Lattices and Physical-Layer Security: A finite-dimensional analysis

Jean-Claude Belfiore
Télécom ParisTech
GDR ISIS, 22 mai 2014

Parts of these results have been obtained in the framework of PHYLAWS project

Part I

Introduction

Outline

The Gaussian Wiretap Channel

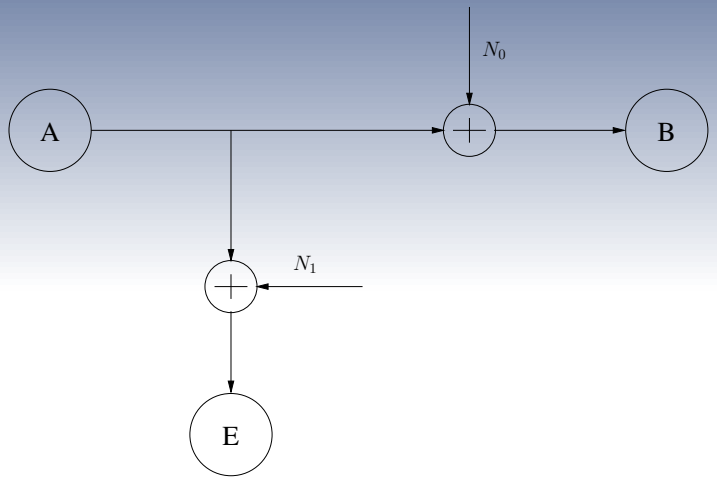


Figure : The Gaussian Wiretap Channel model

The Gaussian Wiretap Channel

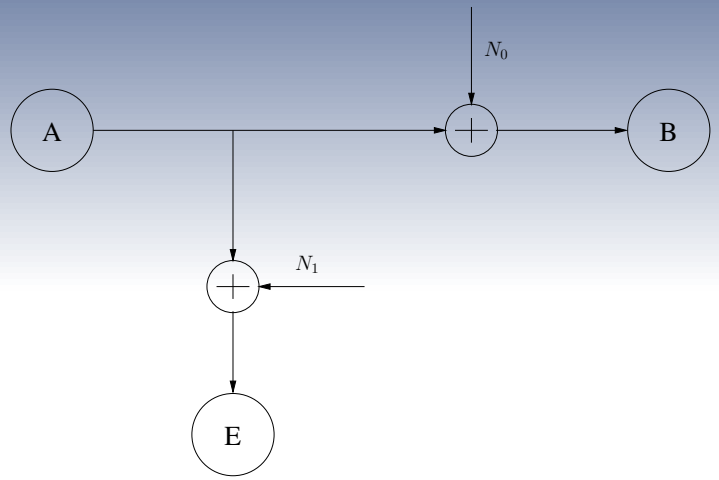


Figure : The Gaussian Wiretap Channel model

The secrecy capacity is given by

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

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

Encoder Design

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

Encoder Design

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

+2 mod (4) Channel

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

$$y = x + 2$$

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

Encoder Design

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

$+2$ **mod** (4) **Channel**

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

$$y = x + 2$$

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

