Lattices for Communication Engineers

Jean-Claude Belfiore

Télécom ParisTech CNRS, LTCI UMR 5141
February, 22 2011

Nanyang Technological University - SPMS

Part I

Introduction

The transmission problem

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

The transmission problem

- Link 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

- Link 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 $\left\{h(t-kT)\, e^{i\frac{2\pi k}{N+1}\Delta f t}\right\}_{k,q}$ 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 used in practice are QAM symbols, components of vector $\boldsymbol{x}$.
- We need to introduce coding $\longrightarrow$ **structure** the QAM symbols.

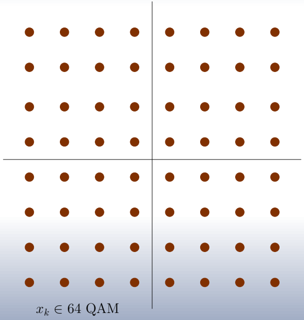


Figure: Symbol from a 64 QAM

Definition and properties

Definition

A **Euclidean** $\mathbb{Z}-$**lattice** is a discrete additive subgroup with rank p, $p \leq n$ of the Euclidean space $\mathbb{R}^n$. We restrict to the case $p = n$ in the sequel.

Definition and properties

Definition

A **Euclidean** $\mathbb{Z}-$**lattice** is a discrete additive subgroup with rank p, $p \leq n$ of the Euclidean space $\mathbb{R}^n$. We restrict to the case $p = n$ in the sequel.

- A lattice $\boldsymbol{\Lambda}$ is a $\mathbb{Z}-$module generated by vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ of $\mathbb{R}^n$.
- An element $\boldsymbol{v}$ of $\boldsymbol{\Lambda}$ can be written as :

$$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \ldots + a_n\boldsymbol{v}_n, \quad a_1, a_2, \ldots, a_n \in \mathbb{Z}$$

Definition and properties

Definition

A **Euclidean** $\mathbb{Z}-$**lattice** is a discrete additive subgroup with rank p, $p \leq n$ of the Euclidean space $\mathbb{R}^n$. We restrict to the case $p = n$ in the sequel.

- A lattice $\boldsymbol{\Lambda}$ is a $\mathbb{Z}-$module generated by vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ of $\mathbb{R}^n$.
- An element $\boldsymbol{v}$ of $\boldsymbol{\Lambda}$ can be written as :

$$\boldsymbol{v} = a_1 \boldsymbol{v}_1 + a_2 \boldsymbol{v}_2 + \ldots + a_n \boldsymbol{v}_n, \quad a_1, a_2, \ldots, a_n \in \mathbb{Z}$$

- The lattice $\boldsymbol{\Lambda}$ can be defined as :

$$\boldsymbol{\Lambda} = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{v}_i \mid a_i \in \mathbb{Z} \right\}$$

Lattices : Generator matrix

- The set of vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ is a **lattice basis**.

Definition

Matrix $\boldsymbol{M}$ whose columns are vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ is a **generator matrix** of the lattice denoted $\Lambda_{\boldsymbol{M}}$.

Lattices : Generator matrix

- The set of vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ is a **lattice basis**.

Definition

Matrix $\boldsymbol{M}$ whose columns are vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ is a **generator matrix** of the lattice denoted $\Lambda_{\boldsymbol{M}}$.

- Each vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)^\top$ in $\Lambda_{\boldsymbol{M}}$, can be written as,

$$\boldsymbol{x} = \boldsymbol{M} \cdot \boldsymbol{z}$$

  where $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)^\top \in \mathbb{Z}^n$.

- Lattice $\Lambda_{\boldsymbol{M}}$ may be seen as the result of a linear transform applied to lattice $\mathbb{Z}^n$ (cubic lattice).

