In(Wireless)-Network Computation

Computing with Lattices

Jean-Claude Belfiore

Telecom ParisTech
February, 5 2013
First European Training School in Network Coding

Universitat Autònoma de Barcelona

Part I

Introduction

Outline

Computing in a network

Distributed computation through a wireless network

- **Wireless Sensor Networks :** Applications to industrial automation and monitoring, agriculture, health, safety ...
- **Large Scale Distributed Computer :** Use the resources of mobile devices for distributed computation or storage.

Computing in a network

Distributed computation through a wireless network

- **Wireless Sensor Networks :** Applications to industrial automation and monitoring, agriculture, health, safety ...
- **Large Scale Distributed Computer :** Use the resources of mobile devices for distributed computation or storage.

Computing, Networking, Physical processing

Unfortunately, in wireless networks, resource is scarce and separation theorems may not apply. We are not interested in decoding all messages sent. We are interested in the result of computation.

Computing in a network

Distributed computation through a wireless network

- **Wireless Sensor Networks :** Applications to industrial automation and monitoring, agriculture, health, safety ...
- **Large Scale Distributed Computer :** Use the resources of mobile devices for distributed computation or storage.

Computing, Networking, Physical processing

Unfortunately, in wireless networks, resource is scarce and separation theorems may not apply. We are not interested in decoding all messages sent. We are interested in the result of computation.

Convergence of Computation and Communication

In a multi-user environment, we can use the broadcast and superposition properties of the wireless channel, seen as a **natural computer**.

Algebraic Objects for Computation

Finite structures for computations

Computation of multivariate polynomials over finite fields or rings yield a huge variety of functions. For instance, if we want to compute a function of pairs of bits, compute polynomials over any ring among the 4 ones of cardinality 4.

Ring
$\mathbb{F}_4$
$\mathbb{F}_2^2$
$\mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0$
$\mathbb{Z}_4$

Table: Rings of cardinality 4

Algebraic Objects for Computation

Finite structures for computations

Computation of multivariate polynomials over finite fields or rings yield a huge variety of functions. For instance, if we want to compute a function of pairs of bits, compute polynomials over any ring among the 4 ones of cardinality 4.

Ring
$\mathbb{F}_4$
$\mathbb{F}_2^2$
$\mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0$
$\mathbb{Z}_4$

Table: Rings of cardinality 4

Signal Space for the Physical Layer ⟶ Ideal Lattices

Codes used on the physical layer should

- be able to achieve the capacity of channels impaired by Gaussian noise.
- be endowed with an algebraic structure related to those finite rings through a ring morphism.

Part II

Lattices

Outline

Maybe you unconsciously use lattices ...

Maybe you unconsciously use lattices ...

What a lattice element could be

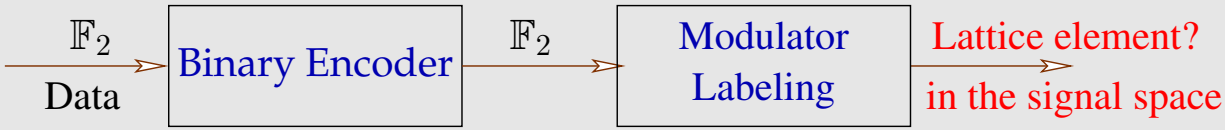


Figure: Encoder and Modulator

Maybe you unconsciously use lattices ...

What a lattice element could be

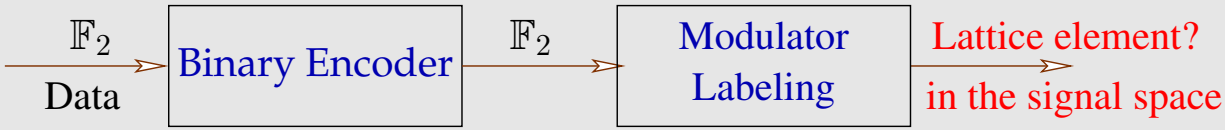


Figure: Encoder and Modulator

Requirements

- Encoder must be **linear**
- Modulation should be **PAM**, **QAM** or **HEX**
- **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

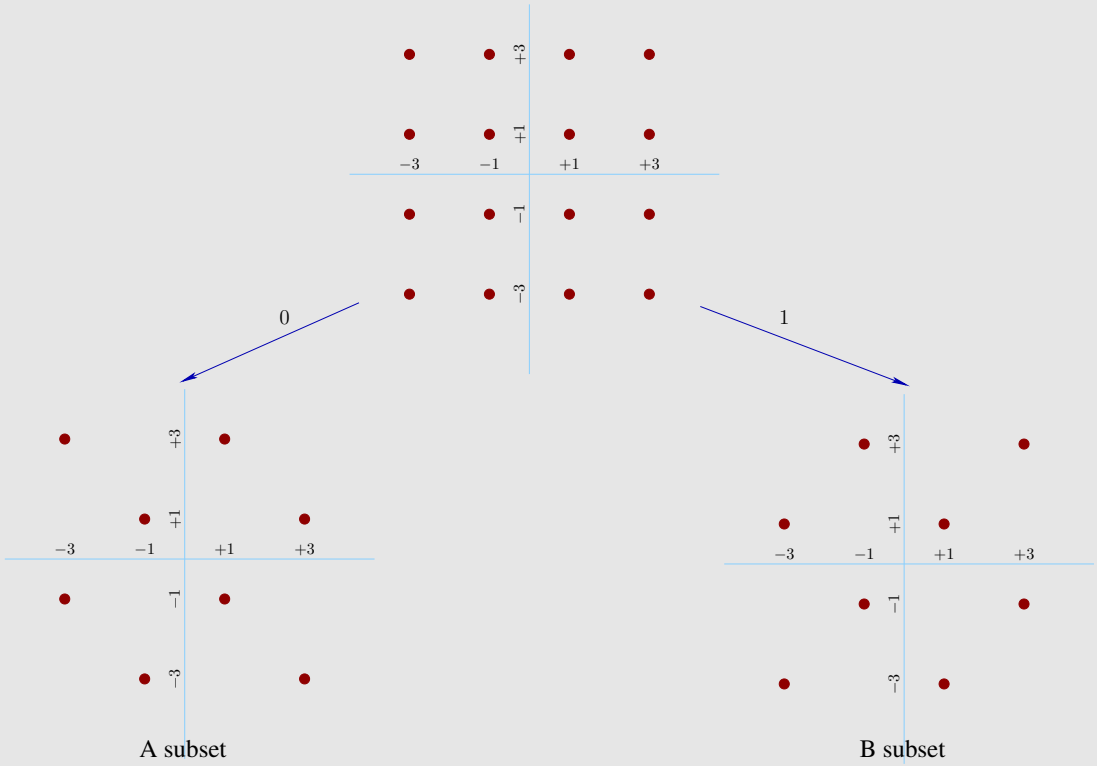


Figure: Labeling of subsets A and B

An example: the D_4 lattice (coding)