Symbol to Bits Labelling

$$s = 2b_1 + b_0$$

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

Encoder Design

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

+2 mod (4) Channel

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

$$y = x + 2$$

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

Symbol to Bits Labelling

$$s = 2b_1 + b_0$$

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

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

Outline

Uniform Noise

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

Uniform Noise

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

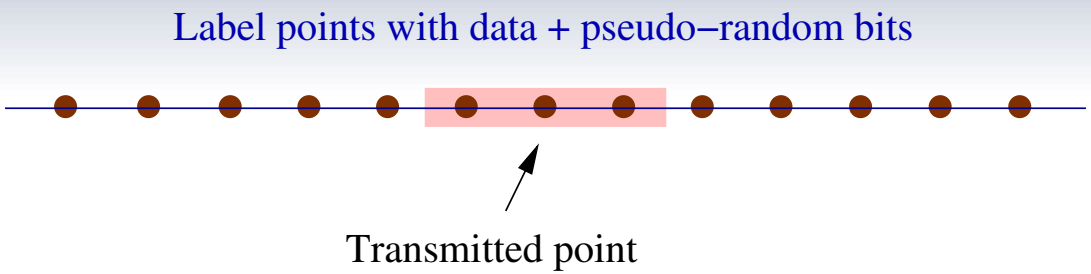


Figure : Constellation corrupted by uniform noise

Uniform Noise

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

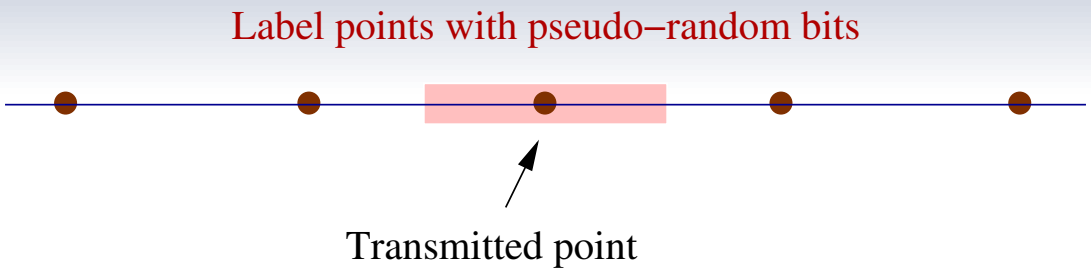


Figure : Points can be decoded **error free**: label with pseudo-random symbols

Uniform Noise

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

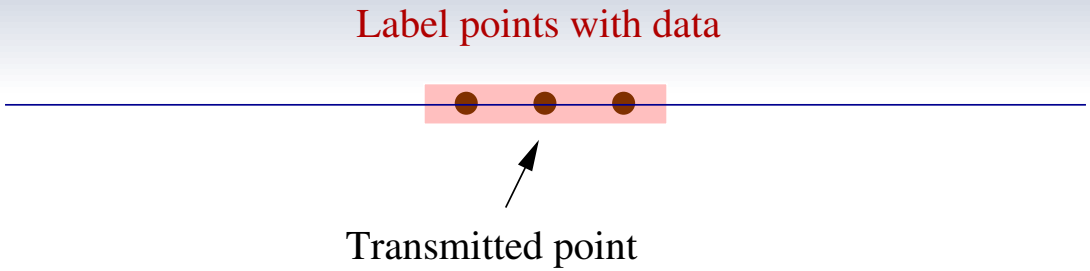


Figure : Points are **not distinguishable**: label with data

