another way of analyzing the asymptotic behavior

Expression of the theta series

For a $2k-$dimensional even unimodular lattice, the Fourier decomposition gives

$$\Theta_\Lambda(z) = E_k(z) + S_k(z,\Lambda) = \sum_{m=0}^{\infty} r(m,\Lambda)\, e^{2i\pi mz}$$

where $S_k(z,\Lambda)$ is a cusp form.

Fourier coefficients

If $S_k(z,\Lambda) = \sum_{m=0}^{\infty} a(m,\Lambda)\, e^{2i\pi mz}$, then,

$$r(m,\Lambda) = \underbrace{\frac{(2\pi)^k}{\zeta(k)\Gamma(k)}\sigma_{k-1}(m)}_{E_k} + \underbrace{a(m,\Lambda)}_{S_k}$$

Asymptotics

Asymptotic analysis gives

$$\begin{cases} \sigma_{k-1}(m) & = O\left(m^{k-1}\right) \\ a(m,\Lambda) & = O\left(m^{\frac{k}{2}}\right) \end{cases}$$

Another way of analyzing the asymptotic behavior

Expression of the theta series

For a $2k$−dimensional even unimodular lattice, the Fourier decomposition gives

$$\Theta_\Lambda(z) = E_k(z) + S_k(z,\Lambda) = \sum_{m=0}^{\infty} r(m,\Lambda)\, e^{2i\pi mz}$$

where $S_k(z,\Lambda)$ is a cusp form.

Fourier coefficients

If $S_k(z,\Lambda) = \sum_{m=0}^{\infty} a(m,\Lambda)\, e^{2i\pi mz}$, then,

$$r(m,\Lambda) = \underbrace{\frac{(2\pi)^k}{\zeta(k)\Gamma(k)}\sigma_{k-1}(m)}_{E_k} + \underbrace{a(m,\Lambda)}_{S_k}$$

Asymptotics

Asymptotic analysis gives

$$\begin{cases} \sigma_{k-1}(m) & = O\left(m^{k-1}\right) \\ a(m,\Lambda) & = O\left(m^{\frac{k}{2}}\right) \end{cases}$$

Conclusion

Coefficients of E_k are asymptotic estimates of the coefficients of Θ_Λ. The secrecy gain of any even unimodular lattice behaves like

$$\boxed{\frac{\vartheta_3^{2k}\left(e^{-\pi}\right)}{E_k\left(e^{-2\pi}\right)}}$$

when $k \to \infty$.

Outline of current Part

Maximum Likelihood Decoding

Best Strategy for the eavesdropper

Signal transmitted by Alice is

$$\boldsymbol{x} = \boldsymbol{d} + \boldsymbol{r}, \qquad \boldsymbol{r} \in \Lambda_e, \boldsymbol{d} \in \Lambda_b / \Lambda_e.$$

Eve maximizes over all possible $\boldsymbol{d}$,

$$\sum_{\boldsymbol{r} \in \Lambda_e} p\left(\boldsymbol{y}_e / \boldsymbol{d}, \boldsymbol{r}\right) \propto \sum_{\boldsymbol{r} \in \Lambda_e} e^{-\frac{\|\boldsymbol{y}_e - \boldsymbol{d} - \boldsymbol{r}\|^2}{2\sigma^2}}$$

where $\boldsymbol{y}_e$ is the signal received by Eve.

An Example

The $2\mathbb{Z}^2$ example

$$\boxed{\sum_{\boldsymbol{x}\in 2\mathbb{Z}^2} e^{-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}}}$$

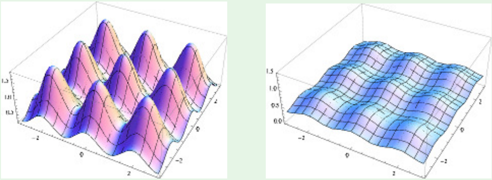


Figure: Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

Flatness Factor

Definition

Let

$$f_{\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{2\sigma^2}}$$

and

$$f_{\sigma,\Lambda}(\boldsymbol{x}) = \sum_{\boldsymbol{\lambda}\in\Lambda} f_{\sigma,\boldsymbol{\lambda}}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}.$$

Then, the **flatness** factor for lattice Λ and parameter σ is

$$\varepsilon_\Lambda(\sigma) = \frac{\max_{\boldsymbol{x}\in\mathscr{R}(\Lambda)} \left| f_{\sigma,\Lambda}(\boldsymbol{x}) - \frac{1}{V(\Lambda)} \right|}{\frac{1}{V(\Lambda)}}$$

which means that $f_{\sigma,\Lambda}(\boldsymbol{x})$ is within $1 \pm \varepsilon_\Lambda(\sigma)$ from the uniform distribution over the Voronoi cell.

Flatness Factor

Definition

Let

$$f_{\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{2\sigma^2}}$$

and

$$f_{\sigma,\Lambda}(\boldsymbol{x}) = \sum_{\boldsymbol{\lambda}\in\Lambda} f_{\sigma,\boldsymbol{\lambda}}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}.$$

Then, the **flatness** factor for lattice Λ and parameter σ is

$$\varepsilon_\Lambda(\sigma) = \frac{\max_{\boldsymbol{x}\in\mathscr{R}(\Lambda)} \left| f_{\sigma,\Lambda}(\boldsymbol{x}) - \frac{1}{V(\Lambda)} \right|}{\frac{1}{V(\Lambda)}}$$

which means that $f_{\sigma,\Lambda}(\boldsymbol{x})$ is within $1 \pm \varepsilon_\Lambda(\sigma)$ from the uniform distribution over the Voronoi cell.

