Explicit Lattice Constructions: From Codes to Number Fields

Jean-Claude Belfiore (†)

in collaboration with Frédérique Oggier (‡)

2015 SP Coding and information School

Unicamp, Brazil

(†) Telecom ParisTech France & (‡) NTU Singapore

Outline

Outline

An example: the partition

QAM Partition à la Ungerboeck

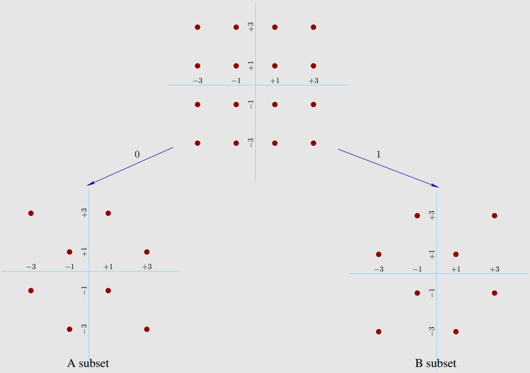


Figure : Labeling of subsets A and B

An example: the encoding → D_4

Encoder

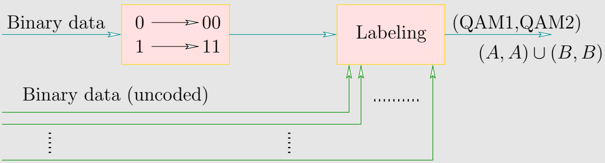


Figure : D_4 encoder

An example: the encoding $\rightarrow D_4$

Encoder

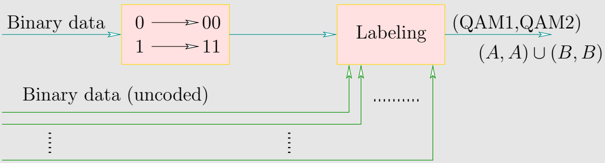


Figure : D_4 encoder

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

An example: the encoding $\to D_4$

Encoder

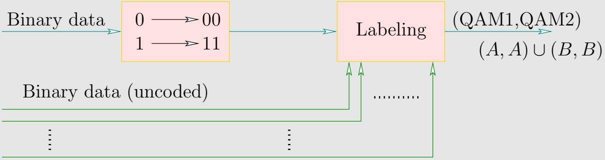


Figure : D_4 encoder

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

One of the simplest examples of "Construction A"

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

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 $v_1, v_2, \ldots, v_n$ is a **lattice basis**.

Definition

Matrix M whose columns are vectors $v_1, v_2, \ldots, v_n$ is a **generator matrix** of the lattice denoted Λ_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 : Properties

- The generator matrix M describes the lattice Λ_M, but it is not unique. All matrices $M \cdot T$ where T has **integer** entries and $\det T = \pm 1$ are generator matrices of Λ_M. T is called a unimodular matrix.
- $G = M^\top \cdot M$ is the **Gram matrix** of the lattice .
- The lattice which has generator matrix is $M^{-\top}$ is called the dual matrix of Λ_M, denoted $\Lambda_M^\star$.

Lattices : 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 .
- The lattice which has generator matrix is $\boldsymbol{M}^{-\top}$ is called the dual matrix of $\Lambda_{\boldsymbol{M}}$, denoted $\Lambda_{\boldsymbol{M}}^{\star}$.

Definitions

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

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

- 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 : Geometric properties (cont.)

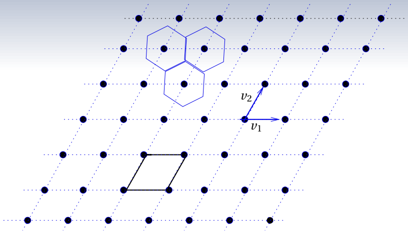
Definition

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

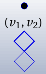
$$\mathcal{V}_\Lambda(\boldsymbol{u}) = \left\{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x} - \boldsymbol{u}\| \leq \left\|\boldsymbol{x} - \boldsymbol{y}\right\|, \quad \boldsymbol{y} \in \Lambda\right\}$$

- 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.

The A_2 lattice



The A_2 lattice



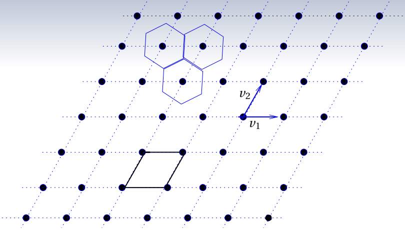
Lattice point

Lattice basis

Fundamental parallelotope

Voronoi region

The A_2 lattice



The A_2 lattice

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

Properties

- Generator matrix is

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

- We also have $\mathbb{Z}\left[\zeta_3\right] = \left\{a + b\zeta_3,\, a, b \in \mathbb{Z}\right\} \simeq A_2$ (Eisenstein integers) where $\zeta_3 = e^{\frac{2\imath\pi}{3}}$.

Outline

Coset Encoding on $\mathbb{Z}$

Lattice $\mathbb{Z}$ is used to transmit information symbols.

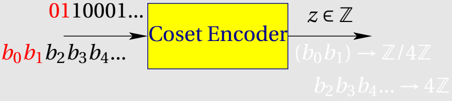


Figure : Special attention to bits b_0 and b_1

Coset Encoding on $\mathbb{Z}$

Lattice $\mathbb{Z}$ is used to transmit information symbols.

$$\underset{b_0 b_1 b_2 b_3 b_4 \ldots}{\xrightarrow{0110001\ldots}} \boxed{\text{Coset Encoder}} \xrightarrow{z \in \mathbb{Z}}$$

$(b_0 b_1) \to \mathbb{Z}/4\mathbb{Z}$

$b_2 b_3 b_4 \ldots \to 4\mathbb{Z}$

Figure : Special attention to bits b_0 and b_1

Coset Encoding on $\mathbb{Z}$

Lattice $\mathbb{Z}$ is used to transmit information symbols.

01 10001...

$b_0 b_1 b_2 b_3 b_4 \ldots \longrightarrow$ $\boxed{\text{Coset Encoder}}$ $\xrightarrow{z \in \mathbb{Z}}$

$(b_0 b_1) \to \mathbb{Z}/4\mathbb{Z}$

$b_2 b_3 b_4 \ldots \to 4\mathbb{Z}$

Figure : Special attention to bits b_0 and b_1

$b_0 b_1$ encoded on $\{0, 1, 2, 3\}$

Coset Encoding on $\mathbb{Z}$

Lattice $\mathbb{Z}$ is used to transmit information symbols.

$$0110001\ldots \quad b_0 b_1 b_2 b_3 b_4 \ldots \longrightarrow \boxed{\text{Coset Encoder}} \xrightarrow{z \in \mathbb{Z}}$$

$$(b_0 b_1) \to \mathbb{Z}/4\mathbb{Z}$$

$$b_2 b_3 b_4 \ldots \to 4\mathbb{Z}$$

Figure : Special attention to bits b_0 and b_1

$b_0 b_1$ encoded on $\{0, 1, 2, 3\}$

Decoding $(b_0 b_1)$

$(b_0 b_1)$ are recovered using the Euclidean division, $z \bmod 4$.

Coset Encoding on $\mathbb{Z}$

Lattice $\mathbb{Z}$ is used to transmit information symbols.

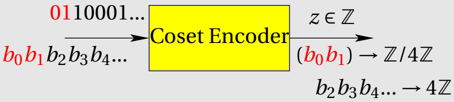


Figure : Special attention to bits b_0 and b_1

$b_0 b_1$ encoded on $\{0, 1, 2, 3\}$

Decoding $(b_0 b_1)$

$(b_0 b_1)$ are recovered using the Euclidean division, $z \bmod 4$.

And with noise..?

What happens if instead of z, we observe $z + \text{noise}$?

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

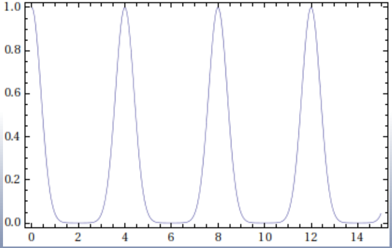


Figure : Sum of Gaussian measures, $\sigma = 0.4$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

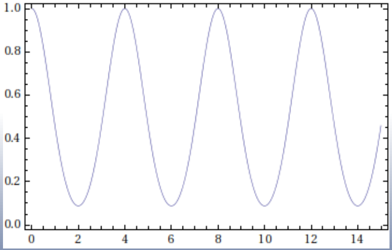


Figure : Sum of Gaussian measures, $\sigma = 0.8$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

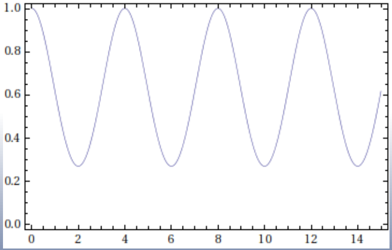


Figure : Sum of Gaussian measures, $\sigma = 1$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

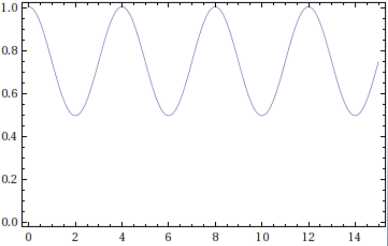


Figure : Sum of Gaussian measures, $\sigma = 1.2$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

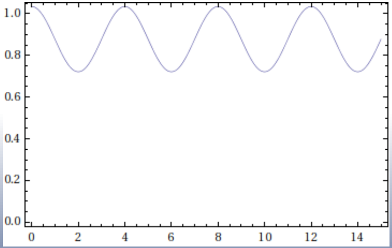


Figure : Sum of Gaussian measures, $\sigma = 1.4$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

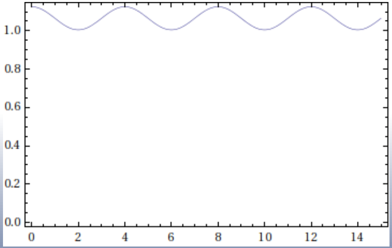


Figure : Sum of Gaussian measures, $\sigma = 1.7$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + v$ where

$$p_v(x) = \frac{1}{\sqrt{2}\pi\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{v}.$$

$\tilde{v}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{v}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

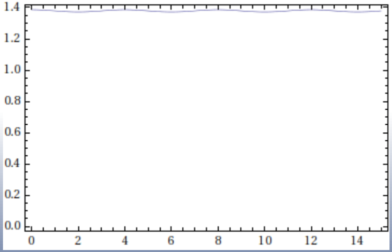


Figure : Sum of Gaussian measures, $\sigma = 2.2$

Noisy observation (with $\mathbb{Z}$)

Suppose $y = z + \nu$ where

$$p_\nu(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}.$$

Receiver **only wants** $b_0 b_1$. It computes

$$\tilde{y} = y \bmod 4 = \underbrace{z \bmod 4}_{b_0 b_1} + \tilde{\nu}.$$

Goes from quasi-**Gaussian** to quasi-**uniform**.

$\tilde{\nu}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{\nu}}(x) \sim \begin{cases} \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}} & x \in [0,4) \\ 0 & x \notin [0,4) \end{cases}$$

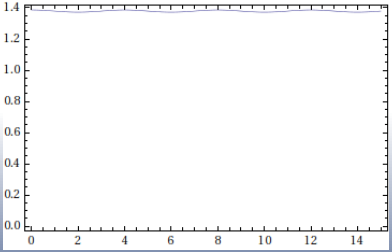


Figure : Sum of Gaussian measures, $\sigma = 2.2$

Lattice Coset Encoding

Nested Lattices

Ingredients

- A “fine” lattice Λ_f
- A “coarse” lattice $\Lambda_c \subset \Lambda_f$

Then, Λ_f / Λ_c is an additive group with

$$\left|\Lambda_f / \Lambda_c\right| = \frac{\mathrm{Vol}\,(\Lambda_c)}{\mathrm{Vol}\left(\Lambda_f\right)}$$

Lattice Coset Encoding

Nested Lattices

Ingredients

- A “fine” lattice Λ_f
- A “coarse” lattice $\Lambda_c \subset \Lambda_f$

Then, Λ_f/Λ_c is an additive group with

$$\left|\Lambda_f/\Lambda_c\right| = \frac{\mathrm{Vol}\,(\Lambda_c)}{\mathrm{Vol}\left(\Lambda_f\right)}$$

$b_0 b_1$	00	11	01	10
Cosets	$\star$	$\square$	$\triangle$	$\circ$

Table : Encoding bits $b_0 b_1$

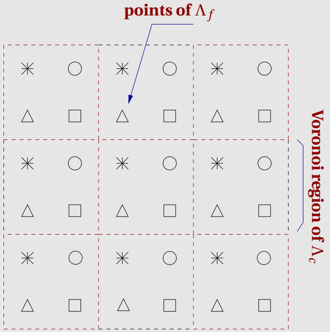


Figure : Example of coset encoding: $\mathbb{Z}^2/2\mathbb{Z}^2$

Noisy observation (any Λ)

Data are encoded in Λ_f/Λ_c. Transmitted vector (in Λ_f) is

$$z = \underbrace{z_c}_{\in\Lambda_c} + \underbrace{z_d}_{\text{coset}}$$

Noisy observation (any Λ)

Data are encoded in Λ_f/Λ_c. Transmitted vector (in Λ_f) is

$$\boldsymbol{z} = \underbrace{\boldsymbol{z}_c}_{\in\Lambda_c} + \underbrace{\boldsymbol{z}_d}_{\text{coset}}$$

Received n–dimensional vector is $\boldsymbol{y} = \boldsymbol{z} + \boldsymbol{v}$ where

$$p_{\boldsymbol{v}}(\boldsymbol{x}) = \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^n e^{-\frac{\|\boldsymbol{x}\|^2}{2\sigma^2}}.$$

Receiver **only wants** data. It computes

$$\tilde{\boldsymbol{y}} = \boldsymbol{y} \bmod \Lambda_c = \underbrace{\boldsymbol{z} \bmod \Lambda_c}_{\text{data}} + \tilde{\boldsymbol{v}}.$$

Noisy observation (any Λ)

Data are encoded in Λ_f/Λ_c. Transmitted vector (in Λ_f) is

$$\boldsymbol{z} = \underbrace{\boldsymbol{z}_c}_{\in\Lambda_c} + \underbrace{\boldsymbol{z}_d}_{\text{coset}}$$

Received $n-$dimensional vector is $\boldsymbol{y} = \boldsymbol{z} + \boldsymbol{v}$ where

$$p_{\boldsymbol{v}}(\boldsymbol{x}) = \left(\frac{1}{\sqrt{2}\pi\sigma}\right)^n e^{-\frac{\|\boldsymbol{x}\|^2}{2\sigma^2}}.$$

Receiver **only wants** data. It computes

$$\tilde{\boldsymbol{y}} = \boldsymbol{y} \bmod \Lambda_c = \underbrace{\boldsymbol{z} \bmod \Lambda_c}_{\text{data}} + \tilde{\boldsymbol{v}}.$$

pdf of $\tilde{\boldsymbol{v}}$

$\tilde{\boldsymbol{v}}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{\boldsymbol{v}}}(\boldsymbol{x}) \sim \begin{cases} \sum_{\boldsymbol{\lambda}\in\Lambda_c} e^{-\frac{(\boldsymbol{x}-\boldsymbol{\lambda})^2}{2\sigma^2}} & \boldsymbol{x} \in \mathcal{V}(\Lambda_c) \\ 0 & \boldsymbol{x} \notin \mathcal{V}(\Lambda_c) \end{cases}$$

where $\mathcal{V}(\Lambda_c)$ is the **Voronoi** region of Λ_c.