Uniform Noise

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

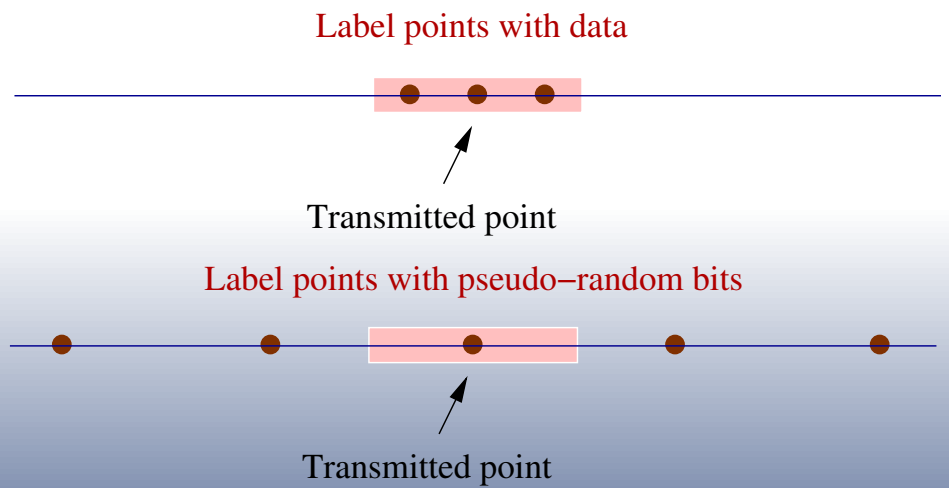


Figure : Constellation corrupted by uniform noise

Uniform Noise

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

Error Probability

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

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

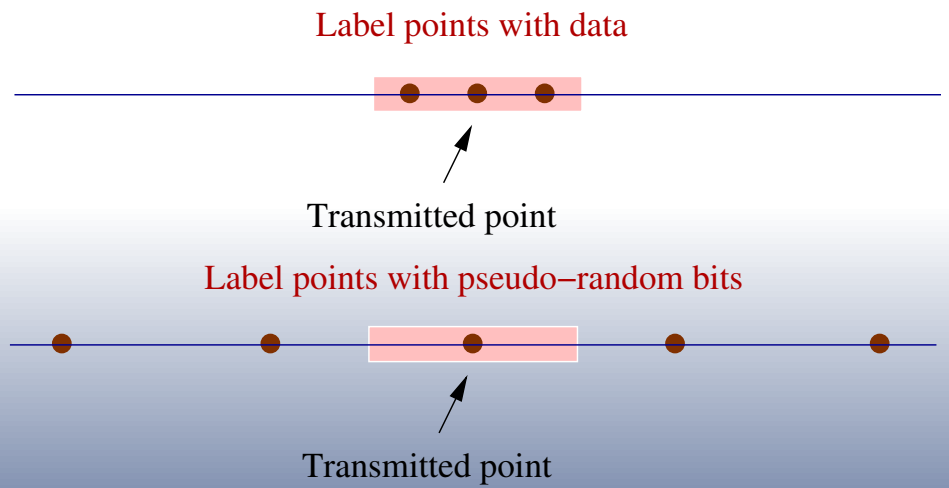


Figure : Constellation corrupted by uniform noise

Coset Coding with Integers

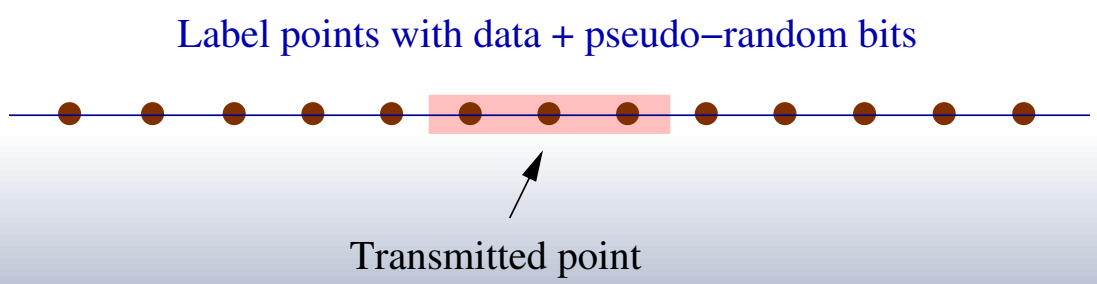


Figure : Constellation corrupted by uniform noise

Coset Coding with Integers

Example

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

$$x = 3q + r$$

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

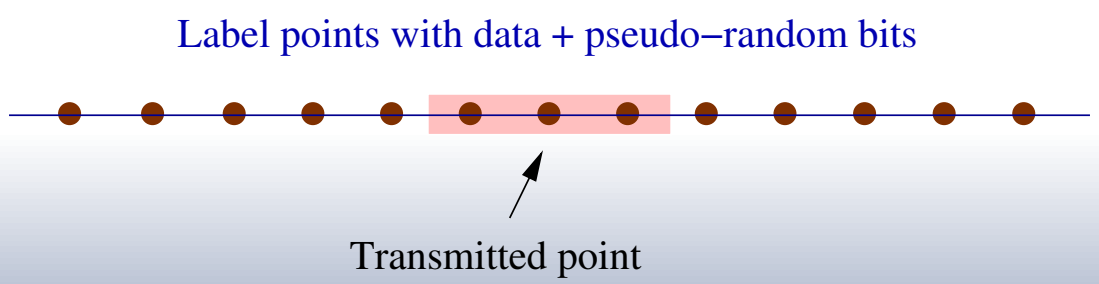


Figure : Constellation corrupted by uniform noise

Lattice Coset Coding

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

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

Table : From the example to the general scheme

Part II

Secrecy Gain and Flatness Factor

Outline

Eve's Probability of Correct Decision (data)