Encoder

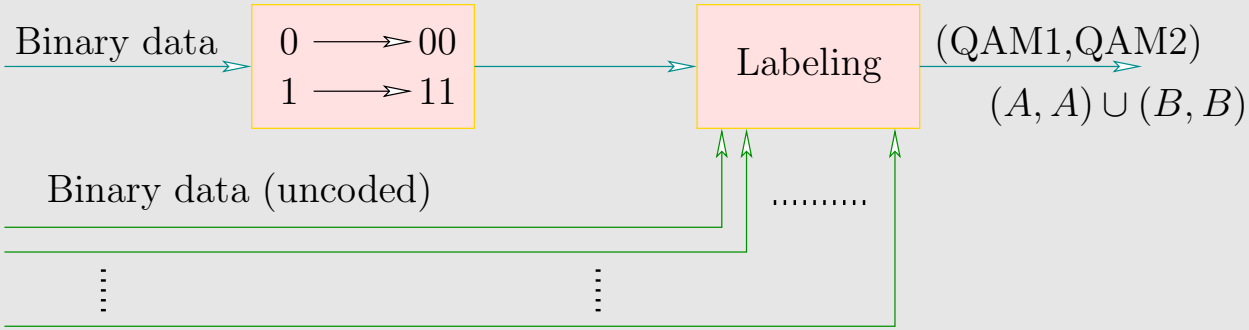


Figure: D_4 encoder

An example: the D_4 lattice (coding)

Encoder

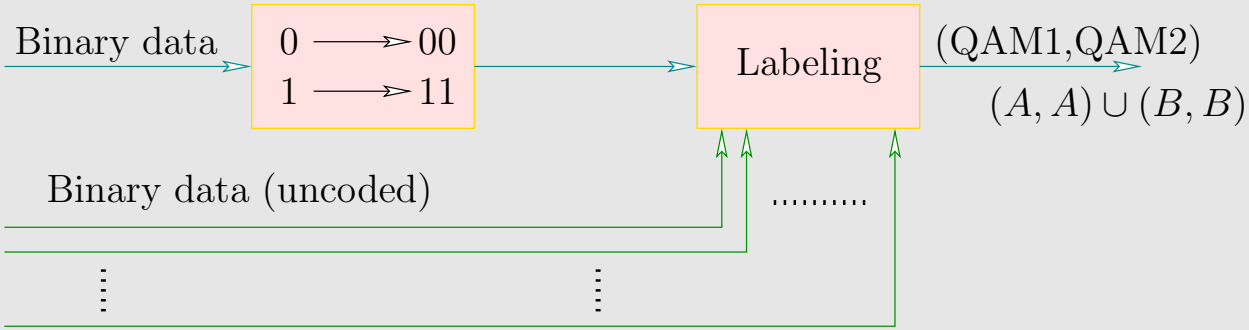


Figure: D_4 encoder

- 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

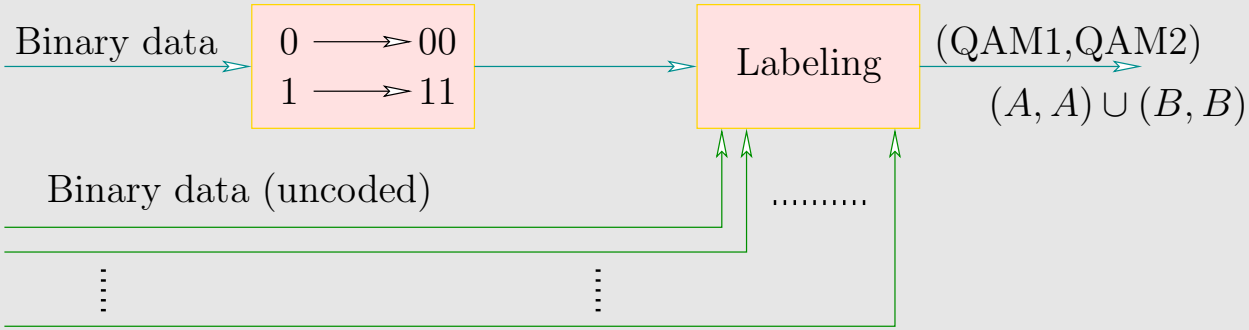


Figure: D_4 encoder

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

One of the simplest examples of "Construction A"

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

Outline

Definition

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

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.

Lattice points

- An element $\boldsymbol{v}$ of $\boldsymbol{\Lambda}$ can be written as :

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

  where $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ is a basis of $\mathbb{R}^n$.

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

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

  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 : Geometric properties

- The generator matrix $\boldsymbol{M}$ describes the lattice $\Lambda_{\boldsymbol{M}}$, but it is not unique. All matrices $\boldsymbol{M} \cdot \boldsymbol{T}$ where $\boldsymbol{T}$ has **integer** entries 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 .

Lattices : Geometric properties

- The generator matrix $\boldsymbol{M}$ describes the lattice $\Lambda_{\boldsymbol{M}}$, but it is not unique. All matrices $\boldsymbol{M} \cdot \boldsymbol{T}$ where $\boldsymbol{T}$ has **integer** entries 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 .

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 $\mathrm{Vol}\left(\Lambda_{\boldsymbol{M}}\right)$.
- 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 : Geometric properties

- The generator matrix $\boldsymbol{M}$ describes the lattice $\Lambda_{\boldsymbol{M}}$, but it is not unique. All matrices $\boldsymbol{M} \cdot \boldsymbol{T}$ where $\boldsymbol{T}$ has **integer** entries 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 .

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

- A **bad** basis is a basis with long vectors (large orthogonality defect).
- A **good** basis (or **reduced** basis) is a basis with short vectors (small orthogonality defect).

Lattices : Geometric properties (cont.)