Noisy observation (any Λ)

Data are encoded in Λ_f/Λ_c. Transmitted vector (in Λ_f) is

$$\boldsymbol{z} = \underbrace{\boldsymbol{z}_c}_{\in\Lambda_c} + \underbrace{\boldsymbol{z}_d}_{\text{coset}}$$

Received $n-$dimensional vector is $\boldsymbol{y} = \boldsymbol{z} + \boldsymbol{v}$ where

$$p_{\boldsymbol{v}}(\boldsymbol{x}) = \left(\frac{1}{\sqrt{2}\pi\sigma}\right)^n e^{-\frac{\|\boldsymbol{x}\|^2}{2\sigma^2}}.$$

Receiver **only wants** data. It computes

$$\tilde{\boldsymbol{y}} = \boldsymbol{y} \bmod \Lambda_c = \underbrace{\boldsymbol{z} \bmod \Lambda_c}_{\text{data}} + \tilde{\boldsymbol{v}}.$$

pdf of $\tilde{\boldsymbol{v}}$

$\tilde{\boldsymbol{v}}$ is a folded Gaussian noise with pdf,

$$p_{\tilde{\boldsymbol{v}}}(\boldsymbol{x}) \sim \begin{cases} \sum_{\boldsymbol{\lambda}\in\Lambda_c} e^{-\frac{(\boldsymbol{x}-\boldsymbol{\lambda})^2}{2\sigma^2}} & \boldsymbol{x} \in \mathcal{V}(\Lambda_c) \\ 0 & \boldsymbol{x} \notin \mathcal{V}(\Lambda_c) \end{cases}$$

where $\mathcal{V}(\Lambda_c)$ is the **Voronoi** region of Λ_c.

$\sum_{\boldsymbol{\lambda}\in\Lambda_c} e^{-\frac{(\boldsymbol{x}-\boldsymbol{\lambda})^2}{2\sigma^2}}$ is a **sum of Gaussian measures** on the lattice Λ_c (Lattice cryptologists have studied this function in the framework of "**Learning with errors**")

Likelihood

Likelihood function $p_{\boldsymbol{y}/\text{data}}\left(\boldsymbol{x}/\boldsymbol{z}_d\right)$ behaves in a similar way,

$$
\begin{aligned}
p_{\boldsymbol{y}/\text{data}}\left(\boldsymbol{x}/\boldsymbol{z}_d\right) \quad & \sim \quad \sum_{\boldsymbol{z}_c \in \Lambda_c} p_{\boldsymbol{y}}\left(\boldsymbol{x}/\boldsymbol{z}, \boldsymbol{z} = \boldsymbol{z}_d + \boldsymbol{z}_c\right) \\
& \sim \quad \sum_{\boldsymbol{\lambda} \in \Lambda_c} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{z}_d-\boldsymbol{\lambda}\|^2}{2\sigma^2}}.
\end{aligned}
$$

Likelihood

Likelihood function $p_{\boldsymbol{y}/\text{data}}\left(\boldsymbol{x}/\boldsymbol{z}_d\right)$ behaves in a similar way,

$$\begin{aligned} p_{\boldsymbol{y}/\text{data}}\left(\boldsymbol{x}/\boldsymbol{z}_d\right) &\sim \sum_{\boldsymbol{z}_c \in \Lambda_c} p_{\boldsymbol{y}}\left(\boldsymbol{x}/\boldsymbol{z}, \boldsymbol{z} = \boldsymbol{z}_d + \boldsymbol{z}_c\right) \\ &\sim \sum_{\boldsymbol{\lambda} \in \Lambda_c} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{z}_d-\boldsymbol{\lambda}\|^2}{2\sigma^2}}. \end{aligned}$$

Sum of Gaussian measures on translated lattice points.

Construction D

Over $\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$;Partition chain:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^m\mathbb{Z}$$

Construction D

Over $\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$;Partition chain:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^m\mathbb{Z}$$

Nested codes

A family of nested binary linear codes of length n:

$$\mathscr{C}_0 \subset \mathscr{C}_1 \subset \mathscr{C}_2 \cdots \subset \mathscr{C}_m$$

Construction D

Over $\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$;Partition chain:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^m\mathbb{Z}$$

Nested codes

A family of nested binary linear codes of length n:

$$\mathscr{C}_0 \subset \mathscr{C}_1 \subset \mathscr{C}_2 \cdots \subset \mathscr{C}_m$$

Construction D

We get

$$\Lambda = 2^m\mathbb{Z}^n + 2^{m-1}\mathscr{C}_{m-1} + 2^{m-2}\mathscr{C}_{m-2} + \cdots + \mathscr{C}_0$$

Construction D

Over $\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$;Partition chain:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^m\mathbb{Z}$$

Nested codes

A family of nested binary linear codes of length n:

$$\mathscr{C}_0 \subset \mathscr{C}_1 \subset \mathscr{C}_2 \cdots \subset \mathscr{C}_m$$

Construction D

We get

$$\Lambda = 2^m\mathbb{Z}^n + 2^{m-1}\mathscr{C}_{m-1} + 2^{m-2}\mathscr{C}_{m-2} + \cdots + \mathscr{C}_0$$

Over a number field

Choose $\mathbb{K}$ a number field with ring of integer $\mathscr{O}_{\mathbb{K}}$. Let $\mathscr{J}$ be an ideal of $\mathscr{O}_{\mathbb{K}}$. We get

$$\mathscr{O}_{\mathbb{K}} = \mathscr{J}^0 \supset \mathscr{J}^1 \supset \mathscr{J}^2 \supset \cdots \supset \mathscr{J}^m$$

with $\mathscr{O}_{\mathbb{K}}/\mathscr{J} \simeq \mathscr{R}$, a finite ring (which is a finite field if $\mathscr{J}$ is a prime ideal).

Construction D

Over $\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$;Partition chain:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^m\mathbb{Z}$$

Nested codes

A family of nested binary linear codes of length n:

$$\mathscr{C}_0 \subset \mathscr{C}_1 \subset \mathscr{C}_2 \cdots \subset \mathscr{C}_m$$

Construction D

We get

$$\Lambda = 2^m\mathbb{Z}^n + 2^{m-1}\mathscr{C}_{m-1} + 2^{m-2}\mathscr{C}_{m-2} + \cdots + \mathscr{C}_0$$

Over a number field

Choose $\mathbb{K}$ a number field with ring of integer $\mathscr{O}_{\mathbb{K}}$. Let $\mathscr{J}$ be an ideal of $\mathscr{O}_{\mathbb{K}}$. We get

$$\mathscr{O}_{\mathbb{K}} = \mathscr{J}^0 \supset \mathscr{J}^1 \supset \mathscr{J}^2 \supset \cdots \supset \mathscr{J}^m$$

with $\mathscr{O}_{\mathbb{K}}/\mathscr{J} \simeq \mathscr{R}$, a finite ring (which is a finite field if $\mathscr{J}$ is a prime ideal).

A family of nested linear codes of length n over $\mathscr{R}$

Construction D

Over $\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$;Partition chain:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^m\mathbb{Z}$$

Nested codes

A family of nested binary linear codes of length n:

$$\mathscr{C}_0 \subset \mathscr{C}_1 \subset \mathscr{C}_2 \cdots \subset \mathscr{C}_m$$

Construction D

We get

$$\Lambda = 2^m\mathbb{Z}^n + 2^{m-1}\mathscr{C}_{m-1} + 2^{m-2}\mathscr{C}_{m-2} + \cdots + \mathscr{C}_0$$

Over a number field

Choose $\mathbb{K}$ a number field with ring of integer $\mathscr{O}_{\mathbb{K}}$. Let $\mathscr{J}$ be an ideal of $\mathscr{O}_{\mathbb{K}}$. We get

$$\mathscr{O}_{\mathbb{K}} = \mathscr{J}^0 \supset \mathscr{J}^1 \supset \mathscr{J}^2 \supset \cdots \supset \mathscr{J}^m$$

with $\mathscr{O}_{\mathbb{K}}/\mathscr{J} \simeq \mathscr{R}$, a finite ring (which is a finite field if $\mathscr{J}$ is a prime ideal).

A family of nested linear codes of length n over $\mathscr{R}$

(Generalized) Construction D

We get

$$\Lambda = \left(\mathscr{J}^m\right)^n + \varphi_1\left(\mathscr{C}_{m-1}\right) + \varphi_2\left(\mathscr{C}_{m-2}\right) + \cdots + \varphi_m\left(\mathscr{C}_0\right)$$

where φ_i is the homomorphism that sends $\mathscr{J}^i/\mathscr{J}^{i+1}$ onto $\mathscr{R}$.

Decoding of construction D [Forney et al., 2000]

$\boldsymbol{y}$ is the received signal,

$$\Lambda = 2^m\mathbb{Z}^n + 2^{m-1}\mathscr{C}_{m-1} + 2^{m-2}\mathscr{C}_{m-2} + \cdots + 2\mathscr{C}_1 + \mathscr{C}_0.$$

- Calculate $\boldsymbol{y} \bmod 2$, then decode $\mathscr{C}_0$. Subtract the decoded codeword from $\boldsymbol{y} \hookrightarrow \boldsymbol{y}_1$.
- Calculate $\boldsymbol{y}_1 \bmod 4$, then decode $2\mathscr{C}_1$. Subtract the decoded codeword from $\boldsymbol{y}_1 \hookrightarrow \boldsymbol{y}_2$.
- $\cdots$
- Find the closest lattice point (in $2^m\mathbb{Z}^n$) of $\boldsymbol{y}_{m-1}$ (**very easy**).

Decoding of construction D [Forney et al., 2000]

$\boldsymbol{y}$ is the received signal,

$$\Lambda = 2^m\mathbb{Z}^n + 2^{m-1}\mathscr{C}_{m-1} + 2^{m-2}\mathscr{C}_{m-2} + \cdots + 2\mathscr{C}_1 + \mathscr{C}_0.$$

- Calculate $\boldsymbol{y} \bmod 2$, then decode $\mathscr{C}_0$. Subtract the decoded codeword from $\boldsymbol{y} \hookrightarrow \boldsymbol{y}_1$.
- Calculate $\boldsymbol{y}_1 \bmod 4$, then decode $2\mathscr{C}_1$. Subtract the decoded codeword from $\boldsymbol{y}_1 \hookrightarrow \boldsymbol{y}_2$.
- $\cdots$
- Find the closest lattice point (in $2^m\mathbb{Z}^n$) of $\boldsymbol{y}_{m-1}$ (**very easy**).

Folded noise

At step i, the noise has pdf (per component),

$$\sim \sum_{k=-\infty}^{+\infty} e^{-\frac{\left(x-2^i k\right)^2}{2\sigma^2}}$$

Outline

A characterization of how flat the sum of Gaussian measures is

Sum of Gaussian measures

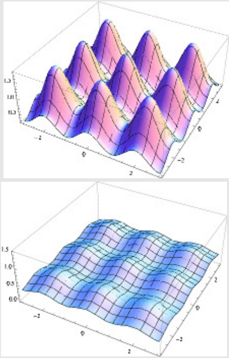
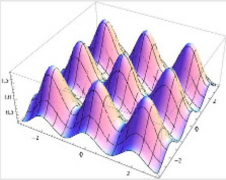


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

A characterization of how flat the sum of Gaussian measures is

Sum of Gaussian measures



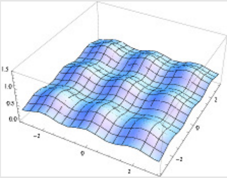


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

How far is the folded noise distribution from the uniform distribution on $\mathcal{V}(\Lambda_c)$?

A characterization of how flat the sum of Gaussian measures is

Sum of Gaussian measures

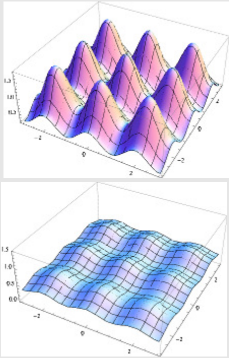


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

How far is the folded noise distribution from the uniform distribution on $\mathcal{V}(\Lambda_c)$?

Flatness factor (L_∞distance) [Ling et al., 2012]

$$\varepsilon_{\Lambda_c}(\sigma) = \max_{\boldsymbol{x}\in\mathcal{V}(\Lambda_c)} \left| \frac{\sum_{\boldsymbol{\lambda}\in\Lambda_c} \left(\frac{1}{2\pi\sigma^2}\right)^{\frac{n}{2}} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}}{1/\mathrm{Vol}(\Lambda_c)} - 1 \right|$$

A characterization of how flat the sum of Gaussian measures is

Sum of Gaussian measures

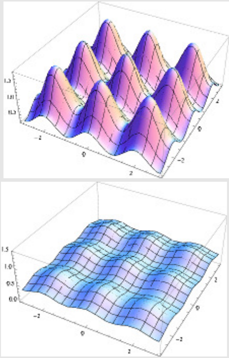


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

How far is the folded noise distribution from the uniform distribution on $\mathcal{V}(\Lambda_c)$?

Flatness factor (L_∞ distance) [Ling et al., 2012]

$$\varepsilon_{\Lambda_c}(\sigma) = \max_{\boldsymbol{x}\in\mathcal{V}(\Lambda_c)} \left| \frac{\sum_{\boldsymbol{\lambda}\in\Lambda_c} \left(\frac{1}{2\pi\sigma^2}\right)^{\frac{n}{2}} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}}{1/\mathrm{Vol}(\Lambda_c)} - 1 \right|$$

The flatness factor can be evaluated,

$$\boxed{\varepsilon_{\Lambda_c}(\sigma) = \left(\frac{\mathrm{Vol}(\Lambda_c)^{\frac{2}{n}}}{2\pi\sigma^2}\right)^{\frac{n}{2}} \underbrace{\sum_{\boldsymbol{\lambda}\in\Lambda_c} e^{-\frac{\|\boldsymbol{\lambda}\|^2}{2\sigma^2}}}_{\Theta_{\Lambda_c}\left(-\frac{\imath}{2\sigma^2}\right)} - 1}$$

Theta Series

Definition

The Theta Series of a lattice Λ is a function of the complex variable,

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

evaluated at $q = e^{\imath\pi\tau}$.

Theta Series

Definition

The Theta Series of a lattice Λ is a function of the complex variable,

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

evaluated at $q = e^{\imath\pi\tau}$.

Classically, for a point-to-point communication, only the first non trivial term is used,

$$\Theta_{\Lambda}(\tau) = 1 + \kappa q^{d^2_{\min}} + \cdots$$

where κ is the **kissing number** and $d^2_{\min}$ is the Euclidean square **minimum distance**.
It comes from the "**union bound**" technique to upperbound the error probability.