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

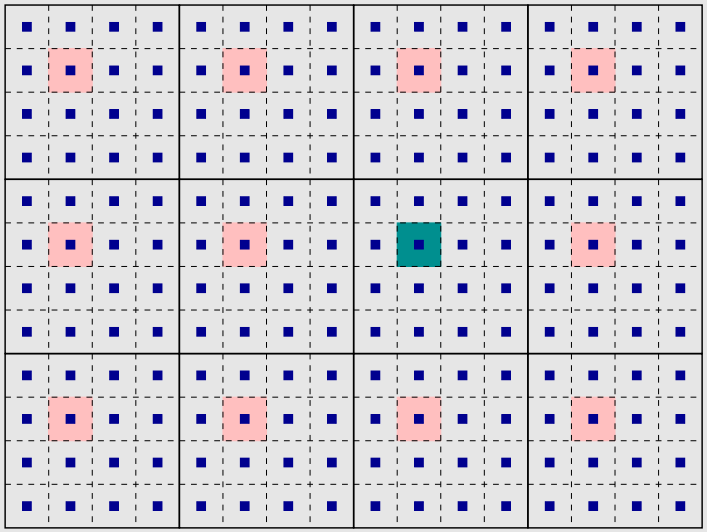


Figure : Eve correctly decodes when finding another coset representative

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

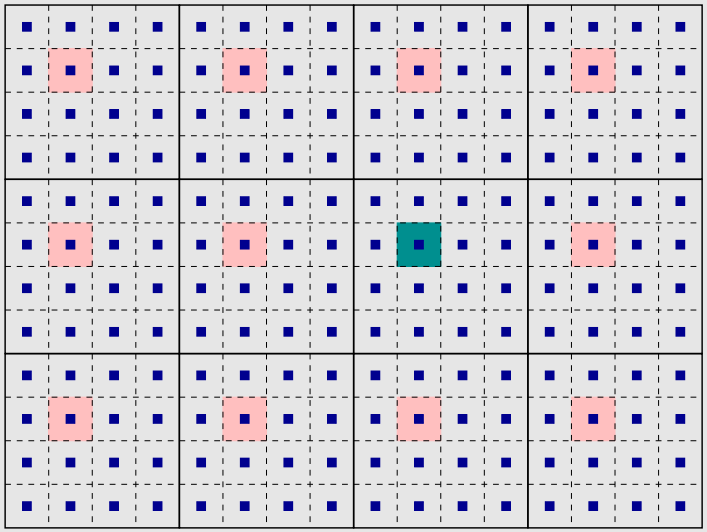


Figure : Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision

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

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

where

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

is the **theta series** of Λ.

Eve's Probability of Correct Decision (data)

Can Eve decode the data?

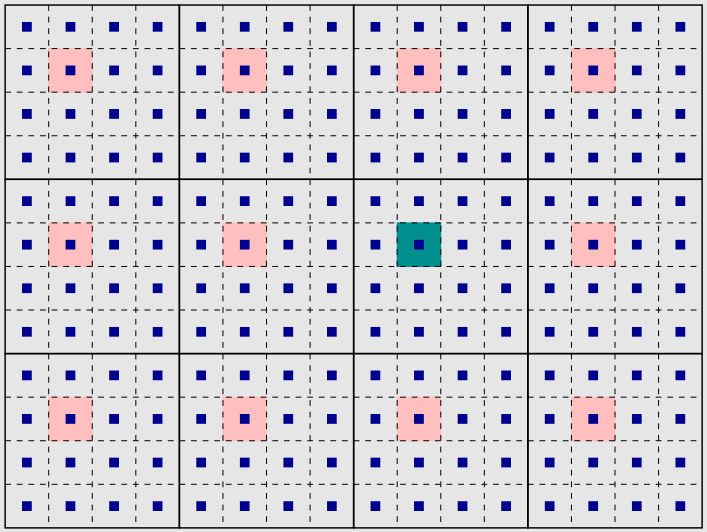


Figure : Eve correctly decodes when finding another coset representative

Eve's Probability of correct decision

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

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

where

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

is the **theta series** of Λ.

Problem

Find Λ minimizing $\Theta_\Lambda(y)$.