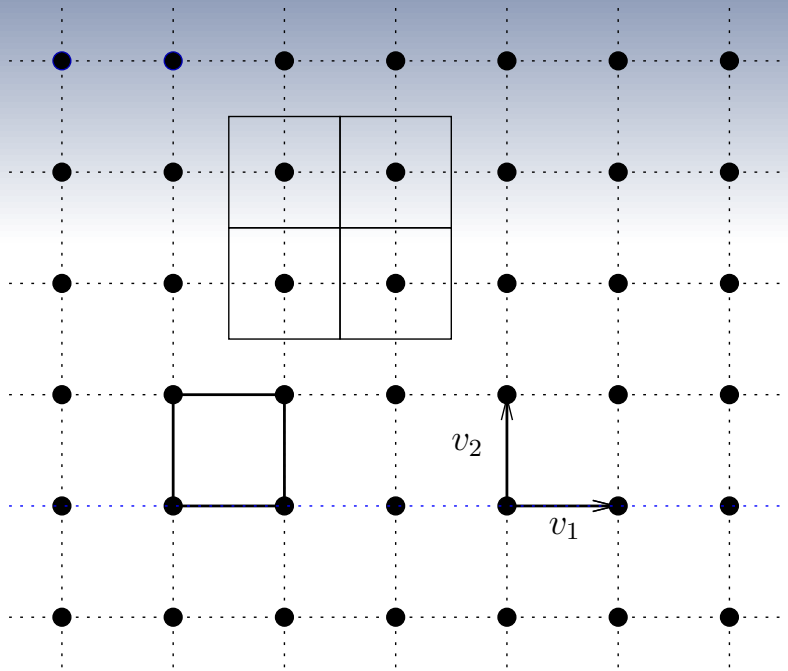
Definition

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

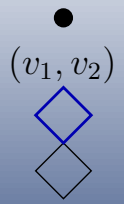
$$\mathcal{V}_\Lambda(\boldsymbol{u}) = \left\{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}-\boldsymbol{u}\| \leq \left\|\boldsymbol{x}-\boldsymbol{y}\right\|, \quad \boldsymbol{y} \in \Lambda\right\}$$

- 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.