Connection with smoothing parameter

Let $\eta_\epsilon(\Lambda) = \sqrt{2\pi}\sigma$ be the **smoothing parameter**, then solve

$$\varepsilon_\Lambda(\sigma) = \epsilon.$$

Flatness Factor

Definition

Let

$$f_{\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{2\sigma^2}}$$

and

$$f_{\sigma,\Lambda}(\boldsymbol{x}) = \sum_{\boldsymbol{\lambda}\in\Lambda} f_{\sigma,\boldsymbol{\lambda}}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}.$$

Then, the **flatness** factor for lattice Λ and parameter σ is

$$\varepsilon_\Lambda(\sigma) = \frac{\max_{\boldsymbol{x}\in\mathscr{R}(\Lambda)} \left| f_{\sigma,\Lambda}(\boldsymbol{x}) - \frac{1}{V(\Lambda)} \right|}{\frac{1}{V(\Lambda)}}$$

which means that $f_{\sigma,\Lambda}(\boldsymbol{x})$ is within $1 \pm \varepsilon_\Lambda(\sigma)$ from the uniform distribution over the Voronoi cell.

Connection with smoothing parameter

Let $\eta_\epsilon(\Lambda) = \sqrt{2\pi}\sigma$ be the **smoothing parameter**, then solve

$$\varepsilon_\Lambda(\sigma) = \epsilon.$$

Expression

We have

$$\varepsilon_\Lambda(\sigma) = \gamma_\Lambda(\sigma)^{\frac{n}{2}} \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right) - 1$$

where $\gamma_\Lambda(\sigma) = \frac{V(\Lambda)^{\frac{2}{n}}}{2\pi\sigma^2}$ is the **GSNR** (Generalized Signal to Noise Ratio).

Mutual Information

Theorem

Let ε_n be the flatness factor of Λ_e on Eve's channel. M *is the message transmitted by Alice and Z^n is what is received by Eve. Then,*

$$I\left(\mathsf{M};Z^n\right) \leq 2nR\varepsilon_n - 2\varepsilon_n \log\left(2\varepsilon_n\right)$$

where R is the rate per dimension.

Mutual Information

Theorem

Let ε_n be the flatness factor of Λ_e on Eve's channel. M *is the message transmitted by Alice and Z^n is what is received by Eve. Then,*

$$I\left(\mathsf{M};Z^n\right) \leq 2nR\varepsilon_n - 2\varepsilon_n \log\left(2\varepsilon_n\right)$$

where R is the rate per dimension.

Corollary

If $\varepsilon_n \to 0$ when $n \to \infty$, then

$$\lim_{n\to\infty} I\left(\mathsf{M};Z^n\right) = 0$$

which guarantees the strong secrecy property of the system.

Mutual Information

Theorem

Let ε_n be the flatness factor of Λ_e on Eve's channel. M is the message transmitted by Alice and Z^n is what is received by Eve. Then,

$$I\left(\mathsf{M};Z^n\right) \leq 2nR\varepsilon_n - 2\varepsilon_n \log(2\varepsilon_n)$$

where R is the rate per dimension.

Corollary

If $\varepsilon_n \to 0$ when $n \to \infty$, then

$$\lim_{n\to\infty} I\left(\mathsf{M};Z^n\right) = 0$$

which guarantees the strong secrecy property of the system.

Average behavior

By using the **Minkowski-Hlawka** theorem, we see that, on average, when n becomes large enough, ε_n behaves like $\gamma_{\Lambda_e}(\sigma)^{\frac{n}{2}}$ which tends to 0 **exponentially** when $\gamma_{\Lambda_e}(\sigma) < 1$.

Illustration I

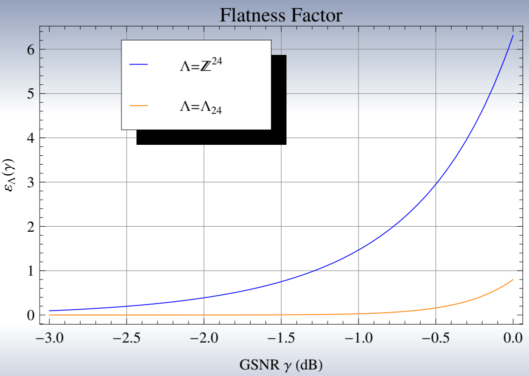


Figure: Flatness Factors in dimension 24

Illustration II

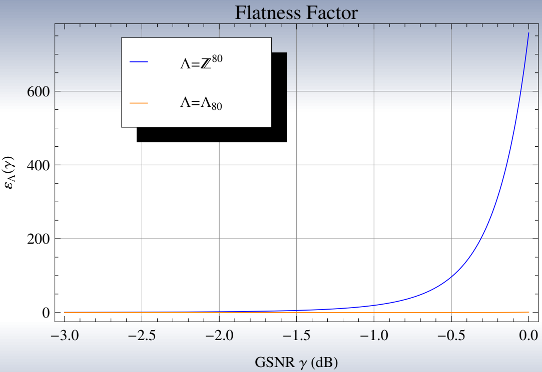


Figure: Some Flatness Factors in dimension 80

Thank You !!