Secrecy function

Definition

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

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

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

Secrecy function

Definition

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

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

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

Examples

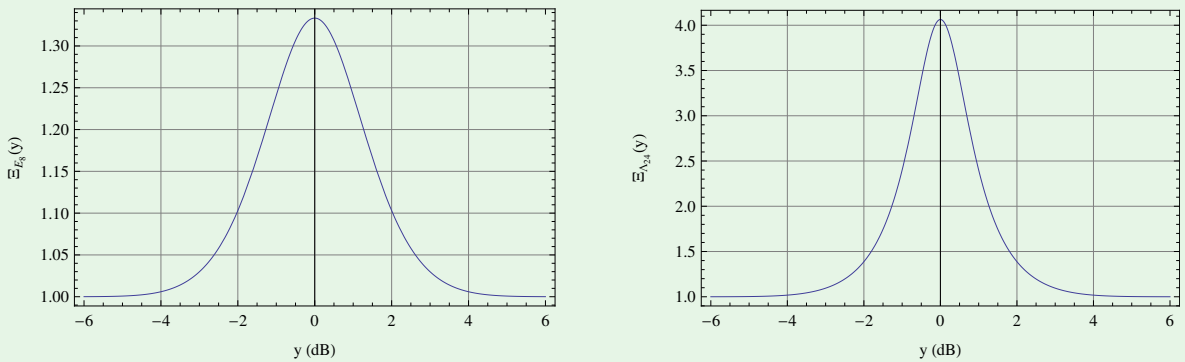


Figure : Secrecy functions of E_8 and Λ_{24}

Secrecy Gain

Definition

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

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

Secrecy Gain

Definition

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

$$\chi^s_\Lambda \triangleq \sup_{y>0} \Xi_\Lambda(y)$$

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

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

Secrecy Gain

Definition

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

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

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

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

Definition

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

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

Conjecture

Conjecture

If Λ is a unimodular lattice, then the strong and the weak secrecy gains coincide.

Corollary

The strong secrecy gain of a unimodular lattice Λ is $\chi^s_\Lambda \triangleq \Xi_\Lambda(1)$.

Conjecture

Conjecture

If Λ is a unimodular lattice, then the strong and the weak secrecy gains coincide.

Corollary

The strong secrecy gain of a unimodular lattice Λ is $\chi_\Lambda^s \triangleq \Xi_\Lambda(1)$.

Calculation of E_8 secrecy gain

From E_8 theta series,

$$\frac{1}{\Xi_{E_8}(1)} = \frac{\frac{1}{2}\left(\vartheta_2(e^{-\pi})^8 + \vartheta_3(e^{-\pi})^8 + \vartheta_4(e^{-\pi})^8\right)}{\vartheta_3(e^{-\pi})^8}$$

$$= \frac{3}{4} \quad \left(\text{since } \frac{\vartheta_2\left(e^{-\pi}\right)}{\vartheta_3\left(e^{-\pi}\right)} = \frac{\vartheta_4\left(e^{-\pi}\right)}{\vartheta_3\left(e^{-\pi}\right)} = \frac{1}{\sqrt[4]{2}}\right)$$

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

Part III

Even Unimodular Lattices

Outline

Even Unimodular Lattices

Example

E_8 or the Leech lattice Λ_{24} are even unimodular.

Even Unimodular Lattices

Example

E_8 or the Leech lattice Λ_{24} are even unimodular.

Properties

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

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

where $n = 24m + 8k$, $k = 0, 1, 2$. A lattice achieving this upperbound is called **extremal**. E_8 and Leech lattice are extremal.

Secrecy Gain of Extremal Lattices

Secrecy Functions in dimensions 72 and 80

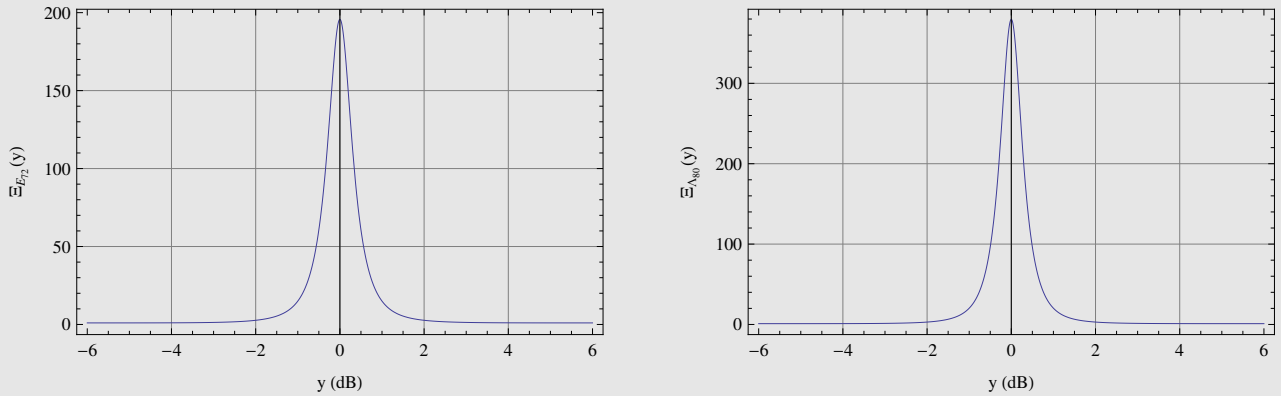


Figure : Secrecy functions of extremal lattices ($n = 72, 80$)