$\mathbb{Z}^2$ lattice



$\mathbb{Z}^2$ lattice



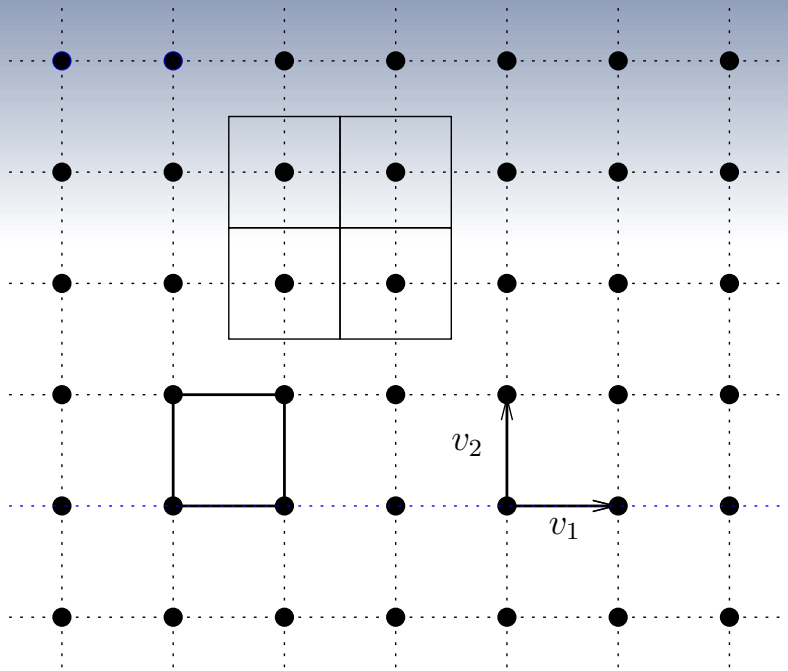
Lattice Point

Lattice Basis

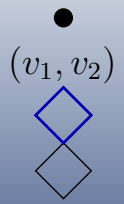
Fundamental Parallelotope

Voronoi region

$\mathbb{Z}^2$ lattice



$\mathbb{Z}^2$ lattice



Lattice Point

Lattice Basis

Fundamental Parallelotope

Voronoi region

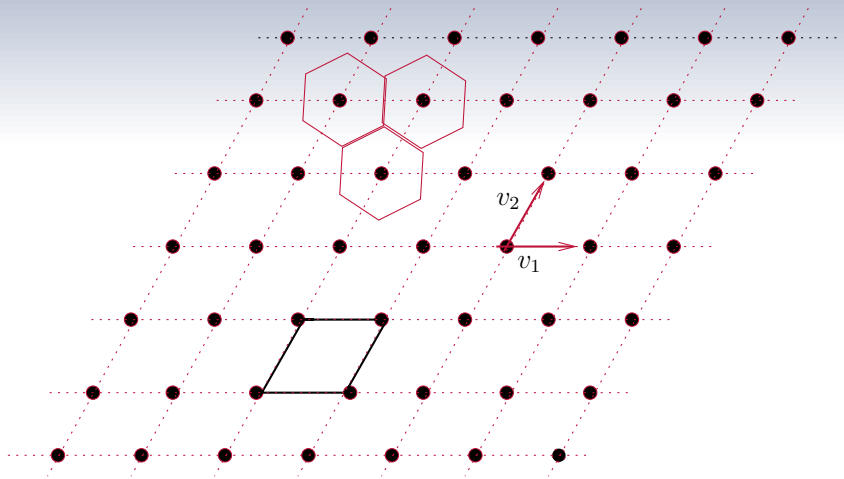
Properties

- Generator matrix is

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

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

A_2 lattice



The A_2 lattice

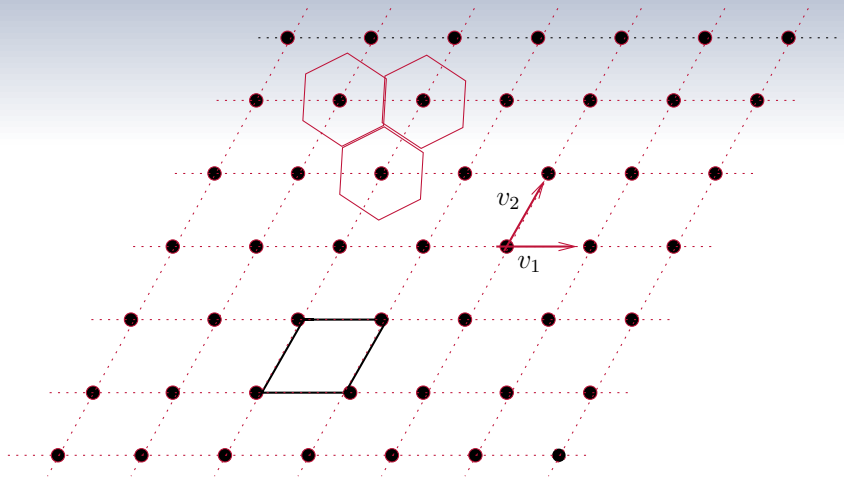
Lattice point

(v_1, v_2) Lattice basis

Fundamental parallelotope

Voronoi region

A_2 lattice



The A_2 lattice

Lattice point

Lattice basis

Fundamental parallelotope

Voronoi region

Properties

- Generator matrix is

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

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

Outline


CONSTRUCTION A
KEEP OUT
Sell
Sellen

Construction A

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

Let q be an integer. Then,

$$\mathbb{Z}/q\mathbb{Z} \quad (\text{integers mod } q)$$

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 for a $\mathbb{Z}-$lattice

Let q be an integer. Then,

$$\mathbb{Z}/q\mathbb{Z} \quad (\text{integers mod } q)$$

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

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

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

Construction A

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

Let q be an integer. Then,

$$\mathbb{Z}/q\mathbb{Z} \quad (\text{integers mod } q)$$

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

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

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

Construction of E_8

E_8 is obtained as

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

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

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

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

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

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.

Outline

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

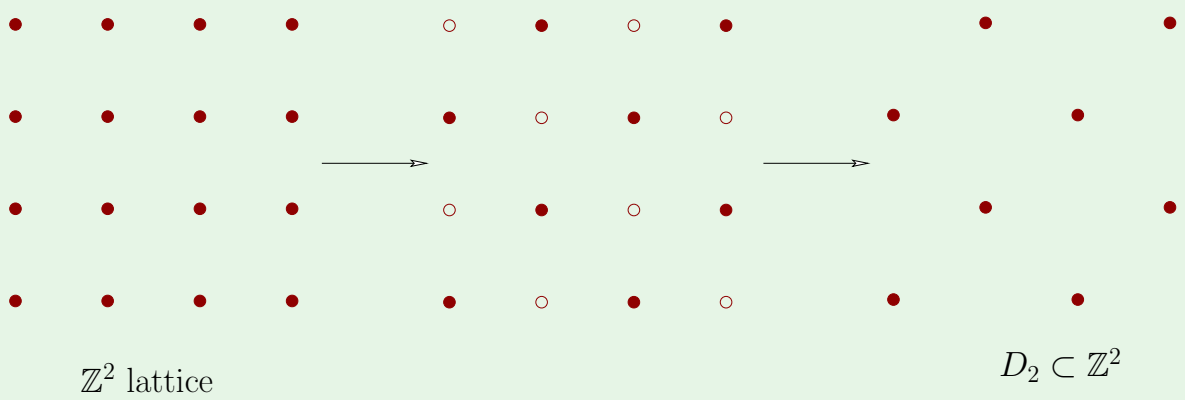


Figure: D_2 as a sublattice of $\mathbb{Z}^2$. Index is 2.

Construction *A*

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

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,

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

Part III

Lattice Codes for the AWGN channel

Outline

What are Lattice Codes? An example

Toy example: the 4−QAM

A code with 4 codewords

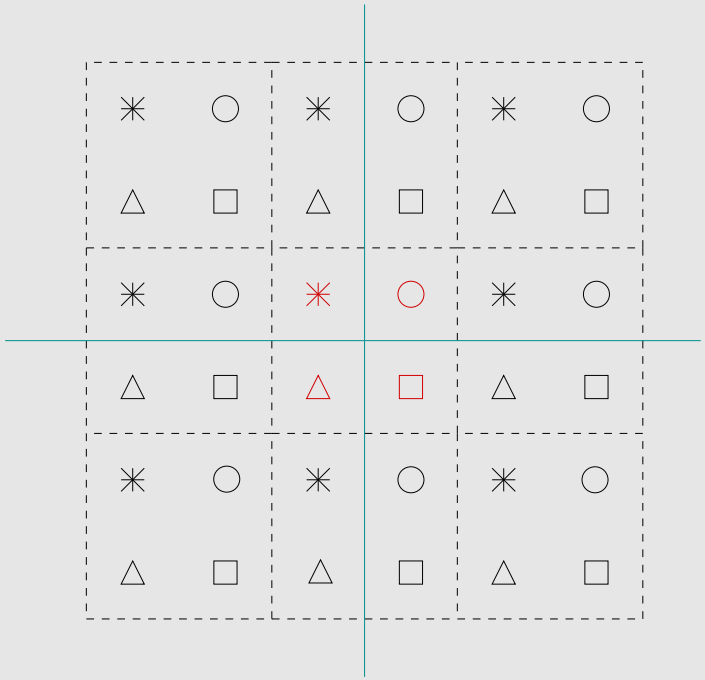


Figure: The 4 codewords are in red. Structure is $\mathbb{Z}^2/2\mathbb{Z}^2$.

What are Lattice Codes? An example

Toy example: the 4−QAM

A code with 4 codewords

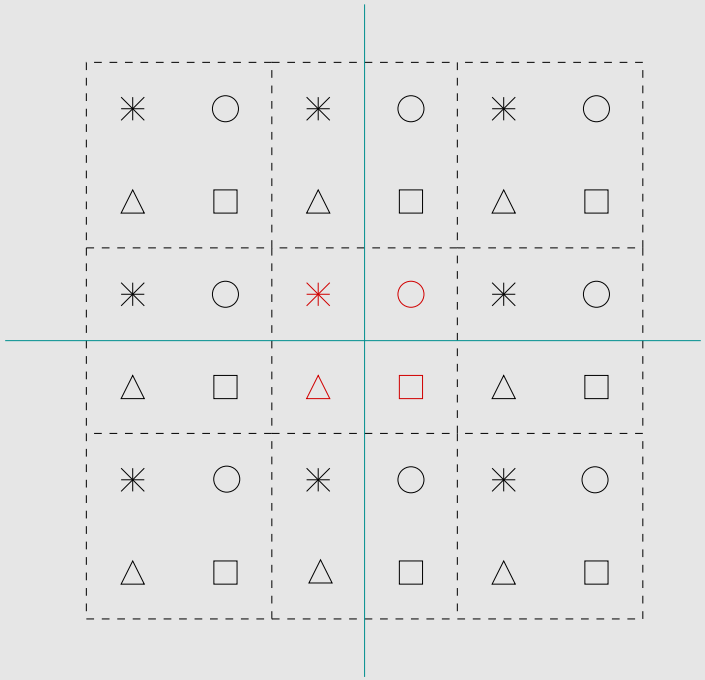


Figure: The 4 codewords are in red. Structure is $\mathbb{Z}^2/2\mathbb{Z}^2$.