Lattices : Elementary Properties (I)

- Let $\boldsymbol{Q} \in \mathcal{M}_n(\mathbb{R})$, such that $\boldsymbol{Q}^\top \cdot \boldsymbol{Q} = \boldsymbol{I}_n$ be an isometry. The two lattices $\Lambda_{\boldsymbol{M}}$ and $\Lambda_{\boldsymbol{Q}\cdot\boldsymbol{M}}$ are said **equivalent**.
- Lattice $\Lambda_{\boldsymbol{Q}\cdot\boldsymbol{M}}$ is a rotated version of $\Lambda_{\boldsymbol{M}}$ if $\det \boldsymbol{Q} = 1$.

Lattices : Elementary Properties (I)

- Let $\boldsymbol{Q} \in \mathscr{M}_n(\mathbb{R})$, such that $\boldsymbol{Q}^\top \cdot \boldsymbol{Q} = \boldsymbol{I}_n$ be an isometry. The two lattices $\Lambda_{\boldsymbol{M}}$ and $\Lambda_{\boldsymbol{Q}\cdot\boldsymbol{M}}$ are said **equivalent**.
- Lattice $\Lambda_{\boldsymbol{Q}\cdot\boldsymbol{M}}$ is a rotated version of $\Lambda_{\boldsymbol{M}}$ if $\det \boldsymbol{Q} = 1$.
- If $\boldsymbol{T} \in \mathscr{M}_n(\mathbb{Z})$ and $\det \boldsymbol{T} \neq \pm 1$, then lattice $\Lambda_{\boldsymbol{M}\cdot\boldsymbol{T}}$ is a **sublattice** of $\Lambda_{\boldsymbol{M}}$.
- We will often consider sublattices of $\mathbb{Z}^n$.

Lattices : Elementary Properties (II)

- The generator matrix $\boldsymbol{M}$ describes the lattice $\Lambda_{\boldsymbol{M}}$, but it is not unique. All matrices $\boldsymbol{M} \cdot \boldsymbol{T}$ with $\boldsymbol{T} \in \mathscr{M}_n(\mathbb{Z})$ and $\det \boldsymbol{T} = \pm 1$ are generator matrices of $\Lambda_{\boldsymbol{M}}$. $\boldsymbol{T}$ is called a unimodular matrix.
- $\boldsymbol{G} = \boldsymbol{M}^\top \cdot \boldsymbol{M}$ is the ***Gram matrix*** of the lattice . $\boldsymbol{M}^\top$ is also a generator matrix of the **dual** of $\Lambda_{\boldsymbol{M}}$.
- We define then gemetric parameters.

Lattices : Elementary Properties (II)

- The generator matrix $\boldsymbol{M}$ describes the lattice $\Lambda_{\boldsymbol{M}}$, but it is not unique. All matrices $\boldsymbol{M}\cdot\boldsymbol{T}$ with $\boldsymbol{T}\in\mathscr{M}_n(\mathbb{Z})$ and $\det\boldsymbol{T}=\pm 1$ are generator matrices of $\Lambda_{\boldsymbol{M}}$. $\boldsymbol{T}$ is called a unimodular matrix.
- $\boldsymbol{G}=\boldsymbol{M}^{\top}\cdot\boldsymbol{M}$ is the ***Gram matrix*** of the lattice . $\boldsymbol{M}^{\top}$ is also a generator matrix of the **dual** of $\Lambda_{\boldsymbol{M}}$.
- We define then gemetric parameters.

Definitions

- The **fundamental parallelotope** of $\Lambda_{\boldsymbol{M}}$ is the region,

$$\mathscr{P}=\left\{\boldsymbol{x}\in\mathbb{R}^n \mid \boldsymbol{x}=a_1\boldsymbol{v}_1+a_2\boldsymbol{v}_2+\ldots+a_n\boldsymbol{v}_n,\ 0\leq a_i<1,\ i=1\ldots n\right\}$$

- The ***fundamental volume*** is the volume of the fundamental parallelotope. It is denoted $\mathrm{vol}(\Lambda_{\boldsymbol{M}})$.
- The fundamental volume of the lattice is $\mathrm{vol}\left(\Lambda_{\boldsymbol{M}}\right)=|\det(\boldsymbol{M})|$, which is $\sqrt{\det(\boldsymbol{G})}$ either.