Theta Series

Definition

The Theta Series of a lattice Λ is a function of the complex variable,

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

evaluated at $q = e^{\imath\pi\tau}$.

Classically, for a point-to-point communication, only the first non trivial term is used,

$$\Theta_\Lambda(\tau) = 1 + \kappa q^{d^2_{\min}} + \cdots$$

where κ is the **kissing number** and $d^2_{\min}$ is the Euclidean square **minimum distance**.
It comes from the "**union bound**" technique to upperbound the error probability.

More recent paradigms need the **full** theta series.

- Coset encoding
- Modulo Λ decoding
- Construction D with "per layer" decoding
- Finite length analysis of compute-and-forward

Theta Series

Definition

The Theta Series of a lattice Λ is a function of the complex variable,

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

evaluated at $q = e^{\imath\pi\tau}$.

Classically, for a point-to-point communication, only the first non trivial term is used,

$$\Theta_\Lambda(\tau) = 1 + \kappa q^{d^2_{\min}} + \cdots$$

where κ is the **kissing number** and $d^2_{\min}$ is the Euclidean square **minimum distance**.
It comes from the "**union bound**" technique to upperbound the error probability.

More recent paradigms need the **full** theta series.

- Coset encoding
- Modulo Λ decoding
- Construction D with "per layer" decoding
- Finite length analysis of compute-and-forward
- **Physical Layer Security**

Outline

The Gaussian Wiretap Channel

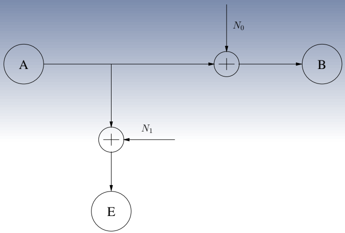


Figure : The Gaussian Wiretap Channel model

The Gaussian Wiretap Channel

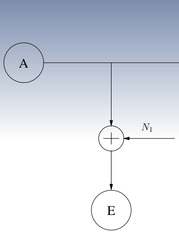


Figure : The Gaussian Wiretap Channel model

The secrecy capacity is given by

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

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

Uniform Noise

Assume that **Alice** $\rightarrow$ **Eve** channel is corrupted by an additive uniform noise

Uniform Noise

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

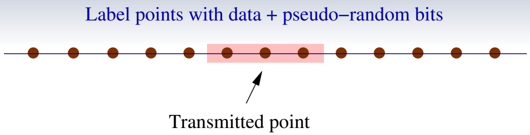


Figure : Constellation corrupted by uniform noise

Uniform Noise

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

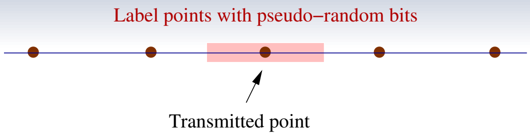


Figure : Points can be decoded **error free**: label with pseudo-random symbols

Uniform Noise

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

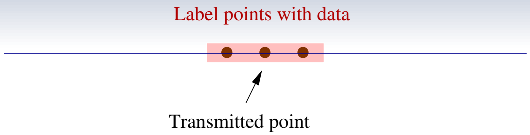


Figure : Points are **not distinguishable**: label with data

Uniform Noise

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

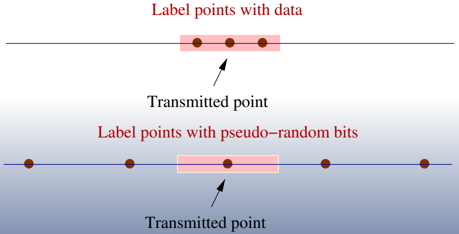


Figure : Constellation corrupted by uniform noise

Uniform Noise

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

Error Probability

Pseudo-random symbols are perfectly decoded by Eve while there is no information leakage.

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

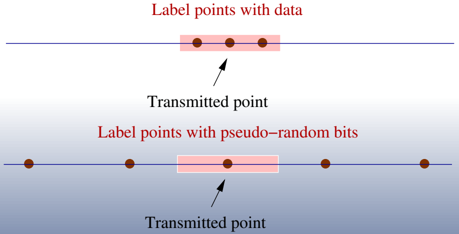


Figure : Constellation corrupted by uniform noise

Coset Coding with Integers

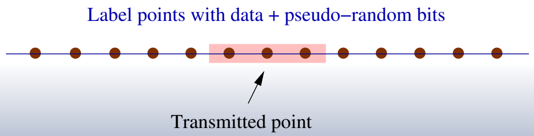


Figure : Constellation corrupted by uniform noise

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 $\mathbb{Z}/3\mathbb{Z}$".

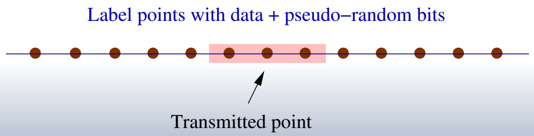


Figure : Constellation corrupted by uniform noise

Lattice Coset Coding

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

	$1-$dimensional
Transmitted lattice	$\mathbb{Z}$
Pseudo-random symbols	$m\mathbb{Z} \subset \mathbb{Z}$
Data	$\mathbb{Z}/m\mathbb{Z}$

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**).

	$n-$dimensional
Transmitted lattice	Fine lattice Λ_b
Pseudo-random symbols	Coarse lattice $\Lambda_e \subset \Lambda_b$
Data	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**).

	$1-$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

Eve's Probability of Correct Decision (data)

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

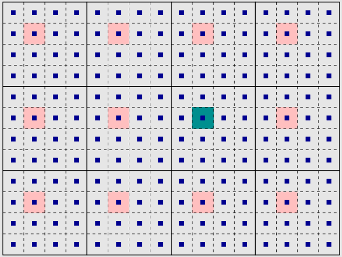


Figure : Eve correctly decodes when finding another coset representative

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

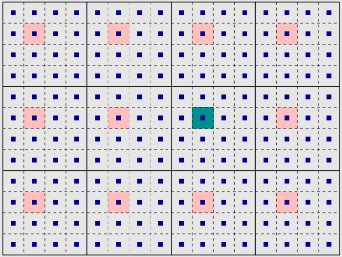


Figure : Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision [Oggier et al., 2011a]

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

where

$$
\boxed{\Theta_\Lambda(\tau) = \sum_{\boldsymbol{\lambda}\in\Lambda} q^{\|\boldsymbol{\lambda}\|^2}, q = e^{\imath\pi\tau}, \tau\in\mathbb{C}, \Im(\tau) > 0}
$$

is the **theta series** of Λ.

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

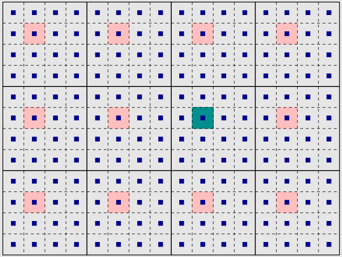


Figure : Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision [Oggier et al., 2011a]

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

where

$$
\boxed{\Theta_{\Lambda}(\tau) = \sum_{\boldsymbol{\lambda}\in\Lambda} q^{\|\boldsymbol{\lambda}\|^2}, q = e^{\imath\pi\tau}, \tau \in \mathbb{C}, \Im(\tau) > 0}
$$

is the **theta series** of Λ.

Problem

Find Λ minimizing $\boxed{\Theta_{\Lambda}(\tau)}$ when τ varies along the positive imaginary semiaxis.

Flatness Factor

Information Leakage [Ling et al., 2012]

Let M be the transmitted secret message and Z^n be the vector received by Eve. Then,

$$I\left(\mathsf{M};\mathsf{Z}^n\right) \le 2\varepsilon_{\Lambda_e}(\sigma)\left(nR - \log\varepsilon_{\Lambda_e}(\sigma)\right)$$

where

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

is the **flatness factor** of the lattice Λ_e.

Flatness Factor

Information Leakage [Ling et al., 2012]

Let M be the transmitted secret message and Z^n be the vector received by Eve. Then,

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

where

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

is the **flatness factor** of the lattice Λ_e.

Probability of correct decision

Probability of correct decision can also been expressed as a function of the flatness factor,

$$P_{c,e} \leq 2^{-nR}\left(\varepsilon_{\Lambda_e}(\sigma) + 1\right)$$

Intuition

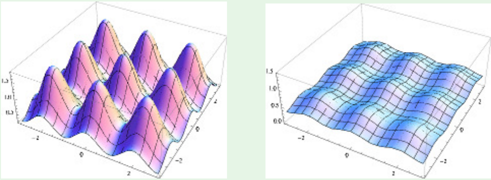


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

Intuition

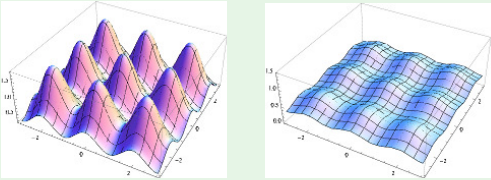


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

Flatness factor

What is the behavior of the flatness factor?

- Other figure of merit?

Secrecy function

Definition [Oggier et al., 2011b]

Let Λ be a $n-$dimensional lattice with fundamental volume λ^n and $\imath y = \tau$. Its **secrecy function** is defined as,

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

where $\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ is the theta series of $\mathbb{Z}$ and $y > 0$.

Secrecy function

Definition [Oggier et al., 2011b]

Let Λ be a $n-$dimensional lattice with fundamental volume λ^n and $\imath y = \tau$. Its **secrecy function** is defined as,

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

where $\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ is the theta series of $\mathbb{Z}$ and $y > 0$.

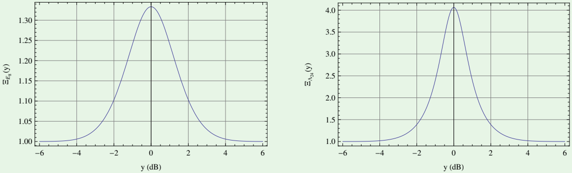


Figure : Secrecy functions of E_8 and Λ_{24}

Secrecy Gain

Definition

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

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

Secrecy Gain

Definition

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

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

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

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

Secrecy Gain

Definition

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

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

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

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

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

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

Outline

Secrecy Gain of some lattices

Secrecy Functions in dimensions 72 and 80 of lattices equal to their dual

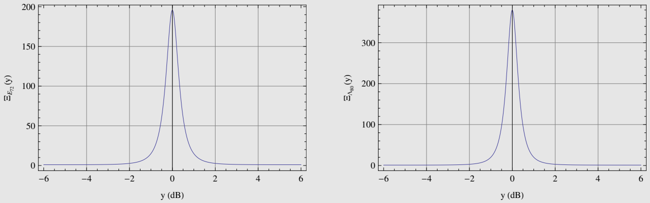


Figure : Secrecy functions in dimensions $n = 72, 80$

Secrecy Gain of some lattices

Secrecy Functions in dimensions 72 and 80 of lattices equal to their dual

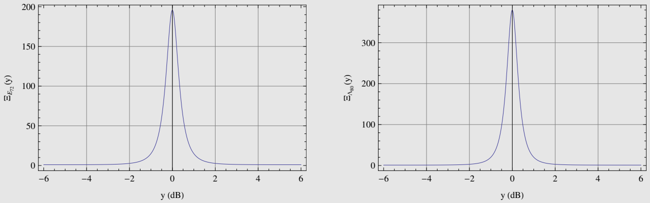


Figure : Secrecy functions in dimensions $n = 72, 80$

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

Table : Secrecy gains of integral lattices equal to their duals

Full theta series or some terms?

Lattice Γ_{72}

Discovered in [Nebe, 2012]. It is integral and equivalent to its dual. Its theta series is,

$$\Theta_{\Gamma_{72}}(\tau) = 1 + 6218175600q^8 + 15281788354560q^{10} + 9026867482214400q^{12} + \cdots$$

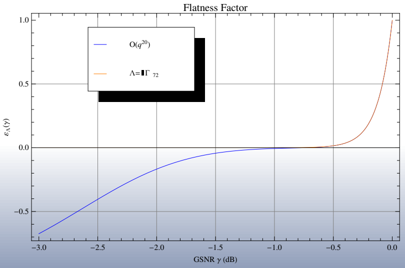


Figure : Approximation of the theta series up to order 20

Outline

Poisson summation formula ($\mathbb{Z}^n$−lattice)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a well-behaved function,

$$\begin{cases} \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x} < \infty \\ \sum_{\boldsymbol{u}\in\mathbb{Z}^n} \left| f(\boldsymbol{x}+\boldsymbol{u}) \right| \quad \text{converges uniformly} \end{cases}$$

and define $F(\boldsymbol{x}) \stackrel{\text{def}}{=} \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{x}+\boldsymbol{u})$.

Poisson summation formula ($\mathbb{Z}^n$−lattice)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a well-behaved function,

$$\begin{cases} \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x} < \infty \\ \sum_{\boldsymbol{u}\in\mathbb{Z}^n} \left| f(\boldsymbol{x}+\boldsymbol{u}) \right| & \text{converges uniformly} \end{cases}$$

and define $F(\boldsymbol{x}) \stackrel{\text{def}}{=} \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{x}+\boldsymbol{u})$.

F is periodic and has Fourier series,

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} a_{\boldsymbol{v}} e^{2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle}$$

Poisson summation formula ($\mathbb{Z}^n$–lattice)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a well-behaved function,

$$\begin{cases} \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x} < \infty \\ \sum_{\boldsymbol{u}\in\mathbb{Z}^n} \left| f(\boldsymbol{x}+\boldsymbol{u}) \right| \quad \text{converges uniformly} \end{cases}$$

and define $F(\boldsymbol{x}) \stackrel{\text{def}}{=} \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{x}+\boldsymbol{u})$.

F is periodic and has Fourier series,

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} a_{\boldsymbol{v}} e^{2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle}$$

$$a_{\boldsymbol{v}} = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \int_{[0,1]^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{y}\rangle} f\left(\boldsymbol{v}+\boldsymbol{y}\right) d\boldsymbol{y}$$

Poisson summation formula ($\mathbb{Z}^n-$lattice)

Let $f:\mathbb{R}^n \to \mathbb{R}$ be a well-behaved function,

$$\begin{cases} \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x} < \infty \\ \sum_{\boldsymbol{u}\in\mathbb{Z}^n} \left| f(\boldsymbol{x}+\boldsymbol{u}) \right| & \text{converges uniformly} \end{cases}$$

and define $F(\boldsymbol{x}) \stackrel{\text{def}}{=} \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{x}+\boldsymbol{u})$.

F is periodic and has Fourier series,

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} a_{\boldsymbol{v}} e^{2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle}$$

$$a_{\boldsymbol{v}} = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \int_{[0,1]^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{y}\rangle} f(\boldsymbol{v}+\boldsymbol{y})\, d\boldsymbol{y}$$

$$a_{\boldsymbol{v}} = \underbrace{\int_{\mathbb{R}^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{z}\rangle} f(\boldsymbol{z})\, d\boldsymbol{z}}_{\text{Fourier transform } \hat{f}(\boldsymbol{v})}$$

Poisson summation formula ($\mathbb{Z}^n$−lattice)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a well-behaved function,

$$\begin{cases} \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x} < \infty \\ \sum_{\boldsymbol{u}\in\mathbb{Z}^n} \left| f(\boldsymbol{x}+\boldsymbol{u}) \right| \quad \text{converges uniformly} \end{cases}$$

and define $F(\boldsymbol{x}) \stackrel{\text{def}}{=} \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{x}+\boldsymbol{u})$.