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

What are Lattice Codes? 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 the representative of $\boldsymbol{x}$ in Λ_c/Λ_s, of smallest length (comparable to an integer Euclidean division). $\boldsymbol{c}$ is a constant vector which ensures that the overall finite 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 the representative of $\boldsymbol{x}$ in Λ_c/Λ_s, of smallest length (comparable to an integer Euclidean division). $\boldsymbol{c}$ is a constant vector which ensures that the overall finite constellation has zero mean.

Lattice Codes

Lattice codes 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 the representative of $\boldsymbol{x}$ in Λ_c/Λ_s, of smallest length (comparable to an integer Euclidean division). $\boldsymbol{c}$ is a constant vector which ensures that the overall finite constellation has zero mean.

Lattice Codes

Lattice codes are the representatives of Λ_c/Λ_s, with smallest length, 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 $\mathbb{Z}^n/2^{\frac{m}{2}}\mathbb{Z}^n$ (m even). 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 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 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 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 distance 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 and E_s the energy per symbol. Compare $\frac{d^2_{\min}}{E_s}$ of the lattice code with the one of $\alpha\mathbb{Z}^n$.

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 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

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

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

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

Coding Gain: Examples

Dimension 8

The Gosset lattice E_8 has generator matrix

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

with $\det\left(\boldsymbol{M}_{E_8}\right) = 1$ and $d^2_{\min} = 2$. 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 Λ_s. Energy per dimension

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

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

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

Normalized Second Order Moment

The parameter

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

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

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

Normalized Second Order Moment

The parameter

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

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

Shaping Gain

The ratio

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

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

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

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

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

Theta series

A third figure of merit for a lattice is its **theta series**

$$\Theta_\Lambda(q)=\sum_{\boldsymbol{x}\in\Lambda} q^{\|\boldsymbol{x}\|^2}$$

which is a key design parameter for the wiretap channel.

Outline

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

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

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.

Good lattices

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

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

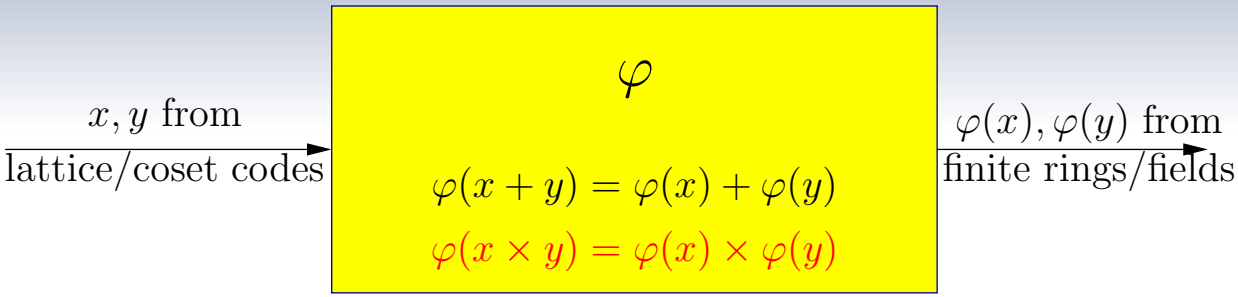
for any value of $P_e > 0$ by using construction A over big alphabets $\mathbb{Z}/p\mathbb{Z}$, p prime.

Part IV

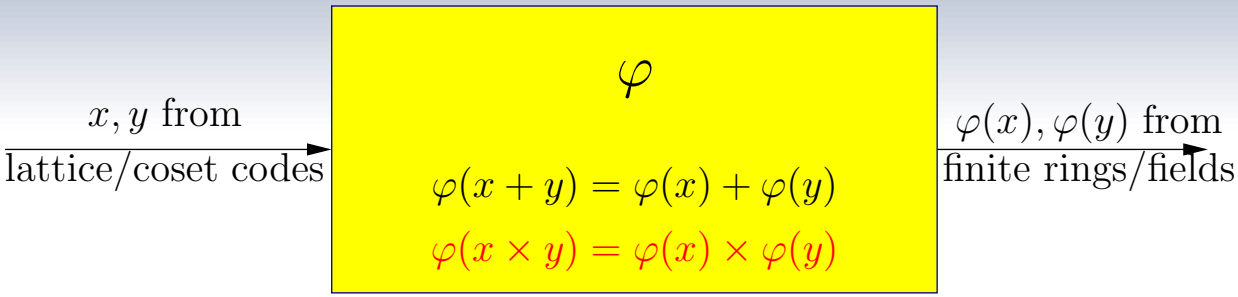
Linear Computing

Outline

From packets to signal space



From packets to signal space



Homomorphic code

Labelling from finite ring $\mathscr{R}$ to the PHY code should be transparent to any function defined on $\mathscr{R}$. We are interested here in **polynomial** functions.

- Additive group morphism is natural due to the lattice structure
- What about ring morphism?

Outline

Introduction

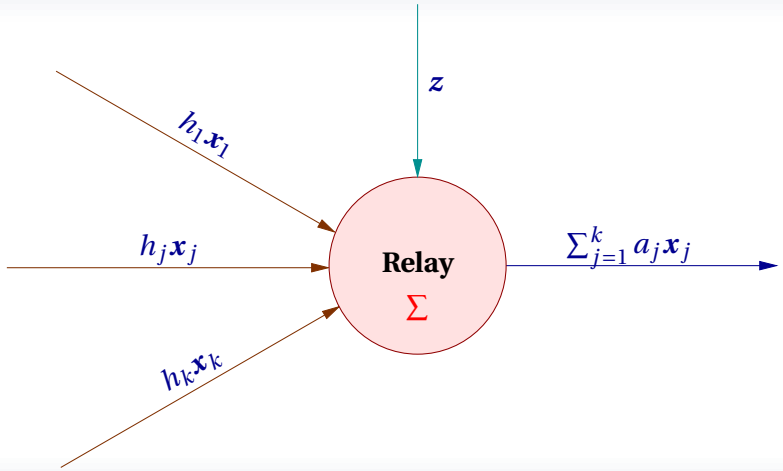
- **[Zhang et al. 06]** introduced the **Physical-layer Network Coding** concept in order to turn the broadcast property of the wireless channel into a capacity boosting advantage. Instead of considering the interference as a nuisance, each relay converts an interfering signal into a combination of simultaneously transmitted codewords.