Lattices : Elementary Properties (III)

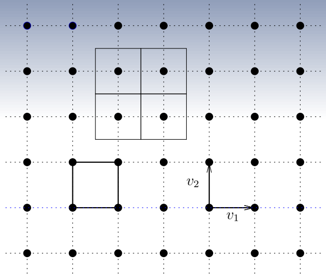
Definition

The ***Voronoï cell*** of a point u belonging to the lattice Λ is the region

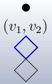
$$\mathcal{V}_{\Lambda}(\boldsymbol{u}) = \left\{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}-\boldsymbol{u}\| \leq \left\|\boldsymbol{x}-\boldsymbol{y}\right\|, \quad \boldsymbol{y} \in \Lambda\right\}$$

- All Voronoï cells of a lattice are translated versions of the Voronoï cell of the zero point. This cell is called **Voronoï cell of the lattice**.
- The fundamental volume of a lattice is equal to the volume of its Voronoï cell.

The $\mathbb{Z}^2$ -lattice

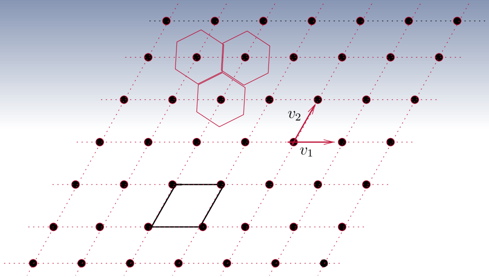


$\mathbb{Z}^2$ lattice



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

The A_2 lattice



The A_2 lattice

●	Lattice point
(v_1, v_2)	Lattice basis
◇	Fundamental parallelotope
◇	Voronoi region

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

Construction A (binary)

Construction A for a $\mathbb{Z}-$lattice

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 (binary)

Construction A for a $\mathbb{Z}-$lattice

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

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

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

Construction A (binary)

Construction A for a $\mathbb{Z}-$lattice

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

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

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

Construction of E_8

E_8 is obtained as

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

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

Construction A (quaternary)

Construction A of the Leech lattice

The Leech lattice can be obtained as

$$2\Lambda_{24} = 2\mathbb{Z}^{24} + (24,12)_{\mathbb{Z}_4}$$

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

$$2\Lambda_{24} = 2\mathbb{Z}^{24} + (24,12)_{\mathbb{Z}_4}$$

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 or D for instance. But one can show that all these constructions are equivalent to construction A with a suitable alphabet (for the code).

Construction D: Barnes-Wall

- 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 a Reed-Müller code (binary) 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

- 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 a Reed-Müller code (binary) 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

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

which can also be considered as a construction A on the ring $\mathscr{R} = \mathbb{F}_2 + u \cdot \mathbb{F}_2, u^2 = 0$ by using the linear code of generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & u & 0 & u \\ 0 & 0 & u & u \end{bmatrix}.$$

Part II

Coding for the Gaussian Channel

What are Lattice Codes? An example

Toy example: the $4-$QAM

A code with 4 codewords

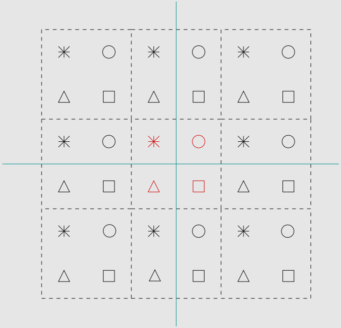


Figure: The 4 codewords are in red. Structure is $\mathbb{Z}^2/2\mathbb{Z}^2$.

What are Lattice Codes? An example

Toy example: the $4-$QAM

A code with 4 codewords

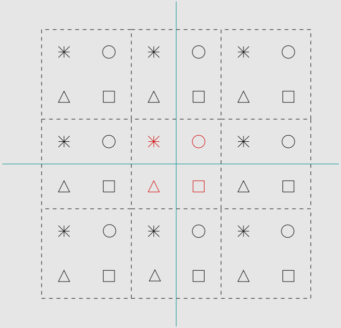


Figure: The 4 codewords are in red. Structure is $\mathbb{Z}^2/2\mathbb{Z}^2$.