F is periodic and has Fourier series,

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} a_{\boldsymbol{v}} e^{2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle}$$

$$a_{\boldsymbol{v}} = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \int_{[0,1]^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{y}\rangle} f(\boldsymbol{v}+\boldsymbol{y})\, d\boldsymbol{y}$$

$$a_{\boldsymbol{v}} = \underbrace{\int_{\mathbb{R}^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{z}\rangle} f(\boldsymbol{z})\, d\boldsymbol{z}}_{\text{Fourier transform } \hat{f}(\boldsymbol{v})}$$

By equating,

$$\sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{x}+\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \hat{f}(\boldsymbol{v})\, e^{2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle}$$

and setting $\boldsymbol{x} = 0$, we get the **Poisson Summation Formula**,

$$\boxed{\sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \hat{f}(\boldsymbol{v})}$$

Poisson summation formula (general case)

Let Λ be an $n-$dimensional lattice with generator matrix $\boldsymbol{A}$, then consider

$$\sum_{\boldsymbol{x}\in\Lambda} f(\boldsymbol{x}) = \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{A}\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \widehat{\left(f\circ\boldsymbol{A}\right)}(\boldsymbol{v})$$

Poisson summation formula (general case)

Let Λ be an $n-$dimensional lattice with generator matrix $\boldsymbol{A}$, then consider

$$\sum_{\boldsymbol{x}\in\Lambda} f(\boldsymbol{x}) = \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{A}\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \widehat{(f\circ\boldsymbol{A})}(\boldsymbol{v})$$

We get,

$$\widehat{(f\circ\boldsymbol{A})}(\boldsymbol{v}) = \int_{\mathbb{R}^n} f(\boldsymbol{A}\boldsymbol{x})\, e^{-2\imath\pi\langle\boldsymbol{v},\boldsymbol{x}\rangle}\, d\boldsymbol{x}$$

Poisson summation formula (general case)

Let Λ be an $n-$dimensional lattice with generator matrix $\boldsymbol{A}$, then consider

$$\sum_{\boldsymbol{x}\in\Lambda} f(\boldsymbol{x}) = \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{A}\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \widehat{(f\circ\boldsymbol{A})}(\boldsymbol{v})$$

We get,

$$\widehat{(f\circ\boldsymbol{A})}(\boldsymbol{v}) = \int_{\mathbb{R}^n} f(\boldsymbol{A}\boldsymbol{x})\, e^{-2\imath\pi\langle\boldsymbol{v},\boldsymbol{x}\rangle}\, d\boldsymbol{x}$$

$$= |\det\boldsymbol{A}|^{-1} \int_{\mathbb{R}^n} f(\boldsymbol{y})\, e^{-2\imath\pi\left\langle \boldsymbol{A}^{-\top}\boldsymbol{v},\boldsymbol{y}\right\rangle}\, d\boldsymbol{y}$$

Poisson summation formula (general case)

Let Λ be an $n-$dimensional lattice with generator matrix $\boldsymbol{A}$, then consider

$$\sum_{\boldsymbol{x}\in\Lambda} f(\boldsymbol{x}) = \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{A}\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \widehat{(f\circ \boldsymbol{A})}(\boldsymbol{v})$$

We get,

$$\widehat{(f\circ \boldsymbol{A})}(\boldsymbol{v}) = \int_{\mathbb{R}^n} f(\boldsymbol{A}\boldsymbol{x})\, e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle} d\boldsymbol{x}$$

$$= |\det \boldsymbol{A}|^{-1} \int_{\mathbb{R}^n} f(\boldsymbol{y})\, e^{-2\imath\pi\left\langle \boldsymbol{A}^{-\top}\boldsymbol{v},\boldsymbol{y}\right\rangle} d\boldsymbol{y}$$

$$= |\det \boldsymbol{A}|^{-1} \hat{f}\left(\boldsymbol{A}^{-\top}\boldsymbol{v}\right)$$

Poisson summation formula (general case)

Let Λ be an $n-$dimensional lattice with generator matrix $\boldsymbol{A}$, then consider

$$\sum_{\boldsymbol{x}\in\Lambda} f(\boldsymbol{x}) = \sum_{\boldsymbol{u}\in\mathbb{Z}^n} f(\boldsymbol{A}\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n} \widehat{(f\circ\boldsymbol{A})}(\boldsymbol{v})$$

We get,

$$\widehat{(f\circ\boldsymbol{A})}(\boldsymbol{v}) = \int_{\mathbb{R}^n} f(\boldsymbol{A}\boldsymbol{x})\, e^{-2\imath\pi\langle\boldsymbol{v},\boldsymbol{x}\rangle}\, d\boldsymbol{x}$$

$$= |\det\boldsymbol{A}|^{-1}\int_{\mathbb{R}^n} f(\boldsymbol{y})\, e^{-2\imath\pi\left\langle\boldsymbol{A}^{-\top}\boldsymbol{v},\boldsymbol{y}\right\rangle}\, d\boldsymbol{y}$$

$$= |\det\boldsymbol{A}|^{-1}\hat{f}\left(\boldsymbol{A}^{-\top}\boldsymbol{v}\right)$$

Poisson Summation formula

Hence,

$$\boxed{\sum_{\boldsymbol{x}\in\Lambda} f(\boldsymbol{x}) = \frac{1}{\mathrm{Vol}(\Lambda)}\sum_{\boldsymbol{y}\in\Lambda^\star}\hat{f}(\boldsymbol{y})}$$

where $\Lambda^\star$ is the **dual lattice** of Λ (with generator matrix $\boldsymbol{A}^{-\top}$).

Outline

Jacobi's formula

We apply the Poisson summation formula to the theta series of a lattice.

Let $f_y(\boldsymbol{u}) = e^{-\pi y \|\boldsymbol{u}\|^2}$ for some $y > 0$ ($\tau = \imath y$). Then,

$$\Theta_\Lambda(iy) = \sum_{\boldsymbol{u} \in \Lambda} f_y(\boldsymbol{u}) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\boldsymbol{v} \in \Lambda^\star} \widehat{f_y}(\boldsymbol{v}).$$

Jacobi's formula

We apply the Poisson summation formula to the theta series of a lattice.

Let $f_y(\boldsymbol{u}) = e^{-\pi y \|\boldsymbol{u}\|^2}$ for some $y > 0$ ($\tau = \imath y$). Then,

$$\Theta_\Lambda\left(iy\right) = \sum_{\boldsymbol{u}\in\Lambda} f_y(\boldsymbol{u}) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\boldsymbol{v}\in\Lambda^\star} \widehat{f_y}(\boldsymbol{v}).$$

where

$$\widehat{f_y}(\boldsymbol{v}) = \int_{\mathbb{R}^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle - \pi y \|\boldsymbol{x}\|^2}\, d\boldsymbol{x}$$

Jacobi's formula

We apply the Poisson summation formula to the theta series of a lattice.

Let $f_y(\boldsymbol{u}) = e^{-\pi y \|\boldsymbol{u}\|^2}$ for some $y > 0$ ($\tau = \imath y$). Then,

$$\Theta_\Lambda\left(iy\right) = \sum_{\boldsymbol{u}\in\Lambda} f_y(\boldsymbol{u}) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\boldsymbol{v}\in\Lambda^\star} \widehat{f_y}(\boldsymbol{v}).$$

where

$$\widehat{f_y}(\boldsymbol{v}) = \int_{\mathbb{R}^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle - \pi y \|\boldsymbol{x}\|^2} d\boldsymbol{x}$$

$$= \prod_{k=1}^{n} \int_{\mathbb{R}} e^{-2\imath\pi v_k x_k - \pi y x_k^2} dx_k$$

Jacobi's formula

We apply the Poisson summation formula to the theta series of a lattice.

Let $f_y(\boldsymbol{u}) = e^{-\pi y \|\boldsymbol{u}\|^2}$ for some $y > 0$ ($\tau = \imath y$). Then,

$$\Theta_\Lambda\left(iy\right) = \sum_{\boldsymbol{u}\in\Lambda} f_y(\boldsymbol{u}) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\boldsymbol{v}\in\Lambda^\star} \widehat{f_y}(\boldsymbol{v}).$$

where

$$\begin{aligned}\widehat{f_y}(\boldsymbol{v}) &= \int_{\mathbb{R}^n} e^{-2\imath\pi\langle\boldsymbol{v},\boldsymbol{x}\rangle - \pi y\|\boldsymbol{x}\|^2}\, d\boldsymbol{x} \\ &= \prod_{k=1}^{n} \int_{\mathbb{R}} e^{-2\imath\pi v_k x_k - \pi y x_k^2}\, dx_k \\ &= y^{-\frac{n}{2}} e^{-\pi\frac{\|\boldsymbol{v}\|^2}{y}}\end{aligned}$$

Jacobi's formula

We apply the Poisson summation formula to the theta series of a lattice.

Let $f_y(\boldsymbol{u}) = e^{-\pi y \|\boldsymbol{u}\|^2}$ for some $y > 0$ ($\tau = \imath y$). Then,

$$\Theta_\Lambda(iy) = \sum_{\boldsymbol{u}\in\Lambda} f_y(\boldsymbol{u}) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\boldsymbol{v}\in\Lambda^\star} \widehat{f_y}(\boldsymbol{v}).$$

where

$$\widehat{f_y}(\boldsymbol{v}) = \int_{\mathbb{R}^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle - \pi y\|\boldsymbol{x}\|^2} d\boldsymbol{x}$$

$$= \prod_{k=1}^{n} \int_{\mathbb{R}} e^{-2\imath\pi v_k x_k - \pi y x_k^2} dx_k$$

$$= y^{-\frac{n}{2}} e^{-\pi\frac{\|\boldsymbol{v}\|^2}{y}}$$

Jacobi's formula [Conway & Sloane, 1998]

The theta series of an $n-$dimensional lattice Λ is related to the theta series of its dual $\Lambda^\star$ as,

$$\boxed{\Theta_{\Lambda^\star}(\tau) = \mathrm{Vol}(\Lambda)\left(\frac{\imath}{\tau}\right)^{\frac{n}{2}} \Theta_\Lambda\left(-\frac{1}{\tau}\right)}$$

by setting $\imath y = \tau$.

Jacobi's formula

We apply the Poisson summation formula to the theta series of a lattice.
Let $f_y(\boldsymbol{u}) = e^{-\pi y \|\boldsymbol{u}\|^2}$ for some $y > 0$ ($\tau = \imath y$). Then,

$$\Theta_\Lambda\left(iy\right) = \sum_{\boldsymbol{u}\in\Lambda} f_y(\boldsymbol{u}) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\boldsymbol{v}\in\Lambda^\star} \widehat{f_y}(\boldsymbol{v}).$$

where

$$\widehat{f_y}(\boldsymbol{v}) = \int_{\mathbb{R}^n} e^{-2\imath\pi\langle \boldsymbol{v},\boldsymbol{x}\rangle - \pi y \|\boldsymbol{x}\|^2} d\boldsymbol{x}$$

$$= \prod_{k=1}^{n} \int_{\mathbb{R}} e^{-2\imath\pi v_k x_k - \pi y x_k^2} dx_k$$

$$= y^{-\frac{n}{2}} e^{-\pi \frac{\|\boldsymbol{v}\|^2}{y}}$$

Jacobi's formula [Conway & Sloane, 1998]

The theta series of an $n-$dimensional lattice Λ is related to the theta series of its dual $\Lambda^\star$ as,

$$\boxed{\Theta_{\Lambda^\star}(\tau) = \mathrm{Vol}(\Lambda) \left(\frac{\imath}{\tau}\right)^{\frac{n}{2}} \Theta_\Lambda\left(-\frac{1}{\tau}\right)}$$

by setting $\imath y = \tau$.

Use Jacobi's formula to get the theta series of Λ $\longrightarrow$ needs a relationship between Λ and $\Lambda^\star$.

Outline

Unimodular lattices

Definition

A lattice Λ of rank n is **unimodular** if

- Λ is integral, i.e. its **Gram** matrix $\boldsymbol{B} = \boldsymbol{A}^{\top} \cdot \boldsymbol{A} \in GL_n(\mathbb{Z})$.
- $\Lambda = \Lambda^{\star}$

Unimodular lattices

Definition

A lattice Λ of rank n is **unimodular** if

- Λ is integral, i.e. its **Gram** matrix $\boldsymbol{B} = \boldsymbol{A}^\top \cdot \boldsymbol{A} \in GL_n(\mathbb{Z})$.
- $\Lambda = \Lambda^\star$

Examples

$\mathbb{Z}^n$ is unimodular, E_8 and Λ_{24} are unimodular.

Definition

Moreover, if the square length of any point of Λ is an even integer, then Λ is an **even unimodular** lattice. E_8 and Λ_{24} are even unimodular.

Theta series as modular forms

Since $\Lambda = \Lambda^\star$ (and $\mathrm{Vol}(\Lambda) = 1$), we get from **Jacobi's identity**,

$$\Theta_\Lambda\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{\imath}\right)^{\frac{n}{2}} \Theta_\Lambda(\tau).$$

From the periodicity of the theta series, and since Λ is even,

$$\Theta_\Lambda(\tau+1) = \Theta_\Lambda(\tau).$$

Theta series as modular forms

Since $\Lambda = \Lambda^\star$ (and $\mathrm{Vol}(\Lambda) = 1$), we get from **Jacobi's identity**,

$$\Theta_\Lambda\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{\imath}\right)^{\frac{n}{2}} \Theta_\Lambda(\tau).$$

From the periodicity of the theta series, and since Λ is even,

$$\Theta_\Lambda(\tau + 1) = \Theta_\Lambda(\tau).$$

Action of $PSL_2(\mathbb{Z})$

The group generated by $\tau \mapsto \tau + 1$ and $\tau \mapsto -\frac{1}{\tau}$ acts on the theta series of an even unimodular lattice. This group is $PSL_2(\mathbb{Z})$. So, for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc = 1$ in $SL_2(\mathbb{Z})$, if Λ is an even unimodular lattice, we have,

$$\boxed{\Theta_\Lambda\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{\frac{n}{2}} \Theta_\Lambda(\tau)}$$

which means that $\Theta_\Lambda(\tau)$ is a **modular form** of weight $\frac{n}{2}$ for the "full" group $SL_2(\mathbb{Z})$.

Theta series of E_8: A Modular form approach

Structure

The set of modular forms of weight k, $M_k(SL_2(\mathbb{Z}))$ is a **vector space** of dimension 0 if $k < 4$ and of dimension 1 when $k = 4$.

Eisenstein

Modular forms of weight 4 are proportional to the **Eisenstein series**

$$E_4(q) = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^{2m}$$

where $\sigma_3(m)$ is the sum of the cubes of the divisors of m.

Theta series of E_8: A Modular form approach

Structure

The set of modular forms of weight k, $M_k(SL_2(\mathbb{Z}))$ is a **vector space** of dimension 0 if $k<4$ and of dimension 1 when $k=4$.