Introduction

- **[Zhang et al. 06]** introduced the **Physical-layer Network Coding** concept in order to turn the broadcast property of the wireless channel into a capacity boosting advantage. Instead of considering the interference as a nuisance, each relay converts an interfering signal into a combination of simultaneously transmitted codewords.

- **[Nazer & Gastpar 09]** proposes a new scheme. The proposed strategy, called **Compute-and-Forward**, exploits interference to obtain higher end-to-end transmission rates between users in a network. The relays are required to decode noiseless **linear equations** of the transmitted messages using the noisy linear combination provided by the channel. The destination, given enough linear combinations, can solve the linear system for its desired messages.

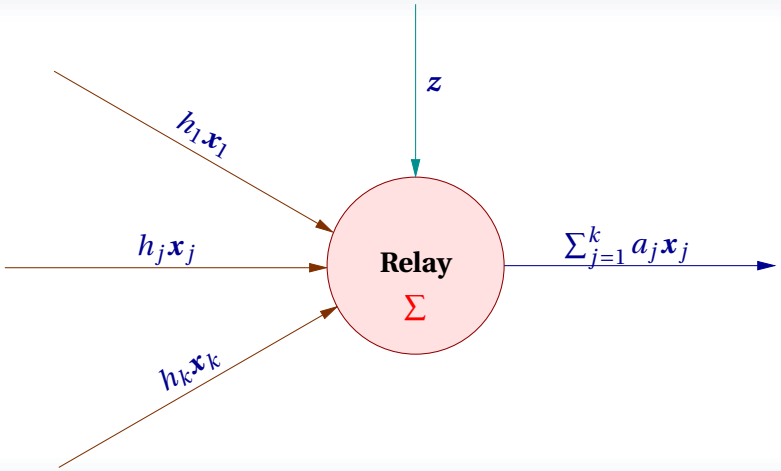
Principles [Nazer & Gastpar 09]



Principles [Nazer & Gastpar 09]

Relay

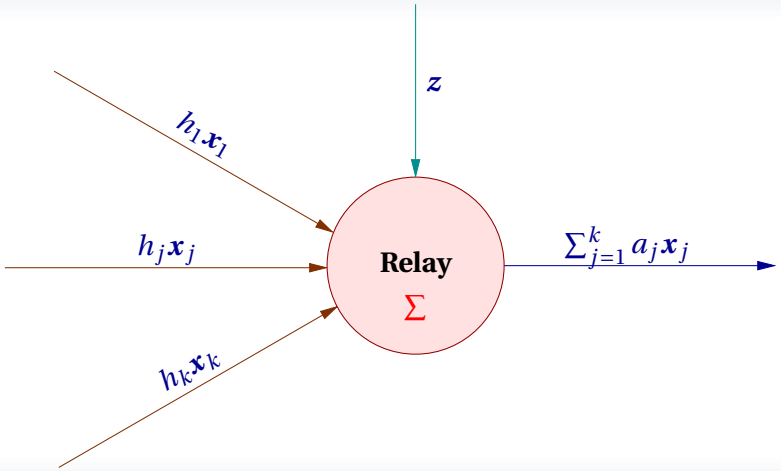
The Relay wants to reliably decode the result of computation $\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j$, $a_j \in \mathbb{Z}$. If $\boldsymbol{x}_j$ are lattice points of some integer lattice, then $\boldsymbol{\lambda}$ is also a lattice point for some lattice.



Principles [Nazer & Gastpar 09]

Relay

The Relay wants to reliably decode the result of computation $\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j$, $a_j \in \mathbb{Z}$. If $\boldsymbol{x}_j$ are lattice points of some integer lattice, then $\boldsymbol{\lambda}$ is also a lattice point for some lattice.



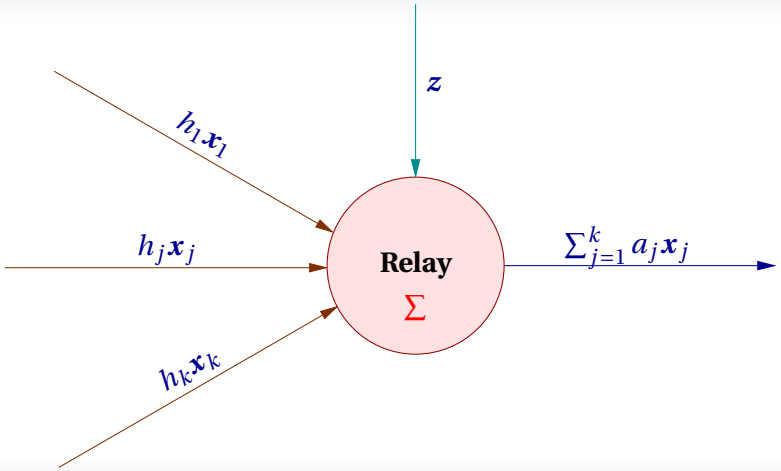
Received signal

Received signal is $\boxed{\boldsymbol{y} = \sum_{j=1}^{k} h_j \boldsymbol{x}_j + \boldsymbol{z}}$ where $\boldsymbol{x}_j \in \Lambda_j \subseteq \mathbb{Z}^n$ are $\mathbb{Z}-$lattice points, $h_j \in \mathbb{C}$ and $\boldsymbol{z}$ iid Gaussian noise. **Note that** $a_j \in \mathbb{Z}$.

Principles [Nazer & Gastpar 09]

Relay

The Relay wants to reliably decode the result of computation $\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j$, $a_j \in \mathbb{Z}$. If $\boldsymbol{x}_j$ are lattice points of some integer lattice, then $\boldsymbol{\lambda}$ is also a lattice point for some lattice.



Received signal

Received signal is $\boxed{\boldsymbol{y} = \sum_{j=1}^{k} h_j \boldsymbol{x}_j + \boldsymbol{z}}$ where $\boldsymbol{x}_j \in \Lambda_j \subseteq \mathbb{Z}^n$ are $\mathbb{Z}-$lattice points, $h_j \in \mathbb{C}$ and $\boldsymbol{z}$ iid Gaussian noise. **Note that** $a_j \in \mathbb{Z}$.

Goal

Be able to compute $\boldsymbol{\lambda}$ reliably.