- Centers of the squares are shifted points of a sublattice.

What are Lattice Codes? The general case

- Take a lattice Λ_c and a sublattice $\Lambda_s \subset \Lambda_c$ 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 the representative of $\boldsymbol{x}$ in Λ_c/Λ_s, of smallest Euclidean norm. $\boldsymbol{c}$ is a constant vector which ensures that the overall finite constellation has zero mean.

What are Lattice Codes? The general case

- Take a lattice Λ_c and a sublattice $\Lambda_s \subset \Lambda_c$ 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 the representative of $\boldsymbol{x}$ in Λ_c / Λ_s, of smallest Euclidean norm. $\boldsymbol{c}$ is a constant vector which ensures that the overall finite constellation has zero mean.

Lattice Codes

Lattice codes are the representatives of the quotient group Λ_c / Λ_s, with smallest Euclidean norm, shifted so that the overall constellation has zero mean.

What are Lattice Codes? The general case

- Take a lattice Λ_c and a sublattice $\Lambda_s \subset \Lambda_c$ 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 the representative of $\boldsymbol{x}$ in Λ_c/Λ_s, of smallest Euclidean norm. $\boldsymbol{c}$ is a constant vector which ensures that the overall finite constellation has zero mean.

Lattice Codes

Lattice codes are the representatives of the quotient group Λ_c/Λ_s, with smallest Euclidean norm, shifted so that the overall constellation has zero mean.

Performance of lattice codes

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

Coding: Minimum distance 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 minimum 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_0 is the power spectrum density of the noise.

Coding: Minimum distance 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 minimum 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_0 is the power spectrum density of the noise.

Minimum distance

We define the minimum distance of the lattice Λ as

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

Energetic considerations

- Communication engineers express error probability as a function of

$$\frac{E_b}{N_0}$$

  where E_b is the required energy to transmit one bit and N_0 is the power spectrum density of the noise.
- 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.

Energetic considerations

- Communication engineers express error probability as a function of

$$\frac{E_b}{N_0}$$

where E_b is the required energy to transmit one bit and N_0 is the power spectrum density of the noise.

- 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 and E_s the energy per symbol. Compare $\frac{d^2_{\min}}{E_s}$ of the lattice code with the one of $\alpha\mathbb{Z}^n$.

Energetic considerations

- Communication engineers express error probability as a function of

$$\frac{E_b}{N_0}$$

where E_b is the required energy to transmit one bit and N_0 is the power spectrum density of the noise.

- 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 and E_s the energy per symbol. Compare $\frac{d^2_{\min}}{E_s}$ of the lattice code with the one of $\alpha\mathbb{Z}^n$.

Fundamental Volume and coding gain

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

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

Coding Gain: Examples

Dimension 4

The checkerboard lattice D_4 has generator matrix

$$M_{D_4} = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

with $\det\left(M_{D_4}\right) = 2$ and $d_{\min}^2 = 2$. Coding gain is

$$\gamma_c(D_4) = \frac{d_{\min}^2}{\mathrm{vol}(D_4)^{\frac{1}{2}}} = \frac{2}{\sqrt{2}} = \sqrt{2}.$$

Coding Gain: Examples

Dimension 8

The Gosset lattice E_8 has generator matrix

$$M_{E_8} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{bmatrix}$$

with $\det\left(M_{E_8}\right) = 1$ and $d^2_{\min} = 2$. Coding gain is

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

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 0 of Λ_s. For high rates, we assume points of Λ_c uniformly distributed in the Voronoï region, so the energy per dimension of the lattice code becomes

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

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 0 of Λ_s. For high rates, we assume points of Λ_c uniformly distributed in the Voronoï region, so the energy per dimension of the lattice code becomes

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

Normalized Second Order Moment

The parameter

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

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 0 of Λ_s. For high rates, we assume points of Λ_c uniformly distributed in the Voronoï region, so the energy per dimension of the lattice code becomes