Eisenstein

Modular forms of weight 4 are proportional to the **Eisenstein series**

$$E_4(q)=1+240\sum_{m=1}^{\infty}\sigma_3(m)q^{2m}$$

where $\sigma_3(m)$ is the sum of the cubes of the divisors of m.

The first even unimodular lattice is of dimension 8 and its theta series is

$$E_4(q)=1+240q^2+2160q^4+6720q^6+\cdots$$

The E_8 lattice

There is one even unimodular lattice of dimension 8, E_8 with theta series,

$$\Theta_{E_8}(q)=E_4(q)=1+240\sum_{m=1}^{\infty}\sigma_3(m)q^{2m}$$

Theta series of E_8: A Coding approach

Define

$$\begin{aligned}\vartheta_3(q) &= \sum_{k=-\infty}^{+\infty} q^{k^2} = \Theta_{\mathbb{Z}}(q)\\ \vartheta_2(q) &= \sum_{k=-\infty}^{+\infty} q^{\left(k+\frac{1}{2}\right)^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(q)\end{aligned}$$

and consider construction A,

$$\begin{aligned}\Lambda &= 2\mathbb{Z}^8 + \mathscr{C}(8,4)_{\mathbb{F}_2}\\ &= \bigcup_{\boldsymbol{x}\in\mathscr{C}} \left(2\mathbb{Z}^8 + \boldsymbol{x}\right)\end{aligned}$$

We get

$$\Theta_\Lambda(q) = \sum_{\boldsymbol{x}\in\mathscr{C}} \Theta_{2\mathbb{Z}^8+\boldsymbol{x}}(q)$$

Theta series of E_8: A Coding approach

Define

$$\begin{aligned}\vartheta_3(q) &= \sum_{k=-\infty}^{+\infty} q^{k^2} = \Theta_{\mathbb{Z}}(q)\\ \vartheta_2(q) &= \sum_{k=-\infty}^{+\infty} q^{\left(k+\frac{1}{2}\right)^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(q)\end{aligned}$$

and consider construction A,

$$\begin{aligned}\Lambda &= 2\mathbb{Z}^8 + \mathscr{C}(8,4)_{\mathbb{F}_2}\\ &= \bigcup_{\boldsymbol{x}\in\mathscr{C}} \left(2\mathbb{Z}^8 + \boldsymbol{x}\right)\end{aligned}$$

We get

$$\Theta_{\Lambda}(q) = \sum_{\boldsymbol{x}\in\mathscr{C}} \Theta_{2\mathbb{Z}^8+\boldsymbol{x}}(q)$$

We have

$$\Theta_{2\mathbb{Z}^8}(q) = \vartheta_3^8\left(q^4\right)$$

and more generally,

$$\Theta_{2\mathbb{Z}^8+\boldsymbol{x}}(q) = \vartheta_3\left(q^4\right)^{n-w(\boldsymbol{x})}\vartheta_2\left(q^4\right)^{w(\boldsymbol{x})}$$

where $w(\boldsymbol{x})$ is the Hamming weight enumerator of $\boldsymbol{x}$.

Theta series of E_8: A Coding approach

Define

$$\begin{aligned}\vartheta_3(q) &= \sum_{k=-\infty}^{+\infty} q^{k^2} = \Theta_{\mathbb{Z}}(q)\\ \vartheta_2(q) &= \sum_{k=-\infty}^{+\infty} q^{\left(k+\frac{1}{2}\right)^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(q)\end{aligned}$$

and consider construction A,

$$\begin{aligned}\Lambda &= 2\mathbb{Z}^8 + \mathscr{C}(8,4)_{\mathbb{F}_2}\\ &= \bigcup_{\boldsymbol{x}\in\mathscr{C}} \left(2\mathbb{Z}^8 + \boldsymbol{x}\right)\end{aligned}$$

We get

$$\Theta_\Lambda(q) = \sum_{\boldsymbol{x}\in\mathscr{C}} \Theta_{2\mathbb{Z}^8+\boldsymbol{x}}(q)$$

We have

$$\Theta_{2\mathbb{Z}^8}(q) = \vartheta_3^8\left(q^4\right)$$

and more generally,

$$\Theta_{2\mathbb{Z}^8+\boldsymbol{x}}(q) = \vartheta_3\left(q^4\right)^{n-w(\boldsymbol{x})}\vartheta_2\left(q^4\right)^{w(\boldsymbol{x})}$$

where $w(\boldsymbol{x})$ is the Hamming weight enumerator of $\boldsymbol{x}$.

E_8 again

Let $w_{\mathscr{C}}(x,y) = x^8 + 14x^4y^4 + y^8$ be the Hamming weight enumerator of $\mathscr{C}$, Λ has theta series,

$$\begin{aligned}\Theta_\Lambda(q) &= w_{\mathscr{C}}\left(\vartheta_3\left(q^4\right), \vartheta_2\left(q^4\right)\right)\\ &= 1 + 240q^4 + 2160q^8 + 6720q^{12} + \cdots\end{aligned}$$

In fact, $\Lambda = \sqrt{2}E_8$.

Extremal Lattices

Theorem

The theta series of an even unimodular lattice, $\Theta_\Lambda(q)$ is an ***isobaric polynomial*** *in E_4 and Δ_{24} where*

$$\begin{aligned}\Delta_{24}(q) &= q\prod_{m=1}^{\infty}\left(1-q^m\right)^{24}\\ &= q-24q^2+252q^3-\cdots\end{aligned}$$

is the Ramanujan form (of weight 12) and even unimodular lattices exist iff their dimension $n\equiv 0\,(8)$.

More precisely, let $n=24m+8k$, with $k\in\{0,1,2\}$;

$$\boxed{\Theta_\Lambda = E_4^{3m+k}+\sum_{j=1}^{m} a_j E_4^{3(m-j)+k}\Delta_{24}^j}$$

Extremal Lattices

Theorem

The theta series of an even unimodular lattice, $\Theta_\Lambda(q)$ is an ***isobaric polynomial*** *in E_4 and Δ_{24} where*

$$\begin{aligned}\Delta_{24}(q) &= q\prod_{m=1}^{\infty}\left(1-q^m\right)^{24}\\ &= q-24q^2+252q^3-\cdots\end{aligned}$$

is the Ramanujan form (of weight 12) and even unimodular lattices exist iff their dimension $n\equiv 0\,(8)$.

More precisely, let $n=24m+8k$, with $k\in\{0,1,2\}$;

$$\boxed{\Theta_\Lambda = E_4^{3m+k}+\sum_{j=1}^{m} a_j E_4^{3(m-j)+k}\Delta_{24}^j}$$

Leech lattice Λ_{24}

We get

$$\begin{aligned}\Theta_{\Lambda_{24}} &= E_4^3+a_1\Delta_{24}\\ &= 1+q^2\left(a_1+720\right)+\cdots\end{aligned}$$

In order to maximize the minimum distance, we choose $a_1=-720$, which gives

$$\begin{aligned}\Theta_{\Lambda_{24}} &= E_4^3-720\Delta_{24}\\ &= 1+196560q^4+16773120q^6+\cdots\end{aligned}$$

Extremal Lattices

Theorem

The theta series of an even unimodular lattice, $\Theta_\Lambda(q)$ is an ***isobaric polynomial*** *in E_4 and Δ_{24} where*

$$\begin{aligned}\Delta_{24}(q) &= q\prod_{m=1}^{\infty}(1-q^m)^{24}\\ &= q-24q^2+252q^3-\cdots\end{aligned}$$

is the Ramanujan form (of weight 12) and even unimodular lattices exist iff their dimension $n\equiv 0\,(8)$.

More precisely, let $n=24m+8k$, with $k\in\{0,1,2\}$;

$$\boxed{\Theta_\Lambda = E_4^{3m+k}+\sum_{j=1}^{m} a_j E_4^{3(m-j)+k}\Delta_{24}^j}$$

Leech lattice Λ_{24}

We get

$$\begin{aligned}\Theta_{\Lambda_{24}} &= E_4^3+a_1\Delta_{24}\\ &= 1+q^2(a_1+720)+\cdots\end{aligned}$$

In order to maximize the minimum distance, we choose $a_1=-720$, which gives

$$\begin{aligned}\Theta_{\Lambda_{24}} &= E_4^3-720\Delta_{24}\\ &= 1+196560q^4+16773120q^6+\cdots\end{aligned}$$

The minimum distance of an even unimodular lattice is upperbounded,

$$d_{\min}^2\le 2m+2.$$

Extremal lattices achieve this bound.

Outline

Constructions based on $\mathbb{Z}$

The Binary case

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$. $1 \in \mathbb{Z}$ is the coset representative of smallest Euclidean weight of $1 \in \mathbb{F}_2$. Construction A is

$$\sqrt{2}\Lambda = 2\mathbb{Z}^n + \mathscr{C}(n,k)_{\mathbb{F}_2}.$$

- Λ is unimodular iff $\mathscr{C}$ is **self dual** (so $k = \frac{n}{2}$ and $\mathscr{C}^{\perp} = \mathscr{C}$).
- Moreover, Λ is even when $\mathscr{C}$ is **doubly even** (all Hamming weights are multiple of 4).
- $d^2_{\min}(\Lambda) \le 2$.

Constructions based on $\mathbb{Z}$

The Binary case

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$. $1 \in \mathbb{Z}$ is the coset representative of smallest Euclidean weight of $1 \in \mathbb{F}_2$. Construction A is

$$\sqrt{2}\Lambda = 2\mathbb{Z}^n + \mathscr{C}(n,k)_{\mathbb{F}_2}.$$

- Λ is unimodular iff $\mathscr{C}$ is **self dual** (so $k = \frac{n}{2}$ and $\mathscr{C}^\perp = \mathscr{C}$).
- Moreover, Λ is even when $\mathscr{C}$ is **doubly even** (all Hamming weights are multiple of 4).
- $d^2_{\min}(\Lambda) \leq 2$.

Lattice E_8

The most famous construction of E_8 is

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

where $\mathscr{C}$ is the extended Hamming code.

Constructions based on $\mathbb{Z}$

The Binary case

$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$. $1 \in \mathbb{Z}$ is the coset representative of smallest Euclidean weight of $1 \in \mathbb{F}_2$. Construction A is

$$\sqrt{2}\Lambda = 2\mathbb{Z}^n + \mathscr{C}(n,k)_{\mathbb{F}_2}.$$

- Λ is unimodular iff $\mathscr{C}$ is **self dual** (so $k = \frac{n}{2}$ and $\mathscr{C}^\perp = \mathscr{C}$).
- Moreover, Λ is even when $\mathscr{C}$ is **doubly even** (all Hamming weights are multiple of 4).
- $d^2_{\min}(\Lambda) \leq 2$.

Lattice E_8

The most famous construction of E_8 is

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

where $\mathscr{C}$ is the extended Hamming code.

The quaternary case

$\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4$. Construction A is

$$2\Lambda = 4\mathbb{Z}^n + \mathscr{C}(n)_{\mathbb{Z}_4}$$

where $\mathscr{C}$ is a type II self dual code over $\mathbb{Z}_4$ (Euclidean weights multiple of 8).

- $d^2_{\min} \leq 4$.

Leech lattice Λ_{24}

Construction A:

$$2\Lambda_{24} = 4\mathbb{Z}^n + \left(QR_{24}\right)_{\mathbb{Z}_4}$$

QR_{24} is a quaternary quadratic residue code.

Constructions based on $\mathbb{Z}[\imath]$

The Binary case

$\mathbb{Z}[\imath]/2\mathbb{Z}[\imath] \simeq \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. Construction A is

$$\sqrt{2}\Lambda = 2\mathbb{Z}[\imath]^n + \mathscr{C}(n)_{\mathbb{F}_2 + u\mathbb{F}_2}.$$

- Λ is unimodular iff $\mathscr{C}$ is **self dual** (so $k = \frac{n}{2}$ and $\mathscr{C}^\perp = \mathscr{C}$).
- Λ is even when $\mathscr{C}$ has Euclidean weights multiple of 4 and $d^2_{\min} \leq 2$.

Constructions based on $\mathbb{Z}[\imath]$

The Binary case

$\mathbb{Z}[\imath]/2\mathbb{Z}[\imath] \simeq \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. Construction A is

$$\sqrt{2}\Lambda = 2\mathbb{Z}[\imath]^n + \mathscr{C}\,(n)_{\mathbb{F}_2+u\mathbb{F}_2}\,.$$

- Λ is unimodular iff $\mathscr{C}$ is **self dual** (so $k = \frac{n}{2}$ and $\mathscr{C}^{\perp} = \mathscr{C}$).
- Λ is even when $\mathscr{C}$ has Euclidean weights multiple of 4 and $d^2_{\min} \leq 2$.

Complex construction of E_8

Equivalent to binary construction D:

$$\sqrt{2}E_8 = 2\mathbb{Z}[\imath]^4 + \mathscr{C}(4)_{\mathbb{F}_2+u\mathbb{F}_2}$$

$\mathscr{C}$: "chaining" of the binary repetition code $(4,1)$ and the binary parity check code $(4,3)$,

$$\mathscr{C} = (4,1) + u\cdot(4,3).$$

Constructions based on $\mathbb{Z}[\imath]$

The Binary case

$\mathbb{Z}[\imath]/2\mathbb{Z}[\imath] \simeq \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. Construction A is

$$\sqrt{2}\Lambda = 2\mathbb{Z}[\imath]^n + \mathscr{C}(n)_{\mathbb{F}_2+u\mathbb{F}_2}.$$

- Λ is unimodular iff $\mathscr{C}$ is **self dual** (so $k = \frac{n}{2}$ and $\mathscr{C}^{\perp} = \mathscr{C}$).
- Λ is even when $\mathscr{C}$ has Euclidean weights multiple of 4 and $d^2_{\min} \leq 2$.

General case

$\mathbb{Z}[\imath]/2^m\mathbb{Z}[\imath] \simeq \mathbb{F}_2[u]/u^{2m}$. Construction A is

$$2^{\frac{m}{2}}\Lambda = 2^m\mathbb{Z}[\imath]^n + \mathscr{C}(n)_{\mathbb{F}_2[u]/u^{2m}}$$

where $\mathscr{C}$ is a self dual code with Euclidean weights multiple of 8.

Complex construction of E_8

Equivalent to binary construction D:

$$\sqrt{2}E_8 = 2\mathbb{Z}[\imath]^4 + \mathscr{C}(4)_{\mathbb{F}_2+u\mathbb{F}_2}$$

$\mathscr{C}$: “chaining” of the binary repetition code $(4,1)$ and the binary parity check code $(4,3)$,

$$\mathscr{C} = (4,1) + u\cdot(4,3).$$

Barnes-Wall BW_{32}

Construction A:

$$2BW_{32} = 4\mathbb{Z}[\imath]^{16} + \mathscr{C}(16)_{\mathbb{F}_2[u]/u^4}$$

equivalent to a binary construction D with 4 chained Reed-Müller codes of length 16.

- $d^2_{\min} = 4$: BW_{32} is extremal.