Computation Rate

Computation Rate

The computation rate defined in **[Nazer & Gastpar 09]** is

$$R_{\text{comp}}(\boldsymbol{h},\boldsymbol{a}) = \log_2\left(\left(\|\boldsymbol{a}\|^2 - \frac{\text{SNR}\left|\boldsymbol{h}^\dagger\boldsymbol{a}\right|^2}{1+\text{SNR}\,\|\boldsymbol{h}\|^2}\right)^{-1}\right)$$

and is achievable by using **nested lattice codes** for $\boldsymbol{x}_i$. The decoded equation is also a **lattice** point.

Limitations for Computation

Lattices as $\mathbb{Z}-$modules

We only have a morphism of modules between the lattice code used (Λ_c/Λ_s) to achieve computation rate and the code on the finite ring $\mathscr{R}$ onto which we wish to compute.

- Only **linear computations** can be done.
- In the finite ring world, we obtain **linear codes** over $\mathscr{R}$ and the only computations that can be done are sums of codewords and multiplications by elements of the finite ring.

Limitations for Computation

Lattices as $\mathbb{Z}-$modules

We only have a morphism of modules between the lattice code used (Λ_c/Λ_s) to achieve computation rate and the code on the finite ring $\mathscr{R}$ onto which we wish to compute.

- Only **linear computations** can be done.
- In the finite ring world, we obtain **linear codes** over $\mathscr{R}$ and the only computations that can be done are sums of codewords and multiplications by elements of the finite ring.

Example

Choose $\Lambda_c = D_4$ and $\Lambda_s = 2D_4$ for all inputs. From

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

we obtain

$$D_4/2D_4 = 2(4,1,1)^{\dagger}_{\mathbb{F}_2} + (4,3,2)_{\mathbb{F}_2}$$

which can be seen as a linear code over $\mathbb{Z}_4$.

Limitations for Computation

Lattices as $\mathbb{Z}-$modules

We only have a morphism of modules between the lattice code used (Λ_c/Λ_s) to achieve computation rate and the code on the finite ring $\mathscr{R}$ onto which we wish to compute.

- Only **linear computations** can be done.
- In the finite ring world, we obtain **linear codes** over $\mathscr{R}$ and the only computations that can be done are sums of codewords and multiplications by elements of the finite ring.

Example

Choose $\Lambda_c = D_4$ and $\Lambda_s = 2D_4$ for all inputs. From

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

we obtain

$$D_4/2D_4 = 2(4,1,1)^{\dagger}_{\mathbb{F}_2} + (4,3,2)_{\mathbb{F}_2}$$

which can be seen as a linear code over $\mathbb{Z}_4$.

Polynomial Codes

How to get the **multiplicative** structure? (the code becomes a ring or an ideal) Use polynomial codes like cyclic codes. Do the same with lattices.

Part V

Computation of a function with lattices

Outline

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

Number fields

Base field

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

1. $\mathbb{F} = \mathbb{Q}$. $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.
2. $\mathbb{F} = \mathbb{Q}(i)$ with $\mathbb{Q}(i) = \{x + iy,\ x, y \in \mathbb{Q}\}$; $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$.
3. $\mathbb{F} = \mathbb{Q}(\omega)$ with $\mathbb{Q}(\omega) = \{x + \omega y,\ x, y \in \mathbb{Q}\}$; $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$. 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 $\mathbb{F}$.

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 $\mathbb{Q}(i) = \{x + iy,\ x, y \in \mathbb{Q}\}$; $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$.
3. $\mathbb{F} = \mathbb{Q}(\omega)$ with $\mathbb{Q}(\omega) = \{x + \omega y,\ x, y \in \mathbb{Q}\}$; $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$. 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: $\mathbb{Q}(\sqrt{5})$

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 $a_i \in \mathcal{O}_{\mathbb{F}}$. We denote this ring $\mathcal{O}_{\mathbb{K}}$.

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.) $\mathbb{Q}(\sqrt{5})$

$\sqrt{5}$ 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 $\mathbb{Q}(\sqrt{5})$ 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 $\mathcal{O}_{\mathbb{K}}$.

Principal Ideal

Definition

Let $\alpha \in \mathcal{O}_{\mathbb{F}}$. The set of of all integer multiples of α is a principal ideal of $\mathcal{O}_{\mathbb{F}}$. We denote it (α) or $\alpha \cdot \mathcal{O}_{\mathbb{F}}$ or $\mathcal{I}_{\alpha}$.

Principal Ideal

Definition

Let $\alpha \in \mathcal{O}_{\mathbb{F}}$. The set of of all integer multiples of α is a principal ideal of $\mathcal{O}_{\mathbb{F}}$. We denote it (α) or $\alpha \cdot \mathcal{O}_{\mathbb{F}}$ or $\mathcal{I}_{\alpha}$.

Example

In $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, the ring of integers is $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. We have $\frac{1+\sqrt{5}}{2} \notin \sqrt{5} \cdot \mathcal{O}_{\mathbb{K}}$ but $5 \in \sqrt{5} \cdot \mathcal{O}_{\mathbb{K}}$ as $5 = \sqrt{5} \cdot \sqrt{5}$.

Principal Ideal

Definition

Let $\alpha \in \mathcal{O}_{\mathbb{F}}$. The set of of all integer multiples of α is a principal ideal of $\mathcal{O}_{\mathbb{F}}$. We denote it (α) or $\alpha \cdot \mathcal{O}_{\mathbb{F}}$ or $\mathcal{I}_{\alpha}$.

Example

In $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, the ring of integers is $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. We have $\frac{1+\sqrt{5}}{2} \notin \sqrt{5} \cdot \mathcal{O}_{\mathbb{K}}$ but $5 \in \sqrt{5} \cdot \mathcal{O}_{\mathbb{K}}$ as $5 = \sqrt{5} \cdot \sqrt{5}$.

Why ideals ?

Ideals will be the key tool to construct lattices endowed with a multiplication.

The Galois group

- Elements of $\mathbb{K}$ have conjugates (the roots of their minimal polynomial)

The Galois group

- Elements of $\mathbb{K}$ have conjugates (the roots of their minimal polynomial)

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

- Elements of $\mathbb{K}$ have conjugates (the roots of their minimal polynomial)

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

- Elements of $\mathbb{K}$ have conjugates (the roots of their minimal polynomial)

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** $x = 0$.

Definition

For an absolute extension, the norm of the principal ideal $\mathcal{I}$ generated by α is

$$N_{\mathbb{K}/\mathbb{Q}}(\mathcal{I}) = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right| = [\mathcal{O}_{\mathbb{K}} : \mathcal{I}]$$

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

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

The product of all components of $\vec{\mathbf{x}}$ 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

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

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

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

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 (complex case)

- If $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{F} = \mathbb{Q}(\omega)$, the same definition applies. But the considered Galois group is the group $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$ and the vector $\vec{\mathbf{x}}$ lies in $\mathbb{C}^n$.
  - Conjugates of x are the roots of the minimal polynomial with coefficients in $\mathbb{F}$.