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

Normalized Second Order Moment

The parameter

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

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

Shaping Gain

The ratio

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

is called the shaping gain of Λ. Its value is upperbounded by the shaping gain of the $n-$dimensional sphere which tends to $\frac{\pi e}{6}$ 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

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

Part III

Nested Lattices and the Secrecy Gain

The Gaussian Wiretap Channel

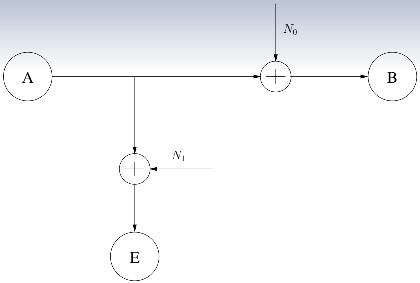


Figure: The Gaussian Wiretap Channel model

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

$+2 \bmod (4)$ 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 $1/2$.

Encoder Design

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

$+2 \bmod (4)$ 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

$$x = 2b_1 + b_0$$

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

$$x = 2b_1 + b_0$$

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.

Uniform Noise

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

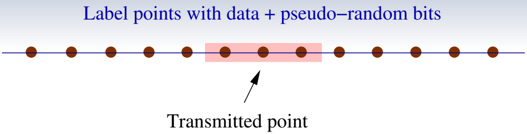


Figure: Constellation corrupted by uniform noise

Uniform Noise

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

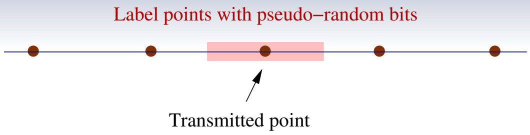


Figure: Points can be decoded **error free**: label with pseudo-random symbols

Uniform Noise

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

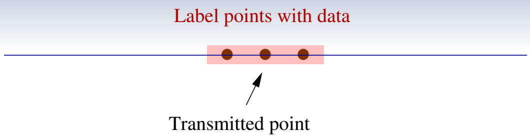


Figure: Points are **not distinguishable**: label with data

Uniform Noise

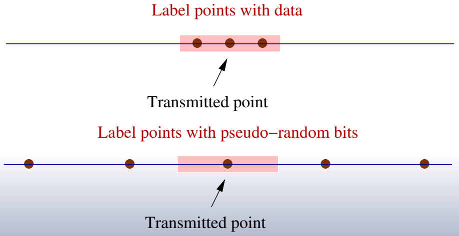


Figure: Constellation corrupted by uniform noise

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.

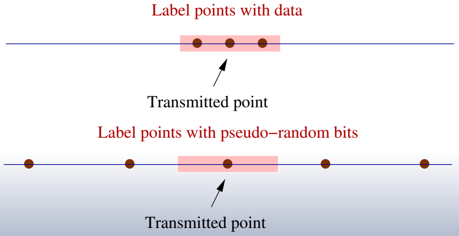


Figure: Constellation corrupted by uniform noise

Coset Coding with Integers

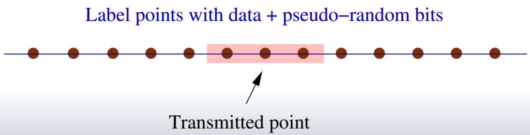


Figure: Constellation corrupted by uniform noise

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 $\mathbb{Z}/3\mathbb{Z}$”.

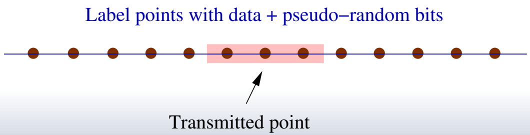


Figure: Constellation corrupted by uniform noise

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**).