More on BW_{32}

Construction D

BW_{32} as a $\mathbb{Z}[\imath]$−lattice:

$$2BW_{32} = (1+\imath)^4\,\mathbb{Z}[\imath]^{16} + (1+\imath)^3\,\mathsf{RM}(4,3) + (1+\imath)^2\,\mathsf{RM}(4,2) + (1+\imath)\,\mathsf{RM}(4,1) + \mathsf{RM}(4,0)$$

Square minimum distance is $d^2_{\min} = 4$.

More on BW_{32}

Construction D

BW_{32} as a $\mathbb{Z}[\imath]$ −lattice:

$$2BW_{32} = (1+\imath)^4 \mathbb{Z}[\imath]^{16} + (1+\imath)^3 \mathrm{RM}(4,3) + (1+\imath)^2 \mathrm{RM}(4,2) + (1+\imath)\mathrm{RM}(4,1) + \mathrm{RM}(4,0)$$

Square minimum distance is $d^2_{\min} = 4$.

Reed-Müller codes

$\mathrm{RM}(4,r)$ is a Reed-Müller code of length 16.

- $r=0$: repetition code
- $r=1$: extended $3-$error correcting BCH code
- $r=2$: extended Hamming code
- $r=3$: parity check code

More on BW_{32}

Construction D

BW_{32} as a $\mathbb{Z}[\imath]$ −lattice:

$$2BW_{32} = (1+\imath)^4\,\mathbb{Z}[\imath]^{16} + (1+\imath)^3\,\mathrm{RM}(4,3) + (1+\imath)^2\,\mathrm{RM}(4,2) + (1+\imath)\,\mathrm{RM}(4,1) + \mathrm{RM}(4,0)$$

Square minimum distance is $d_{\min}^2 = 4$.

Reed-Müller codes

$\mathrm{RM}(4,r)$ is a Reed-Müller code of length 16.

- $r=0$: repetition code
- $r=1$: extended 3−error correcting BCH code
- $r=2$: extended Hamming code
- $r=3$: parity check code

Theta series

$32=24+8$: $m=1, k=1$ so that $d_{\min}^2 \le 2m+2=4$

$$\begin{aligned}\Theta_{BW_{32}} &= E_4^4 + a_1\Delta_{24}E_4\\ &= 1+(a_1+960)\,q^2+\cdots\end{aligned}$$

Set $a_1 = -960$,

$$\begin{aligned}\Theta_{BW_{32}} &= E_4^4 - 960\Delta_{24}E_4\\ &= 1+146880q^4+64757760q^6+\cdots\end{aligned}$$

Outline

$\ell-$modular lattices

Definition

A lattice Λ of rank n is $\ell-$**modular** if

- Λ is integral, i.e. its **Gram** matrix $\boldsymbol{B} = \boldsymbol{A}^{\top} \cdot \boldsymbol{A} \in GL_n(\mathbb{Z})$.
- There exists a similarity φ (isometry $+$ scaling) of similarity factor equal to ℓ such that

$$\varphi\left(\Lambda^{\star}\right) = \Lambda \text{ and } \left\langle \varphi(\boldsymbol{x}), \varphi(\boldsymbol{x}) \right\rangle = \ell \left\langle \boldsymbol{x}, \boldsymbol{y} \right\rangle, \ \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n.$$

- Moreover, if the square length of any point of Λ is an even integer, then Λ is an **even** $\ell-$**modular** lattice.

$\ell-$modular lattices

Definition

A lattice Λ of rank n is $\ell-$**modular** if

- Λ is integral, i.e. its **Gram** matrix $\boldsymbol{B} = \boldsymbol{A}^\top \cdot \boldsymbol{A} \in GL_n(\mathbb{Z})$.
- There exists a similarity φ (isometry + scaling) of similarity factor equal to ℓ such that
$$\varphi\left(\Lambda^\star\right) = \Lambda \text{ and } \langle \varphi(\boldsymbol{x}), \varphi(\boldsymbol{x}) \rangle = \ell \langle \boldsymbol{x}, \boldsymbol{y} \rangle,\ \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n.$$
- Moreover, if the square length of any point of Λ is an even integer, then Λ is an **even** $\ell-$**modular** lattice.

Examples

D_4 and Λ_{16} are $2-$modular, A_2 and K_{12} are $3-$modular, the Maaß lattice $(n = 8)$ is $5-$modular, the Barnes lattice $(n = 6)$ is $7-$modular. All are even.

Property

The determinant of a $\ell-$modular lattice is $\ell^{\frac{n}{2}}$.

Extremal Lattices

Theorem [Quebbemann, 1995, Quebbemann, 1997]

When $\sigma_1(\ell)$ divides 24, the theta series of a (strongly) even $\ell-$modular lattice, $\Theta_\Lambda(q)$ is an isobaric polynomial in $\Theta_{\ell,\min}(q)$ and $\Delta_\ell(q)$ where

$$\Delta_\ell(q) = \prod_{m|\ell} \eta\left(q^m\right)^{\frac{24}{\sigma_1(\ell)}}$$

$\eta(q) = q^{\frac{1}{24}} \prod_{j=1}^{\infty}\left(1-q^j\right)$ is the Dedekind eta function and $\Theta_{\ell,\min}(q)$ is the theta series of the smallest (strongly) even $\ell-$modular lattice.

Extremal Lattices

Theorem [Quebbemann, 1995, Quebbemann, 1997]

When $\sigma_1(\ell)$ divides 24, the theta series of a (strongly) even $\ell-$modular lattice, $\Theta_\Lambda(q)$ is an isobaric polynomial in $\Theta_{\ell,\min}(q)$ and $\Delta_\ell(q)$ where

$$\Delta_\ell(q) = \prod_{m|\ell} \eta\left(q^m\right)^{\frac{24}{\sigma_1(\ell)}}$$

$\eta(q) = q^{\frac{1}{24}} \prod_{j=1}^{\infty}\left(1-q^j\right)$ is the Dedekind eta function and $\Theta_{\ell,\min}(q)$ is the theta series of the smallest (strongly) even $\ell-$modular lattice.

Examples

Here are the smallest even (strongly) $\ell-$modular lattices when $\sigma_1(\ell)$ divides 24:

ℓ	1	2	3	5	7	11	23
n	8	4	2	4	2	2	2
$\Lambda_{\ell,\min}$	E_8	D_4	A_2	QQF_4	$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$	$\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$	$\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$

Table : Smallest even modular lattices (ℓ prime)

Extremal Lattices

Theorem [Quebbemann, 1995, Quebbemann, 1997]

When $\sigma_1(\ell)$ divides 24, the theta series of a (strongly) even $\ell-$modular lattice, $\Theta_\Lambda(q)$ is an isobaric polynomial in $\Theta_{\ell,\min}(q)$ and $\Delta_\ell(q)$ where

$$\Delta_\ell(q) = \prod_{m|\ell} \eta(q^m)^{\frac{24}{\sigma_1(\ell)}}$$

$\eta(q) = q^{\frac{1}{24}} \prod_{j=1}^{\infty} \left(1 - q^j\right)$ is the Dedekind eta function and $\Theta_{\ell,\min}(q)$ is the theta series of the smallest (strongly) even $\ell-$modular lattice.

Examples

Here are the smallest even (strongly) $\ell-$modular lattices when $\sigma_1(\ell)$ divides 24:

ℓ	6	14	15
n	4	4	4
$\Lambda_{\ell,\min}$	$A_2 + \sqrt{2}A_2$	$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] + \sqrt{2}\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$	$E(15)$

Table : Smallest even strongly modular lattices (ℓ composite)

ℓ−Modular Lattices ($\ell = 3$)

Smallest Lattice

Hexagonal lattice A_2 with theta series,

$$\Theta_{A_2}(q) = \vartheta_3\left(q^2\right)\vartheta_3\left(q^6\right) + \vartheta_2\left(q^2\right)\vartheta_2\left(q^6\right)$$

and

$$\Delta_3(q) = \left[\eta(q)\,\eta\left(q^3\right)\right]^6$$

Example: $\ell = 3$

More precisely, let $n = 12m + 2k$, with $k \in \{0, 1, 2, 3, 4, 5\}$;

$$\boxed{\Theta_\Lambda = \Theta_{A_2}^{6m+k} + \sum_{j=1}^{m} a_j \Theta_{A_2}^{6(m-j)+k} \Delta_3^j}$$

ℓ −Modular Lattices ($\ell = 3$)

Smallest Lattice

Hexagonal lattice A_2 with theta series,

$$\Theta_{A_2}(q) = \vartheta_3\left(q^2\right)\vartheta_3\left(q^6\right) + \vartheta_2\left(q^2\right)\vartheta_2\left(q^6\right)$$

and

$$\Delta_3(q) = \left[\eta(q)\,\eta\left(q^3\right)\right]^6$$

Example: $\ell = 3$

More precisely, let $n = 12m + 2k$, with $k \in \{0,1,2,3,4,5\}$;

$$\boxed{\Theta_\Lambda = \Theta_{A_2}^{6m+k} + \sum_{j=1}^{m} a_j \Theta_{A_2}^{6(m-j)+k} \Delta_3^j}$$

Coxeter Todd K_{12}

We get

$$\begin{aligned} \Theta_{K_{12}} &= \Theta_{A_2}^6 + a_1 \Delta_3 \\ &= 1 + q^2(a_1 + 36) + \cdots \end{aligned}$$

In order to maximize the minimum distance, we choose $a_1 = -36$, which gives

$$\begin{aligned} \Theta_{K_{12}} &= \Theta_{A_2}^6 - 36\Delta_3 \\ &= 1 + 756q^4 + 4032q^6 + 20412q^8 + \cdots \end{aligned}$$

$\ell-$Modular Lattices ($\ell = 3$)

Smallest Lattice

Hexagonal lattice A_2 with theta series,

$$\Theta_{A_2}(q) = \vartheta_3\left(q^2\right)\vartheta_3\left(q^6\right) + \vartheta_2\left(q^2\right)\vartheta_2\left(q^6\right)$$

and

$$\Delta_3(q) = \left[\eta(q)\,\eta\left(q^3\right)\right]^6$$

Example: $\ell = 3$

More precisely, let $n = 12m + 2k$, with $k \in \{0,1,2,3,4,5\}$;

$$\boxed{\Theta_\Lambda = \Theta_{A_2}^{6m+k} + \sum_{j=1}^{m} a_j \Theta_{A_2}^{6(m-j)+k} \Delta_3^j}$$

Coxeter Todd K_{12}

We get

$$\begin{aligned}\Theta_{K_{12}} &= \Theta_{A_2}^6 + a_1\Delta_3 \\ &= 1 + q^2(a_1 + 36) + \cdots\end{aligned}$$

In order to maximize the minimum distance, we choose $a_1 = -36$, which gives

$$\begin{aligned}\Theta_{K_{12}} &= \Theta_{A_2}^6 - 36\Delta_3 \\ &= 1 + 756q^4 + 4032q^6 + 20412q^8 + \cdots\end{aligned}$$

The minimum distance of an even $3-$modular lattice is upperbounded,

$$d_{\min}^2 \leq 2m + 2.$$

ℓ−modular lattices ($\ell = 7$)

Smallest Lattice

Lattice $\Lambda_{2,7} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ with theta series,

$$\Theta_{\Lambda_{2,7}}(q) = \vartheta_3\left(q^2\right)\vartheta_3\left(q^{14}\right) + \vartheta_2\left(q^2\right)\vartheta_2\left(q^{14}\right)$$

and

$$\Delta_7(q) = \left[\eta(q)\,\eta\left(q^7\right)\right]^3$$

Example: $\ell = 7$

More precisely, let $n = 6m + 2k$, with $k \in \{0, 1, 2\}$;

$$\boxed{\Theta_\Lambda = \Theta_{\Lambda_{2,7}}^{3m+k} + \sum_{j=1}^{m} a_j \Theta_{\Lambda_{2,7}}^{3(m-j)+k} \Delta_7^j}$$

$\ell-$modular lattices ($\ell = 7$)

Smallest Lattice

Lattice $\Lambda_{2,7} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ with theta series,

$$\Theta_{\Lambda_{2,7}}(q) = \vartheta_3\left(q^2\right)\vartheta_3\left(q^{14}\right) + \vartheta_2\left(q^2\right)\vartheta_2\left(q^{14}\right)$$

and

$$\Delta_7(q) = \left[\eta(q)\,\eta\left(q^7\right)\right]^3$$

Example: $\ell = 7$

More precisely, let $n = 6m + 2k$, with $k \in \{0, 1, 2\}$;

$$\boxed{\Theta_\Lambda = \Theta_{\Lambda_{2,7}}^{3m+k} + \sum_{j=1}^{m} a_j \Theta_{\Lambda_{2,7}}^{3(m-j)+k} \Delta_7^j}$$

Barnes lattice P_6

We get

$$\begin{aligned}\Theta_{P_6} &= \Theta_{\Lambda_{2,7}}^3 + a_1 \Delta_7 \\ &= 1 + q^2(a_1 + 6) + \cdots\end{aligned}$$

In order to maximize the minimum distance, we choose $a_1 = -6$, which gives

$$\begin{aligned}\Theta_{P_6} &= \Theta_{\Lambda_{2,7}}^6 - 6\Delta_7 \\ &= 1 + 42q^4 + 56q^6 + 84q^8 + 168q^{10} + \cdots\end{aligned}$$

$\ell-$modular lattices ($\ell = 7$)

Smallest Lattice

Lattice $\Lambda_{2,7} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ with theta series,

$$\Theta_{\Lambda_{2,7}}(q) = \vartheta_3\left(q^2\right)\vartheta_3\left(q^{14}\right) + \vartheta_2\left(q^2\right)\vartheta_2\left(q^{14}\right)$$

and

$$\Delta_7(q) = \left[\eta(q)\,\eta\left(q^7\right)\right]^3$$

Example: $\ell = 7$

More precisely, let $n = 6m + 2k$, with $k \in \{0, 1, 2\}$;

$$\boxed{\Theta_\Lambda = \Theta_{\Lambda_{2,7}}^{3m+k} + \sum_{j=1}^{m} a_j \Theta_{\Lambda_{2,7}}^{3(m-j)+k} \Delta_7^j}$$

Barnes lattice P_6

We get

$$\begin{aligned}\Theta_{P_6} &= \Theta_{\Lambda_{2,7}}^3 + a_1\Delta_7 \\ &= 1 + q^2(a_1 + 6) + \cdots\end{aligned}$$

In order to maximize the minimum distance, we choose $a_1 = -6$, which gives

$$\begin{aligned}\Theta_{P_6} &= \Theta_{\Lambda_{2,7}}^6 - 6\Delta_7 \\ &= 1 + 42q^4 + 56q^6 + 84q^8 + 168q^{10} + \cdots\end{aligned}$$

The minimum distance of an even $7-$modular lattice is upperbounded,

$$d_{\min}^2 \le 2m + 2.$$

$\ell-$modular lattices ($\ell = 5$)

Smallest Lattice

$4-$dimensional lattice QQF_4 with theta series,

$$\Theta_{QQF4}(q) = 1+6q^2+18q^4+24q^6+42q^8+6q^{10}+\cdots$$

and

$$\Delta_5(q) = \left[\eta(q)\,\eta\left(q^5\right)\right]^4$$

Example: $\ell = 7$

More precisely, let $n = 4m+2k$, with $k \in \{0,1\}$;

$$\boxed{\Theta_\Lambda = \Theta_{5,\min}^{2m+k} + \sum_{j=1}^{m} a_j \Theta_{5,\min}^{2(m-j)+k} \Delta_5^j}$$