Secrecy Gain of Extremal Lattices

Secrecy Functions in dimensions 72 and 80

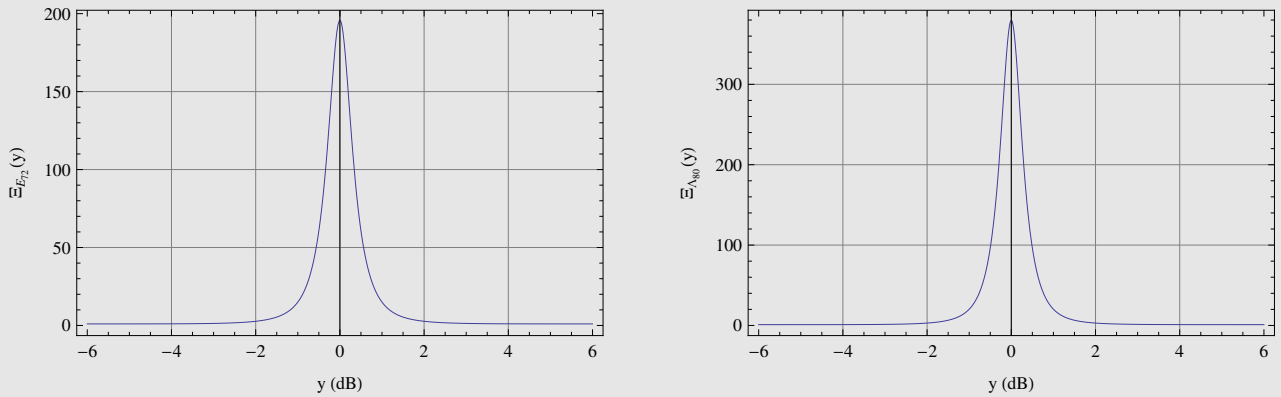


Figure : Secrecy functions of extremal lattices ($n = 72, 80$)

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

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

Secrecy Gain of extremal Even Unimodular Lattices

Theorem

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

Secrecy Gain of extremal Even Unimodular Lattices

Theorem

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

Proof.

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

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

with $E_4 = \frac{1}{2}\left(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8\right)$, $\Delta = \frac{1}{256}\left(\vartheta_2\vartheta_3\vartheta_4\right)^8$ and $b_j \in \mathbb{C}$. As the lattice is extremal, b_j are computed by solving a linear system with integer coefficients, so $b_j \in \mathbb{Q}$. As

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

we obtain

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

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

Asymptotic behavior (I)

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

Question

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

Asymptotic behavior (I)

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

Question

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

First answer

Apply the Siegel-Weil formula,

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

where

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

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

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

Asymptotic behavior (II)

Maximal Secrecy gain

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

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

Asymptotic behavior (II)

Maximal Secrecy gain

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

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

Behavior of Eisenstein Series

We have

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

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

Asymptotic behavior (II)