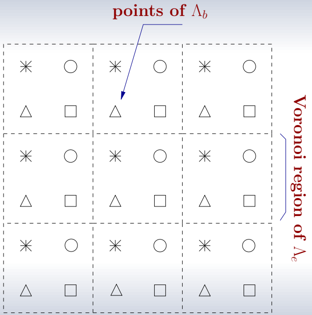


Figure: Example of coset coding

Part IV

The Secrecy Gain

Eve's Probability of Correct Decision (data)

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

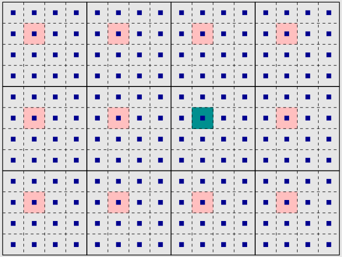


Figure: Eve correctly decodes when finding another coset representative

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

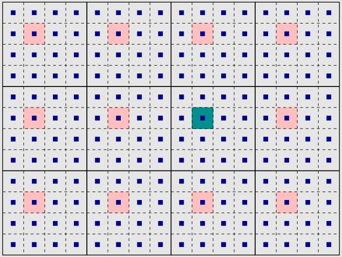


Figure: Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision

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

$$\simeq \left(\frac{1}{\sqrt{2\pi N_1}}\right)^n \mathrm{Vol}\left(\Lambda_b\right) \Theta_{\Lambda_e}\left(\frac{1}{2\pi N_1}\right)$$

where

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

is the theta series of Λ.

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

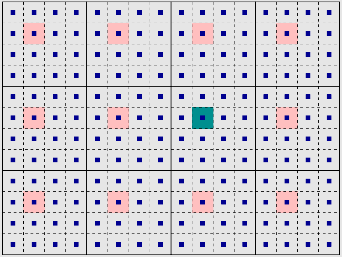


Figure: Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision

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

$$\simeq \left(\frac{1}{\sqrt{2\pi N_1}}\right)^n \mathrm{Vol}\left(\Lambda_b\right) \Theta_{\Lambda_e}\left(\frac{1}{2\pi N_1}\right)$$

where

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

is the theta series of Λ.

Problem

Minimize

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

for some y.

Secrecy function

Definition

Let Λ be a $n-$dimensional lattice with 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 $\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ (Jacobi theta function) and $y > 0$.

Secrecy function

Definition

Let Λ be a $n-$dimensional lattice with 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 $\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ (Jacobi theta function) and $y > 0$.

Examples

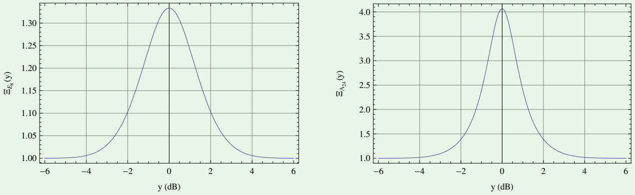


Figure: Secrecy functions of E_8 and Λ_{24}

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

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

Definition

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

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

Secrecy Gain

Definition

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

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

Definition

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

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

- 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),

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

First 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*

$$\chi_{\Lambda}^{s} \triangleq \Xi_{\Lambda}(1)$$

First 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

$$\chi_\Lambda^s \triangleq \Xi_\Lambda(1)$$

Calculation of E_8 secrecy gain

From E_8 theta series,

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

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

Asymptotic behavior for unimodular lattices

- Want to study the behavior of even unimodular lattices when $n \to \infty$.

Question

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

Asymptotic behavior for unimodular lattices

- Want to study the behavior of even unimodular lattices when $n \to \infty$.

Question

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

First answer

Apply the Siegel-Weil formula,

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

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

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

Asymptotic behavior (II)

Maximal Secrecy gain

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

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

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 $(k \to \infty)$.

Asymptotic behavior (II)

Maximal Secrecy gain

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

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

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

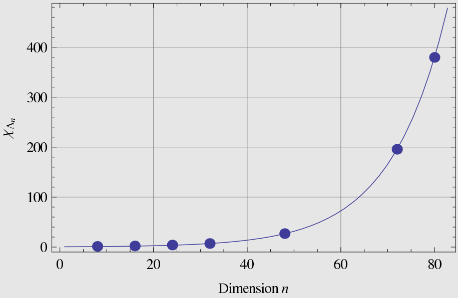


Figure: Lower bound of the minimal secrecy gain as a function of n from Siegel-Weil formula.