$\ell-$modular lattices ($\ell = 5$)

Smallest Lattice

$4-$dimensional lattice QQF_4 with theta series,

$$\Theta_{QQF4}(q) = 1+6q^2+18q^4+24q^6+42q^8+6q^{10}+\cdots$$

and

$$\Delta_5(q) = \left[\eta(q)\,\eta\left(q^5\right)\right]^4$$

Example: $\ell = 7$

More precisely, let $n = 4m+2k$, with $k \in \{0,1\}$;

$$\boxed{\Theta_\Lambda = \Theta_{5,\min}^{2m+k} + \sum_{j=1}^{m} a_j \Theta_{5,\min}^{2(m-j)+k} \Delta_5^j}$$

Maaß lattice M_8

We get

$$\begin{aligned} \Theta_{M_8} &= \Theta_{5,\min}^2 + a_1 \Delta_5 \\ &= 1 + q^2\,(a_1+12) + \cdots \end{aligned}$$

In order to maximize the minimum distance, we choose $a_1 = -6$, which gives

$$\begin{aligned} \Theta_{M_8} &= \Theta_{5,\min}^6 - 12\Delta_5 \\ &= 1 + 120q^4 + 240q^6 + 600q^8 + \cdots \end{aligned}$$

$\ell-$modular lattices ($\ell = 5$)

Smallest Lattice

$4-$dimensional lattice QQF_4 with theta series,

$$\Theta_{QQF4}(q) = 1+6q^2+18q^4+24q^6+42q^8+6q^{10}+\cdots$$

and

$$\varDelta_5(q) = \left[\eta(q)\,\eta\left(q^5\right)\right]^4$$

Example: $\ell = 7$

More precisely, let $n = 4m+2k$, with $k \in \{0,1\}$;

$$\boxed{\Theta_\Lambda = \Theta_{5,\min}^{2m+k} + \sum_{j=1}^{m} a_j \Theta_{5,\min}^{2(m-j)+k} \varDelta_5^j}$$

Maaß lattice M_8

We get

$$\begin{aligned}\Theta_{M_8} &= \Theta_{5,\min}^2 + a_1 \varDelta_5\\ &= 1 + q^2(a_1+12) + \cdots\end{aligned}$$

In order to maximize the minimum distance, we choose $a_1 = -6$, which gives

$$\begin{aligned}\Theta_{M_8} &= \Theta_{5,\min}^6 - 12\varDelta_5\\ &= 1 + 120q^4 + 240q^6 + 600q^8 + \cdots\end{aligned}$$

The minimum distance of an even $5-$modular lattice is upperbounded,

$$d_{\min}^2 \leq 2m+2.$$

Outline

Modular lattices $\ell = 3$

Construction A

Let $\zeta = \frac{1+\sqrt{-3}}{2}$. Then, construction

$$\sqrt{2}\Lambda = 2\mathbb{Z}\left[\zeta\right]^n + \mathscr{C}\left(n,k\right)_{\mathbb{F}_4}$$

gives an Hermitian $\mathbb{Z}\left[\zeta\right]-$lattice. Its trace lattice is a $\mathbb{Z}-$lattice which is $3-$modular when $\mathscr{C}$ is self dual (with $k = \frac{n}{2}$) for the Hermitian product over $\mathbb{F}_4$ ($d^2_{\text{min}}\left(\Lambda\right) \leq 4$).

Mapping

We have $\mathbb{Z}\left[\zeta\right]/2\mathbb{Z}\left[\zeta\right] \simeq \mathbb{F}_4$ since 2 is inert in $\mathbb{Z}\left[\zeta\right]$.

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}\left[\zeta\right]/2\mathbb{Z}\left[\zeta\right]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

Modular lattices $\ell = 3$

Construction A

Let $\zeta = \frac{1+\sqrt{-3}}{2}$. Then, construction

$$\sqrt{2}\Lambda = 2\mathbb{Z}\left[\zeta\right]^n + \mathscr{C}\left(n,k\right)_{\mathbb{F}_4}$$

gives an Hermitian $\mathbb{Z}\left[\zeta\right]-$lattice. Its trace lattice is a $\mathbb{Z}-$lattice which is $3-$modular when $\mathscr{C}$ is self dual (with $k = \frac{n}{2}$) for the Hermitian product over $\mathbb{F}_4$ ($d^2_{\min}\left(\Lambda\right) \leq 4$).

Mapping

We have $\mathbb{Z}\left[\zeta\right]/2\mathbb{Z}\left[\zeta\right] \simeq \mathbb{F}_4$ since 2 is inert in $\mathbb{Z}\left[\zeta\right]$.

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}\left[\zeta\right]/2\mathbb{Z}\left[\zeta\right]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

Construction of K_{12}

Let $\mathscr{C}$ be the $(6,3)$ hexacode over $\mathbb{F}_4$. Then, the trace lattice of

$$2\mathbb{Z}\left[\zeta\right]^6 + \mathscr{C}\left(6,3\right)_{\mathbb{F}_4}$$

is equivalent to K_{12}.

Modular lattices $\ell = 3$

Construction A

Let $\zeta = \frac{1+\sqrt{-3}}{2}$. Then, construction

$$\sqrt{2}\Lambda = 2\mathbb{Z}[\zeta]^n + \mathscr{C}(n,k)_{\mathbb{F}_4}$$

gives an Hermitian $\mathbb{Z}[\zeta]$−lattice. Its trace lattice is a $\mathbb{Z}$−lattice which is 3−modular when $\mathscr{C}$ is self dual (with $k = \frac{n}{2}$) for the Hermitian product over $\mathbb{F}_4$ ($d^2_{\min}(\Lambda) \leq 4$).

Mapping

We have $\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta] \simeq \mathbb{F}_4$ since 2 is inert in $\mathbb{Z}[\zeta]$.

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

Construction of K_{12}

Let $\mathscr{C}$ be the $(6,3)$ hexacode over $\mathbb{F}_4$. Then, the trace lattice of

$$2\mathbb{Z}[\zeta]^6 + \mathscr{C}(6,3)_{\mathbb{F}_4}$$

is equivalent to K_{12}.

Hexacode

Self dual MDS code of length 6 over $\mathbb{F}_4$ with generator matrix,

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix}$$

K_{12}: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

K_{12}: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

Cosets theta series

- Coset 0 has theta series

$$\theta_{=0}(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{12}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{12}\right)$$

- Other cosets have theta series

$$\theta_{\neq 0}(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{12}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{12}\right)$$

K_{12}: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

Hexacode

Hamming weight enumeration is

$$w_H(x,y) = x^6 + 45x^2y^4 + 18y^6$$

Cosets theta series

- Coset 0 has theta series

$$\theta_{=0}(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{12}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{12}\right)$$

- Other cosets have theta series

$$\theta_{\neq 0}(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{12}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{12}\right)$$

K_{12}: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta]$	0	1	ζ	ζ^2
w_E^2	0	2	2	2

Table : Coset representatives

Cosets theta series

- Coset 0 has theta series

$$\theta_{=0}(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{12}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{12}\right)$$

- Other cosets have theta series

$$\theta_{\neq 0}(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{12}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{12}\right)$$

Hexacode

Hamming weight enumeration is

$$w_H(x,y) = x^6 + 45x^2y^4 + 18y^6$$

Theta series

We get

$$\begin{aligned}\Theta_{K_{12}}(q) &= w_H\left(\theta_{=0}(q), \theta_{\neq 0}(q)\right) \\ &= 1 + 756q^4 + 4032q^6 + \cdots\end{aligned}$$

Modular lattices $\ell = 7$

Construction A

Let $\alpha = \frac{1+\sqrt{-7}}{2}$. Then, construction

$$\sqrt{2}\Lambda = 2\mathbb{Z}[\alpha]^n + \mathscr{C}(n)_{\mathbb{F}_2\times\mathbb{F}_2}$$

gives an Hermitian $\mathbb{Z}[\alpha]$ −lattice. Its trace lattice is a $\mathbb{Z}$−lattice which is 7−modular when $\mathscr{C}$ is self dual for the Hermitian product over $\mathbb{F}_2 \times \mathbb{F}_2$ ($d^2_{\min}(\Lambda) \leq 4$).

We have $\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha] \simeq \mathbb{F}_2 \times \mathbb{F}_2$ since 2 is split in $\mathbb{Z}[\alpha]$.

$\mathbb{F}_2 \times \mathbb{F}_2$	$0 = (0,0)$	$1 = (1,1)$	$(1,0)$	$(0,1)$
$\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$	0	1	α	$1-\alpha = \bar{\alpha}$
w_E^2	0	2	4	4

Table : Coset representatives

Modular lattices $\ell = 7$

Construction of P_6

There exists a self dual code $\mathscr{C}$ over $\mathbb{F}_2 \times \mathbb{F}_2$ such that the trace lattice of

$$2\mathbb{Z}[\alpha]^3 + \mathscr{C}(3)_{\mathbb{F}_2 \times \mathbb{F}_2}$$

is equivalent to P_6.

$\mathscr{C}(3)_{\mathbb{F}_2 \times \mathbb{F}_2}$

Self dual code of length 3 over $\mathbb{F}_2 \times \mathbb{F}_2$ defined by using the binary parity-check codes for the first bit and the repetition code for the second one.

Construction A

Let $\alpha = \frac{1+\sqrt{-7}}{2}$. Then, construction

$$\sqrt{2}\Lambda = 2\mathbb{Z}[\alpha]^n + \mathscr{C}(n)_{\mathbb{F}_2 \times \mathbb{F}_2}$$

gives an Hermitian $\mathbb{Z}[\alpha]-$lattice. Its trace lattice is a $\mathbb{Z}-$lattice which is $7-$modular when $\mathscr{C}$ is self dual for the Hermitian product over $\mathbb{F}_2 \times \mathbb{F}_2$ ($d^2_{\min}(\Lambda) \leq 4$).

We have $\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha] \simeq \mathbb{F}_2 \times \mathbb{F}_2$ since 2 is split in $\mathbb{Z}[\alpha]$.

$\mathbb{F}_2 \times \mathbb{F}_2$	$0 = (0,0)$	$1 = (1,1)$	$(1,0)$	$(0,1)$
$\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$	0	1	α	$1-\alpha = \bar{\alpha}$
w_E^2	0	2	4	4

Table : Coset representatives

P_6: From weight enumeration to theta series

Cosets theta series

- Coset 0 has theta series

$$\theta_0(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{28}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{28}\right)$$

- Coset 1 has theta series

$$\theta_1(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{28}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{28}\right)$$

- Other cosets have theta series

$$\theta_\alpha(q) = \frac{1}{2}\vartheta_2(q)\vartheta_2\left(q^7\right)$$

$\mathbb{F}_2 \times \mathbb{F}_2$	$0 = (0,0)$	$1 = (1,1)$	$(1,0)$	$(0,1)$
$\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$	0	1	α	$1-\alpha=\bar{\alpha}$
w_E^2	0	2	4	4

Table : Coset representatives

P_6: From weight enumeration to theta series

Cosets theta series

- Coset 0 has theta series

$$\theta_0(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{28}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{28}\right)$$

- Coset 1 has theta series

$$\theta_1(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{28}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{28}\right)$$

- Other cosets have theta series

$$\theta_\alpha(q) = \frac{1}{2}\vartheta_2(q)\,\vartheta_2\left(q^7\right)$$

Code over $\mathbb{F}_2 \times \mathbb{F}_2$

Symmetrized weight enumerator is

$$swe(x,y,z) = x^3 + 3y^2z + 3xz^2 + z^3$$

$\mathbb{F}_2 \times \mathbb{F}_2$	$0 = (0,0)$	$1 = (1,1)$	$(1,0)$	$(0,1)$
$\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$	0	1	α	$1-\alpha = \bar{\alpha}$
w_E^2	0	2	4	4

Table : Coset representatives

P_6: From weight enumeration to theta series

Cosets theta series

- Coset 0 has theta series

$$\theta_0(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{28}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{28}\right)$$

- Coset 1 has theta series

$$\theta_1(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{28}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{28}\right)$$

- Other cosets have theta series

$$\theta_\alpha(q) = \frac{1}{2}\vartheta_2(q)\vartheta_2\left(q^7\right)$$

Code over $\mathbb{F}_2 \times \mathbb{F}_2$

Symmetrized weight enumerator is

$$swe(x,y,z) = x^3 + 3y^2z + 3xz^2 + z^3$$

We get

$$\begin{aligned}\Theta_{P_6}(q) &= swe\left(\theta_0(q), \theta_1(q), \theta_\alpha(q)\right)\\ &= 1 + 42q^4 + 56q^6 + 84q^8 + \cdots\end{aligned}$$

$\mathbb{F}_2 \times \mathbb{F}_2$	$0 = (0,0)$	$1 = (1,1)$	$(1,0)$	$(0,1)$
$\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$	0	1	α	$1-\alpha = \bar{\alpha}$
w_E^2	0	2	4	4

Table : Coset representatives

Modular lattices $\ell = 5$

Golden ring

$\mathbb{K} = \mathbb{Q}\left(\sqrt{5}\right)$ has ring of integers $\mathscr{O}_{\mathbb{K}} = \mathbb{Z}\left[\phi\right]$ where $\phi = \frac{1+\sqrt{5}}{2}$ is the Golden ratio. Its Galois group has one non trivial element

$$\sigma : \sqrt{5} \mapsto -\sqrt{5}$$

$\mathscr{O}_{\mathbb{K}}$ is a Principal Ideal Domain.

Modular lattices $\ell = 5$

Golden ring

$\mathbb{K} = \mathbb{Q}\left(\sqrt{5}\right)$ has ring of integers $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\phi\right]$ where $\phi = \frac{1+\sqrt{5}}{2}$ is the Golden ratio. Its Galois group has one non trivial element

$$\sigma : \sqrt{5} \mapsto -\sqrt{5}$$

$\mathcal{O}_{\mathbb{K}}$ is a Principal Ideal Domain.

Embedding

Embedding in the ambient space through the canonical embedding $\upsilon : z \in \mathcal{O}_{\mathbb{K}} \mapsto \begin{pmatrix} z \\ \sigma(z) \end{pmatrix}$

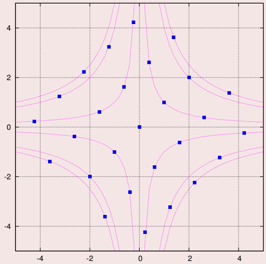


Figure : Lattice $\mathcal{O}_{\mathbb{K}}$

Modular lattices $\ell = 5$

Golden ring

$\mathbb{K} = \mathbb{Q}\left(\sqrt{5}\right)$ has ring of integers $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\phi\right]$ where $\phi = \frac{1+\sqrt{5}}{2}$ is the Golden ratio. Its Galois group has one non trivial element

$$\sigma : \sqrt{5} \mapsto -\sqrt{5}$$

$\mathcal{O}_{\mathbb{K}}$ is a Principal Ideal Domain.