Maximal Secrecy gain

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

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

Behavior of Eisenstein Series

We have

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

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

Bound from Siegel-Weil Formula vs. Extremal lattices

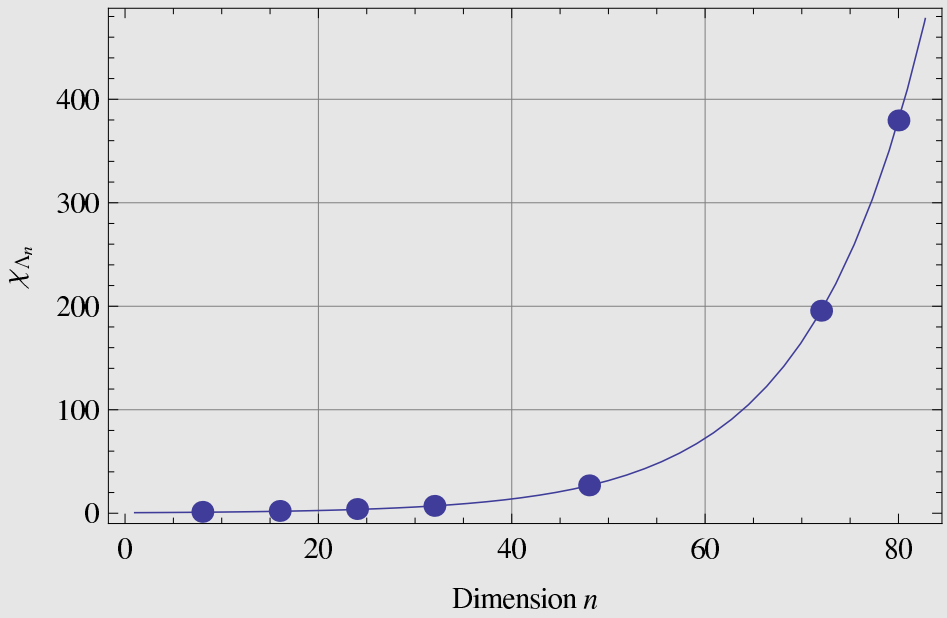


Figure : Lower bound of the minimal secrecy gain as a function of n from Siegel-Weil formula. **Points** correspond to **extremal lattices**.

Another way of analyzing the asymptotic behavior

Expression of the theta series

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

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

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

Another way of analyzing the asymptotic behavior

Expression of the theta series

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

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

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

Fourier coefficients

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

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

Another way of analyzing the asymptotic behavior

Expression of the theta series

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

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

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

Fourier coefficients

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

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

Asymptotics

Asymptotic analysis gives

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

Another way of analyzing the asymptotic behavior

Expression of the theta series

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

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

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

Fourier coefficients

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

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

Asymptotics

Asymptotic analysis gives

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

Conclusion

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

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

when $k \to \infty$.

Outline

Flatness Factor

Information Leakage

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

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

where

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

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

Flatness Factor

Information Leakage

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

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

where

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

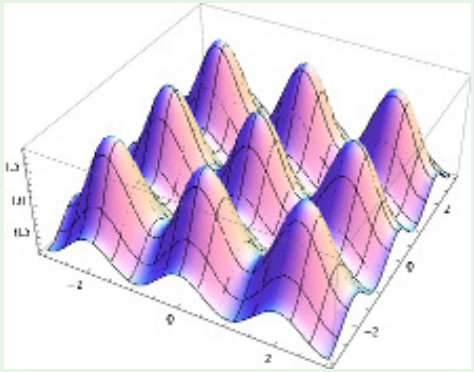
is the **flatness factor** of the lattice Λ_n.

Remark

True definition of the flatness factor is

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

Intuition



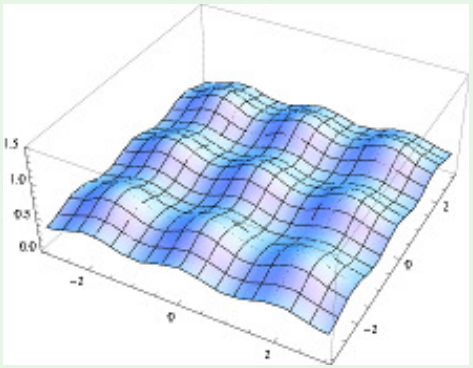
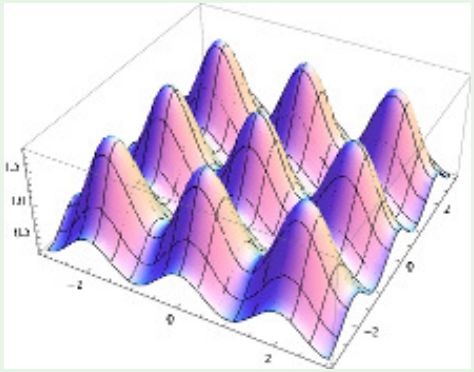


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

Intuition



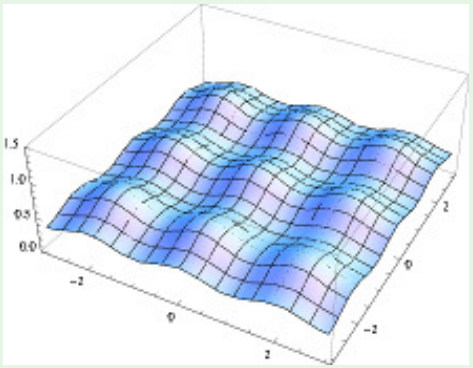


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

Goal

Is it possible to obtain a vanishing flatness factor? For which values of σ?