The canonical embedding (complex case)

- If $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{F} = \mathbb{Q}(\omega)$, the same definition applies. But the considered Galois group is the group $\mathrm{Gal}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$ and the vector $\vec{\mathbf{x}}$ lies in $\mathbb{C}^n$.
  - Conjugates of x are the roots of the minimal polynomial with coefficients in $\mathbb{F}$.

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

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

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

Outline

Some Lattice Encryption Schemes

Lattice problems

- Shortest Vector Problem
- Closest Point Decoding
- ...

Some Lattice Encryption Schemes

Lattice problems

- Shortest Vector Problem
- Closest Point Decoding
- ...

Conjecture

There is no polynomial time algorithm that approximates **lattice problems** to within polynomial factors.

Some Lattice Encryption Schemes

Lattice problems

- Shortest Vector Problem
- Closest Point Decoding
- ...

Conjecture

There is no polynomial time algorithm that approximates **lattice problems** to within polynomial factors.

Public-key crypto-system

Transmit a lattice point + a small error.

- **Public key:** A "bad" basis of Λ.
- **Private key:** A "good" basis of Λ.

From homomorphic encryption to homomorphic coding

Coding/Encryption should be transparent to any function.

From homomorphic encryption to homomorphic coding

Coding/Encryption should be transparent to any function.

Polynomial code through construction A (generalization of a cyclic code).
Instead of being defined as an ideal of $\mathscr{R}[X]/X^n-1$, C is defined as an ideal of $\mathscr{R}[X]/\phi(X)$.

Construction of D_4

As an ideal lattice

$\mathbb{F} = \mathbb{Q}(i)$; $\mathbb{K} = \mathbb{F}(\zeta_8)$; $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i][\zeta_8]$; Canonical embedding of $\mathcal{O}_{\mathbb{K}}$:

$$\begin{bmatrix} 1 & \zeta_8 \\ 1 & -\zeta_8 \end{bmatrix} = \sqrt{2}\ \text{Unitary Matrix}$$

which means that $\Lambda_{\mathcal{O}_{\mathbb{K}}} \simeq \mathbb{Z}[i]^2 \simeq \mathbb{Z}^4$. Take $\mathcal{I} = (1+\zeta_8)$. Obviously, $N_{\mathbb{K}/\mathbb{F}}(\mathcal{I}) = (1+i)$.

$$(1+i)\,\mathbb{Z}[i]^2 \subset \Lambda_{\mathcal{I}} \subset \mathbb{Z}[i]^2$$

Construction of D_4

As an ideal lattice

$\mathbb{F} = \mathbb{Q}(i)$; $\mathbb{K} = \mathbb{F}(\zeta_8)$; $\mathcal{O}_\mathbb{K} = \mathbb{Z}[i][\zeta_8]$; Canonical embedding of $\mathcal{O}_\mathbb{K}$:

$$\begin{bmatrix} 1 & \zeta_8 \\ 1 & -\zeta_8 \end{bmatrix} = \sqrt{2}\ \text{Unitary Matrix}$$

which means that $\Lambda_{\mathcal{O}_\mathbb{K}} \simeq \mathbb{Z}[i]^2 \simeq \mathbb{Z}^4$. Take $\mathcal{I} = (1+\zeta_8)$. Obviously, $N_{\mathbb{K}/\mathbb{F}}(\mathcal{I}) = (1+i)$.

$$(1+i)\,\mathbb{Z}[i]^2 \subset \Lambda_\mathcal{I} \subset \mathbb{Z}[i]^2$$

Connection with construction A

We can say that

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

where $(2,1)_{\mathbb{F}_2}$ is the binary cyclic code of length 2 and generator polynomial $1+X$ (since minimal polynomial of ζ_8 is $X^2 - i$).

Construction of E_8

As an ideal lattice

$\mathbb{F} = \mathbb{Q}(\omega)$; $\mathbb{K} = \mathbb{F}(\zeta_{24})$; $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega][\zeta_{24}]$; Check that

$$\Lambda_{\mathcal{O}_{\mathbb{K}}} \simeq \mathbb{Z}[\omega]^4 \simeq A_2^4.$$

Take $\mathscr{I} = \left(1 + \zeta_{24} - \zeta_{24}^2\right)$. $N_{\mathbb{K}/\mathbb{F}}(\mathscr{I}) = (2+\omega)$.

$$(2+\omega)\,\mathbb{Z}[\omega]^4 \subset \Lambda_{\mathscr{I}} \subset \mathbb{Z}[\omega]^4$$

Construction of E_8

As an ideal lattice

$\mathbb{F} = \mathbb{Q}(\omega)$; $\mathbb{K} = \mathbb{F}(\zeta_{24})$; $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega][\zeta_{24}]$; Check that

$$\Lambda_{\mathcal{O}_{\mathbb{K}}} \simeq \mathbb{Z}[\omega]^4 \simeq A_2^4.$$

Take $\mathcal{I} = \left(1 + \zeta_{24} - \zeta_{24}^2\right)$. $N_{\mathbb{K}/\mathbb{F}}(\mathcal{I}) = (2+\omega)$.

$$(2+\omega)\,\mathbb{Z}[\omega]^4 \subset \Lambda_{\mathcal{I}} \subset \mathbb{Z}[\omega]^4$$

Connection with construction A

We can say that

$$\Lambda_{\mathcal{I}} = (2+\omega)\,\mathbb{Z}[\omega]^4 + (4,2)_{\mathbb{F}_3} \simeq E_8$$

where $(4,2)_{\mathbb{F}_3}$ is the ternary negacyclic code of length 4 and generator polynomial $1 + X - X^2$ (since minimal polynomial of ζ_{24} is $X^4 + \omega$).

Open Problems

On the Coding side

Find a family of ideal lattices which could achieve capacity of the Gaussian channel when $n \to \infty$ and are decodable.

Open Problems

On the Coding side

Find a family of ideal lattices which could achieve capacity of the Gaussian channel when $n \to \infty$ and are decodable.

Computation Rates, fields, ideals

- **Computation Rate:** Same work as in the linear case (**Compute-and-Forward**) has to be performed.
- **Choice of field, ideal ...:** related to the functions that have to be computed

Thank You !!