Golden Lattices

Integer (in $\mathcal{O}_{\mathbb{K}}$) linear combination of a set of linearly independent vectors. A Golden lattice Λ gives rise to a $\mathbb{Z}$−lattice through the trace form

$$\boldsymbol{x}, \boldsymbol{y} \in \Lambda \mapsto \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left(\langle \boldsymbol{x}, \boldsymbol{y} \rangle\right)$$

Embedding

Embedding in the ambient space through the canonical embedding $\upsilon : z \in \mathcal{O}_{\mathbb{K}} \mapsto \begin{pmatrix} z \\ \sigma(z) \end{pmatrix}$

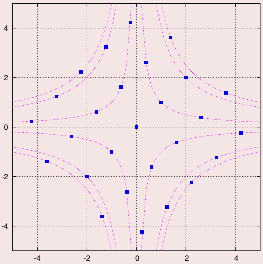


Figure : Lattice $\mathcal{O}_{\mathbb{K}}$

Modular lattices $\ell = 5$

Construction A

Construction

$$\sqrt{2}\Lambda = 2\mathbb{Z}\left[\phi\right]^n + \mathscr{C}\left(n,k\right)_{\mathbb{F}_4}$$

gives a $\mathbb{Z}\left[\phi\right]$ −lattice. Its trace lattice is a $\mathbb{Z}$−lattice which is 5−modular when $\mathscr{C}$ is self dual (with $k = \frac{n}{2}$) for the scalar product over $\mathbb{F}_4$ ($d^2_{\min}\left(\Lambda\right) \leq 4$).

Mapping

We have $\mathbb{Z}\left[\phi\right]/2\mathbb{Z}\left[\phi\right] \simeq \mathbb{F}_4$ since 2 is inert in $\mathbb{Z}\left[\phi\right]$.

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}\left[\phi\right]/2\mathbb{Z}\left[\phi\right]$	0	1	ϕ	ϕ^2
$w^2_E(x) = \mathrm{Tr}\left(x^2\right)$	0	2	3	3

Table : Coset representatives

Construction of M_8 [Hou et al., 2014]

Let $\mathscr{C}$ be a self dual $(4,2)$ over $\mathbb{F}_4$. Then, the trace lattice of

$$2\mathbb{Z}\left[\phi\right]^4 + \mathscr{C}\left(4,2\right)_{\mathbb{F}_4}$$

is 5−modular.

Choose the MDS code of length 4 over $\mathbb{F}_4$ with generator matrix,

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & \omega & \omega+1 \\ 0 & 1 & \omega+1 & \omega \end{bmatrix}$$

M_8: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\phi]/2\mathbb{Z}[\phi]$	0	1	ϕ	ϕ^2
$w_E^2(x) = \mathrm{Tr}\left(x^2\right)$	0	2	3	3

Table : Coset representatives

M_8: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\phi]/2\mathbb{Z}[\phi]$	0	1	ϕ	ϕ^2
$w_E^2(x) = \mathrm{Tr}\left(x^2\right)$	0	2	3	3

Table : Coset representatives

Cosets theta series

- Coset 0 has theta series

$$\theta_0(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{20}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{20}\right)$$

- Coset 1 has theta series

$$\theta_1(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{20}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{20}\right)$$

- Other cosets have theta series

$$\theta_\phi(q) = \frac{1}{2}\vartheta_2(q)\vartheta_2\left(q^5\right)$$

M_8: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\phi]/2\mathbb{Z}[\phi]$	0	1	ϕ	ϕ^2
$w_E^2(x) = \mathrm{Tr}(x^2)$	0	2	3	3

Table : Coset representatives

Code over $\mathbb{F}_4$

Symmetrized weight enumerator is

$$swe(x,y,z) = x^4 + 12xyz^2 + y^4 + 2z^4$$

Cosets theta series

- Coset 0 has theta series

$$\theta_0(q) = \vartheta_3\left(q^4\right)\vartheta_3\left(q^{20}\right) + \vartheta_2\left(q^4\right)\vartheta_2\left(q^{20}\right)$$

- Coset 1 has theta series

$$\theta_1(q) = \vartheta_2\left(q^4\right)\vartheta_3\left(q^{20}\right) + \vartheta_3\left(q^4\right)\vartheta_2\left(q^{20}\right)$$

- Other cosets have theta series

$$\theta_\phi(q) = \frac{1}{2}\vartheta_2(q)\vartheta_2\left(q^5\right)$$

M_8: From weight enumeration to theta series

Embedding

$\mathbb{F}_4$	0	1	ω	ω^2
$\mathbb{Z}[\phi]/2\mathbb{Z}[\phi]$	0	1	ϕ	ϕ^2
$w_E^2(x) = \mathrm{Tr}(x^2)$	0	2	3	3

Table : Coset representatives

Code over $\mathbb{F}_4$

Symmetrized weight enumerator is

$$swe(x,y,z) = x^4 + 12xyz^2 + y^4 + 2z^4$$

Cosets theta series

- Coset 0 has theta series

$$\theta_0(q) = \vartheta_3(q^4)\vartheta_3(q^{20}) + \vartheta_2(q^4)\vartheta_2(q^{20})$$

- Coset 1 has theta series

$$\theta_1(q) = \vartheta_2(q^4)\vartheta_3(q^{20}) + \vartheta_3(q^4)\vartheta_2(q^{20})$$

- Other cosets have theta series

$$\theta_\phi(q) = \frac{1}{2}\vartheta_2(q)\vartheta_2(q^5)$$

We get

$$\begin{aligned}\Theta_{M_8}(q) &= swe(\theta_0(q), \theta_1(q), \theta_\phi(q)) \\ &= 1 + 120q^4 + 240q^6 + 600q^8 + \cdots\end{aligned}$$

Outline

Large values of n (even unimodular)

Expression of the theta series

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

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

where $S_k(\tau,\Lambda)$ is a cusp form and E_k an Eisenstein series.

Large values of n (even unimodular)

Expression of the theta series

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

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

where $S_k(\tau,\Lambda)$ is a cusp form and E_k an Eisenstein series.

Fourier coefficients

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

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

Large values of n (even unimodular)

Expression of the theta series

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

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

where $S_k(\tau,\Lambda)$ is a cusp form and E_k an Eisenstein series.

Fourier coefficients

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

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

Asymptotics

Asymptotic analysis gives

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

Large values of n (even unimodular)

Expression of the theta series

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

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

where $S_k(\tau,\Lambda)$ is a cusp form and E_k an Eisenstein series.

Fourier coefficients

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

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

Asymptotics

Asymptotic analysis gives

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

Conclusion

All even unimodular lattices except a set of measure $\to 0$ have theta series

$$\boxed{\Theta_\Lambda(q) = E_k\left(q^2\right)}$$

when $k \to \infty$.

Outline

The inefficiency of binary construction A [Lin et al., 2014]

Construction

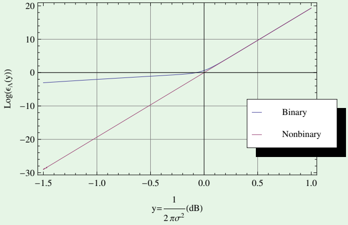
Binary construction **A** of even unimodular lattices

$$\Lambda = 2\mathbb{Z}^n + \mathscr{C}\left(n, \frac{n}{2}\right)\mathbb{F}_2$$

where $\mathscr{C}$ is doubly-even self dual.

The inefficiency of binary construction A [Lin et al., 2014]

Flatness factor (dimension 192)



Construction

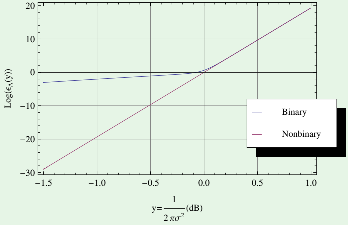
Binary construction **A** of even unimodular lattices

$$\Lambda = 2\mathbb{Z}^n + \mathscr{C}\left(n, \frac{n}{2}\right)_{\mathbb{F}_2}$$

where $\mathscr{C}$ is doubly-even self dual.

The inefficiency of binary construction A [Lin et al., 2014]

Flatness factor (dimension 192)



Construction

Binary construction **A** of even unimodular lattices

$$\Lambda = 2\mathbb{Z}^n + \mathscr{C}\left(n, \frac{n}{2}\right)_{\mathbb{F}_2}$$

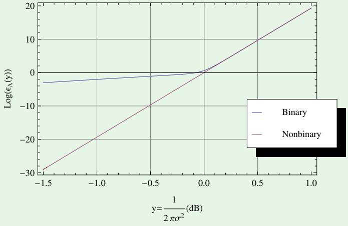
where $\mathscr{C}$ is doubly-even self dual.

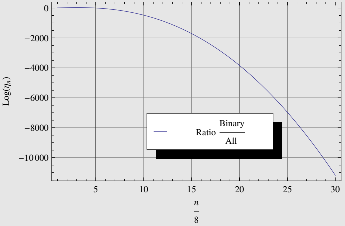
Concentration result not valid?

"All codes are good, except those we can think of." (**G. Battail**)

The inefficiency of binary construction A [Lin et al., 2014]

Flatness factor (dimension 192)





Construction

Binary construction **A** of even unimodular lattices

$$\Lambda = 2\mathbb{Z}^n + \mathscr{C}\left(n, \frac{n}{2}\right)\mathbb{F}_2$$

where $\mathscr{C}$ is doubly-even self dual.

Concentration result not valid?

”All codes are good, except those we can think of.” (**G. Battail**)

Binary lattices are very scarce

The measure of the set of binary lattices $\to 0$ when $n \to \infty$.

Asymptotics of the flatness factor

Flatness factor of an even unimodular lattice

For n large enough, randomly choose an even unimodular lattice Λ_n. Then, set $y = \frac{1}{2\pi\sigma^2}$ (and $k = \frac{n}{2}$),

$$\begin{aligned}\varepsilon_{\Lambda_n}(\sigma) &= y^{\frac{n}{2}}\Theta_{\Lambda_n}(iy) - 1 \\ &\simeq y^k E_k(iy) - 1 \\ &\simeq y^k\end{aligned}$$

Asymptotics of the flatness factor

Flatness factor of an even unimodular lattice

For n large enough, randomly choose an even unimodular lattice Λ_n. Then, set $y = \frac{1}{2\pi\sigma^2}$ (and $k = \frac{n}{2}$),

$$\begin{aligned} \varepsilon_{\Lambda_n}(\sigma) &= y^{\frac{n}{2}} \Theta_{\Lambda_n}(iy) - 1 \\ &\simeq y^k E_k(iy) - 1 \\ &\simeq y^k \end{aligned}$$

Asymptotics for even unimodular lattices

We thus get

$$\varepsilon_{\Lambda_n}(\sigma) \underset{n\to\infty}{\to} \begin{cases} 0 & \sigma^2 > \frac{1}{2\pi} \to \text{strong secrecy} \\ 1 & \sigma^2 = \frac{1}{2\pi} \\ \infty & \sigma^2 < \frac{1}{2\pi} \end{cases}$$

Perspectives

Large dimensions

Compute (at least approximately) theta series of lattices already proposed in large dimensions

- Low Density Lattice Codes [Sommer et al., 2008]
- Construction A with LDPC codes over $\mathbb{F}_p$ [di Pietro et al., 2013]
- Intersection of Λ^n and of $\pi\left(\Lambda^n\right)$ where π is a permutation of components [Boutros et al., 2014]
- Construction D with polar codes [Yan & Ling, 2012]

Perspectives

Large dimensions

Compute (at least approximately) theta series of lattices already proposed in large dimensions

- Low Density Lattice Codes [Sommer et al., 2008]
- Construction A with LDPC codes over $\mathbb{F}_p$ [di Pietro et al., 2013]
- Intersection of Λ^n and of $\pi(\Lambda^n)$ where π is a permutation of components [Boutros et al., 2014]
- Construction D with polar codes [Yan & Ling, 2012]

Medium dimensions

From the knowledge we have of theta series, construct medium dimension lattices.

Expression of the flatness factor

$$\varepsilon_{\Lambda_c}(\sigma) = \max_{\boldsymbol{x}\in\mathcal{V}(\Lambda_c)} \left| \frac{\sum_{\boldsymbol{\lambda}\in\Lambda_c} \left(\frac{1}{2\pi\sigma^2}\right)^{\frac{n}{2}} e^{-\frac{\|\boldsymbol{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}}{1/\mathrm{Vol}\left(\Lambda_c\right)} - 1 \right|.$$

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

$$\begin{aligned}
\left|\mathrm{Vol}\left(\Lambda\right) f_{\sigma,\Lambda}\left(\boldsymbol{x}\right) - 1\right| &= \left| \sum_{\boldsymbol{\lambda}^\star\in\Lambda^\star} e^{-2\pi^2\sigma^2\|\boldsymbol{\lambda}^\star\|^2} \cos\left(2\pi\left\langle\boldsymbol{\lambda}^\star,\boldsymbol{x}\right\rangle\right) - 1 \right| \\
&\le \left| \sum_{\boldsymbol{\lambda}^\star\in\Lambda^\star} e^{-2\pi^2\sigma^2\|\boldsymbol{\lambda}^\star\|^2} - 1 \right| \\
&= \mathrm{Vol}\left(\Lambda\right) f_{\sigma,\Lambda}\left(\mathbf{0}\right) - 1 \\
&= \frac{\mathrm{Vol}\left(\Lambda\right)}{\left(\sqrt{2\pi}\sigma\right)^n} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{\lambda}\|^2}{2\sigma^2}} - 1 \\
&= \frac{\mathrm{Vol}\left(\Lambda\right)}{\left(\sqrt{2\pi}\sigma\right)^n} \Theta_\Lambda\left(\frac{\imath}{2\pi\sigma^2}\right) - 1
\end{aligned}$$

References

Conway, J. & Sloane, N. (1998).
Sphere packings, Lattices and Groups.
Springer-Verlag, 3rd edition.

di Pietro, N., Boutros, J. J., Zemor, G., & Brunei, L. (2013).
New results on low-density integer lattices.
In *2013 Information Theory and Applications Workshop (ITA)* (pp. 1–6).: IEEE.

Forney, D., Trott, M. D., & Chung, S. Y. (2000).
Sphere-bound-achieving coset codes and multilevel coset codes.
IEEE Transactions on Information Theory, 46, 820–850.

Hou, X., Lin, F., & Oggier, F. (2014).
Construction and Secrecy Gain of a Family of 5-modular Lattices.
In *ITW 2014*.

Lin, F., Ling, C., & Belfiore, J.-C. (2014).
Secrecy gain, flatness factor, and secrecy-goodness of even unimodular lattices.
In *Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT)*.

Ling, C., Luzzi, L., Belfiore, J.-C., & Stehlé, D. (2012).
Semantically Secure Lattice Codes for the Gaussian Wiretap Channel.

Nebe, G. (2012).
An even unimodular 72-dimensional lattice of minimum 8.
Journal fur die Reine und Angewandte Mathematik, (pp. 237–247).

Oggier, F., Solé, P., & Belfiore, J.-C. (2011a).
Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis.

Oggier, F., Solé, P., & Belfiore, J.-C. (2011b).