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 $k = \frac{n}{2}$),

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

Strong secrecy for even unimodular lattices

We thus get

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

Outline

Construction A

Construction A using $\mathbb{Z}$

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

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

Construction A

Construction A using $\mathbb{Z}$

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

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

Construction of D_4

D_4 is obtained as

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

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

Construction A

Construction A using $\mathbb{Z}$

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

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

Construction of D_4

D_4 is obtained as

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

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

Construction of E_8

E_8 is obtained as

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

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

Construction A (quaternary)

Construction A of the Leech lattice

The **Leech lattice** can be obtained as

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

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

Construction A (quaternary)

Construction A of the Leech lattice

The **Leech lattice** can be obtained as

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

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

Other constructions

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

Constructions with codes

Binary construction A

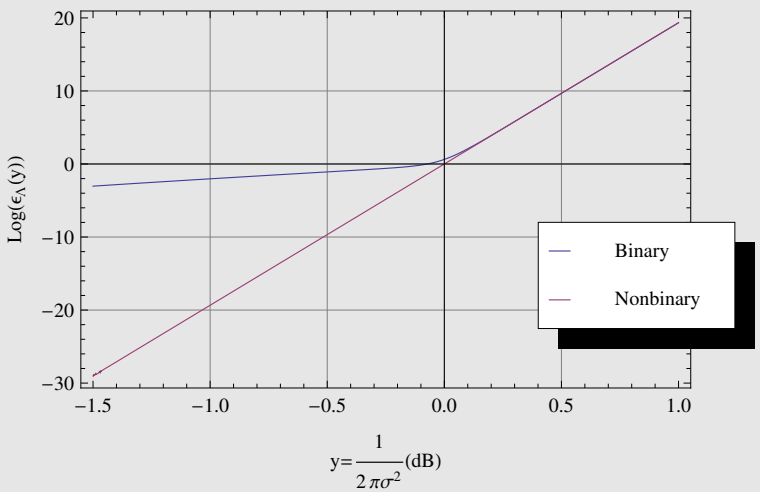


Figure : Even Unimodular Lattice in dimension 168: binary **vs** general case

Constructions with codes

Binary construction A

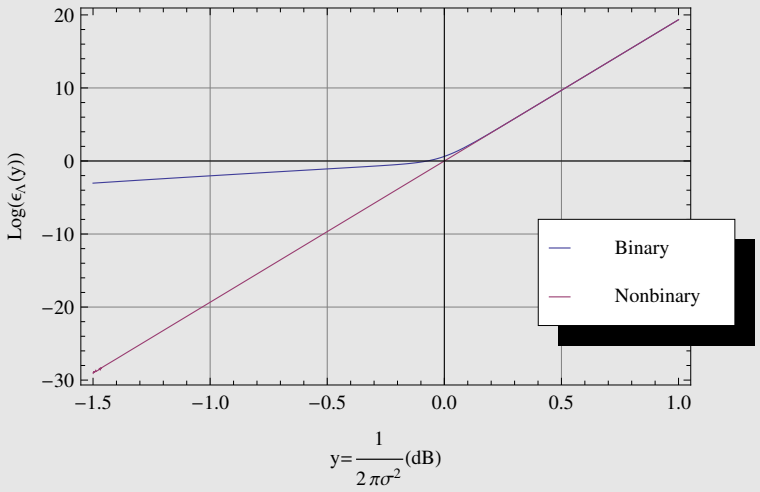


Figure : Even Unimodular Lattice in dimension 168: binary **vs** general case

Binary lattices: a set of negligible measure

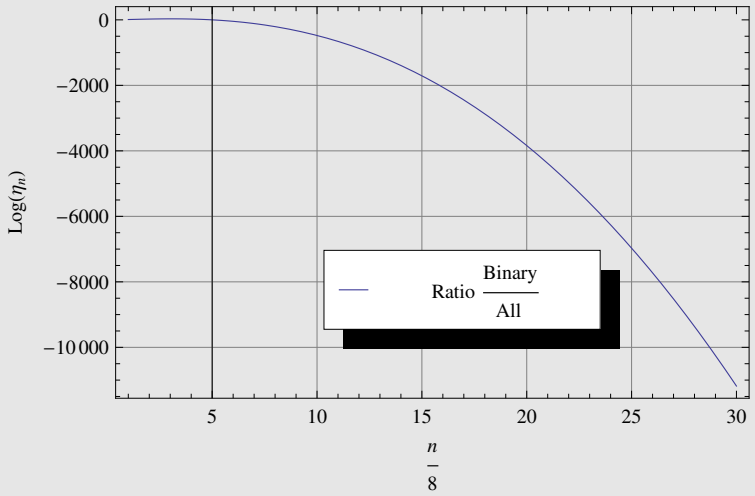


Figure : Binary Even Unimodular Lattice : How many they are?