Part V

Wireless Channels - Other Lattices

Design Criterion

- Assume a wireless communication system transmitting on q subcarriers sufficiently spaced and during n channel uses.
- Assume Rayleigh fadings and 2 codewords $\boldsymbol{X}$ and $\boldsymbol{T}$ such that

$$\boldsymbol{X} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & & \ddots & \vdots \\ x_{q1} & x_{q2} & \cdots & x_{qn} \end{bmatrix} \quad \boldsymbol{T} = \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & & \ddots & \vdots \\ t_{q1} & t_{q2} & \cdots & t_{qn} \end{bmatrix}.$$

Design Criterion

- Assume a wireless communication system transmitting on q subcarriers sufficiently spaced and during n channel uses.
- Assume Rayleigh fadings and 2 codewords $\boldsymbol{X}$ and $\boldsymbol{T}$ such that

$$\boldsymbol{X} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & & \ddots & \vdots \\ x_{q1} & x_{q2} & \cdots & x_{qn} \end{bmatrix} \quad \boldsymbol{T} = \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & & \ddots & \vdots \\ t_{q1} & t_{q2} & \cdots & t_{qn} \end{bmatrix}.$$

Pairwise Error Probability

Error probability will be dominated by

$$\max_{\boldsymbol{X},\boldsymbol{T}} P(\boldsymbol{X} \to \boldsymbol{T}) \cong \max_{\boldsymbol{X},\boldsymbol{T}} \prod_{i=1}^{q} \left\| \boldsymbol{x}_i - \boldsymbol{t}_i \right\|^{-2} \left(\frac{\Gamma}{4} \right)^{-n}$$

where Γ is the average signal to noise ratio and $\boldsymbol{x}_i$ (resp. $\boldsymbol{t}_i$) is the i^{th} row of $\boldsymbol{X}$ (resp. $\boldsymbol{T}$). This equality is valid if, for any i, $\boldsymbol{x}_i \neq \boldsymbol{t}_i$. Hence, one has to find a code which maximizes

$$\min_{\boldsymbol{X},\boldsymbol{T}} \mu(\boldsymbol{X},\boldsymbol{T}) = \min_{\boldsymbol{X},\boldsymbol{T}} \prod_{i=1}^{q} \left\| \boldsymbol{x}_i - \boldsymbol{t}_i \right\|^{2}$$

Lattice formulation over number fields

Control the product in $\mu(X, T)$

The product $\prod_{i=1}^{q} \|\boldsymbol{x}_i - \boldsymbol{t}_i\|^2$ which becomes $\mu(\boldsymbol{X}) = \prod_{i=1}^{q} \|\boldsymbol{x}_i\|^2$ by linearity can be controled by introducing the algebraic norm in a well-chosen algebraic Galois extension $\mathbb{K}$ of degree q.

- Let $(\sigma_1, \sigma_2, \ldots, \sigma_q)$ be the Galois group of $\mathbb{K}$. Use the canonical embedding so that

$$\boldsymbol{X} = \begin{bmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_n) \\ \vdots & & \ddots & \vdots \\ \sigma_q(x_1) & \sigma_q(x_2) & \cdots & \sigma_q(x_n) \end{bmatrix}$$

Lattice formulation over number fields

Control the product in $\mu(X, T)$

The product $\prod_{i=1}^{q} \|\boldsymbol{x}_i - \boldsymbol{t}_i\|^2$ which becomes $\mu(\boldsymbol{X}) = \prod_{i=1}^{q} \|\boldsymbol{x}_i\|^2$ by linearity can be controled by introducing the algebraic norm in a well-chosen algebraic Galois extension $\mathbb{K}$ of degree q.

- Let $(\sigma_1, \sigma_2, \ldots, \sigma_q)$ be the Galois group of $\mathbb{K}$. Use the canonical embedding so that

$$\boldsymbol{X} = \begin{bmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_n) \\ \vdots & & \ddots & \vdots \\ \sigma_q(x_1) & \sigma_q(x_2) & \cdots & \sigma_q(x_n) \end{bmatrix}$$

Metric and Norm

Then metric $\mu(\boldsymbol{X})$ can be written as

$$\mu(\boldsymbol{X}) = N\left(\|\boldsymbol{x}\|^2\right) = N\left(\sum_{i=1}^{n} x_i^2\right)$$

where N is for the algebraic norm and $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$.

Construction of $\mathcal{O}_{\mathbb{K}}$ –lattices

- A construction A for $\mathcal{O}_{\mathbb{K}}$ –lattices where $\mathcal{O}_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$ can be given where a $\mathcal{O}_{\mathbb{K}}$ –lattice is a $\mathcal{O}_{\mathbb{K}}$ –module.

Construction of $\mathscr{O}_{\mathbb{K}}$ −lattices

- A construction A for $\mathscr{O}_{\mathbb{K}}$ −lattices where $\mathscr{O}_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$ can be given where a $\mathscr{O}_{\mathbb{K}}$ −lattice is a $\mathscr{O}_{\mathbb{K}}$ −module.

Construction A (binary) over $\mathscr{O}_{\mathbb{K}}$

Take, for instance $q = 2$, $\mathbb{K} = \mathbb{Q}\left(\sqrt{2}\right)$. So, we have $\mathscr{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$. Consider the principal ideal

$$\mathscr{I} = \sqrt{2} \cdot \mathbb{Z}[\sqrt{2}].$$

As $N(\mathscr{I}) = 2$, then $\mathbb{Z}[\sqrt{2}] / \mathscr{I} = \mathbb{F}_2$. So, we can construct $\mathscr{O}_{\mathbb{K}}$ −lattices in that way,

$$\Lambda = \mathscr{I}^n + \mathscr{C}$$

where $\mathscr{C}$ is a binary linear code of length n.

Construction of $\mathcal{O}_{\mathbb{K}}$ −lattices

- A construction A for $\mathcal{O}_{\mathbb{K}}$ −lattices where $\mathcal{O}_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$ can be given where a $\mathcal{O}_{\mathbb{K}}$ −lattice is a $\mathcal{O}_{\mathbb{K}}$ −module.

Construction A (binary) over $\mathcal{O}_{\mathbb{K}}$

Take, for instance $q = 2$, $\mathbb{K} = \mathbb{Q}\left(\sqrt{2}\right)$. So, we have $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$. Consider the principal ideal

$$\mathcal{I} = \sqrt{2} \cdot \mathbb{Z}[\sqrt{2}].$$

As $N(\mathcal{I}) = 2$, then $\mathbb{Z}[\sqrt{2}] / \mathcal{I} = \mathbb{F}_2$. So, we can construct $\mathcal{O}_{\mathbb{K}}$ −lattices in that way,

$$\Lambda = \mathcal{I}^n + \mathcal{C}$$

where $\mathcal{C}$ is a binary linear code of length n.

Construction A (quaternary) over $\mathcal{O}_{\mathbb{K}}$

Here, take $q = 2$, $\mathbb{K} = \mathbb{Q}\left(\sqrt{5}\right)$. So, we have $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\phi]$ where $\phi = \frac{1+\sqrt{5}}{2}$. Consider the ideal $\mathcal{I} = 2 \cdot \mathbb{Z}[\sqrt{\phi}]$. As $N(\mathcal{I}) = 4$ and $\mathcal{I}$ is prime, then $\mathbb{Z}[\sqrt{\phi}] / \mathcal{I} = \mathbb{F}_4$. So, we have

$$\Lambda = \mathcal{I}^n + \mathcal{C}$$

where $\mathcal{C}$ is a linear code of length n over $\mathbb{F}_4$.

Perspectives

- $\mathcal{O}$–lattices where $\mathcal{O}$ is a maximal order of some division algebra for the MIMO case
- Nested lattices for other applications in which 2 or more data streams must be constructed
  - Han and Kobayashi
  - Wyner-Ziv
  - ...
- Nested "exotic" lattices on other Dedekind domains?

Thank You !!